Nessus Scan Report

OS Security Patch Assessment Not Available (Info)

Host: 192.168.29.200
Plugin ID: 117886
Risk Factor: None
CVE: N/A
Description: 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.

Nessus Scan Information (Info)

Host: 192.168.29.200
Plugin ID: 19506
Risk Factor: None
CVE: N/A
Description: 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- Whether the display of superseded patches is enabled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.

Common Platform Enumeration (CPE) (Info)

Host: 192.168.29.200
Plugin ID: 45590
Risk Factor: None

CVE: N/A
Description: 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.

Target Credential Status by Authentication Protocol - No Credentials Provided (Info)

Host: 192.168.29.200
Plugin ID: 110723
Risk Factor: None
CVE: N/A
Description: 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.

Device Type (Info)

Host: 192.168.29.200
Plugin ID: 54615
Risk Factor: None
CVE: N/A
Description: 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).

OS Fingerprints Detected (Info)

Host: 192.168.29.200

Plugin ID: 209654

Risk Factor: None

CVE: N/A

Description: 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.

SSL Cipher Block Chaining Cipher Suites Supported (Info)

Host: 192.168.29.200

Plugin ID: 70544

Risk Factor: None

CVE: N/A

Description: The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

SSL Perfect Forward Secrecy Cipher Suites Supported (Info)

Host: 192.168.29.200

Plugin ID: 57041

Risk Factor: None

CVE: N/A

Description: 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.

SSL Perfect Forward Secrecy Cipher Suites Supported (Info)

Host: 192.168.29.200

Plugin ID: 57041

Risk Factor: None

CVE: N/A

Description: 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.

SSL/TLS Recommended Cipher Suites (Info)

Host: 192.168.29.200

Plugin ID: 156899

Risk Factor: None

CVE: N/A

Description: The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support 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_SHA256

TLSv1.2:
- 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

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

TLS Version 1.2 Protocol Detection (Info)

Host: 192.168.29.200
Plugin ID: 136318
Risk Factor: None
CVE: N/A
Description: The remote service accepts connections encrypted using TLS 1.2.

TLS Version 1.2 Protocol Detection (Info)

Host: 192.168.29.200
Plugin ID: 136318
Risk Factor: None
CVE: N/A
Description: The remote service accepts connections encrypted using TLS 1.2.

TLS Version 1.3 Protocol Detection (Info)

Host: 192.168.29.200
Plugin ID: 138330
Risk Factor: None
CVE: N/A
Description: The remote service accepts connections encrypted using TLS 1.3.

SSL Cipher Suites Supported (Info)

Host: 192.168.29.200

Plugin ID: 21643

Risk Factor: None

CVE: N/A

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

OS Identification (Info)

Host: 192.168.29.200

Plugin ID: 11936

Risk Factor: None

CVE: N/A

Description: 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.

SSL Certificate 'commonName' Mismatch (Info)

Host: 192.168.29.200

Plugin ID: 45410

Risk Factor: None

CVE: N/A

Description: The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

SSL Self-Signed Certificate (Medium)

Host: 192.168.29.200

Plugin ID: 57582

Risk Factor: Medium

CVE: N/A

Description: The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

SSL Certificate Cannot Be Trusted (Medium)

Host: 192.168.29.200

Plugin ID: 51192

Risk Factor: Medium

CVE: N/A

Description: 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.

SSL Certificate Cannot Be Trusted (Medium)

Host: 192.168.29.200
Plugin ID: 51192
Risk Factor: Medium
CVE: N/A
Description: 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.

OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) (Info)

Host: 192.168.29.200

Plugin ID: 97993

Risk Factor: None

CVE: N/A

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