Ubuntu – 192.168.217.131

Report generated by Tenable Nessus™ Thu, 10 Oct 2024 19:53:59 Egypt Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.217.131

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	1	55

Host Information

IP:	192.168.217.131
MAC Address:	00:0C:29:09:9C:D7
OS:	Linux Kernel 5.4.0-196-generic on Ubuntu 20.04

Vulnerabilities

200807 - urllib3 Python Library < 1.26.19, < 2.2.2 (CVE-2024-37891)

Synopsis

A Python library installed on the remote host is affected by a vulnerability.

Description

urllib3 is a user-friendly HTTP client library for Python. When using urllib3's proxy support with 'ProxyManager', the 'Proxy-Authorization' header is only sent to the configured proxy, as expected. However, when sending HTTP requests without using urllib3's proxy support, it's possible to accidentally configure the 'Proxy-Authorization' header even though it won't have any effect as the request is not using a forwarding proxy or a tunneling proxy. In those cases, urllib3 doesn't treat the 'Proxy-Authorization' HTTP header as one carrying authentication material and thus doesn't strip the header on cross-origin redirects.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?7b44847c

Solution

Upgrade to urllib3 version 1.26.19, 2.2.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

4.4 (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

3.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0004

CVSS v2.0 Base Score

4.6 (CVSS2#AV:N/AC:H/Au:M/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2024-37891
XREF	IAVA:2024-A-0363

Plugin Information

Published: 2024/06/21, Modified: 2024/10/07

Plugin Output

tcp/0

```
Installed version : 1.25.8
Fixed version     : 1.26.19
```

10114 - 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

4.2

EPSS Score

0.8808

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

icmp/0

```
The remote clock is synchronized with the local clock.
```

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version      : None
Vendor       : VMware, Inc.
Release Date : 11/12/2020
Secure boot  : disabled
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without 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 any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Local checks have been enabled.
```

45590 - 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: 2024/09/03

Plugin Output

tcp/0

```
Following application CPE's matched on the remote system :

  cpe:/a:exiv2:libexiv2:0.25
  cpe:/a:exiv2:libexiv2:0.27.2
  cpe:/a:gnome:gnome-shell:3.36.9 -> GNOME gnome-shell -
  cpe:/a:gnupg:libgcrypt:1.8.5 -> GnuPG Libgcrypt
  cpe:/a:haxx:libcurl:7.68.0 -> Haxx libcurl
  cpe:/a:openbsd:openssh:8.2 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:8.2p1 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.0.1d -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.1.1f -> OpenSSL Project OpenSSL
  cpe:/a:tukaani:xz:5.2.4 -> Tukaani XZ
  cpe:/a:vim:vim:8.1 -> Vim
  cpe:/a:vmware:open_vm_tools:11.3.0 -> VMware Open VM Tools
  x-cpe:/a:libndp:libndp:1.7
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2024/09/03

Plugin Output

tcp/0

```
Hostname : osboxes
  osboxes (hostname command)
```

54615 - 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: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2024/02/05

Plugin Output

tcp/0

```
The following IPv4 addresses are set on the remote host :

 - 127.0.0.1 (on interface lo)
 - 192.168.217.131 (on interface ens33)
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2022/02/23

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :

 - ::1 (on interface lo)
 - fe80::4667:1a40:bad5:bd1c (on interface ens33)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

```
The following MAC address exists on the remote host :

  - 00:0c:29:09:9c:d7 (interface ens33)
```

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2023/11/17

Plugin Output

tcp/0

```
ens33:
  MAC : 00:0c:29:09:9c:d7
  IPv4:
    - Address : 192.168.217.131
        Netmask : 255.255.255.0
        Broadcast : 192.168.217.255
  IPv6:
    - Address : fe80::4667:1a40:bad5:bd1c
        Prefixlen : 64
        Scope : link
lo:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
        Scope : host
```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:
  ens33:
    ipv4_gateways:
      192.168.217.2:
        subnets:
         - 0.0.0.0/0
Interface Routes:
  ens33:
    ipv4_subnets:
     - 169.254.0.0/16
     - 192.168.217.0/24
    ipv6_subnets:
     - fe80::/64
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:0C:29:09:9C:D7 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:09:9C:D7
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2024/09/24

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ ens33
  + IPv4
    - Address       : 192.168.217.131
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::4667:1a40:bad5:bd1c
      Assign Method : static
```

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

https://gnupg.org/download/index.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2024/09/26

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.2.5
  Version : 1.8.5

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.8.5
```

200214 - Libndp Installed (Linux / Unix)

Synopsis

Libndp is installed on the remote Linux / Unix host.

Description

Libndp is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://github.com/jpirko/libndp

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2024/09/26

Plugin Output

tcp/0

```
Path          : libndp0 1.7-0ubuntu1.1 (via package manager)
Version       : 1.7
Managed by OS : True
```

157358 - Linux Mounted Devices

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.

/bin/df -h /bin/lsblk /bin/mount -l

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           389M  1.7M  388M   1% /run
/dev/sda1       217G  7.8G  198G   4% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/loop0      128K  128K     0 100% /snap/bare/5
/dev/loop3       62M   62M     0 100% /snap/core20/1081
/dev/loop1       56M   56M     0 100% /snap/core18/2128
/dev/loop5       75M   75M     0 100% /snap/core22/1621
/dev/loop2       56M   56M     0 100% /snap/core18/2846
/dev/loop4       64M   64M     0 100% /snap/core20/2379
/dev/loop7      219M  219M     0 100% /snap/gnome-3-34-1804/93
/dev/loop6      350M  350M     0 100% /snap/gnome-3-38-2004/143
/dev/loop9      768K  768K     0 100% /snap/gnome-characters/726
/dev/loop8      242M  242M     0 100% /snap/gnome-3-38-2004/70
/dev/loop11     640K  640K     0 100% /snap/gnome-characters/797
/dev/loop10     896K  896K     0 100% /snap/gnome-logs/123
/dev/loop12     506M  506M     0 100% /snap/gnome-42-2204/176
/dev/loop15     219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop13     2.3M  2.3M     0 100% /snap/gnome-calculator/955
/dev/loop14     1.7M  1.7M     0 100% /snap/gnome-system-monitor/186
/dev/loop16     2.5M  2.5M     0 100% /snap/gnome-system-monitor/163
```

```
/dev/loop17      39M   39M     0 100% /snap/snapd/21759
/dev/loop18      92M   92M     0 100% /snap/gtk-common-themes/1535
/dev/loop19      66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop20     640K  640K     0 100% /snap/gnome-logs/106
/dev/loop21     2.5M  2.5M     0 100% /snap/gnome-calculator/884
/dev/sda3       265G   22M  252G   1% /home
tmpfs           389M   40K  389M   1% /run/user/1000


$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
loop0    7:0    0     4K  1 loop /snap/bare/5
loop1    7:1    0  55.4M  1 loop /snap/core18/2128
loop2    7:2    0  55.4M  1 loop /snap/core18/2846
loop3    7:3    0  61.8M  1 loop /snap/core20/1081
loop4    7:4     [...]
```

193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

```
Via date: EDT -0400
Via timedatectl: Time zone: America/New_York (EDT, -0400)
Via /etc/timezone: America/New_York
Via /etc/localtime: EST5EDT,M3.2.0,M11.1.0
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2024/03/13

Plugin Output

tcp/0

```
-----------[ User Accounts ]-----------

User         : osboxes
Home folder  : /home/osboxes
Start script : /bin/bash
Groups       : osboxes
               lpadmin
               cdrom
               sambashare
               sudo
               plugdev
               dip
               adm

----------[ System Accounts ]----------

User         : root
Home folder  : /root
Start script : /bin/bash
Groups       : root

User         : daemon
Home folder  : /usr/sbin
Start script : /usr/sbin/nologin
Groups       : daemon

User         : bin
Home folder  : /bin
Start script : /usr/sbin/nologin
```

```
Groups       : bin

User         : sys
Home folder  : /dev
Start script : /usr/sbin/nologin
Groups       : sys

User         : sync
Home folder  : /bin
Start script : /bin/sync
Groups       : nogroup

User         : games
Home folder  : /usr/games
Start script : /usr/sbin/nologin
Groups       : games

User         : man
Home folder  : /var/cache/man
Start script : /usr/sbin/nologin
Groups       : man

User         : lp
Home folder  : /var/spool/lpd
Start script : /usr/sbin/nologin
Groups       : lp

User         : mail
Home folder  : /var/mail
Start script : /usr/sbin/nologin
Groups       : mail

User         : news
Home folder  : /var/spool/news
Start script : /usr/sbin/nologin
Groups       : news

