

W12D4

## Cyber Security & Ethical Hacking

### Progetto

### [RemediationMeta]

#### ★ INDICE

#### 1 Scansione iniziale Nessus

#### 2 Implementazione delle Azioni di Rimedio (via Telnet)

#### 3 Critical issues resolved

**3.1** vsftpd 2.3.4 Backdoor (porta 21/FTP, Critical - p.702)

**3.2** UnrealIRCd Backdoor (porte 6667/6697/IRC, Critical - p.821)

**3.3** Samba Username Map Script RCE (porte 139/445/SMB, Critical - p.142)

**3.4** Bind Shell Backdoor (porta 1524, Critical - p.96)

**3.5** Opzionale Apache Log4Shell CVE-2021-45046 (porta 80/HTTP, High - p.4-6)

#### 4 Scan nmap delle porte vulnerabili per conferma

**4.1** vsftpd 2.3.4 Backdoor (porta 21/FTP, Critical - p.702)

**4.2** UnrealIRCd Backdoor (porte 6667/6697/IRC, Critical - p.821)

**4.3** Samba Username Map Script RCE (porte 139/445/SMB, Critical - p.142)

**4.4** Bind Shell Backdoor (porta 1524, Critical - p.96)

**4.5** Opzionale Apache Log4Shell CVE-2021-45046 (porta 80/HTTP, High - p.4-6)

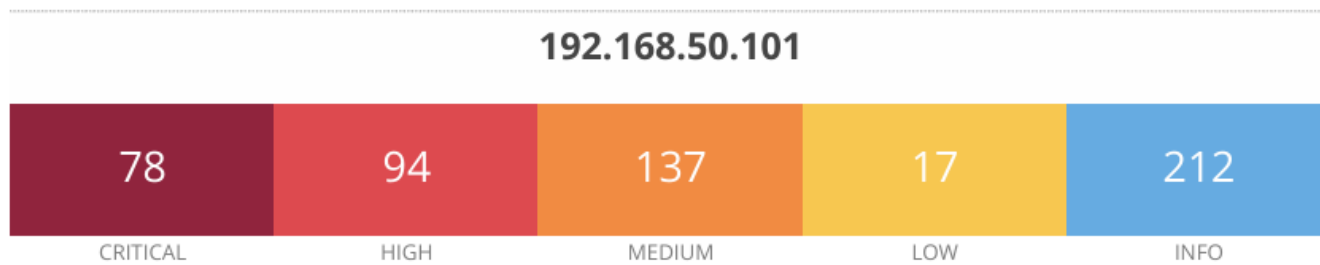
#### 5 Scansione Finale, Confronto e Conclusione

## 1 Scansione iniziale Nessus

### Analisi della Scansione Iniziale (**W12D4\_ Metasploitable2\_1**)

#### Dati dal report:

- ❑ **Grafico** (pagina 4): 78 Critical, 94 High, 137 Medium, 17 Low, 212 Info
- ❑ **Host**: 192.168.50.101 (Metasploitable2), OS Ubuntu 8.04 (kernel 2.6.24)
- ❑ **Scelta vulnerabilità**
  - ⇒ **CRITICAL** nvsftpd 2.3.4 (pagina 702): Versione vulnerabile con backdoor nota (RCE su porta 21/FTP; banner "220 (vsFTPd 2.3.4)")
  - ⇒ **CRITICAL** UnrealIRCd (pagina 821): Processo /usr/bin/unrealircd su porte 6667/6697 (backdoor nota, RCE)
  - ⇒ **CRITICAL** Samba vulnerabilities (pagine 142, 162, 168, 170, 219, 243, 245, 367, 447, 521, 658, 685, 714, 871, 872, 873, 907): Molteplici, inclusa USN-1423-1 (Critical, CVE-2012-2111, RCE/DoS su porte 139/445; versione Samba 3.0.20-Debian)
  - ⇒ **[OPZIONALE - CRITICAL]** Bind Shell Backdoor (pagina 96): Shell aperta su porta 1524 senza autenticazione (Critical, RCE root; Nessus ha eseguito "id" e ottenuto uid=0(root))
  - ⇒ **HIGH** Apache Log4Shell CVE-2021-45046 (High, pagine 4-6): RCE su porta 80/HTTP via Log4j



