Scaning-20April

Report generated by Tenable Nessus™ Tue, 22 Apr 2025 15:40:12 Pakistan Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Vulnerabilities by Plugin

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.0037

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

44.228.249.3 (icmp/0)

```
The difference between the local and remote clocks is -1 seconds.
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

44.228.249.3 (udp/0)

```
For your information, here is the traceroute from 192.168.18.28 to 44.228.249.3 :
192.168.18.28
192.168.18.1
202.163.124.29
10.15.225.49
192.168.200.97
192.168.4.13
192.168.69.94
?
154.54.60.174
154.54.47.145
?
154.54.169.197
154.54.7.129
154.54.166.73
154.54.165.213
154.54.45.166
154.54.44.141
154.54.43.14
?
44.228.249.3

Hop Count: 22
```

11153 (1) - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

44.228.249.3 (tcp/80/www)

```
A web server seems to be running on this port.
```

11219 (1) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

44.228.249.3 (tcp/80/www)

```
Port 80/tcp was found to be open
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/03/31

Plugin Output

44.228.249.3 (tcp/0)

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

44.228.249.3 (tcp/0)

```
44.228.249.3 resolves as ec2-44-228-249-3.us-west-2.compute.amazonaws.com.
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

44.228.249.3 (tcp/0)

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202504202009
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
```

```
Scan name : Scaning-20April
Scan policy used : Advanced Scan
Scanner IP : 192.168.18.28
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 50
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/4/22 15:12 Pakistan Standard Time (UTC +05:00)
Scan duration : 1659 sec
Scan for malware : no
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

44.228.249.3 (tcp/0)

34277 (1) - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.

If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. However, this is assuming there are no intermediate devices between the scanner and the target. Firewalls often block ICMP, which will prevent responses that identify closed ports. The scanning primarily relies on the absence of a response to identify open ports and in complex environments with many intermediate devices, the detection can often be unreliable.

UDP scanning takes a long time to complete. The scanner must limit the number of concurrent probes because ICMP is often rate limited. Also, since open ports do not respond, the scanner must wait for a timeout period to be reasonably sure that no response will be received.

Given the typical environments being scanned today, the results of this plugin should be thoroughly vetted and be used as weak signals for further investigation. It is likely that a large number of assets will be detected if there are intermediate devices between the scanner and the targets. Consider using the netstat or SNMP port enumeration options instead if possible.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

44.228.249.3 (udp/0)

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

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.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/04/15

Plugin Output

44.228.249.3 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel -> Linux Kernel
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

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).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

44.228.249.3 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 65
```

209654 (1) - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

44.228.249.3 (tcp/0)

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 14.04 Linux Kernel 3.13
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
   P1:B10113:F0x12:W62727:O0204ffff:M1412:
   P2:B10113:F0x12:W62643:O0204ffff0402080affffffff4445414401030307:M1412:
   P3:B00000:F0x00:W0:O0:M0
   P4:191004_7_p=80R
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations