Vulnerability Scan Report

Generated on: 2025-06-26 12:45:43

Host Scan Summary

Host: 127.0.0.1

[Info] OS Security Patch Assessment Not Available (Port 0/tcp)

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 assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

[Info] Common Platform Enumeration (CPE) (Port 0/tcp)

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

[Info] Nessus Scan Information (Port 0/tcp)

This plugin displays, for each tested host, information about the scan 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- Whether the display of superseded patches is enabled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.

[Info] Target Credential Status by Authentication Protocol - No Credentials Provided (Port 0/tcp)

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error 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 than for Linux targets.

[Info] Device Type (Port 0/tcp)

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

[Info] OS Fingerprints Detected (Port 0/tcp)

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

[Info] OS Identification (Port 0/tcp)

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 operating system in use. It is also possible sometimes to guess the version of the operating system.

[Medium] SSL Certificate Cannot Be Trusted (Port 8834/tcp)

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

[Info] OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) (Port 0/tcp)

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

[Info] SSL Certificate Information (Port 8834/tcp)

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

[Info] SSL Perfect Forward Secrecy Cipher Suites Supported (Port 8834/tcp)

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

[Info] TLS Version 1.3 Protocol Detection (Port 8834/tcp)

The remote service accepts connections encrypted using TLS 1.3.

[Info] TLS Version 1.2 Protocol Detection (Port 8834/tcp)

The remote service accepts connections encrypted using TLS 1.2.

[Info] SSL Cipher Suites Supported (Port 8834/tcp)

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

[Info] SSL / TLS Versions Supported (Port 8834/tcp)

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

[Info] HyperText Transfer Protocol (HTTP) Information (Port 8834/tcp)

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

[Info] Nessus Server Detection (Port 8834/tcp)

A Nessus daemon is listening on the remote port.

[Info] Strict Transport Security (STS) Detection (Port 8834/tcp)

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

[Info] HTTP Server Type and Version (Port 8834/tcp)

This plugin attempts to determine the type and the version of the   remote web server.

[Info] VMware ESX/GSX Server Authentication Daemon Detection (Port 912/tcp)

The authentication daemon for VMware ESX or GSX was detected on the remote host.

[Info] VMware ESX/GSX Server Authentication Daemon Detection (Port 902/tcp)

The authentication daemon for VMware ESX or GSX was detected on the remote host.

[Info] Service Detection (Port 912/tcp)

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

[Info] Service Detection (Port 902/tcp)

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

[Info] Service Detection (Port 8834/tcp)

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

[Info] Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) (Port 445/tcp)

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.

[Info] Host Fully Qualified Domain Name (FQDN) Resolution (Port 0/tcp)

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

[Info] Microsoft Windows SMB Versions Supported (remote check) (Port 445/tcp)

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

[Info] WMI Not Available (Port 445/tcp)

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

[Info] Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure (Port 445/tcp)

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

[Info] Service Detection (Port 8834/tcp)

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

[Info] Netstat Connection Information (Port 0/tcp)

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

[Info] Microsoft Windows SMB NativeLanManager Remote System Information Disclosure (Port 445/tcp)

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

[Info] Windows NetBIOS / SMB Remote Host Information Disclosure (Port 445/tcp)

The remote host is listening on UDP port 137 or TCP port 445, and replies 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.

[Info] DCE Services Enumeration (Port 49669/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] DCE Services Enumeration (Port 49668/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] DCE Services Enumeration (Port 49667/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] DCE Services Enumeration (Port 49666/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] DCE Services Enumeration (Port 49665/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] DCE Services Enumeration (Port 49664/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] DCE Services Enumeration (Port 445/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] DCE Services Enumeration (Port 135/tcp)

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

[Info] Microsoft Windows SMB Service Detection (Port 445/tcp)

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

[Info] Netstat Portscanner (SSH) (Port 53118/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 53116/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 53117/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 53121/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 53122/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 53120/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 1900/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 138/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 137/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 63785/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 56439/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 55367/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 54996/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 54984/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 54509/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 51934/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 51228/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 5355/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 5353/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 5050/udp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 139/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 49669/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 49668/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 49667/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 49666/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 49665/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 49664/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 8834/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 7680/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 5040/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 912/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 902/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 445/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

[Info] Netstat Portscanner (SSH) (Port 135/tcp)

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.