| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 10028 | DNS Server BIND version Directive Remote Version Detection | It is possible to obtain the version number of the remote DNS server. | The remote host is running BIND or another DNS server that reports itsversion number when it receives a special request for the text'version.bind' in the domain 'chaos'. This version is not necessarily accurate and could even be forged, assome DNS servers send the information based on a configuration file. | It is possible to hide the version number of BIND by using the'version' directive in the 'options' section in named.conf. | 53 | udp |
| 10092 | FTP Server Detection | An FTP server is listening on a remote port. | It is possible to obtain the banner of the remote FTP server byconnecting to a remote port. | n/a | 21 | tcp |
| 10092 | FTP Server Detection | An FTP server is listening on a remote port. | It is possible to obtain the banner of the remote FTP server byconnecting to a remote port. | n/a | 2121 | tcp |
| 10107 | HTTP Server Type and Version | A web server is running on the remote host. | This plugin attempts to determine the type and the version of the remote web server. | n/a | 80 | tcp |
| 10114 | ICMP Timestamp Request Remote Date Disclosure | It is possible to determine the exact time set on the remote host. | The remote host answers to an ICMP timestamp request. This allows anattacker to know the date that is set on the targeted machine, whichmay assist an unauthenticated, remote attacker in defeating time-basedauthentication protocols.Timestamps returned from machines running Windows Vista / 7 / 2008 /2008 R2 are deliberately incorrect, but usually within 1000 seconds ofthe actual system time. | Filter out the ICMP timestamp requests (13), and the outgoing ICMPtimestamp replies (14). | 0 | icmp |
| 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure | It was possible to obtain the network name of the remote host. | The remote host is listening on UDP port 137 or TCP port 445, andreplies to NetBIOS nbtscan or SMB requests.Note that this plugin gathers information to be used in other plugins,but does not itself generate a report. | n/a | 137 | udp |
| 10223 | RPC portmapper Service Detection | An ONC RPC portmapper is running on the remote host. | The RPC portmapper is running on this port.The portmapper allows someone to get the port number of each RPCservice running on the remote host by sending either multiple lookuprequests or a DUMP request. | n/a | 111 | udp |
| 10263 | SMTP Server Detection | An SMTP server is listening on the remote port. | The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers, it is recommended youdisable it if you do not use it. | Disable this service if you do not use it, or filter incoming trafficto this port. | 25 | tcp |
| 10267 | SSH Server Type and Version Information | An SSH server is listening on this port. | It is possible to obtain information about the remote SSH server bysending an empty authentication request. | n/a | 22 | tcp |
| 10281 | Telnet Server Detection | A Telnet server is listening on the remote port. | The remote host is running a Telnet server, a remote terminalserver. | Disable this service if you do not use it. | 23 | tcp |
| 10287 | Traceroute Information | It was possible to obtain traceroute information. | Makes a traceroute to the remote host. | n/a | 0 | udp |
| 10342 | VNC Software Detection | The remote host is running a remote display software (VNC). | The remote host is running VNC (Virtual Network Computing), which usesthe RFB (Remote Framebuffer) protocol to provide remote access tographical user interfaces and thus permits a console on the remotehost to be displayed on another. | Make sure use of this software is done in accordance with yourorganization's security policy and filter incoming traffic to thisport. | 5900 | tcp |
| 10397 | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure | It is possible to obtain network information. | It was possible to obtain the browse list of the remote Windows systemby sending a request to the LANMAN pipe. The browse list is the listof the nearest Windows systems of the remote host. | n/a | 445 | tcp |
| 10437 | NFS Share Export List | The remote NFS server exports a list of shares. | This plugin retrieves the list of NFS exported shares. | Ensure each share is intended to be exported. | 2049 | tcp |
| 10662 | Web mirroring | Nessus can crawl the remote website. | This plugin makes a mirror of the remote website(s) and extracts thelist of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the'Options' section of the client. | n/a | 80 | tcp |
| 10719 | MySQL Server Detection | A database server is listening on the remote port. | The remote host is running MySQL, an open source database server. | n/a | 3306 | tcp |
| 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure | It was possible to obtain information about the remote operatingsystem. | Nessus was able to obtain the remote operating system name and version(Windows and/or Samba) by sending an authentication request to port139 or 445. Note that this plugin requires SMB to be enabled on thehost. | n/a | 445 | tcp |
| 10863 | SSL Certificate Information | This plugin displays the SSL certificate. | This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate. | n/a | 25 | tcp |
| 10863 | SSL Certificate Information | This plugin displays the SSL certificate. | This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate. | n/a | 5432 | tcp |
| 10881 | SSH Protocol Versions Supported | A SSH server is running on the remote host. | This plugin determines the versions of the SSH protocol supported bythe remote SSH daemon. | n/a | 22 | tcp |
| 11002 | DNS Server Detection | A DNS server is listening on the remote host. | The remote service is a Domain Name System (DNS) server, whichprovides a mapping between hostnames and IP addresses. | Disable this service if it is not needed or restrict access tointernal hosts only if the service is available externally. | 53 | tcp |
| 11002 | DNS Server Detection | A DNS server is listening on the remote host. | The remote service is a Domain Name System (DNS) server, whichprovides a mapping between hostnames and IP addresses. | Disable this service if it is not needed or restrict access tointernal hosts only if the service is available externally. | | udp |
| 11011 | Microsoft Windows SMB Service Detection | A file / print sharing service is listening on the remote host. | The remote service understands the CIFS (Common Internet File System)or Server Message Block (SMB) protocol, used to provide shared accessto files, printers, etc between nodes on a network. | n/a | 139 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 11011 | Microsoft Windows SMB Service Detection | A file / print sharing service is listening on the remote host. | The remote service understands the CIFS (Common Internet File System)or Server Message Block (SMB) protocol, used to provide shared accessto files, printers, etc between nodes on a network. | n/a | 445 | tcp |
| 11032 | Web Server Directory Enumeration | It is possible to enumerate directories on the web server. | This plugin attempts to determine the presence of various commondirectories on the remote web server. By sending a request for adirectory, the web server response code indicates if it is a validdirectory or not. | n/a | 80 | tcp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 111 | tcp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | | udp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 2049 | tcp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | | udp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 34478 | udp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 46942 | tcp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 51373 | udp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 52754 | tcp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 55637 | tcp |
| 11111 | RPC Services Enumeration | An ONC RPC service is running on the remote host. | By sending a DUMP request to the portmapper, it was possible toenumerate the ONC RPC services running on the remote port. Using thisinformation, it is possible to connect and bind to each service bysending an RPC request to the remote port. | n/a | 55889 | udp |
| 11153 | Service Detection (HELP Request) | The remote service could be identified. | It was possible to identify the remote service by its banner or bylooking at the error message it sends when it receives a 'HELP'request. | n/a | 3306 | tcp |
| 11154 | Unknown Service Detection: Banner Retrieval | There is an unknown service running on the remote host. | Nessus was unable to identify a service on the remote host even thoughit returned a banner of some type. | n/a | 512 | tcp |
| 11154 | Unknown Service Detection: Banner Retrieval | There is an unknown service running on the remote host. | Nessus was unable to identify a service on the remote host even thoughit returned a banner of some type. | n/a | 8787 | tcp |
| 11156 | IRC Daemon Version Detection | The remote host is an IRC server. | This plugin determines the version of the IRC daemon. | n/a | 6667 | tcp |
| 11156 | IRC Daemon Version Detection | The remote host is an IRC server. | This plugin determines the version of the IRC daemon. | n/a | 6697 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 21 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 22 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 23 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 25 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 53 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 80 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 111 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 139 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 445 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 512 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 513 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 514 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 1099 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 1524 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 2049 