User         : uucp
Home folder  : /var/spool/uucp
Start script : /usr/sbin/nologin
Groups       : uucp

User         : proxy
Home folder  : /bin
Start script : /usr/sbin/nologin
Groups       : proxy

User         : www-data
Home folder  : /var/www
Start script : /usr/sbin/nologin
Groups       : www-data

User         : backup
Home folder  : /var/backups
Start script : /usr/sbin/nologin
Groups       : backup

User         : list
Home folder  : /var/list
Start script : /usr/sbin/nologin
Groups       : list

User         : irc
Home folder  : /var/run/ircd
Start script : /usr/sbin/nologin
Groups       : irc

User         : gnats
Home folder  : /var/lib/gnats
Start script : /usr/sbin/nologin
```

```
Groups        : gnats

User          : nobody
Ho [...]
```

19506 - 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: 2024/10/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202410081533
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Ubuntu - 192.168.217.131
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.217.1
Port scanner(s) : netstat
Port range : default
Ping RTT : 101.016 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'osboxes' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 50
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/10/10 19:50 Egypt Standard Time
Scan duration : 186 sec
Scan for malware : no
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/07/24

Plugin Output

udp/5353/mdns

```
Port 5353/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/07/24

Plugin Output

udp/37268

```
Port 37268/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/07/24

Plugin Output

udp/39710

```
Port 39710/udp was found to be open
```

11936 - 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: 2024/10/01

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 5.4.0-196-generic on Ubuntu 20.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 5.4.0-196-generic on Ubuntu 20.04
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2024/09/03

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :
Linux osboxes 5.4.0-196-generic #216-Ubuntu SMP Thu Aug 29 13:26:53 UTC 2024 x86_64 x86_64 x86_64
 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
bullseye/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 13.411335 seconds
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.

Account  : osboxes
Protocol : SSH
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/09/24

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.2p1
Banner  : SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2024/10/07

Plugin Output

tcp/0

```
Nessus detected 5 installs of OpenSSL:

  Path               : /usr/bin/openssl
  Version            : 1.1.1f
  Associated Package : openssl 1.1.1f-1ubuntu2.23
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Version            : 1.1.1f
  Associated Package : libssl1.1

  Path               : /usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Version            : 1.1.1f
  Associated Package : libssl1.1

  Path               : /usr/lib/x86_64-linux-gnu/libssl.so.1.0.0
  Version            : 1.0.1d
```

```
  Associated Package : libssl1.0.0

  Path               : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.0.0
  Version            : 1.0.0
  Associated Package : libssl1.0.0

We are unable to retrieve version info from the following list of OpenSSL files. However, these
 installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/lib4758cca.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libchil.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libatalla.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libsureware.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcswift.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libaep.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgost.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libnuron.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libpadlock.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libubsec.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgmp.so
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

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.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/09/26

Plugin Output

tcp/0

```
. You need to take the following action :

[ urllib3 Python Library < 1.26.19, < 2.2.2 (CVE-2024-37891) (200807) ]

+ Action to take : Upgrade to urllib3 version 1.26.19, 2.2.2  or later.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  kex-strict-s-v00@openssh.com

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
```

```
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

102094 - SSH Commands Require Privilege Escalation

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0507

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

tcp/0

```
Login account : osboxes
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
  Escalation method  : (none)
  Plugins :
  - Plugin Filename : bios_get_info_ssh.nasl
    Plugin ID       : 34098
    Plugin Name     : BIOS Info (SSH)
    - Command  : "LC_ALL=C dmidecode"
      Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
      Error    : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
 Permission denied"
    - Command  : "LC_ALL=C /usr/sbin/dmidecode"
      Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
      Error    : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
 Permission denied"
```

```
 - Plugin Filename : enumerate_aws_ami_nix.nasl
   Plugin ID       : 90191
   Plugin Name     : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
   - Command  : "/usr/sbin/dmidecode -s system-version 2>&1"
     Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
Permission denied"
     Error    : ""
 - Plugin Filename : enumerate_oci_nix.nasl
   Plugin ID       : 154138
   Plugin Name     : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
   - Command  : "LC_ALL=C dmidecode -s chassis-asset-tag 2>&1"
     Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
Permission denied"
     Error    : ""
   - Command  : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
     Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
Permission denied"
     Error    : ""
 - Plugin Filename : host_tag_nix.nbin
   Plugin ID       : 87414
   Plugin Name     : Host Tagging (Linux)
   - Command  : "sh -c \"echo 1e7fed19f05d4b2c8860482ddbd046ba > /etc/tenable_tag && echo OK\""
     Response : null
     Error    : "sh: 1: cannot create /etc/tenable_tag: Permission denied"
 - Plugin Filename : linux_kernel_speculative_execution_detect.nbin
   Plugin ID       : 125216
   Plugin  [...]
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

