

BYTE REBELS



PROGETTO S5-L5

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



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.



<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

CONFIG INIZIALE

S5-L5

CONFIGURAZIONE INIZIALE
DELLA RETE LOCALE PER I TEST IN TOTALE
SICUREZZA E NON INVASIVI

```
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

IMPOSTAZIONI NUOVA SCANSIONE

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

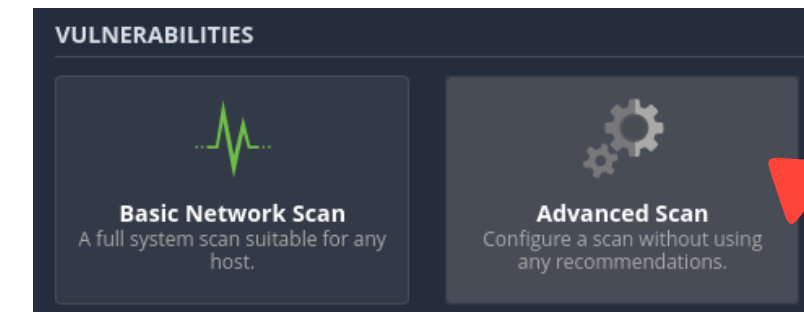
Folder: Test

Targets: 10.10.10.100

Upload Targets Add File

Save Cancel

Per iniziare a cercare una nuova scansione abbiamo prima di tutto impostato i parametri corretti per lo scan dell'**Host** Metasploitable2 come in figura.
Inserendo come target l'**IP** di Meta2



E di conseguenza la tipologia di Port Scanner da utilizzare, inserendo OLTRE a **SYN** anche la **TCP**

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: ON

Web Crawler

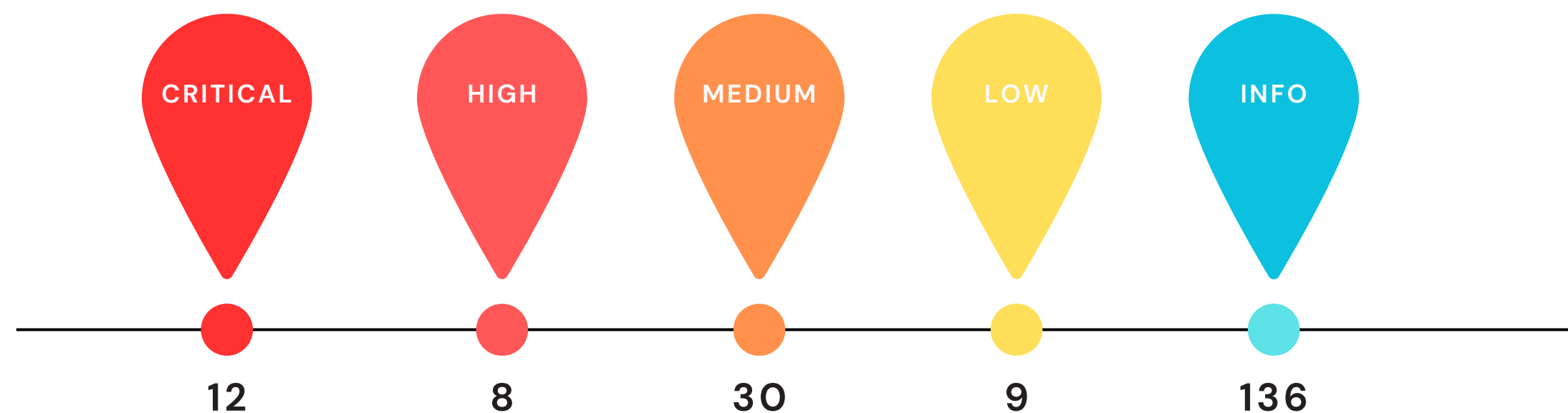
Start crawling from: /

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

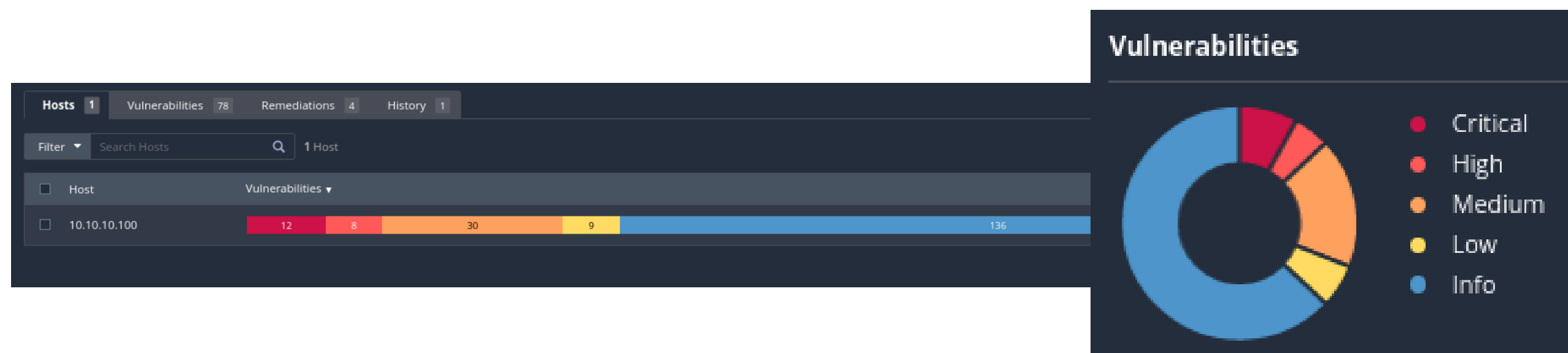
Maximum pages to crawl: 1000

Abilitando lo scan anche per le **Web applications**

VULNERABILITA' TROVATE



Ovviamente l'Host Meta2 è stato creato volutamente **iper-vulnerabile**, nonostante ciò abbiamo riscontrato *"solamente"* **12 CRITICAL** e **8 HIGH**



VULNERABILITA' TROVATE

Questo è il report in dettaglio delle main **vulnerabilità** riscontrate:

CRITICAL HIGH MEDIUM LOW INFO

S5-L5 10.10.10.100 / 10.10.10.100

Configure Audit Trail Launch Report Export

Vulnerabilities 78

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	4 Phpmyadmin (Multiple Issues)	CGI abuses	4	
<input type="checkbox"/> CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/> MIXED	3 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	15 SSL (Multiple Issues)	General	28	
<input type="checkbox"/> MIXED	5 ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/> MIXED	2 Twiki (Multiple Issues)	CGI abuses	2	
<input type="checkbox"/> Collapse Menu (1)	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

Per non farci sfuggire nulla, abbiamo eseguito una rapida scansione con **Nmap** sul target 10.10.10.100

Trovando di conseguenza tutte le **porte in ascolto**

