

BYTE REBELS



PROJECT S5-L5

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



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.



<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

INITIAL CONFIG

S5-L5

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

```
PF Sense [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: eec1a128b05733668b9c

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
LAN2 (opt1)    -> em2      -> v4: 10.10.10.1/24
```

Pf Sense:

LAN1 (rete kali) 192.168.1.1/24

LAN2 (rete meta) 10.10.10.1/24

.....

```
Metasploitable 2 (Lezione 1 - Rete Settata) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

msfadmin@metasploitable:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:75:1a:b4
          inet addr:10.10.10.100 Bcast:10.10.10.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe75:1ab4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:537556 errors:0 dropped:0 overruns:0 frame:0
          TX packets:387045 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:78124290 (74.5 MB)  TX bytes:168042246 (160.2 MB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Metasploitable2:

10.10.10.100

.....

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)~[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.100/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::a00:27ff:fe21:b1d0/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Kali:

192.168.1.100

New Scan / Advanced Dynamic Scan

[Back to Scan Templates](#)

Settings Credentials Dynamic Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: S5-L5

Description: #ByteRebels

Folder: Test

Targets: 10.10.10.100

Upload Targets Add File

Save Cancel

NEW SCAN SETTINGS

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

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**

Network Port Scanners

☒ TCP

☐ Override automatic firewall detection

☒ Use soft detection

☐ Use aggressive detection

