BYTE REBELS

PROJECT
S5-L5

CANNAVACCIUOLO DAVIDE
DI MAIO PAOLO
FORLENZA SIMONE
RUSSO FEDERICO - LEADER
TIZZI FEDERICO
VAN ZWAM ARJEN

Nessus
vulnerability scanner

TRACE

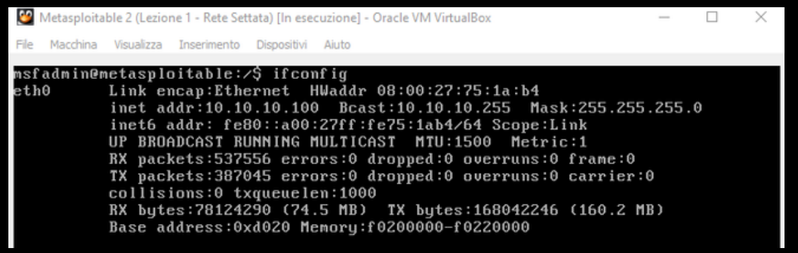
Perform a full scan on the Metasploitable target.
Choose from a minimum of 2 up to a maximum of 4 critical / high vulnerabilities and try to implement remediation actions.
N.B. the remedial actions, at this stage, could also be well-configured firewall rules in order to possibly limit the exposure of vulnerable services.
However, we recommend that you perhaps use this approach for no more than one vulnerability.
To demonstrate the effectiveness of the remediation actions, scan the target again and compare the results with those previously obtained.
For the purposes of the solution, we have chosen the vulnerabilities in yellow in the figure on slide 3.

INITIAL CONFIG

S5-L5

INITIAL CONFIGURATION
OF THE LOCAL NETWORK FOR COMPLETELY
SAFE AND NON-INVASIVE TESTS

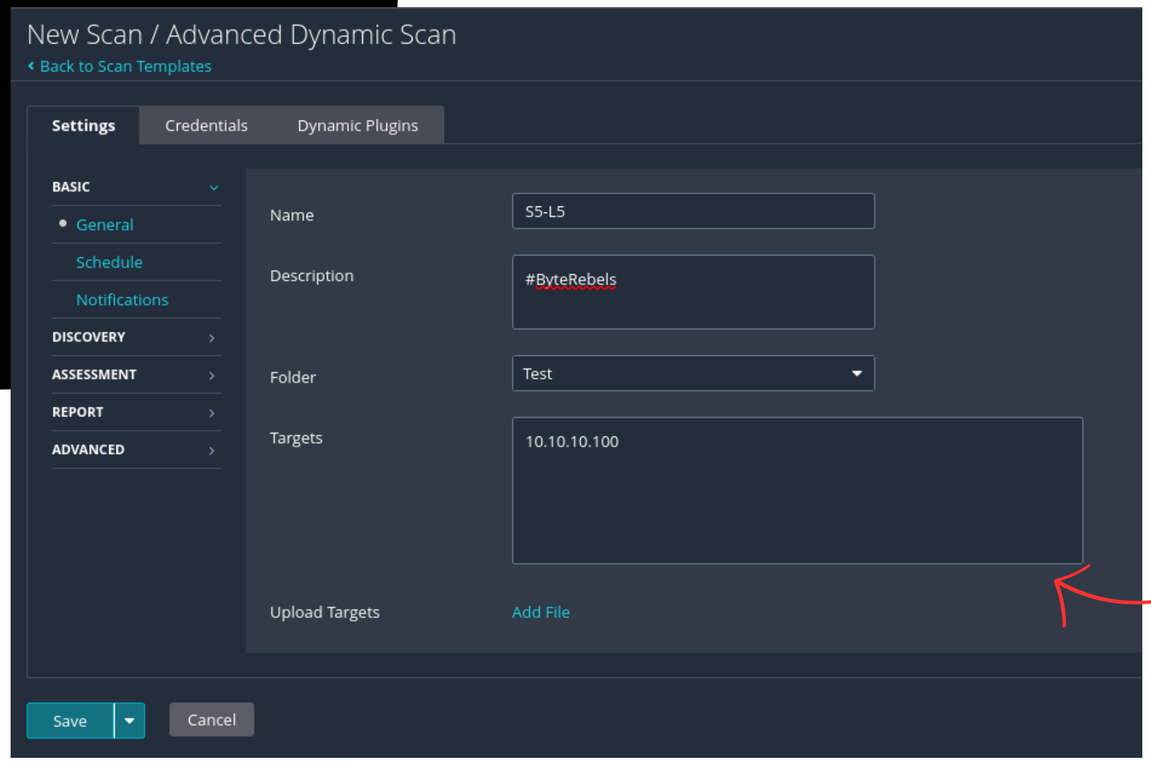
Pf Sense:
LAN1 (rete kali) 192.168.1.1/24
LAN2 (rete meta) 10.10.10.1/24

