
**ID:** 432891
**Sample Name:** nmap-7.91-setup.exe
**Cookbook:** default.jbs
**Time:** 21:53:42
**Date:** 10/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

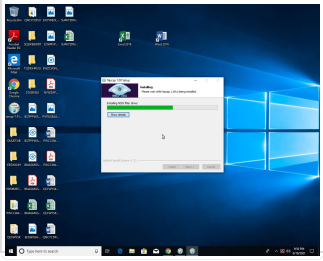
# Analysis Report nmap-7.91-setup.exe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | nmap-7.91-setup.exe |
| Analysis ID: | 432891 |
| MD5: | 5df3bf0234f0c2a… |
| SHA1: | 7474a3c2c44e61.. |
| SHA256: | c4683097a26152.. |
| Infos: | |

Most interesting Screenshot:



### Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

HTMLPhisher
Predator

| | |
|---|---|
| Score: | 40 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Compliance

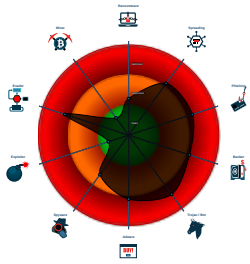
HIGH
MODERATE
LOW

| | |
|---|---|
| Score: | 50 |
| Range: | 0 - 100 |

### Signatures

- Yara detected HtmlPhish10
- Yara detected Predator
- Changes security center settings (no…
- Contains VNC / remote desktop func…
- Install WinpCap (used to filter netwo…
- NDIS Filter Driver detected (likely us…
- Uses schtasks.exe or at.exe to add …
- Yara detected Ncat Network tool
- AV process strings found (often use…
- Antivirus or Machine Learning detec…
- Checks if Antivirus/Antispyware/Fire…
- Contains capabilities to detect virtua…
- Contains functionality for read data f…

### Classification



## Process Tree

- **System is w10x64**
- nmap-7.91-setup.exe (PID: 2432 cmdline: 'C:\Users\user\Desktop\nmap-7.91-setup.exe' MD5: 5DF3BF0234F0C2AF2C470F98243C788F)
  - npcap-1.00.exe (PID: 5912 cmdline: 'C:\Users\user\AppData\Local\Temp\nsyA5D0.tmp\npcap-1.00.exe' /loopback_support=no MD5: FC8CB1B4677C90859AF51C8C664E755D)
    - NPFInstall.exe (PID: 2024 cmdline: 'C:\Users\user\AppData\Local\Temp\nsb823.tmp\NPFInstall.exe' -n -check_dll MD5: F93EEDCB0DF2EF914ED51CC927A1FDE9)
      - conhost.exe (PID: 2224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - NPFInstall.exe (PID: 2052 cmdline: 'C:\Program Files\Npcap\NPFInstall.exe' -n -c MD5: F93EEDCB0DF2EF914ED51CC927A1FDE9)
      - conhost.exe (PID: 4864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - pnputil.exe (PID: 4008 cmdline: pnputil.exe -e MD5: F4C3BD7A47ACE4BEE4D864B299391DC1)
        - conhost.exe (PID: 4152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - NPFInstall.exe (PID: 6052 cmdline: 'C:\Program Files\Npcap\NPFInstall.exe' -n -iw MD5: F93EEDCB0DF2EF914ED51CC927A1FDE9)
      - conhost.exe (PID: 3032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - NPFInstall.exe (PID: 5212 cmdline: 'C:\Program Files\Npcap\NPFInstall.exe' -n -i MD5: F93EEDCB0DF2EF914ED51CC927A1FDE9)
      - conhost.exe (PID: 404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4876 cmdline: SCHTASKS.EXE /Create /F /RU SYSTEM /SC ONSTART /TN npcapwatchdog /TR "C:\Program Files\Npcap\CheckStatus.bat" /NP MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 4696 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1288 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3688 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4348 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5044 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3224 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6128 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5512 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 1956 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6024 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4744 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s NetSetupSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5204 cmdline: c:\windows\system32\svchost.exe -k dcomlaunch -p -s DeviceInstall MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - drvinst.exe (PID: 5216 cmdline: DrvInst.exe '4' '0' 'C:\Users\user\AppData\Local\Temp\{7e40bce9-63ed-3549-a69d-3044b7b23662}\NPCAP.inf' '9' '405306be3' '0000000000001A8' 'WinSta0\Default' '00000000000001AC' '208' 'C:\Program Files\Npcap' MD5: 46F5A16FA391AB6EA97C602B4D2E7819)
- **cleanup**

## Malware Configuration

No configs have been found

# Yara Overview

## Dropped Files

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| C:\Program Files (x86)\Nmap\nselib\data\http-fingerprints.lua | Hacktool_Strings_p0wnedShell | p0wnedShell Runspace Post Exploitation Toolkit - file p0wnedShell.cs | Florian Roth | • 0x152c6:$x2: windows/meterpreter |
| C:\Program Files (x86)\Nmap\nmap-service-probes | JoeSecurity_HtmlPhish_10 | Yara detected HtmlPhish_10 | Joe Security | |
| C:\Users\user\AppData\Local\Temp\nsyA5CF.tmp | Hacktool_Strings_p0wnedShell | p0wnedShell Runspace Post Exploitation Toolkit - file p0wnedShell.cs | Florian Roth | • 0x179e2a7:$x2: windows/meterpreter |
| C:\Users\user\AppData\Local\Temp\nsyA5CF.tmp | iKAT_tools_nmap | Generic rule for NMAP - based on NMAP 4 standalone | Florian Roth | • 0xc816e9:$s0: Insecure.Org<br>• 0x42c9762:$s1: Copyright (c) Insecure.Com<br>• 0x1bec9:$s2: Nmap<br>• 0x1bed7:$s2: Nmap<br>• 0x1bf11:$s2: nmap<br>• 0x1c15a:$s2: Nmap<br>• 0x1c1cd:$s2: Nmap<br>• 0x1c1d5:$s2: Nmap<br>• 0x1c335:$s2: nmap<br>• 0x1d528:$s2: nmap<br>• 0x1d536:$s2: nmap<br>• 0x1d688:$s2: Nmap<br>• 0x1e68c:$s2: Nmap<br>• 0x1e720:$s2: Nmap<br>• 0x1e794:$s2: nmap<br>• 0x1ed4c:$s2: Nmap<br>• 0x1ed76:$s2: Nmap<br>• 0x1eefb:$s2: Nmap<br>• 0x1ef8b:$s2: nmap<br>• 0x22f43:$s2: Nmap<br>• 0x22f74:$s2: Nmap |
| C:\Users\user\AppData\Local\Temp\nsyA5CF.tmp | JoeSecurity_Predator | Yara detected Predator | Joe Security | |
| Click to see the 1 entries | | | | |

# Sigma Overview

**System Summary:**

**Sigma detected: Failed Code Integrity Checks**

# Signature Overview

Click to jump to signature section

**AV Detection:**

**Yara detected Predator**

**Phishing:**

**Yara detected HtmlPhish10**

## Compliance:

- Uses 32bit PE files
- Found installer window with terms and condition text
- Creates a directory in C:\Program Files
- Creates install or setup log file
- Creates license or readme file
- PE / OLE file has a valid certificate
- Binary contains paths to debug symbols

## Networking:

- NDIS Filter Driver detected (likely used to intercept and sniff network traffic)
- Yara detected Ncat Network tool

## E-Banking Fraud:

- Yara detected Predator
- Install WinpCap (used to filter network traffic)

## Spam, unwanted Advertisements and Ransom Demands:

- Install WinpCap (used to filter network traffic)

## Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

## Lowering of HIPS / PFW / Operating System Security Settings:

- Changes security center settings (notifications, updates, antivirus, firewall)

## Stealing of Sensitive Information:

- Yara detected Predator

## Remote Access Functionality:

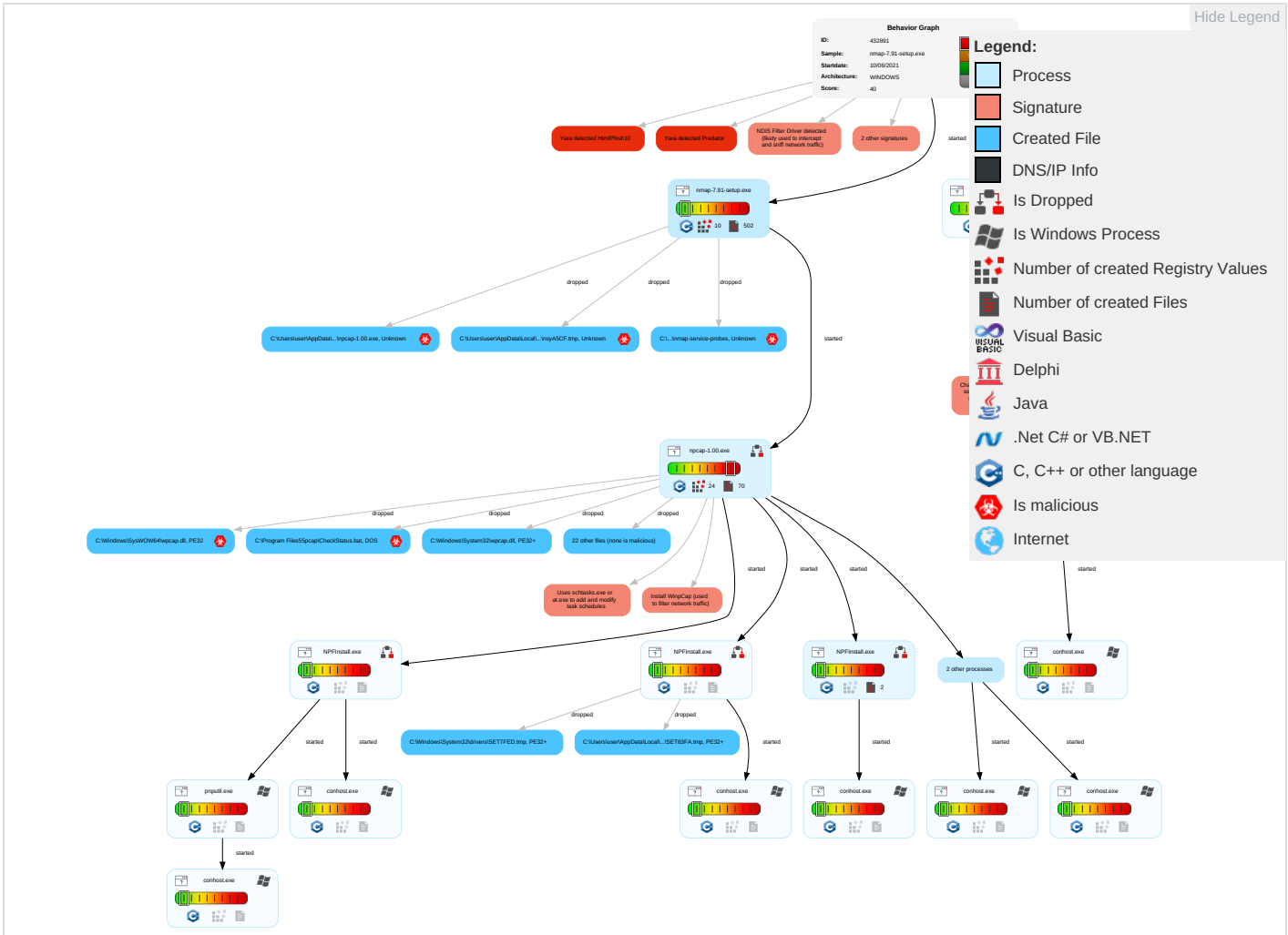
- Yara detected Predator
- Contains VNC / remote desktop functionality (version string found)

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Com and ( |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 1 | DLL Side-Loading 1 | DLL Side-Loading 1 | Disable or Modify Tools 1 | Network Sniffing 2 | System Time Discovery 1 | Remote Desktop Protocol 1 | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encry Chan |
| Default Accounts | Native API 2 | Windows Service 3 | Access Token Manipulation 1 | Deobfuscate/Decode Files or Information 1 | Input Capture 2 1 | File and Directory Discovery 4 | Remote Desktop Protocol | Input Capture 2 1 | Exfiltration Over Bluetooth | Remo Softw |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Com and ( |
|---|---|---|---|---|---|---|---|---|---|---|
| Domain Accounts | Command and Scripting Interpreter 2 | Scheduled Task/Job 1 | Windows Service 3 | Obfuscated Files or Information 1 | Security Account Manager | Network Sniffing 2 | SMB/Windows Admin Shares | Clipboard Data 1 | Automated Exfiltration | Steg |
| Local Accounts | Scheduled Task/Job 1 | Logon Script (Mac) | Process Injection 1 2 | Software Packing 1 | NTDS | System Information Discovery 4 6 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Proto Impe |
| Cloud Accounts | Cron | Network Logon Script | Scheduled Task/Job 1 | DLL Side-Loading 1 | LSA Secrets | Query Registry 1 | SSH | Keylogging | Data Transfer Size Limits | Fallb Chan |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | File Deletion 1 | Cached Domain Credentials | Security Software Discovery 8 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multil Comm |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Masquerading 3 2 | DCSync | Virtualization/Sandbox Evasion 3 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Comm Used |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Virtualization/Sandbox Evasion 3 | Proc Filesystem | Process Discovery 3 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Appli Laye |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Access Token Manipulation 1 | /etc/passwd and /etc/shadow | Remote System Discovery 1 | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web |
| Supply Chain Compromise | AppleScript | At (Windows) | At (Windows) | Process Injection 1 2 | Network Sniffing | Process Discovery | Taint Shared Content | Local Data Staging | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | File T Proto |

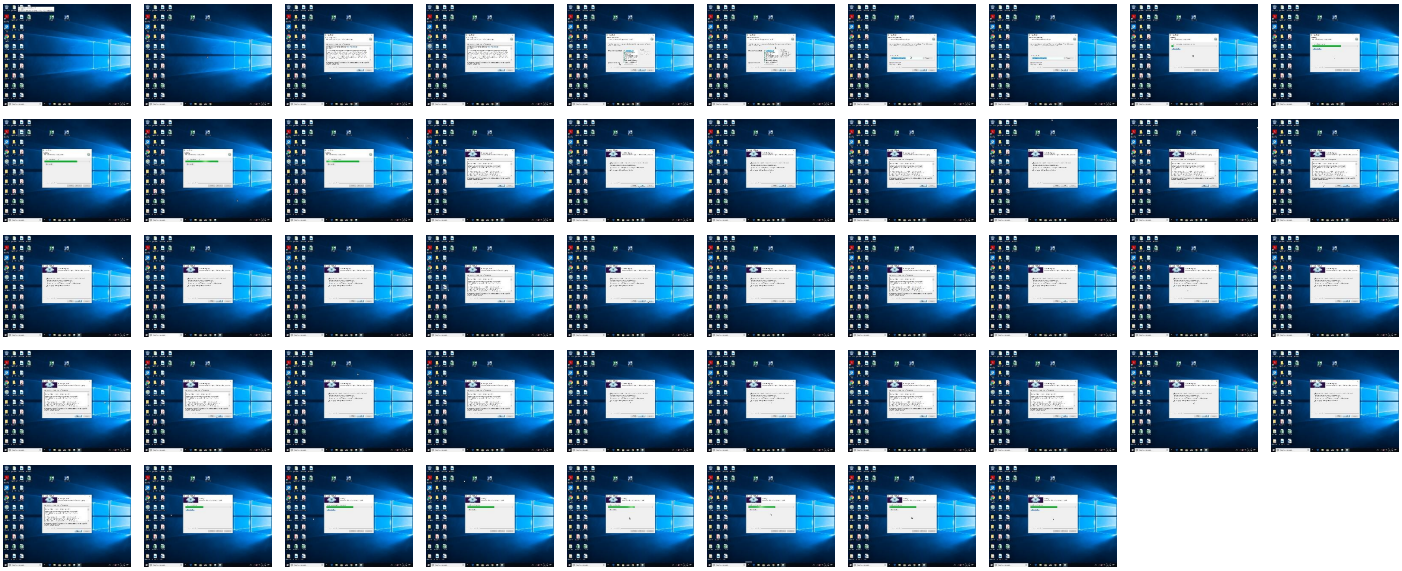
## Behavior Graph



# Screenshots

## Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.




# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| nmap-7.91-setup.exe | 3% | Virustotal | | Browse |
| nmap-7.91-setup.exe | 0% | Metadefender | | Browse |
| nmap-7.91-setup.exe | 0% | ReversingLabs | | |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Program Files\Npcap\NPFInstall.exe | 0% | Metadefender | | Browse |
| C:\Program Files\Npcap\NPFInstall.exe | 0% | ReversingLabs | | |
| C:\Program Files\Npcap\Uninstall.exe | 0% | Metadefender | | Browse |
| C:\Program Files\Npcap\Uninstall.exe | 3% | ReversingLabs | | |
| C:\Program Files\Npcap\npcap.sys | 0% | Metadefender | | Browse |
| C:\Program Files\Npcap\npcap.sys | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\InstallOptions.dll | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\InstallOptions.dll | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\NPFInstall.exe | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\NPFInstall.exe | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\SimpleSC.dll | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\SimpleSC.dll | 4% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\System.dll | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\System.dll | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\nsExec.dll | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\nsExec.dll | 0% | ReversingLabs | | |

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.2.nmap-7.91-setup.exe.2c54f6a.2.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://nmap.org) | 0% | Avira URL Cloud | safe | |
| http://underground.org.mx) | 0% | Avira URL Cloud | safe | |
| http://arc.opensolaris.org/caselog/PSARC/2006/638/stlisten_protocolv2.pdf | 0% | Virustotal | | Browse |
| http://arc.opensolaris.org/caselog/PSARC/2006/638/stlisten_protocolv2.pdf | 0% | Avira URL Cloud | safe | |
| http://arc.opensolaris.org/caselog/PSARC/2006/638/stdiscover_protocolv2.pdf | 0% | Virustotal | | Browse |
| http://arc.opensolaris.org/caselog/PSARC/2006/638/stdiscover_protocolv2.pdf | 0% | Avira URL Cloud | safe | |
| http://10.0.200.116:50000 | 0% | Avira URL Cloud | safe | |
| http://purenetworks.com/HNAP1/GetDeviceSettings | 0% | Avira URL Cloud | safe | |
| http://purenetworks.com/HNAP1/SetDeviceSettings | 0% | Avira URL Cloud | safe | |
| http://osvdb.org/ | 0% | Avira URL Cloud | safe | |
| http://purenetworks.com/HNAP1/GetDeviceSettings2 | 0% | Avira URL Cloud | safe | |
| http://https://dynamic.t | 0% | URL Reputation | safe | |
| http://https://dynamic.t | 0% | URL Reputation | safe | |
| http://https://dynamic.t | 0% | URL Reputation | safe | |
| http://https://www.shodan.io) | 0% | Avira URL Cloud | safe | |
| http://hcsw.org/blog.pl | 0% | Avira URL Cloud | safe | |
| http://https://npcap.org/) | 0% | Avira URL Cloud | safe | |
| http://www.security-assessment.com/files/advisories/2010-02-22_Multiple_Adobe_Products-XML_External_ | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| No contacted domains info |
|---|

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|

### Private

| IP |
|---|
| 127.0.0.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 432891 |
| Start date: | 10.06.2021 |
| Start time: | 21:53:42 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 10m 59s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | nmap-7.91-setup.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 35 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal40.spre.phis.bank.troj.adwa.evad.winEXE@37/881@0/1 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 90.7% (good quality ratio 79.7%)<br>• Quality average: 66.9%<br>• Quality standard deviation: 34% |
| HCA Information: | • Successful, ratio: 61%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

## Simulations

### Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 21:54:55 | API Interceptor | 2x Sleep call for process: svchost.exe modified |
| 21:56:10 | API Interceptor | 1x Sleep call for process: MpCmdRun.exe modified |
| 21:56:38 | Task Scheduler | Run new task: npcapwatchdog path: "C:\Program Files\Npcap\CheckStatus.bat" |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\InstallOptions.dll | http://https://nmap.org/dist/nmap-7.91-setup.exe | Get hash | malicious | Browse | |
| C:\Program Files\Npcap\NPFInstall.exe | http://https://nmap.org/dist/nmap-7.91-setup.exe | Get hash | malicious | Browse | |
| C:\Program Files\Npcap\npcap.sys | http://https://nmap.org/dist/nmap-7.91-setup.exe | Get hash | malicious | Browse | |
| C:\Program Files\Npcap\Uninstall.exe | http://https://nmap.org/dist/nmap-7.91-setup.exe | Get hash | malicious | Browse | |
| C:\Users\user\AppData\Local\Temp\nsb823.tmp\NPFInstall.exe | http://https://nmap.org/dist/nmap-7.91-setup.exe | Get hash | malicious | Browse | |

# Created / dropped Files

| C:\Program Files (x86)\Nmap\3rd-party-licenses.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 56784 |
| Entropy (8bit): | 5.11142771880872 |
| Encrypted: | false |
| SSDEEP: | 1536:Znx1q2ikzURtvQEI/epJ1G3VCI7C3lEciOCbf+eURVWLoIuWR1tWVYUPOg:Znx1q2ikYXvQl/QJ8VlCXiOCbGeQVGoh |
| MD5: | 67978D8B551E1027287D85B404FB7FCC |
| SHA1: | 71C8FB2B1AF422DCAE605E70790D75903642D82C |
| SHA-256: | 7E591E8AB4F22CF464098FEA9AD63BA7FDCF4D4042B0163EA85191FF7723C012 |
| SHA-512: | 8E662E99CB7E128AB402FEC95EA8D802BE77B305CE70C8F41D3CFA7B45A512ADFD91EDCB03C32DAC4EF1E68CA85AF469B2AB38CF732D3EFACD866473EF68E2B6 |
| Malicious: | false |
| Preview: | $Id: 3rd-party-licenses.txt 38073 2020-10-02 13:55:49Z dmiller $..This file is a list of the licenses of the third-party software used by.Nmap and the other tools distributed with it. What follows is a.description of each third-party package. At the end of this file is the.license of each. The license of Nmap itself is in the LICENSE file...On all platforms, Nmap is normally linked with:. o libpcap: Network packet capture library. Distributed with Nmap in the. libpcap subdirectory.. http://www.tcpdump.org/. o l ibdnet: Networking library, used for low-level tasks such as sending. ethernet frames. A modified version is distributed with Nmap in the. libdnet-stripped subdirectory. A summary of Nmap-local modifications. is in the file NMAP_MODIFICATIONS.. http://code.google.com/p/libdnet/. o PCRE: Perl-compatible regular expressions. PCRE is part of Nmap's. version detection and is also made available as an NSE library.. Distributed with Nmap in the libpcre subdirectory.. |

| C:\Program Files (x86)\Nmap\CHANGELOG | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |

| C:\Program Files (x86)\Nmap\CHANGELOG | |
|---|---|
| Category: | dropped |
| Size (bytes): | 756783 |
| Entropy (8bit): | 4.841071121836609 |
| Encrypted: | false |
| SSDEEP: | 6144:XHp4V47ZEPtoA8bbPu1zVNE4ecOS4bI/Lw6u8Gqwpx92RvCs5y7fKrnpruQ4XQtA:XHpz7ZWkgtQ8Gppx92ZCs4f2F3Y1/jH |
| MD5: | 764C2D732766C5A9683CA7100D1A16AD |
| SHA1: | B7134AA9A796A5F19A911351957C13BC3E9894B1 |
| SHA-256: | CF3E88E0E0E6A3748A8B9E7D71A27076A628E347909E4FFF34FED03661007E1A |
| SHA-512: | 7CD5F0CFEF297634C4A1326F893CD23FA9423748D2B90678E0FF54BDA8CC51A076E018F82F5B85DF0B5BFB5E4F2E5925F88C4FF3F6D8AAB8009E74F81A5B88BF |
| Malicious: | false |
| Preview: | #Nmap Changelog ($Id: CHANGELOG 38101 2020-10-09 22:43:50Z dmiller $); -*-text-*-..Nmap 7.91 [2020-10-09]..o [GH#2148][Zenmap] Fix a crash in the profile editor due to a missing import...o [GH#2139][Nsock][Windows] Demote the IOCP Nsock engine because of some known. issues that will take longer to resolve. The previous default "poll" engine. will be used instead...o [GH#2138][Nsock][Windows] Fix a crash in service scan due to a previously-unknown. error being returned from the IOCP Nsock engine. [Daniel Miller]..o [NSE][GH#2136][GH#2137] Fix several places where Lua's os.time was being used. to represent dates prior to January 1, 1970, which fails on Windows. Notably,. NSE refused to run in UTC+X timezones with the error "time result cannot be. represented in this installation" [Cl.ment Notin, nnposter, Daniel Miller]..o [NSE][GH#2128] MySQL library was not properly parsing server responses,. resulting in script crashes. [nnposter]..o [GH#2135] Silence the irrelevant warning, " |

| C:\Program Files (x86)\Nmap\LICENSE | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 28788 |
| Entropy (8bit): | 4.654065587727344 |
| Encrypted: | false |
| SSDEEP: | 384:vm6noOFMkPIGNqv78dt94WPLzWD5ZUWfUBr1Ss6+vNcVL6fxH341AYSkM+XaaAg:vm+WOgcvLPLzc5OLCkfdytSkhaaAg |
| MD5: | C83CD0CEDC337FADD3A95B6819E33F52 |
| SHA1: | 4E8A8E71A6804B2B5161C4E5E6601C5041E7266A |
| SHA-256: | 8254A9BC733F3312C6DCFE0D5A129C29E96ECB8B33408C652A8C7BEB2E25B471 |
| SHA-512: | 3911ACB93C05BA684BBF602BDB5B8CB0CBA213861274FD5C96DA8AB484B49BC4422DA7753F6A9ADC6824145706390DE82954963CCD46A22A6943D4E9FC76EC8 |
| Malicious: | false |
| Preview: | Nmap Public Source License Version 0.92.For more information on this license, see https://nmap.org/npsl/..0. Preamble..The intent of this license is to establish freedom to share and change.the software regulated by this license under the open source model. It.also includes a Contributor Agreement and disclaims any warranty on.Covered Software. Proprietary software companies wishing to use or.incorporate Covered Software within their programs must contact.Licensor to purchase a separate license. Open source developers who.wish to incorporate parts of Covered Software into free software with.conflicting licenses may write Licensor to request a waiver of terms...If the Nmap Project (directly or through one of it's commercial.licensing customers) has granted you additional rights to Nmap or Nmap.OEM, those additional rights take pr ecedence where they conflict with.the terms of this license agreement...This License represents the complete agreement concerning subject.matter hereof. It cont |

| C:\Program Files (x86)\Nmap\README-WIN32 | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 186 |
| Entropy (8bit): | 4.3520225057251265 |
| Encrypted: | false |
| SSDEEP: | 3:DRKLhgKRLnOxLLzxyMKxKZRS585N6jKJOLM/6JFrS5qWFRLkIFER3R0ZK5MiqEFL:Dq6KRLn8LEKRA85N6jKRKKBRLp4uYkEB |
| MD5: | 5BEEB5B810E2B69A003A3E2BF0B858AA |
| SHA1: | 358369E6E37CE10363D9D7A731AF5A988551728A |
| SHA-256: | D648AB626E65BB0BA45C9A35771CBB9578BBDFC94F27A8A9DE7D1B785D205285 |
| SHA-512: | 5650DACE2A647D8FB2695E55A2A66054ED81458D53B757B739099DFDB29177197A2B91DAF3EE8CDC1634CECA0C630B22BA1336D83733E5D1BBBF95E68335B1A |
| Malicious: | false |
| Preview: | Details on installation, compilation, and limitation of the Nmap.Security Scanner on the Windows platform is now available in the Nmap.Installation Guide at https://nmap.org/install/ ... |

| C:\Program Files (x86)\Nmap\Uninstall.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 78232 |
| Entropy (8bit): | 5.631110133223318 |
| Encrypted: | false |
| SSDEEP: | 1536:cRNwgSHfkxXML2ktkAk0DsTcHgdLeAyNnaJ/WUUfm:wNSkpML2ktlDsTcHceABhv |
| MD5: | 769C7963222530DBAD66C95CD43E6ACC |
| SHA1: | 69C5FB99A8FCA64BB742D82D1C23BBDC531199D1 |

| C:\Program Files (x86)\Nmap\Uninstall.exe | |
|---|---|
| SHA-256: | 05EF1EDCCB9BD8384CAE87C4B43221D33B1C423A0A79708B0C50045E38588C37 |
| SHA-512: | D7D517EAC03760412E977031187EA2E73E25A5A2FEF3202F8303030EB58FC17C0526924C6FD293C0BE5746A718B54BD4CCE2B2898951FDD9433EDD1296C6652( |
| Malicious: | false |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L....:.V.....`..... ..*1.....p....@.....P.....r.....$u.....N.....p..\|..... .....text...f^.....`..... ..`.rdata.....p.....d.....@..@.data.....x.....@....ndata..... .....rsrc....N.....P...~.....@..@..... ..... ..... |

| C:\Program Files (x86)\Nmap\icon1.ico | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 15086 |
| Entropy (8bit): | 3.630480316255235 |
| Encrypted: | false |
| SSDEEP: | 96:OyLN5qXsn1PkwpTtKDHEHSXhb3zXHDnH04:OYD0s1xZkSkhbDXHDnj |
| MD5: | 3F6D5FC3817FFB1BAFF6DA512CF35A0B |
| SHA1: | F0385358159CAD5FD4A2F320E82C84E7F430C71D |
| SHA-256: | 02B1101B85CFFAB2A7765CB47EE258C8BD851CA7B5CA622D70FF312773AD7FF5 |
| SHA-512: | A790FD5CCF8E147B4A4B7C226D3C8DCACC7577148F1F6F65134647BC0CF84505C9ED0E9AE5DF2CD7F6ACC035774498753A112315A94AE738595799F67D40BE4 |
| Malicious: | false |
| Preview: | ..... .h...6... .... .....00.... ..%..F...(..... ..... .....@..... .....g..nm.....ty.c.....e..kQ.z.....v..ve..b.....a.m.....{... i.....j...r.....;.....i...w.....S.....t.....).....w..zO.....i.....^...M.....Q..v ..... |

| C:\Program Files (x86)\Nmap\libcrypto-1_1.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1861656 |
| Entropy (8bit): | 7.014859884529778 |
| Encrypted: | false |
| SSDEEP: | 49152:Q5PeRYIa2KS+bTZJuC9Ix62UVsPbzx8DQt1CPwDv3uFfJHoiXK:Q5PeRYIa2KS+bzQLUV6zx8C1CPwDv3uI |
| MD5: | A0D081DF4B020C6685FD52C9D6520F19 |
| SHA1: | 188DF871E5C7A29AA3F9BFDAA3FC20C2C9E9BEEF |
| SHA-256: | EB5D9B61F8A7C6AD05B331973E5228B6AF3D3E4AF607FB4B5E7B38AE914D3266 |
| SHA-512: | 5093D45561A525EA46EDE58D32B1E4E076779EB0F136B9B94BB7981FF5B2BEC276321A99ABD7771FF5BE204068DB7FDF601B9C095A0830A2AD0B63911DEC103 |
| Malicious: | false |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sG`..)3..)3..)3.C.3..)3.C.3..)3.C.3..)3.C.3..)3a..3..)3..(3&.)3..)3..)3 .@.3..)3.@.3..)3.@.3..)3.@.3..)3Rich..)3.....PE..L...`.s_.....!.....i.....)w....@.....0r.....r.....J..... .....hq..@.....text..... ..`.rdata...}.....~.....@..@.data....I.....p.....@....rsrc.....@..@.rel oc.....@..B..... ..... |

| C:\Program Files (x86)\Nmap\libssh2.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 209944 |
| Entropy (8bit): | 6.687134900549294 |
| Encrypted: | false |
| SSDEEP: | 6144:6hwzk1OrDcLvFtX1VaQRTGKR+OS6ha+l2WZFDRvR:JzkQrDcbFtX1oQRT3p5lHT |
| MD5: | 29AEBC72C07999F2ECF6B701DEE7DBFB |
| SHA1: | 4DA85497FD81C8708F507F41CD25B01D8A6F4A7F |
| SHA-256: | 3EEFA2F126A264A7CD3E63FBE2918B4C1468E0E0A501B7941630AC0C3B7EEBB5 |
| SHA-512: | 0ADC3CA7729DADDF8712488C88A26611E48F66A9E1D0818F3CDB0A0BD7614E5A626A29C68412883BEAC0A27B37D07570AB1FBF46C5122787E2CC8D666C04B7 2 |
| Malicious: | false |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7+.\|sJ./sJ./sJ./5.7/qJ./5.5/vJ./5../.J./5../qJ./~.7/qJ./..!/tJ./sJ./.J./ ~../kJ./~.6/rJ./~.1/rJ./~.4/rJ./RichsJ./.....PE..L.....s_.....!.....h.....p.....`.....@.....0.....x....0.....@.... ..`...8.....@.....<.....text....f.....h..... ..`.rdata..^.....I.....@..@.data...H.... .....@....rsrc.....0.....@. .@.reloc.....@.....@..B..... ..... |

| C:\Program Files (x86)\Nmap\libssl-1_1.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 386584 |
| Entropy (8bit): | 6.41257135671652 |
| Encrypted: | false |
| SSDEEP: | 6144:8o3IgY1cgVJa/Cl6e3Qgej6v0HMzNyAj4YPk1tbOH7AFPYzumnO1TRu/wdmfS+Nq:C1zVJa/Cl6e3Qgej6vwMzNyAj4YPk1tN |
| MD5: | 137C4D33739D4B2C78E2DE05DBE9AC5B |
| SHA1: | 3C116C2A472902D8C2ECD16371EB6D18910003C6 |
| SHA-256: | D340F6A2C25920C97EB72824DE21D312CCC662BF82932743A8FBE3615CC0263F |
| SHA-512: | 0D0C9ECEF2DB141B5E2D97B66BA55B9FB6F0F78BACF0399B3359AB7CB8C6B973EDCE09471ED8BC1BD79E824652AB5FABDC602138B6C36799EF12B033EA8EE835 |
| Malicious: | false |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A>..._._._....._.C...._.C...._.C./.._.C...._....._._..^.../.)_....._....._.. ...._.Rich._.....PE..L.....s_.....!.....w.....HX....@.....@...;..P.....2.....@..... .....text..... ..`.rdata...W.....X.....@..@.data...`6...p...4...\.....@....rsrc.....@..@.reloc...2.....4.....@..B. ..... ..... |

| C:\Program Files (x86)\Nmap\licenses\BSD-modified.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 868 |
| Entropy (8bit): | 4.850867780772286 |
| Encrypted: | false |
| SSDEEP: | 24:gUno0PbOlprYFTJJyprYFTcQLe/R3SBTPf9TVoEOk3:/TOorYJCrYJte3GP1TV/3 |
| MD5: | 5EB289217C160E2920D2E35BDDC36453 |
| SHA1: | BF0CB439D0CA55615B5060EE09D77AF3DDC9518D |
| SHA-256: | 8A54594D257E14A5260AC770F1633516CB51E3FC28C40136CE2697014EDA7AFD |
| SHA-512: | CD8AEA0F35B44BB5E82610B19E6BC2C2CD3D4F77859C517AB5623DD0FE3873236D43EB322E138DD529D4596C331B46FAA9C0568F58EF20E62E40915EAAD66BB |
| Malicious: | false |
| Preview: | License: BSD..Redistribution and use in source and binary forms, with or without.modification, are permitted provided that the following conditions.are met:.. 1. Redistr ibutions of source code must retain the above copyright. notice, this list of conditions and the following disclaimer.. 2. Redistributions in binary form must reproduce the above copyright. notice, this list of conditions and the following disclaimer in. the documentation and/or other materials provided with the. distribution.. 3. The names of the authors may not be used to endorse or promote. products derived from this software without specific prior. written permission...THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR.IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED.WARRANTIES OF MERCHA NTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.. |

| C:\Program Files (x86)\Nmap\licenses\BSD-simplified | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1465 |
| Entropy (8bit): | 5.079965824321681 |
| Encrypted: | false |
| SSDEEP: | 24:NUneZXoPbO9FTnJzFTzTN799R432stOkJW6Wm3hyxtdfy33tGW+ZvTHBN7LN1B:RaO9JxJzn9R432srJWK3hEtI33tG/VHl |
| MD5: | 600F7C6B7EE7221F4F2F784A78BDB41A |
| SHA1: | 8DADC10542E641AE6F55EA5548BC39B080C2A0C6 |
| SHA-256: | C1D818296FA860C0F4103C714591EB8AC2AF2AD1945D763C7B9DAE8C9E4E7E5B |
| SHA-512: | F17133F59952B37FA8597856459D6A34ABDC729B8FD8E8CF8596AD21CAED4A82A91526338280E25D7B1F2D23D12CC36B69BCFF5888FD349083C78BF649D6536( |
| Malicious: | false |
| Preview: | Copyright. All rights reserved...Redistribution and use in source and binary forms, with or without modification,.are permitted provided that the following conditions are met:.. 1. Redistributions of source code must retain the above copyright notice,. this list of conditions and the following disclaimer... 2. Redistributions in binary form must reproduce the above copyright notice,. this list of conditions and the following disclaimer in the documentation. and/or other materials provided with the distribu tion...THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS'' AND ANY EXPRESS OR IMPLIED.WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF.MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT.SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,.INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NO T.LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR.PROFITS; |

| C:\Program Files (x86)\Nmap\licenses\LGPL-2 | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 25292 |
| Entropy (8bit): | 4.621640808555452 |

| C:\Program Files (x86)\Nmap\licenses\LGPL-2 | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 384:xt5UwOVAIZ4zZyydV+X6wFDVxnFw7xqsv/t+zP8EfHinIhFkspNM9b/7upt0M6Qv:xtuFmIHiV+DnFM/gReSNm/7GtX6Qv |
| MD5: | 3BF50002AEFD002F49E7BB854063F7E7 |
| SHA1: | BF50BAC24E7EC325DBB09C6B6C4DCC88A7D79E8F |
| SHA-256: | D245807F90032872D1438D741ED21E2490E1175DC8AA3AFA5DDB6C8E529B58E5 |
| SHA-512: | 697DF393FBC529F7BE805BDF7B18A064EA8F1D85241A1F50CB9A720E8CDEC87319F53F62E000BD613113198D5A802E22F0EC7426BBB4562E423DA8BA3FFB71E5 |
| Malicious: | false |
| Preview: | .. GNU LIBRARY GENERAL PUBLIC LICENSE... Version 2, June 1991.. Copyright (C) 1991 Free Software Foundation, Inc.. .. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Everyone is permitted to copy and distribute verbatim copies. of this license document, but changing it is not allowed...[This is the first released version of the library GPL. It is. numbered 2 because it goes with version 2 of the ordinary GPL.]..... Preamble.. The licenses for most software are designed to take away your.freedom to share and change it. By contrast, the GNU General Public.Licenses are intended to guarantee your freedom to share and change.free software--to make sure the software is free for all its users... This license, the Library General Public License, applies to some.specially designated Free Software Foundation software, and to any.other libraries whose authors decide to use it. You can use it for.your libraries, too... When we speak of free software, we are referring |

| C:\Program Files (x86)\Nmap\licenses\LGPL-2.1 | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 26440 |
| Entropy (8bit): | 4.612889177653709 |
| Encrypted: | false |
| SSDEEP: | 384:XX56OuAbnn0UX+X6wFDVxnFw7xqsvzt+z/k8E9HinIhFkspcM9bc7upt0MZuQy:XX5trR+DnFMz1ReScmc7GtXZuQy |
| MD5: | A916467B91076E631DD8EDB7424769C7 |
| SHA1: | 597BF5F9C0904BD6C48AC3A3527685818D11246D |
| SHA-256: | 32434AFCC8666BA060E111D715BFDB6C2D5DD8A35FA4D3AB8AD67D8F850D2F2B |
| SHA-512: | D9842B27DD5ED4E255C3D7EEAD771D999257D7D0E8114E15E3508B7FA52A797B8D6280364615 90E7AB50E36E54ABBD5CB7A42D05CF1D1BA9F5C4A77B97424F5 |
| Malicious: | false |
| Preview: | .. GNU LESSER GENERAL PUBLIC LICENSE... Version 2.1, February 1999.. Copyright (C) 1991, 1999 Free Software Foundation, Inc.. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies. of this license document, but changing it is not allowed...[This is the first released version of the Lesser GPL. It also counts. as the successor of the GNU Library Public License, version 2, hence. the version number 2.1.]..... Preamble.. The licenses for most software are designed to take away your.freedom to share and change it. By contrast, the GNU General Public.Licenses are intended to guarantee your freedom to share and change.free software--to make sure the software is free for all its users... This license, the Lesser General Public License, applies to some.specially designated software packages--typically libraries--of the.Free Software Foundation and other authors who decide to use it. You.can use it too, but |

| C:\Program Files (x86)\Nmap\licenses\LIBLINEAR-license.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1486 |
| Entropy (8bit): | 5.165339807857781 |
| Encrypted: | false |
| SSDEEP: | 24:IWUnogbOYrYFT5JOrYFTFvxBTPx9LFmr43sEskCaWROt32sByxtdfy33tZolTHv:IpOYrYJWrYJ5zPbxmr43JD32sBEtI336 |
| MD5: | AA069C170D333FFF306F5284F5E2C427 |
| SHA1: | 11B4AAB10A36CB53CBC34914898F370C012E714E |
| SHA-256: | A7A153D7E4EFBC66F5DC332A279E1A4A99A8805A7057A89B8188BD94280675C9 |
| SHA-512: | 886E0049055D1B7396C1C3C38937B3A57BF437F38DAE4E8677DB5CF7BEADF81C282128ADAFC1C5718B37D1951D94D6AEE976B9100128771A7783176B4F9659F |
| Malicious: | false |
| Preview: | .Copyright (c) 2007-2011 The LIBLINEAR Project..All rights reserved...Redistribution and use in source and binary forms, with or without.modification, are permitted provided that the following conditions.are met:..1. Redistributions of source code must retain the above copyright.notice, this list of conditions and the following disclaimer...2. Redistributions in binary form must reproduce the above copyright.notice, this list of conditions and the following disclaimer in the.documentation and/or other materials provided with the distribution...3. Neither name of copyright holders nor the names of its contributors.may be used to endorse or promote products derived from this software .without specific prior written permission....THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS.``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT.LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR.A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL TH |

| C:\Program Files (x86)\Nmap\licenses\Libdnet-license.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1460 |
| Entropy (8bit): | 5.158057709080036 |
| Encrypted: | false |
| SSDEEP: | 24:571ubUno4LbOIhrYFTw4JLZirYFTdLeW0BTPD9TR432sBOkUTOJ32s3yTtTfRzSM:57gkfOorYJ1irYJdZoPZTR432s/J32sA |
| MD5: | 3986C8674A86A1A1652737CDAECD6EF7 |
| SHA1: | 8A7D9026468153574B91528092FD891DD62F70C7 |

| C:\Program Files (x86)\Nmap\licenses\Libdnet-license.txt | |
|---|---|
| SHA-256: | 1D6836269212A5112788D98E07BA9ED4FF9144E1D4C191B7C3A2A15073BE3A85 |
| SHA-512: | CDA6D951D689AA3DD2D24282B035795F30800D7716C4C6E942B7588B6C01B799D0B76FFB5E7F1301C41C5E9A3876EB5C6E86EC343F2F5DD89EF2CD6E9002C0C |
| Malicious: | false |
| Preview: | Copyright (c) 2000-2006 Dug Song <dugsong@monkey.org>.All rights reserved, all wrongs reversed...Redistribution and use in source and binary forms, with or with out.modification, are permitted provided that the following conditions .are met:..1. Redistributions of source code must retain the above copyright. notice, this list of conditions and the following disclaimer.. .2. Redistributions in binary form must reproduce the above. copyright notice, this list of conditions and the following. disclaime r in the documentation and/or other materials provided. with the distribution...3. The names of the authors and copyright holders may not be used . to endorse or prom ote products derived from this software . without specific prior written permission...THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED .WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES .OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE.DI SCLAIMED. IN NO EVENT SHALL THE AUTHOR B |

| C:\Program Files (x86)\Nmap\licenses\Lua-license.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1066 |
| Entropy (8bit): | 5.10949742673841 |
| Encrypted: | false |
| SSDEEP: | 24:9Yr4JHBH0yPP3gtAHw1hl9QHcsUv48Ok4/+dbo3oqxFD:m8JplPvEDvQHcs5ITc3omFD |
| MD5: | 3EBB14E9752F0C7DBC687E0BD302BAA5 |
| SHA1: | D2DA2BD4F8577C12E667EA04E332F2A6561C6301 |
| SHA-256: | F4759DE4DBDCB2297F0913AFEE664E7177606ECA2BAEF55920DB161C41E5C03C |
| SHA-512: | FC41DB24883CC545E9C1F1769696D1389ABF72C77E2720D93BFA637DEF0C9D3B512451D276AE40994FDBE359B407CBA8F02284430033EDAA0A3E6825F409ED0 |
| Malicious: | false |
| Preview: | Copyright . 1994.2016 Lua.org, PUC-Rio..Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copi es of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:..The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software...THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIO |

| C:\Program Files (x86)\Nmap\licenses\MIT | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1065 |
| Entropy (8bit): | 5.095562000694795 |
| Encrypted: | false |
| SSDEEP: | 24:8rmJHHH0yN3gtsHw1hj9QHOsUv4eOk4/+/m3oqLF5n:8aJHlxE35QHOs5exm3ogF5n |
| MD5: | B28808853537299BAE3B2025E2C38D89 |
| SHA1: | 00BEFDB0045F9E81F4919CB3928C25B149622AF0 |
| SHA-256: | 2367A894A18178677800179DE62B46D374DADA7C15999E11942BCD3A236BD0AE |
| SHA-512: | 87AA9BD50E106522A38BDDF1877550FC724668A78163E59197BE624319CEE052351C83F6C97B946E3D1DB84569F4427543BD0F54BCCD65F3506447DD60807BA6 |
| Malicious: | false |
| Preview: | Copyright (c) <year> <copyright holders>..Permission is hereby granted, free of charge, to any person obtaining a copy.of this software and associated documentation files (the "Software"), to deal.in the Software without restriction, including without limitation the rights.to use, copy, modify, merge, publish, distribute, sublicense, and/or sell.co pies of the Software, and to permit persons to whom the Software is.furnished to do so, subject to the following conditions:..The above copyright notice and this permission notice shall be included in.all copies or substantial portions of the Software...THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,.FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGE MENT. IN NO EVENT SHALL THE.AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER.LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,.OUT OF OR IN CONNECTION |

| C:\Program Files (x86)\Nmap\licenses\MPL-1.1 | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 25755 |
| Entropy (8bit): | 4.627449807901279 |
| Encrypted: | false |
| SSDEEP: | 384:ZuCPLhqsT7Wlj7gwZFUoBjyKddfnpdp9dlKBAbN1EkhbVs5IsUfTNTukkv2n:bPLhCAijy+F9T9hGdasUfTkkkv2n |
| MD5: | BFE1F75D606912A4111C90743D6C7325 |
| SHA1: | ABA8D76D0AF67D57DA3C3C321CAA59F3D242386B |
| SHA-256: | 53692A2ED6C6A2C6EC9B32DD0B820DFAE91E0A1FCDF625CA9ED0BDF8705FCC4F |
| SHA-512: | FBDDECCEA689BA830DF464C144C1258EC696AE6D797B5E98AD86AA9419A8BFFBF6CC2E4614CC1A8497B495D3BB18BFD0CB7B1CF2B0BB4459E9C31DBEE1CF70F6 |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\licenses\MPL-1.1 | |
|---|---|
| Preview: | MOZILLA PUBLIC LICENSE. Version 1.1.. ----------..1. Definitions... 1.0.1. "Commercial Use" means distribution or otherwise making the. Covered Code available to a third party... 1.1. "Contributor" means each entity that creates or contributes to. the creation of Modifications... 1.2. "Contributor Version" means the combination of the Original. Code, prior Modifications used by a Contributor, and the Modifications. made by that particular Contributor... 1.3. "Covered Code" means the Original Code or Modifications or the. combination of the Original Code and Modifications, in each case. including portions thereof... 1.4. "Electronic Distribution Mechanism" means a mechanism generally. accepted in the software development community for the ele ctronic. transfer of data... 1.5. "Executable" means Covered Code in any form other than Source. C |

| C:\Program Files (x86)\Nmap\licenses\OpenSSL-license.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 6126 |
| Entropy (8bit): | 5.128501186223271 |
| Encrypted: | false |
| SSDEEP: | 96:MLZFOrYJQrYJTqBMvgQgk3bzAxxnkVb+ck1ibrYJArYJOHb2Lli3+3zX4TZCCg:uZFOrsQrslvgQgk3eZ+Y1ibrsArsQ2iK |
| MD5: | 2100BDC885AC4CDC9783C562639DDC1F |
| SHA1: | 102073B66C9BE39953F62AF2EB238629F7D50883 |
| SHA-256: | 3560FF8A21669AF3AFC45F95587324DF8565089DD99E7676709B26C3157DFA55 |
| SHA-512: | 7A9CB296D6DE9257DD9BDD891D5F02A039DB6F2781046C418B8AD03DB04B1D2D7573F88D3D8BAE8B287A937342D8FC1E2DD6ADA84C6AB0C486BB2DCBB36C6C6 |
| Malicious: | false |
| Preview: | . LICENSE ISSUES. ==========.. The OpenSSL toolkit stays under a dual license, i.e. both the conditions of. the OpenSSL License and the original SSLeay license apply to the toolkit.. See below for the actual license texts... OpenSSL License. ----------../* ========== ==========. * Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.. *. * Redistribution and use in source and binary forms, with or without. * modification, are permitted provided that the following conditions. * are met:. *. * 1. Redistributions of source code must retain the above copyright. * notice, this list of conditions and the following disclaimer. . *. * 2. Redistributions in binary form must reproduce the above copyright. * notice, this list of conditions and the following d isclaimer in. * the documentation and/or other materials provided with the. * distribution.. *. * 3. All advertising materials mentioning features or use |

| C:\Program Files (x86)\Nmap\licenses\PCRE-license.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2496 |
| Entropy (8bit): | 5.163737021258413 |
| Encrypted: | false |
| SSDEEP: | 48:20FocUUzZO9JyrYJWPkLY7PlO432sHj32sZEtY17wBHw:V6cUKM9JyrYJWPkLY5F3X31EBQ |
| MD5: | 1144C29D8B432C81629C78B6E14D0B63 |
| SHA1: | C5ACB2598E023AB1D8B4AC2DB0914C70F0F89765 |
| SHA-256: | D494463CDAD306784AC07648F34C2CBC5ABD2A4B8B87262381E036C25572F161 |
| SHA-512: | 4860B06A39F0CAED49344C3B11004FD6A45B26EF2DB3078FDFE385A17ED1CAD5A5424457D336F209FF81D1F383E84F13AD8BEB9404C2ECE67DDF1A477710278A |
| Malicious: | false |
| Preview: | PCRE LICENCE.----------..PCRE is a library of functions to support regular expressions whose syntax.and semantics are as close as possible to those of the Perl 5 langua ge...Release 7 of PCRE is distributed under the terms of the "BSD" licence, as.specified below. The documentation for PCRE, supplied in the "doc".directory, is distributed under the same terms as the software itself...The basic library functions are written in C and are freestanding. Also.included in the distribution is a set of C++ wrapper functions....THE BASIC LIBRARY FUNCTIONS.----------..Written by: Philip Hazel.Email local part: ph10.Email domain: cam.ac.uk..University of Cambridge Computing Service,.Cambridge, England...Copyright (c) 1997-2008 University of Cambridge.All rights reserved....THE C++ WRAPPER FUNCTIONS.----------..Contributed by: Google Inc...Copyright (c) 2007-2008, Google Inc..All rights reserved....THE "BSD" LICENCE.----------..Redistribution and |

| C:\Program Files (x86)\Nmap\licenses\WinPcap-license.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 13143 |
| Entropy (8bit): | 5.1429130886731 |
| Encrypted: | false |
| SSDEEP: | 384:8grsirsQP3zBCrsYrseM5B8uPrsYrsMMOB8rsYrs0U9pBgTLUzrsYrsGKqXDcUB1:fJdzBC5A5B8k5aOB85rypBgnUz5EqXDv |
| MD5: | B155231690DDCD93762E0AF73C2FCAEA |
| SHA1: | 29728470B493ED96ABAB2CB93352C03270964A17 |
| SHA-256: | 50BB666E8E1554E1AB9A12373CE5A004994EC0749217E68D3A75FA09170A52A3 |
| SHA-512: | 8E1222A8D011F228B74A05051025C6D6FF0C4B868B43366F82D3EE633E5CF1D2D9E0F5EC9CDF983A17CAB1B368FFEF25FEB4ED5FBCE2484E58CEF84957CA640 |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\licenses\WinPcap-license.txt | |
|---|---|
| Preview: | Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy)..Copyright (c) 2005 - 2010 CACE Technologies, Davis (California)..All rights reserved...Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:..1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. .2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. .3. Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. ..THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE |

| C:\Program Files (x86)\Nmap\licenses\zlib-license.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 996 |
| Entropy (8bit): | 4.4378119941928835 |
| Encrypted: | false |
| SSDEEP: | 24:3xm0M+/jxAb/oyhQNKMTp4/GE+wjqt8PgBA:g03/jeb/bh6KMTp4/z3jqeCA |
| MD5: | 2CCDC892B6EE23C9F8143908A843A8E3 |
| SHA1: | F6A50421E3063A75058AE312E1CAAEACAAAD0A9A |
| SHA-256: | E9DA8EFE5E5876FADCB38AF76F9DFDF5C1F4626EDEDA003E01D0514FBC1077DD |
| SHA-512: | F49701CFDC4103DC5F2680E68A8ECFAF00CC9AC70A2FE2293D81918EE4483707BEEA0EC0EBB5C6E810F343010D332FE6E2EE6BD2308F4BA42C33E1DD3EB76C6 |
| Malicious: | false |
| Preview: | . Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler.. This software is provided 'as-is', without any express or implied. warranty. In no event will the authors be held liable for any damages. arising from the use of this software... Permission is granted to anyone to use this software for any purpose,. including commercial applications, and to alter it and redistribute it. freely, subject to the following restrictions:.. 1. The origin of this software must not be misrepresented; you must not. claim that you wrote the original software. If you use this software. in a product, an acknowledgment in the product documentation would be. appreciated but is not required.. 2. Altered source versions must be plainly marked as such, and must not be. misrepresented as being the original software.. 3. This notice may not be removed or altered from any source distribution... Jean-loup Gailly Mark Adler. jloup@gzip.org madler@alumni.caltech.edu.. |

