

Procediamo con la configurazione della nostra macchina virtuale Metasploitable:IP192.168.50.101

1)Prima vulnerabilità :

The screenshot shows a Nessus vulnerability scan report for a VNC Server. The title is "CRITICAL VNC Server 'password' Password". The description states: "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." The solution is to "Secure the VNC service with a strong password." The output shows "Nessus logged in using a password of 'password'." The risk information indicates a "Risk Factor: Critical" and a "CVSS v2.0 Base Score: 10.0".

Port	Hosts
5900 / tcp / vnc	192.168.50.101

Apriamo la macchina virtuale e seguiamo i seguenti passaggi:

a)digitiamo :- sudo su→ vncpasswd\_(impostiamo la password)

b)dopo di che :

```
use 'fg' to return to nano.

[2]+  Stopped                  sudo nano /etc/exports
root@metasploitable:/home/msfadmin# sudo su
root@metasploitable:/home/msfadmin# sudo nano /etc/exports
```

c)andiamo sul file exports sempre con sudo su:

Inseriamo al posto dell'asterisco l'IP della nostra macchina (192.168.50.101)

```
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)
#
/      192.168.50.101(rw,sync,no_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
```

2)

51988  
shell

Bind

Vulnerabilities	
51988 - Bind Shell Backdoor Detection	
Synopsis	The remote host may have been compromised.
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.
Risk Factor	
Critical	
CVSS v3.0 Base Score	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS v2.0 Base Score	
192.168.50.101	4

Backdoor detection.

Eseguiamo questo comando con il quale specifichiamo che dall'IP di Kali qualsiasi tcp venga Droppato sulla porta interessata.(1524)

```
Chain OUTPUT (policy ACCEPT)
target      prot opt source                               destination
root@metasploitable:/home/msfadmin# sudo iptables -I INPUT -p tcp -s 192.168.50.100 --dport 1524 -j DROP_
```

3)11356 -  
Exported

NFS  
Share

11356 - NFS Exported Share Information Disclosure	
Synopsis	It is possible to access NFS shares on the remote host.
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.
Risk Factor	
Critical	
CVSS v2.0 Base Score	10.0 (CVSS2:BAV:N/AC:L/Au:N/C:C/I:C/A:C)
References	CVE-1999-0170 CVE-1999-0211 CVE-1999-0554
Exploitable With	Metasploit (true)
Plugin Information	Published: 2003/02/12, Modified: 2018/09/17
Plugin Output	udp/2049/tcp-nfs

Information Disclosure

Lo abbiamo risolto nel punto 1 inserendo l'ip di Meta.