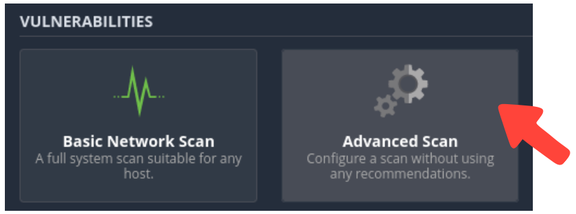


Metasploitable2:
10.10.10.100

Kali:
192.168.1.100

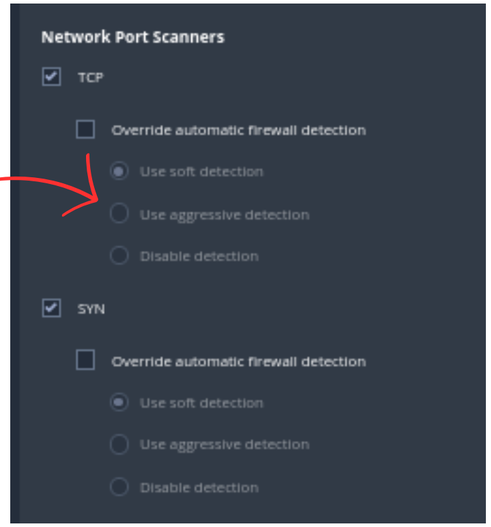
NEW SCAN SETTINGS

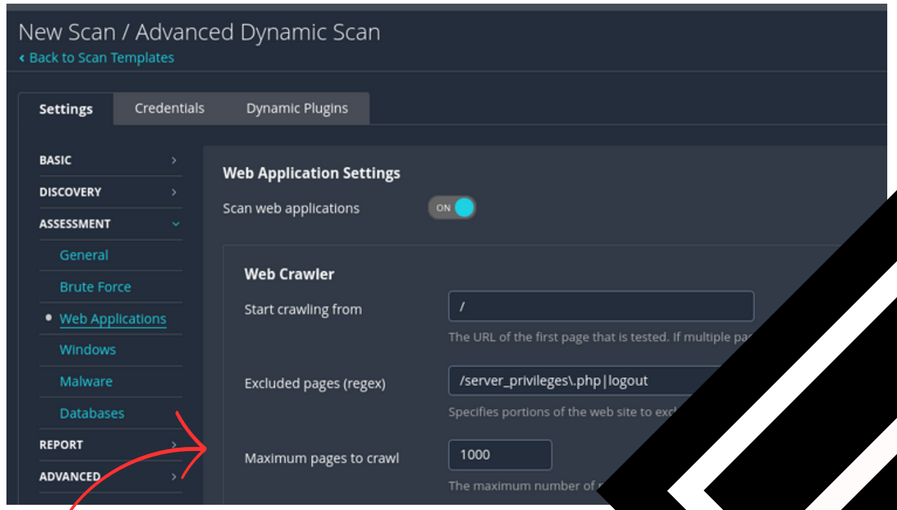




To start looking for a new scan we first of all set the correct parameters for the Metasploitable2 ***Host*** *scan as shown in the figure.*
By entering the Meta2 ***IP*** *as target*