#### ○ **PDF ALLEGATO: W12D4\_ Metasploitable2\_1**

⇒ **Dettagli PDF:** 909 pagine

## **2 Implementazione delle Azioni di Rimedio (via Telnet)**

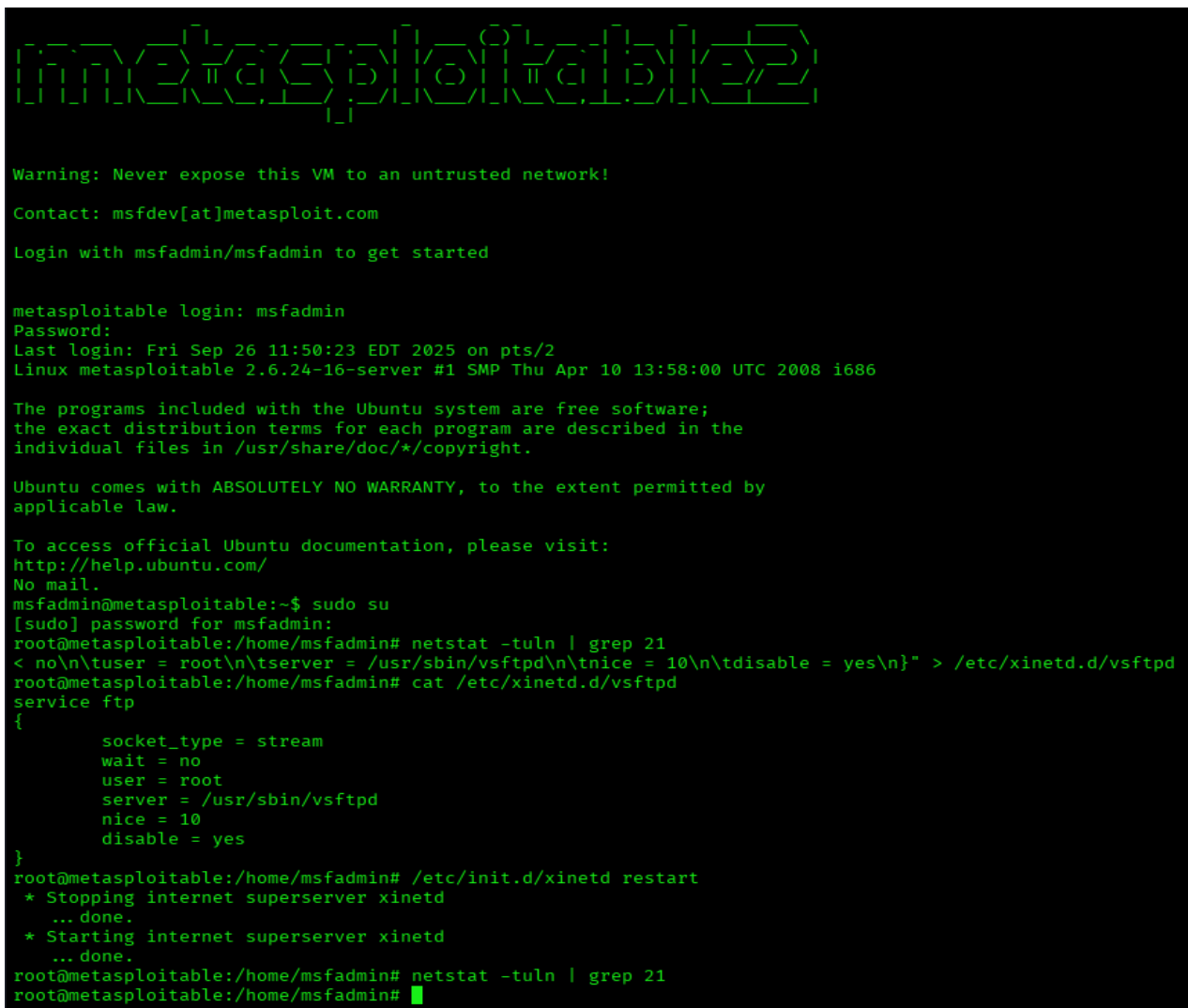
- Accedo a Metasploitable2 da Kali con `telnet 192.168.50.101`
- Poi verifico prima con `netstat -tuln | grep [porta aperta]` per ogni servizio
- Applico il rimedio

### 3 Critical issues resolved

#### 3.1 vsftpd 2.3.4 Backdoor (porta 21/FTP, Critical - p.702)

- ⇒ **Problema** La vulnerabilità consiste in una backdoor nella versione 2.3.4 di vsftpd, che permette l'esecuzione remota di codice (RCE) aprendo una shell su porta 6200 se l'username termina con **attacker:)** Il servizio è esposto sulla porta 21, rendendo il sistema vulnerabile a accessi non autorizzati
- ⇒ **Rimedio** Disabilitare il servizio sovrascrivendo la configurazione in /etc/xinetd.d/vsftpd con **disable = yes**, riavviando xinetd per applicare la modifica e chiudere la porta 21

📸 [Allego screenshot fasi di risoluzione vulnerabilità]



```
metasploitable

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Sep 26 11:50:23 EDT 2025 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

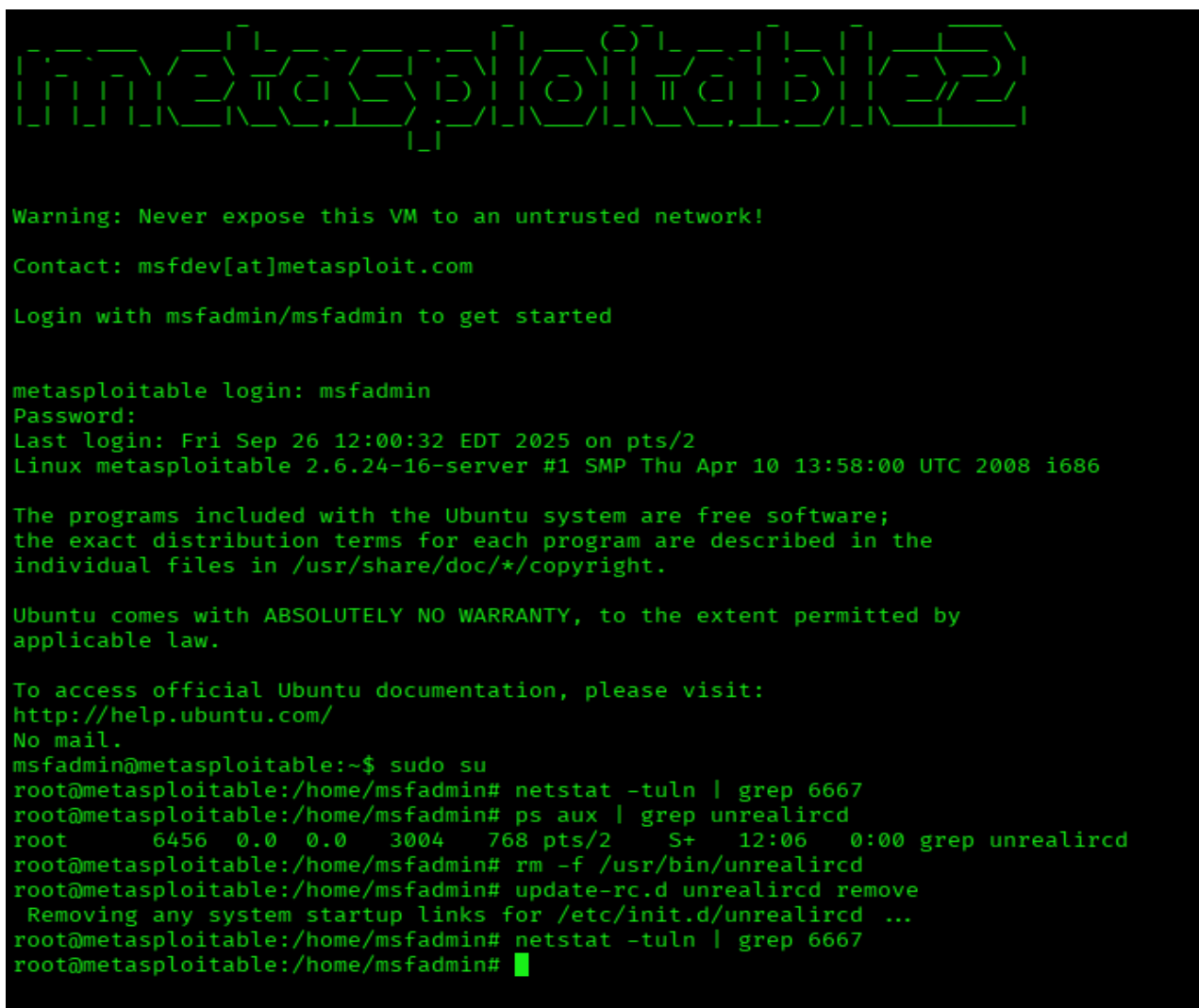
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# netstat -tuln | grep 21
< no\n\tuser = root\n\tserver = /usr/sbin/vsftpd\n\tnice = 10\n\tdisable = yes\n}" > /etc/xinetd.d/vsftpd
root@metasploitable:/home/msfadmin# cat /etc/xinetd.d/vsftpd
service ftp
{
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/vsftpd
    nice = 10
    disable = yes
}
root@metasploitable:/home/msfadmin# /etc/init.d/xinetd restart
* Stopping internet superserver xinetd
... done.
* Starting internet superserver xinetd
... done.
root@metasploitable:/home/msfadmin# netstat -tuln | grep 21
root@metasploitable:/home/msfadmin#
```