```
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

DESCRIZIONE

*Almeno una delle condivisioni **NFS** esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.*

2

SOLUZIONE

*Configura **NFS** sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.*

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



RISOLUZIONE

I file `/etc/hosts.allow` e `/etc/hosts.deny` vengono comunemente utilizzati con i wrapper SSH e TCP. Abbiamo dunque editato i due file per non renderli accessibili dall'esterno.

```
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

DESCRIZIONE

*Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il **controllo** del sistema.*

2

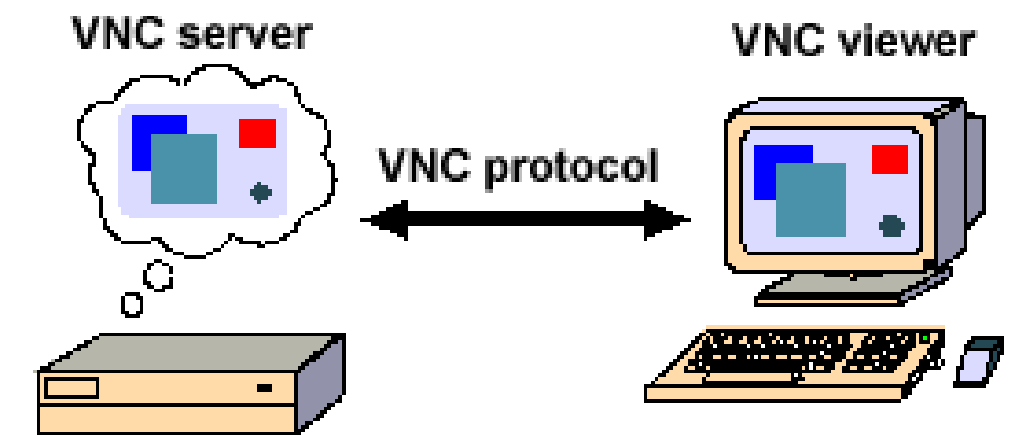
SOLUZIONE

Proteggi il servizio VNC con una password complessa.

3

OUTPUT

Nessus logged in using a password of "password".





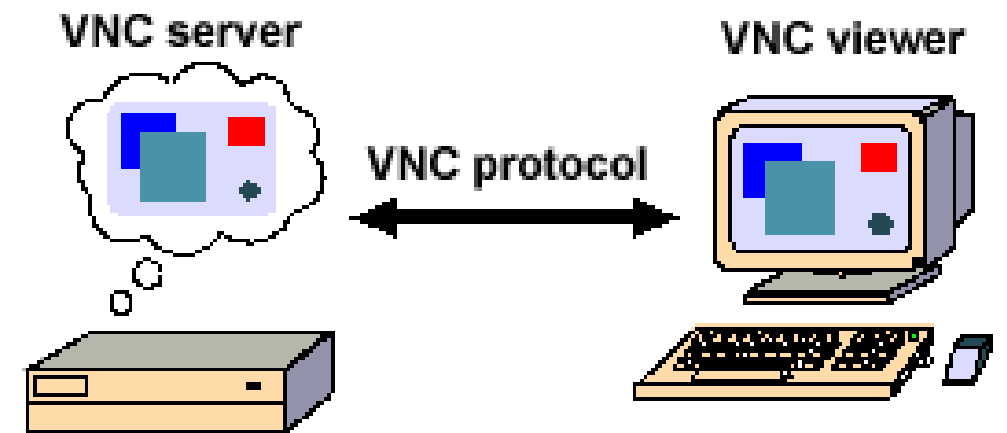

VNC Server 'password' Password

CRITICAL

RISOLUZIONE

*Molto semplicemente abbiamo
cambiato la password di default
tramite il comando: **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

DESCRIZIONE

*Una shell è in ascolto sulla porta remota **senza** che sia richiesta alcuna autenticazione.*

Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

2

SOLUZIONE

Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

3

OUTPUT

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

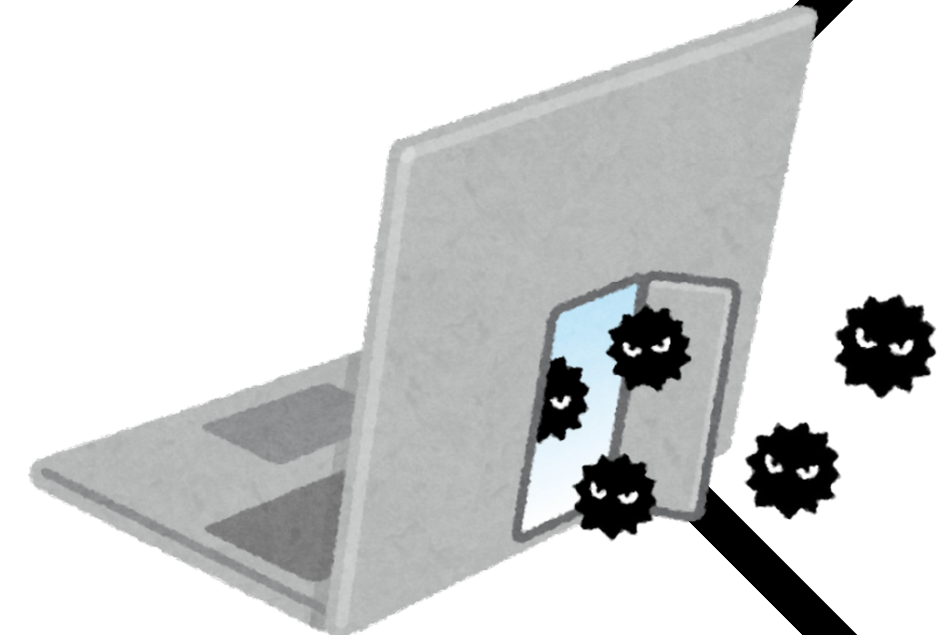
This produced the following truncated output (limited to 10 lines)

----- snip -----

```
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
```

```
root@metasploitable:/#
```

----- snip -----





Bind Shell Backdoor Detection

CRITICAL

Abbiamo proceduto di conseguenza a chiuderla per tutti gli altri host col comando:
`sudo iptables -A INPUT -p tcp --dport 1524 -j DROP`

RISOLUZIONE

Dopo aver stabilito con **`nmap`** che la porta aperta di Bind Shell era la **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:/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:~$
```

