Backdoors Family for Nessus

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Severity | 檢測結果 |

|  |  |  |  |
| --- | --- | --- | --- |
| 161761 | Linux BPFDoor Detection (Direct Check) | critical |  |
| 161476 | Potential Exposure to BPFDoor (Local Check - Linux) | critical |  |
| 126261 | MacOS Malicious File Detection: User Defined Malware | critical |  |
| 126260 | MacOS Malicious File Detection | critical |  |
| 126259 | Linux Malicious File Detection: User Defined Malware | critical |  |
| 126258 | Linux Malicious File Detection | critical |  |
| 124649 | YARA Scan Setup (Linux) | info |  |
| 124648 | YARA Scan Cleanup (Linux) | info |  |
| 122316 | Ncat TLS Listener | critical |  |
| 110271 | SingTel Backdoor Detection (ForgotDoor) | high |  |
| 106629 | WinShell Trojan Detection | critical |  |
| 103302 | Piriform CCleaner 5.33.6162 Backdoor | critical |  |
| 97863 | YARA Memory Scan (Linux) | critical |  |
| 97862 | YARA File Scan (Linux) | critical |  |
| 91224 | Malicious Process Detection: User Defined Malware Running (Mac OS X) | critical |  |
| 91223 | Malicious Process Detection: User Defined Malware Running (Linux) | critical |  |
| 90255 | G\_Door Malware Detection | critical |  |
| 90254 | NetSpy Malware Services Detection | critical |  |
| 86151 | Cisco IOS SYNful Knock Implant | critical |  |
| 80518 | ASUS Router 'infosvr' Remote Command Execution | critical |  |
| 78430 | ZXShell Malware Services Detection | critical |  |
| 78429 | Hikit Backdoor Detection | critical |  |
| 77606 | SYAC DigiEye Backdoor Detection | high |  |
| 73461 | HP StoreVirtual Storage Remote Unauthorized Access | high |  |
| 73104 | ZTE F460 / F660 Cable Modems web\_shell\_cmd.gch Administrative Backdoor | critical |  |
| 80457 | LusyPOS Malware Detection | critical |  |
| 71807 | ScMM DSL Modem/Router Backdoor Detection | critical |  |
| 71264 | Reputation of macOS Executables: Never seen process(es) | info |  |
| 71263 | Mac OS X Malicious Process Detection | critical |  |
| 71262 | Reputation of Linux Executables: Never seen process(es) | info |  |
| 71261 | Linux Malicious Process Detection | critical |  |
| 69555 | KINS Banking Trojan/Data Theft (credentialed check) | critical |  |
| 66391 | Linux/Cdorked.A Backdoor | critical |  |
| 58182 | DNSChanger Malware Detection | medium |  |
| 51988 | Bind Shell Backdoor Detection | critical |  |
| 50658 | Stuxnet Worm Detection (uncredentialed check) | critical |  |
| 49270 | Stuxnet Worm Detection | critical |  |
| 49211 | Here You Have Email Worm Detection | critical |  |
| 46882 | UnrealIRCd Backdoor Detection | critical |  |
| 45085 | Zeus/Zbot Banking Trojan/Data Theft (credentialed check) | critical |  |
| 45006 | Energizer DUO USB Battery Charger Software Backdoor (credentialed check) | critical |  |
| 45005 | Arugizer Backdoor Detection | critical |  |
| 36217 | Conficker P2P Service Detection | critical |  |
| 36036 | Conficker Worm Detection (uncredentialed check) | critical |  |
| 33951 | Generic Backdoor Detection (banner check) | critical |  |
| 32376 | Fake SMTP/FTP Server Detection (possible backdoor) | critical |  |
| 31854 | Malware Payload Code detection | critical |  |
| 23910 | Compromised Windows System (hosts File Check) | critical |  |
| 19429 | Zotob Worm Detection | critical |  |
| 18392 | IRC Bot Detection | critical |  |
| 18391 | SMTP Server Non-standard Port Detection | medium |  |
| 18367 | Kibuv Worm Detection | critical |  |
| 18263 | TFTP Backdoor Detection | critical |  |
| 18164 | TCP Port 0 Open: Possible Backdoor | info |  |
| 15746 | Microsoft IE FRAME/IFRAME/EMBED Tag Overflow (Bofra Worm Detection) | critical |  |
| 15586 | MoonLit Virus Backdoor Detection | critical |  |
| 15583 | Unpassworded 'bash' Backdoor Account | critical |  |