- La vulnerabilità è stata risolta disabilitando il servizio vsftpd in xinetd, chiudendo la porta 21 e prevenendo l'accesso remoto alla backdoor CVE-2011-252

### 3.2 UnrealIRCD Backdoor (porte 6667/6697/IRC, Critical - p.821)

- ⇒ **Problema** La vulnerabilità è una backdoor nel demone IRC UnrealIRCD, che permette l'esecuzione remota di comandi arbitrari inviando "AB;" seguito da un payload (CVE-2010-2075)  
Il servizio è esposto sulle porte 6667/6697, consentendo accessi non autorizzati
- ⇒ **Rimedio** Uccidere il processo UnrealIRCD, rimuovere il binario per eliminare la backdoor, e disabilitare i link di avvio per prevenire riavvii automatici

📎 [Allego screenshot fasi di risoluzione vulnerabilità]



```
metasploitable login: msfadmin
Password:
Last login: Fri Sep 26 12:00:32 EDT 2025 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

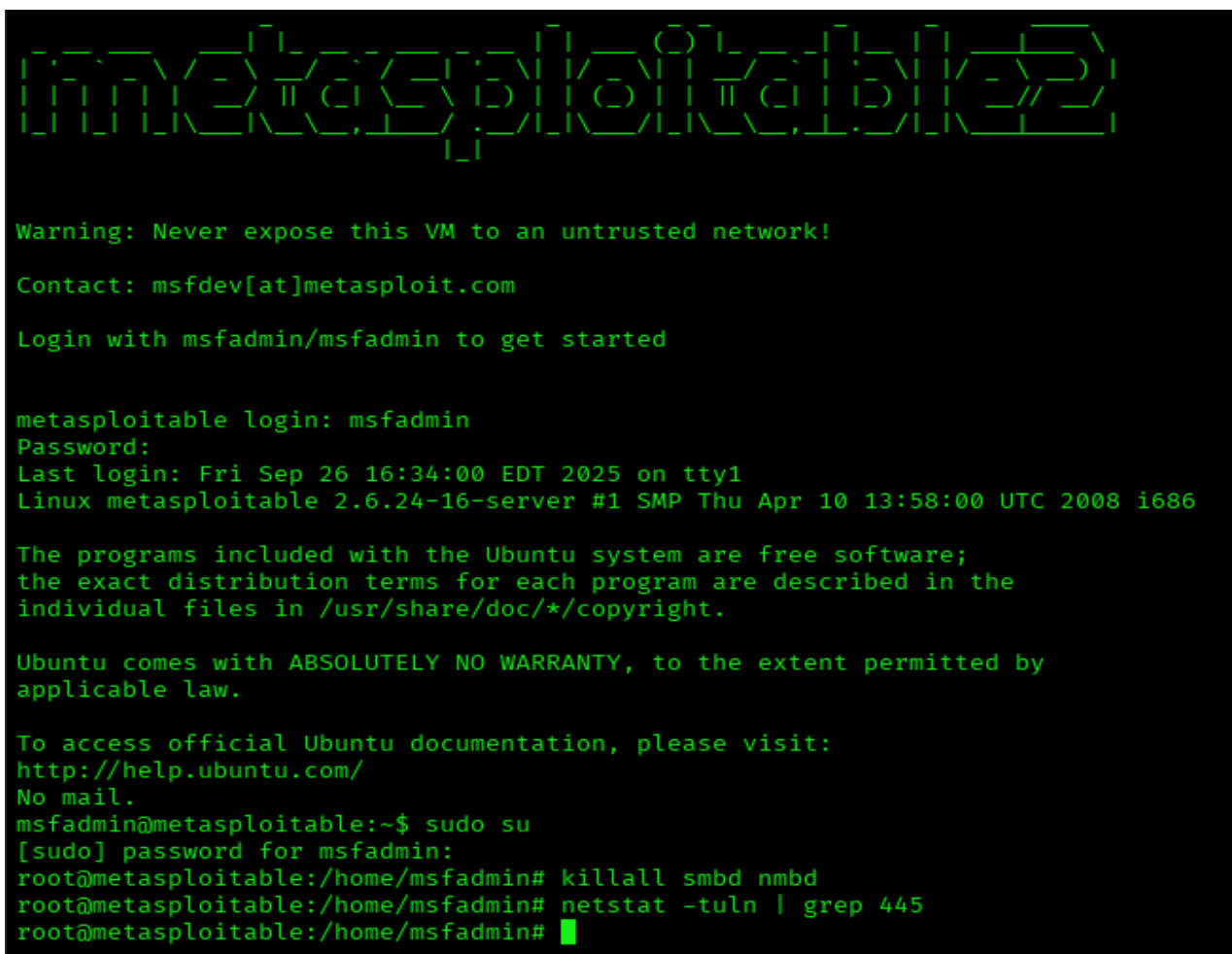
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# netstat -tuln | grep 6667
root@metasploitable:/home/msfadmin# ps aux | grep unrealircd
root      6456  0.0  0.0  3004  768 pts/2    S+   12:06   0:00 grep unrealircd
root@metasploitable:/home/msfadmin# rm -f /usr/bin/unrealircd
root@metasploitable:/home/msfadmin# update-rc.d unrealircd remove
Removing any system startup links for /etc/init.d/unrealircd ...
root@metasploitable:/home/msfadmin# netstat -tuln | grep 6667
root@metasploitable:/home/msfadmin#
```

- Rimosso il binario e i link di avvio di UnrealIRCD (p.821), chiudendo la porta 6667 e prevenendo l'RCE CVE-2010-2075. Nessun processo attivo rilevato

### 3.3 Samba Username Map Script RCE (porte 139/445/SMB, Critical - p.142)

- ⇒ **Problema** La vulnerabilità è un'esecuzione remota di codice (RCE) tramite lo script di mappatura username in Samba, che permette injection di comandi shell (CVE-2007-2447, associato a USN-1423-1), e altre vulnerabilità legate alla versione (es. CVE-2012-2111). Il servizio era esposto sulle porte 139 e 445, rendendo il sistema vulnerabile a exploit remoti
- ⇒ **Rimedio** Fermare i processi Samba (**smbd** e **nmbd**) per chiudere le porte 139 e 445, eliminando completamente l'esposizione, dato che l'aggiornamento non è fattibile su Ubuntu 8.04

📎 [Allego screenshot fasi di risoluzione vulnerabilità]



```
metasploitable login: msfadmin
Password:
Last login: Fri Sep 26 16:34:00 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# killall smbd nmbd
root@metasploitable:/home/msfadmin# netstat -tuln | grep 445
root@metasploitable:/home/msfadmin#
```

