

Scansione e azioni di rimedio

Consegna S5:L5 – Progetto pratico del venerdì

Flavio Scognamiglio

Traccia



Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti. Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Tipo di scansione

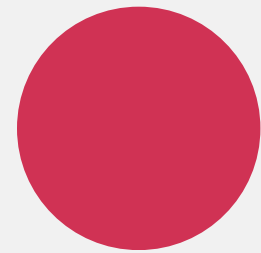
Obiettivo: Metasploitable (192.168.1.101)

Come già dimostrato nelle mie slide dell'esercitazione del giorno prima, è possibile effettuare da Nessus vari tipi di scansioni, incluse **scansioni avanzate** all'interno delle quali vanno specificati vari parametri. Questo serve a rendere la ricerca di vulnerabilità più **efficiente** e mirata.

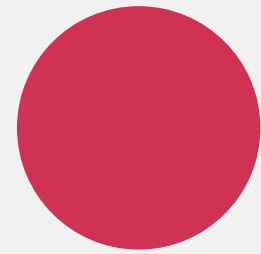
Si possono anche disabilitare plugin non rilevanti per il bersaglio, ottimizzando così il processo di scansione. Questo dipende anche da come sono state effettuate le fasi precedenti, come l'information gathering, per ottenere una mappatura accurata del sistema da analizzare.

Per questo tipo di esercitazione ho effettuato una scansione di base, consapevole che avrebbe individuato almeno la maggior parte delle vulnerabilità citate nella traccia, avendo già precedentemente eseguito test più mirati e approfonditi sulla stessa macchina.

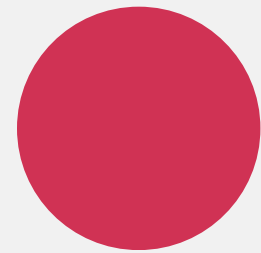
Principali vulnerabilità scansione di base



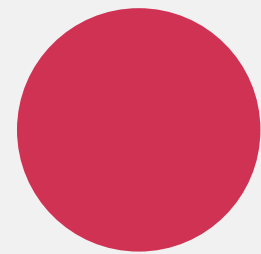
NFS Exported



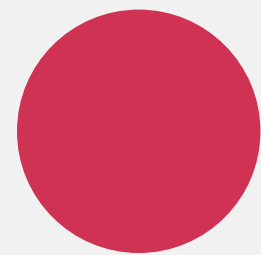
VNC Server password



Bind shell backdoor detection



UnrealIRCd Backdoor detection



Rexecd Service Detection

Metasploitable-test-1 / 192.168.1.101
[← Back to Hosts](#)

Vulnerabilities 104

Filter Search Vulnerabilities 104 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/>	MIXED	Apache Tomcat (Multiple Issues)	Web Servers
<input type="checkbox"/>	MIXED	Phpmyadmin (Multiple Issues)	CGI abuses
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/>	MIXED	PHP (Multiple Issues)	CGI abuses
<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Detection	Service detection

NFS Exported Share Information Disclosure

Il vulnerability scanner ci fornisce tutte le informazioni necessarie per capire il funzionamento di questa vulnerabilità. Inoltre, cosa più importante, ci fornisce i CVE (Common Vulnerabilities and Exposures): **CVE-1999-0170 - CVE-1999-0211 - CVE-1999-0554**

NFS (Network File System) su Metasploitable presenta una vulnerabilità significativa dovuta a configurazioni non sicure e permessi inappropriati. Questo protocollo di condivisione file, se non configurato correttamente, può essere soggetto a accessi non autorizzati e spoofing, consentendo a potenziali attaccanti di ottenere accesso privilegiato ai file e alle directory condivise attraverso la rete.

Con nmap e con lo **script nfs** possiamo evidenziare i risultati per le porte coinvolte **111** e **2049**. Entrambe sono aperte, e sulla porta 111 vi è la directory “/” sotto NFS mount

CRITICAL

NFS Exported

Description

At least one of the NFS shares exported on the remote host allows read (and possibly write) files on the remote host.

Solution

Configure NFS on the remote host.

Output

The following NFS shares are exported on the remote host:

+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp

Parrot Terminal

FileModificaVisualizzaCercaTerminaleAiuto

\$sudo nmap --script=nfs* 192.168.1.101 -sV -sS -p 111,2049

[sudo] password di satana:

Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-28 11:33 CEST

Nmap scan report for 192.168.1.101

Host is up (0.00035s latency).

