

Scansione tramite Nessus e risoluzione vulnerabilità

Ai fini della consegna per il progetto per il Modulo 3 è stata svolta una scansione tramite Nessus sulla macchina target Metasploitable 2 (192.168.32.101), questa ha evidenziato diverse vulnerabilità critiche. Lo scopo dell'esercitazione prevedeva di correggerne 4 o 5.

Filter

Search Vulnerabilities

64 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
<div><div></div><div>CRITICAL</div></div>	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	10.0		Unix Operating System Unsupported Version Detection	General	1	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghos...	Web Servers	1	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	9.8		Bind Shell Backdoor Detection	Backdoors	1	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>MIXED</div></div>	<div><div></div></div> DNS (Multiple Issues)	DNS	4	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>CRITICAL</div></div>	<div><div></div></div> SSL (Multiple Issues)	Gain a shell remotely	3	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>HIGH</div></div>	7.5		NFS Shares World Readable	RPC	1	<div><div></div></div>	<div><div></div></div>
<div><div></div><div>HIGH</div></div>	7.5	6.7	Samba Badlock Vulnerability	General	1	<div><div></div></div>	<div><div></div></div>

Host Details

IP:

192.168.50.101

MAC:

08:00:27:6E:A9:F1

OS:

Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start:

January 24 at 2:21 PM

End:

January 24 at 2:52 PM

Elapsed:

31 minutes

KB:

[Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

1° Criticità

Vulnerabilities	64				
CRITICAL VNC Server 'password' Password	Plugin Details				
Description The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.	Severity: Critical ID: 61708 Version: \$Revision: 1.2 \$ Type: remote Family: Gain a shell remotely Published: August 29, 2012 Modified: September 24, 2015				
Solution Secure the VNC service with a strong password.	Risk Information Risk Factor: Critical CVSS v2.0 Base Score: 10.0 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C				
Output Nessus logged in using a password of "password". To see debug logs, please visit individual host <table><tr><th>Port</th><th>Hosts</th></tr><tr><td>5900 / tcp / vnc</td><td>192.168.50.101</td></tr></table>	Port	Hosts	5900 / tcp / vnc	192.168.50.101	Vulnerability Information Default Account: true Exploited by Nessus: true
Port	Hosts				
5900 / tcp / vnc	192.168.50.101				

```
e.gpg Could not resolve 'security.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security,
18n/Translation-en_US.bz2 Could not resolve 'security.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security,
cted/i18n/Translation-en_US.bz2 Could not resolve 'security.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security,
se/i18n/Translation-en_US.bz2 Could not resolve 'security.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security,
erse/i18n/Translation-en_US.bz2 Could not resolve 'security.ubuntu.com'
W: Some index files failed to download, they have been ignored, or old ones
instead.
W: You may want to run apt-get update to correct these problems
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin# _
```

La prima vulnerabilità ad essere presa in esame è stata la “VNC Server ‘password’ Password”, la soluzione proposta da Nessus richiedeva un cambio di password VNC con una più sicura. Il cambio è stato effettuato direttamente dalla macchina Metasploitable 2: utilizzando i comandi di super amministratore è stato inserito il comando “vncpasswd” per poter cambiare password, la nuova password digitata non risulta visibile sulla shell di metasploit, ma il cambio è avvenuto con successo visto che la successiva scansione con Nessus non ha riportato la vulnerabilità.

2° Criticità



CRITICAL Bind Shell Backdoor Detection

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the following request :  
  
This produced the following truncated output (limited to 10 lines) :  
..... snip .....  
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:/#  
  
..... snip .....
```

To see debug logs, please visit individual host

Port **Hosts**

Plugin Details

Severity: Critical
ID: 51988
Version: 1.10
Type: remote
Family: Backdoors
Published: February 15, 2011
Modified: April 11, 2022

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

La seconda vulnerabilità risolta è stata la “Bind Shell Backdoor Detection”, Nessus ha rilevato una Backdoor nella shell di Metasploit tramite la porta 1524. Prima di cominciare a risolvere questa criticità è stata eseguita una scansione “nmap -sV 192.168.32.101” evidenziando come la porta 1524 fosse aperta e sfruttabile per eventuali attacchi. Preso atto della situazione è stato lanciato il comando netcat “nc 192.168.32.101 1524” così facendo è stato possibile “sfruttare” la backdoor come root@metasploitable, da qui è stato lanciato il comando “netstat -an | grep 192.168.32.101” per vedere quali utenti fossero in ascolto con determinate porte ed è stata evidenziata una connessione fra Metasploitable e la macchina Kali. Per poter interrompere questa connessione è stata utilizzata la regola firewall “iptables -A INPUT -p tcp -dport 1524 -j DROP”, un successivo lancio di “nmap -sV 192.168.32.101” ha evidenziato la porta 1524 con la dicitura “filtered” chiudendo la connessione fra le due macchine. Una successiva scansione Nessus non ha presentato la criticità “Bind Shell Backdoor Detection”, risultando così essere stata risolta correttamente.