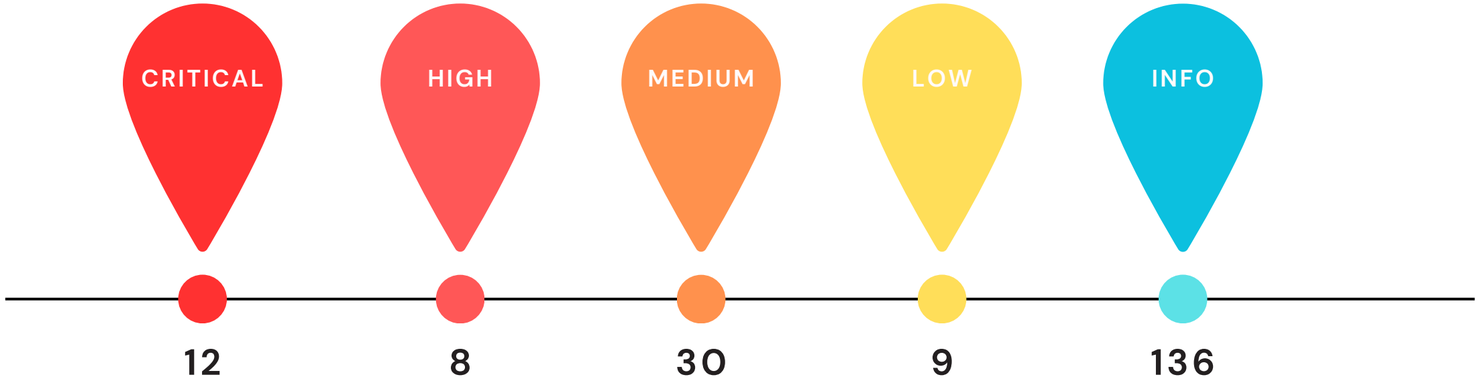
And consequently the typology of Port Scanner to use, inserting the ***TCP*** *IN ADDITION to* ***SYN***