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 2121 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 3306 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 3632 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 5432 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 5900 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 6000 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 6667 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 6697 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 8009 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 8180 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 8787 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 41513 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 46942 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 52754 | tcp |
| 11219 | Nessus SYN scanner | It is possible to determine which TCP ports are open. | This plugin is a SYN 'half-open' port scanner. It shall be reasonablyquick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scansagainst broken services, but they might cause problems for less robustfirewalls and also leave unclosed connections on the remote target, ifthe network is loaded. | Protect your target with an IP filter. | 55637 | tcp |
| 11419 | Web Server Office File Inventory | The remote web server hosts office-related files. | This plugin connects to the remote web server and attempts to findoffice-related files such as .doc, .ppt, .xls, .pdf etc. | Make sure that such files do not contain any confidential or otherwisesensitive information and that they are only accessible to those withvalid credentials. | 80 | tcp |
| 11424 | WebDAV Detection | The remote server is running with WebDAV enabled. | WebDAV is an industry standard extension to the HTTP specification.It adds a capability for authorized users to remotely add and managethe content of a web server.If you do not use this extension, you should disable it. | http://support.microsoft.com/default.aspx?kbid=241520 | 80 | tcp |
| 11819 | TFTP Daemon Detection | A TFTP server is listening on the remote port. | The remote host is running a TFTP (Trivial File Transfer Protocol)daemon. TFTP is often used by routers and diskless hosts to retrievetheir configuration. It can also be used by worms to propagate. | Disable this service if you do not use it. | 69 | udp |
| 11936 | OS Identification | It is possible to guess the remote operating system. | Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP,SNMP, etc.), it is possible to guess the name of the remote operatingsystem in use. It is also possible sometimes to guess the version ofthe operating system. | n/a | 0 | tcp |
| 14788 | IP Protocols Scan | This plugin detects the protocols understood by the remote IP stack. | This plugin detects the protocols understood by the remote IP stack. | n/a | 0 | tcp |
| 17219 | phpMyAdmin Detection | The remote web server hosts a database management application writtenin PHP. | The remote host is running phpMyAdmin, a web-based MySQLadministration tool written in PHP. | n/a | 80 | tcp |
| 17975 | Service Detection (GET request) | The remote service could be identified. | It was possible to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 6667 | tcp |
| 17975 | Service Detection (GET request) | The remote service could be identified. | It was possible to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 6697 | tcp |
| 18261 | Apache Banner Linux Distribution Disclosure | The name of the Linux distribution running on the remote host wasfound in the banner of the web server. | Nessus was able to extract the banner of the Apache web server anddetermine which Linux distribution the remote host is running. | If you do not wish to display this information, edit 'httpd.conf' andset the directive 'ServerTokens Prod' and restart Apache. | 0 | tcp |
| 19288 | VNC Server Security Type Detection | A VNC server is running on the remote host. | This script checks the remote VNC server protocol version and theavailable 'security types'. | n/a | 5900 | tcp |
| 19506 | Nessus Scan Information | This plugin displays information about the Nessus scan. | This plugin displays, for each tested host, information about thescan itself : - The version of the plugin set. - The type of scanner (Nessus or Nessus Home). - The version of the Nessus Engine. - The port scanner(s) used. - The port range scanned. - The ping round trip time - Whether credentialed or third-party patch management checks are possible. - Whether the display of superseded patches is enabled - The date of the scan. - The duration of the scan. - The number of hosts scanned in parallel - The number of checks done in parallel | n/a | 0 | tcp |
| 19941 | TWiki Detection | The remote web server hosts a Wiki system written in Perl. | The remote host is running TWiki, an open source wiki system writtenin Perl. | n/a | 80 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 21643 | SSL Cipher Suites Supported | The remote service encrypts communications using SSL. | This plugin detects which SSL ciphers are supported by the remoteservice for encrypting communications. | n/a | 25 | tcp |
