Metasploitable

Report generated by Nessus™ Thu, 24 Nov 2022 06:48:14 EST

192.168.32.102

Scan Information

Start time:	Thu Nov 24 06:20:55 2022
End time:	Thu Nov 24 06:48:14 2022

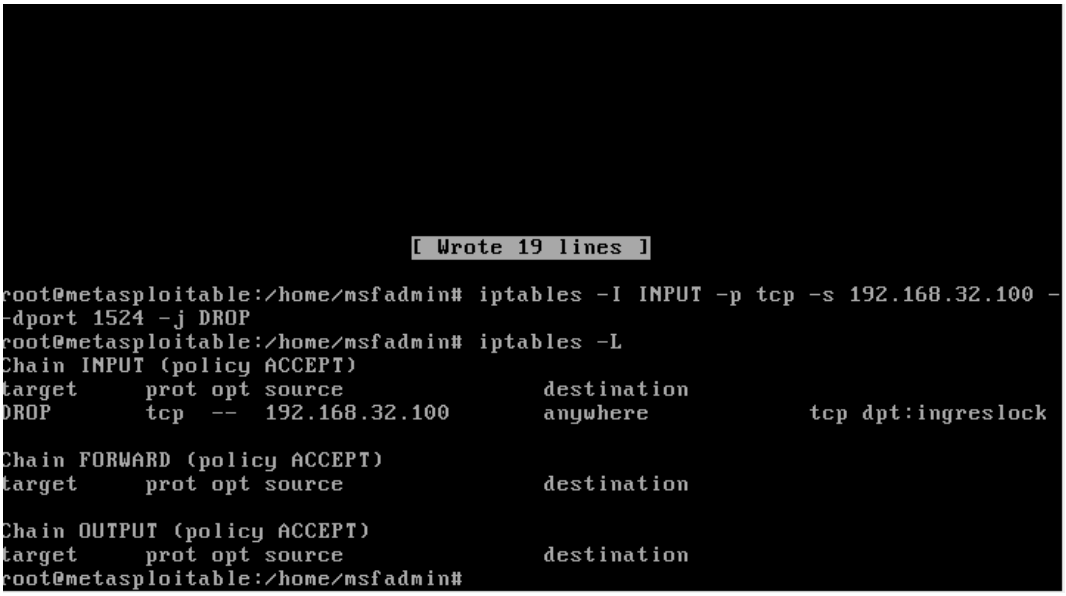
Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.32.102
MAC Address:	08:00:27:E2:A5:64
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

51988 - Bind Shell Backdoor Detection CRITICAL

Descrizione:
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla connettendosi alla porta remota e inviando direttamente i comandi.

Soluzione:
Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.
Usando il firewall di Linux, iptables, andiamo ad inserire la regola per bloccare la backdoor; con –I inseriamo la nuova regola, con –p specifichiamo il protocollo, -s per specificare l’IP sorgente, --dport per specificare la porta e con –j inseriamo l’azione (in questo caso DROP):



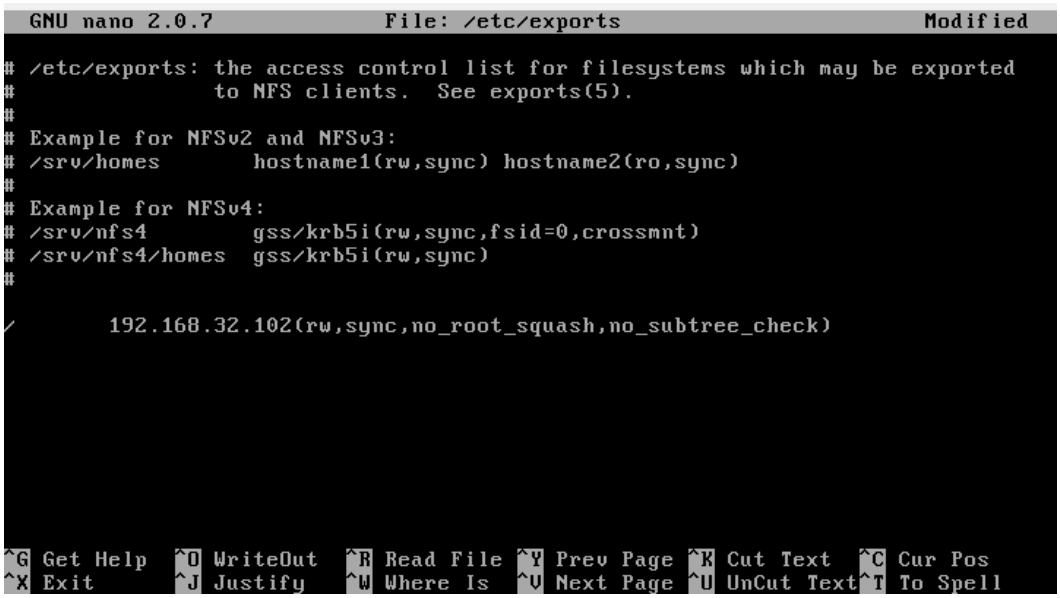
N.B. : Metasploitable non va riavviato e deve rimanere acceso, le regole inserite su iptables si cancellano una volta riavviato il sistema.

Porta:
tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure CRITICAL

Descrizione:
Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione:
Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.
Su Metasploitable con il comando sudo nano /etc/exports andiamo ad inserire l'IP di Metasploitable; come vediamo nell'immagine sotto, questa è l' access control list del file system:



Porta:
udp/2049/rpc-nfs

61708 - VNC Server 'password' Password — CRITICAL

Descrizione:
Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un aggressore remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Soluzione:
Proteggete il servizio VNC con una password forte.
Su Metasploitable cambiamo la password usando i privilegi di root, mettiamo il comando vncpasswd ed inseriamo una password più forte. Tutto qui.

```
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 loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# msfadmin
bash: msfadmin: command not found
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

Porta:
tcp/5900/vnc

10203 - rexecd Service Detection — CRITICAL

Descrizione:
Il servizio rexecd è in esecuzione sull'host remoto. Questo servizio è stato progettato per consentire agli utenti di una rete di eseguire comandi in remoto. Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi può essere abusato da un utente malintenzionato per eseguire la scansione di un host di terze parti.

Soluzione:
Commentare la riga 'exec' in /etc/inetd.conf e riavviare il processo inetd.

```
  GNU nano 2.0.7            File: /etc/inetd.conf                      Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec            stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/in.rexecd
ingreslock stream tcp nowait root /bin/bash bash -i

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ? _
 Y Yes
 N No            ^C Cancel
```

Porta: tcp/512

Effettuando poi una seconda scansione, possiamo vedere come le criticità sono state risolte:

192.168.32.102

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	3	17	5	71

Vulnerabilities — Total: 101

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability