METASPLOITABLE2:

VULNERABILITY ASSESSMENT

REPORT - dopo scansione Nessus

Scan Information

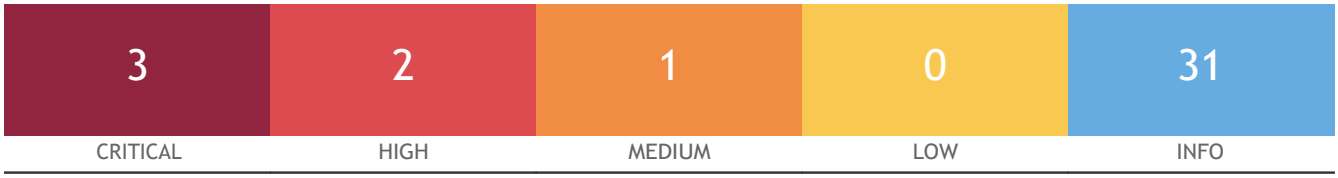
Start time: Mon May 8 20:12:45 2023
End time: Mon May 8 20:27:35 2023

Host Information

Netbios Name: **METASPLOITABLE**

IP:192.168.50.101
MAC Address: 08:00:27:A0:26:54
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

192.168.50.101



Vulnerabilities

Total: 37

9.8 - 9.0 134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Sinossi
C'è un connettore A JP vulnerabile in ascolto sull'host remoto.

Descrizione
È stata rilevata una vulnerabilità di lettura/inclusione di file in un connettore JP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

http://www.nessus.org/u?8ebe6246 http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e https://access.redhat.com/security/cve/CVE-2020-1745 https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234 http://www.nessus.org/u?dd772531

Soluzione
Aggiorna la configurazione A JP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

Fattore di rischio alto

CVSS v3.0 Base Score
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score 9.0

CVSS v2.0 Base Score
7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2020-1745
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021

Plugin Information
Published: 2020/03/24, Modified: 2023/05/03

Plugin Output tcp/8009/ajp13

```
0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F  ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00  asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C  .localhost.
                                                          ...........
                                                          l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06  ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41  ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00  ccept-Language..
0x0060:  0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00  .en-US,en;q=0.5.
0x0070:  A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45  ....0...Accept-E
0x0080:  6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20  ncoding...gzip,
0x0090:  64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D  deflate, sdch...
0x00A0:  43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09  Cache-Control...
0x00B0:  6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F  max-age=0.
                                                          ...........
                                                          Mo
0x00C0:  7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D  zilla...Upgrade-
0x00D0:  49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74  Insecure-Request
0x00E0:  73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68  s...1.
                                                          ..........
                                                          text/h
0x00F0:  74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73  tml.....localhos
0x0100:  74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C  t...!javax.servl
0x0110:  65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65  et.include.reque
0x0120:  73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61  st_uri...1.
                                                          ..........
                                                          ja
0x0130:  76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C  vax.servlet.incl
0x0140:  75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10  ude.path_info...
0x0150:  2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C  /WEB-INF/web.xml
0x0160:  00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65  ..."javax.servle
0x0170:  74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65  t.include.servle
0x0180:  74 5F 70 61 74 68 00 00 00 00 FF                 t_path.....
```

10.0 - 33850 Unix Operating System Unsupported Version Detection

Sinossi
Il sistema operativo in esecuzione sull'host remoto non è più supportato.

Descrizione
In base al numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.
La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione
Aggiorna a una versione del sistema operativo Unix attualmente supportata.

Fattore di rischio critico

CVSS v3.0 Base Score
10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001-A-0502
XREF	IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2023/04/18

Plugin Output tcp/0

10.1 10.0* 5.9 11356 NFS Exported Share Information Disclosure

Sinossi
È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione
Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

Soluzione
Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Fattore di rischio critico

VPR Score 5.9

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0170

CVE CVE-1999-0211
CVE CVE-1999-0554
Exploitable With Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2018/09/17

Plugin Output udp/2049/rpc-nfs

7.5 - 42256 NFS Shares World Readable

Sinossi
Il server NFS remoto esporta condivisioni leggibili da tutti.

Descrizione
Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (basato su nome host, IP o intervallo IP).