90707 - SSH SCP Protocol Detection

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

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 as the 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11
SSH supported authentication : publickey,password
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22869 - Software Enumeration (SSH)

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2022/09/06

Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Debian Linux system :

  ii   accountsservice  0.6.55-0ubuntu12~20.04.7  amd64  query and manipulate user account
 information
  ii   acl  2.2.53-6  amd64  access control list - utilities
  ii   acpi-support  0.143  amd64  scripts for handling many ACPI events
  ii   acpid  1:2.0.32-1ubuntu1  amd64  Advanced Configuration and Power Interface event daemon
  ii   adduser  3.118ubuntu2  all  add and remove users and groups
  ii   adwaita-icon-theme  3.36.1-2ubuntu0.20.04.2  all  default icon theme of GNOME (small subset)
  ii   aisleriot  1:3.22.9-1  amd64  GNOME solitaire card game collection
  ii   alsa-base  1.0.25+dfsg-0ubuntu5  all  ALSA driver configuration files
  ii   alsa-topology-conf  1.2.2-1  all  ALSA topology configuration files
  ii   alsa-ucm-conf  1.2.2-1ubuntu0.13  all  ALSA Use Case Manager configuration files
  ii   alsa-utils  1.2.2-1ubuntu2.1  amd64  Utilities for configuring and using ALSA
  ii   amd64-microcode  3.20191218.1ubuntu1.2  amd64  Processor microcode firmware for AMD CPUs
  ii   anacron  2.3-29  amd64  cron-like program that doesn't go by time
  ii   apg  2.2.3.dfsg.1-5  amd64  Automated Password Generator - Standalone version
  ii   app-install-data-partner  19.04  all  Application Installer (data files for partner
 applications/repositories)
  ii   apparmor  2.13.3-7ubuntu5.4  amd64  user-space parser utility for AppArmor
  ii   apport  2.20.11-0ubuntu27.27  all  automatically generate crash reports for debugging
  ii   apport-gtk  2.20.11-0ubuntu27.27  all  GTK+ frontend for the apport crash report system
```

```
  ii   apport-symptoms  0.23  all  symptom scripts for apport
  ii   appstream  0.12.10-2  amd64  Software component metadata management
  ii   apt  2.0.10  amd64  commandline package manager
  ii   apt-config-icons  0.12.10-2  all  APT configuration snippet to enable icon downloads
  ii   apt-config-icons-hidpi  0.12.10-2  all  APT configuration snippet to enable HiDPI icon
downloads
  ii   apt-utils  2.0.10  amd64  package m [...]
```

25220 - 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

tcp/0

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host, however this credential
did not have sufficient privileges for all planned checks :

User:       'osboxes'
Port:       22
Proto:      SSH
Method:     password


See the output of the following plugin for details :

  Plugin ID   : 102094
  Plugin Name : SSH Commands Require Privilege Escalation
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :

User:       'osboxes'
Port:       22
Proto:      SSH
Method:     password
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot   system boot  5.4.0-196-generi Thu Oct 10 12:35   still running

wtmp begins Thu Oct 10 12:35:26 2024
```

10287 - 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

udp/0

```
For your information, here is the traceroute from 192.168.217.1 to 192.168.217.131 :
192.168.217.1
192.168.217.131

Hop Count: 1
```

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma

- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://xz.tukaani.org/xz-utils/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2024/09/26

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

  Path               : /usr/bin/xz
  Version            : 5.2.4
  Associated Package : xz-utils 5.2.4-1ubuntu1.1
  Confidence         : High
```

```
   Managed by OS      : True
   Version Source     : Package

   Path               : /lib/x86_64-linux-gnu/liblzma.so.5.2.4
   Version            : 5.2.4
   Associated Package : liblzma5 5.2.4-1ubuntu1.1
   Confidence         : High
   Managed by OS      : True
   Version Source     : Package
```

198218 - Ubuntu Pro Subscription Detection

Synopsis

The remote Ubuntu host has an active Ubuntu Pro subscription.

Description

The remote Ubuntu host has an active Ubuntu Pro subscription.

See Also

https://documentation.ubuntu.com/pro/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/31, Modified: 2024/07/05

Plugin Output

tcp/0

```
This machine is NOT attached to an Ubuntu Pro subscription. However, it may have previously been
 attached.

The following details were gathered from /var/lib/ubuntu-advantage/status.json:

Binary Path                  : /var/lib/ubuntu-advantage
Binary Version               : 34~18.04
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.4  0.2 102792 11836 ?        Ss   12:35   0:04 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    12:35   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   12:35   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   12:35   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   12:35   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   12:35   0:00 [mm_percpu_wq]
root           9  0.0  0.0      0     0 ?        S    12:35   0:00 [ksoftirqd/0]
root          10  0.0  0.0      0     0 ?        I    12:35   0:00 [rcu_sched]
root          11  0.0  0.0      0     0 ?        S    12:35   0:00 [migration/0]
root          12  0.0  0.0      0     0 ?        S    12:35   0:00 [idle_inject/0]
root          14  0.0  0.0      0     0 ?        S    12:35   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    12:35   0:00 [cpuhp/1]
root          16  0.0  0.0      0     0 ?        S    12:35   0:00 [idle_inject/1]
root          17  0.0  0.0      0     0 ?        S    12:35   0:00 [migration/1]
root          18  0.0  0.0      0     0 ?        S    12:35   0:00 [ksoftirqd/1]
root          20  0.0  0.0      0     0 ?        I<   12:35   0:00 [kworker/1:0H-kblockd]
root          21  0.0  0.0      0     0 ?        S    12:35   0:00 [kdevtmpfs]
root          22  0.0  0.0      0     0 ?        I<   12:35   0:00 [netns]
root          23  0.0  0.0      0     0 ?        S    12:35   0:00 [rcu_tasks_kthre]
root          24  0.0  0.0      0     0 ?        S    12:35   0:00 [kauditd]
root          25  0.0  0.0      0     0 ?        I    12:35   0:00 [kworker/0:2-events]
root          26  0.0  0.0      0     0 ?        S    12:35   0:00 [khungtaskd]
root          27  0.0  0.0      0     0 ?        S    12:35   0:00 [oom_reaper]
root          28  0.0  0.0      0     0 ?        I<   12:35   0:00 [writeback]
root          29  0.0  0.0  [...]
```

152743 - Unix Software Discovery Commands Not Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.

Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

* Inadequate scan user permissions,

* Failed privilege escalation,

* Intermittent network disruption, or

* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Failures in commands used to assess Unix software:

  strings -v                  :
    bash: strings: command not found


Account  : osboxes
Protocol : SSH
```

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

https://kb.vmware.com/s/article/340

http://www.nessus.org/u?c0628155

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2024/09/26

Plugin Output

tcp/0

```
Path    : /usr/bin/vmtoolsd
Version : 11.3.0
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2024/09/26

Plugin Output

tcp/0

```
Path    : /usr/bin/vim.tiny
Version : 8.1
```

198234 - gnome-shell Installed (Linux / UNIX)

Synopsis

gnome-shell is installed on the remote Linux / UNIX host.

Description

gnome-shell is installed on the remote Linux / UNIX host.

See Also

https://gitlab.gnome.org/GNOME/gnome-shell/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/31, Modified: 2024/09/26

Plugin Output

tcp/0

```
Path    : /usr/bin/gnome-shell
Version : 3.36.9
Managed : 1
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2024/10/07

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.6.0
  Version            : 7.68.0
  Associated Package : libcurl4 7.68.0-1ubuntu2.24
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.6.0
  Version            : 7.68.0
  Associated Package : libcurl3-gnutls 7.68.0-1ubuntu2.24
  Managed by OS      : True
```

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2024/09/26

Plugin Output

tcp/0

```
Nessus detected 2 installs of libexiv2:

  Path               : /usr/lib/x86_64-linux-gnu/libexiv2.so.14.0.0
  Version            : 0.25
  Associated Package : libexiv2-14 0.25-3.1ubuntu0.18.04.11
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libexiv2.so.0.27.2
  Version            : 0.27.2
  Associated Package : libexiv2-27 0.27.2-8ubuntu2.7
  Managed by OS      : True
```

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

  - mDNS hostname       : osboxes.local.
```