☐ Disable detection

☒ SYN

☐ Override automatic firewall detection

☒ Use soft detection

☐ Use aggressive detection

☐ Disable detection

New Scan / Advanced Dynamic Scan

[Back to Scan Templates](#)

Settings Credentials Dynamic Plugins

BASIC

DISCOVERY

ASSESSMENT

General

Brute Force

Web Applications

Windows

Malware

Databases

REPORT

ADVANCED

Web Application Settings

Scan web applications ☒

Web Crawler

Start crawling from: /

The URL of the first page that is tested. If multiple pages are specified, they will be crawled in order.

Excluded pages (regex): /server_privileges.php|logout

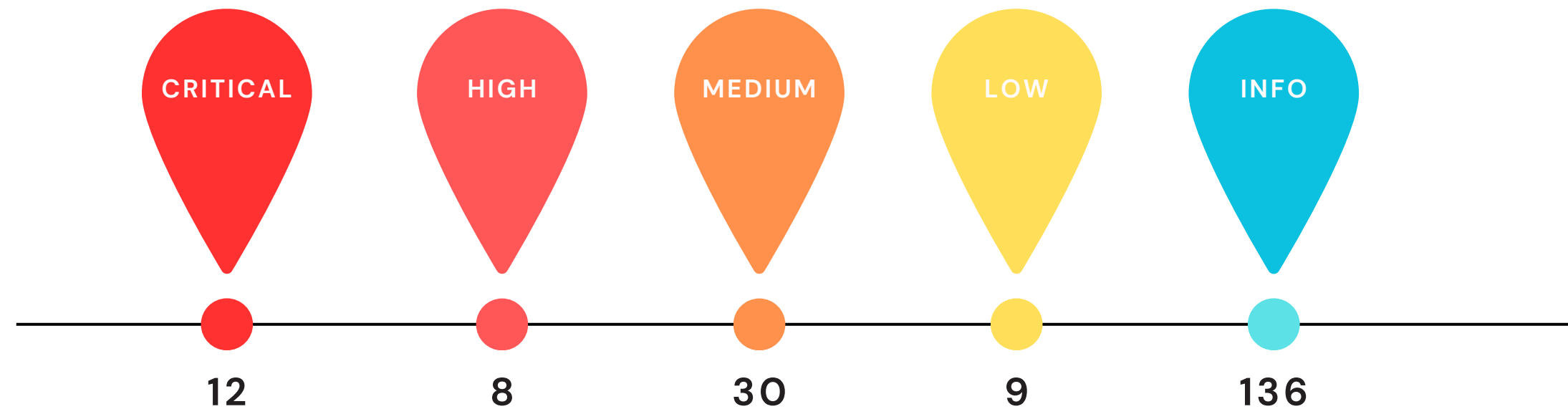
Specifies portions of the web site to exclude from crawling.

Maximum pages to crawl: 1000

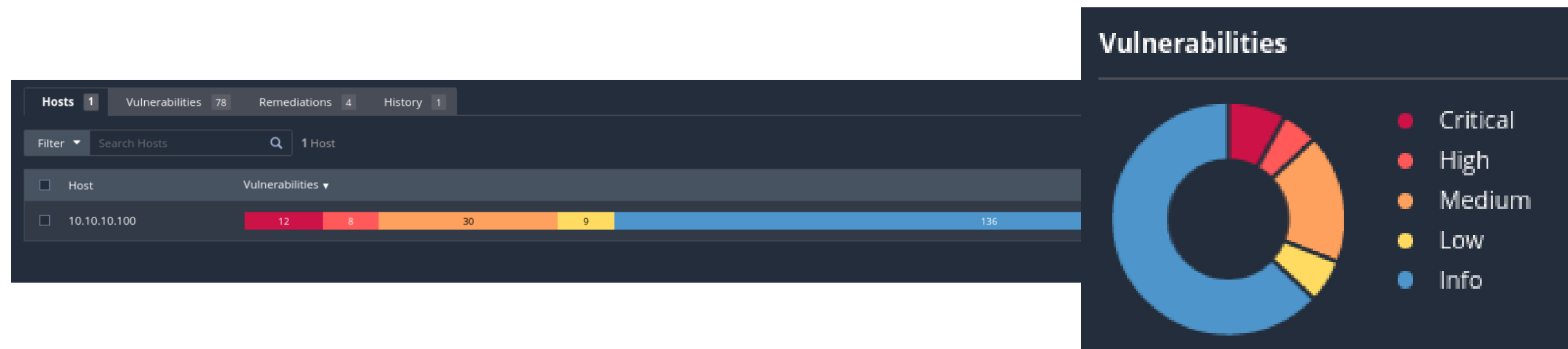
The maximum number of pages to crawl.

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:

CRITICAL

HIGH

MEDIUM

LOW

INFO

S5-L5 10.10.10.100 / 10.10.10.100

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities78

Filter

Search Vulnerabilities

78 Vulnerabilities

<input type="checkbox"/>	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	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	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	Phpmyadmin (Multiple Issues)	CGI abuses	4		
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/>	MIXED	PHP (Multiple Issues)	CGI abuses	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)	General	28		
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5		
<input type="checkbox"/>	MIXED	Twiki (Multiple Issues)	CGI abuses	2		
<input type="checkbox"/>		6.5		TLS Version 1.0 Protocol Detection	Service detection	2		

Host Details

IP:10.10.10.100

OS:Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start:Today at 4:42 AM

End:Today at 5:09 AM

Elapsed:27 minutes

KB:[Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

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