Guarda anche:http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Soluzione
Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

Fattore di rischio medio

CVSS v3.0 Base Score
7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/26, Modified: 2020/05/05

Plugin Output tcp/2049/rpc-nfs

7.5 6.7 90509 Samba Badlock Vulnerability

Sinossi

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

Descrizione

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nell'autorità di sicurezza locale

(Domain Policy) (LSAD) a causa di una negoziazione errata del livello di autenticazione sui canali RPC (Remote Procedure Call). Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati sensibili sulla sicurezza nel database di Active Directory (AD) o la disabilitazione di servizi critici.

Guarda anche: http://badlock.org https://www.samba.org/samba/security/CVE-2016-2118.html

Soluzione

Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Fattore di rischio medio

CVSS v3.0 Base Score
7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

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

VPR Score 6.7

CVSS v2.0 Base Score
6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

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

References

BID	86002
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output tcp/445/cifs

5.3 - 12217 DNS Server Cache Snooping Remote Information Disclosure N/A - 10223 RPC portmapper Service Detection

Sinossi

Il server DNS remoto è vulnerabile agli attacchi di snooping della cache.

Descrizione

Il server DNS remoto risponde alle query per i domini di terze parti che non hanno il bit di ricorsione impostato.

Ciò potrebbe consentire a un utente malintenzionato remoto di determinare quali domini sono stati risolti di recente tramite questo server dei nomi e quindi quali host sono stati visitati di recente.

Ad esempio, se un utente malintenzionato fosse interessato a sapere se la tua azienda utilizza i servizi online di un particolare istituto finanziario, sarebbe in grado di utilizzare questo attacco per costruire un modello statistico relativo all'utilizzo aziendale di tale istituto finanziario. Naturalmente, l'attacco può essere utilizzato anche per trovare partner B2B, modelli di navigazione Web, server di posta esterni e altro ancora.

Nota: se si tratta di un server DNS interno non accessibile alle reti esterne, gli attacchi sarebbero limitati alla rete interna. Ciò può includere dipendenti, consulenti e potenziali utenti su una rete ospite o connessione Wi-Fi, se supportata.

Guarda anche: http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Soluzione

Contattare il fornitore del software DNS per una correzione.

Fattore di rischio medio

CVSS v3.0 Base Score
5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/04/27, Modified: 2020/04/07

Plugin Output udp/53/dns

N/A - 21186 AJP Connector Detection

N/A - 18261 Apache Banner Linux Distribution Disclosure N/A - 45590 Common Platform Enumeration (CPE)

N/A - 11002 DNS Server Detection

N/A - 72779 DNS Server Version Detection

N/A - 35371 DNS Server hostname.bind Map Hostname Disclosure N/A - 54615 Device Type

N/A - 35716 Ethernet Card Manufacturer Detection N/A - 86420 Ethernet MAC Addresses

N/A - 10397 Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

N/A - 10785 Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version

INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	87872	Unbound DNS Resolver Remote Version Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

- indicates the v3.0 score was not available; the v2.0 score is shown
-

Plugin ID,CVE,CVSS v2.0 Base Score,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin Output,STIG Severity,CVSS v3.0 Base Score,CVSS v2.0 Temporal Score,CVSS v3.0 Temporal Score,VPR Score,Risk Factor,BID,XREF,MSKB,Plugin Publication Date,Plugin Modification Date,Metasploit,Core Impact,CANVAS
"10150","","","None","192.168.50.101","udp","137","Windows NetBIOS / SMB Remote Host Information Disclosure","It was possible to obtain the network name of the remote host.","The remote host is listening on UDP port 137 or TCP port 445, 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.","n/a","","The following 7 NetBIOS names have been gathered :

METASPLOITABLE = Computer name
METASPLOITABLE = Messenger Service
METASPLOITABLE = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Workgroup / Domain name
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.","","","","","","","None","","","","1999/10/12","2021/02/10","","","","
"10223","CVE-1999-0632","0.0","None","192.168.50.101","udp","111","RPC portmapper Service Detection","An ONC RPC portmapper is running on the remote host.","The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP

request.","n/a","","","","0.0","","","","None","","","","1999/08/19","2019/10/04","","","",""
"10287","","","None","192.168.50.101","udp","0","Traceroute Information","It was possible to obtain traceroute information.","Makes a traceroute to the remote host.","n/a","","For your information, here is the traceroute from 192.168.50.100 to 192.168.50.101 : 192.168.50.100
?

Hop Count: 1
","","","","","","","","None","","","","1999/11/27","2023/05/03","","","",""
"10397","","","None","192.168.50.101","tcp","445","Microsoft Windows SMB LanMan Pipe Server Listing Disclosure","It is possible to obtain network information.","It was possible to obtain the browse list of the remote Windows system
by sending a request to the LANMAN pipe. The browse list is the list
of the nearest Windows systems of the remote host.","n/a","","
Here is the browse list of the remote host :

METASPLOITABLE (os : 0.0)
","","","","","","","","None","","","","2000/05/09","2022/02/01","","","",""
"10437","","","None","192.168.50.101","tcp","2049","NFS Share Export List","The remote NFS server exports a list of shares.","This plugin retrieves the list of NFS exported shares.","Ensure each share is intended to be
exported.","http://www.tldp.org/HOWTO/NFS-HOWTO/security.html","
Here is the export list of 192.168.50.101 :

  / *
","","","","","","","","None","","","","2000/06/07","2019/10/04","","","",""
"10785","","","None","192.168.50.101","tcp","445","Microsoft Windows SMB NativeLanManager Remote System Information Disclosure","It was possible to obtain information about the remote operating
system.","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.","n/a","","The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
","","","","","","","","None","","","","2001/10/17","2021/09/20","","","",""
"11002","","","None","192.168.50.101","tcp","53","DNS Server Detection","A DNS server is listening on the remote host.","The remote service is a Domain Name System (DNS) server, which
provides a mapping between hostnames and IP addresses.","Disable this service if it is not needed or restrict access to
internal hosts only if the service is available
externally.","https://en.wikipedia.org/wiki/Domain_Name_System","","","","","","","None","","","","2003/02/13","2017/05/16","","","",""
"11002","","","None","192.168.50.101","udp","53","DNS Server Detection","A DNS server is listening on the remote host.","The remote service is a Domain Name System (DNS) server, which
provides a mapping between hostnames and IP addresses.","Disable this service if it is not needed or restrict access to
internal hosts only if the service is available
externally.","https://en.wikipedia.org/wiki/Domain_Name_System","","","","","","","None","","","","2003/02/13","2017/05/16","","","",""

"11011","","","None","192.168.50.101","tcp","139","Microsoft Windows SMB Service Detection","A file / print sharing service is listening on the remote host.","The remote service understands the CIFS (Common Internet File System)
or Server Message Block (SMB) protocol, used to provide shared access
to files, printers, etc between nodes on a network.","n/a","","
An SMB server is running on this port.
","","","","","","","None","","","","2002/06/05","2021/02/11","","",""
"11011","","","None","192.168.50.101","tcp","445","Microsoft Windows SMB Service Detection","A file / print sharing service is listening on the remote host.","The remote service understands the CIFS (Common Internet File System)
or Server Message Block (SMB) protocol, used to provide shared access
to files, printers, etc between nodes on a network.","n/a","","
A CIFS server is running on this port.
","","","","","","","None","","","","2002/06/05","2021/02/11","","",""
"11111","","","None","192.168.50.101","tcp","111","RPC Services Enumeration","An ONC RPC service is running on the remote host.","By sending a DUMP request to the portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
","","","","","","","None","","","","2002/08/24","2011/05/24","","",""
"11111","","","None","192.168.50.101","tcp","2049","RPC Services Enumeration","An ONC RPC service is running on the remote host.","By sending a DUMP request to the portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on TCP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
","","","","","","","None","","","","2002/08/24","2011/05/24","","",""
"11111","","","None","192.168.50.101","tcp","33042","RPC Services Enumeration","An ONC RPC service is running on the remote host.","By sending a DUMP request to the portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on TCP port 33042 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
","","","","","","","None","","","","2002/08/24","2011/05/24","","",""
"11111","","","None","192.168.50.101","tcp","48691","RPC Services Enumeration","An ONC RPC service is running on the remote host.","By sending a DUMP request to the portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on TCP port 48691 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
","","","","","","","None","","","","","2002/08/24","2011/05/24","","","",""
"11111","","","None","192.168.50.101","tcp","49988","RPC Services Enumeration","An ONC
RPC service is running on the remote host.","By sending a DUMP request to the
portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on TCP port 49988 :