Enabling scanning also for ***Web applications***

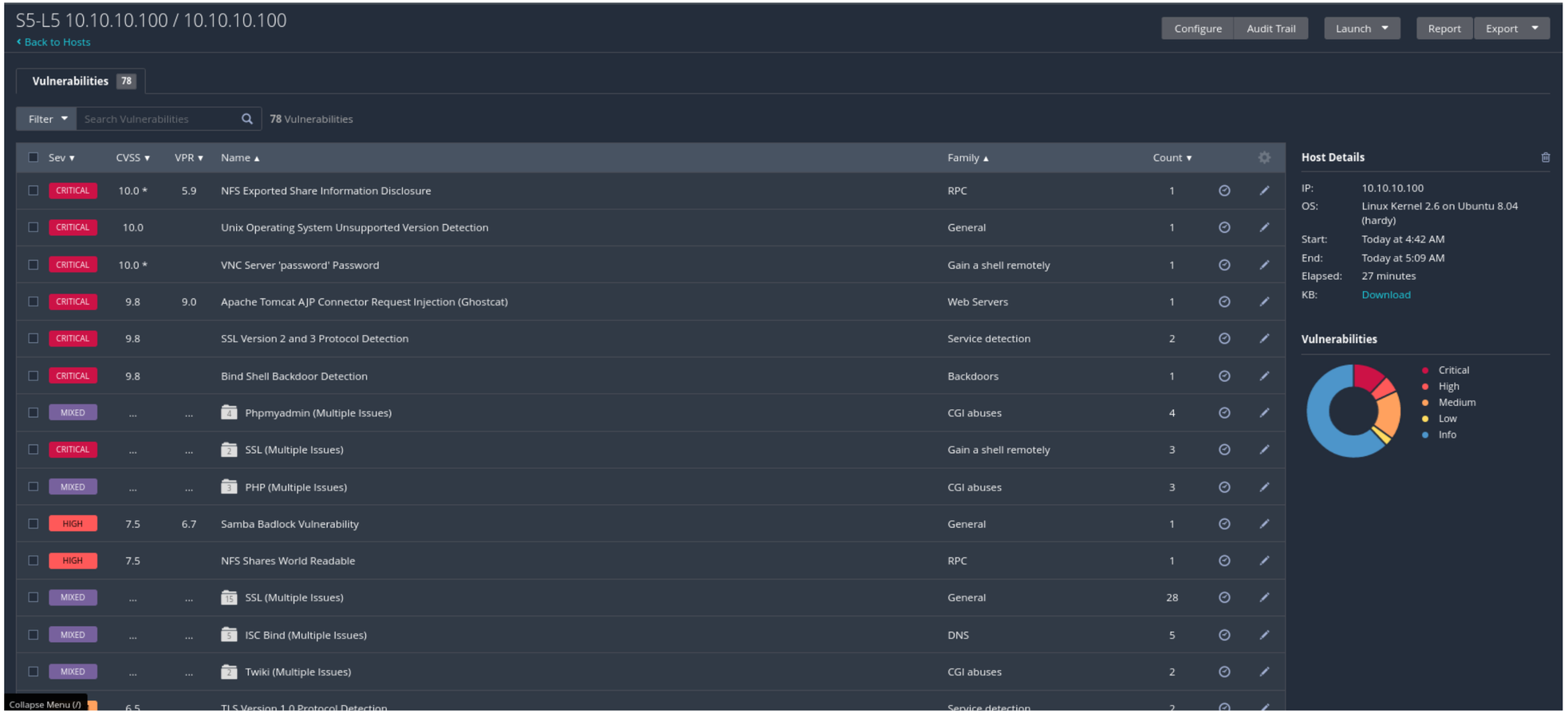
VULNERABILITIES FOUND



Obviously the Meta2 Host was deliberately created **hyper-vulnerable**, despite this we found "only" **12 CRITICAL** and **8 HIGH**

VULNERABILITIES FOUND

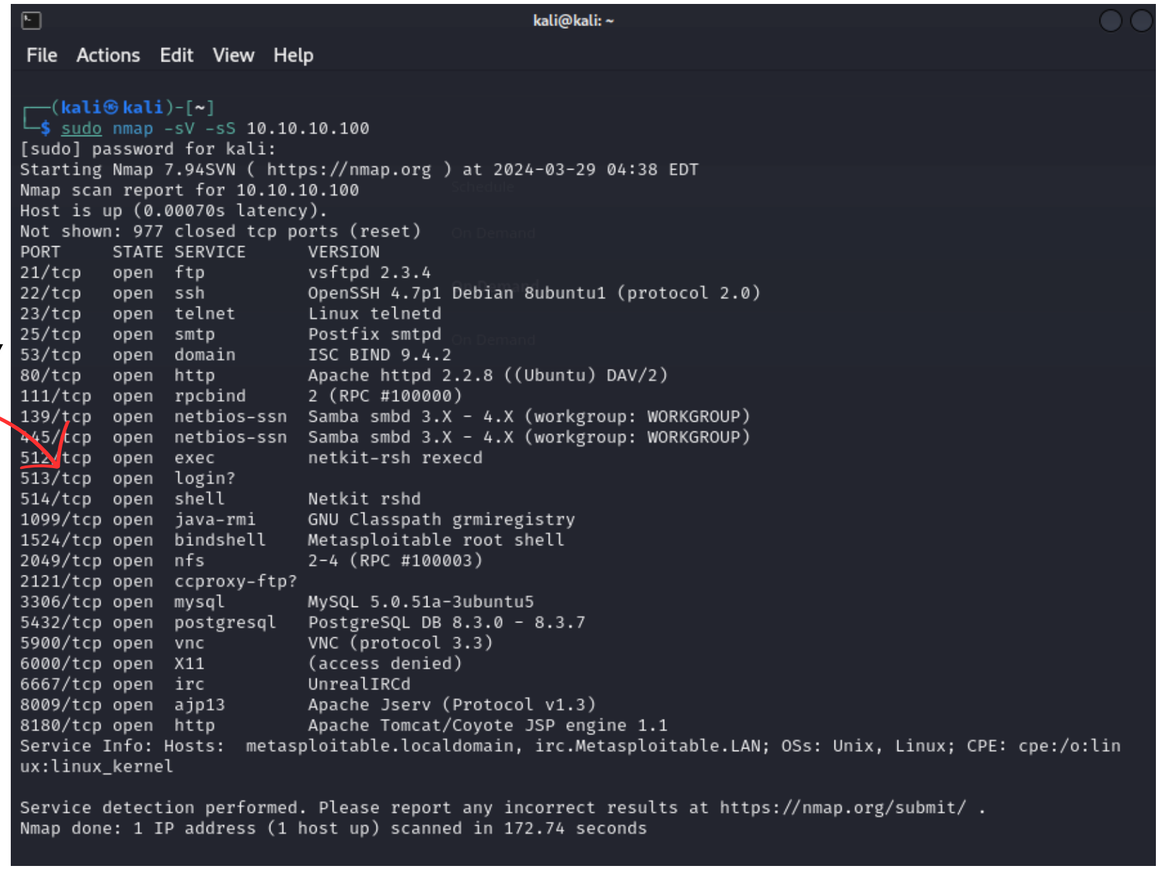
This is the report in detail of the **main vulnerabilities** found:



SCAN NMAP

To make sure we didn't miss anything, we ran a quick scan with **Nmap** on target 10.10.10.100

*Finding all of them accordingly the **port** listening*



REMEDIATION ACTION

1. NFS EXPORTED SHARE INFORMATION DISCLOSURE
   CRITICAL

2. VNC SERVER 'PASSWORD' PASSWORD
   CRITICAL

3. BIND SHELL BACKDOOR DETECTION
   CRITICAL

NFS Exported Share Information Disclosure

CRITICAL

1 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.*

2 SOLUTION

*Configure **NFS** on the remote host so that only authorized hosts can mount its remote shares.*

3 OUTPUT

The following NFS shares could be mounted :

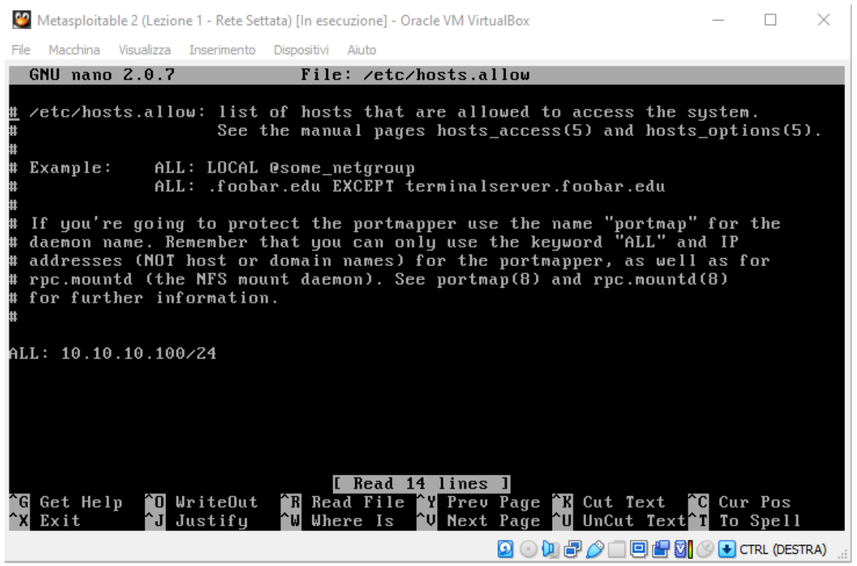
```
+ /
  + Contents of / :
- .
- ..
- bin        -home          -media       -root    -usr
- boot       -initrd        -mnt         -sbin    -var
- cdrom      -initrd.img    -nohup.out   -srv     -vmlinuz
- dev        -lib           -opt         -sys
- etc        -lost+found    -proc        -tmp
```

