

# MODULO 3

## TEST



Andrea Ferrantino

**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.**



192.168.32.101



#### Vulnerabilities

Total: 107

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	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*	-	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

# VNC SERVER

neta / Plugin #61708  
Back to Vulnerabilities

Configure Audit Trail Launch Report Export

Vulnerabilities 62

**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	192.168.32.101

**Plugin Details**

Severity: Critical  
ID: 61708  
Version: \$Revision: 1.2 \$  
Type: remote  
Family: Gain a shell remotely  
Published: August 29, 2012  
Modified: September 24, 2015

**Risk Information**

Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

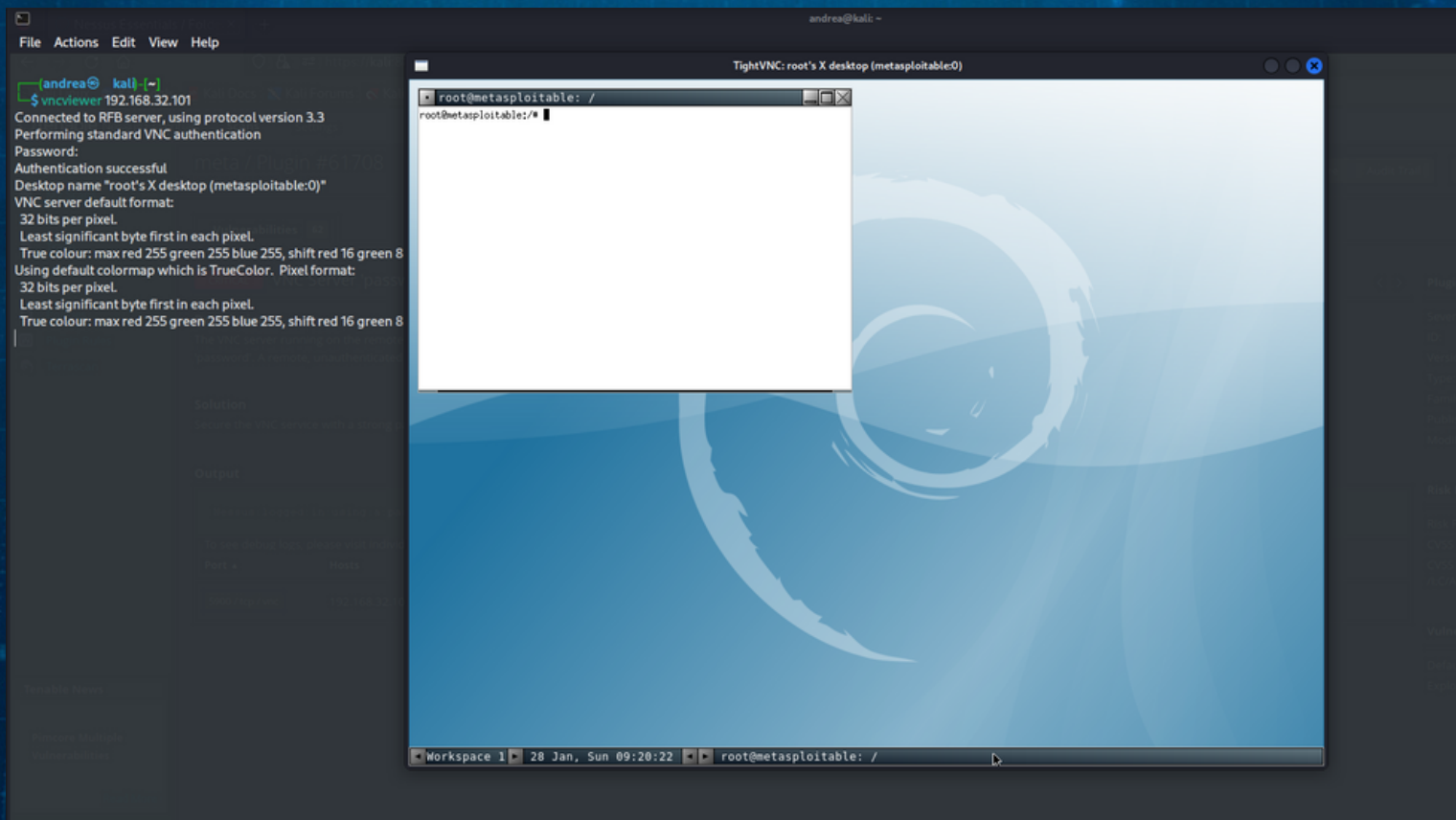
Default Account: true  
Exploited by Nessus: true

Per risolvere questa vulnerabilità lanciamo il comando “sudo su” dal terminale di metasploitable per ottenere i permessi di root, successivamente lanciamo “vnc passwd” inserendo la nuova password

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
```



In seguito controlliamo che sia andato tutto a buon fine digitando nel terminale di kali “vncviewer 192.168.32.101”.



# NFS EXPORTED SHARE INFORMATION DISCLOSURE

The screenshot shows the Tenable Nessus interface for a vulnerability scan. The main panel displays the details for vulnerability 11356, titled "NFS Exported Share Information Disclosure". The severity is marked as "CRITICAL". The description states: "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." The solution suggests: "Configure NFS on the remote host so that only authorized hosts can mount its remote shares." The output section shows a list of NFS shares that could be mounted, including "/" and "/boot". On the right, the "Plugin Details" section provides additional information: Severity: Critical, ID: 11356, Version: 1.21, Type: remote, Family: RPC, Published: March 12, 2003, Modified: August 30, 2023. The "Risk Information" section shows a Vulnerability Priority Rating (VPR) of 5.9, Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, and CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C.

Per risolvere questa vulnerabilità andiamo a modificare il file con il seguente comando "sudo nano /etc/exports" cancellando parte del contenuto come screen qui sotto

The screenshot shows a terminal window titled "Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox". The terminal is running 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)
#
# *(r,sync,root_squash,no_subtree_check)
```

At the bottom of the terminal, a status bar indicates "[ Wrote 12 lines ]". The prompt at the bottom is "root@metasploitable:/home/msfadmin#".



# BIND SHELL BACKDOOR DETECTION

meta / Plugin #51988 Configure Audit Trail

[Back to Vulnerabilities](#)

Vulnerabilities 57

**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	192.168.32.101

Per risolvere questa vulnerabilità andiamo su metasploitable e modifichiamo la regola del firewall con il seguente comando: “iptables -I INPUT -p tcp --dport (numero porta) -j DROP” salvando successivamente la regola con “iptables-save”

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$ ipt table-save
-bash: ipt: command not found
msfadmin@metasploitable:~$ iptables-save
msfadmin@metasploitable:~$
```

Quindi notiamo che facendo un'altra scan da nessus le vulnerabilità elencate sono risolte:

Nessus Essentials / Folders

My Scans

All Scans

Trash

Resources

Policies

Plugin Rules

Terrascan

Tenable News

Pimcore Multiple Vulnerabilities

Read More

meta / 192.168.32.101

Back to Hosts

Configure

Vulnerabilities 44

Filter Search Vulnerabilities 44 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8		Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		Samba Badlock Vulnerability	General	1
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	5.3		HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MIXED	...	...	SSL (Multiple Issues)	General	14
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2
LOW	2.6 *		X Server Detection	Service detection	1
INFO	...	...	SMB (Multiple Issues)	Windows	7

Host Details

IP: 192.168.32.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Start: Today at 11:30 PM

Vulnerabilities

Critical

High

Medium

Low

Info