| 15570 | PostNuke Trojaned Distribution | high |  |
| 15520 | w32.spybot.fcd Worm Infection Detection | high |  |
| 15517 | Hacker Defender Backdoor Detection | critical |  |
| 15405 | Unmanarc Remote Control Server (URCS) Detection | critical |  |
| 14841 | IRC Bot ident Server Detection | critical |  |
| 14834 | Radmin (Remote Administrator) Port 10002 - Possible GDI Compromise | high |  |
| 14818 | MS04-028 Exploitation Backdoor Account Detection | high |  |
| 14184 | Zincite.A (MyDoom.M) Backdoor Detection | critical |  |
| 12287 | Microsoft IIS Download.Ject Trojan Detection | high |  |
| 12266 | W32.Dabber Worm Detection | critical |  |
| 12252 | Korgo Worm Detection | critical |  |
| 12219 | Sasser Virus Detection | high |  |
| 12128 | Agobot.FO Backdoor Detection | critical |  |
| 12111 | PhatBOT Backdoor Detection | critical |  |
| 12063 | Bagle.B Worm Detection | high |  |
| 12029 | MyDoom Virus Backdoor Detection | critical |  |
| 12027 | Bagle Worm Removal | critical |  |
| 12017 | NCASE Software Detection | high |  |
| 12013 | DOWNLOADWARE Software Detection | high |  |
| 12012 | CYDOOR Software Detection | medium |  |
| 12004 | VCATCH Spyware Detection | high |  |
| 12003 | TIMESINK Spyware Detection | high |  |
| 11881 | Wollf Backdoor Detection | critical |  |
| 11880 | Fluxay Sensor Detection | critical |  |
| 11855 | RemoteNC Backdoor Detection | critical |  |
| 11854 | FsSniffer Backdoor Detection | high |  |
| 11839 | MS03-039 Exploitation Backdoor Account Detection | critical |  |
| 11733 | Bugbear.B Worm Detection | critical |  |
| 11713 | Desktop Orbiter Unpassworded Access Remote Reboot DoS | critical |  |
| 11707 | Bugbear.B Web Backdoor Detection | critical |  |
| 11691 | Desktop Orbiter Server Detection | high |  |
| 11633 | Lovgate Virus Detection | critical |  |
| 11187 | 4553 Parasite Mothership Backdoor Detection | critical |  |
| 11170 | Alcatel OmniSwitch 7700/7800 Switches Backdoor Access (deprecated) | critical |  |
| 11157 | Trojan Horse Detection | medium |  |
| 11135 | Bugbear Worm Detection | critical |  |
| 11123 | Radmin (Remote Administrator) Port 4899 Detection | info |  |
| 11118 | alya.cgi CGI Backdoor Detection | high |  |
| 11003 | Microsoft IIS Potentially Compromised Host Detection | critical |  |
| 10921 | RemotelyAnywhere SSH Detection | info |  |
| 10920 | RemotelyAnywhere WWW Detection | info |  |
| 10646 | Lion Worm Detection | critical |  |
| 10501 | Trinity v3 Trojan Detection | critical |  |
| 10409 | SubSeven Trojan Detection | critical |  |
| 10389 | Cart32 Backdoor Password Arbitrary Command Execution | high |  |
| 10391 | mstream DDoS Handler Detection | medium |  |
| 10390 | mstream DDoS Agent Detection | medium |  |
| 10368 | Dansie Shopping Cart Backdoor Detection | critical |  |
| 10350 | Shaft Trojan Detection | critical |  |
| 10307 | Trin00 for Windows Trojan Detection | critical |  |
| 10036 | CDK Backdoor Detection | critical |  |
| 10132 | Kuang2 the Virus Detection | critical |  |
| 10288 | Trin00 Trojan Detection | critical |  |
| 10274 | SyGate Backdoor Detection | high |  |
| 10270 | Stacheldraht Trojan Detection | critical |  |
| 10316 | WinSATAN Backdoor Detection | high |  |
| 10283 | TFN (Tribe Flood Network) Trojan Detection | critical |  |
| 10152 | NetBus 2.x Software Detection | high |  |
| 10151 | NetBus 1.x Software Detection | high |  |
| 10024 | BackOrifice Software Detection | critical |  |
| 10186 | Portal of Doom Backdoor Detection | critical |  |
| 10094 | GirlFriend Backdoor Detection | critical |  |
| 10093 | GateCrasher Backdoor Detection | critical |  |
| 10053 | DeepThroat Backdoor Detection | critical |  |
| 10005 | NetSphere Backdoor Detection | critical |  |
| 10080 | Linux FTP Server Backdoor Detection | critical |  |
| 10070 | Finger Backdoor Detection | critical |  |