| C:\Program Files (x86)\Nmap\nmap-mac-prefixes | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 717314 |
| Entropy (8bit): | 5.281530953021449 |
| Encrypted: | false |
| SSDEEP: | 12288:nCyTabAQeea6GiYOCrPTxlyx1erdXVR16Oy6eBgp7GD1bZ/Xt6m32FPrZkpZDhnB:kW5wQUhw6y/xh1 |
| MD5: | F22D11852A42CB3017B41C73BF53D39E |
| SHA1: | B34485E1DB5A4C376676EF73C5DC330825F84026 |
| SHA-256: | B3F07F756AC95D68B9C753AF68B06BA16001536F5BF95CD9343DEC688537A8D4 |
| SHA-512: | 34AB5F8F36FD29C087857937FA4588CE4A7F3CB582FFE3BEA351970AF8AE39862A062863069170503EE0DC4796680AE967FAD80679CA19524182C1317DF15241 |
| Malicious: | false |
| Preview: | # $Id: nmap-mac-prefixes 38008 2020-09-08 21:08:24Z dmiller $ generated with make-mac-prefixes.pl.# Original data comes from http://standards.ieee.org/regauth/oui/oui.txt.# These values are known as Organizationally Unique Identifiers (OUIs).# See http://standards.ieee.org/faqs/OUI.html.# We have added a few unregistered OUIs at the end..002272 American Micro-Fuel Device.00D0EF IGT.086195 Rockwell Automation.F4BD9E Cisco Systems.5885E9 Realme Chongqing MobileTelecommunications.BC2392 BYD Precision Manufacture Company.405582 Nokia.A4E31B Nokia.D89790 Commonwealth Scientific and Industrial Research Organisation.883A30 Aruba, a Hewlett Packard Enterprise Company.B8A58D Axe Group Holdings Limited.50CEE3 Gigafirm.co.LTD.98E743 Dell.C419D1 Telink Semiconductor (Shanghai).887E25 Extreme Networks.086083 zte.E01954 zte.10327E Huawei Device.F8084F Sagemcom Broadband SAS.30FBB8 Huawei Technologies.F497C2 Nebulon.A44519 Xiaomi Communications.68DBF5 Amazon Technologies.2446C8 Motorola Mobility, a L |

| C:\Program Files (x86)\Nmap\nmap-os-db | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 5033049 |
| Entropy (8bit): | 5.431975276623881 |
| Encrypted: | false |
| SSDEEP: | 12288:oNsGfluyiJCtL+45rF4OgFRxSVECuE+qmYQxLGD/+kZiM57uMmxCZX8A2D+uAZkN:oJrVMCEAyuzjyaLW33ZxvH |
| MD5: | 10D567BC7D20345C4FC7B0813C8B65D1 |
| SHA1: | 7CFEDA56890B38B9D3BE204F3E422887AFC38061 |
| SHA-256: | 9CF57876AD8E6DF9A38D5ED9CDB8AFD150F5FE41C2927173366F5FB6B7F319DC |
| SHA-512: | 4C88A9B1BAAA049B74B2CB2B55CE3B5FE835CFA1B9E378A8B8073656593DEDB60F644ABD07FB98685B2542E7EB4986D41F7FA0B2283D1257ED35A175DEFE727D |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nmap-os-db | |
|---|---|
| Preview: | # Nmap OS Fingerprinting 2nd Generation DB. -*- mode: fundamental; -*-.# $Id: nmap-os-db 38073 2020-10-02 13:55:49Z dmiller $.#.# Contributions to this database are welcome. If Nmap obtains a new.# fingerprint (and test conditions are favorable), it will print out a.# URL you can use to submit the fingerprint. If Nmap guesses wrong,.# please see https://nmap.org/submit/ ..#.# By submitting fingerprints you are transfering any and all copyright.# interest in the data to Insecure.Com LLC so it can modifie d,.# incorporated into Nmap, relicensed, etc..#.# This collection of fingerprint data is (C) 1996-2020 by Insecure.Com.# LLC. It is distributed under the Nmap Public Source license as.# provided in the LICENSE file of the source distribution or at.# https://nmap.org/data/LICENSE . Note that this license.# requires you to license your own work under a compatible open source.# license. If you wish to embed Nmap technology into proprietary.# software, we sell alternative licenses (cont |

| C:\Program Files (x86)\Nmap\nmap-payloads | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 20943 |
| Entropy (8bit): | 4.912456355159182 |
| Encrypted: | false |
| SSDEEP: | 384:EMQmLkeohBdW1+hBbvEl+UCNGyZWxEbkhg68AKb:EMQmLHohBzTQlyeeAKb |
| MD5: | 445571D858F1BE75C25A39FC60D9FC0E |
| SHA1: | 27724A435AE5E2BD327B9E4FBFBA29FE644B9056 |
| SHA-256: | C95F84AA6955651F8FE99B96223D1CA97B889F9B8C98A66E60337477D3F956BD |
| SHA-512: | 86D9289473057A9BBF6149A3C88F442C8EEC6BF69CB3DF87CFB09B5B5DBB5E1F5C6CDFD38D934DC5B92EB9155CCEE862F79858D1C24D69D9283114474F3913E |
| Malicious: | false |
| Preview: | # Nmap nmap payload database -*- mode: fundamental; -*-.# $Id: nmap-payloads 38073 2020-10-02 13:55:49Z dmiller $.#.# These payloads are sent with every host di scovery or port scan probe.# by default. This database should only include payloads that are.# unlikely to crash services, trip IDS alerts, or change state on the.# server. The idea behind these is to evoke a response using a payload..# Some of them are taken from nmap-service-probes..#.# This collection of data is (C) 1996-2010 by Insecu re.Com.# LLC. It is distributed under the Nmap Public Source license as.# provided in the LICENSE file of the source distribution or at.# https://nmap.org/data/LICENSE . Note that this license.# requires you to license your own work under a compatible open source.# license. If you wish to embed Nmap technology into proprietary.# softwa re, we sell alternative licenses (contact sales@insecure.com)..# Dozens of software vendors already license Nmap technology such as.# host discovery, port scann |

| C:\Program Files (x86)\Nmap\nmap-protocols | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 6703 |
| Entropy (8bit): | 4.312542205140055 |
| Encrypted: | false |
| SSDEEP: | 96:NIt0/iHc1XxJlU1FzU+P1ukbHv/rf/MC8r+cH9lu0fG0tYuK8CnxEw:322XflUjzU+P1DbPjfRsHzMnxZ |
| MD5: | 6D0F93E99CF9CF764F0A8E8B25C724C2 |
| SHA1: | 683CA626F967E8FDD320F20890DF04E945A66E73 |
| SHA-256: | E00EB6472DF8D8E99B202D32268237145AFB9DA22B3B8D8B988287F27E7DD1F7 |
| SHA-512: | 5BCF27707FB8178D04C17F74968ACFEDF1636F4846FFDAC7F1C6593BCE28D8096F1264E99DD74A6C721D71FE9E42120B57E2E801D02B4DF00FE7DE62CCB96CC |
| Malicious: | false |
| Preview: | # This list of protocols is distributed with the -*- mode: fundamental; -*-.# Nmap Security Scanner ( https://nmap.org ).#.# This list is based on IEEE data at.# http://www.iana.org/assignments/protocol-numbers.# Last updated: 2015-06-17.hopopt 0 # IPv6 Hop-by-Hop Option.icmp 1 # Internet Control Message.igmp 2 # Internet Group Management.ggp 3 # Gateway-to-Gateway.ipv4 4 # IP in IP (encapsulation).st 5 # Stream.tcp 6 # Transmission Control.cbt 7 # CBT.egp 8 # Exterior Gateway Protocol.igp 9 # any private interior gateway.bbn-rcc-mon 10 # BBN RCC Monitoring.nvp-ii 11 # Network Voice Protocol.pup 12 # PARC universal packet protocol.argus 13 # ARGUS.emcon 14 # EMCON.xnet 15 # Cross Net Debugger.chaos 16 # Chaos.udp 17 # User Datagram.mux 1 |

| C:\Program Files (x86)\Nmap\nmap-rpc | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 43755 |
| Entropy (8bit): | 5.184863409539125 |
| Encrypted: | false |
| SSDEEP: | 768:FiGux69zT3tWnqCdjX3f+ucCNz6znDAWAEeOxOA/vL5ik1W7hd0Y:FfiMTuqCdjz2Bw9x |
| MD5: | 4584100EA406259722DDCEF717E62822 |
| SHA1: | 7222E7A8E12FF73D66D9B398B608073D9B892CD5 |
| SHA-256: | DCD5D5B24D4C1D9B89505F6E277383FA33564A47F183401B7FCF72AF05517061 |
| SHA-512: | 44482B75E10C499D020F26DF995916A9D09526D61728BAE2B3D018988A11D82CE8BAF4DEE2EC174C3490081F5DFBCC64AF60D2B5C6E1BAF1D22DBD12A68B54E |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nmap-rpc | |
|---|---|
| Preview: | # $Id: nmap-rpc 38073 2020-10-02 13:55:49Z dmiller $ -*- mode: fundamental; -*-.#.# /**********.# * nmap-rpc -- Known RPC numbers. Nmap uses them for RPC grinding. *.# * Thanks to Eilon Gishri, Vik Bajaj, Fyodor, and other members of *.# * the Nmap community for contributing entries. Someday we might *.# * reorder this with the most popular services first to make scans *.# * faster. *.# **********/.#.# This collection of data is (C) 1996-2020 by Insecure.Com LLC..# It is distributed under the Nmap Public Source license as.# provided in the LICENSE file of the source distribution or at.# https://svn.nmap.org/nmap/LICENSE . Note that this license.# requires you to license your own work under a compatable open source.# license. If you wish to embed Nmap technolog |

| C:\Program Files (x86)\Nmap\nmap-service-probes | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2497787 |
| Entropy (8bit): | 5.552130827910342 |
| Encrypted: | false |
| SSDEEP: | 24576:hv+cMKG6P7comwtmea8NVUfh0O3/9l8BKlOpV5uw61OgxgZyeuKM:hdMKhtmeV+Vl0KFOSgseuKM |
| MD5: | 38781F3126F9B691DA7C2883DF88DBDA |
| SHA1: | 07FDDC4F5B263428E7A42FDF9FC0592E4A9DD74A |
| SHA-256: | 549E0EF7967D7F7E23EA16F8BBA65222061E18579CC6F9DB77202B4C97EA8DBF |
| SHA-512: | 23986BB53E5B690A44FA6AB0693E0BB50233F5BA8F3D0FEDF9A1E47473FD266E7B3A2347C8DD427943B2F207AF73504CC048D873E2C7B0DC532F6F940634260 |
| Malicious: | **true** |
| Yara Hits: | • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Program Files (x86)\Nmap\nmap-service-probes, Author: Joe Security |
| Preview: | # Nmap service detection probe list -*- mode: fundamental; -*-.# $Id: nmap-service-probes 38073 2020-10-02 13:55:49Z dmiller $.#.# This is a database of custom probes and expected responses that the.# Nmap Security Scanner ( https://nmap.org ) uses to.# identify what services (eg http, smtp, dns, etc.) are listening on.# open ports. Contributions to this database are welcome..# Instructions for obtaining and submitting service detection fingerprints can.# be found in the Nmap Network Scanning book and online at.# https://nmap.org/book/vscan-community.html.#.# This collection of probe data is (C) 1998-2020 by Insecure.Com.# LLC. It is distributed under the Nmap Public Source license as.# provided in the LICENSE file of the source distribution or at.# https://nmap.org/data/LICENSE . Note that this license.# requires you to license your own work under a compatible open source.# license. If you wish to embed Nmap technology into proprietary.# software, we sell alternative licenses (con |

| C:\Program Files (x86)\Nmap\nmap-services | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1001818 |
| Entropy (8bit): | 5.070297475339513 |
| Encrypted: | false |
| SSDEEP: | 6144:yELcAkO1z4qqGF7NjhbTukptiC+3xpluKqHfeYpsG/ZfmkkwefzjoX5C:yn4qGNptipluKqHfd/Z8zjoX5C |
| MD5: | 28339E926A04AC0BC3321E4D1F603C6D |
| SHA1: | 368B4E0629D5ECF1FE920B183EBE6C630BF63E1B |
| SHA-256: | 9CFCFB13011F5A78D0FDE4257D0DBEC263B6D37BFA4E3FDA7C7E1484B4E35B1C |
| SHA-512: | A25571B7FA40BBA2C83C37C6933E239865ED4C44D6851442401861CD0328DD5C14D3989FBB0468B3268364178390FFABA8F51EA42A213800FA8DC9E79E93A3A1 |
| Malicious: | false |
| Preview: | # THIS FILE IS GENERATED AUTOMATICALLY FROM A MASTER - DO NOT EDIT..# EDIT /nmap-private-dev/nmap-services-all IN SVN INSTEAD..# Well known service port numbers -*- mode: fundamental; -*-.# From the Nmap Security Scanner ( https://nmap.org/ ).#.# $Id: nmap-services 38073 2020-10-02 13:55:49Z dmiller $.#.# Derived from IANA data and our own research.#.# This collection of service data is (C) 1996-2020 by Insecure.Com.# LLC. It is distributed under the Nmap Public Source license as.# provided in the LICENSE file of the source distribution or at.# https://svn.nmap.org/nmap/LICENSE . Note that this license.# requires you to license your own work under a compatable open source.# license. If you wish to embed Nmap technology into proprietary.# software, we sell alternative licenses (contact sales@insecure.com)..# Dozens of software vendors already license Nmap technology such as.# host discovery, port scanning, OS detection, and version detection..# For more details, see https://nmap.org/ |

| C:\Program Files (x86)\Nmap\nmap.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2892824 |
| Entropy (8bit): | 5.612956631739243 |
| Encrypted: | false |
| SSDEEP: | 24576:ePk74SDtft1tRwal1GALs/GuXuBbljo93qxSe/yB/hP0e9ebEsz8mjNo:5h5tVGwgg1o93qxSQE/hP0e90z4mjNo |
| MD5: | 6FF5BC2D67C7493033AEA3030CA4B9E4 |
| SHA1: | 3E6D7F8B1A54A84C87C0579364E1216B51AD45D9 |
| SHA-256: | BBE903455474B7A4373FA86966EF24217B08D570BD7F53E152DE6F21869EB32A |
| SHA-512: | 2D65D091FDACAF2377F7344D4FC02B397D9D8D841C46B58D681B039E3645EAEE149EF138BB049CF468BF795683E206884DD8D76499E21F42F3389BE8B2962DF |
| Malicious: | false |
| Preview: | MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....vsz...)...)...).F.)...)'..)...).F.)...).F.)...).F.)...)d..)...).E.)...).E.)...)..).)...).E.)...).E.)...).E.)...)...)...).E.)...)Rich...).....PE..L...X._.....$...<.....}.....@....@.....0.-...@.....-..@.....,.....-.....0H..8.....@.....@.....text....".....$..... ..`.rdata..`....@.....(.....@..@.data.....P.....0.....@..._RDATA..0....p-.....*.....@..@.rsrc....@....-..B...*.....@..@.reloc.....-.....4+.....@..B..... |

| C:\Program Files (x86)\Nmap\nmap.xsl | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 31936 |
| Entropy (8bit): | 4.9140329158116 |
| Encrypted: | false |
| SSDEEP: | 768:ppvUn5hcVZM2fNBzPSTDcCvns9z1ARqATyCdokqFyq0qi287HWx:ppvc5UZM2fNBzPSTDcCvns9z1ARqATy9 |
| MD5: | E82D7756256566703B2F5A10C78C8D0A |
| SHA1: | F90C79D60B4A72C33477CD4FEB0624C8A262B37E |
| SHA-256: | DBB8939C4331A9269915E4B05FA8605462B47A2CCC04D042418531C8ED8F20F1 |
| SHA-512: | 1EE9C3F6C8C7DE24A2BEF5D422297AAE572634A950A51380B0EAFAC77002888974438F0579D041EE7C6221CB62F776A2C730A1FD59D5EC6C1DAD5E2C39E7E1<br>D |
| Malicious: | false |
| Preview: | <?xml version="1.0"?>. ==========. nmap.xsl stylesheet version 0.9c. last change: 2010-12-28. Benjamin Erb, http://www.benjamin-erb.de.========== ==========. Copyright (c) 2004-2006 Benjamin Erb. All rights reserved... Redistribution and use in source and binary forms, with or without. modification, are permitted provided that the following conditions. are met:. 1. Redistributions of source code must retain the above copyright. notice, this list of conditions and the following disclaimer.. 2. Redistributions in binary form must reproduce the above copyright. notice, this list of conditions and the following disclaimer in the. do cumentation and/or other materials provided with the distribution.. 3. The name of the author may not be used to endorse or promote products. derived from this |

| C:\Program Files (x86)\Nmap\nmap_performance.reg | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 192 |
| Entropy (8bit): | 5.237630375274039 |
| Encrypted: | false |
| SSDEEP: | 3:0QOvibgLCgT/K/TCirM0Aa3ACOBSKLV/fZ4VK9BcMNmLV/xovWRcGcQLU9HYBS+w:bOvPLC6/KbC1073AhkKLV1+wyVt3LU9b |
| MD5: | 3CD4A36A0DCC9E0E79D1DF1D6CC712DF |
| SHA1: | A9B6FE5C0E01AEC042E68C2BC700A721C4ECC995 |
| SHA-256: | E77D7B5158EC99D19E552025FACF50F477A2F2B1DC3EF2F198520CFA76E9707F |
| SHA-512: | D3D5AB7CC0943DD7AE85445449249109EEB5F871E1C7BAF3139CD9E2D3858F70040102DC30B089FC99EE82EBBF99335C2323B1D070552CF7E565A1AC70EF248 |
| Malicious: | false |
| Preview: | REGEDIT4..[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters].."MaxUserPort"=dword:0000fffe.."TcpTimedWaitDelay"=dword:0<br>000001e.."StrictTimeWaitSeqCheck"=dword:00000001.... |

| C:\Program Files (x86)\Nmap\nse_main.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 48522 |
| Entropy (8bit): | 4.725769575717454 |
| Encrypted: | false |
| SSDEEP: | 768:BWFdkaxh3Khel97rTBZJ/QrS4mEjOKNrzv5iNcD1s2V7CIyV8d7v5yWfYeaEVoMJ:BSkuOe7cBFrj5iNc5GlccWfYeaEVoOCq |
| MD5: | E41BCC656EC62BB1D8B678A51DD9A4C2 |
| SHA1: | 9415480C57A4923B0E27685B71141AD95F6B8F00 |
| SHA-256: | FBEEF2AA795EB41BFCD90BBD1CF17A806D9A486B8939AE48DE8E3C548E8F6E29 |
| SHA-512: | 2AC276C34BD259153124DA18149E73F418561512B3A9713D15FC117BFF6A5FB5E433508DE17A5B96FE6D2E469531E9BDDA7DAEE311E5398C872E7C43C54BE15 |
| Malicious: | false |
| Preview: | -- Arguments when this file (function) is called, accessible via ....-- [1] The NSE C library. This is saved in the local variable cnse for.-- access throughout the file..-- [2] The list of categories/files/directories passed via --script..-- The actual arguments passed to the anonymous main function:.-- [1] The list of hosts we run against..--.-- When making changes to this code, please ensure you do not add any.-- code relying global indexing. Instead, create a local below for the.-- global you need access to. This protects the engine from possible.-- replacements made to the global environment, speeds up access, and.-- documents dependencies..--.-- A few notes about the safety of the engine, that is, the ability for.-- a script developer to crash or otherwise stall NSE. The purpose of noting.-- these attack vectors is more to show the difficulty in accidentally.-- breaking the system than to indicate a user may wish to break the.-- system through these means..-- - A scr |

| C:\Program Files (x86)\Nmap\nselib\afp.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 74827 |
| Entropy (8bit): | 4.924254548358027 |
| Encrypted: | false |
| SSDEEP: | 1536:0jZisW4LI2eYwgrhJRZ2L5GzMtKObq9fJWR096Zd9n99B9r49o949f9/FfUt9c9i:0joj4LI2eYwgrhJf2L5GzM4Obq9km9ml |
| MD5: | DBE3B21AA1F1C7B65E9847C13185EBEA |
| SHA1: | E40BD28AF7D9F6066B0A6B4FF14935CE3FAEB507 |

**C:\Program Files (x86)\Nmap\nselib\afp.lua**

| | |
|---|---|
| SHA-256: | 367DAB2331AEBCD58CE9914FE7780000939577198860AB26104EA18DE8E7A530 |
| SHA-512: | 54A8DCA8FCCD4245D1F3E712782392DC7BA8FDD849835F30FAEDD76801A84908F775E63CB01AEC07F6CCD70DAD1B7AABAC1D906D1AF8E3EEC4C67AEA7DC<br>118C |
| Malicious: | false |
| Preview: | ---.-- This library was written by Patrik Karlsson <patrik@cqure.net> to facilitate.-- communication with the Apple AFP Service. It is not feature complete and.-- still missing several functions..--.-- The library currently supports.-- * Authentication using the DHX UAM (CAST128).-- * File reading and writing.-- * Listing sharepoints.-- * Listing d irectory contents.-- * Querying ACLs and mapping user identities (UIDs).--.-- The library was built based on the following reference:.-- http://developer.apple.com/mac/li brary/documentation/Networking/Reference/AFP_Reference/Reference/reference.html.-- http://developer.apple.com/mac/library/documentation/Networking/Conceptual/AF P/AFPSecurity/AFPSecurity.html#//apple_ref/doc/uid/TP40000854-CH232-CHBBAGCB.--.-- Most functions have been tested against both Mac OS X 10.6.2 and Netatalk 2.0.3.--.-- The library contains the following four classes.-- * <code>Response</code>.-- ** A class used as return value by functions in the <code>Proto</code> cl |

**C:\Program Files (x86)\Nmap\nselib\ajp.lua**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 17061 |
| Entropy (8bit): | 4.744146355649658 |
| Encrypted: | false |
| SSDEEP: | 384:EnHFnwKQQ5/NHMdBXZlZmwCx4DWLuNQ98v/zdE4X:EnNwG/NHMdBbZRCx4DGIQevDX |
| MD5: | 5E8792AB819D3B65C3DDDF55AB691EB0 |
| SHA1: | FD15EBAA125F8AE44ADF60ECB2A101C0D8F377A9 |
| SHA-256: | D4C825FD6588992A501DE023DA1554924768390867F32DEDC051FAE636B05910 |
| SHA-512: | B61D9B94986EF801C29C0D18A22C1EECF4B525A1F5EF7223F03D2B654F46BD14AE3F3E799B6A5EE5B79D6E4059B3A7E54C4DFE785CF027DFC565DE684AD48F<br>12 |
| Malicious: | false |
| Preview: | local base64 = require "base64".local http = require "http".local match = require "match".local nmap = require "nmap".local stdnse = require "stdnse".local string = require "string".local table = require "table".local url = require "url"._ENV = stdnse.module("ajp", stdnse.seeall)..---.-- A basic AJP 1.3 implementation based on documentation available from Apache.-- mod_proxy_ajp; http://httpd.apache.org/docs/2.2/mod/mod_proxy_ajp.html.--.-- @author Patrik Karlsson <patrik@cqure.net>.--..AJP = {.. -- The magic prefix that has to be present in all requests. Magic = 0x1234,.. -- Methods encoded as numeric values. Method = {. ['OPTIONS'] = 1,. ['GET'] = 2,. ['HEAD'] = 3,. ['POST'] = 4,. ['PUT'] = 5,. ['DELETE'] = 6,. ['TRACE'] = 7,. ['PROPFIND'] = 8,. ['PROPPATCH'] = 9,. ['MKCOL'] = 10,. ['COPY'] = 11,. ['MOVE'] = 12,. ['LOCK'] = 13,. ['UNLOCK'] = 14,. ['ACL'] = 15,. ['REPORT'] = 16,. ['VERSION-CONTROL'] = 17,. ['CHECKIN'] = 18,. |

**C:\Program Files (x86)\Nmap\nselib\amqp.lua**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 10657 |
| Entropy (8bit): | 4.678473106800801 |
| Encrypted: | false |
| SSDEEP: | 192:PsKVVQ4a0wGF6ETAmEuZtjg4jCQ6jWcyluJujoztYxqroFO6h7bQgNerCFDQNL3B:pS4aKtgfK7X8cOnX |
| MD5: | 49DBEACB9D5BB33FE18B52B44DCF0073 |
| SHA1: | 8DC027C6C5F8B1974F0C1F4424214FEE5192B142 |
| SHA-256: | 6955B1EFBFB2CF41A7F00284A168EBACE551730ED5FFA7FB12F19DCAE2F35BDF |
| SHA-512: | B8CC730C7A294117219B1B06D12901B391A36E048F2BB2DFF86D2F2E2D1E0EE802BB2C6580C3BBAAA7BCC790E36E5A2B8C4884FE55DFC360F7662D8499A292<br>9 |
| Malicious: | false |
| Preview: | ---.-- The AMQP library provides some basic functionality for retrieving information.-- about an AMQP server's properties..--.-- Summary.-- -------.-- The library currently supports the AMQP 0-9 and 0-8 protocol specifications..--.-- Overview.-- --------.-- The library contains the following classes:.--.-- o AMQP.-- - This class contains the core functions needed to communicate with AMQP.--.-- @args amqp.version Can be used to specify the client version to use (currently, 0-8, 0-9 or 0-9-1).--.-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html.-- @author Sebastian Dragomir <velorien@gmail.com>..-- Version 0.1..-- Created 05/04/2011 - v0.1 - created by Sebastian Dragomir <velorien@gmail.com>..local match = require "match".local nmap = require "nmap".local stdnse = require "stdnse".local string = require "string".local table = require "table"._ENV = stdnse.module("amqp", stdnse.seeall);...AMQP = {.. -- protocol versions sent by the server. versions = {. [0x0800 |

