

W12D4 – Pratica

Epic Education Srl

Analisi delle vulnerabilità e azioni di rimedio

(target Metasploitable)

Simone Giordano

30/09/2025



Contatti:

Tel: 3280063044

Email: mynameisimone@gmail.com

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

Sommario

Sintesi esecutiva	3
Perimetro	3
Panoramica delle vulnerabilità	3
51988 Bind Shell Backdoor Detection	4
Exploit	4
Remediation	5
VNC Server 'password' Password	6
Exploit	6
Remediation	7
Browsable Web Directories	8
Exploit	8
Remediation	9

Sintesi esecutiva

Il sistema presenta **29 vulnerabilità critiche**, potenzialmente sfruttabili per ottenere accesso remoto, eseguire codice arbitrario o compromettere l'integrità del sistema.

Le **97 vulnerabilità ad alta gravità** indicano esposizione significativa a minacce note, spesso legate a software obsoleto o configurazioni insicure.

Le **voci informative (233)** suggeriscono una superficie d'attacco ampia e necessitano di analisi per identificare potenziali vettori futuri.

Sono state prese in esame 2 vulnerabilità Critical e 1 vulnerabilità Medium e sono state risolte.

Perimetro

Host Information

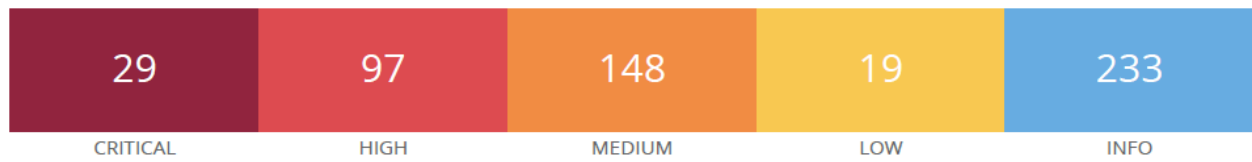
Netbios Name: METASPLOITABLE

IP: 192.168.50.101

MAC Address: 08:00:27:E4:29:4E

OS: Linux Kernel 2.6.24-16-server on Ubuntu 8.04esto.

Panoramica delle vulnerabilità



51988 Bind Shell Backdoor Detection

W12D1 Metasploitable / Plugin #51988

[← Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 113 Remediations 70 Notes 30 History 3

CRITICAL Bind Shell Backdoor Detection

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.

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 .....
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.101

Exploit

Connessione tramite **netcat** con coppia *IP:porta* ed esplorazione file e cartelle per accertare la vulnerabilità.

```
(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
```

W12D4 SIMONE GIORDANO

4

Remediation

Con il comando `sudo lsof -i :1524` (**lsof** elenca i file aperti dai processi, **-i** filtra per connessioni di rete, **:1524** restringe l'output alle connessioni sulla porta 1524) notiamo che **xinetd** accetta una connessione e ha avviato **bash** in background per gestirla.

xinetd con PID 4411 è in ascolto sulla porta 1524 (*:ingreslock (LISTEN))

C'è una shell **bash** con PID 4658 (utente **root**) con una connessione **ESTABLISHED** tra 192.168.50.101:1525 e 192.168.50.100:47154.

```
root@metasploitable:/# sudo lsof -i :1524
COMMAND  PID USER  FD   TYPE DEVICE SIZE NODE NAME
xinetd   4411 root   12u  IPv4  11962      TCP *:ingreslock (LISTEN)
bash     4658 root    0u  IPv4  12327      TCP 192.168.50.101:ingreslock→192.168.50.100:47154 (ESTABLISHED)
bash     4658 root    1u  IPv4  12327      TCP 192.168.50.101:ingreslock→192.168.50.100:47154 (ESTABLISHED)
bash     4658 root    2u  IPv4  12327      TCP 192.168.50.101:ingreslock→192.168.50.100:47154 (ESTABLISHED)
bash     4658 root   255u  IPv4  12327      TCP 192.168.50.101:ingreslock→192.168.50.100:47154 (ESTABLISHED)
lsof     4894 root    0u  IPv4  12327      TCP 192.168.50.101:ingreslock→192.168.50.100:47154 (ESTABLISHED)
lsof     4894 root    1u  IPv4  12327      TCP 192.168.50.101:ingreslock→192.168.50.100:47154 (ESTABLISHED)
lsof     4894 root    2u  IPv4  12327      TCP 192.168.50.101:ingreslock→192.168.50.100:47154 (ESTABLISHED)
```

Termino **bash** (PID 4658)