 - program: 100024 (status), version: 1
","","","","","","","None","","","","","2002/08/24","2011/05/24","","","",""
"11111","","","None","192.168.50.101","udp","111","RPC Services Enumeration","An ONC
RPC service is running on the remote host.","By sending a DUMP request to the
portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2
","","","","","","","None","","","","","2002/08/24","2011/05/24","","","",""
"11111","","","None","192.168.50.101","udp","2049","RPC Services Enumeration","An ONC
RPC service is running on the remote host.","By sending a DUMP request to the
portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on UDP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
","","","","","","","None","","","","","2002/08/24","2011/05/24","","","",""
"11111","","","None","192.168.50.101","udp","36660","RPC Services Enumeration","An ONC
RPC service is running on the remote host.","By sending a DUMP request to the
portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on UDP port 36660 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
","","","","","","","None","","","","","2002/08/24","2011/05/24","","","",""

"11111","","","None","192.168.50.101","udp","52586","RPC Services Enumeration","An ONC RPC service is running on the remote host.","By sending a DUMP request to the portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on UDP port 52586 :

 - program: 100024 (status), version: 1
","","","","","","","None","","","","2002/08/24","2011/05/24","","",""
"11111","","","None","192.168.50.101","udp","57987","RPC Services Enumeration","An ONC RPC service is running on the remote host.","By sending a DUMP request to the portmapper, it was possible to
enumerate the ONC RPC 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.","n/a","","
The following RPC services are available on UDP port 57987 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
","","","","","","","None","","","","2002/08/24","2011/05/24","","",""
"11219","","","None","192.168.50.101","tcp","21","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 21/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","",""
"11219","","","None","192.168.50.101","tcp","22","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 22/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","",""
"11219","","","None","192.168.50.101","tcp","23","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 23/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","",""

"11219","","","None","192.168.50.101","tcp","25","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 25/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","","
"11219","","","None","192.168.50.101","tcp","53","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 53/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","","
"11219","","","None","192.168.50.101","tcp","80","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 80/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","","
"11219","","","None","192.168.50.101","tcp","111","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 111/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","","
"11219","","","None","192.168.50.101","tcp","139","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 139/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","","
"11219","","","None","192.168.50.101","tcp","445","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It

shall be 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.","Protect your target with an IP filter.","","Port 445/tcp was found
to be open","","","","","","","None","","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","512","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 512/tcp was found
to be open","","","","","","","None","","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","513","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 513/tcp was found
to be open","","","","","","","None","","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","514","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 514/tcp was found
to be open","","","","","","","None","","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","1099","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 1099/tcp was
found to be open","","","","","","","None","","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","1524","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 1524/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","2049","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 2049/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","2121","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 2121/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","3306","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 3306/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","3632","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 3632/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","5432","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 5432/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","5900","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 5900/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","6000","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 6000/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","6667","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 6667/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","8009","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 8009/tcp was
found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","",""
"11219","","","None","192.168.50.101","tcp","8180","Nessus SYN scanner","It is possible to
determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It
shall be 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.","Protect your target with an IP filter.","","Port 8180/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","","
"11219","","","None","192.168.50.101","tcp","8787","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be 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.","Protect your target with an IP filter.","","Port 8787/tcp was found to be open","","","","","","","None","","","","2009/02/04","2023/05/03","","","","
"11356","CVE-1999-0170","10.0","Critical","192.168.50.101","udp","2049","NFS Exported Share Information Disclosure","It is possible to access NFS shares on the remote host.","At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage
this to read (and possibly write) files on remote host.","Configure NFS on the remote host so that only authorized hosts can
mount its remote shares.","","
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
    - etc
    - home
    - initrd
    - initrd.img
    - lib
    - lost+found
    - media
    - mnt
    - nohup.out
    - opt
    - proc
    - root
    - sbin
    - srv
    - sys
    - tmp
    - usr
    - var
    - vmlinuz
","","","","","","5.9","Critical","","","","2003/03/12","2018/09/17","true","","","
"11356","CVE-1999-0211","10.0","Critical","192.168.50.101","udp","2049","NFS Exported Share Information Disclosure","It is possible to access NFS shares on the remote host.","At least one of the NFS shares exported by the remote server could be

mounted by the scanning host. An attacker may be able to leverage
this to read (and possibly write) files on remote host.","Configure NFS on the remote
host so that only authorized hosts can
mount its remote shares.","","
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
    - etc
    - home
    - initrd
    - initrd.img
    - lib
    - lost+found
    - media
    - mnt
    - nohup.out
    - opt
    - proc
    - root
    - sbin
    - srv
    - sys
    - tmp
    - usr
    - var
    - vmlinuz
","","","","","","5.9","Critical","","","","2003/03/12","2018/09/17","true","",""
"11356","CVE-1999-0554","10.0","Critical","192.168.50.101","udp","2049","NFS Exported
Share Information Disclosure","It is possible to access NFS shares on the remote
host.","At least one of the NFS shares exported by the remote server could be
mounted by the scanning host. An attacker may be able to leverage
this to read (and possibly write) files on remote host.","Configure NFS on the remote
host so that only authorized hosts can
mount its remote shares.","","
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
    - etc

- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz

","","","","","","5.9","Critical","","","","2003/03/12","2018/09/17","true","","" "11936","","","None","192.168.50.101","tcp","0","OS Identification","It is possible to guess the remote operating system.","Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP,
SNMP, etc.), it is possible to guess the name of the remote operating
system in use. It is also possible sometimes to guess the version of
the operating system.","n/a","","
Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP

The remote host is running Linux Kernel 2.6 on Ubuntu 8.04
(gutsy)","","","","","","","None","","","","2003/12/09","2022/03/09","","","" "12217","","","5.0","Medium","192.168.50.101","udp","53","DNS Server Cache Snooping Remote Information Disclosure","The remote DNS server is vulnerable to cache snooping attacks.","The remote DNS server responds to queries for third-party domains
that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have
recently been resolved via this name server, and therefore which hosts
have been recently visited.

For instance, if an attacker was interested in whether your company
utilizes the online services of a particular financial institution,
they would be able to use this attack to build a statistical model
regarding company usage of that financial institution. Of course, the
attack can also be used to find B2B partners, web-surfing patterns,
external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside
networks, attacks would be limited to the internal network. This
may include employees, consultants and potentially users on
a guest network or WiFi connection if supported.","Contact the vendor of the DNS

software for a fix.","http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf","
Nessus sent a non-recursive query for example.edu
and received 1 answer :

93.184.216.34
","","5.3","","","","","Medium","","","","2004/04/27","2020/04/07","","","","
"18261","","","None","192.168.50.101","tcp","0","Apache Banner Linux Distribution Disclosure","The name of the Linux distribution running on the remote host was found in the banner of the web server.","Nessus was able to extract the banner of the Apache web server and
determine which Linux distribution the remote host is running.","If you do not wish to display this information, edit 'httpd.conf' and
set the directive 'ServerTokens Prod' and restart Apache.","","
The Linux distribution detected was :
 - Ubuntu 8.04 (gutsy)
","","","","","","","None","","","","2005/05/15","2022/03/21","","","","
"19506","","","None","192.168.50.101","tcp","0","Nessus Scan Information","This plugin displays information about the Nessus scan.","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.","n/a","","Information about this scan :

Nessus version : 10.5.1
Nessus build : 20008
Plugin feed version : 202305081407
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Metasploit2
Scan policy used : Basic Network Scan
Scanner IP : 192.168.50.100
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 140.723 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1

Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2023/5/8 20:12 CEST
Scan duration : 883 sec
Scan for malware : no
","","","","","","","None","","","","2005/08/26","2023/04/27","","","",""
"21186","","","None","192.168.50.101","tcp","8009","AJP Connector Detection","There is an AJP connector listening on the remote host.","The remote host is running an AJP (Apache JServ Protocol) connector, a
service by which a standalone web server such as Apache communicates
over TCP with a Java servlet container such as
Tomcat.","n/a","http://tomcat.apache.org/connectors-doc/
http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html","
The connector listing on this port supports the ajp13 protocol.
","","","","","","","None","","","","2006/04/05","2019/11/22","","","",""
"22964","","","None","192.168.50.101","tcp","22","Service Detection","The remote service could be identified.","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.","n/a","","An SSH server is running on this
port.","","","","","","","None","","","","2007/08/19","2023/03/29","","","",""
"22964","","","None","192.168.50.101","tcp","80","Service Detection","The remote service could be identified.","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.","n/a","","A web server is running on this
port.","","","","","","","None","","","","2007/08/19","2023/03/29","","","",""
"25240","","","None","192.168.50.101","tcp","445","Samba Server Detection","An SMB server is running on the remote host.","The remote host is running Samba, a CIFS/SMB server for Linux and
Unix.","n/a","https://www.samba.org/","","","","","","","","None","","","","2007/05/16","2022/10/12","","","",""
"33850","","10.0","Critical","192.168.50.101","tcp","0","Unix Operating System Unsupported Version Detection","The operating system running on the remote host is no longer
supported.","According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product
will be released by the vendor. As a result, it is likely to contain
security vulnerabilities.","Upgrade to a version of the Unix operating system that is currently
supported.","","

Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases

","","10.0","","","","Critical","","IAVA:0001-A-0502;IAVA:0001-A-
0648","","2008/08/08","2023/04/18","","",""
"35371","","","None","192.168.50.101","udp","53","DNS Server hostname.bind Map
Hostname Disclosure","The DNS server discloses the remote host name.","It is possible to
learn the remote host name by querying the remote
DNS server for 'hostname.bind' in the CHAOS domain.","It may be possible to disable this
feature. Consult the vendor's
documentation for more information.","","
The remote host name is :

vpn-gw-prod-004.mil0-tgb.ff.avast.com
","","","","","","","None","","","","2009/01/15","2011/09/14","","",""
"35716","","","None","192.168.50.101","tcp","0","Ethernet Card Manufacturer
Detection","The manufacturer can be identified from the Ethernet OUI.","Each ethernet
MAC address starts with a 24-bit Organizationally
Unique Identifier (OUI). These OUIs are registered by
IEEE.","n/a","https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4","
The following card manufacturers were identified :

08:00:27:A0:26:54 : PCS Systemtechnik GmbH
","","","","","","","None","","","","2009/02/19","2020/05/13","","",""
"42256","","5.0","High","192.168.50.101","tcp","2049","NFS Shares World Readable","The
remote NFS server exports world-readable shares.","The remote NFS server is exporting
one or more shares without
restricting access (based on hostname, IP, or IP range).","Place the appropriate
restrictions on all NFS shares.","http://www.tldp.org/HOWTO/NFS-
HOWTO/security.html","
The following shares have no access restrictions :

  / *
","","7.5","","","","","Medium","","","","2009/10/26","2020/05/05","","",""
"45590","","","None","192.168.50.101","tcp","0","Common Platform Enumeration (CPE)","It
was possible to enumerate CPE names that matched on the remote
system.","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.","n/a","http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe","
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:8.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server
cpe:/a:php:php:5.2.4 -> PHP PHP
cpe:/a:samba:samba:3.0.20 -> Samba Samba
","","","","","","","None","","","","2010/04/21","2023/05/03","","","",""
"53335","","","None","192.168.50.101","tcp","111","RPC portmapper (TCP)","An ONC RPC portmapper is running on the remote host.","The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC
service running on the remote host by sending either multiple lookup
requests or a DUMP
request.","n/a","","","","","","","","None","","","","2011/04/08","2011/08/29","","","",""
"54615","","","None","192.168.50.101","tcp","0","Device Type","It is possible to guess the remote device type.","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).","n/a","","Remote device type : general-purpose
Confidence level : 95
","","","","","","","None","","","","2011/05/23","2022/09/09","","","",""
"66334","","","None","192.168.50.101","tcp","0","Patch Report","The remote host is missing several patches.","The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install
to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin,
it will always run and cannot be disabled.","Install the patches listed below.","","

. You need to take the following action :

[Samba Badlock Vulnerability (90509)]

+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

","","","","","","","None","","","","2013/07/08","2023/05/03","","","",""
"72779","","","None","192.168.50.101","udp","53","DNS Server Version Detection","Nessus was able to obtain version information on the remote DNS
server.","Nessus was able to obtain version information by sending a special TXT
record query to the remote host.

Note that this version is not necessarily accurate and could even be
forged, as some DNS servers send the information based on a
configuration file.","n/a","","
DNS server answer for ""version.bind"" (over UDP) :

unbound 1.13.2
","","","","","","","None","","IAVT:0001-T-0937","","2014/03/03","2020/09/22","","","",""
"86420","","","None","192.168.50.101","tcp","0","Ethernet MAC Addresses","This plugin gathers MAC addresses from various sources and
consolidates them into a list.","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.","n/a","","The following is a consolidated list of detected MAC
addresses:
  - 08:00:27:A0:26:54
","","","","","","","None","","","","2015/10/16","2020/05/13","","","",""
"87872","","","None","192.168.50.101","tcp","53","Unbound DNS Resolver Remote Version
Detection","It was possible to obtain the version number of the remote DNS server.","The
remote host is running the Unbound DNS resolver.