**C:\Program Files (x86)\Nmap\nselib\anyconnect.lua**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 4410 |
| Entropy (8bit): | 4.777144184424326 |
| Encrypted: | false |
| SSDEEP: | 96:rX1+gLgsudKLqsM4vcAFnz3im+zNzbFiae+:rl+gEsudQa4Fmj6r+ |
| MD5: | B21F05025E4D3BF2651D83DCD6397BC9 |
| SHA1: | 6F7823CDEE9E9AB1D597656310FB97B5EAFC3063 |
| SHA-256: | C37C53A455A018E646C9A456B416286E7C3E066ADFF887F8B7D4D723FDE36580 |
| SHA-512: | 9475C6F2D7A2267EF699E6969DCF26E5CC8AE6DED206842173092B7FC4CA445DF9763F66CA98BD3CA8C0E53105EE919CD4178C6C6EA89E7245883070DF174E |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\anyconnect.lua | |
|---|---|
| Preview: | ---.-- This library implements HTTP requests used by the Cisco AnyConnect VPN Client.--.-- @author Patrik Karlsson <patrik@cqure.net>.--.-- @args anyconnect.group AnyConnect tunnel group (default: VPN).-- @args anyconnect.mac MAC address of connecting client (default: random MAC).-- @args anyconnect.version Version of connecting client (default: 3.1.05160).-- @args anyconnect.ua User Agent of connecting client (default: AnyConnect Darwin_i386 3.1.05160)..local http = require('http').local stdnse = require('stdnse').local url = require('url').local table = require('table').local rand = require "rand"..local args_group= stdnse.get_script_args('anyconnect.group') or "VPN".local args_mac= stdnse.get_script_args('anyconnect.mac').local args_ver = stdnse.get_script_args('anyconnect.version') or "3.1.05160".local args_ua = stdnse.get_script_args('anyconnect.ua') or ("AnyConnect Darwin_i386 %s"):format(args_ver)..._ENV = stdnse.module("anyconnect", stdnse.seeall)..Cisco = {..  Util = {..gen |

| C:\Program Files (x86)\Nmap\nselib\asn1.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 14923 |
| Entropy (8bit): | 4.7838167993195135 |
| Encrypted: | false |
| SSDEEP: | 384:8uzsV3FeDGcMipMROm9qg1t2/zw7TxvVGw7bIbX:8uzsV3FQ7ro2cvVAw78bX |
| MD5: | 319C26949816C6530795F6E64582385E |
| SHA1: | B3B0587F7098D8C160D18CA8DC7C0778066E1F54 |
| SHA-256: | 28C31E265DCB8C13CCB8DEFEBB864CB52D6C56E1487D638DC3F24790493926DD |
| SHA-512: | D14CC4538DC6ABEB039BE485803DEAF6C59AF68091203E5F61127B641D4D0DEF0AACBF137555CCE574A994A64760B072E5F5651642A02BF2A279B5867FBF8AEC |
| Malicious: | false |
| Preview: | ---.-- ASN.1 functions..--.-- Large chunks of this code have been ripped right out from <code>snmp.lua</code>..--.-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html.--.-- @author Patrik Karlsson.-- @class module.-- @name asn1.--..-- Version 0.3.-- Created 01/12/2010 - v0.1 - Created by Patrik Karlsson <patrik@cqure.net>.-- Revised 01/28/2010 - v0.2 - Adapted to create a framework for SNMP, LDAP and future protocols.-- Revised 02/02/2010 - v0.3 - Changes: o Re-designed so that ASN1Encoder and ASN1Decoder are separate classes.--  o Each script or library should now create its own Encoder and Decoder instance.--..local math = require "math".local stdnse = require "stdnse".local string = require "string".local table = require "table"._ENV = stdnse.module("asn1", stdnse.seeall)..BERCLASS = {.  Universal = 0,.  Application = 64,.  ContextSpecific = 128,.  Private = 192.}..--- The decoder class.--.ASN1Decoder = {..  new = function(self,o).o = o |

| C:\Program Files (x86)\Nmap\nselib\base32.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 7533 |
| Entropy (8bit): | 5.146984881866505 |
| Encrypted: | false |
| SSDEEP: | 192:eorQH4U2vAh54Jz9fMqJqX9CgWn9B6ZUMWfuD3v0IA8dgY/CY+u+:eornU2vAh5K9YX9fYB/duD3v08CYX+ |
| MD5: | EDE433892DFF24061C5158515D4B72AB |
| SHA1: | 0A0DB9D5C7ABD92D3A595F574CF268A21BB10124 |
| SHA-256: | 5D2E9D9DB77C0F7C9D12E6D24765E5E073A2775EBC3E521395D507B67D1B8FDC |
| SHA-512: | EAF269081E113A95388FD5EDC0C2D5D7BE716789B57474B28F1AE29C742EF703CE46235FBF752284C22923ADB527AD3A16488C326CCC534CC455CFDBEB28DEF |
| Malicious: | false |
| Preview: | -- The MIT License (MIT).-- Copyright (c) 2016 Patrick Joseph Donnelly (batrick@batbytes.com).--.-- Permission is hereby granted, free of charge, to any person obtaining a copy of.-- this software and associated documentation files (the "Software"), to deal in.-- the Software without restriction, including without limitation the rights to.-- use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies.-- of the Software, and to permit persons to whom the Software is furnished to do.-- so, subject to the following conditions:.--.-- The above copyright notice and this permission notice shall be included in all.-- copies or substantial portions of the Software..--.-- THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.-- IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,.-- FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE.-- AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER.-- LIA |

| C:\Program Files (x86)\Nmap\nselib\base64.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 5975 |
| Entropy (8bit): | 5.275684344420563 |
| Encrypted: | false |
| SSDEEP: | 96:eEyXuFRQH4fMoaEDA7CnmY4JvnqvFMtupuw+io6y9s9+Yv4wPiiN7pDcqGCY+1+:eorQH4UZJm4JvnqvFMtGbly9s9+Yv4wM |
| MD5: | 4339D65DB1CFECE2F70B250E22301BDA |
| SHA1: | 1CBA059AEA5DA8B16222CB2F4F7A5E59A610356C |
| SHA-256: | 09A3F5E4E59AC683EAE92D1AD653C58DFFCD504542E7E3CFDCC5AE00D3DA797D |
| SHA-512: | 7E7E8F75470AE2D3F1D97699AB8DECF117D49DAA2FE804471A310A3B20C2DFF12B03A352E16CEA6BD6BCE9AE69DFE5F177E68A4CDD85D80D546F9C78F00235A |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\base64.lua | |
|---|---|
| Preview: | -- The MIT License (MIT).-- Copyright (c) 2016 Patrick Joseph Donnelly (batrick@batbytes.com).--.-- Permission is hereby granted, free of charge, to any person obtaining a copy of.-- this software and associated documentation files (the "Software"), to deal in.-- the Software without restriction, including without limitation the rights to.-- use, c opy, modify, merge, publish, distribute, sublicense, and/or sell copies.-- of the Software, and to permit persons to whom the Software is furnished to do.-- so, subject to the following conditions:.--.-- The above copyright notice and this permission notice shall be included in all.-- copies or substantial portions of the Software..--.-- THE SOFTWA RE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.-- IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHA NTABILITY,.-- FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE.-- AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER.-- LIA |

| C:\Program Files (x86)\Nmap\nselib\bin.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 13303 |
| Entropy (8bit): | 4.798479161474145 |
| Encrypted: | false |
| SSDEEP: | 384:YVJanGwV5ubVt7dnbYKvMvGv6vEvJdaA60r5Ikco+:uwV5u37dnjvMvGv6vEvJdaA6VTo+ |
| MD5: | A9324843A7102954E8C829A162280BCB |
| SHA1: | FC3F42B692720DA72B8F27EDD86A3FBB44C44E14 |
| SHA-256: | 0D2A11A35416543D460507DF70EDD22488046F1468F7FE6DE02D01A4AB93C01A |
| SHA-512: | BE6BE95E536F345295B56C7CD75A4AA346D82580C7E56B6946A1709878892099398D88F4D18484AF9E9DD208EC746788775CFE587BA1890914D30EFA6205C050 |
| Malicious: | false |
| Preview: | ---.-- Pack and unpack binary data..--.-- THIS LIBRARY IS DEPRECATED! Please use builtin Lua 5.3 string.pack facilities..--.-- A problem script authors often face is the necessity of encoding values.-- into binary data. For example after analyzing a protocol the starting.-- point to write a script could be a hex dump, which serves as a pr eamble.-- to every sent packet. Prior to Lua 5.3, NSE included a bin library, based on lpack.-- (http://www.tecgraf.puc-rio.br/~lhf/ftp/lua/) by Luiz Henrique de Figueiredo..-- This library is now reimplemented using Lua 5.3 string.pack facilities. New scripts and libraries.-- should adopt Lua 5.3's native string.pack..--.-- The Binlib functions take a format string to encode and decode binary.-- data. Packing and unpacking are controlled by the following operator.-- characters:.-- * <code>H</code> hex string.-- * <code>x</code> null byte.-- * <code>z</code> zero-terminated string.-- * <code>p</code> string preceded by 1-byte integer length.-- * <code> |

| C:\Program Files (x86)\Nmap\nselib\bitcoin.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 18690 |
| Entropy (8bit): | 4.5774743884370785 |
| Encrypted: | false |
| SSDEEP: | 384:r+bEljf4X/gNSdbeS4z8VqqUgDbj3nlZ8gTTPgsvKCiX:rZljALj1DPWX |
| MD5: | B4F75F3104879A2FABDA0A1B04A2A7DF |
| SHA1: | 183FEDEE069724F8CE81910A38663483A63E84E6 |
| SHA-256: | C290B8EEA498900BA49DEA246C09698A4B90BAE695EFA574AA3345B195A72809 |
| SHA-512: | 18AA389C13DB541E9A2D78BD195A72A76FE1ABDD8ACFFDF945E01C1D6792245B1CEB4F9E4B07F386B679D94456E6DDC2B53759E371FFD9B6E4DDB52ABFDBC 9B0 |
| Malicious: | false |
| Preview: | ---.-- This library implements a minimal subset of the BitCoin protocol.-- It currently supports the version handshake and processing Addr responses..--.-- The library co ntains the following classes:.--.-- * NetworkAddress - Contains functionality for encoding and decoding the.-- BitCoin network address structure..--.-- * Request - Classs containing BitCoin client requests.-- o Version - The client version exchange packet.--.-- * Response - Class containing BitCoin server responses.-- o Version - The server version exchange packet.-- o VerAck - The server version ACK packet.-- o Addr - The server address packet.-- o Inv - The server inventory pa cket.--.-- * Helper - The primary interface to scripts.--.--@author Patrik Karlsson <patrik@cqure.net>.--@author Andrew Orr <andrew@andreworr.ca>.--@copyright Same as Nmap--See https://nmap.org/book/man-legal.html..--.-- Version 0.2.--.-- Created 11/09/2011 - v0.1 - created by Patrik Karlsson <patri |

| C:\Program Files (x86)\Nmap\nselib\bits.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2604 |
| Entropy (8bit): | 4.879565507470764 |
| Encrypted: | false |
| SSDEEP: | 48:Kqzi8VtGqssJLreU/9LO4+gPCm/O/ZHcG6oA6dA64aA6xWA6iA6MQ6Fl6al6Il68:K9ktqUlO4+ICm2x8GlAgAhaAZArAlQqz |
| MD5: | 7F5684174542116734C3796DEDBEE1E8 |
| SHA1: | 39269E68D93D1C82705B0701ADFA0A876964B7C8 |
| SHA-256: | E562A9014192D266487D54225057EB70823CEB2D93256CFAC49BBAC13D46874A |
| SHA-512: | FCFED8E70C80F70B1384C458DFCC543FD3AFC39016099A4E19854C76D75B3ACDCA0C8622D35E690EB45E5DBC6C8CCAF6863C21D4606BEF1818548D0285F715 4 |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\bits.lua | |
|---|---|
| Preview: | ---.-- Bit manipulation library..--.-- @author Patrick Donnelly <batrick@batbytes.com>.-- @copyright Same as Nmap -- see https://nmap.org/book/man-legal.html.-- @see https://www.lua.org/manual/5.3/manual.html#3.4.2.--.-- @class module.-- @name bits..local assert = assert.local error = error.local unittest = require "unittest"..local _ENV = {}..--- Reverses bits in integer..--.-- @param n The integer..-- @param size The bit width of the integer (default: 8)..-- @return The reversed integer..function reverse (n, size). if not size or size == 8 then. n = n & 0xff. n = (n & 0xf0) >> 4 \| (n & 0x0f) << 4. n = (n & 0xcc) >> 2 \| (n & 0x33) << 2. n = (n & 0xaa) >> 1 \| (n & 0x55) << 1. n = n & 0xff. elseif size == 32 then. n = n & 0xffffffff. n = ((n >> 1) & 0x55555555) \| ((n & 0x55555555) << 1);. n = ((n >> 2) & 0x33333333) \| ((n & 0x33333333) << 2);. n = ((n >> 4) & 0x0F0F0F0F) \| ((n & 0x0F0F0F0F) << 4);. n = ((n >> 8) |

| C:\Program Files (x86)\Nmap\nselib\bittorrent.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 36615 |
| Entropy (8bit): | 4.486801494858452 |
| Encrypted: | false |
| SSDEEP: | 384:hi+xZKskV86wiryOFvR82olsbYcsGToXLkLiyKQ6s3NefQBbvtcxX:/K9V8ULvGvNcsmMLqiyx6s3AfgbexX |
| MD5: | 2F72FF4E67D0A9EA64CFEFAE4BA87016 |
| SHA1: | 8D8A76615697C93878BC7A0DFBE7962FB470BF51 |
| SHA-256: | B6870EBFC8C191AC5EC1A6C63104EFF6A72B576C2B0DDB56FB9D107858C275D0 |
| SHA-512: | 32C025CE710D948FE9179661A67016C6DF6AC62F394A1128FA9F752E7B7BFF95B9A91118F8265DFF7BD7BEADCE7E57D2526D79B1EFB1DC8508F773F7536E327 |
| Malicious: | false |
| Preview: | --- Bittorrent and DHT protocol library which enables users to read.-- information from a torrent file, decode bencoded (bittorrent.-- encoded) buffers, find peers associated with a certain torrent and.-- retrieve nodes discovered during the search for peers..--.-- For more information on the Bittorrent and DHT protocol go to:.-- http://www.bittorrent.org/beps/bep_0000.html.--.-- The library contains the class <code>Torrent</code> and the function bdecode(buf).--.-- How this library is likely to be used:.-- <code>.-- local filename = "/home/user/name.torrent".-- local torrent = bittorrent.Torrent:new().-- torrent:load_from_file(filename).-- torrent:trackers_peers() -- to load peers from the trackers.-- torrent:dht_peers() -- to further load peers using the DHT protocol from existing peers.-- </code>.-- After these operations the peers and nodes can be found in <code>torrent.peers</code> and.-- <code>torrent.nodes</code> tables respectively.--.-- @author Gorjan Petrovski.-- @licens |

| C:\Program Files (x86)\Nmap\nselib\bjnp.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 9780 |
| Entropy (8bit): | 4.512007594005359 |
| Encrypted: | false |
| SSDEEP: | 192:zYcU4u8Gj+QklzwQnGbV4B1aMQACSSq14iZj8H7Mzj9X:zYcCRKVGBHeX |
| MD5: | 80227C1B25D3AF81192266027B3770F5 |
| SHA1: | A60F3469A34B80E4E800A0324819DCD26C40746E |
| SHA-256: | 235FE1C28B2C8F067C4A57D2B8A28E32A604884FA6F09A16DC153F6ABB617A32 |
| SHA-512: | DB97D339AEDB0D971C0B9A1C7B7D111F6F4C7CAA9BBA824E2D8BB580BCF379232533840D4F8F21BDCB619E2067979B3462553EB925253521128F12B31B20767 |
| Malicious: | false |
| Preview: | ---.-- An implementation of the Canon BJNP protocol used to discover and query.-- Canon network printers and scanner devices..--.-- The implementation is pretty much based on Wireshark decoded messages.-- the cups-bjnp implementation and the usual guesswork..--.-- @author Patrik Karlsson <patrik [at] cqure.net>.--..local nmap = require("nmap").local os = require("os").local stdnse = require("stdnse").local table = require("table").local string = require "string".local stringaux = require "string aux".._ENV = stdnse.module("bjnp", stdnse.seeall)..BJNP = {.. -- The common BJNP header. Header = {.. new = function(self, o). o = o or {}. o = {. id = o.id or "BJNP",. type = o.type or 1,. code = o.code,. seq = o.seq or 1,. session = o.session or 0,. length = o.length or 0,. }. assert(o.code, "code argument required"). setmetatable(o, self). self.__index = self. return o. end,.. parse = function(data). |

| C:\Program Files (x86)\Nmap\nselib\brute.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 51888 |
| Entropy (8bit): | 4.461197683557342 |
| Encrypted: | false |
| SSDEEP: | 768:DekBr6y01FMm8r2oub+FFJb3GcH6lVv6msjNUxjXHn+v47+WhVQefsgc3SecO4Xl:TBep1un7bNV6jNsjXHnn7+W7xJV1 |
| MD5: | 440CC9B92CE29AADC9D7B9C10C692E9C |
| SHA1: | 100266D09E07B70A7E2C752CCAC4CF23BBAB608C |
| SHA-256: | A66E2EE710B1410055FF8B15040A789B431484C4D069452321692051FC3B860E |
| SHA-512: | 97348F35963CE507D0DA2C8BD0C0270680D230780ED2A70B1E07B6F1F251B5F0CBE156706C9DBDCB14E10DD98F48B5FC15C2AD9DC5404BF36BBD98AC9BE867B |
| Malicious: | false |
| Preview: | ---.-- The brute library is an attempt to create a common framework for performing.-- password guessing against remote services..--.-- The library currently attempts to parallelize the guessing by starting.-- a number of working threads and increasing that number gradually until.-- brute.threads limit is reached. The starting number of threads can be set.-- with brute.start argument, it defaults to 5. The brute.threads argument.-- defaults to 20. It is worth noticing that the number of working threads.-- will grow exponentially until any error occurs, after that the engine.-- will switch to linear growth..--.-- The library contains the following classes:.-- * <code>Engine</code>.-- ** The actual engine doing the brute-forcing ..-- * <code>Error</code>.-- ** Class used to return errors back to the engine..-- * <code>Options</code>.-- ** Stores any options that should be used during brute-forcing..--.-- In order to make use of the framework a script needs to implement a Driver.-- class. |

| C:\Program Files (x86)\Nmap\nselib\cassandra.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 5610 |
| Entropy (8bit): | 4.911967894334497 |
| Encrypted: | false |
| SSDEEP: | 96:Gy27Lk2dyHi1YfFYf038k73DwYm2LRHz6SV6R11dUxfzjL7LfzjddlhJ9XoJd5wC:GHQ2dwl38k73DwYm4RHz6u6f1qrshHoH |
| MD5: | AD0FD17D5794369C0515A98359B91C79 |
| SHA1: | 9DBA47E9D07FE5569995917183D5F71700E4BB26 |
| SHA-256: | 29EB735C7E2A9D51DACCFE40CFBAF0BE3945B536B6F5F9F6D2E7D13619533A07 |
| SHA-512: | AAA20052A19213B30DEC9CE88811CA9D309992FBEDBFFFDBBCF203AD6E1A1BAF90876CDB5B0719AEED6BE27BE8872D8CFE39FB2BF9051BCD4524B0E399A2786F |
| Malicious: | false |
| Preview: | ---.-- Library methods for handling Cassandra Thrift communication as client.--.-- @author Vlatko Kosturjak.-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html.--.-- Version 0.1.--..local stdnse = require "stdnse".local string = require "string"._ENV = stdnse.module("cassandra", stdnse.seeall)..--[[.. Cassandra Thrift protocol implementation... For more information about Cassandra, see:.. http://cassandra.apache.org/..]]--..-- Protocol magic strings.CASSANDRAREQ = "\x80\x01\x00\x01".CASSANDRARESP = "\x80\x01\x00\x02".CASSLOGINMAGIC = "\x00\x00\x00\x01\x0c\x00\x01\x0d\x00\x01\x0b\x0b\x00\x00\x00\x02".LOGINSUCC = "\x00\x00\x00\x01\x00".LOGINFAIL = "\x00\x00\x00\x01\x0b".LOGINACC = "\x00\x00\x00\x01\x0c"..--Returns string in cassandra format for login.--@param username to put in for mat.--@param password to put in format.--@return str : string in cassandra format for login.function loginstr (username, password). return CASSANDRAREQ. .. string.pack(">s4", "login"). .. |

| C:\Program Files (x86)\Nmap\nselib\citrixxml.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 16385 |
| Entropy (8bit): | 5.049177271540105 |
| Encrypted: | false |
| SSDEEP: | 384:M7d9TvB0HveZxuzohKMvV4yphM6f1+8nGvqK3jWX:M7d9TvB0PeZphKshnGvqYWX |
| MD5: | 3293C7F8ABB2B1D27E61AC10BDA488D1 |
| SHA1: | 48406453DBBA20C52E9B38CA6F81F52FC855227B |
| SHA-256: | CC8770593AE1D224C5578F0410A6EB4DCBF19F68B294C650AF8098AF2D945D51 |
| SHA-512: | CC1B30C40BC50DC923CD1148AC8440EF64F0DC5A2606E3CDD25CF471DABFAD0050C733D0744383A680E435483D930A187E20F5A8A4DD407280971EBDA4B1FE7 |
| Malicious: | false |
| Preview: | ---.-- This module was written by Patrik Karlsson and facilitates communication.-- with the Citrix XML Service. It is not feature complete and is missing several.-- functions and parameters..--.-- The library makes little or no effort to verify that the parameters submitted.-- to each function are compliant with the DTD.--.-- As all functions handling requests take their parameters in the form of tables,.-- additional functionality can be added while not breaking existing scripts.--.-- Details regarding the requests/responses and their parameters can be found in.-- the NFuse.DTD included with Citrix MetaFrame/Xenapp.--.-- This code is based on the information available in:.-- NFuse.DTD - Version 5.0 (draft 1) 24 January 2008.--....local http = require "http".local stdnse = require "stdnse".local string = require "string".local table = require "table"._ENV = stdnse.module("citrixxml", stdnse.seeall)..--- Decodes html-entities to chars eg.   => <space>.--.-- @param xmldata string t |

| C:\Program Files (x86)\Nmap\nselib\coap.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 76903 |
| Entropy (8bit): | 4.897024033092226 |
| Encrypted: | false |
| SSDEEP: | 1536:vODKJIL39ODAl4KHHENZ0qIjeNJ60qmxiHcGTzeWHvfN6L7m:GlL39ODAl4KHHENZ0qIjKlqmxJGTzeMz |
| MD5: | C7C996FB8AC6C29535DE054D3B5D5AB4 |
| SHA1: | 0FCA72CED8E17A900D414E963CCB1A7C12753716 |
| SHA-256: | 4F089957334E99A37F71612274E130644412E97EB702BEB279ED7272C735552D |
| SHA-512: | A79C70D5BDDD7517CDEBB8425B7501617F936BF0A7DDF7DC1A2A45855B813E9EF81CDB695C7AC149C56FC7ABCB52AE281542C4652456B4FF82F4D86A012EDF9 |
| Malicious: | false |
| Preview: | local comm = require "comm".local json = require "json".local lpeg = require "lpeg".local math = require "math".local nmap = require "nmap".local stdnse = require "stdnse".local string = require "string".local stringaux = require "stringaux".local table = require "table".local unittest = require "unittest"._ENV = stdnse.module("coap", stdnse.seeall)..---.-- An implementation of CoAP.-- https://tools.ietf.org/html/rfc7252.--.-- This library does not currently implement the entire CoAP protocol,.-- only those behaviours which are necessary for existing scripts are.-- included. Extending to accommodate additional control packets should.-- not be difficult..--.-- @author "Mak Kolybabi <mak@kolybabi.com>".-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html..COAP = {}..COAP.build = nil.COAP.parse = nil..COAP.header = {}.COAP.header.build = nil.COAP.header.parse = nil..COAP.header.codes = {}.COAP.header.codes.build = nil.COAP.header.codes.parse = nil..COAP.header.options = { |

| C:\Program Files (x86)\Nmap\nselib\comm.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |

| C:\Program Files (x86)\Nmap\nselib\comm.lua | |
|---|---|
| Size (bytes): | 11295 |
| Entropy (8bit): | 4.641920513034916 |
| Encrypted: | false |
| SSDEEP: | 192:tYdc1towf2gEqaOl0uOxUoVCuOxV44otApJPzINvo5X8gKCiya84GgGZXYiX:tYit+uOxU6CuOxVzp+Nv0a87bX |
| MD5: | 1DB5B74211D74152D379766B2F357998 |
| SHA1: | E0C123333DF8F1329795F963731CD9ABB506C631 |
| SHA-256: | 1652C2B78B9565262C2D0389DE1A9822ABF7CEEFECC15D62FA09EAAE4B36541D |
| SHA-512: | 917E800F91233863FB2EE1827B100F102215C6F447C45960441501C43856F4615085E02DFF9E500186F503EB716AE6C9D599AA7A2C760710C4FF467224EE1A5E |
| Malicious: | false |
| Preview: | ---.-- Common communication functions for network discovery tasks like.-- banner grabbing and data exchange..--.-- The functions in this module return values appropriate for use with.-- exception handling via <code>nmap.new_try</code>..--.-- These functions may be passed a table of options, but it's not required. The.-- keys for the options table are:.-- * <code>bytes</code> - minimum number of bytes to read..-- * <code>lines</code> - minimum number of lines to read..-- * <code>proto</code> - string, prot ocol to use. Default <code>"tcp"</code>.-- * <code>timeout</code> - override timeout in milliseconds. This overrides all other timeout defaults, but can be overridden by specific connect and request timeouts (below).-- * <code>connect_timeout</code> - socket timeout for connection. Default: same as <code>stdnse.get_timeout</code>.-- * <code>request_timeout</code> - additional socket timeout for requests. This is added to the connect_timeout to get a total time for a request to receive |

| C:\Program Files (x86)\Nmap\nselib\creds.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 18700 |
| Entropy (8bit): | 4.633856764074264 |
| Encrypted: | false |
| SSDEEP: | 384:7Ncqd8+8ZXT8ZBSOFDcdGYTjGeYl4WRZ5qigrIhYs5yw/zWlX:ZbdhMiJDOGY34bRZ5oMhYskw7eX |
| MD5: | CF30791F06D59A804D416BDA935E02A7 |
| SHA1: | F8CDF03E915F7380A55614137F0FBA66177457CD |
| SHA-256: | BE51D0586E2E549F3591F2D59678577C9CF740EBA81960E260000F81E16C21A4 |
| SHA-512: | 5EB8C84F3D00AF9BCF97CDA2E1D209A3162F19CF915DD56BC244771D9D9F0EAE9CD571581D7451CB91CF94C42D6D573355381942DBED7D9579048EB309C837A |
| Malicious: | false |
| Preview: | --- The credential class stores found credentials in the Nmap registry.--.-- The credentials library may be used by scripts to store credentials in.-- a common format in the nmap registry. The Credentials class serves as.-- a primary interface for scripts to the library..--.-- The State table keeps track of possible account states and a correspondi ng.-- message to return for each state..--.-- The following code illustrates how a script may add discovered credentials.-- to the database:.-- <code>.-- local c = creds. Credentials:new( {"myapp"}, host, port ).-- c:add("patrik", "secret", creds.State.VALID ).-- </code>.--.-- The following code illustrates how a script can return a table of discovered.-- credentials at the end of execution:.-- <code>.-- return tostring(creds.Credentials:new({"myapp"}, host, port)).-- </code>.--.-- Another script can iterate over cr edential already discovered by other.-- scripts just by referring to the same tag:.-- <code>.-- local c = creds.Credentials:new({" |

| C:\Program Files (x86)\Nmap\nselib\cvs.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 3120 |
| Entropy (8bit): | 4.925474931629765 |
| Encrypted: | false |
| SSDEEP: | 96:pg97OGd+31EDzra1GGNbj5c3yeR8ODL8X:KVOGd+lIP6GGNuyeR8ODL8X |
| MD5: | DD0BB5DA85E777E91B31D260694CDC50 |
| SHA1: | 9B24D8AD709EF47E06E075DDC4C319B7E4394059 |
| SHA-256: | B3124EB8057BF81E553E7F8082202B5DE8B507CD964476F275C2453AFD180925 |
| SHA-512: | A8FEDA77037A2EB68B4AA11F90233C6CF09F3D3A1EDC3EABBD94ED4077863B3D065CACE115F58BBD6E120B32AA0AE436D31D92BEFA88D35233C9B444D485AD58 |
| Malicious: | false |
| Preview: | ---.-- A minimal CVS (Concurrent Versions System) pserver protocol implementation which currently only supports authentication..--.-- @author Patrik Karlsson <p atrik@cqure.net>.-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html.--..-- Version 0.1.-- Created 07/13/2011 - v0.1 - created by Patrik Karlsson <patrik@cqure.net>...local nmap = require "nmap".local stdnse = require "stdnse".local string = require "string".local table = require "table"._ENV = stdnse.module("cvs", stdnse.seeall)...Helper = {.. new = function(self, host, port). local o = { host = host, port = port }. setmetatable(o, self). self.__index = self. return o. end,.. connect = function(self, socket). self.socket = socket or nmap.new_socket(). return self.socket:connect(self.host, self.port). end,.. login = function(self, repo, user, pass ). assert(repo, "No repository was specified"). assert(user, "No user was specified"). assert(pass, "No pass was specified").. -- Ad |