```
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:/o:lin  
ux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 172.74 seconds
```



REMEDIATION ACTION

1

CRITICAL

NFS EXPORTED SHARE
INFORMATION DISCLOSURE

2

CRITICAL

VNC SERVER
'PASSWORD' PASSWORD

3

CRITICAL

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.

```
Metasploitable 2 (Lezione 1 - Rete Settata) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:  ALL: LOCAL @some_netgroup
#          ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
ALL: 10.10.10.100/24
[ Read 14 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

FILE `hosts.allow`
ALL: 10.10.10.100/24

```
Metasploitable 2 (Lezione 1 - Rete Settata) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/hosts.deny Modified
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL: ALL EXCEPT 10.10.10.100
^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

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

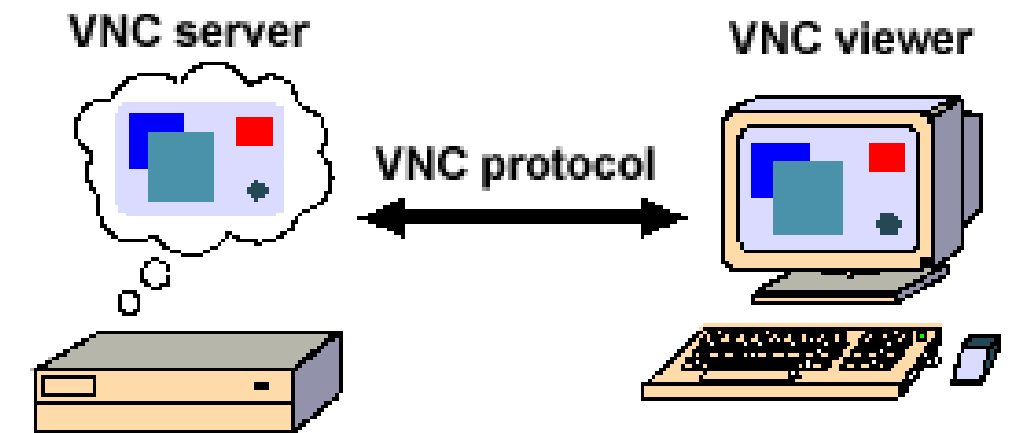
SOLUTION

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

3

OUTPUT

Nessus logged in using a password of "password".





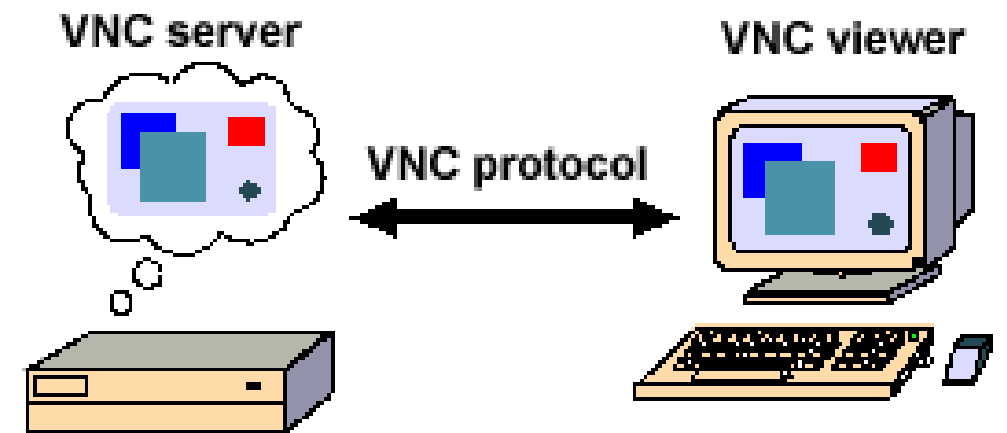

VNC Server 'password' Password

CRITICAL

RESOLUTION

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

```
Metasploitable 2 (Lezione 1 - Rete Settata) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```





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

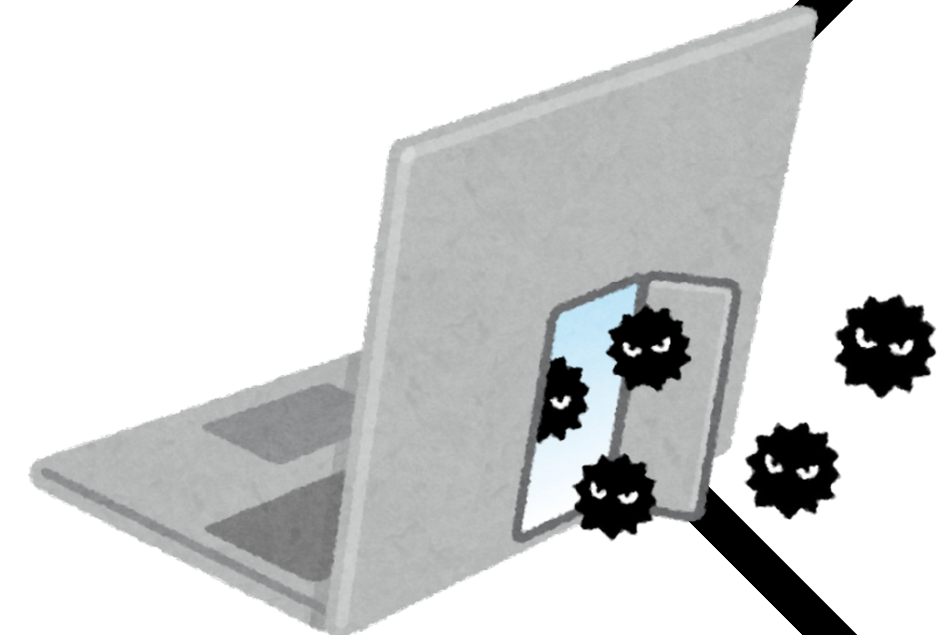
Nessus was able to execute the command "id" using the following request :