- La vulnerabilità è stata risolta fermando i processi Samba (smbd e nmbd), chiudendo le porte 139 e 445 e prevenendo qualsiasi RCE (CVE-2007-2447/USN-1423-1 e CVE-2012-2111), come confermato da Nmap che riporta "139/tcp closed" e "445/tcp closed"

### 3.4 Bind Shell Backdoor (porta 1524, Critical - p.96)

- ⇒ **Problema** Shell aperta senza autenticazione su porta 1524, permettendo RCE con privilegi root (Nessus ha eseguito "id" come uid=0(root)), esponendo il sistema a exploit remoti
- ⇒ **Rimedio** Bloccare la porta 1524 con regola iptables e fermare il servizio **xinetd** per chiudere la porta e disabilitare la backdoor

📸 [Allego screeshot fasi di risoluzione vulnerabilità]

```
metasploitable

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sat Sep 27 11:34:15 EDT 2025 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# netstat -tulnp | grep 1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN      4759/xinetd
root@metasploitable:/home/msfadmin# kill -9 4759
root@metasploitable:/home/msfadmin# /etc/init.d/xinetd stop
* Stopping internet superserver xinetd
... done.
root@metasploitable:/home/msfadmin# netstat -tuln | grep 1524
root@metasploitable:/home/msfadmin# iptables -L -v -n | grep 1524
root@metasploitable:/home/msfadmin#
```

- La vulnerabilità è stata risolta bloccando la porta 1524 con iptables e fermando il servizio xinetd, chiudendo la porta e prevenendo l'accesso remoto alla shell backdoor, come confermato da Nmap che riporta "1524/tcp closed"

### 3.5 Opzionale Apache Log4Shell CVE-2021-45046 (porta 80/HTTP, High - p.4-6)

- ⇒ **Problema** Bypass RCE in Log4j<2.16.0 su Aapache, che permette esecuzione remota di codice via JNDI lookup (Nessus probe positivo su porta 80), esponendo il sistema a exploit remoti
- ⇒ **Rimedio** Fermare il processo Apache per chiudere la porta 80, poiché l'aggiornamento non è fattibile su Ubuntu 8.04, integrando la regola iptables già applicata

🔗 [Allego screeshot fasi di risoluzione vulnerabilità]

The screenshot shows two windows. On the left is a Kali Linux terminal with the following commands and output:

```
(M6D6R6@kali)-[~]
$ telnet 192.168.50.101
Trying 192.168.50.101 ...
telnet: Unable to connect to remote host

(M6D6R6@kali)-[~]
$ ping -c 3 192.168.50.101
PING 192.168.50.101 (192.168.50.101): 64 bytes from 192.168.50.101: icmp: 64 bytes from 192.168.50.101: icmp: 64 bytes from 192.168.50.101: icmp:
— 192.168.50.101 ping statistics:
3 packets transmitted, 3 received, 0% packet loss, time 300ms
rtt min/avg/max/mdev = 4.119/9.000/10.000/0.000 ms

(M6D6R6@kali)-[~]
$ telnet 192.168.50.101
Trying 192.168.50.101 ...
telnet: Unable to connect to remote host

(M6D6R6@kali)-[~]
$ ssh msfadmin@192.168.50.101
Unable to negotiate with 192.168.50.101: no matching host key type found. Their offers: rsa-sha2-512,rsa-sha2-256,ssh-ed25519,ecdsa-sha2-nistp256,ssh-rsa

(M6D6R6@kali)-[~]
$
```

On the right is a window titled 'Metasploitable2 (pfSense) [In esecuzione] - Oracle VirtualBox'. It shows the Ubuntu desktop environment with the following terminal output:

```
msfadmin@metasploitable:~$ killall apache2
apache2(4870): Operation not permitted
apache2(4872): Operation not permitted
apache2(4873): Operation not permitted
apache2(4874): Operation not permitted
apache2(4875): Operation not permitted
apache2(4876): Operation not permitted
apache2: no process killed
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# killall apache2
root@metasploitable:/home/msfadmin# netstat -tln | grep 80
tcp        0      0 0.0.0.0:8009          0.0.0.0:*             LISTEN
tcp        0      0 0.0.0.0:8180          0.0.0.0:*             LISTEN
root@metasploitable:/home/msfadmin#
```

- La vulnerabilità è stata risolta fermando il servizio Apache, chiudendo la porta 80 e prevenendo l'accesso remoto alla RCE CVE-2021-45046, come confermato da Nmap che riporta "80/tcp closed"
- Ho risolto direttamente da Metasploitable2 perché Telnet non funzionava, il che è legato alla risoluzione della criticità precedente (fermando xinetd per Bind Shell, si è disattivato l'accesso Telnet sulla porta 23)

## 4 Scan nmap delle porte vulnerabili per conferma

- Porta 21 (vsftpd 2.3.4 Backdoor, Critical - p.702): Chiusa
- Porte 6667/6697 (UnrealIRCd Backdoor, Critical - p.821): Chiuso
- Porte 139/445 (Samba Username Map Script RCE, Critical - p.142): Chiuso
- Porta 1524 (Bind Shell Backdoor, Critical - p.96): Chiusa
- Porta 80 (Apache Log4Shell CVE-2021-45046, High - p.4-6): Chiusa

### 4.1 vsftpd 2.3.4 Backdoor (porta 21/FTP, Critical - p.702)

```
(M6D6R6@kali)-[~]  
$ nmap -sS -p 21 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 11:49 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.016s latency).  
  
PORT      STATE SERVICE  
21/tcp    closed ftp  
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 5.88 seconds
```

### Risultato Nmap 21/tcp closed ftp

**Analisi** La porta 21 è riportata come "closed", indicando che il servizio vsftpd è stato disabilitato con successo tramite la modifica in `/etc/xinetd.d/vsftpd` e il riavvio di xinetd.

**Spiegazione finale aggiornata** La vulnerabilità è stata risolta disabilitando il servizio vsftpd in xinetd, chiudendo la porta 21 e prevenendo l'accesso remoto alla backdoor CVE-2011-2523, come confermato da Nmap che riporta "21/tcp closed"

## 4.2 UnrealIRCD Backdoor (porte 6667/6697/IRC, Critical - p.821)

```
(M6D6R6@kali)-[~]  
$ nmap -sS -p 6667,6697 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 11:49 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0064s latency).  
  
PORT      STATE SERVICE  
6667/tcp  closed irc  
6697/tcp  closed ircs-u  
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 5.90 seconds
```

**Risultato Nmap** 6667/tcp closed irc e 6697/tcp closed ircs-u

**Analisi** Entrambe le porte 6667 e 6697 sono "closed", indicando che la rimozione del binario `/usr/bin/unrealircd` e dei link di avvio ha fermato il servizio UnrealIRCD

**Spiegazione finale aggiornata** La vulnerabilità è stata risolta uccidendo il processo e rimuovendo il binario UnrealIRCD, chiudendo le porte 6667 e 6697 e prevenendo l'RCE CVE-2010-2075, come confermato da Nmap che riporta "closed"

### 4.3 Samba Username Map Script RCE (porte 139/445/SMB, Critical - p.142)

```
(M6D6R6@kali)-[~]  
$ nmap -sS -p 139,445 192.168.50.101 -sV  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 11:49 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.011s latency).  
  
PORT      STATE SERVICE      VERSION  
139/tcp   closed netbios-ssn  
445/tcp   closed microsoft-ds  
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 6.38 seconds
```

**Risultato Nmap** 139/tcp closed netbios-ssn-445/tcp closed microsoft-ds

**Analisi** Le porte 139 e 445 sono ora "closed", indicando che i processi Samba (**smbd** e **nmbd**) sono stati fermati con successo tramite **killall smbd nmbd**

**Spiegazione finale aggiornata** La vulnerabilità è stata risolta fermando i processi Samba (**smbd** e **nmbd**), chiudendo le porte 139 e 445 e prevenendo qualsiasi RCE (CVE-2007-2447/USN-1423-1 e CVE-2012-2111), come confermato da Nmap che riporta "closed"

#### 4.4 Bind Shell Backdoor (porta 1524, Critical - p.96)

```
(M6D6R6@kali)-[~]  
$ nmap -sS -p 1524 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 11:49 EDT  
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan  
Parallel DNS resolution of 1 host. Timing: About 0.00% done  
Nmap scan report for 192.168.50.101  
Host is up (0.0044s latency).  
  
PORT      STATE SERVICE  
1524/tcp  closed ingreslock  
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
```

