

# “CONSEGNA ESAME S5L5”

Iannone Luca

“TRACCIA”



**Esercizio**  
Traccia e requisiti

## 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.



Progetto S5/L5 - PDF

**Esercizio**  
Traccia e requisiti

<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

L'esercizio è stato svolto utilizzando l'applicazione NESSUS per la ricerca di eventuali criticità poste sull'IP:192.168.50.101

Riconducibile alla macchina di META siccome la risoluzione di tutte le criticità ci avrebbe messo nella condizione di

sostituire componenti hardware abbiamo risolto solo alcune di esse come possiamo vedere nel proseguo della medesima relazione

## “RISOLUZIONE AL PROBLEMA SULLA PASSWORD DEL VNC SERVER”

**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**  
Beerus logged in using a password of "password".  
To see debug logs, please visit individual host

Port	Hosts
5900 / tcp / vnc	192.168.50.101

**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 la seguente criticità siamo andati a variare la “**password**”-“**VNC server**” in modo da risolverla inquanto la non risoluzione della medesima avrebbe permesso ad un eventuale attaccante connesso da remoto il controllo del sistema.

## “RISOLUZIONE ALLA CRITICITA’ SU <<RLOGIN>> E <<RSH SERVICE>>”

<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Det...	Service detection	1		
<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detec...	Service detection	1		

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet                  stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                   dgram  udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
#shell                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
#login                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i
```

Per risolvere la seguente criticità abbiamo commentato sulla linea di “**login**” e “**exec**” .

Successivamente abbiamo fatto il restart del servizio “**xinetd**”.

## “RISOLUZIONE DELLE CRITICITA’ RELATIVI ALLA VULNERABILITA’ BIND SHELL BACKDOOR DETECTION”

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.

```
root@metasploitable:/home/msfadmin# sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```

Questa criticità è stata risolta andando a chiudere la porta “**tcp:1524**” attraverso la riga di comando sovrastante.

La non risoluzione della seguente criticità avrebbe potuto permettere la connessione di un attaccante da porta remota il quale avrebbe potuto modificare, cancellare o inviare comandi direttamente.



Inoltre avrebbe potuto inserire un codice malevolo .

```

Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:CA:2B:54 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds

```

Come si può evincere dall'immagine sovrastante è stato eseguito un comando `<<nmap>>` per controllare che la porta **“tcp:1524”** risultasse effettivamente **“filtrata”** dal **“firewall”**.

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Bac...	Backdoors	1	
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported S...	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating ...	General	1	
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'pas...	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 a...	Service detection	2	
<input type="checkbox"/>	MIXED	...	...	 DNS (Multi...	DNS	4	
<input type="checkbox"/>	CRITICAL	...	...	 SSL (Multip...	Gain a shell remotely	3	
<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service D...	Service detection	1	

Successivamente è stato eseguito un controllo ulteriore attraverso **NESSUS** per controllare che la **vulnerabilità** fosse del tutto **INATTIVA**

# “RISOLUZIONE DELLA CRITICITA’ : NFS EXPORTED SHARE INFORMATION DISCLOSURE”

Filter	Search Vulnerabilities	Q	57 Vulnerabilities				
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	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	⊙	✎
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	⊙	✎
<input type="checkbox"/> MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	⊙	✎
<input type="checkbox"/> CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	⊙	✎
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	⊙	✎
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	⊙	✎
<input type="checkbox"/> MIXED	...	...	SSL (Multiple Issues)	ISC Bind (Multiple Issues)	28	⊙	✎

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.

### Output

The following NFS shares could be mounted :

```
+ /
+ Contents of / :
- .
- ..
- 7E,UTW.}R
- bin
- boot
more...
```

To see debug logs, please visit individual host

Port

Hosts

2049 / udp / rpc-nfs

192.168.49.101



```

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

# /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)
#
/mnt/mysgareddir 192.168.49.0/24(rw,sync,root_squash,no_subtree_check)

[ Read 12 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   ^V Next Page  ^U UnCut Text  ^T To Spell

```

Questa criticità è stata risolta limitando gli accessi ai soli utenti sotto lo stesso **Network** così da impedire a utenti esterni l'accesso.

La non risoluzione di questa problematica avrebbe potuto permettere ad un attaccante sia la lettura che la scrittura dei file da un host remoto.

## “SCANNER FINALE CON LE CRITICITA’ RISOLTE NON PIU’ “ IDENTIFICATE”

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	
MIXED	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	4	
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	
MIXED	...	...	PHP (Multiple Issues)	CGI abuses	3	
HIGH	8.3		CGI Generic SQL Injection (blind)	CGI abuses	1	
HIGH	7.5 *		CGI Generic Command Execution	CGI abuses	1	
HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses	1	
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5	
MIXED	...	...	Twiki (Multiple Issues)	CGI abuses	2	
MEDIUM	6.8 *		CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1	

Come possiamo vedere le criticità che abbiamo risolto non vengono visualizzate all'interno della scansione eseguita successivamente all'applicazione delle risoluzioni delle medesime.