| C:\Program Files (x86)\Nmap\nselib\data\dns-srv-names | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 994 |
| Entropy (8bit): | 4.244525815838589 |
| Encrypted: | false |
| SSDEEP: | 12:x2yrP6vXJtkzGGlItlCs6CcOW4WEmlOfH+mSA815Tamv6ozvB9H9HS:NP858GGlltECRmlOP+mS715GWzB9H9HS |
| MD5: | C4867D3D0BD280B0F2B8897BD74D49BC |

| C:\Program Files (x86)\Nmap\nselib\data\dns-srv-names | |
|---|---|
| SHA1: | 5ADA3DED07A8B3B4D76ED4D0DE3C2E452A88B633 |
| SHA-256: | 7898B97ADBB71294B51B28CA1AB867739A557AED4FACB2F8D69AA46B0E9E7B8B |
| SHA-512: | 7C175AC7794714A03878AED5BC800F0D79B32776FF9CE50FE1B832BCBFBEAE995270EBE70524E99EADD8568E82620F710D7D5FC69B5FB8FD4EA45F7DFEC02C29 |
| Malicious: | false |
| Preview: | _afpovertcp._tcp._aix._tcp._autodiscover._tcp._caldav._tcp._certificates._tcp._client._smtp._cmp._tcp._crls._tcp._crl._tcp._finger._tcp._ftp._tcp._gc._tcp._h323be._tcp._h323be._udp._h323cs._tcp._h323cs._udp._h323ls._tcp._h323ls._udp._h323rs._tcp._hkps._tcp._hkp._tcp._http._tcp._iax.udp._imaps._tcp._imap._tcp._jabber-client._tcp._jabber-client._udp._jabber._tcp._jabber._udp._kerberos-adm._tcp._kerberos._tcp._kerberos._tcp.dc._msdcs._kerberos._udp._kpasswd._tcp._kpasswd._udp._ldap._tcp._ldap._tcp.dc._msdcs._ldap._tcp.gc._msdcs._ldap._tcp.pdc._msdcs._msdcs._mysqlsrv._tcp._nntp._tcp._ntp._udp._ocsp._tcp._pgpkeys._tcp._pgprevokations._tcp._PKIXREP._tcp._pop3s._tcp._pop3._tcp._sipfederationtls._tcp._sipinternal._tcp._sipinternaltls._tcp._sips._tcp._sip._tcp._sip._tls._sip._udp._smtp._tcp._ssh._tcp._stun._tcp._stun._udp._svcp._tcp._tcp._telnet._tcp._test._tcp._tls._udp._vlmcs._tcp._vlmcs._udp._whois._tcp._wpad._tcp._xmpp-client._tcp._xmpp-client._udp._xmpp-server._tcp._xmpp-server._udp. |

| C:\Program Files (x86)\Nmap\nselib\data\drupal-modules.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 243495 |
| Entropy (8bit): | 4.414863708201327 |
| Encrypted: | false |
| SSDEEP: | 6144:gthsjrS4kZyjXZclGjMB3jyDFWzTrGwzPZElPi7:0hs3SZZyjp6jB3jGUzfzPqhi7 |
| MD5: | D47B27A8608013F5E4A55AC173CEEF5D |
| SHA1: | 5013E333E32B352C8D1C00759A831D019FFC53C1 |
| SHA-256: | D4C921466E544E9BC4377D5CF770B734AC3F27B54A6732A6E8F6936388B0C317 |
| SHA-512: | E2321E87CAE1ABAE54A31A30A78E5C622B2E83165A00BD044C507B79AC9031F129CB18142067099F8B2954E9B1F106416C74AAC9E9E04A87871BD30AA47047C8 |
| Malicious: | false |
| Preview: | views.token.ctools.pathauto.libraries.entity.admin_menu.date.imce.jquery_update.ckeditor.wysiwyg.link.webform.backup_migrate.rules.module_filter.google_analytics.views_slideshow.features.xmlsitemap.metatag.captcha.colorbox.media.entityreference.panels.field_group.devel.views_bulk_operations.menu_block.transliteration.l10n_update.imce_wysiwyg.globalredirect.variable.i18n.context.imageapi.advanced_help.filefield.email.page_title.lightbox2.ds.strongarm.superfish.imagefield.calendar.imagecache.references.field_collection.block_class.job_scheduler.menu_attributes.redirect.addressfield.mailsystem.nice_menus.diff.flexslider.taxonomy_menu.file_entity.feeds.media_youtube.node_clone.admin_views.smtp.special_menu_items.auto_nodetitle.jquery_ui.insert.cck.quicktabs.mimemail.views_php.content_access.jcarousel.print.plupload.votingapi.poormanscron.simplenews.filefield_sources.extlink.honeypot.facetapi.logintoboggan.search_api.uuid.commerce.custom_breadcrumbs.views_data_export.oauth.better_formats.si |

| C:\Program Files (x86)\Nmap\nselib\data\drupal-themes.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 13855 |
| Entropy (8bit): | 4.439246344287885 |
| Encrypted: | false |
| SSDEEP: | 192:arI7lm06r1pKq+vr4/A2Jf+r639PlrvRl6ZUFC1hNbF0zpW4Xqgp55fw+hE/fr2u:Esm08/Kq4gf9tSZWQziWcfk26yR0 |
| MD5: | 63A44AF5A33E6B2707B9C5AA0B6AC239 |
| SHA1: | 7961FE6D95454F695D6D8A9CA50F22ABFFF5E4C1 |
| SHA-256: | D6E522F2C059A55FB9DF3227D9762BA9DFAACA2B7A3FE3E8E17566BE6D38A47F |
| SHA-512: | ED9B90ACED93B160735A0BC936D580708E555DBFF285ED50E1C5DCC17B1F587308ABFD8F83A7DE0A1CE0CF14D489EEBDA6E1035C01577F13DD1EB18EA678F92B |
| Malicious: | false |
| Preview: | zen.omega.bootstrap.adaptivetheme.corporateclean.adminimal_theme.marinelli.tao.danland.business.framework.rubik.bluemasters.fusion.shiny.skeletontheme.pixture_reloaded.corolla.nucleus.mayo.omega_kickstart.professional_theme.sky.nexus.andromeda.acquia_marina.mix_and_match.basic.responsive.responsive_bartik.responsive_blog.simplecorp.rootcandy.best_responsive.zeropoint.business_responsive_theme.acquia_prosper.mothership.touch.bamboo.busy.genesis.ninesixty.corporate.ember.aurora.venture_theme.zircon.corkedscrewer.jackson.zurb_foundation.responsive_business.bluez.multipurpose.responsive_green.oa_radix.creative.tb_sirate.urbansolice.impact_theme.footheme.mobile.cti_flex.kanji.radix.journalcrunch.dark_elegant.fresh.blogbuzz.gratis.likable.acquia_slate.boron.business_theme.newsflash.seven.clean_theme.fontfolio.plasma.simpleclean.magazeen_lite.metropolis.clean.company.blueprint.tb_purity.openchurch_theme.platon.colourise.black_premium.blogger_theme.metro_zymphonies_theme.elegant_theme.tma.corp |

| C:\Program Files (x86)\Nmap\nselib\data\enterprise_numbers.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1358909 |
| Entropy (8bit): | 5.504370604058812 |
| Encrypted: | false |
| SSDEEP: | 24576:jb+HpmwOjjZ0DvXo7NW7fboz1fK3gUQGDqXzpXMpEIJr:/+H4wOx0DQ47bo1jUQO08pXr |
| MD5: | 3EAF5CAC6DD43A3F7CAA870289C12C92 |
| SHA1: | B8140290460483CD8FC2835FE184764F8F36D0A3 |
| SHA-256: | 22603ECD64462EE420923D6C7B923F8E03A4DFAB0776AA498F33169756BEB334 |
| SHA-512: | FD143C935179D8C76C9782F77E3530D6423F54A401F57C7B9CCEC2BC1C96DD723311B25DAFA9AE4B64F0E2F7A818F6566A0C29285EE86C606F347F7AF73E144 |

| C:\Program Files (x86)\Nmap\nselib\data\enterprise_numbers.txt | |
|---|---|
| Malicious: | false |
| Preview: | # curl -L http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers \| perl -lne 'if(/^\d/){$x=$_}elsif($x){print"$x\t$_";$x=undef}'.1.NxNetworks.2.IBM (https://w3.ibm.com/standards).3.Carnegie Mellon.4.Unix.5.ACC.6.TWG.7.CAYMAN.8.PSI.9.ciscoSystems.10.NSC.11.Hewlett-Packard.12.Epilogue.13.U of Tennessee.14.BBN Technologies.15.Xylogics, Inc..16.Timeplex.17.Canstar.18.Wellfleet.19.TRW.20.MIT.21.EON.22.Fibronics.23.Novell.24.Spider Systems.25.NSFNET.26.Hughes LAN Systems.27.Intergraph.28.Interlan.29.Vitalink Communications.30.Ulana.31.NSWC.32.Santa Cruz Operation.33.MRV Communications, In-Reach Product Division.34.Cray.35.Nortel Networks.36.DEC.37.Touch.38.Network Research Corp..39.Baylor College of Medicine.40.NMFECC-LLNL.41.SRI.42.Sun Microsystems.43.3Com.44.CMC.45.SynOptics.46.Cheyenne Software.47.Prime Computer.48.MCNC/North Carolina.49.Chippcom.50.Optical Data Systems.51.gated.52.Enterasys Networks Inc..53.Apollo Computers.54.DeskTalk Systems, Inc..55.SSDS.56.Castle Rock |

| C:\Program Files (x86)\Nmap\nselib\data\favicon-db | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 6875 |
| Entropy (8bit): | 5.3532490866896065 |
| Encrypted: | false |
| SSDEEP: | 192:ZClPZ0ZR+HM9FSdLAWku3tP1YNoIu2DR6W7IYq:+PZE9a0xu7YNLu2E9Yq |
| MD5: | 9E2112F5FC76E8038E6C1D0888007760 |
| SHA1: | BFF4494175947C7D3389DABA792E1AC74E8A9685 |
| SHA-256: | D42C4890548963412F8E2146ED54834D94ED1AD6489F87F55C662C9A82C14F77 |
| SHA-512: | 4917B9788CD7162118BDBB051AB75BBCB145364285ED5F084FF2967A6BDFF7978AFA12C957D7E5DCF00A8DCA508B98479C2159C584ED4C3FFCB7294996D413 |
| Malicious: | false |
| Preview: | # These are the most common icons from a scan of all dmoz sites in January.# 2010. Icons are listed in decreasing order by frequency...# Commented-out lines are those that are too broad to be useful in.# identification...156515DA3C0F7DC6B2493BD5CE43F795: Nmap Project.# D41D8CD98F00B204E9800998ECF8427E: empty file.9CEAE7A3C88FC451D59E24D8D5F6F166: Parallels Plesk Panel.63B982EDDD64D44233BAA25066DB6BC1: Joomla! CMS.DCEA02A5797CE9E36F19B7590752563E: Parallels Plesk Panel.64CA706A50715E421B6C2FA0B32ED7EC: Parallels Plesk Panel.6C4EC806C82AB04D6B7D857E6FB68F95: Doteasy web hosting.1CE0C63F8BD1E5D3376EC0AE95A41C08: Parallels Plesk Panel.# ECAA... is a UTF-8 byte order mark, so may be more general..ECAA88F7FA0BF610A5A26CF545DCD3AA: Demand Media domain parking.5B0E3B33AA166C88CEE57F83DE1D4E55: DotNetNuke CMS.59A0C7B6E4848CCDABCEA0636EFDA02B: Blogger blog hosting.6F767458B952D4755A795AF0E4E0AA17: Yahoo! web hosting.E1E8BDC3CE87340AB6EBE467519CF245: BlueHost web hosting.DF055C65114B64B29EA68721F |

| C:\Program Files (x86)\Nmap\nselib\data\http-default-accounts-fingerprints.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 60489 |
| Entropy (8bit): | 4.807294368953702 |
| Encrypted: | false |
| SSDEEP: | 768:E42Z6pjzu16iFO8WD1DvoAmmB+RBPni6xk7vnad3V8zPIyNYs70NWkFs7RWrCZgI:06Jzo4xcAmmo6Xnbt0kjIBevJb |
| MD5: | A4EE6FF42D1DE5ED6CEE72D681C90258 |
| SHA1: | 3A66E8385A5548A14602EF02D2A533406937A2C3 |
| SHA-256: | F8501E0587F0939E75DE6C2309B63FB1BA3A553653D2FA1BC85D4A5F950AEC4C |
| SHA-512: | 8310D115E50B5719A74180C46B32E5B5C31F9805D415CB82BE040BEC12CF887B0C9F5CC1D22E7A96E336880D62C0ED8D1401C63F935E8246A391C5C7E26F828 |
| Malicious: | false |
| Preview: | local base64 = require "base64".local http = require "http".local json = require "json".local math = require "math".local shortport = require "shortport".local stdnse = require "stdnse".local table = require "table".local tableaux = require "tableaux".local url = require "url".local have_openssl, openssl = pcall(require, 'openssl')..---.-- http-default-accounts-fingerprints.lua.-- This file contains fingerprint data for http-default-accounts.nse.--.-- STRUCTURE:.-- * <code>name</code> - Descriptive name.-- * <code>cpe</code> - Official CPE Dictionary entry (optional).-- * <code>category</code> - Category.-- * <code>login_combos</code> - Table of default credential pairs.---- * <code>username</code>.---- * <code>password</code>.-- * <code>paths</code> - Table of likely locations (paths) of the target.-- * <code>target_check</code> - Validation function of the target (optional).-- * <code>login_check</code> - Login function of the target.---..---.-- Requests given path using http.get() b |

| C:\Program Files (x86)\Nmap\nselib\data\http-devframework-fingerprints.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 13168 |
| Entropy (8bit): | 4.476205374823237 |
| Encrypted: | false |
| SSDEEP: | 192:dRTB/2vfBX6szxgCg83SLtngrfgFfgD9BFA5V4/:dZxcfd6szxgCyLtngrfgFfgD9BFAS |
| MD5: | 449AE4C82E135254A9D30B301B7B55D7 |
| SHA1: | 91F9F24E6DA9E6C6F677CAD3E5F7109CAA5D74B6 |
| SHA-256: | 5C341864DDE4B0B44BEF7A36165FD5AF349F215BDBAB324387D5134C969BB5A6 |
| SHA-512: | 18DC9116D0D1572468CB336C597E49712D01D0F552A073412B2A3F119585179FC9D558A3E1230FF452A202CB5A5484AF16C59C8563927D1ABDFDCC4BB1B235E |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\data\http-devframework-fingerprints.lua | |
|---|---|
| Preview: | local http = require "http".local string = require "string".local table = require "table"..---.-- http-devframework-fingerprints.lua.-- This file contains fingerprint data for http-devframework.nse.--.-- STRUCTURE:.-- * <code>name</code> - Descriptive name.-- * <code>rapidDetect</code> - Callback function that is called in the beginning.-- of detection process. It takes the host and port of the target website as.-- arguments..-- * <code>consumingDetect</code> - Callback function that is called for each.-- spidered page. It takes the body of the response (HTML source code) and the.-- requested path as arguments..---...tools = { Django = { rapidDetect = function(host, port).. -- Check if the site gives that familiar Django admin login page.. local response = http.get(host, port, "/admin/").. if response.body then. if string.find(respons e.body, "Log in \| Django site admin") or. string.find(response.body, "this_is_the_login_form") or. str |

| C:\Program Files (x86)\Nmap\nselib\data\http-fingerprints.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 237421 |
| Entropy (8bit): | 4.06986314622259 |
| Encrypted: | false |
| SSDEEP: | 1536:bmLHaT1hucEVHtRtZJdJkcE7j30ORIrDpb1rcR0F06XMg/aJqUzz52Dk6:KLslR0Dpb1rcR0F06XMg/CqUB2r |
| MD5: | 0C00DF88D4CA32B27CADAE64D242BE4C |
| SHA1: | A0B436CE29EE3B17C8CAAA29F17B5CDC4AF59171 |
| SHA-256: | DB570C1CBE271279D160889F60A69DCC6DD20683CEFE3AF71582549A5EF29A8B |
| SHA-512: | 8E0EB7A81C2B6823DCDE952DF2A17193623BE197C8D5A00FC56259CC67D987F867DC880CE2054A936A444DE9407651233732FB241BF13D3540E3555901999A9A |
| Malicious: | false |
| Yara Hits: | • Rule: Hacktool_Strings_p0wnedShell, Description: p0wnedShell Runspace Post Exploitation Toolkit - file p0wnedShell.cs, Source: C:\Program Files (x86)\Nmap\nselib\data\http-fingerprints.lua, Author: Florian Roth |
| Preview: | local io = require "io".local string = require "string".local table = require "table"..---HTTP Fingerprint files, compiled by Ron Bowes with a special thanks to....-- o Kevin Johnson (@secureideas) for the fingerprints that come with Yokoso.-- http://yokoso.inguardians.com.-- o Jason H. (@jhaddix) for helping out with a whole pile of fingerprints he's.-- collected.-- o Bob Dooling.-- o Robert Rowley for the awesome open source cms and README checks.-- http://www.irvineunderground.org.--.-- This file is released under the Nmap license; see:.-- https://nmap.org/book/man-legal.html.--.-- @args http-fingerprints.nikto-db-path Looks at the given path for nikto database..-- It then converts the records in nikto's database into our Lua table format.-- and adds them to our current fingerprints if they don't exist already..-- Unfortunately, our current implementation has some limitations:.-- * It doesn't support records with more than one 'dontmatch' patterns f |

| C:\Program Files (x86)\Nmap\nselib\data\http-folders.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 8503 |
| Entropy (8bit): | 4.281312709326015 |
| Encrypted: | false |
| SSDEEP: | 192:XjGZqOIv4Y5jme++JK1AjfoewGxs17Hrr/6mfeLa3:XjKIv4xemKjfoKSHrDfOa3 |
| MD5: | A785468BFFD73D65E1FF9DA135EBBD2B |
| SHA1: | 0ACFE6B048455EC6AC6AC2223B836CE9C84C24D5 |
| SHA-256: | 4094EBC956980DE9328D8458A73D622B9049A4051FE32CCD8E545314C5EBC71F |
| SHA-512: | 88F2CE1B6D2E9754116156312D96B3B6DCC099740F1AEEBC088CAC57D023E0FE10E3B30960092B6F251FB42FD732B884D34FF10C8B5B3013111624537CC13F96 |
| Malicious: | false |
| Preview: | /.git/./.htaccess/./1/./2/./3/./4/./5/./6/./7/./8/./9/./10/./a/./acceso/./access/./accesswatch/./acciones/./account/./accounting/./active/./activex/./adm/./admcgi/./admentor/./admin/./admin_/./admin.back/./admin-bak/./Admin_files/./administration/./administrator/./admin-old/./adminuser/./adminweb/./adminWeb/./admisapi/./AdvWebAdmin/./Agent/./agentes/./Agents/./Album/./AlbumArt/./AlbumArt_/./allow/./analog/./anthill/./apache/./apache2/./app/./appl/./applets/./application/./applications/./applmgr/./apply/./apps/./appsec/./ar/./archive/./archives/./arcsight/./asa/./asp/./atc/./atom/./aut/./auth/./authadmin/./author/./authors/./aw/./ayuda/./b/./b2-include/./back/./backend/./backup/./backups/./bad/./bak/./banca/./banco/./bank/./banner/./banner01/./banners/./bar/./batch/./bb-dnbd/./bbv/./bdata/./bdatos/./beef/./beta/./billpay/./bin/./binaries/./binary/./blog/./boadmin/./boot/./bottom/./browse/./browser/./bsd/./btauxdir/./bug/./bugs/./bugzilla/./buy/./buynow/./c/./cache/./cached/./cache-stats |

| C:\Program Files (x86)\Nmap\nselib\data\http-sql-errors.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2889 |
| Entropy (8bit): | 4.973052692201362 |
| Encrypted: | false |
| SSDEEP: | 48:j++CokFYa5fhuV1d4XQu8LbjMuMXMvVP5Pglrbc01bDqhmLqHxWaNd2yxrgUgxcX:tFuYic1d4Au83jMuMXMvVhoOIqQLGWSV |
| MD5: | 5093E698CF4FB9B090FC511D601FACA3 |
| SHA1: | 831785C2C1E86AAABC36B818950D63982C8CA982 |
| SHA-256: | EEFD27DED1D048B5F613A6AC5D4CD9DBC20C3C894BDC6B2319677419A964DACB |
| SHA-512: | 5FE2C0A70C5DE54D043EE2AEDEB3A405C9A1CA5AA528BD660895B063F24D82047FCEBBCDD67C7D3D9AD1DB0E1FDF0C9DD94EF9088F5A1AB5E6CD9AB2BF428CB2 |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\data\http-sql-errors.lst | |
|---|---|
| Preview: | # this list is taken from http://code.google.com/p/fuzzdb/ as allowed by its New BSD license.# some entries have been deleted because they caused a lot of false positives .A syntax error has occurred.ADODB%.Field error.ASP%.NET is configured to show verbose error messages.ASP%.NET_SessionId.Active Server Pages error.An error occured.An illegal character has been found in the statement.An unexpected token \"END%-OF%-STATEMENT\" was found.CLI Driver.Call to member function.Can\'t connect to local.Custom Error Message.DB2 Driver.DB2 Error.DB2 ODBC.Died at.Disallowed Parent Path.Error Diagnostic Information.Error Message : Error loading required libraries.Error Report.Error converting data type varchar to numeric.Error executing Database Query.Fatal error.Incorrect syntax near.Internal Server Error.Invalid Path Character.Invalid procedure call or argument.Invision Power Board Database Error.JDBC Driver.JDBC Error.JDBC MySQL.JDBC Oracle.JDBC SQL.Microsoft JET Database.Microsoft OLE DB Provid |

| C:\Program Files (x86)\Nmap\nselib\data\http-web-files-extensions.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1058 |
| Entropy (8bit): | 4.2620678001307 |
| Encrypted: | false |
| SSDEEP: | 24:TgjIBM0QgspL9iLGsYx+nBWUgUDNAApNhydBpGvSAzdWTEMapjwx2p:kMBM0BsjCGsEPNUBLDKAJWTGjwMp |
| MD5: | ED4D6E7F679F31978D985333218E8A6C |
| SHA1: | E5A03CE3C47C2A482F546AEAFA834968C44446FB |
| SHA-256: | AFF15B905BB6578B06B219C659716F5E925B1791C510684F91CF178B19DBF81F |
| SHA-512: | C8D0EDD29A202EF2F721DBCE4F6F977FA45D931E5EDD3E5B0FF9C50B3D0E150A651D5BEB72539847B5FCE4F044893D57E208A0EEF21EACEDD269ED3F498A77F |
| Malicious: | false |
| Preview: | a4p.a5w.adp.adr.aex.alx.ap.aro.asa.asax.ascx.ashx.asmx.asp.aspx.asr.atom.att.awm.axd.bml.bok.browser.btapp.bwp.cdf.cer.cfm.cfml.cgi.cha.chat.chm.cms.codasite.compressed.con.cpg.crdownload.crl.crt.cshtml.csp.csr.css.dap.dbm.dcr.der.dhtml.disco.discomap.dll.dml.do.dochtml.docmhtml.dothtml.download.dtd.dwt.ece.edge.epibrw.esproj.ewp.fcgi.fmp.fwp.gne.gsp.hdm.hdml.htaccess.htc.htm.html.htx.hxs.hype.idc.ihtml.iqy.itms.itpc.iwdgt.jcz.jhtml.jnlp.js.json.jsp.jspa.jspx.jst.jvs.jws.las.lasso.lassoapp.lbc.less.maff.map.mapx.master.mht.mhtml.moz.mspx.mvc.mvr.nxg.nzb.obml.ognc.opml.oth.p12.p7.p7b.p7c.pac.page.pem.php%d?.phtm.phtml.pl.ppthtml.pptmhtml.prf.pro.psp.ptw.pub.qbo.qf.qrm.rhtml.rjs.rna.rss.rt.rw3.rwp.rwsw.rwtheme.saveddeck.sdb.seam.sht.shtm.shtml.site.sitemap.sites2.spc.srf.ssp.stc.stl.stm.stml.stp.suck.svc.svr.swz.tvpi.tvvi.ucf.uhtml.url.vbd.vbhtml.vlp.vrml.vsdisco.wbxml.wdgt.web.webarchive.webbookmark.webhistory.webloc.website.webz.wgp.wgt.whtt.widget.wml.wn.woa.wpp.wpx.wrf.wsdl.xbel.xbl. |

| C:\Program Files (x86)\Nmap\nselib\data\idnaMappings.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 621926 |
| Entropy (8bit): | 5.297993620057116 |
| Encrypted: | false |
| SSDEEP: | 6144:bp4+nlxWr4slH/85IAQ6WE7S3tL4+elf+j/lVw0S4pBSSOMSb342Cn58DYwwzeMd:bW/a/Cb3TgLDTWS0Ptod |
| MD5: | 84F50D50957ECC2ECBAAE286C8AD9751 |
| SHA1: | 3986FD3251A7FCDA5B17D0CDECF31A80D521AC21 |
| SHA-256: | F5FA072626E1B374A74E00BEF7267BB2529C82704DAE13EA9BD2DB1C9343DE46 |
| SHA-512: | 6A9930BEA68F6C4D61718F22A6BA4F9036A1AD7CC88B3F135CF2B4BB27A4E4134DBA4C4BA255987BEF89715A4EB316859B12FAC6AE4EE467CE9E3B804A4D7516 |
| Malicious: | false |
| Preview: | ---.-- Library mapping for handling codepoints according to IDNA standard..--.-- All the mappings are imported from Version 10.0.0 of UTS #46, Unicode IDNA.-- Compatibility Processing..-- References:.-- * http://www.unicode.org/Public/idna/10.0.0/.--.-- @author Rewanth Cool.-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html..local stdnse = require "stdnse"._ENV = stdnse.module("idnaMappings", stdnse.seeall)..-- The Unicode Consortium approved the mappings below..tbl = {. [0x002F] = {status="disallowed"}, -- SOLIDUS. -- HYPHEN-MINUS..FULL STOP. [0x002D] = {status="valid"},. [0x002E] = {status="valid"},. [0x0041] = 0x0061, -- LATIN CAPITAL LETTER A. [0x0042] = 0x0062, -- LATIN CAPITAL LETTER B. [0x0043] = 0x0063, -- LATIN CAPITAL LETTER C. [0x0044] = 0x0064, -- LATIN CAPITAL LETTER D. [0x0045] = 0x0065, -- LATIN CAPITAL LETTER E. [0x0046] = 0x0066, -- LATIN CAPITAL LETTER F. [0x0047] = 0x0067, -- LATIN CAPITAL LETTER G. [0x0048] = 0x0068, -- LATIN CAPITAL LETTER H. [0x |