PORTSTATESERVICEVERSION

111/tcpopenrpcbind 2 (RPC #100000)

| nfs-statfs:

| Filesystem1K-blocksUsedAvailableUse%MaxfilesizeMaxlink

|_ /7282168.01619332.05295836.024%2.0T32000

| rpcinfo:

| programversionport/protoservice

| 1000002111/tcprpcbind

| 1000002111/udprpcbind

| 1000032,3,42049/tcpnfs

| 1000032,3,42049/udpnfs

| 1000051,2,335565/udpmountd

| 1000051,2,351910/tcpmountd

| 1000211,3,435718/udpnlockmgr

| 1000211,3,458541/tcpnlockmgr

| 100024142267/tcpstatus

|_ 100024152299/udpstatus

| nfs-ls: Volume /

| access: Read Lookup Modify Extend Delete NoExecute

| PERMISSIONUIDGIDSIZETIMEFILENAME

| drwxr-xr-x0040962012-05-14T03:35:33bin

| drwxr-xr-x0040962010-04-16T06:16:02home

Metasploit (

Reference

CVE-1999-0170

CVE-1999-0211

CVE-1999-0554

Reference I

CVE-1999-0170

CVE-1999-0211

CVE-1999-0554

| drwxr-xr-x0040962010-04-28T04:06:37usr

|_

| nfs-showmount:

|_ / *

2049/tcp open nfs2-4 (RPC #100003)

MAC Address: BC:24:11:DF:07:8D (Unknown)

Rimedio vulnerabilità NFS

L'obiettivo è chiaramente quello di non consentire a tutti di accedere ai volumi condivisibili, e quindi modificare opportunamente le configurazioni per restringere il campo di accesso o limitarlo unicamente a determinati **host** di una specifica rete.

```
# 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)
msfadmin@metasploitable:~$ cat /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#               ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
ALL:ALL
msfadmin@metasploitable:~$ _
```

Il file `/etc/exports` configura la condivisione dei volumi tramite NFS, includendo il path (`/`) per permettere l'accesso completo a tutti i client. Nel file `/etc/hosts.allow`, la configurazione `ALL:ALL` consente a tutti gli host di tentare di connettersi ai servizi di rete. È essenziale rivedere e modificare queste configurazioni per limitare l'accesso solo agli host autorizzati o a reti specifiche, migliorando così la sicurezza complessiva del sistema.

VNC server password

Il vulnerability scanner ci segnala un problema sul servizio VNC di controllo remoto, esattamente sulla porta **5900**. Ci dice che la password utilizzata per il login è troppo debole, ed effettivamente dimostra come sia semplice attraverso il bruteforce scoprirla: "**password**".

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.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.1.101 

Rimedio vuln VNC

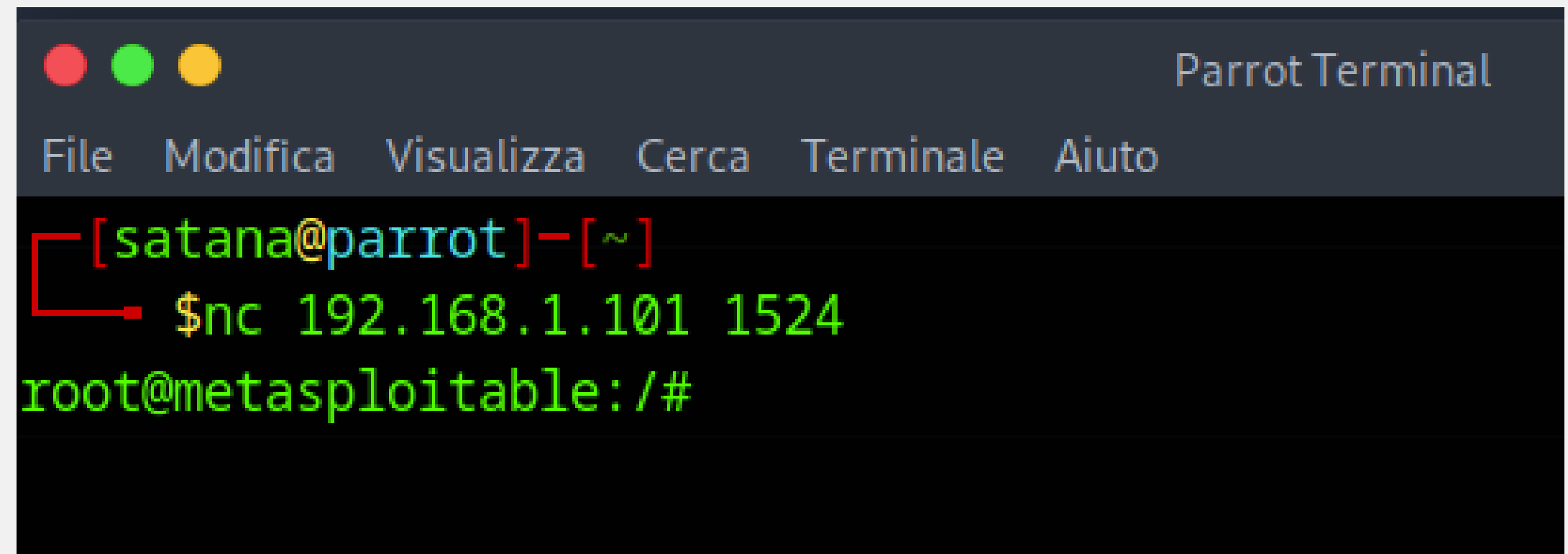
Banalmente, andrebbe cambiata la password applicando e **aggiungendo** ulteriori policy SERIE come quelle descritte nel report dell'azienda Theta. Per la password ci basterà il comando **vncpasswd**. In aggiunta si potrebbe ragionare su una eventuale restrizione degli accessi autorizzati e quindi applicare alcune **regole al firewall** (simili ma ovviamente con parametri diversi, a quelle che ho riportato per risolvere il problema della bindshell) per gestire meglio il traffico verso la porta utilizzata da vnc.

```
msfadmin@metasploitable:~$ vncpasswd  
Using password file /home/msfadmin/.vnc/passwd  
Password: _
```


Bind shell backdoor detection

Questa vulnerabilità è saltata fuori in varie occasioni passate durante l'apprendimento di altri tool.
Anche nessus ci segnala quindi che sulla porta **1524** vi è una bella **backdoor**!

Si tratta semplicemente di una shell Bash legata alla porta 1524/tcp. Eseguirà tutto ciò che viene inviato a quella porta su Bash e risponderà con il relativo **output**



```
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto
[satana@parrot]-[~]
$nc 192.168.1.101 1524
root@metasploitable:/#
```

Poniamo rimedio a questa bind shell

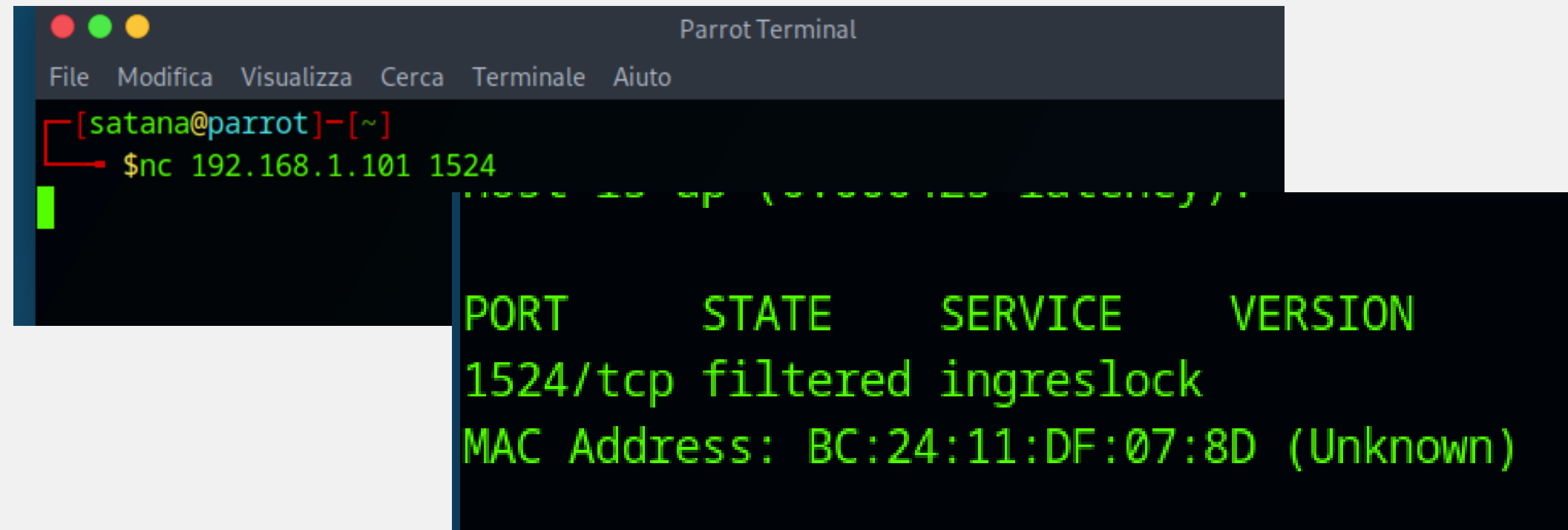
Prima di tutto bisogna identificare il **PID** della bindshell (netstat) e **terminarlo**, eliminando anche eventuali **persistenze** (magari reinstallando e aggiornando il sistema). Il comando: **sudo fuser -k -n tcp 1524** potrebbe fare al caso nostro.

```
sfadmin@metasploitable:~$ sudo fuser -k -n tcp 1524
1524/tcp:          4529
sfadmin@metasploitable:~$ _
```