| 21643 | SSL Cipher Suites Supported | The remote service encrypts communications using SSL. | This plugin detects which SSL ciphers are supported by the remoteservice for encrypting communications. | n/a | 5432 | tcp |
| 22227 | RMI Registry Detection | An RMI registry is listening on the remote host. | The remote host is running an RMI registry, which acts as a bootstrapnaming service for registering and retrieving remote objects withsimple names in the Java Remote Method Invocation (RMI) system. | n/a | 1099 | tcp |
| 22227 | RMI Registry Detection | An RMI registry is listening on the remote host. | The remote host is running an RMI registry, which acts as a bootstrapnaming service for registering and retrieving remote objects withsimple names in the Java Remote Method Invocation (RMI) system. | n/a | 41513 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 21 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 22 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 23 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 25 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 80 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 1524 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 2121 | tcp |
| 22964 | Service Detection | The remote service could be identified. | Nessus was able to identify the remote service by its banner or bylooking at the error message it sends when it receives an HTTPrequest. | n/a | 5900 | tcp |
| 24004 | WebDAV Directory Enumeration | Several directories on the remote host are DAV-enabled. | WebDAV is an industry standard extension to the HTTP specification.It adds a capability for authorized users to remotely add and managethe content of a web server.If you do not use this extension, you should disable it. | Disable DAV support if you do not use it. | 80 | tcp |
| 24260 | HyperText Transfer Protocol (HTTP) Information | Some information about the remote HTTP configuration can be extracted. | This test gives some information about the remote HTTP protocol - theversion used, whether HTTP Keep-Alive and HTTP pipelining are enabled,etc... This test is informational only and does not denote any securityproblem. | n/a | 80 | tcp |
| 25220 | TCP/IP Timestamps Supported | The remote service implements TCP timestamps. | The remote host implements TCP timestamps, as defined by RFC1323. Aside effect of this feature is that the uptime of the remote host cansometimes be computed. | n/a | 0 | tcp |
| 25240 | Samba Server Detection | An SMB server is running on the remote host. | The remote host is running Samba, a CIFS/SMB server for Linux andUnix. | n/a | 445 | tcp |
| 26024 | PostgreSQL Server Detection | A database service is listening on the remote host. | The remote service is a PostgreSQL database server, or a derivativesuch as EnterpriseDB. | Limit incoming traffic to this port if desired. | 5432 | tcp |
| 33817 | CGI Generic Tests Load Estimation (all tests) | Load estimation for web application tests. | This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.Note that the script does not try to compute this duration based on external factors such as the network and web servers loads. | n/a | 80 | tcp |
| 35371 | DNS Server hostname.bind Map Hostname Disclosure | The DNS server discloses the remote host name. | It is possible to learn the remote host name by querying the remoteDNS server for 'hostname.bind' in the CHAOS domain. | It may be possible to disable this feature. Consult the vendor'sdocumentation for more information. | 53 | udp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 39470 | CGI Generic Tests Timeout | Some generic CGI attacks ran out of time. | Some generic CGI tests ran out of time during the scan. The resultsmay be incomplete. | Consider increasing the 'maximum run time (minutes)' preference forthe 'Web Applications Settings' in order to prevent the CGI scanningfrom timing out. Less ambitious options could also be used, such as : - Test more that one parameter at a time per form : 'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'. - 'Stop after one flaw is found per web server (fastest)' under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'. - In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'. | 80 | tcp |
| 39519 | Backported Security Patch Detection (FTP) | Security patches are backported. | Security patches may have been 'backported' to the remote FTP serverwithout changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote anysecurity problem. | n/a | 2121 | tcp |
| 39520 | Backported Security Patch Detection (SSH) | Security patches are backported. | Security patches may have been 'backported' to the remote SSH serverwithout changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote anysecurity problem. | n/a | 22 | tcp |
| 39521 | Backported Security Patch Detection (WWW) | Security patches are backported. | Security patches may have been 'backported' to the remote HTTP serverwithout changing its version number.Banner-based checks have been disabled to avoid false positives.Note that this test is informational only and does not denote anysecurity problem. | n/a | 80 | tcp |
| 40773 | Web Application Potentially Sensitive CGI Parameter Detection | An application was found that may use CGI parameters to controlsensitive information. | According to their names, some CGI parameters may control sensitivedata (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclosesensitive data or be prone to tampering that could result in privilegeescalation. These parameters should be examined to determine whattype of data is controlled and if it poses a security risk.** This plugin only reports information that may be useful for auditors** or pen-testers, not a real flaw. | Ensure sensitive data is not disclosed by CGI parameters. Inaddition, do not use CGI parameters to control access to resources orprivileges. | 80 | tcp |
| 42088 | SMTP Service STARTTLS Command Support | The remote mail service supports encrypting traffic. | The remote SMTP service supports the use of the 'STARTTLS' command toswitch from a cleartext to an encrypted communications channel. | n/a | 25 | tcp |
| 43111 | HTTP Methods Allowed (per directory) | This plugin determines which HTTP methods are allowed on various CGIdirectories. | By calling the OPTIONS method, it is possible to determine which HTTPmethods are allowed on each directory.The following HTTP methods are considered insecure: PUT, DELETE, CONNECT, TRACE, HEADMany frameworks and languages treat 'HEAD' as a 'GET' request, albeitone without any body in the response. If a security constraint wasset on 'GET' requests such that only 'authenticatedUsers' couldaccess GET requests for a particular servlet or resource, it would bebypassed for the 'HEAD' version. This allowed unauthorized blindsubmission of any privileged GET request.As this list may be incomplete, the plugin also tests - if 'Thoroughtests' are enabled or 'Enable web applications tests' is set to 'yes'in the scan policy - various known HTTP methods on each directory andconsiders them as unsupported if it receives a response code of 400,403, 405, or 501.Note that the plugin output is only informational and does notnecessarily indicate the presence of any security vulnerabilities. | n/a | 80 | tcp |
| 45410 | SSL Certificate 'commonName' Mismatch | The 'commonName' (CN) attribute in the SSL certificate does not matchthe hostname. | The service running on the remote host presents an SSL certificate forwhich the 'commonName' (CN) attribute does not match the hostname onwhich the service listens. | If the machine has several names, make sure that users connect to theservice through the DNS hostname that matches the common name in thecertificate. | 25 | tcp |
| 45410 | SSL Certificate 'commonName' Mismatch | The 'commonName' (CN) attribute in the SSL certificate does not matchthe hostname. | The service running on the remote host presents an SSL certificate forwhich the 'commonName' (CN) attribute does not match the hostname onwhich the service listens. | If the machine has several names, make sure that users connect to theservice through the DNS hostname that matches the common name in thecertificate. | 5432 | tcp |
| 45590 | Common Platform Enumeration (CPE) | It was possible to enumerate CPE names that matched on the remotesystem. | By using information obtained from a Nessus scan, this plugin reportsCPE (Common Platform Enumeration) matches for various hardware andsoftware products found on a host. Note that if an official CPE is not available for the product, thisplugin computes the best possible CPE based on the informationavailable from the scan. | n/a | 0 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 47830 | CGI Generic Injectable Parameter | Some CGIs are candidate for extended injection tests. | Nessus was able to to inject innocuous strings into CGI parametersand read them back in the HTTP response.The affected parameters are candidates for extended injection testslike cross-site scripting attacks.This is not a weakness per se, the main purpose of this test is to speedup other scripts. The results may be useful for a human pen-tester. | n/a | 80 | tcp |
| 48204 | Apache HTTP Server Version | It is possible to obtain the version number of the remote Apache HTTPserver. | The remote host is running the Apache HTTP Server, an open source webserver. It was possible to read the version number from the banner. | n/a | 80 | tcp |
| 48243 | PHP Version Detection | It was possible to obtain the version number of the remote PHPinstallation. | Nessus was able to determine the version of PHP available on theremote web server. | n/a | 80 | tcp |
| 49704 | External URLs | Links to external sites were gathered. | Nessus gathered HREF links to external sites by crawling the remoteweb server. | n/a | 80 | tcp |
| 49705 | Web Server Harvested Email Addresses | Email addresses were harvested from the web server. | Nessus harvested HREF mailto: links and extracted email addresses bycrawling the remote web server. | n/a | 80 | tcp |
| 50344 | Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header | The remote web server does not take steps to mitigate a class of webapplication vulnerabilities. | The remote web server in some responses sets a permissiveContent-Security-Policy (CSP) frame-ancestors response header or doesnot set one at all.The CSP frame-ancestors header has been proposed by the W3C WebApplication Security Working Group as a way to mitigate cross-sitescripting and clickjacking attacks. | Set a non-permissive Content-Security-Policy frame-ancestors headerfor all requested resources. | 80 | tcp |
| 50345 | Missing or Permissive X-Frame-Options HTTP Response Header | The remote web server does not take steps to mitigate a class of webapplication vulnerabilities. | The remote web server in some responses sets a permissiveX-Frame-Options response header or does not set one at all.The X-Frame-Options header has been proposed by Microsoft as a way tomitigate clickjacking attacks and is currently supported by all majorbrowser vendors | Set a properly configured X-Frame-Options header for all requestedresources. | 80 | tcp |
| 50845 | OpenSSL Detection | The remote service appears to use OpenSSL to encrypt traffic. | Based on its response to a TLS request with a specially craftedserver name extension, it seems that the remote service is using theOpenSSL library to encrypt traffic.Note that this plugin can only detect OpenSSL implementations thathave enabled support for TLS extensions (RFC 4366). | n/a | 25 | tcp |
| 50845 | OpenSSL Detection | The remote service appears to use OpenSSL to encrypt traffic. | Based on its response to a TLS request with a specially craftedserver name extension, it seems that the remote service is using theOpenSSL library to encrypt traffic.Note that this plugin can only detect OpenSSL implementations thathave enabled support for TLS extensions (RFC 4366). | n/a | 5432 | tcp |
| 51891 | SSL Session Resume Supported | The remote host allows resuming SSL sessions. | This script detects whether a host allows resuming SSL sessions byperforming a full SSL handshake to receive a session ID, and thenreconnecting with the previously used session ID. If the serveraccepts the session ID in the second connection, the server maintainsa cache of sessions that can be resumed. | n/a | 25 | tcp |
| 52703 | vsftpd Detection | An FTP server is listening on the remote port. | The remote host is running vsftpd, an FTP server for UNIX-likesystems written in C. | n/a | 21 | tcp |
| 53335 | RPC portmapper (TCP) | An ONC RPC portmapper is running on the remote host. | The RPC portmapper is running on this port. The portmapper allows someone to get the port number of each RPCservice running on the remote host by sending either multiple lookuprequests or a DUMP request. | n/a | 111 | tcp |
| 54615 | Device Type | It is possible to guess the remote device type. | Based on the remote operating system, it is possible to determinewhat the remote system type is (eg: a printer, router, general-purposecomputer, etc). | n/a | 0 | tcp |
| 56984 | SSL / TLS Versions Supported | The remote service encrypts communications. | This plugin detects which SSL and TLS versions are supported by theremote service for encrypting communications. | n/a | 25 | tcp |
| 56984 | SSL / TLS Versions Supported | The remote service encrypts communications. | This plugin detects which SSL and TLS versions are supported by theremote service for encrypting communications. | n/a | 5432 | tcp |
| 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported | The remote service supports the use of SSL Perfect Forward Secrecyciphers, which maintain confidentiality even if the key is stolen. | The remote host supports the use of SSL ciphers that offer PerfectForward Secrecy (PFS) encryption. These cipher suites ensure thatrecorded SSL traffic cannot be broken at a future date if the server'sprivate key is compromised. | n/a | 25 | tcp |
| 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported | The remote service supports the use of SSL Perfect Forward Secrecyciphers, which maintain confidentiality even if the key is stolen. | The remote host supports the use of SSL ciphers that offer PerfectForward Secrecy (PFS) encryption. These cipher suites ensure thatrecorded SSL traffic cannot be broken at a future date if the server'sprivate key is compromised. | n/a | 5432 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 65792 | VNC Server Unencrypted Communication Detection | A VNC server with one or more unencrypted 'security-types' is runningon the remote host. | This script checks the remote VNC server protocol version and theavailable 'security types' to determine if any unencrypted'security-types' are in use or available. | n/a | 5900 | tcp |
| 66334 | Patch Report | The remote host is missing several patches. | The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin,it will always run and cannot be disabled. | Install the patches listed below. | 0 | tcp |
| 70544 | SSL Cipher Block Chaining Cipher Suites Supported | The remote service supports the use of SSL Cipher Block Chainingciphers, which combine previous blocks with subsequent ones. | The remote host supports the use of SSL ciphers that operate in CipherBlock Chaining (CBC) mode. These cipher suites offer additionalsecurity over Electronic Codebook (ECB) mode, but have the potential toleak information if used improperly. | n/a | 25 | tcp |
