



Vulnerability scanner su Metasploitable

Ho effettuato una scannerizzazione delle vulnerabilità sull'host metasploitable utilizzando il programma Nessus su kali, specificando le porte più comuni cioè dalla prima fino alla 1024. Dopo aver effettuato la scannerizzazione Nessus ci da tutte le vulnerabilità dal livello più critico. Vado a risolvere quindi alcune delle vulnerabilità critiche che la scannerizzazione ha trovato.

Report delle vulnerabilità prima di risolvere alcune di esse

192.168.178.69



Vulnerabilities

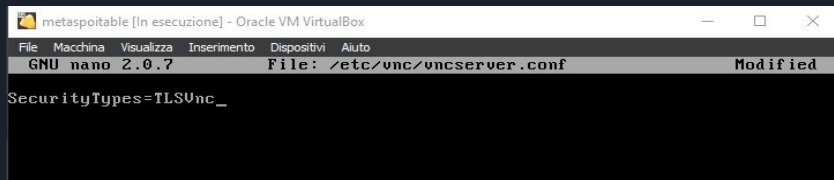
Total: 118

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	10205	rlogin Service Detection
HIGH	7.5*	6.7	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled

Vulnerabilità critica:

Questa vulnerabilità riguarda il server VNC che dice avere una password debole. Quindi il nostro scopo è rafforzare la password. La soluzione è, essere root su meta, poi aprire il file con il comando `nano /etc/vnc/vncserver.conf`, si aprirà un file dove noi dobbiamo scrivere la stringa `"SecurityTypes=TLSTLSvnc"`. Una volta fatto questo salviamo il file e riavviare la macchina.



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/vnc/vncserver.conf Modified
SecurityTypes=TLSTLSvnc_
```

CRITICAL

VNC Server 'password' Password

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.

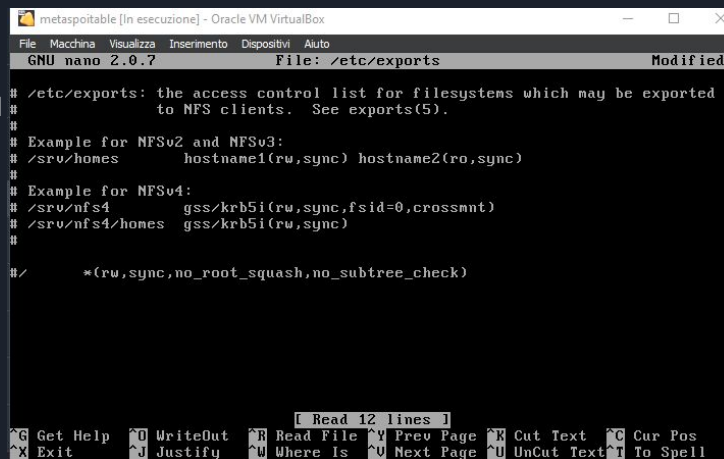
Solution

Secure the VNC service with a strong password.

Vulnerabilità critica:

Questa vulnerabilità permette ad un attaccante di scrivere o leggere file sull'host remoto, perchè NFS non è configurato per far accedere ai suoi remote shares solo da host autorizzati.

La soluzione è stato, aprire il file con il comando “nano /etc/exports” e nel file che ci apre avremo l'ultima stringa (/ *(rw, sync, no_root_squash ... etc) che dovremo eliminare oppure metto semplicemente il # per far diventare quella stringa un commento. Una volta fatto questo salviamo il file e riavviare la macchina.

A screenshot of a terminal window titled 'metasploitable [In esecuzione] - Oracle VM VirtualBox'. The terminal shows the GNU nano 2.0.7 editor editing the file /etc/exports. The content of the file is as follows:

```
# /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 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)
#
#/* *(rw,sync,no_root_squash,no_subtree_check)
```

The bottom of the terminal shows a status bar with 'Read 12 lines' and various keyboard shortcuts like '^G Get Help', '^X Exit', '^O WriteOut', '^J Justify', '^R Read File', '^W Where Is', '^Y Prev Page', '^U Next Page', '^C Cur Pos', '^T To Spell', and '^U UnCut Text'.

CRITICAL

NFS Exported Share Information Disclosure

Description

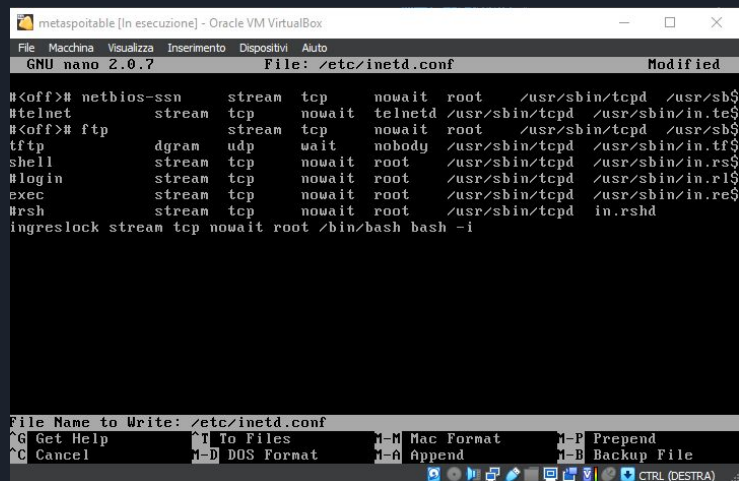
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

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

Vulnerabilità alta:

Questa vulnerabilità riguarda il servizio rlogin, questo servizio è vulnerabile dato che i dati trasmessi tra il client e il server sono in chiaro, permettendo ad un hacker di intercettare i login e le password. La soluzione a questo problema è aprire il file “nano /etc/inetd.conf” e mettere come commento la stringa login con il # in modo tale da disattivare la stringa. Infine, salvare e riavviare la macchina.



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf Modified

#<off># netbios-ssn stream tcp nowait root /usr/sbin/tcpd /usr/sbin/
#telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd
#<off># ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.ftpd
tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd
shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd
#login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogind
exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd
#rsh stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd
ingreslock stream tcp nowait root /bin/bash bash -i

File Name to Write: /etc/inetd.conf
^G Get Help ^T To Files M-M Mac Format M-P Prepend
^C Cancel M-D DOS Format M-A Append M-B Backup File
CTRL (DESTRA)
```

HIGH

rlogin Service Detection

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

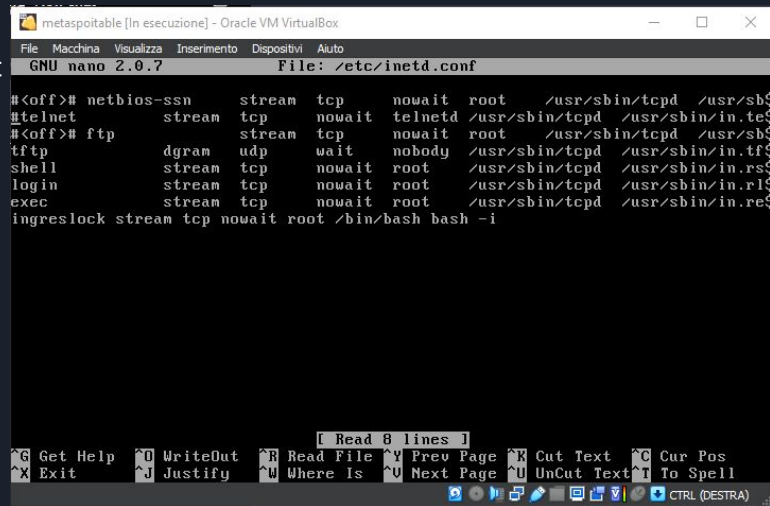
Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Vulnerabilità media:

Questa vulnerabilità indica che l'host remoto sta utilizzando un server Telnet su un canale non criptato. Per questo motivo tutti i dati di login e i comandi sono visibili permettendo un attacco man-in-the-middle facendo intercettare una sessione Telnet ottenendo tutti i dati sensibili. SSH è preferibile a Telnet dato che protegge le credenziali dall'essere intercettate. Come soluzione dobbiamo aprire il file con il comando "nano /etc/inetd.conf" e sulla seconda stringa dove troviamo scritto "telnet stream tcp nowait etc..." dobbiamo mettere il # prima della stringa mettendola come commento quindi disattivando il telnet. Dopo aver disattivato il telnet server dobbiamo essere sicuri che la porta 22 del SSH sia attiva, questo si può controllare aprendo il file con il comando "nano /etc/ssh/sshd_config" e vedere che la Port 22 sia scritta e attiva.



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
#telnet               stream  tcp    nowait  telnetd  /usr/sbin/tcpd  /usr/sbin/tcpd
#<off># ftp           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
tftp                 dgram   udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/tcpd
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
login                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/tcpd
ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page  ^U UnCut Text ^T To Spell
[Icons] CTRL (DESTRA)
```

```
# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
```

MEDIUM

Unencrypted Telnet Server

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Report finale delle vulnerabilità

192.168.178.69



Vulnerabilities

Total: 116

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
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)
CRITICAL	10.0*	-	46882	UnrealIRCd Backdoor Detection
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
HIGH	7.5*	-	10245	rsh Service Detection
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	-	136808	ISC BIND Denial of Service

MEDIUM	5.9	-	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	-	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	-	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	-	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	-	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	-	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)