```

(kali㉿kali)-[~]
$ nmap -sV 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-27 11:54 EST
Nmap scan report for 192.168.32.101
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

```

(kali㉿kali)-[~]
$ nc 192.168.32.101 1524
root@metasploitable:/# netsta -an | grep 192.168.32.101
bash: netsta: command not found
root@metasploitable:/# netstat -an | grep 192.168.32.101
tcp        0      0 192.168.32.101:53      0.0.0.0:*               LISTEN
tcp        0      0 192.168.32.101:1524    192.168.50.100:35304    ESTABLISHED
tcp        0      0 192.168.32.101:6667    192.168.50.100:47998    ESTABLISHED
udp        0      0 192.168.32.101:137     0.0.0.0:*
udp        0      0 192.168.32.101:138     0.0.0.0:*
udp        0      0 192.168.32.101:53      0.0.0.0:*
udp        0      0 192.168.32.101:36606   192.168.1.254:53       ESTABLISHED
root@metasploitable:/# iptables -P INPUT 1524 DROP
Try `iptables -h' or 'iptables --help' for more information.
Bad argument `DROP'
root@metasploitable:/# iptables -A INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/# netstat -an | grep 192.168.32.101

```

```

Nmap scan report for 192.168.32.101
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.92 seconds

```

3° Criticità

CRITICAL

NFS Exported Share Information Disclosure

< >

Description

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.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

The following NFS shares could be mounted :

```
+ /
+ Contents of / :
+ ..
+ ..
+ bin
+ boot
more...
```

To see debug logs, please visit individual host

Port ▲

Hosts

2049 / udp / rpc-nfs

192.168.50.101

Plugin Details

Severity: Critical

ID: 11356

Version: 1.21

Type: remote

Family: RPC

Published: March 12, 2003

Modified: August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 730 days +

Product Coverage: Low

CVSSV3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9

La terza criticità affrontata risulta essere la “NFS Exported Share Information Disclosure”. Questa vulnerabilità è stata risolta direttamente dalla macchina metasploit entrando e modificando il file `/etc/exports` dopo aver usato il comando da amministratore `“sudo nano /etc/exports”`. Dopo essere entrati nel file sono state modificate le voci `“hostname 1”` e `“hostname 2”` sostituite con l’IP di Metasploit. È stata effettuata una scansione Nessus per vedere se questa fosse stata risolta, ma dopo essere stata rilevata nuovamente si è proceduto con il sostituire `“*”` con l’IP Metasploit e sono stati rimossi le voci `“no_”` fra parentesi. Una successiva scansione Nessus non ha più rilevato la criticità lasciando intendere che fosse stata risolta.

```
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes 192.168.32.101(rw,sync) 192.168.32.101(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/*(rw,sync,no_root_squash,no_subtree_check)
```

```
GNU nano 2.0.7 File: /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes 192.168.32.101(rw,sync) 192.168.32.101(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
192.168.32.101(rw,sync,root_squash,subtree_check)
```

4° Criticità

CRITICAL

SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

<https://www.czhogier.com/academic/papers/openssl.pdf>

Plugin Details

Severity: Critical

ID: 20007

Version: 1.34

Type: remote

Family: Service detection

Published: October 12, 2005

Modified: April 4, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

In the news: true

La quarta vulnerabilità critica identificata riguarda la “SSL Version 2 and 3 Protocol Detection”, la corretta risoluzione è stata effettuata dal browser Mozilla Firefox direttamente dalla macchina Kali. Nella barra di ricerca è stato inserito il testo “about:config”, accettato il rischio è stato inserito “tls” nella nuova barra di ricerca della pagina e modificato il valore da “3” a “0” della voce “security.tls.version.min”. Una nuova scansione non ha rilevato la criticità, risultando così risolta.

Firefox about:config

search

tls

Show only modified preferences

security.tls.ech.disable_grease_on_fallback	true	
security.tls.ech.grease_http3	false	
security.tls.ech.grease_probability	0	
security.tls.ech.grease_size	100	
security.tls.enable_0rtt_data	true	
security.tls.enable_delegated_credentials	true	
security.tls.enable_post_handshake_auth	false	
security.tls.hello_downgrade_check	true	
security.tls.insecure_fallback_hosts		
security.tls.version.enable-deprecated	false	
security.tls.version.fallback-limit	4	
security.tls.version.max	4	
security.tls.version.min	0	
security.tls13.aes_128_gcm_sha256	true	
security.tls13.aes_256_gcm_sha384	true	
security.tls13.chacha20_poly1305_sha256	true	