Sudo kill -TERM 4658 Chiede al processo di terminare in modo ordinato: chiudere file, liberare risorse, scrivere log, salvare lo stato, ecc.

sleep 2 Concede una pausa di 2 secondi, per dare al processo il tempo di terminare ordinatamente.

sudo kill -9 4658 Forza l'immediata terminazione del processo dal kernel.

```
root@metasploitable:/# sudo kill -TERM 4658
root@metasploitable:/# sleep 2
root@metasploitable:/# sudo kill -9 4658
```

Fermo e disabilito **xinetd**

```
root@metasploitable:/# sudo systemctl stop xinetd
root@metasploitable:/# sudo systemctl disable xinetd
```

Tramite **nmap** possiamo verificare che lo stato della porta in ascolto di **ingreslock** sia chiusa.

```
(kali㉿kali)-[~]
└─$ nmap -p 1524 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 06:51 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00091s latency).

PORT      STATE SERVICE
1524/tcp  closed ingreslock
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

Se riprovo a collegarmi tramite **netcat** la connessione viene rifiutata

```
(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
```

VNC Server 'password' Password

W12D1 Metasploitable / Plugin #61708

[Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 113 Remediations 70 Notes 30 History 3

CRITICAL VNC Server 'password' Password

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.

Solution

Secure the VNC service with a strong password.

Output

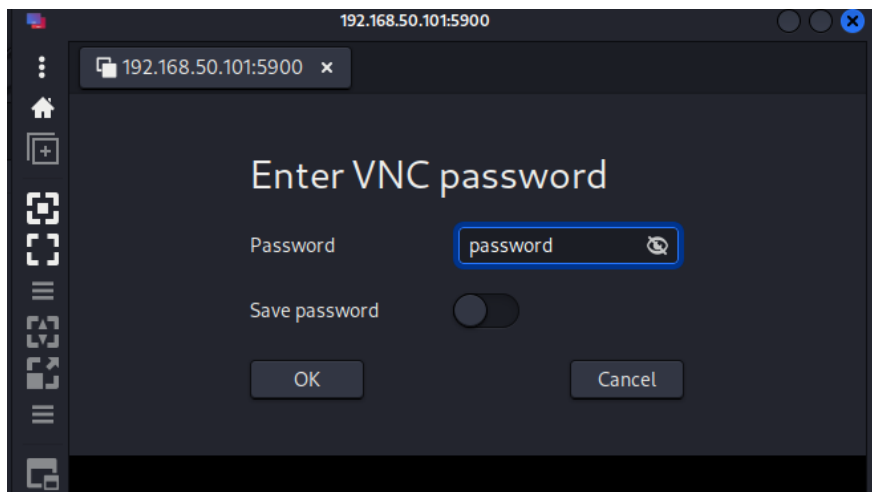
Nessus logged in using a password of "password".

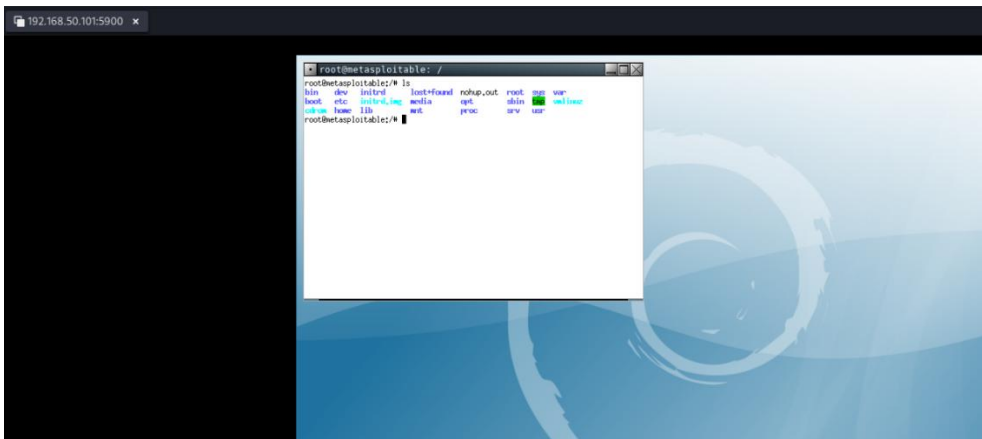
To see debug logs, please visit individual host

Port	Hosts
5900 / tcp / vnc	192.168.50.101

Exploit

Sono entrato nel server VNC di Metasploitable tramite Remmina inserendo la psw "password".





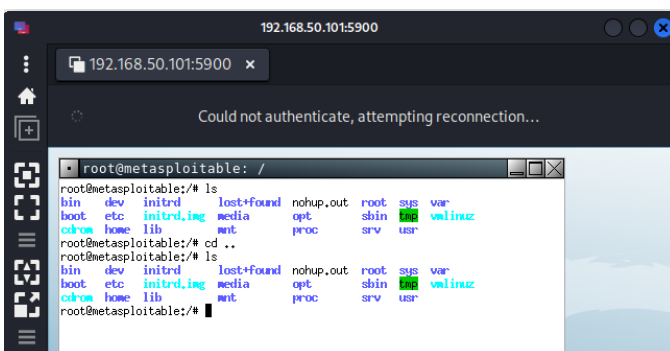
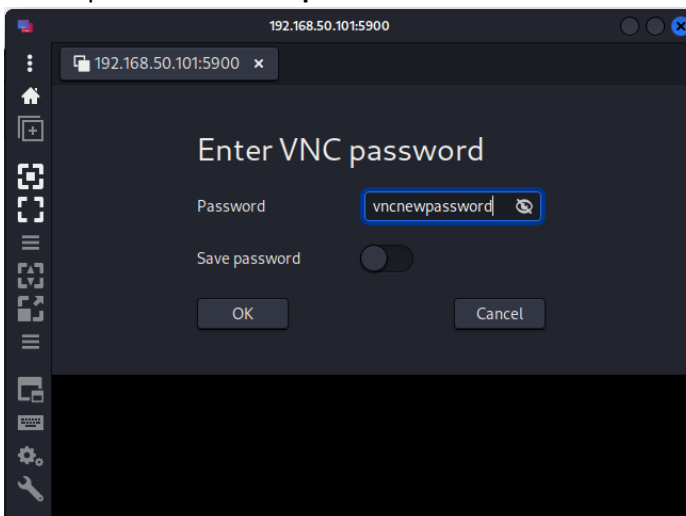
Remediation

MODIFICA PASSWORD

In Metasploitable, ho eseguito il comando **vncpasswd** come utente root per cambiare la password e ho impostato come nuova psw **vncnewpassword**. La nuova password è ancora debole ma serviva giusto per testare la procedura, ho evitato password complesse perché Metasploitable non consente di visualizzare i caratteri digitati.

Ho eseguito il kill del processo risalendo al Job ID e poi l'ho riavviato con il comando **vncserver :5900** per essere sicuro che la nuova password fosse effettiva.

Nuova password **vncnewpassword**



Browsable Web Directories

MEDIUM Browsable Web Directories

Description
Multiple Nessus plugins identified directories on the web server that are browsable.

Solution
Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

See Also
<http://www.nessus.org/u?0a35179e>

Output

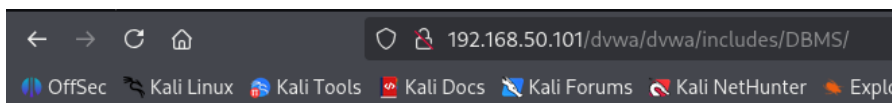
```
The following directories are browsable :  
  