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

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

RESOLUTION

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

```
kali@kali: ~  
File Actions Edit View Help  
$ 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:/o:linux:linux_kernel
```

```
Metasploitable 2 (Lezione 1 - Rete Settata) [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
--table -t table      network interface name ([+] for wildcard)  
--verbose -v          table to manipulate (default: 'filter')  
--line-numbers        verbose mode  
--exact -x            print line numbers when listing  
[!] --fragment -f     expand numbers (display exact values)  
--modprobe=<command> match second or further fragments only  
--set-counters PKTS BYTES try to insert modules using this command  
[!] --version -V      set the counter during insert/append  
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 (you 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 tcp dpt:ingreslock  
DROP tcp -- anywhere tcp dpt:ingreslock  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
msfadmin@metasploitable:~$
```

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



```
kali@kali: ~  
File Actions Edit View Help  
$ sudo nmap -sV -TS 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
```



Apache Tomcat AJP Connector Request Injection (Ghostcat)

CRITICAL

1

DESCRIPTION

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

2

SOLUTION

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.





Apache Tomcat AJP Connector Request Injection (Ghostcat)

CRITICAL

1

SOLUTION

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.





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
VULNERABILITY (PMASA-2019-3)

5

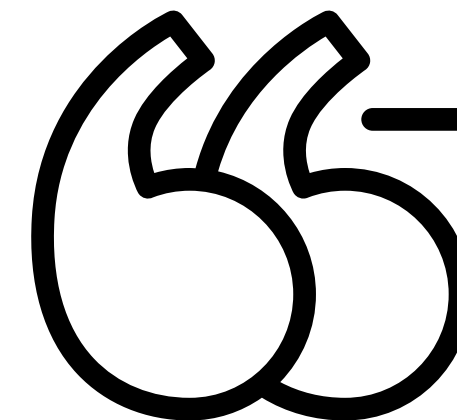
HIGH

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.*

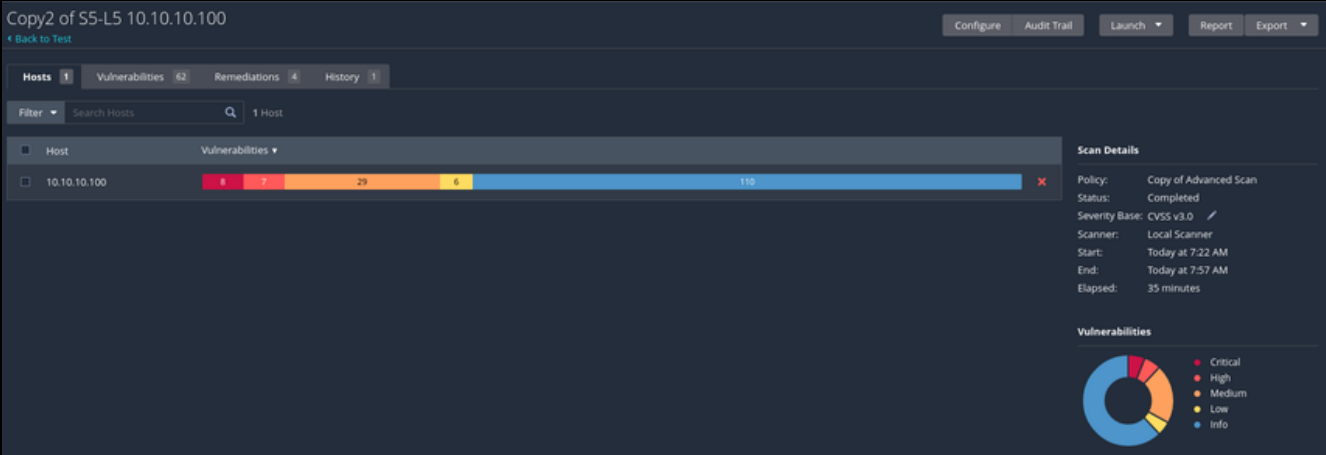
Often, just by keeping the tools, services and OS updated we significantly reduce vulnerabilities!!



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

