

S5L5 PROGETTO

ALESSANDRO MARASCA

EPICODE - CS0124

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.

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

VNC SERVER 'password' PASSWORD

PROBLEMA

COME SUGGERITO DALLO
SCREEN E DALLA TRACCIA,
OSSERVIAMO COME SIA
POSSIBILE ACCEDERE AL VNC
DA KALI LINUX, QUINDI
DOBBIAMO ANDARE A
MODIFICARE LA PASSWORD

SOLUZIONE

MODIFICHIAMO LA PSW PER
RISOLVERE LA CRITICITÀ
DIRETTAMENTE DALLA SHELL
DI METASPLOITABLE 2

```
Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
-n numeric-only IP addresses, no DNS
-o file hex dump of traffic
-p port local port number
-r randomize local and remote ports
-q secs quit after EOF on stdin and delay of secs
-s addr local source address
-T tos set Type Of Service
-t answer TELNET negotiation
-u UDP mode
-v verbose [use twice to be more verbose]
-w secs timeout for connects and final net reads
-C Send CRLF as line-ending
-z zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\'-data').

(kali@kali)-[~]
$ nc 192.168.49.101 5900
RFB 003.003
^C

(kali@kali)-[~]
$ vncviewer 192.168.49.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

```
4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
Alizza Inserimento Dispositivi Aiuto
TightVNC: root's X desktop (
root@metasploitable: /
cdrom home lib mnt proc srv usr
root@metasploitable:/# cd media
root@metasploitable:/media# ls
cdrom cdrom0 floppy floppy0
root@metasploitable:/media# cd ..
root@metasploitable:/# ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt/sbin tmp/vmlinuz
cdrom home lib mnt proc srv usr
root@metasploitable:/# sudo su
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
root@metasploitable:/#
```

ESITO

STABILITA UNA CONNESSIONE CON METASPLOITABLE 2 (NC IP + PORTA 5900) E INSERITA LA PASSWORD “PASSWORD” ACCEDIAMO ALLA SHELL DI METASPLOITABLE 2.

A QUESTO PUNTO ACCEDIAMO COME **ROOT** SU META, ENTRIAMO IN VNCPASSWD E MODIFICHIAMO LA PASSWORD (È CONSIGLIATA UNA PWD DI ALMENO 8 CARATTERI COMPOSTI DA ALMENO UNA LETTERA MAIUSCOLA, UN NUMERO E UN CARATTERE SPECIALE.

COME POSSIAMO OSSERVARE NON È PIÙ POSSIBILE ACCEDERE.

CRITICITÀ RISOLTA



```
kali@kali: ~  
File Actions Edit View Help  
-w secs          timeout for connects and final net reads  
-C              Send CRLF as line-ending  
-z              zero-I/O mode [used for scanning]  
port numbers can be individual or ranges: lo-hi [inclusive];  
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').  
  
(kali@kali)-[~]  
$ nc 192.168.49.101 5900  
RFB 003.003  
^C  
  
(kali@kali)-[~]  
$ vncviewer 192.168.49.101  
Connected to RFB server, using protocol version 3.3  
Performing standard VNC authentication  
Password:  
Authentication successful  
Desktop name "root's X desktop (metasploitable:0)"  
VNC server default format:  
  32 bits per pixel.  
  Least significant byte first in each pixel.  
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0  
Using default colormap which is TrueColor. Pixel format:  
  32 bits per pixel.  
  Least significant byte first in each pixel.  
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0  
^CCleanupSignalHandler called  
  
(kali@kali)-[~]  
$ vncviewer 192.168.49.101  
Connected to RFB server, using protocol version 3.3  
Performing standard VNC authentication  
Password:  
Authentication failure  
  
(kali@kali)-[~]  
$
```

NFS EXPORTED SHARED INFORMATION DISCLOSURE

NFS configurato erroneamente può fornire a un attaccante accesso non autorizzato a dati sensibili o ottenere la shell sul proprio sistema

Come risolvere?

MITIGATION

01

Imposta le restrizioni appropriate su tutte le condivisioni NFS, ad esempio limitando gli indirizzi IP che possono montare le condivisioni esposte

02

Imposta le restrizioni appropriate su tutte le condivisioni NFS, ad esempio limitando gli indirizzi IP che possono montare le condivisioni esposte.

03

Non esportare l' home directory .

04

Utilizza l'opzione "root_squash" nelle impostazioni NFS per impedire agli utenti root remoti di accedere alla condivisione con privilegi elevati.

GRAZIE

PROGETTO
S5L5

ALESSANDRO MARASCA
EPICODE - CS0124