Altri consigli relativi ai firewall, ad esempio iptables:

sudo iptables -A INPUT -p tcp --dport 1254 -j DROP

in alternativa il firewall di ubuntu (essendo metasploitable una vecchia versione di ubuntu) ufw:
sudo ufw allow && sudo ufw deny 1254



The screenshot shows a Parrot Terminal window with a menu bar (File, Modifica, Visualizza, Cerca, Terminale, Aiuto). The terminal output shows a netcat listener on 192.168.1.101 port 1524. A connection is established, and a nmap scan is performed, resulting in the following output:

```
PORT      STATE      SERVICE      VERSION
1524/tcp  filtered  ingreslock
MAC Address: BC:24:11:DF:07:8D (Unknown)
```

UnrealIRCd Backdoor detection

L'UnrealIRCd Backdoor è una vulnerabilità nota scoperta nel 2010 che interessa una versione compromessa del software **UnrealIRCd**, un popolare **server IRC**.

CRITICAL

UnrealIRCd Backdoor Detection

>

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
<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

The remote IRC server is running as :

uid=0(root) gid=0(root)

To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	192.168.1.101

Plugin Details

Severity: Critical

ID: 46882

Version: 1.16

Type: remote

Family: Backdoors

Published: June 14, 2010

Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Functional

Age of Vuln: 730 days +

Product Coverage: Low

CVSSV3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4

Una versione di UnrealIRCd distribuita dal sito ufficiale conteneva una backdoor che permetteva agli attaccanti di eseguire comandi arbitrari sul server con i privilegi dell'utente che eseguiva il processo UnrealIRCd.

L'attaccante può inviare una stringa specifica a qualsiasi porta su cui UnrealIRCd è in ascolto. Questa stringa attiva la backdoor e permette l'esecuzione di comandi.

Mitigazione UnrealIRCd

Ho individuato tre modi per risolvere questo problema:

Aggiornare UnrealIRCd a una versione non compromessa

```
nohup /usr/bin/rmiregistry >/dev/null 2>&1 &  
nohup /usr/bin/unrealircd &  
rm -f /root/.vnc/*.pid  
HOME=/root LOGNAME=root USER=root nohup /usr/bin/vncserver :0 >/root/vnc.log 2  
1 &  
nohup /usr/sbin/druby_timeserver.rb &  
  
exit 0  
msfadmin@metasploitable:~$
```

Disinstallare la versione compromessa e reinstallare da fonti verificate

Disabilitare unrealircd da /etc/rc.local e rimuovere la directory da /etc/unreal

Rexecd Service Detection

Questo servizio è noto per essere vulnerabile a exploitation tramite l'invio di comandi non sicuri, potenzialmente consentendo l'accesso non autorizzato al sistema. La sua rilevazione è cruciale per valutare la sicurezza e applicare le necessarie misure di protezione, come la disattivazione del servizio o l'implementazione di filtri firewall per limitarne l'accesso.

Mitigazione

Per mitigare commentarlo la riga relativa ad exec

Riporto quanto segnalato dal sw:

Il servizio Rexecd è in esecuzione su questo host. Rexecd (Remote Process Execution) ha lo stesso tipo di funzionalità di rsh: puoi eseguire comandi shell su un computer remoto.

La differenza principale è che rexecd esegue l'autenticazione leggendo il nome utente e la password *non crittografati* dal socket.

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

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

Grazie

Flavio Scognamiglio

Nessu
essential 