

PROJECT MODULE 3

FATIMA NARDA NICOLETT RODRIGUEZ ORTEGA

1) TRACCIA

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** 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

2) SCANSIONE INIZIALE

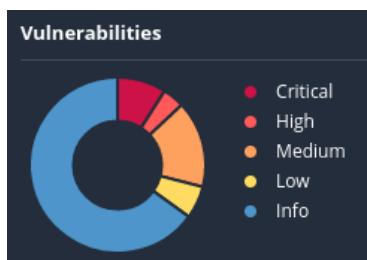
Metasploitable

[Back to All Scans](#) [Configure](#) [Audit Trail](#)

Hosts 1 Vulnerabilities 55 Remediations 2 History 3

Filter Search Vulnerabilities 55 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	🔄	✎
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄	✎
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	🔄	✎
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	🔄	✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	🔄	✎
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	28	🔄	✎
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsole...	Misc.	1	🔄	✎
<input type="checkbox"/>	MIXED	SSH (Multiple Issues)	Misc.	6	🔄	✎
<input type="checkbox"/>	MIXED	SMB (Multiple Issues)	Misc.	2	🔄	✎
<input type="checkbox"/>	MIXED	TLS (Multiple Issues)	Misc.	2	🔄	✎
<input type="checkbox"/>	MIXED	TLS (Multiple Issues)	SMTP problems	2	🔄	✎
<input type="checkbox"/>	LOW	2.6 *		X Server Detection	Service detection	1	🔄	✎



Dalla scansione si possono visualizzare 7 vulnerabilità critiche, delle quali risolveremo 2, ovvero:

- VNC Server 'password' password;
- Bind Shell Backdoor Detection.

3) METASPLOITABLE REMEDIATION

- VNC SERVER 'PASSWORD' 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	192.168.50.2

Descrizione: Il server VNC (Visual Network Computing) in esecuzione sul host remoto è protetta da una password debole. Nessus è stato in grado di accedere usando l'autenticazione VNC e come password la parola 'password'. Un attaccante non identificato da remoto potrebbe sfruttare ciò per prendere controllo del sistema.

Soluzione: Proteggere il servizio VNC con una password forte.

```
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
```

Con privilegi di amministratore, lanciamo il comando “vncpasswd” e cambiamo la password in una parola differente da ‘password’.

kali@kali: ~

File Actions Edit View Help

```
(kali@kali)-[~]
$ vncviewer 192.168.50.2
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
```

TightVNC: root's X desktop (metasploitable:0)