Note that the version detected is not necessarily accurate and could
even be forged, as some DNS servers send the information based on a
configuration file.","n/a","https://nlnetlabs.nl/projects/unbound/about/","
  Version : unbound 1.13.2
","","","","","","","None","","","","2016/01/12","2019/11/22","","","",""
"90509","CVE-2016-2118","6.8","High","192.168.50.101","tcp","445","Samba Badlock
Vulnerability","An SMB server running on the remote host is affected by the Badlock
vulnerability.","The version of Samba, a CIFS/SMB server for Linux and Unix, running on
the remote host is affected by a flaw, known as Badlock, that exists
in the Security Account Manager (SAM) and Local Security
Authority (Domain Policy) (LSAD) protocols due to improper
authentication level negotiation over Remote Procedure Call (RPC)
channels. A man-in-the-middle attacker who is able to able to
intercept the traffic between a client and a server hosting a SAM
database can exploit this flaw to force a downgrade of the
authentication level, which allows the execution of arbitrary Samba
network calls in the context of the intercepted user, such as viewing
or modifying sensitive security data in the Active Directory (AD)
database or disabling critical services.","Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2
or later.","http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html","
Nessus detected that the Samba Badlock patch has not been applied.
","","7.5","5.0","6.5","6.7","Medium","86002","CERT:813296","","2016/04/13","2019/11/20","
","","","
"96982","","","None","192.168.50.101","tcp","445","Server Message Block (SMB) Protocol
Version 1 Enabled (uncredentialed check)","The remote Windows host supports the
SMBv1 protocol.","The remote Windows host supports Server Message Block Protocol
version 1 (SMBv1). Microsoft recommends that users discontinue the use
of SMBv1 due to the lack of security features that were included in
later SMB versions. Additionally, the Shadow Brokers group reportedly
has an exploit that affects SMB; however, it is unknown if the exploit
affects SMBv1 or another version. In response to this, US-CERT
recommends that users disable SMBv1 per SMB best practices to mitigate
these potential issues.","Disable SMBv1 according to the vendor instructions in Microsoft
KB2696547. Additionally, block SMB directly by blocking TCP port 445
on all network boundary devices. For SMB over the NetBIOS API, block
TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary
devices.","https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-
smbv1-smbv2-and-smbv3-in-windows-and
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3","

The remote host supports SMBv1.
","","","","","","","None","","IAVT:0001-T-0710","","2017/02/03","2020/09/22","","","","
"100871","","","None","192.168.50.101","tcp","445","Microsoft Windows SMB Versions Supported (remote check)","It was possible to obtain information about the version of SMB running
on the remote host.","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.","n/a","","
The remote host supports the following versions of SMB :
  SMBv1
","","","","","","","None","","","","2017/06/19","2019/11/22","","","","
"104887","","","None","192.168.50.101","tcp","445","Samba Version","It was possible to obtain the samba version from the remote
operating system.","Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445.
Note that this plugin requires SMB1 to be enabled on the host.","n/a","","
The remote Samba Version is : Samba 3.0.20-
Debian","","","","","","","None","","","","2017/11/30","2019/11/22","","","","
"110723","","","None","192.168.50.101","tcp","0","Target Credential Status by Authentication Protocol - No Credentials Provided","Nessus was able to find common ports used for local checks,
however, no credentials were provided in the scan policy.","Nessus was not able to successfully authenticate directly to 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.","n/a","","SSH was detected on port 22 but no credentials were provided.

SSH local checks were not enabled.