| 70544 | SSL Cipher Block Chaining Cipher Suites Supported | The remote service supports the use of SSL Cipher Block Chainingciphers, which combine previous blocks with subsequent ones. | The remote host supports the use of SSL ciphers that operate in CipherBlock Chaining (CBC) mode. These cipher suites offer additionalsecurity over Electronic Codebook (ECB) mode, but have the potential toleak information if used improperly. | n/a | 5432 | tcp |
| 70657 | SSH Algorithms and Languages Supported | An SSH server is listening on this port. | This script detects which algorithms and languages are supported bythe remote service for encrypting communications. | n/a | 22 | tcp |
| 84574 | Backported Security Patch Detection (PHP) | Security patches have been backported. | Security patches may have been 'backported' to the remote PHP installwithout changing its version number.Banner-based checks have been disabled to avoid false positives.Note that this test is informational only and does not denote anysecurity problem. | n/a | 80 | tcp |
| 85601 | Web Application Cookies Not Marked HttpOnly | HTTP session cookies might be vulnerable to cross-site scriptingattacks. | The remote web application sets various cookies throughout a user'sunauthenticated and authenticated session. However, one or more ofthose cookies are not marked 'HttpOnly', meaning that a maliciousclient-side script, such as JavaScript, could read them. The HttpOnlyflag is a security mechanism to protect against cross-site scriptingattacks, which was proposed by Microsoft and initially implemented inInternet Explorer. All modern browsers now support it.Note that this plugin detects all general cookies missing the HttpOnlycookie flag, whereas plugin 48432 (Web Application Session CookiesNot Marked HttpOnly) will only detect session cookies from anauthenticated session missing the HttpOnly cookie flag | Each cookie should be carefully reviewed to determine if it containssensitive data or is relied upon for a security decision.If possible, add the 'HttpOnly' attribute to all session cookiesand any cookies containing sensitive data. | 80 | tcp |
| 85602 | Web Application Cookies Not Marked Secure | HTTP session cookies might be transmitted in cleartext. | The remote web application sets various cookies throughout a user'sunauthenticated and authenticated session. However, there areinstances where the application is running over unencrypted HTTP orthe cookies are not marked 'secure', meaning the browser could sendthem back over an unencrypted link under certain circumstances. As aresult, it may be possible for a remote attacker to intercept thesecookies.Note that this plugin detects all general cookies missing the 'secure'cookie flag, whereas plugin 49218 (Web Application Session CookiesNot Marked Secure) will only detect session cookies from anauthenticated session missing the secure cookie flag | Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data. | 80 | tcp |
| 91815 | Web Application Sitemap | The remote web server hosts linkable content that can be crawled byNessus. | The remote web server contains linkable content that can be used togather information about a target. | n/a | 80 | tcp |
| 96982 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) | The remote Windows host supports the SMBv1 protocol. | The remote Windows host supports Server Message Block Protocolversion 1 (SMBv1). Microsoft recommends that users discontinue the useof SMBv1 due to the lack of security features that were included inlater SMB versions. Additionally, the Shadow Brokers group reportedlyhas an exploit that affects SMB; however, it is unknown if the exploitaffects SMBv1 or another version. In response to this, US-CERTrecommends that users disable SMBv1 per SMB best practices to mitigatethese potential issues. | Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices. | 445 | tcp |
| 100669 | Web Application Cookies Are Expired | HTTP cookies have an 'Expires' attribute that is set with a past dateor time. | The remote web application sets various cookies throughout a user'sunauthenticated and authenticated session. However, Nessus hasdetected that one or more of the cookies have an 'Expires' attributethat is set with a past date or time, meaning that these cookies willbe removed by the browser. | Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.If needed, set an expiration date in the future so the cookie willpersist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie. | 80 | tcp |
| 100871 | Microsoft Windows SMB Versions Supported (remote check) | It was possible to obtain information about the version of SMB runningon the remote host. | Nessus was able to obtain the version of SMB running on the remotehost by sending an authentication request to port 139 or 445.Note that this plugin is a remote check and does not work on agents. | n/a | 445 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 104887 | Samba Version | It was possible to obtain the samba version from the remote operating system. | Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host. | n/a | 445 | tcp |