NFS Exported Share Information Disclosure

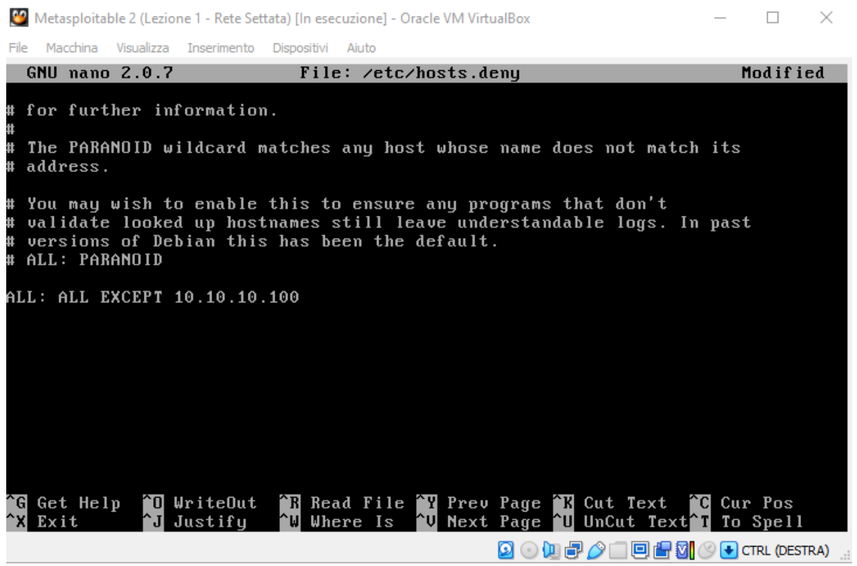
CRITICAL

RESOLUTION

*The /etc/hosts.**allow** and /etc/hosts.**deny** files are commonly used with SSH and TCP wrappers.*
We therefore edited the two files so as not to make them accessible from the outside.



*FILE **hosts.allow***
ALL: 10.10.10.100/24



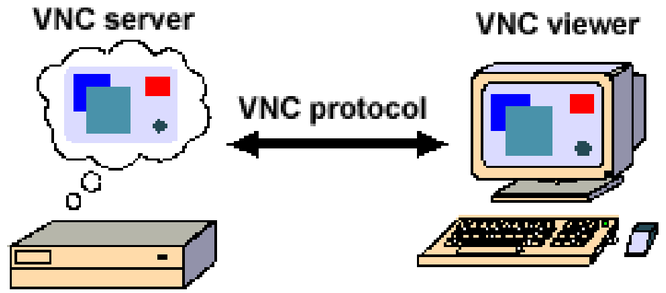
*FILE **hosts.deny***
ALL: ALL EXCEPT 10.10.10.100/24

VNC Server 'password' Password

CRITICAL

1 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.*



2 SOLUTION

*Secure the **VNC** service with a strong password.*

3 OUTPUT

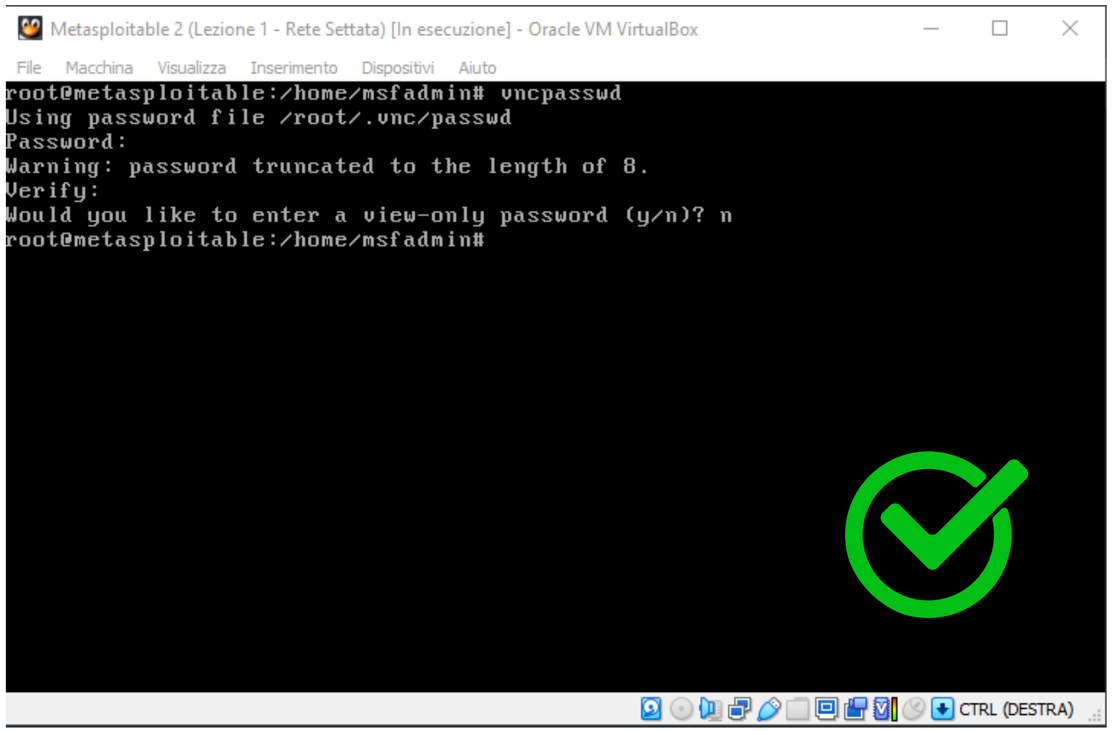
Nessus logged in using a password of "password".

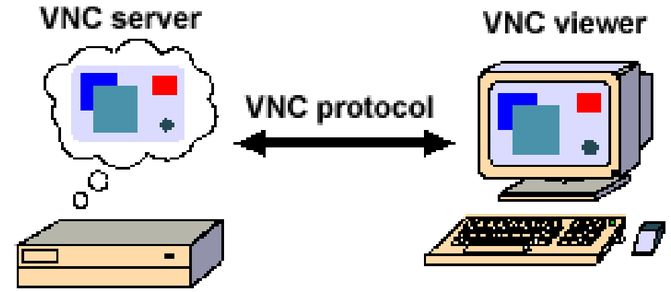
VNC Server 'password' Password

CRITICAL

RESOLUTION

Very simply we changed the default password
via the command: ***vncpasswd***



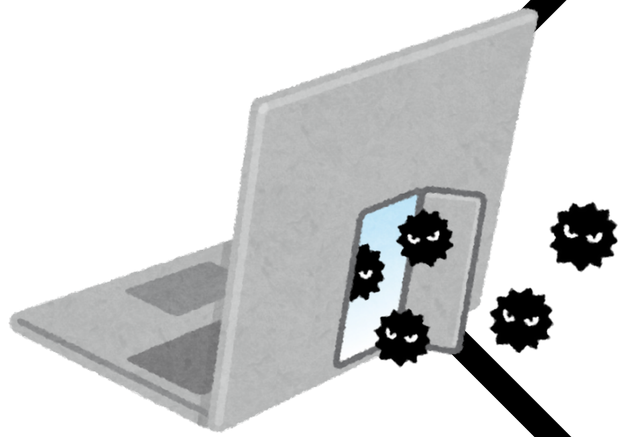


Bind Shell Backdoor Detection

CRITICAL

1 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.*



2 SOLUTION

Verify if the remote host has been compromised, and reinstall the system if necessary.