","","","","","","","None","","IAVB:0001-B-0504","","2018/06/27","2023/02/13","","","","
"117886","","","None","192.168.50.101","tcp","0","OS Security Patch Assessment Not Available","OS Security Patch Assessment is not available.","OS Security Patch Assessment is not available on the remote host.
This does not necessarily indicate a problem with the scan.
Credentials may not have been provided, OS security patch 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.","n/a","","
The following issues were reported :

  - Plugin   : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message   :
Credentials were not provided for detected SSH service.
","","","","","","","None","","IAVB:0001-B-0515","","2018/10/02","2021/07/12","","","","
"134862","CVE-2020-1745","7.5","Critical","192.168.50.101","tcp","8009","Apache Tomcat AJP Connector Request Injection (Ghostcat)","There is a vulnerable AJP connector listening on the remote host.","A file read/inclusion vulnerability was found in AJP connector. A
 remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).","Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.","http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70","
Nessus was able to exploit the issue using the following request :

0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F   ....HTTP/1.1.../

```
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060:  0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00    .en-US,en;q=0.5.
0x0070:  A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45    ....0...Accept-E
0x0080:  6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20    ncoding...gzip,
0x0090:  64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D    deflate, sdch...
0x00A0:  43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09    Cache-Control...
0x00B0:  6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F    max-age=0.....Mo
0x00C0:  7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D    zilla...Upgrade-
0x00D0:  49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74    Insecure-Request
0x00E0:  73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68    s...1.....text/h
0x00F0:  74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73    tml.....localhos
0x0100:  74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C    t...!javax.servl
0x0110:  65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65    et.include.reque
0x0120:  73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61    st_uri...1....ja
0x0130:  76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C    vax.servlet.incl
0x0140:  75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10    ude.path_info...
0x0150:  2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C    /WEB-INF/web.xml
0x0160:  00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65    ...""javax.servle
0x0170:  74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65    t.include.servle
0x0180:  74 5F 70 61 74 68 00 00 00 00 FF                   t_path.....
```

This produced the following truncated output (limited to 10 lines) :

```
---------------------------- snip ----------------------------
...<?xml version=""1.0"" encoding=""ISO-8859-1""?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements.  See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the ""License""); you may not use this file except in compliance with
the License.  You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0
[...]

---------------------------- snip ----------------------------
","","9.8","6.5","9.4","9.0","High","","CISA-KNOWN-EXPLOITED:2022/03/17;CEA-ID:CEA-
2020-0021","","2020/03/24","2023/05/03","","",""
"134862","CVE-2020-1938","7.5","Critical","192.168.50.101","tcp","8009","Apache Tomcat
AJP Connector Request Injection (Ghostcat)","There is a vulnerable AJP connector
listening on the remote host.","A file read/inclusion vulnerability was found in AJP
connector. A
 remote, unauthenticated attacker could exploit this vulnerability to
read web application files from a vulnerable server. In instances where
the vulnerable server allows file uploads, an attacker could upload
malicious JavaServer Pages (JSP) code within a variety of file types
```

and gain remote code execution (RCE).","Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.","http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70","
Nessus was able to exploit the issue using the following request :

```
0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060:  0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00    .en-US,en;q=0.5.
0x0070:  A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45    ....0...Accept-E
0x0080:  6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20    ncoding...gzip,
0x0090:  64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D    deflate, sdch...
0x00A0:  43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09    Cache-Control...
0x00B0:  6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F    max-age=0.....Mo
0x00C0:  7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D    zilla...Upgrade-
0x00D0:  49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74    Insecure-Request
0x00E0:  73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68    s...1.....text/h
0x00F0:  74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73    tml.....localhos
0x0100:  74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C    t...!javax.servl
0x0110:  65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65    et.include.reque
0x0120:  73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61    st_uri...1....ja
0x0130:  76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C    vax.servlet.incl
0x0140:  75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10    ude.path_info...
0x0150:  2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C    /WEB-INF/web.xml
0x0160:  00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65    ...""javax.servle
0x0170:  74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65    t.include.servle
0x0180:  74 5F 70 61 74 68 00 00 00 00 FF                   t_path.....
```

This produced the following truncated output (limited to 10 lines) :

```
------------------------------ snip ------------------------------
...<?xml version=""1.0"" encoding=""ISO-8859-1""?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements.  See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the ""License""); you may not use this file except in compliance with
```

the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0
[...]

---------- snip ----------
","","9.8","6.5","9.4","9.0","High","","CISA-KNOWN-EXPLOITED:2022/03/17;CEA-ID:CEA-2020-0021","","2020/03/24","2023/05/03","","",""
"135860","","","None","192.168.50.101","tcp","445","WMI Not Available","WMI queries could not be made against the remote host.","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.","n/a","https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page","Can't connect to the 'root\CIMV2' WMI
namespace.","","","","","","","None","","","","2020/04/21","2023/05/03","","",""