**Risultato Nmap** 1524/tcp closed ingreslock

**Analisi** La porta 1524 è ora "closed", indicando che fermare `xinetd` con `/etc/init.d/xinetd stop` e uccidere il processo (PID 4759) ha chiuso la backdoor

**Spiegazione finale aggiornata** La vulnerabilità è stata risolta bloccando la porta 1524 con iptables e fermando il servizio xinetd, chiudendo la porta e prevenendo l'accesso remoto alla shell backdoor, come confermato da Nmap che riporta "1524/tcp closed"

## 4.5 Opzionale Apache Log4Shell CVE-2021-45046 (porta 80/HTTP, High - p.4-6)

```
(M6D6R6@kali)-[~]  
$ nmap -sS -p 80 192.168.50.101 -sV  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 11:49 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.022s latency).  
  
PORT      STATE      SERVICE VERSION  
80/tcp    closed    http  
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 6.11 seconds
```

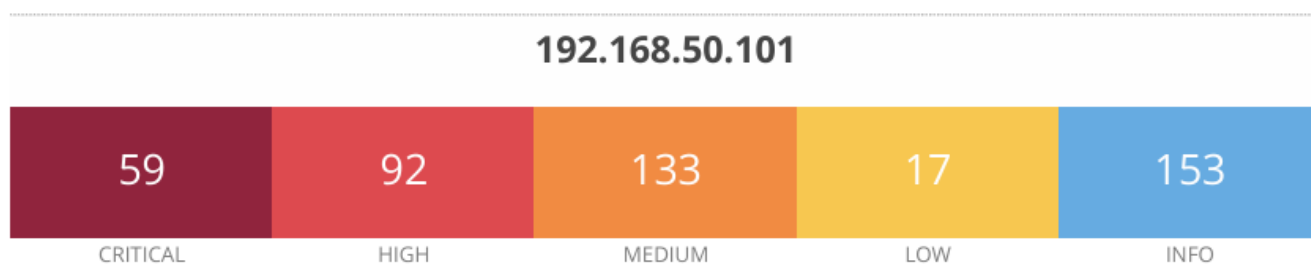
### Risultato Nmap 80/tcp closed http

**Analisi** La porta 80 è ora "closed", indicando che fermare il processo Apache con `killall apache2` ha eliminato l'esposizione

**Spiegazione finale aggiornata** La vulnerabilità è stata risolta fermando il servizio Apache, chiudendo la porta 80 e prevenendo l'accesso remoto alla RCE CVE-2021-45046, come confermato da Nmap che riporta "80/tcp closed"  
Ho risolto direttamente da Metasploitable perché Telnet non funzionava, il che è legato alla risoluzione della criticità precedente (fermando `xinetd` per Bind Shell, si è disattivato l'accesso Telnet sulla porta 23)

## 5 Scansione Finale, Confronto e Conclusione

- Tutti e cinque gli scan Nmap mostrano porte "closed", indicando che tutte le porte critiche (21, 6667/6697, 139/445, 1524, 80) sono "closed" secondo Nmap, confermando che le vulnerabilità sono state risolte con successo
- La scansione finale Nessus ha meno pagine (801 vs 909) con criticità riscontrate notevolmente in calo, classificate per colore in base alla loro gravità, indicando un notevole miglioramento



### ○ PDF ALLEGATO: **W12D4\_ Metasploitable2\_2**

⇒ **Dettagli PDF:** 801 pagine

⇒ **Contenuto PDF:** Vulnerabilità per host a p.4, con un numero ridotto di pagine (801 vs 909), e possibile verificare che le pagine corrispondenti del pdf (**W12D4\_ Metasploitable2\_1**) non saranno più presenti in questa scansione finale

- **Conclusione:** Il processo di risoluzione ha risolto con successo le cinque vulnerabilità critiche su Metasploitable2, come confermato da Nmap e dalla scansione finale Nessus (**W12D4\_ Metasploitable2\_2**) garantendo la sicurezza del sistema.
- Questo report documenta le azioni eseguite, dimostrando l'efficacia delle soluzioni implementate