3 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 ------------------------------
```

Bind Shell Backdoor Detection

CRITICAL

RESOLUTION

*After establishing with **nmap** that the open Bind Shell port was **1524***

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sS 10.10.10.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 04:38 EDT
Nmap scan report for 10.10.10.100
Host is up (0.00070s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet       Linux telnetd
25/tcp   open  smtp         Postfix smtpd
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec         netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell        Netkit rshd
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe
ux:linux_kernel
```

We therefore proceeded to close it for all the other hosts with the command:
sudo iptables -A INPUT -p tcp --dport 1524 -j DROP

```
Metasploitable 2 (Lezione 1 - Rete Settata) [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
                                        network interface name ([+] for wildcard)
  --table       -t table               table to manipulate (default: `filter')
  --verbose     -v                     verbose mode
  --line-numbers                       print line numbers when listing
  --exact       -x                     expand numbers (display exact values)
[!] --fragment  -f                     match second or further fragments only
  --modprobe=<command>                 try to insert modules using this command
  --set-counters PKTS BYTES            set the counter during insert/append
[!] --version   -V                     print package version.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$ iptables -L
iptables v1.3.8: can't initialize iptables table `filter': Permission denied (yo
u must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$
CTRL (DESTRA)
```

*We tried the command again with **Nmap** and rightly port 1524 is now **filtered***

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ sudo nmap -sV -T5 10.10.10.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 06:40 EDT
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 06:43 (0:00:00 remaining)
Nmap scan report for 10.10.10.100
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet       Linux telnetd
25/tcp   open     smtp         Postfix smtpd
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec         netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell        Netkit rshd
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ccproxy-ftp?
3306/tcp open     mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
pe:/o:linux:linux_kernel
```

MISCELLANEOUS..

1 CRITICAL

APACHE TOMCAT AJP CONNECTOR REQUEST INJECTION (GHOSTCAT)

2 CRITICAL

SSL VERSION 2 AND 3 PROTOCOL DETECTION

3 CRITICAL

UNIX OPERATING SYSTEM UNSUPPORTED VERSION DETECTION

4 CRITICAL

PHPMYADMIN PRIOR TO 4.8.6 SQLI VULNERABLITY (PMASA-2019-3)

5 HIGH

SAMBA BADLOCK VULNERABILITY

6 HIGH

ISC BIND SERVICE DOWNGRADE / REFLECTED DOS

ATTENTION

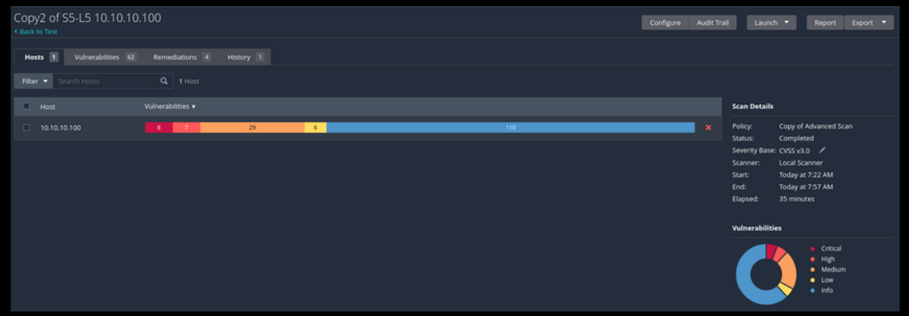
*We have also found other vulnerabilities which, in order to be resolved, would **simply** be necessary to update the services to which they refer.*

Often, just by keeping the tools, services and OS updated we significantly reduce vulnerabilities!!

CONCLUSION

At the end of all the remediation actions we tried the scan advanced by **Nessus** again and with enormous satisfaction we found that the vulnerabilities
they have all been previous **SOLVED**.

New Scan



New Scan