Abbiamo riprovato il comando con **`Nmap`** e giustamente la porta 1524 ora è **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
```




ALTRO..



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

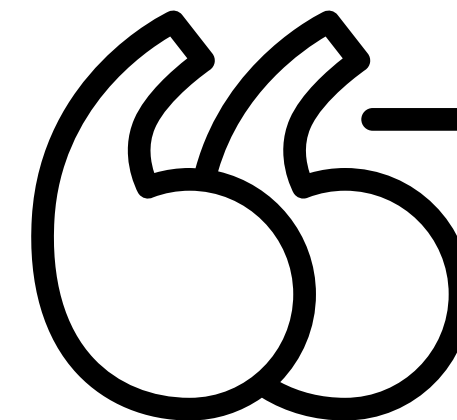
HIGH

SAMBA BADLOCK VULNERABILITY

6

HIGH

ISC BIND SERVICE DOWNGRADE /
REFLECTED DOS



ATTENZIONE

*Abbiamo trovato anche altre vulnerabilità che per essere risolte basterebbe **soltanto** aggiornare i servizi a cui fanno riferimento.*

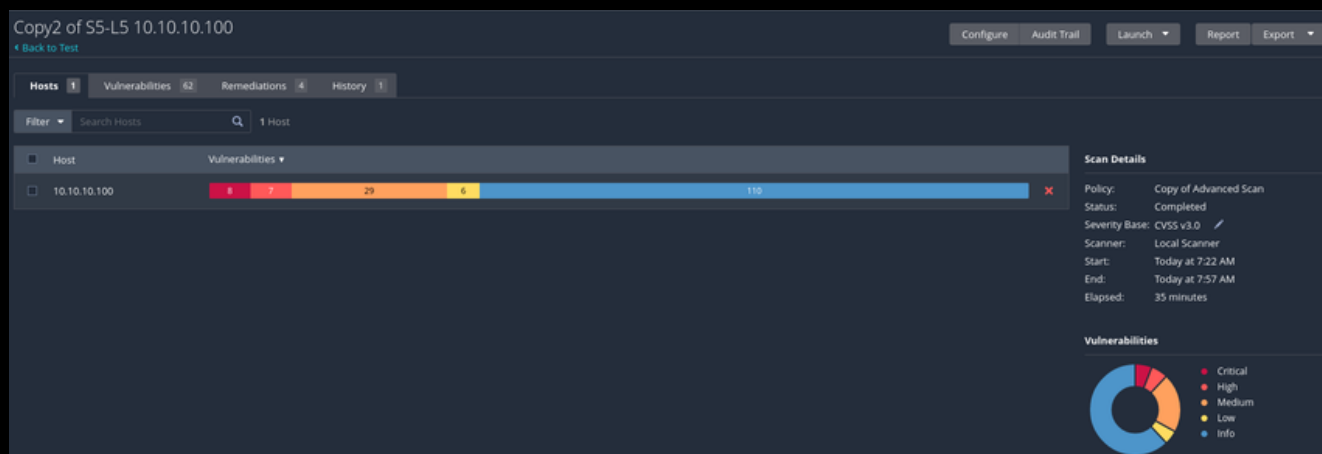
Spesso, solamente mantenendo aggiornati i tools, servizi e SO andiamo ad abbattere notevolmente le vulnerabilità!!



CONCLUSIONI

Al termine di tutte le remediation action abbiamo provato di nuovo lo scan avanzato da **Nessus** e con enorme soddisfazione abbiamo riscontrato che le vulnerabilità precedenti sono state tutte **RISOLTE**.

Nuovo scan



Nuovo scan

Copy2 of S5-L5 10.10.10.100 / 10.10.10.100

Configure Audit Trail Launch Report Export

Back to Hosts

Vulnerabilities 62

Filter Search Vulnerabilities 62 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
CRITICAL	10.0 *	5.1	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	2		
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1		
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
MIXED	Phpmyadmin (Multiple Issues)	CGI abuses	4		
MIXED	PHP (Multiple Issues)	CGI abuses	3		
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1		
MIXED	SSL (Multiple Issues)	General	28		
MIXED	ISC Bind (Multiple Issues)	DNS	5		
MIXED	Twiki (Multiple Issues)	CGI abuses	2		
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2		
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1		

Host Details

IP: 10.10.10.100
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 7:31 AM
End: Today at 7:57 AM
Elapsed: 27 minutes
KB: Download

Vulnerabilities

Critical
High
Medium
Low
Info