root@metasploitable: /

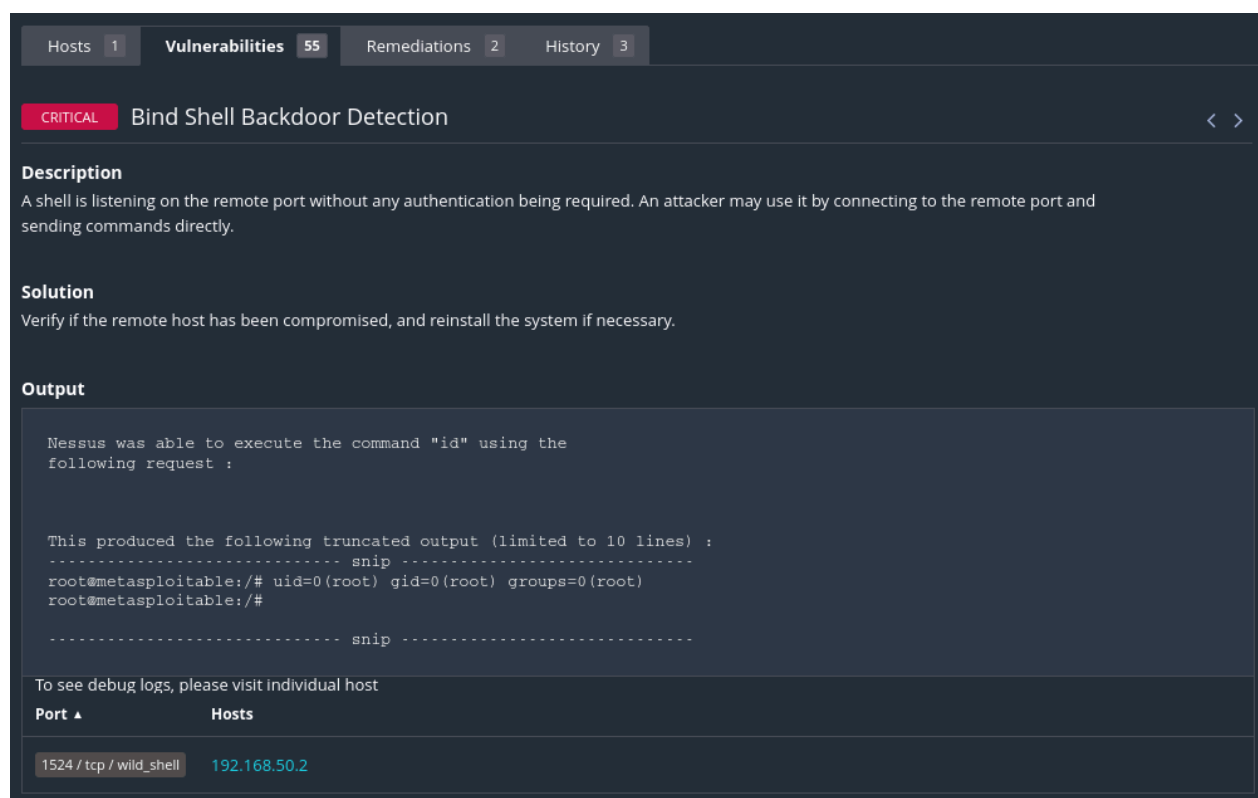
root@metasploitable:~

Verifichiamo da Kali se la nuova password funziona usando il comando “ *vncviewer* ”, ci consente di connetterci a un server VNC e visualizzare l'interfaccia grafica da remoto di Metasploitable.

```
(kali@kali)-[~]
$ vncviewer 192.168.50.2
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

Ho tentato ad inserire la precedente password per verificare che sia stata correttamente sostituita.

● BIND SHELL BACKDOOR DETECTION



Hosts 1 Vulnerabilities 55 Remediations 2 History 3

CRITICAL Bind Shell Backdoor Detection

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.

Output

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
..... snip .....
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.2

Descrizione: Su una porta remota, in questo caso 1524. una shell senza autenticazione è in ascolto. Un attaccante potrebbe sfruttare questa situazione connettendosi alla porta remota e inviando comandi direttamente.

Soluzione: Verificare se l'host remoto è stato compromesso, e reinstallare il sistema se necessario. Inoltre, bisogna chiudere la backdoor per respingere il traffico proveniente dalla porta 1524.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN2

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Any

Destination Address

/

Destination Port Range

(other)

1524

(other)

1524

From

Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Creiamo una regola firewall su pfSense al fine di bloccare il traffico che arriva alla porta 1524, la salviamo e la applichiamo alla sua rete.

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

Inoltre, lanciamo il comando “`sudo iptables -I INPUT -p tcp -dport 1524 -j DROP`” che consiste in una regola del firewall iptables che opera direttamente sul sistema di Metasploitable. Il traffico, corrispondente alla porta 1524/tcp, con questa regola dovrà essere droppato, ovvero rifiutato senza alcuna risposta.

4) SCANSIONE FINALE

Metasploitable						Configure	Audit Trail
Back to My Scans							
Hosts 1 Vulnerabilities 53 Remediations 2 History 4							
Filter Search Vulnerabilities 53 Vulnerabilities							
<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/>	CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1	🔄 ✎
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄 ✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄 ✎
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	🔄 ✎
<input type="checkbox"/>	CRITICAL	📁 2 SSL (Multiple Issues)	Gain a shell remotely	3	🔄 ✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	🔄 ✎
<input type="checkbox"/>	HIGH	7.5		Samba Badlock Vulnerability	General	1	🔄 ✎
<input type="checkbox"/>	MIXED	📁 15 SSL (Multiple Issues)	General	28	🔄 ✎
<input type="checkbox"/>	MIXED	📁 5 ISC Bind (Multiple Issues)	DNS	5	🔄 ✎
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔄 ✎
<input type="checkbox"/>	MEDIUM	5.9		SSL Anonymous Cipher Suites Supported	Service detection	1	🔄 ✎
<input type="checkbox"/>	MEDIUM	5.9		SSL DROWN Attack Vulnerability (Decrypting RSA with Obsole...	Misc.	1	🔄 ✎
<input type="checkbox"/>	MIXED	📁 6 SSH (Multiple Issues)	Misc.	6	🔄 ✎
<input type="checkbox"/>	MIXED	📁 2 SMB (Multiple Issues)	Misc.	2	🔄 ✎
<input type="checkbox"/>	MIXED	📁 2 TLS (Multiple Issues)	Misc.	2	🔄 ✎
<input type="checkbox"/>	MIXED	📁 2 TLS (Multiple Issues)	SMTP problems	2	🔄 ✎
<input type="checkbox"/>	LOW	2.6 *		X Server Detection	Service detection	1	🔄 ✎