| 106716 | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) | It was possible to obtain information about the dialects of SMB2 and SMB3 availableon the remote host. | Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445. | n/a | 445 | tcp |
| 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided | Nessus was able to find common ports used for local checks,however, no credentials were provided in the scan policy. | Nessus was not able to successfully authenticate directly to theremote target on an available authentication protocol. Nessus wasable to connect to the remote port and identify that the servicerunning on the port supports an authentication protocol, but Nessusfailed to authenticate to the remote service using the providedcredentials. There may have been a protocol failure that preventedauthentication from being attempted or all of the provided credentialsfor the authentication protocol may be invalid. See plugin output forerror details.Please note the following :- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets | n/a | 0 | tcp |
| 117886 | OS Security Patch Assessment Not Available | OS Security Patch Assessment is not available. | OS Security Patch Assessment is not available on the remote host.This does not necessarily indicate a problem with the scan.Credentials may not have been provided, OS security patch assessmentmay not be supported for the target, the target may not have beenidentified, or another issue may have occurred that prevented OSsecurity patch assessment from being available. See plugin output fordetails.This plugin reports non-failure information impacting the availabilityof OS Security Patch Assessment. Failure information is reported byplugin 21745 : 'OS Security Patch Assessment failed'. If a targethost is not supported for OS Security Patch Assessment, plugin110695 : 'OS Security Patch Assessment Checks Not Supported' willreport concurrently with this plugin. | n/a | 0 | tcp |
| 118224 | PostgreSQL STARTTLS Support | The remote service supports encrypting traffic. | The remote PostgreSQL server supports the use of encryptioninitiated during pre-login to switch from a cleartext to anencrypted communications channel. | n/a | 5432 | tcp |
| 132634 | Deprecated SSLv2 Connection Attempts | Secure Connections, using a deprecated protocol were attempted as part of the scan | This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later. | n/a | 0 | tcp |
| 135860 | WMI Not Available | WMI queries could not be made against the remote host. | WMI (Windows Management Instrumentation) is not available on theremote host over DCOM. WMI queries are used to gather informationabout the remote host, such as its current state, network interfaceconfiguration, etc.Without this information Nessus may not be able to identify installedsoftware or security vunerabilities that exist on the remote host. | n/a | 445 | tcp |
| 149334 | SSH Password Authentication Accepted | The SSH server on the remote host accepts password authentication. | The SSH server on the remote host accepts password authentication. | n/a | 22 | tcp |
| 153588 | SSH SHA-1 HMAC Algorithms Enabled | The remote SSH server is configured to enable SHA-1 HMAC algorithms. | The remote SSH server is configured to enable SHA-1 HMAC algorithms.Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC asthe security of HMAC does not rely on the underlying hash function being resistant to collisions.Note that this plugin only checks for the options of the remote SSH server. | n/a | 22 | tcp |

| Plugin ID | Name | Synopsis | Description | Solution | Port | Protocol |
|---|---|---|---|---|---|---|
| 156899 | SSL/TLS Recommended Cipher Suites | The remote host advertises discouraged SSL/TLS ciphers. | The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enablesupport for the following cipher suites:TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256 - 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305 - 0x00,0x9E DHE-RSA-AES128-GCM-SHA256 - 0x00,0x9F DHE-RSA-AES256-GCM-SHA384This is the recommended configuration for the vast majority of services, as it is highly secure and compatible withnearly every client released in the last five (or more) years. | Only enable support for recommened cipher suites. | 25 | tcp |
| 156899 | SSL/TLS Recommended Cipher Suites | The remote host advertises discouraged SSL/TLS ciphers. | The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enablesupport for the following cipher suites:TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256 - 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305 - 0x00,0x9E DHE-RSA-AES128-GCM-SHA256 - 0x00,0x9F DHE-RSA-AES256-GCM-SHA384This is the recommended configuration for the vast majority of services, as it is highly secure and compatible withnearly every client released in the last five (or more) years. | Only enable support for recommened cipher suites. | 5432 | tcp |