| C:\Program Files (x86)\Nmap\nselib\data\ike-fingerprints.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 61424 |
| Entropy (8bit): | 5.049962771359542 |
| Encrypted: | false |
| SSDEEP: | 1536:/mbbQZqf18uS0TbjrWyp0htkFq5StddtDxCtuGgBPVu4EqR/2+E76fp2riakEtW+:/mbbQZqf18uS0TbjrWyp0htkFq5StddW |
| MD5: | CB94D10BAB6781E469A37BB792C0A794 |
| SHA1: | B49E5811B3D5E47D5A29F29DBC3961AFE3D71D9D |
| SHA-256: | 706C51F66C1183B1AF00A3F2FA703B59C089AC067DF7910BF17E0C0BF70ACC35 |
| SHA-512: | 11F2934917DE2B3C1C0D0D4CC41F41A9EA0E217FC7BDE3343B581CBC4688A321A5F96499E29DBE3AD6FE67B2B67BE223DFFEEAB6718105159AF7B56E57566AEF |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\data\ike-fingerprints.lua | |
|---|---|
| Preview: | local table = require 'table'..--[[.This is compiled list of known IKE vendor IDs...Most of the VIDs have been copied from ike-scan with permission from.the original author, Roy Hills, so a big 'thank you' is in order..-- http://www.nta-monitor.com/wiki/index.php/Ike-scan_Documentation..Unknown ids:. ab926d9ee113a0219557fcc54e52865c (Citrix NetScaler ?). 5062b335bc20db32c0d54465a2f70100 (fortigate ?). 4f4540454371496d7a684644 (linksys ?). 9436e8d67174ef9aed068d5ad5213f187a3f8ba600000160000061e (Netscreen 5XP running ScreenOS 4.0.r3)..]]..author = {"Jesper Kueckelhahn", "Roy Hills"}.license = "Simplified (2-clause) BSD license--See https://nmap.org/svn/docs/licenses/BSD-simplified"...fingerprints = {};..----------.-- Vendor ID Fingerprints.---------- |

| C:\Program Files (x86)\Nmap\nselib\data\jdwp-class\JDWPExecCmd.class | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1103 |
| Entropy (8bit): | 5.473871978150859 |
| Encrypted: | false |
| SSDEEP: | 24:S7RrJkyQulgPlIIXQHWPuzEWPfshgmixKMvOc:S8yFlgPlCWPuzEifshwD7 |
| MD5: | 6FA3D82616BBA4E0FF671FC6DF9787FC |
| SHA1: | 572A3EE68E728812B7E71C9D62B14150736D25E9 |
| SHA-256: | 07324B71438054FEBC1A0BE08133D08959B76E119558322107498F76B3BD44B7 |
| SHA-512: | BD8385DC4CC369BA9C2BF068335B1625F9133AB15E2D9F6231CBFBD30E1A5AE3B2C60885BB93D252F0222263B8611B5BA370D73638DA0AAF63A8106B357D103A |
| Malicious: | false |
| Preview: | .....3.G....!..".....!....#..$....%..&.'..&.(..)..*..+.,....-...../..0.1..2..3..4..5...<init>...()V...Code...LineNumberTable...run..&(Ljava/lang/String;)Ljava/lang/String;...StackMapTable..6..7..)..3...SourceFile...JDWPExecCmd.java.....java/lang/StringBuilder..8.9... output:...:.;..<..=.>..?.@...java/io/BufferedReader...java/io/InputStreamReader..7..A.B....C....D..E.;..6..F.;.....java/lang/Exception...JDWPExecCmd...java/lang/Object...java/lang/String...java/lang/Process...append..-(Ljava/lang/String;)Ljava/lang/StringBuilder;...toString...()Ljava/lang/String;...java/lang/Runtime...getRuntime...()Ljava/lang/Runtime;...exec..'(Ljava/lang/String;)Ljava/lang/Process;...getInputStream...()Ljava/io/InputStream;...(Ljava/io/InputStream;)V...(Ljava/io/Reader;)V...readLine...trim.!.....*.....u...Y...*.....L...*...M...Y...Y,.....N.:.-...Y:..."...Y...+.....L.....Y...+.....L...M+.....o.r..... |

| C:\Program Files (x86)\Nmap\nselib\data\jdwp-class\JDWPExecCmd.java | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 865 |
| Entropy (8bit): | 5.004808862781372 |
| Encrypted: | false |
| SSDEEP: | 12:8GwfH7eNIbP8rAcNDYCoSt33wCgFrg4xSvRPBBvsue2uWAEAJgaEN5G8sDoN4:qfFb0rPD1o23IF4vRPvZeLWRsgaE68Z4 |
| MD5: | DD2769BF90FBA3D9C17C1C35EA52EF07 |
| SHA1: | CC7F98B988473B802C2712FBFD712B025B4C7DB3 |
| SHA-256: | 8F30D00EA5EAA5C4020406DAA5A4628538829C5B13953E535C96B4F4BC1DB2C5 |
| SHA-512: | 59294A0BF13CEF851047310EF926E27F294B6C32102429C29F4FBD3B54F2F00531557331E6DFD35D712A555914E4447BC1B42DA0AB982061D33B7518D154834D |
| Malicious: | false |
| Preview: | import java.io.*;../* This is the JDWPExecCmd source used for jdwp-exec script to execute. * a command on the remote system.. *. * It just executes the shell command passed as string argument to. * run() function and returns its output.. *. * Compile simply with:. * javac JDWPExecCmd.java (should be in the nselib/data/ directory).. *. * author = "Aleksandar Nikolic". * license = "Same as Nmap--See https://nmap.org/book/man-legal.html".*/..public class JDWPExecCmd {. public static String run(String cmd) {...String result = cmd + " output:\n";...try{....Process p = Runtime.getRuntime().exec(cmd);....BufferedReader in = new BufferedReader(new InputStreamReader(p.getInputStream()));....String line = null;....while ((line = in.readLine()) != null) {.....result += line.trim()+"\n";....}....result += "\n";...}catch(Exception ex){....}...return result;..}.}. |

| C:\Program Files (x86)\Nmap\nselib\data\jdwp-class\JDWPSystemInfo.class | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2162 |
| Entropy (8bit): | 5.64658542717645 |
| Encrypted: | false |
| SSDEEP: | 48:xpiV+rEAyFlCAMurBpCskNxTFh8No2z/QMw80eVkEJi43pTYrZUJ:U9FluulosOL8aLX8vi6p8O |
| MD5: | A7F888DAED3A426D880E98976AFE2067 |
| SHA1: | 5CCB04C5E561AB69F13EA596673E46E31E4B4F24 |
| SHA-256: | EA50C59AB2C2369E24E0396905B44D827C47FCD5FFF59B2E04F947C2EB888E8C |
| SHA-512: | 9C3B0C1FAE6AF35F9BB4F3703A1616EC70FAED7811C25D4BEB36831F2F877782E80515762191381073872EACA4C6BAB17A1DD93390B000515F8A697DE800A330 |
| Malicious: | false |
| Preview: | .....3....-.;..<..=....;....>..?..@.A..@.B....C..D....E..F..@.G....H..I.J..K..I.L..M..I.N..O..I.P..Q..R..S.T..U..V..W..X..Y..Z..[..\..]..^..._..`..a..%.;..b....c..S.d..,.e..f.g..h..i...<init>...()V...Code...LineNumberTable...run...()Ljava/lang/String;...StackMapTable..j..k...main...([Ljava/lang/String;)V...SourceFile...JDWPSystemInfo.java..../.....java/lang/StringBuilder..l.m...Available processors: ..n..o.p..q.r..l.s.....t.3...Free memory: ..u.v..l.w..x..y.z...File system root: ..{.3...Total space (bytes): ..|.v...Free space (bytes): ..}.v...Name of the OS: ...os.name..~.....OS Version : ...os.version...OS patch level : ...sun.os.patch.level...OS Architecture: ...os.arch...Java version: ...java.version...Username: ...user.name...User home: ...user.home...java/util/Date...System time: ..l.....2.3.....JDWPSystemInfo...java/lang/Object...java/lang/String...[Ljava/io/File;...append..-(Ljava/lang/String;)Ljava/lang/StringBuilder;...java/lang/Runtime...getRuntime...()Ljava/l |

| C:\Program Files (x86)\Nmap\nselib\data\jdwp-class\JDWPSystemInfo.java | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1555 |
| Entropy (8bit): | 4.98796508919239 |
| Encrypted: | false |
| SSDEEP: | 48:4XLfUejJBpBQMW+GFDVlbzMSW45kJGyjxVuHSsPVGs:4XLcejzMl+GFDVlbzMB45PyjxQy8X |
| MD5: | 567932E2E0AEFA97D458DE20F581478E |
| SHA1: | B7C9924CEA2F320B06BA45049B2A66A0AE0A239F |
| SHA-256: | 928EF633E4A8E80668010957B7AE64B9E840E4D0FA88251A4FBC4A9D0DA1B5DA |
| SHA-512: | 33CAC44381BFE0540DD7BAFD07BDFA9584E4FA6EDE64E6BE4A32092AEE0DCA41D7E42737C43A782D03AC35166BC764A246ABB98586DD6C47BD7B1A1D44183<br>2B1 |
| Malicious: | false |
| Preview: | import java.io.*;.import java.util.Date;./* This is the JDWPSystemInfo source used for jdwp-info script to get remote. * system information.. *. * Compile simply with:. * javac JDWPSystemInfo.java (should be in the nselib/data/jdwp-class directory).. *. * author = "Aleksandar Nikolic". * license = "Same as Nmap--See https://nmap.org/book/man-legal.html".*/..public class JDWPSystemInfo {.  public static String run() {...String result = "";...result += "Available processors: " +  Runtime.getRuntime().availableProcessors() + "\n";...result += "Free memory: " + Runtime.getRuntime().freeMemory() + "\n";...File[] roots = File.listRoots();...for (File root : roots) {....result += "File system root: " + root.getAbsolutePath() + "\n";....result += "Total space (bytes): " + root.getTotalSpace() + "\n";....result += "Free space (bytes): " + root.getFreeSpace() + "\n";...}...result += "Name of the OS: " + System.getProperty("os.name") + "\n";...result += "OS Version : " + System.getProperty("os. |

| C:\Program Files (x86)\Nmap\nselib\data\jdwp-class\README.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 977 |
| Entropy (8bit): | 4.878067975469626 |
| Encrypted: | false |
| SSDEEP: | 24:XOWxOvNTLCCzMEUW2KcTsDnr9H3mbg+Xptf534gAWRhV:XO6wNTLzIEP2Kc4pmE+5tf534gX9 |
| MD5: | 572552CBAC6E1ED44F456660816FDE22 |
| SHA1: | 0917FE2AAC6767CB4BF7F28EE7F268F3770C9A1B |
| SHA-256: | C89A0A7AD184BC75CB077BB49C9920BBBEA886B222790112C00715E2672B2B37 |
| SHA-512: | 5108B00027434DF8B6CDC3535B83499052F4614C1030207852CED1C3AA0182B883CCE70ECD4E46A59AAB5721087EC23A3D27F40AE5A20D5F07D6C2623911050 |
| Malicious: | false |
| Preview: | This directory contains sources and compiled classes.used by jdwp-* scripts...All classes must have run() method defined which is.expected to return a string..Method run() can have arguments, but then the scripts.would need to be modified to add those arguments when.class is injected. As JDWPExecCmd has a run() method.which accepts a string as its argument, see.jdwp-exec script for details of passing the.arguments to a method via JDWP..Arguments need to be tagged with their respective type..For other tags see http://docs.oracle.com/javase/6/docs/technotes/guides/jni/spec/types.html#wp9502 ..Example from jdwp-exec:...local cmdID..status,cmdID = jdwp.createString(socket,0,cmd)..local runArgs = string.pack(">B I8", 0x4c, cmdID) -- 0x4c is object type tag..-- invoke run method..local result..status, result = jdwp.invokeObjectMethod(socket,0,injectedClass.instance,injectedClass.thread,injectedClass.id,runMethodID,1,runArgs)..To compile these sources:.# javac *.java... |

| C:\Program Files (x86)\Nmap\nselib\data\mgroupnames.db | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 18460 |
| Entropy (8bit): | 4.785131069272309 |
| Encrypted: | false |
| SSDEEP: | 192:gwdGQn+p0rFaC3/T9R82lHP9FQEEG5D4WPswRbQLteLzbkn89zBrbY8vemDr8lRh:fdrfRaCv5R8uHPGWPqaQngBXWus |
| MD5: | A7849253480CD43E3441C64E7C9AC7F4 |
| SHA1: | 3E7C48173268662FA2A7137E3D0B7DB05C4B85B2 |
| SHA-256: | B20D16181F5A52B9AB260E0923D8AC4C2C94957E7548A0E083F4D5FAEA0FA394 |
| SHA-512: | C8CC1E8CC93B81A13DB1A0504CAFDD0DD7010CC3B48E1414C3F9B2C941ECD439C9A5E5EBF0E47F0A826D65F1F7BD95C7B3FACE9AEB88FE4800CD841C50DB<br>81C5 |
| Malicious: | false |
| Preview: | 224.0.0.0.224.0.0.0.Base Address (Reserved) (rfc1112).224.0.0.1.224.0.0.1.All Systems on this Subnet (rfc1112).224.0.0.2.224.0.0.2.All Routers on this Subnet.224.0.0.3.224.0.0.3.Unassigned.224.0.0.4.224.0.0.4.DVMRP  Routers (rfc1075).224.0.0.5.224.0.0.5.OSPFIGP  OSPFIGP All Routers (rfc2328).224.0.0.6.224.0.0.6.OSPFIGP  OSPFIGP Designated Routers (rfc2328).224.0.0.7.224.0.0.7.ST Routers (rfc1190).224.0.0.8.224.0.0.8.ST Hosts (rfc1190).224.0.0.9.224.0.0.9.RIP2 Routers (rfc1723).224.0.0.10.224.0.0.10.EIGRP Routers.224.0.0.11.224.0.0.11.Mobile-Agents.224.0.0.12.224.0.0.12.DHCP Server / Relay Agent.224.0.0.13.224.0.0.13.All PIM Routers.224.0.0.14.224.0.0.14.RSVP-ENCAPSULATION.224.0.0.15.224.0.0.15.all-cbt-routers (rfc2189).224.0.0.16.224.0.0.16.designated-sbm.224.0.0.17.224.0.0.17.all-sbms.224.0.0.18.224.0.0.18.VRRP (rfc5798).224.0.0.19.224.0.0.19.IPAllL1ISs.224.0.0.20.224.0.0.20.IPAllL2ISs.224.0.0.21.224.0.0.21.IPAllIntermediate Systems.224.0.0.22.224.0.0.22.IGMP.224.0.0.23.224.0.0.23.G |

| C:\Program Files (x86)\Nmap\nselib\data\mysql-cis.audit | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 9796 |

| C:\Program Files (x86)\Nmap\nselib\data\mysql-cis.audit | |
|---|---|
| Entropy (8bit): | 5.162467992782524 |
| Encrypted: | false |
| SSDEEP: | 192:EEfCHXd3e+mH83emhAGC1Y22vND2caP92CQ623oM2iPh2aJI2F9xKlW3:EEfMdOrcumhAGyhK0F6dwaME |
| MD5: | 25CBF8C4FCF5D200991C99F4694B0B6F |
| SHA1: | 750E9AE1B88C068FEA0D2614033FB63FC444189A |
| SHA-256: | 64CB0AF05E9C6E1E9A011D75039F30E94D674D2129196A3841058B3B93068D92 |
| SHA-512: | 691774FCDE13EB5C910EFCAD18B01FC5B54EB132D1FBBD2F8F797983324BAE8D1AE310BE033A994F47D8716A01846B823C8B4ADC4F2C8827D64F846DAA3DE9CF |
| Malicious: | false |
| Preview: | local stdnse = require "stdnse".local tab = require "tab".local table = require "table"..-- Defined in mysql-audit.nse.-- makes nse-check-globals complain, but that's ok.local test = test..TEMPLATE_NAME="CIS MySQL Benchmarks v1.0.2"..-- These accounts should be treated as admins and excluded from some of the results.AD MIN_ACCOUNTS={"root", "debian-sys-maint"}..-- Checks whether a resultset is empty or not.local function isEmpty(rows). if ( #rows > 0 ) then return false end. return tr ue.end..-- Extracts a column from a row and return all occurances as an array.local function col2tab(rs, cname). local tab = {}. local cpos. for i=1, #rs.cols do. if ( rs.col s[i].name == cname ) then. cpos = i. break. end. end. if ( not(cpos) ) then. return. end. for _, row in ipairs(rs.rows) do table.insert(tab, row[cpos]) end. return tab.end..local function createINstmt(tab). local tab2 = {}. for i=1, #tab do tab2[i] = ("'%s'"):format(tab[i]) end. return table.concat(tab2, |

| C:\Program Files (x86)\Nmap\nselib\data\oracle-default-accounts.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 8317 |
| Entropy (8bit): | 4.841889406065689 |
| Encrypted: | false |
| SSDEEP: | 192:2VuNd+aCpoRlUVCJTWJHxIaPrNNpPGvxcd0TaFIIPQGr:NIaCSRlUV4WJH/PZyvxcdaarPQY |
| MD5: | 97D95F7217BDE0F086091DE943AE2227 |
| SHA1: | 3FCDD9F3F79D8124172372B42660E6D148619C25 |
| SHA-256: | B576395DF271841B6A164B72909D7F69E8227FAB321167D979EFF80F35DA8D60 |
| SHA-512: | 8DE37612C82E855ED29687C49CE1BED3154AEDFBBE66C7484FBAE761021B7378F790242DF7838C3B513739ED8BDEF3B322E633E2FB645ECAE73C7F2D4B05680 |
| Malicious: | false |
| Preview: | #!comment: This password file was created from the hashes in dfltpass.sql a.#!comment: script created by Oracle to scan databases for default credentials..AASH/ AASH.ABA1/ABA1.ABM/ABM.AD_MONITOR/LIZARD.ADAMS/WOOD.ADS/ADS.ADSEUL_US/WELCOME.AHL/AHL.AHM/AHM.AK/AK.AL/AL.ALA1/ALA1.ALLU SERS/ALLUSERS.ALR/ALR.AMA1/AMA1.AMA2/AMA2.AMA3/AMA3.AMA4/AMA4.AMF/AMF.AMS/AMS.AMS1/AMS1.AMS2/AMS2.AMS3/AMS3.AMS4/AMS4.AM SYS/AMSYS.AMV/AMV.AMW/AMW.ANNE/ANNE.AOLDEMO/AOLDEMO.AP/AP.APA1/APA1.APA2/APA2.APA3/APA3.APA4/APA4.APPLEAD/APPLEAD.APPLSY S/FND.APPLSYS/APPS.APPLSYSPUB/PUB.APPS/APPS.APS1/APS1.APS2/APS2.APS3/APS3.APS4/APS4.AQDEMO/AQDEMO.AQJAVA/AQJAVA.AQUSER/A QUSER.AR/AR.ARA1/ARA1.ARA2/ARA2.ARA3/ARA3.ARA4/ARA4.ARS1/ARS1.ARS2/ARS2.ARS3/ARS3.ARS4/ARS4.ART/ART.ASF/ASF.ASG/ASG.ASL/ASL.ASN/AS N.ASO/ASO.ASP/ASP.AST/AST.AUC_GUEST/AUC_GUEST.AUTHORIA/AUTHORIA.AX/AX.AZ/AZ.B2B/B2B.BAM/BAM.BCA1/BCA1.BCA2/BCA2.BEN/BEN.BIC/BIC.BI L/BIL.BIM/BIM.BIS/BIS.BIV/BIV.BIX/BIX.BLAKE/PAPER.BMEADOWS/BMEADOWS.BNE/BNE.BOM/BOM.BP01/BP01.BP02/B |

| C:\Program Files (x86)\Nmap\nselib\data\oracle-sids | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 5173 |
| Entropy (8bit): | 4.72202257441554 |
| Encrypted: | false |
| SSDEEP: | 96:Otx7gVWGKso5hlfBDyzgOMDs3mNNi+r/hYxsDv+mBKU9m7cpNswJ721Xk8HK5Mr1:x7KRh3PtbPBDuem2D58HK5MrtEVW/Q2x |
| MD5: | 6B9FDC77E794229D2DBF825DDD8D631B |
| SHA1: | E477D3112534B7BF307B3793AB229F04F06B8C28 |
| SHA-256: | B3C41F298AED355CD0A0F37DED8BEC50DEAE684BEA44E2B7B50709877EEFC502 |
| SHA-512: | 69C8D36F069ED279CF480495A2AD40803C1E89E595442C6C1B7AC0C2A3FF712A53B023145D6F30549405A781FC090965F8D90EF265A7E68180698E5C526C3EC2 |
| Malicious: | false |
| Preview: | #!comment: This database is made by Red Database Security and was released.#!comment: under the Nmap license by Alexander Kornbrust..#!comment: Ref: http://secl ists.org/nmap-dev/2009/q4/645.ORCL.XE.ASDB.IASDB.OEMREP.ORCL.WORLD.ADV1.ADVCPROD.AIX10.AIX11.AIX9.APEX.ARIS.ASDB0.ASDB1.ASDB2.ASDB 3.ASDB4.ASDB5.ASDB6.ASDB7.ASDB8.ASDB9.ASG817.ASG817P.ASG817T.ATRPROD.ATRTEST.BLA.BOOKS.BUDGET.C630.CTM4_0.CTM4_1.CTM4_6. D.D10.D8.D9.DB.DB01.DB02.DB03.DB1.DB2.DB2EDU.DB2PROD.DB2TEST.DB3.DBA.DBA1.DBA2.DBA3.DBA4.DBA5.DBA6.DBA7.DBA8.DBA9.DBX.DEMO.DEV.DEV 0.DEV01.DEV1.DEV2.DEV3.DEV4.DEV5.DEV6.DEV7.DEV8.DEV9.DEVEL.DIA1.DIA2.DIS.DWH.DWHDB.DWHPROD.DWHTEST.DWRHS.EARTH.ELCARO.EM RS2.EOF.ERP.ESOR.FINDEC.FINPROD.FNDFS_HR1.FNDFS_HR2.FPRD.GR01.GR02.GR03.HCDMO.HEDGEHOG.HPUX10.HPUX11.HPUX9.HR.HR0.HR1.HR 2.HR3.HR4.HR5.HR6.HR7.HR8.HR9.HRDMO.HTMLDB.IAGTS.INCD.ISD01.ISD06.ISP.ISP01.ISP1.ISP2.ISQ1.ITS.IXOS.KRAUS.KRONOS.LDAP.LIN10.LIN11. LIN9.LINUX101.LINUX1011.LINUX1012.LINUX1013.LINUX1014.LINUX1015.LINUX102.LINUX1021.LINUX10 |

| C:\Program Files (x86)\Nmap\nselib\data\packetdecoders.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 29943 |
| Entropy (8bit): | 4.60103713934378 |
| Encrypted: | false |

| C:\Program Files (x86)\Nmap\nselib\data\packetdecoders.lua | |
|---|---|
| SSDEEP: | 768:WurlOezIV1M9uf30ODk8lWTq8FLU6vnElicXdli5C:dlOvHM9u5kN8K6nti8dli5C |
| MD5: | A20802714EAB29943483F4B7D4CC6C3C |
| SHA1: | 1D16EB445E5A5CA9891B1345A9B9FFC73816A116 |
| SHA-256: | 7E4E0D4238631794E4D04EE5924485569879C301AFB80B2EC5A09667DA6070BB |
| SHA-512: | E414EDD04C24ED25D6130DFB430D9639651C1670B5E87F868D4DDEAB07D7D6809E6336661BCF054DAA6EBDB1807607DBAF26F37FE27BB88B58D77BD2D49B4E83 |
| Malicious: | false |
| Preview: | local ipOps = require "ipOps".local packet = require "packet".local stdnse = require "stdnse".local string = require "string".local stringaux = require "stringaux".local tab = require "tab".local table = require "table".local target = require "target"..--- The following file contains a list of decoders used by the.-- broadcast-listener script. A decoder can be either "ethernet" based or IP.-- based. As we're only monitoring broadcast traffic (ie. traffic not.-- explicitly addressed to us) we're mainly dealing with:.-- o UDP broadcast or multicast traffic.-- o ethernet broadcast traffic.--.-- Hence, the Decoder table defines two sub tables ether and udp..-- In order to match an incoming UDP p acket the destination port number is.-- used, therefore each function is indexed based on their destination port.-- for the udp based decoders. For the ether table each d ecoder function is.-- indexed according to a pattern that the decoding engine attempts to match..--.-- Each decoder defines three |

| C:\Program Files (x86)\Nmap\nselib\data\passwords.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 40388 |
| Entropy (8bit): | 4.620717013058523 |
| Encrypted: | false |
| SSDEEP: | 768:a8/YPRywhL+J37355t3dqVbHk8Wyz86jX5/p34WsprHDMmPgLWHf:aXPRyw9+JL3Pt3wVbQfgp/p3EprbPgLs |
| MD5: | AB2AF238CB3E7D200D22D1E85315DD1C |
| SHA1: | 776EDFDD82F49B0FFCB1AEFB61AC17D5FB4DB786 |
| SHA-256: | 4117FDE172949E0F827AC130C48DFCF0C20DFB9D4B045E3B14C29CEBDC505D8A |
| SHA-512: | C4CD6FD26B5068203DDB77A243441501A2199C73928AA309CC60BC75134C01972E0376ABCD66556926050CA2E3623375DBF065EB259049B3E792ADE1DD49C59 |
| Malicious: | false |
| Preview: | #!comment: This collection of data is (C) 1996-2020 by Insecure.Com LLC..#!comment: It is distributed under the Nmap Public Source license as.#!comment: provided in the LICENSE file of the source distribution or at.#!comment: https://svn.nmap.org/nmap/LICENSE . Note that this license.#!comment: requires you to license your own work under a compatable open source.#!comment: license. If you wish to embed Nmap technology into proprietary.#!comment: software, we sell alternative licenses (contact sales@insecure.com)..#!comment: Dozens of software vendors already license Nmap technology such as.#!comment: host discovery, port scanning, OS detect ion, and version detection..#!comment: For more details, see https://nmap.org/book/man-legal.html..123456.12345.123456789.password.iloveyou.princess.12345678.12 34567.abc123.nicole.daniel.monkey.babygirl.qwerty.lovely.654321.michael.jessica.111111.ashley.000000.iloveu.michelle.tigger.sunshine.chocolate.password1.soccer. anthony.friends.purple.angel.b |

| C:\Program Files (x86)\Nmap\nselib\data\pixel.gif | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 51 |
| Entropy (8bit): | 3.8913513755198355 |
| Encrypted: | false |
| SSDEEP: | 3:CUyzKbT//thn:02T/rn |
| MD5: | E9FAE08644270A188B88378EF8ECD4CC |
| SHA1: | D2617CBA030C6AF572E55F739145A70D76876E40 |
| SHA-256: | 38C81820EF65FE7A518846979199F868BF5C4C1C15F40CAE7C7681F946853B64 |
| SHA-512: | 12FA79DF59877E56B8ABFB41D737F4C494F729DB013FF3848017FFB6A20BEFF5B07A19CAD0CC63E73D1CF2A537EFEC934CFC6F0ED8A43506D1DFBD9131F61CCD |
| Malicious: | false |
| Preview: | GIF89a.....!..!!comment!!.,.....D..;. |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\README | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 758 |
| Entropy (8bit): | 4.410466513740218 |
| Encrypted: | false |
| SSDEEP: | 12:WjmjD6cSxElJHy/37ixVFMwFps3RsOg8Gx8lJ5o01AQ+l4HIPIgnckqlJEGg:Wjm/AxWHy/3Gxv/URjg1xOFP1oPIgck9 |
| MD5: | BF239F422D90302A3CA7BAFCCBC94902 |
| SHA1: | 608B3D89F62478B7647622F101875BE4A5E0C09B |
| SHA-256: | EF074EC2A6E1D13EB618A210F48FB57BE31007CEB8F9435D107BEC2B01820A29 |
| SHA-512: | 89DA9DF7131751E9D79E40CF87547B6663858FB7DA1578D90721B8AFAE41568E8D8411CACAE51A972CFFC553CD0466F041E600AFED5E1AB3491C346A76E61DCC |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\README | |
|---|---|
| Preview: | The files in this directory are the data files required for smb-psexec.nse...The .lua files are configurations. Each of these defines a profile for a.psexec execution...n map_service.exe is a program that facilitates the operation of smb-psexec.nse..It is uploaded to the remote host and runs the programs it's directed to run,.redirecting their output to a file. This file is then downloaded by the.script and displayed to the user...Because nmap_service.exe is tagged as spyware by some antivirus software, it is.no longer distributed together with nmap. You can download it from.https://nmap.org/psexec/nmap_service.exe or compile it from the provided.sources. The smb-psexec.nse script will remind you if you run it and.nmap_service.exe is not available.. |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\backdoor.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 921 |
| Entropy (8bit): | 4.548638998640834 |
| Encrypted: | false |
| SSDEEP: | 24:LSYUk0eF7BxD/K0P+GQvDMFRekkHWUVxAyWF/Jw:GYUXc3K0P+JDMr2WUDAyWFBw |
| MD5: | 37B8607134FD4615E166E0A241FC5A5E |
| SHA1: | C46561460873B7CD803872E8F119D788AD1140E5 |
| SHA-256: | 953F229D3E3ABC2B63D82C43F921398E07542DE5FBC8759A7219E2350A22D0A1 |
| SHA-512: | 6ACB2EB632E29FE0CAAA8517C0594A23367565D372A22BFEC1794B9455F9E2B3106874975AECADA55D23B013E2AADD0E4423D83DE64108EE5E9BF0FC11A51EE6 |
| Malicious: | false |
| Preview: | ---This config file is designed for adding a backdoor to the system. It has a few.-- options by default, only one enabled by default. I suggest.--.-- Note that none of these modules are included with Nmap by default...-- Any variable in the 'config' table in smb-psexec.nse can be overriden in the.-- 'overrides' table. Most of them are not really recommended, such as the host,.-- key, etc..overrides = {}.--overrides.timeout = 40..modules = {}.local mod..-- TODO: allow the user to specify parameters.--Note: password can't be longer than 14-characters, otherwise the program pauses for.-- a response.mod = {}.mod.upload = false.mod.name = "Adding a user account: $username/$password".mod.program = "net".mod.args = "user $username $password /add".mod.maxtime = 2.mod.noblank = true.mod.req_args = {'username','password'}.table.insert(modules, mod).. |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\default.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 5426 |
| Entropy (8bit): | 4.5408645567988515 |
| Encrypted: | false |
| SSDEEP: | 96:b4RTmCF5S+FLFb7zRrFwFN3FHF4FE0F7joP5j2FF3v:b8PS+hn6vd6FVdchj2Pv |
| MD5: | C89B14931D3BDC79FE64A2ABC643FC3E |
| SHA1: | DCB835B33C30F0E3D0EF6A5AC5CB2437A8D39E0F |
| SHA-256: | 48DCDB781F54FD44E204671463952C7B834D42086EE4AD84982A08808FF55C9A |
| SHA-512: | A43077A140C6F32CA61778F463B0E3B6E8B3D6EA310CA85FDF64F11B217E47686C3FC6666D57B1D6893A88A09EB46E0EEFE5699B2F8F4E0347785DD79C5ABD9 |
| Malicious: | false |
| Preview: | ---This is the default configuration file. It simply runs some built-in Window.-- programs to gather information about the remote system. It's intended to be.-- simple, demonstrate some of the concepts, and not break/alte anything...local table = require "table"..-- Any variable in the 'config' table in smb-psexec.nse can be overriden in the.-- 'overrides' table. Most of them are not really recommended, such as the host,.-- key, etc..overrides = {}.--overrides.timeout = 40..modules = {}.local mod..-- Get the Windows version. For some reason we can't run this directly, but it works ok.-- if we run it through cmd.exe..mod = {}.mod.upload = false.mod.name = "Windows version".mod.program = "cmd.exe".mod.args = "/c \"ver\"".mod.maxtime = 1.mod.noblank = true.table.insert(modules, mod)..-- Grab the ip and mac address(es) from ipconfig. The output requires quite a bit of cleanup.-- to end up being usable and pretty..mod = {}.mod.upl |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\drives.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1334 |
| Entropy (8bit): | 4.275887578425276 |
| Encrypted: | false |
| SSDEEP: | 24:uXjg7BxD/K0P+GQvx0Vz5bK4HVvQuwCKeVmuwCKgnVcbS:Q03K0P+Jx01BK4HaCKeACKQ8S |
| MD5: | 5C7E00D9B296D1BC1AE5CDA80711DFBD |
| SHA1: | EE013587C4BEB06A0E605F588669BCCF73B45CDD |
| SHA-256: | 550D24B6AF264274BFB5F394BDCF2E6C93A1E2F963A4A80ED8A08C0722DEC73E |
| SHA-512: | 389BBC7E18586FF3CA6D0033C8C17684093D362273CDD64EBB52F6B56C9956549E63FB3894DD6720CA547A1213155ADD98E82C883AD0444FBF1C3D8AC40650F |
| Malicious: | false |
| Preview: | ---This configuration file pulls info about a given harddrive..-- Any variable in the 'config' table in smb-psexec.nse can be overriden in the.-- 'overrides' table. Most of them are not really recommended, such as the host,.-- key, etc..overrides = {}.--overrides.timeout = 40..modules = {}.local mod..mod = {}.mod.upload = false.mod.name = "Drive type".mod.program = "fsutil".mod.args = "fsinfo drivetype $drive".mod.req_args = {"drive"}.mod.maxtime = 1.table.insert(modules, mod)..mod = {}.mod.upload = false.mod.name = "Drive info".mod.program = "fsutil".mod.args = "fsinfo ntfsinfo $drive".mod.req_args = {"drive"}.mod.replace = {{" :","":"}}.mod.maxtime = 1.table.insert(modules, mod)..mod = {}.mod.upload = false.mod.name = "Drive type".mod.program = "fsutil".mod.args = "fsinfo statistics $drive".mod.req_args = {" |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\examples.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2358 |
| Entropy (8bit): | 4.522016971777209 |
| Encrypted: | false |
| SSDEEP: | 48:3t3K0P+TxZmrgm1DFsKJbL6ifFqCuFUweCuFSU8FJV8W:3xTm9sFM/rFArFuFP8W |
| MD5: | BE67046A8B025B7ACE948927210EC153 |
| SHA1: | C0A3BAE580BE726866AB550453255D1A1076D658 |
| SHA-256: | FF7530D8162DD25DB50A7DA729AB64DE77015E615A60BBA658619C317F175822 |
| SHA-512: | 74F531E1D7DE411A8F46FE3266D5C15FB2FD290B175739B3067CDEAF512DB4007AA94DC677FE851C796730568C5C786C7FDC77D68E87F502FE6C86A211593FF |
| Malicious: | false |
| Preview: | ---This configuration file contains the examples given in smb-psexec.nse...-- Any variable in the 'config' table in smb-psexec.nse can be overriden in the.-- 'overrides' table. Most of them are not really recommended, such as the host,.-- key, etc..overrides = {}.overrides.timeout = 40..modules = {}.local mod..mod = {}.mod.upload = false. mod.name = "Membership of 'administrators' from 'net localgroup administrators'".mod.program = "net.exe".mod.args = "localgroup administr ators".table.insert(modules, mod)..mod = {}.mod.upload = false.mod.name = "Example 2: Membership of 'administrators', cleaned".mod.program = "net.exe".mod.args = "localgroup administrators".mod.remove = {"The command completed", "%-%-%-%-%-%-%-%-%-%-", "Members", "Alias name", "Comment"}.mod.noblank = true.table.insert(modules, mod)..mod = {}.mod.upload = false.mod.name = "Example 3: IP Addr |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\experimental.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 712 |
| Entropy (8bit): | 4.5149649118007975 |
| Encrypted: | false |
| SSDEEP: | 12:a0R4yu/PDaGekXDx9KHUkolriG7ZqvpVGRXYISF1IAoQVo8IAjF1GZ:/Du/7BxD/K0P+GQvLCSF1InQVpFjF1o |
| MD5: | 9E10DC886A86A56F1EA087E958DFE244 |
| SHA1: | ABCA2570BC33A2718546FB7B7253C22815593696 |
| SHA-256: | B921C52ABFAC3202709DC739141D0DF8FB37CD8115E8CDE0E3DF809760367F77 |
| SHA-512: | 6687EFC9387679837C4462803653209F315A045738278E4131CADB9E35F7E0432710DAF0E4A02E75A0CD477DCF39B67DCD6AEC9019E3BF9EA485E80A6D439402 |
| Malicious: | false |
| Preview: | ---This is the configuration file for modules that aren't quite ready for prime.-- time yet....-- Any variable in the 'config' table in smb-psexec.nse can be overriden in the.-- 'o verrides' table. Most of them are not really recommended, such as the host,.-- key, etc..overrides = {}.--overrides.timeout = 40..modules = {}.local mod...-- I can't get fport to work for me, so I'm going to leave this one in 'experimental' for now.--mod = {}.--mod.upload = true.--mod.name = "Fport".--mod.program = "F port.exe".--mod.url = "http://www.foundstone.com/us/resources/proddesc/fport.htm".--mod.maxtime = 1.--mod.noblank = true.--table.insert(modules, mod).. |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\network.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 4111 |
| Entropy (8bit): | 4.539636670118338 |
| Encrypted: | false |
| SSDEEP: | 96:eTmoSlF4FE0F7joP5j2Fb7zRrFwFN3FFKrF13F6:8Sl6FVdchj2n6vMHM |
| MD5: | 2469EA5509E68600FC61968192E45384 |
| SHA1: | ACB710319F296081AB8921EB1B3769D90DDC036F |
| SHA-256: | 316F3B7E468A063173CBD17A14CDE345EAE44E89848D2550349D8EE954ED78FB |
| SHA-512: | 9EEFC959F0CA659CB744E7CC4B49A35FEE69F98952B65AC8209662541633564BC3F8A6EA7A097984776D8838DB7F3023B32CD9D2E2CD16AF79DFF3671FCA386 |
| Malicious: | false |
| Preview: | ---More verbose network scripts..-- Any variable in the 'config' table in smb-psexec.nse can be overriden in the.-- 'overrides' table. Most of them are not really recomme nded, such as the host,.-- key, etc..overrides = {}.--overrides.timeout = 40..modules = {}.local mod..-- Grab the ip and mac address(es) from ipconfig. The output requires quite a bit of cleanup.-- to end up being usable and pretty..mod = {}.mod.upload = false.mod.name = "IP Address and MAC Address from 'ipconfig.exe '".mod.program = "ipconfig.exe".mod.args = "/all".mod.maxtime = 1.mod.find = {"IP Address", "Physical Address", "Ethernet adapter"}.mod.re place = {{"%. ", ""}, {"-", ":"}, {"Physical Address", "MAC Address"}}.table.insert(modules, mod)..-- Dump the arp cache of the system..mod = {}.mod.name = "ARP Cache from arp.exe".mod.program = 'arp.exe'.mod.upload = false.mod.args = '-a'.mod.remove |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\nmap_service.c | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 10757 |
| Entropy (8bit): | 5.222999608152912 |
| Encrypted: | false |
| SSDEEP: | 192:u9wgJ+KaqZqNJ14sCEw9xMzcQS6XIzl5LL1qlXuu6b:AwgJ+K3qv+sCERzFSrLwb6b |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\nmap_service.c | |
|---|---|
| MD5: | D00B393331693E6AF23D5264077EE0F0 |
| SHA1: | 9A73833B436F4ACB5077F41FCA3248598BE1069C |
| SHA-256: | 0EA7D885CC0CD9D07A88AC3C835430BD1B390A69DA84B1748354E131F4D87A6A |
| SHA-512: | 8C929EB10C7BBE2CC9F45532E0C95D8E37734D51B8DA246741C1A4B6FAAA0F8773F49B1EF1F3BA1C832B449BBBE3E027D17125115EAC2DC48153F4C82DFE9E3E |
| Malicious: | false |
| Preview: | /**This is the program that's uploaded to a Windows machine when psexec is run. It acts as a Windows.. * service, since that's what Windows expects. When it is started, it's passed a list of programs to.. * run. These programs are all expected to be at the indicated path (whether they were uploaded or.. * they were always present makes no difference)... *.. * After running the programs, the output from each of them is ciphered with a simple xor encryption.. * (the encryption key is passed as a parameter; because it crosses the wire, it isn't really a.. * security feature, more of validation/obfuscation to prevent sniffers from grabbing the output. This.. * output is placed in a temp file. When the cipher is complete, the output is moved into a new file... * When Nmap detects the presence of this new file, it is downloaded, then all files, temp files, and.. * the service (this program) is deleted... *.. * One interesting note is that executable files don't require a specific extension t |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\nmap_service.vcproj | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 4000 |
| Entropy (8bit): | 5.159437455953481 |
| Encrypted: | false |
| SSDEEP: | 48:cxSdLygmKNEkypkEHMad1jwl1gm56u/axNlYqew/dFMgmKNEkypkdRaMVQdQUMwm:BRz07fSzo1zNa5kNCootth6xJbI4 |
| MD5: | A80CA72117C84954A13B16C4DBB1E77A |
| SHA1: | 973770432A609B1F958064D11ACC445A26983A79 |
| SHA-256: | 338FFD2610A2F9010253F7A910727802F9A7A2AF3CF865D2E2F98412DED17FDF |
| SHA-512: | 50221EBC97CF0640564A9EF93A0C9A99DAE3EA27C482B64E66A4FD0DE133F8B73EAE433AE7562ED00E5ACAEE19E401F6507BCDC428F5F17B93CE70332EC24D5B |
| Malicious: | false |
| Preview: | <?xml version="1.0" encoding="Windows-1252"?>..<VisualStudioProject...ProjectType="Visual C++"...Version="9.00"...Name="nmap_service"...ProjectGUID="{ECFB8033-F0DA-40FA-9C47-DBE06DAB6A5F}"...RootNamespace="nmap_service"...Keyword="Win32Proj"...TargetFrameworkVersion="196613"...>...<Platforms>....<Platform.....Name="Win32"..../>...</Platforms>...<ToolFiles>...</ToolFiles>...<Configurations>....<Configuration.....Name="Debug\|Win32".....OutputDirectory="$(SolutionDir)$(ConfigurationName)".....IntermediateDirectory="$(ConfigurationName)".....ConfigurationType="1".....CharacterSet="1".....>.....<Tool.....Name="VCPreBuildEventTool"...../>.....<Tool.....Name="VCCustomBuildTool"...../>.....<Tool.....Name="VCXMLDataGeneratorTool"...../>.....<Tool.....Name="VCWebServiceProxyGeneratorTool"...../>.....<Tool.....Name="VCMIDLTool"...../>.....<Tool.....Name="VCCLCompilerTool".....Optimization="0".....PreprocessorDefinitions="WIN32;_DEBUG;_CONSOLE".....MinimalRebuild="true".....BasicRuntimeC |

| C:\Program Files (x86)\Nmap\nselib\data\psexec\pwdump.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1841 |
| Entropy (8bit): | 4.618119488798928 |
| Encrypted: | false |
| SSDEEP: | 48:kc3K0P+JJWFX8HLR12aRFS8a+rHQFhVnxpo:kATmPWFXaRF04QFnno |
| MD5: | 9F7A62B8843B3D175D703CC465D86199 |
| SHA1: | BC30AC0DC1BB8AC89477FABA2B26E12B858FE693 |
| SHA-256: | F9B81709A81D43793C57437A483BB18B2F862E25AF3324E760B1177B1F48AA78 |
| SHA-512: | 0BDF82956AFABC5E3ADD8C3E3FDE12DB65F070BB025227E4F90FC9807137E506A6CB540CADC4E875CC9893F64BEE7ABC125D261DFD7EF23D9FF7EFA642825B3D |
| Malicious: | false |
| Preview: | ---This config file is designed for running password-dumping scripts. So far,.-- it supports pwdump6 2.0.0 and fgdump..--.-- Note that none of these modules are included with Nmap by default...-- Any variable in the 'config' table in smb-psexec.nse can be overriden in the.-- 'overrides' table. Most of them are not really recommended, such as the host,.-- key, etc..overrides = {}.--overrides.timeout = 40..modules = {}.local mod..--mod = {}.--mod.upload = true.--mod.name = "PwDump6 2.0.0".--mod.program = "PwDump.exe".--mod.args = "localhost".--mod.maxtime = 10.--mod.include_stderr = false.--mod.url = "http://www.foofus.net/fizzgig/pwdump/".--table.insert(modules, mod)..---Uncomment if you'd like to use PwDump6 1.7.2 (considered obsolete, but still works)..-- Note that for some reason, this and 'fgdump' don't get along (fgdump only produces a blank.-- file if these are run together).--mod = {}.--mod.upload = true |

| C:\Program Files (x86)\Nmap\nselib\data\publickeydb | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1762 |
| Entropy (8bit): | 5.991090064797007 |
| Encrypted: | false |
| SSDEEP: | 48:uCi+OlP5eF2gQ3KvJVg7t3qqkPl5eFV3HtyDnFTly:uCifP5eFg8f1/t5eFCDfy |
| MD5: | 0324C3D356E882CFF25D410817176C9A |
| SHA1: | B49539D63A8CF55138F3308D917DBA526FE2DD9C |
| SHA-256: | CF13E3EA20C3E94F38547B92FA1A63C75D6588A5099B846B979A8B58D6B84350 |
| SHA-512: | CB49EC9277BFD1017E2981DFD96A0342052DA3A3629333D3C461AC16D78378B13ADA9A91D8E868C72FA1E5729903C781A1848FDB7A7DBDBBC378C9731436A3 |

| C:\Program Files (x86)\Nmap\nselib\data\publickeydb | |
|---|---|
| Malicious: | false |
| Preview: | AAAAB3NzaC1kc3MAAACBAISAE3CAX4hsxTw0dRc0gx8nQ41r3Vkj9OmG6LGeKWRmpy7C6vaExuupjxid76fd4aS56lCUEEoRlJ3zE93qoK9acI6EGqGQFLuD Z0fqMyRSX+ilf+1HDo/TRyuraggxp9Hj9LMpZVbpFATMm0+d9Xs7eLmaJjuMsowNlOf8NFdHAAAAFQCwdvqOAkR6QhuiAapQ/9iVuR0UAQAAAIBpLMo4dhSe WkChfv659WLPftxRrX/HR8YMD/jqa3R4PsVM2g6dQ1191nHugtdV7uaMeOqOJ/QRWeYM+UYwT0Zgx2LqvgVSjNDfdjk+ZRY8x3SmExFi62mKFoTGSOCXfcAf uanjaoF+sepnaiLUd+SoJShGYHoqR2QWiysTRqknlwAAAIBLEgYmr9XCSqjENFDVQPFELYKT7Zs9J87PjPS1AP0qF1OoRGZ5mefK6X/6VivPAUWmmmev/BuA s8M1HtfGeGGzMzDIiU/WZQ3bScLB1Ykrcjk7TOFD6xrnk/inYAp5l29hjidoAONcXoHmUAMYOKqn63Q2AsDpExVcmfj99/BlpQ==,root,Quantum DXi V1000 2.2.1 static root publickey accepted,source:http://www.exploit-db.com/exploits/32372/.AAAAB3NzaC1kc3MAAACBAKwKBw7D4OA1H/uD4htdh04TBIHdbSjeXUSnWJsce8C0tvoB01 Yarjv9TFj+tfeDYVWtUK1DA1JkyqSuoAtDANJzF4I6Isyd0KPrW3dHFTcg6Xlz8d3KEaHokY93NOmB/xWEkhme8b7Q0U2iZie2pgWbTLXV0FA+lhskTtPHW3+VAAAAFQDR yayUlVZKXEweF3bUe03zt9e8VQAAAIAEPK1k3Y6ErAbIl96dnUCnZjuWQ7xXy062pf63QuRWI6LYSscm3f1pEknWUNFr/erQ02pkfi2eP9uHl1 |

| C:\Program Files (x86)\Nmap\nselib\data\rtsp-urls.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 2894 |
| Entropy (8bit): | 5.025621128946615 |
| Encrypted: | false |
| SSDEEP: | 48:q6z1HxmkBBEhwDSaIGvI/EQa4avafuipUPuPEWQtZXaay5KRZ77e00STPx/xdL2t:hxA4XCdpWuPZ0q5KPDPx/xd+sLCxhdnd |
| MD5: | ADBC812E651866B1873BAB5CD3A5B06E |
| SHA1: | 53CCAA2D7513349ACF4574CF31FB860F2AAC2905 |
| SHA-256: | B3CD6CB9ED5C1E3443F545A7FCC39D00401D655E6E112CF7764F02E16D4F71C3 |
| SHA-512: | BFDB73694B2AF26EEC6E62F46629F9B2443E0CE886B84EBC35EA550A87698A273038E99D34F6ADD696E473E889EFEDEFE0B7C14630E262331E8F4981ED68362 |
| Malicious: | false |
| Preview: | #!comment: The following dictionary contains a list of well-known RTSP URLs.#!comment: used by common video surveillance equipment.././0./0/video1./1./1.AMP./1/ 1:1/main./1/cif./1/stream1./11./12./4./CAM_ID.password.mp2./CH001.sdp./GetData.cgi./H264./HighResolutionVideo./HighResolutionvideo./Image.jpg./LowResolutionVide o./MJPEG.cgi./MediaInput/h264./MediaInput/h264/stream_1./MediaInput/mpeg4./ONVIF/MediaInput./ONVIF/channel1./PSIA/Streaming/channels/0?videoCodecType= H.264./PSIA/Streaming/channels/1./PSIA/Streaming/channels/1?videoCodecType=MPEG4./PSIA/Streaming/channels/h264./Possible./ROH/channel/11./Streaming/Ch annels/1./Streaming/Channels/101./Streaming/Channels/102./Streaming/Channels/103./Streaming/Channels/2./Streaming/Unicast/channels/101./Streaming/chan nels/101./Video?Codec=MPEG4&Width=720&Height=576&Fps=30./VideoInput/1/h264/1./access_code./access_name_for_stream_1_to_5./av0_0./av0_1./av2./avn=2./ax is-media/media.amp./axis-media/media.amp?videocodec=h264&resolution=640x480./cam |

| C:\Program Files (x86)\Nmap\nselib\data\snmpcommunities.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1048 |
| Entropy (8bit): | 4.959172811079107 |
| Encrypted: | false |
| SSDEEP: | 24:K+tL4Uug0YzGvFyWLR5X7SVB7BmIWB3lW0T8guwSE:vt0Uu4HuR5rm7JSVW0QR5E |
| MD5: | 413517449697032C95370F7073E4C27D |
| SHA1: | BEACAB61E5685D18805174C09B864139FE8A678F |
| SHA-256: | B0F575CF33A5BD07ED77529DA9D1024EB321C2D8BDE201828A98985A654C3C2D |
| SHA-512: | D09C990150EF8B0EEB70E4353703CEA4915461BF0F49725A9FAC64026E0B7E2B932D24E882EB680A441757ACE0FA4D45944E288E89E640CB900E39376F9FA431 |
| Malicious: | false |
| Preview: | #!comment: This collection of data is (C) 1996-2020 by Insecure.Com LLC..#!comment: It is distributed under the Nmap Public Source license as.#!comment: provided in the LICENSE file of the source distribution or at.#!comment: https://svn.nmap.org/nmap/LICENSE . Note that this license.#!comment: requires you to license your own work under a compatable open source.#!comment: license. If you wish to embed Nmap technology into proprietary.#!comment: software, we sell alternative licenses (contact sales@insecure.com)..#!comment: Dozens of software vendors already license Nmap technology such as.#!comment: host discovery, port scanning, OS detect ion, and version detection..#!comment: For more details, see https://nmap.org/book/man-legal.html..public.private.snmpd.mngt.cisco.admin.PUBLIC.PRIVATE.#!comment: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps3.rmonmgmtuicommunity.#!comment: http://www.phenoelit.org/dpl/dpl. html.secret.cascade.ANYCOM.ILM |

| C:\Program Files (x86)\Nmap\nselib\data\ssl-fingerprints | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 85484 |
| Entropy (8bit): | 4.203298769350572 |
| Encrypted: | false |
| SSDEEP: | 1536:8vlV/zzckILNOX3ea76czXoPhCxI7T8URmbE1bWa/OZw3aD+eDM:cn/zEK3nOmYIYT8BaFeg |
| MD5: | DCAC694228C9D58E9BF46436C636288E |
| SHA1: | 2DD4FBE495FE621378A04B7DCFB9AC1F4494DC69 |
| SHA-256: | 0D8A9DE4ACE9704A8779B157BD1BE109E01AAB1B7E306D0ED7B3A68DFB0652C1 |
| SHA-512: | E7755E59CDD13F2333E23FC3324DE26B1548586342BE5BC35FF8DE4AD70A9E338EB36F41B95A2F19980436C33352E408C7EB6E4A6C9FECD8D318C48D4F1F1E5 D |
| Malicious: | false |

| C:\Program Files (x86)\Nmap\nselib\data\ssl-fingerprints | |
|---|---|
| Preview: | # SHA-1 hashes of SSL certificates that have known private keys. Most.# of these are from Little Black Box 0.1.# (http://code.google.com/p/littleblackbox/), which has this copyright.# notice:.#.# Copyright (c) 2010 Craig Heffner.#.# Permission is hereby granted, free of charge, to any person obtaining a copy.# of this software and associated documentation files (the "Software"), to deal.# in the Software without restriction, including without limitation the rights.# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell.# copies of the Software, and to permit persons to whom the Software is.# furnished to do so, subject to the following conditions:.#.# The above copyright notice and this permission notice shall be included in.# all copies or substantial portions of the Software..#.# THE SOFTWARE IS PROVIDED "AS IS", WIT HOUT WARRANTY OF ANY KIND, EXPRESS OR.# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,.# FITNESS FOR A P ARTICULAR PURPOSE AN |

| C:\Program Files (x86)\Nmap\nselib\data\targets-ipv6-wordlist | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 16707 |
| Entropy (8bit): | 3.4786417643674326 |
| Encrypted: | false |
| SSDEEP: | 384:vPVSN4bwQpsY3HI+MwXBqd6rMs0O7mk49OyL27xLUoFcb:HUh0FXdlBxrMspykEOD7xLQb |
| MD5: | 26A1BB873B708840DE12572E07E772A0 |
| SHA1: | E402723CFF0282830C6F769933E965567F709148 |
| SHA-256: | F29411E814C049D008E4401973AC759890296D531E75CF41AB6DFCA2500060B1 |
| SHA-512: | 02D2222DF594EFB76DFA1CDA589BB40E5231520C5B651FCF360EA47D3CB4B2E8097C6A45912D209D259C5D45884D6284BB35719AC5B18A08A28E22F7A6ED662 |
| Malicious: | false |
| Preview: | # This list generated from the Moby wordlist and the Moby Language wordlist,.# using simple substitutions and selecting for 3-letter words, multiples of.# 4-letters, and removing words beginning with 0 (as they do not display.# "nicely" in a shortened IPv6 address).# http://icon.shef.ac.uk/Moby/.# http://nedbatchelder.com/text/hexwords.html.1337.31337.100.1005.1007.1007ab1e.100b.100d.100f.1010.1011.101a.101e.105.1055.10551e55.1057.105a.105e.105e57e5.105f.107.1070.1075.1077.1077a55e.1077a57e.107a.107e.10a.10ad.10ad1e55.10adab1e.10af.10b.10b0.10b5.10b7.10ba.10be.10be1e55.10bef007.10c.10c0.10c0f0c0.10ca.10ca11ed.10d.10d0.10da.10de.10e.10eb.10ed.10effe15.10f.10f7.10f71e55.110.11b.11c.11d.11e.155.155d.157.15b.15c.15d.15e.171.175.17a.17ab.17c.17d.17f.1a0.1a05.1a1.1a10.1a11.1a1a.1a5.1a50.1a55.1a55a11e.1a57.1a5a.1a5e.1a7.1a70.1a705015.1a75.1a77.1a7a.1a7e.1a7e1057.1aa.1ab.1ab0.1ab5.1ab7.1abbe11a.1abe.1abe11ed.1abefac7.1ac.1ac5.1ac7.1ac705e5.1ac7a5e5.1ac7a7e5.1ac7a7ed.1ac7e5ce.1ac7ea15.1ac7ead0. |

| C:\Program Files (x86)\Nmap\nselib\data\tftplist.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 3521 |
| Entropy (8bit): | 5.005824487277645 |
| Encrypted: | false |
| SSDEEP: | 48:M8BWuf4kStFwFvf+B98iK6AjPE+wNFdJCXPP1Zq+S+X9QJ:M8BJstFwU9iPEhrCXxH9m |
| MD5: | 4A8B5A8308E4188A82508A79B80A77C5 |
| SHA1: | 69A2438C4D413E93BBD4B99902BF7355C109B7DF |
| SHA-256: | 683FEA3BF1C1EC1435243DA75ED41C7A9B467BB0EB8DAC9688AA1B13483AA6D1 |
| SHA-512: | 57359983E2A7CF74A428CEC3D521210A5EB0AB5683F98DFD9BA42F6C81BEC3D07592A71E959FCBF531725B91D2D38E6811872DF897E5F7A35E46125E9345C114 |
| Malicious: | false |
| Preview: | 000000000000-directory.xml.{mac}-directory.xml.000000000000-directory~.xml.000000000000-phone.cfg.{mac}-phone.cfg.000000000000.cfg.{mac}.cfg.256T.CM.323tosip1_1.bin.4601_02_readme_R2_3.txt.4601dbte1_82.bin.4602_02SWSIPreadme_R1_1.txt.4602dbte1_82.bin.4602sbte1_82.bin.4610_20_readme_R2_3.txt.4610_20_readme_SIP_R2_2.txt.4624_12_06readme_1_8_3.txt.4625_readme_2_5.txt.4690_010707.bin.4690_readme_1_7_7.txt.46xxreadme_111405.txt.46xxsettings.txt.46xxupgrade.scr.6100-113.bin.7200-118.bin.CFE.bin.CP7912010301SIP050608A.sbin.CP7905010301SIP050608A.sbin.H323.cfg.OS79XX.TXT.P003-07-5-00.bin.P003-07-5-00.sbn.P003-08-11-00.bin.P003-08-11-00.sbn.P003-08-2-00.bin.P003-08-2-00.sbn.P003-08-3-00.bin.P003-08-3-00.sbn.P003-08-6-00.bin.P003-08-6-00.sbn.P003-08-9-00.bin.P003-08-9-00.sbn.P003-8-12-00.bin.P003-8-12-00.sbn.P0S3-07-5-00.bin.P0S3-07-5-00.loads.P0S3-07-5-00.sb2.P0S3-08-11-00.loads.P0S3-08-11-00.sb2.P0S3-08-2-00.loads.P0S3-08-2-00.sb2.P0S3-08-3-00.loads.P0S3-08-3-00.sb2.P0S3-08-6-00.loads.P0S3-08- |

| C:\Program Files (x86)\Nmap\nselib\data\usernames.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 72 |
| Entropy (8bit): | 3.7755665448319142 |
| Encrypted: | false |
| SSDEEP: | 3:BJoIMgBIKMWR3L1voIMLTjI0C8JD2OWJ:vmAMW5y0oJAJ |
| MD5: | 31990EB67231E20EA645DCCDA8F9B621 |
| SHA1: | CF23EE3F8ABCC45DB84F86FF8132690A37F244B7 |
| SHA-256: | 07C7CFA57C0550A90F6453DC7EE2A5F90C062229DFC3FC09D9DF5DE7F3D1D308 |
| SHA-512: | 425355574AA5DC9F8064D5D0716CD87453A637017183B5F42C00A3D4E917070D9FBD9DEFC82D4B1720633E3E9BE4071447027AEB8A4CE63575B1E60323E54491 |
| Malicious: | false |
| Preview: | root.admin.administrator.webadmin.sysadmin.netadmin.guest.user.web.test. |

| C:\Program Files (x86)\Nmap\nselib\data\vhosts-default.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |

| C:\Program Files (x86)\Nmap\nselib\data\vhosts-default.lst | |
|---|---|
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 717 |
| Entropy (8bit): | 4.289707927472557 |
| Encrypted: | false |
| SSDEEP: | 12:oIKteQltM+pjj9A202ITjvAefRMBvRIAt8XnLUgiV7y/KEQdVpQvKMx7heqMZjW7:VmtM4jGqITjhuBvRIAELeV7BEQcZY/hO |
| MD5: | 39DE15C4FE61E85C015AA03A3DB4D8EC |
| SHA1: | AA6C5EC7216D3A3C4FDF17CCA1520EA7A45217AF |
| SHA-256: | 85DED2C225C76D49F038E93728F4EDC968ED2D02658300DECCACEFA0D03EAE50 |
| SHA-512: | B9AC0B48A149F71C7551D0BA23F24AFB96C09B35EC7ABFDA983CE55225FDCA0E8D40C7EE82550CE88709B94DFF01375C8AF1B68BC06001A8C89332806D3EA8<br>3 |
| Malicious: | false |
| Preview: | admin.administration.ads.adserver.alerts.alpha.ap.apache.app.apps.appserver.aptest.auth.backup.beta.blog.cdn.chat.citrix.cms.corp.crs.cvs.database.db.demo.dev.d<br>evel.development.devsql.devtest.dhcp.direct.dmz.dns.dns0.dns1.dns2.download.en.erp.eshop.exchange.f5.fileserver.firewall.forum.ftp.ftp0.git.gw.help.helpdesk.hom<br>e.host.http.id.images.info.internal.internet.intra.intranet.ipv6.lab.ldap.linux.local.log.mail.mail2.mail3.mailgate.main.manage.mgmt.mirror.mobile.monitor.mssql.mta.mx.mx<br>0.mx1.mysql.news.noc.ns.ns0.ns1.ns2.ns3.ntp.ops.oracle.owa.pbx.s3.secure.server.shop.sip.smtp.sql.squid.ssh.ssl.stage.stats.svn.syslog.test.test1.test2.testing.<br>upload.vm.vnc.voip.vpn.web.web2test.webftp.whois.wiki.www.www2.xml. |

| C:\Program Files (x86)\Nmap\nselib\data\vhosts-full.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 3849 |
| Entropy (8bit): | 4.3262536157645055 |
| Encrypted: | false |
| SSDEEP: | 96:Z4JuS1pK4MVVGDVi5tkFPY2YgekVXd2B7+4Q/ab:CUohDViqBTVXd2BGab |
| MD5: | 35A9DD23DF5A3AF2CD0AC4903178D28E |
| SHA1: | F12C8529FFE5D39AFFB26D842025D29668BB1A78 |
| SHA-256: | 21E94510EB5436FD01EC253658165ADAAEC23E6D11618C70D42851D56EE221B7 |
| SHA-512: | 0B8A72B47E32A0C7A763822483B532E91F3D6E8AD10389D6F0A2312843666BFB6C7D25D4BDDF21E4A3DB834CAE0510C9A542430EED1353BB25C960B0A357D69 |
| Malicious: | false |
| Preview: | .abbot.admin.administration.ads.adserver.alerts.alpha.ap.apache.api.app.apps.appserver.aptest.arch.artifactory.assembla.atd.athena.atollon.attask.attix.attix5.auth.automa<br>tedqa.backend.backup.bacula.badboy.basecamp.bazaar.beta.bitkeeper.bkp.blog.branch.brightwork.broadwave.bromine.bugtracker.bugzilla.build.businessdriver.campus.c<br>atchlimited.ccc.cdn.centraldesktop.cerebro.chat.citrix.civicrm.clarizen.clearcase.clearquest.clif.clockingit.cms.codebeamer.codendi.codesourcery.codeville.collabtive.comp<br>uware.concordion.conformiq.corp.cppunit.crm.crs.cruisecontrol.cubictest.cucumber.cunit.cvs.cvsnt.darcs.dartenium.database.db.dcvs.debbugs.demo.dev.devel.develop<br>ment.devsql.devtest.dhcp.dieseltest.digitaltester.direct.distract.dmz.dns.dns0.dns1.dns2.dolibarr.dotproject.download.dune.durable.duxqa.dynamics.easy.egroupwar<br>e.eload.elvior.empirix.en.endeavour.enterprise.epesi.epesibim.erp.eshop.etester.eventum.exchange.f5.fasttrack.feng.fileserver.firefly.firewall.flumotion.flyspray.fogbugz.<br>foro.forum |

| C:\Program Files (x86)\Nmap\nselib\data\wp-plugins.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1011517 |
| Entropy (8bit): | 4.414740113278736 |
| Encrypted: | false |
| SSDEEP: | 12288:hauFLusIpXE0APADu/2NbioG7QdI0RnMAwGVr85nAxjICe3fXVw1Gd83XuZ6:cuFCFnAPAD7wgdSBhcUCICY6 |
| MD5: | E2DFF67FE30327458E98A910AE36B6F0 |
| SHA1: | 4F6F582278560C0FCACA97EC8AFF6A886AC6CE73 |
| SHA-256: | 35121E07E5D485A9074CE6CBD0110335AA52FEAB764D3A6BD49AFBC04777F165 |
| SHA-512: | D1F9AB026ECB9D2C260E8414731A1415F46CAD167C44A4E3C3342624985EDD1183664AD281414F864992028E0481D3149C67884AA48B0DF53688FBA4EE1EFECE |
| Malicious: | false |
| Preview: | # WordPress plugins, sorted by popularity. See.# http://seclists.org/nmap-dev/2011/q2/352 and.# http://seclists.org/nmap-dev/2011/q2/att-352/wp-plugins_pl.bin.# for the s<br>cript used to make this file..# Generated by.# svn list http://plugins.svn.wordpress.org \| sed 's/\/$//' \| parallel --eta -N 1 -j 20 "echo '{}' \$(curl -s 'https://api.wordpress.or<br>g/plugins/info/1.0/{}.json' \| jq .downloaded)" \| grep -v 'null$' \| sort -k 2,2 -n -r \| cut -d ' ' -f 1 > wp-plugins.lst..akismet.contact-form-7.wordpress-seo.jetpack.all-in-one-seo-<br>pack.wordfence.woocommerce.google-sitemap-generator.wordpress-importer.nextgen-gallery.google-analytics-for-wordpress.wp-super-cache.tinymce-advanced<br>.wptouch.better-wp-security.siteorigin-panels.updraftplus.w3-total-cache.google-analytics-dashboard-for-wp.wp-pagenavi.si-contact-form.advanced-custom-fields.ma<br>ilchimp-for-wp.the-events-calendar.add-to-any.duplicator.wysija-newsletters.ninja-forms.wp-smushit.buddypress.ewww-image-optimizer.so-widgets-bundle.really-simp |

| C:\Program Files (x86)\Nmap\nselib\data\wp-themes.lst | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 48801 |
| Entropy (8bit): | 4.419809600836397 |
| Encrypted: | false |
| SSDEEP: | 768:yN7ffVEkg+JQi/jxg7Pn4nEjrUwl65PrG4O9DO1lEUj9THrVRactIA4:s+H+lxtn+rSNrGF+EGjrVActIz |

| C:\Program Files (x86)\Nmap\nselib\data\wp-themes.lst | |
|---|---|
| MD5: | 7688DB92BBE5F861217CA5742BDEFFDC |
| SHA1: | E0D4F6A6C5BA1D4AB927634A6D761EA2D0C91DB6 |
| SHA-256: | 366FE94AB4BF4CA4733E1B432CA38DD68044C4AF90418174EF780C4DC0631D43 |
| SHA-512: | 326D82D5FE936BB5903BA27D923AF9B147334FA2A74DFD2386B480EA5BD7A2DF8233115CE562E516F765C75FFE8DE84C82DAA82113FA44C119FC4F1E033B737 |
| Malicious: | false |
| Preview: | twentyeleven.twentytwelve.twentyten.twentythirteen.twentyfourteen.twentyfifteen.responsive.customizr.zerif-lite.virtue.storefront.atahualpa.twentysixteen.vantage.hueman.spacious.evolve.colorway.graphene.sydney.ifeature.mh-magazine-lite.generatepress.mantra.omega.onetone.coraline.pinboard.thematic.sparkling.catch-box.make.colormag.enigma.custom-community.mystique.alexandria.delicate.lightword.attitude.inove.magazine-basic.raindrops.minamaze.zbench.point.eclipse.portfolio-press.twentyseventeen.travelify.swift-basic.iconic-one.arcade-basic.bouquet.pixel.sliding-door.pilcrow.simple-catch.tempera.destro.p2.sunspot.sundance.dusk-to-dawn.onepress.mosaia.dynamic-news-lite.parabola.parament.dazzling.accesspress-lite.optimizer.one-page.chaostheory.business-lite.duster.constructor.nirvana.sixteen.esquire.beach.next-saturday.flat.hatch.minimatica.radiate.accelerate.oxygen.accesspress-parallax.swift.spun.wp-creativix.suevafree.hemingway.pink-touch-2.motion.fruitful.steira.news.llorix-one-lite.adven |

| C:\Program Files (x86)\Nmap\nselib\datafiles.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 11320 |
| Entropy (8bit): | 4.692675692245523 |
| Encrypted: | false |
| SSDEEP: | 192:RwskbOVvXuY0dVhb+0RJnq0YA1KJ1AKL5AVJ72aQ+Mn/xH9dBVEbpreTh82uh8Iu:Rwskb62YuVh40YA1LS5A6aQ5/x7Me184 |
| MD5: | 59E3AD114B11B731BF74CCC38B688DB3 |
| SHA1: | B361780DF85ABA5B48C66F952E050455C0BAC202 |
| SHA-256: | 927DD61D3C1A46243DC9242EEBF3C4919AE0CCFAE200FE4328F6A3804B067680 |
| SHA-512: | 96E76803D960721611B67DF71A58AEDFCB15DD371EFD11C338DA095A87DC2AA9CC0AD169569E1FD10A162D0451D1BA7D6B9EEB7B83DD8E452596945F6DD94E65 |
| Malicious: | false |
| Preview: | ---.-- Read and parse some of Nmap's data files: <code>nmap-protocols</code>,.-- <code>nmap-rpc</code>, <code>nmap-services</code>, and.-- <code>nmap-mac-prefixes</code>..--.-- The functions in this module return values appropriate for use with exception.-- handling via <code>nmap.new_try</code>. On success, they return true and.-- the function result. On failure, they return false and an error message..-- @author Kris Katterjohn 03/2008.-- @author jah 08/2008.-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html..local io = require "io".local nmap = require "nmap".local stdnse = require "stdnse".local string = require "string".local table = require "table"._ENV = stdnse.module("datafiles", stdnse.seeall)...---.-- Capture patterns for common data files, indexed by filename..-- @class table.-- @name common_files.-- @see parse_file.local common_files = {.  ["nmap-rpc"]       = { [function(ln) return tonumber( ln:match( "^%s*[^%s#]+%s+(%d+)" ) ) end] = "^%s*([^%s#]+)%s+%d+" |

| C:\Program Files (x86)\Nmap\nselib\datetime.lua | |
|---|---|
| Process: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 8257 |
| Entropy (8bit): | 4.806590618653038 |
| Encrypted: | false |
| SSDEEP: | 192:28UtHcvLBt7LdbJn7ciYgfS7xIXCkdF1KIIZ+:27tHcvLzwkdzKbZ+ |
| MD5: | 17C3C60211CE7AA8220D354E7FC86530 |
| SHA1: | F037329193893777A64CE8276F96CEC512D330F58 |
| SHA-256: | DF366D1A7D46FE35D61FC800453348BE9F107C013832D389C4C74DCE49FAEAC9 |
| SHA-512: | 912B8B32973B8F9580A59ECC8F7BA830BC0E01AE409864F8E3F6E9E375648770070D403FBF3ADFC6BA881DB99BFDF91D441226CFDA55580F9AD8DB5981F6D5CD |
| Malicious: | false |
| Preview: | --- Functions for dealing with dates and timestamps.--.-- @copyright Same as Nmap--See https://nmap.org/book/man-legal.html.-- @class module.-- @name datetime.-- @author Daniel Miller..local stdnse = require "stdnse".local os = require "os".local math = require "math".local string = require "string"._ENV = stdnse.module("datetime", stdnse.seeall)..local difftime = os.difftime.local time = os.time.local date = os.date..local floor = math.floor.local fmod = math.fmod..local format = string.format.local match = string.match..--- Record a time difference between the scanner and the target.--.-- The skew will be recorded in the host's registry for later retrieval and.-- analysis. Adjusts for network distance by subtracting half the smoothed.-- round-trip time..--.--@param host The host being scanned.--@param timestamp The target timestamp, in seconds..--@param received The local time the stamp was received, in seconds..function record_skew(host, timestamp, received).  local skew_tab = host. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive |
| Entropy (8bit): | 7.999941757087116 |

## General

| | |
|---|---|
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | nmap-7.91-setup.exe |
| File size: | 27278840 |
| MD5: | 5df3bf0234f0c2af2c470f98243c788f |
| SHA1: | 7474a3c2c44e612387d1ff176179187ddc1b9bfc |
| SHA256: | c4683097a2615252eeddab06c54872efb14c2ee2da8997b1c73844e582081a79 |
| SHA512: | 5603f7097ef816672bad8c91d773096f1b5e356aa893126711c5d19cfcf6116461b8479ba52a123ad0c0cf5a74d4b38b888c7fdfbf0206010b1f476ee31fca08 |
| SSDEEP: | 786432:MmMCGcZxe4AMQr+TahplM72oULS/t4yWDp0yXfb:/Sj4xQ6WlM72ovtbWDp9b |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L.....:V.....^..... ..l2.....p....@ |

## File Icon

| | |
|---|---|
| Icon Hash: | e0d08cf8d8ccc8e0 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40326c |
| Entrypoint Section: | .text |
| Digitally signed: | true |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x56FF3A96 [Sat Apr 2 03:20:54 2016 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |
| File Version Major: | 4 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 4 |
| Subsystem Version Minor: | 0 |
| Import Hash: | b1a57b635b23ffd553b3fd1e0960b2bd |

### Authenticode Signature

| | |
|---|---|
| Signature Valid: | **true** |
| Signature Issuer: | CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US |
| Signature Validation Error: | **The operation completed successfully** |
| Error Number: | 0 |
| Not Before, Not After | • 4/30/2020 5:00:00 PM 5/7/2021 5:00:00 AM |
| Subject Chain | • CN=Insecure.Com LLC, O=Insecure.Com LLC, L=Seattle, S=Washington, C=US, SERIALNUMBER=200010310013, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US |
| Version: | 3 |
| Thumbprint MD5: | BB381AD7F010E2E2F2F63D01C7134805 |
| Thumbprint SHA-1: | 4CE89794FE2D2F7E30121F10BCF76AC3CCF77CA9 |
| Thumbprint SHA-256: | ED81C57DC455569CED035211A11C74110BF820DF0D8B09BF23024C6F0D9BAF95 |
| Serial: | 09256314069E7E6A88CB823075C0D9C9 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x5c74 | 0x5e00 | False | 0.661860039894 | data | 6.42936498783 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x7000 | 0x1196 | 0x1200 | False | 0.458767361111 | data | 5.20373620342 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x9000 | 0x3e058 | 0x600 | False | 0.439453125 | data | 4.12443350165 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .ndata | 0x48000 | 0x4e000 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rsrc | 0x96000 | 0x4e18 | 0x5000 | False | 0.562158203125 | data | 5.67340139927 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

### Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States |  |

## Network Behavior

### Network Port Distribution

### UDP Packets

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

## Analysis Process: nmap-7.91-setup.exe PID: 2432 Parent PID: 5856

### General

| | |
|---|---|
| Start time: | 21:54:31 |
| Start date: | 10/06/2021 |
| Path: | C:\Users\user\Desktop\nmap-7.91-setup.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\nmap-7.91-setup.exe' |
| Imagebase: | 0x400000 |
| File size: | 27278840 bytes |
| MD5 hash: | 5DF3BF0234F0C2AF2C470F98243C788F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

#### Key Value Modified

## Analysis Process: svchost.exe PID: 4696 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:54:27 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff77b480000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: svchost.exe PID: 1288 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:54:55 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

**Registry Activities** Show Windows behavior

## Analysis Process: npcap-1.00.exe PID: 5912 Parent PID: 2432

### General

| | |
|---|---|
| Start time: | 21:54:56 |
| Start date: | 10/06/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\nsyA5D0.tmp\npcap-1.00.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\AppData\Local\Temp\nsyA5D0.tmp\npcap-1.00.exe' /loopback_support=no |
| Imagebase: | 0x400000 |
| File size: | 791136 bytes |
| MD5 hash: | FC8CB1B4677C90859AF51C8C664E755D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

**Registry Activities** Show Windows behavior

**Key Created**

**Key Value Created**

**Key Value Modified**

## Analysis Process: svchost.exe PID: 3688 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:55:03 |
| Start date: | 10/06/2021 |

| | |
|---|---|
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: svchost.exe PID: 4348 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:55:06 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: svchost.exe PID: 5044 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:55:07 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**Registry Activities** Show Windows behavior

## Analysis Process: svchost.exe PID: 3224 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:55:08 |
| Start date: | 10/06/2021 |

| | |
|---|---|
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k NetworkService -p |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: SgrmBroker.exe PID: 6128 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:55:08 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\SgrmBroker.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\SgrmBroker.exe |
| Imagebase: | 0x7ff78f240000 |
| File size: | 163336 bytes |
| MD5 hash: | D3170A3F3A9626597EEE1888686E3EA6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: svchost.exe PID: 5512 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:55:09 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### Registry Activities

Show Windows behavior

## Analysis Process: svchost.exe PID: 6024 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:55:13 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |

| | |
|---|---|
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: MpCmdRun.exe PID: 1956 Parent PID: 5512

### General

| | |
|---|---|
| Start time: | 21:56:09 |
| Start date: | 10/06/2021 |
| Path: | C:\Program Files\Windows Defender\MpCmdRun.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable |
| Imagebase: | 0x7ff635f60000 |
| File size: | 455656 bytes |
| MD5 hash: | A267555174BFA53844371226F482B86B |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Written**

## Analysis Process: conhost.exe PID: 3944 Parent PID: 1956

### General

| | |
|---|---|
| Start time: | 21:56:10 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: NPFInstall.exe PID: 2024 Parent PID: 5912

### General

| | |
|---|---|
| Start time: | 21:56:18 |
| Start date: | 10/06/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\nsb823.tmp\NPFInstall.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Users\user\AppData\Local\Temp\nsb823.tmp\NPFInstall.exe' -n -check_dll |
| Imagebase: | 0x7ff6ac940000 |
| File size: | 307544 bytes |

| | |
|---|---|
| MD5 hash: | F93EEDCB0DF2EF914ED51CC927A1FDE9 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Antivirus matches: | • Detection: 0%, Metadefender, Browse<br>• Detection: 0%, ReversingLabs |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: conhost.exe PID: 2224 Parent PID: 2024

### General

| | |
|---|---|
| Start time: | 21:56:19 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: NPFInstall.exe PID: 2052 Parent PID: 5912

### General

| | |
|---|---|
| Start time: | 21:56:20 |
| Start date: | 10/06/2021 |
| Path: | C:\Program Files\Npcap\NPFInstall.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Npcap\NPFInstall.exe' -n -c |
| Imagebase: | 0x7ff6c2aa0000 |
| File size: | 307544 bytes |
| MD5 hash: | F93EEDCB0DF2EF914ED51CC927A1FDE9 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Antivirus matches: | • Detection: 0%, Metadefender, Browse<br>• Detection: 0%, ReversingLabs |

## Analysis Process: conhost.exe PID: 4864 Parent PID: 2052

### General

| | |
|---|---|
| Start time: | 21:56:21 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |

| | |
|---|---|
| Imagebase: | 0x7ff6b2800000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: pnputil.exe PID: 4008 Parent PID: 2052

### General

| | |
|---|---|
| Start time: | 21:56:21 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\pnputil.exe |
| Wow64 process (32bit): | false |
| Commandline: | pnputil.exe -e |
| Imagebase: | 0x7ff612ae0000 |
| File size: | 259072 bytes |
| MD5 hash: | F4C3BD7A47ACE4BEE4D864B299391DC1 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: conhost.exe PID: 4152 Parent PID: 4008

### General

| | |
|---|---|
| Start time: | 21:56:22 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: NPFInstall.exe PID: 6052 Parent PID: 5912

### General

| | |
|---|---|
| Start time: | 21:56:23 |
| Start date: | 10/06/2021 |
| Path: | C:\Program Files\Npcap\NPFInstall.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Npcap\NPFInstall.exe' -n -iw |
| Imagebase: | 0x7ff6c2aa0000 |
| File size: | 307544 bytes |
| MD5 hash: | F93EEDCB0DF2EF914ED51CC927A1FDE9 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: conhost.exe PID: 3032 Parent PID: 6052

### General

| | |
|---|---|
| Start time: | 21:56:24 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: NPFInstall.exe PID: 5212 Parent PID: 5912

### General

| | |
|---|---|
| Start time: | 21:56:24 |
| Start date: | 10/06/2021 |
| Path: | C:\Program Files\Npcap\NPFInstall.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Npcap\NPFInstall.exe' -n -i |
| Imagebase: | 0x7ff6c2aa0000 |
| File size: | 307544 bytes |
| MD5 hash: | F93EEDCB0DF2EF914ED51CC927A1FDE9 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: conhost.exe PID: 404 Parent PID: 5212

### General

| | |
|---|---|
| Start time: | 21:56:25 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: svchost.exe PID: 4744 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:56:25 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k netsvcs -p -s NetSetupSvc |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |

| | |
|---|---|
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: svchost.exe PID: 5204 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 21:56:26 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | c:\windows\system32\svchost.exe -k dcomlaunch -p -s DeviceInstall |
| Imagebase: | 0x7ff7488e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: drvinst.exe PID: 5216 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 21:56:27 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\drvinst.exe |
| Wow64 process (32bit): | false |
| Commandline: | DrvInst.exe '4' '0' 'C:\Users\user\AppData\Local\Temp\{7e40bce9-63ed-3549-a69d-3044b7b23662}\NPCAP.inf' '9' '405306be3' '00000000000001A8' 'WinSta0\Default' '000000000000001AC' '208' 'C:\Program Files\Npcap' |
| Imagebase: | 0x7ff716db0000 |
| File size: | 166912 bytes |
| MD5 hash: | 46F5A16FA391AB6EA97C602B4D2E7819 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: schtasks.exe PID: 4876 Parent PID: 5912

### General

| | |
|---|---|
| Start time: | 21:56:35 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | SCHTASKS.EXE /Create /F /RU SYSTEM /SC ONSTART /TN npcapwatchdog /TR "C:\Program Files\Npcap\CheckStatus.bat" /NP |
| Imagebase: | 0x370000 |
| File size: | 185856 bytes |
| MD5 hash: | 15FF7D8324231381BAD48A052F85DF04 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: conhost.exe PID: 4228 Parent PID: 4876

### General

| | |
|---|---|
| Start time: | 21:56:36 |
| Start date: | 10/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x1080000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

# Disassembly

## Code Analysis