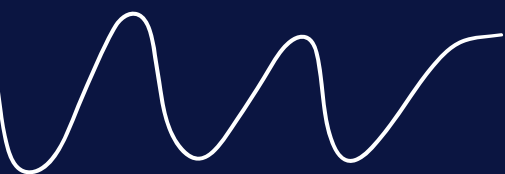


ACTIVITY



PROGETTO S5/L5



Scansionare metasploitable con Nessus e
risolvere da 2 a 4 vulnerabilità critiche

by Davide Lecci

VULNERABILITY LIST

Elenco delle vulnerabilità identificate con Nessus

VNC SERVER 'PASSWORD' PASSWORD

VNC Server è un servizio per la condivisione remota della macchina che consente ad utenti esterni di controllarla. Nessus ci segnala che è riuscito ad entrare poiché il servizio è protetto da una password debole, quindi un black hat potrebbe prendere il controllo di meta.

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
Solution Secure the VNC service with a strong password.		ID:	61708
		Version:	\$Revision: 1.2 \$
		Type:	remote
		Family:	Gain a shell remotely
		Published:	August 29, 2012
		Modified:	September 24, 2015

REMEDIATION ACTION

Per la vulnerabilità di **VNC** è stato necessario cambiare la password per accedere al servizio inserendone una più robusta, in questo modo l'accesso viene bloccato in quanto non viene trovata la password corretta. Per maggiore sicurezza ho cambiato la password di accesso sia per l'utente admin che per l'utente root.

```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Oct 27 03:26:50 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password: _
```

NFS EXPORTED SHARE INFORMATION DISCLOSURE

NFS è un protocollo che consente di accedere a determinate cartelle e file da remoto come se fossero sul nostro pc. Un black hat quindi potrebbe visualizzare questi file e cartelle e anche effettuare operazioni di scrittura su di esse montandole sul proprio host.

CRITICAL NFS Exported Share Information Disclosure		< > Plugin Details	
Description		Severity:	Critical
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.		ID:	11356
		Version:	1.21
		Type:	remote
		Family:	RPC
		Published:	March 12, 2003
		Modified:	August 30, 2023
Solution			
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.			

REMEDIATION ACTION

Per quanto riguarda **NFS** per risolvere la vulnerabilità è stato necessario andare sul file exports contenuto nella cartella /etc e modificarlo come si può vedere nello screenshot seguente:

```
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw, sync) hostname2(ro, sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw, sync, fsid=0, crossmnt)
# /srv/nfs4/homes gss/krb5i(rw, sync)
#

/home/msfadmin/nsf_share *(rw, sync, root_squash, no_subtree_check)

[ Wrote 12 lines ]

msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server start
* Exporting directories for NFS kernel daemon...
exportfs: Warning: /home/msfadmin/nsf_share does not exist
* Starting NFS kernel daemon
msfadmin@metasploitable:~$
```

Ho creato una cartella per la condivisione che ho lasciato vuota e ho puntato a quella cartella scrivendo il path nel file. Una volta fatto ciò ho cambiato l'impostazione **no_root_squash** in **root_squash**, questo fa sì che il sistema forzi l'utente che prova ad accedere come root, ad accedere come un utente anonimo perché gli assegnerà un id anonimo aumentando così la sicurezza. Per concludere la modifica è necessario restartare il servizio con l'apposito comando che si vede nello screenshot.

BIND SHELL BACKDOOR DETECTION


La vulnerabilità Bind Shell Backdoor Detection ci dice che una shell è in ascolto sulla porta remota senza che sia richiesta autenticazione. Un black hat potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Per risolvere questa vulnerabilità, dovremmo verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.

CRITICAL Bind Shell Backdoor Detection		Plugin Details	
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.	Severity:	Critical
		ID:	51988
Version:		1.10	
Type:		remote	
Family:		Backdoors	
Published:		February 15, 2011	
Modified:		April 11, 2022	

REMEDIATION ACTION

Per risolvere il problema ho effettuato una scansione dei servizi con nmap in quanto Nessus mi diceva che la porta interessata era la 1524

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.21 

```
└─$ nmap -sV 192.168.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 13:20 CEST
Nmap scan report for 192.168.1.21
Host is up (0.00030s 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 rshd
513/tcp   open  login           OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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  ftp             ProFTPD 1.3.1
3306/tcp  open  mysql           MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql      PostgreSQL DB 8.3.0 - 8.3.7
5901/tcp  open  vnc             VNC (protocol 3.3)
6001/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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.40 seconds
```

Ho cercato quale processo fosse attivo su metasploitable su quella porta lì:

```
xinetd 4524 root 11u IPv4 12236 TCP *:512 (LISTEN)
xinetd 4524 root 12u IPv4 12237 TCP *:1524 (LISTEN)
```

Ho aggiunto una chain tramite iptables per bloccare le connessioni in entrata sulla porta 1524, in questo modo viene bloccata la back door.

```
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
```

UNREALIRC BACKDOOR DETECTION

Questa vulnerabilità permette ad un attaccante di inserire codice malevolo su un server vulnerabile o comunque di leggerne le informazioni. Questo tipo di problema si riscontra sui server Apache Tomcat

CRITICAL UnrealIRCd Backdoor Detection		Plugin Details
Description The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.	Solution Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	
	See Also	
		Severity: Critical
		ID: 46882
		Version: 1.16
		Type: remote
		Family: Backdoors
		Published: June 14, 2010
		Modified: April 11, 2022

REMEDIATION ACTION

Per risolvere il problema ho effettuato due azioni. Ho inserito una regola nel firewall iptables per bloccare le connessioni in entrata sulla porta segnalata da nessus

```
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 6667 -j DROP
```

APACHE TOMCAT AJP CONNECTOR REQUEST INJECTION

Attraverso la mancanza di autenticazione sul file server.xml di Tomcat un blackhat potrà accedere ai server vulnerabili e leggere file o uploadare codice malevolo tramite file JSP

CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)		Plugin Details
Description 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).	Solution 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.	
		Severity: Critical
		ID: 134862
		Version: 1.42
		Type: remote
		Family: Web Servers
		Published: March 24, 2020
		Modified: September 25, 2023

REMEDIATION ACTION

Per questo problema sono andato a modificare il file **server.xml** nella cartella di TomCat ed ho disabilitato la riga che creava la vulnerabilità in questo modo ho disabilitato il servizio.

```
<!-- <Connector port="8009"
      enableLookups="false" redirectPort="8443" protocol="AJP/1.3" req$
```