

CONSEGNA ESERCIZIO S5L5

RISOLUZIONE VULNERABILITA' VNC SERVER

The screenshot displays the Nessus Essentials interface within a Kali Linux virtual machine. The main window shows a vulnerability report for the VNC Server 'password' Password. The report is categorized as 'CRITICAL' and includes a description, solution, output, and plugin details.

SCANSIONE PER ESERCIZIO ESAME S5L5 / Plugin #61708

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	192.168.50.101

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

Tenable News

- D-Link D-View 8 Unauthenticated Probe-Core Server ...

Per risolvere la seguente criticità siamo andati a variare la **password del server VNC** mettendone una più sicura in modo da non permettere ad un attaccante di entrare con facilità.

RISOLUZIONE VULNERABILITA' "RLOGIN SERVICE DETECTION" E "RSH SERVICE DETECTION"

<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 reso commenti la linea di **login** e **exec**, rendendole quindi **#login** e **#exec**.

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

RISOLUZIONE DELLA 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.

```
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 possiamo dall'immagine di sopra è stato eseguito un comando <<nmap>> per controllare che la porta **tcp:1524** risultasse effettivamente **filtered** 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 scomparsa.

RISOLUZIONE DELLA CRITICITA' : NFS EXPORTED SHARE INFORMATION DISCLOSURE

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   ^U Next Page  ^U UnCut Text ^T To Spell
[ Icons ] CTRL (DESTRA)
```

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