http://192.168.50.101/dav/  
http://192.168.50.101/dvwa/dvwa/  
http://192.168.50.101/dvwa/dvwa/css/  
http://192.168.50.101/dvwa/dvwa/images/  
http://192.168.50.101/dvwa/dvwa/includes/  
http://192.168.50.101/dvwa/dvwa/includes/DBMS/  
http://192.168.50.101/dvwa/dvwa/js/  
http://192.168.50.101/mutillidae/documentation/  
http://192.168.50.101/mutillidae/styles/  
http://192.168.50.101/mutillidae/styles/ddsmoothmenu/  
http://192.168.50.101/test/  
http://192.168.50.101/test/testoutput/
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	192.168.50.101

Exploit

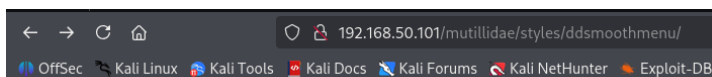
Attraverso il browser è possibile muoversi tra e cartelle e i file.



Index of /dvwa/dvwa/includes/DBMS

Name	Last modified	Size	Description
Parent Directory		-	
DBMS.php	06-Jun-2010 23:59	2.4K	
MySQL.php	06-Jun-2010 23:59	2.9K	
PGSQL.php	06-Jun-2010 23:59	3.4K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80



Index of /mutillidae/styles/ddsmoothm

Name	Last modified	Size	Description
Parent Directory		-	
ddsmoothmenu-v.css	11-Apr-2011 20:14	1.2K	
ddsmoothmenu.css	21-Jan-2012 21:41	2.2K	
readme.txt	11-Apr-2011 20:14	58	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80

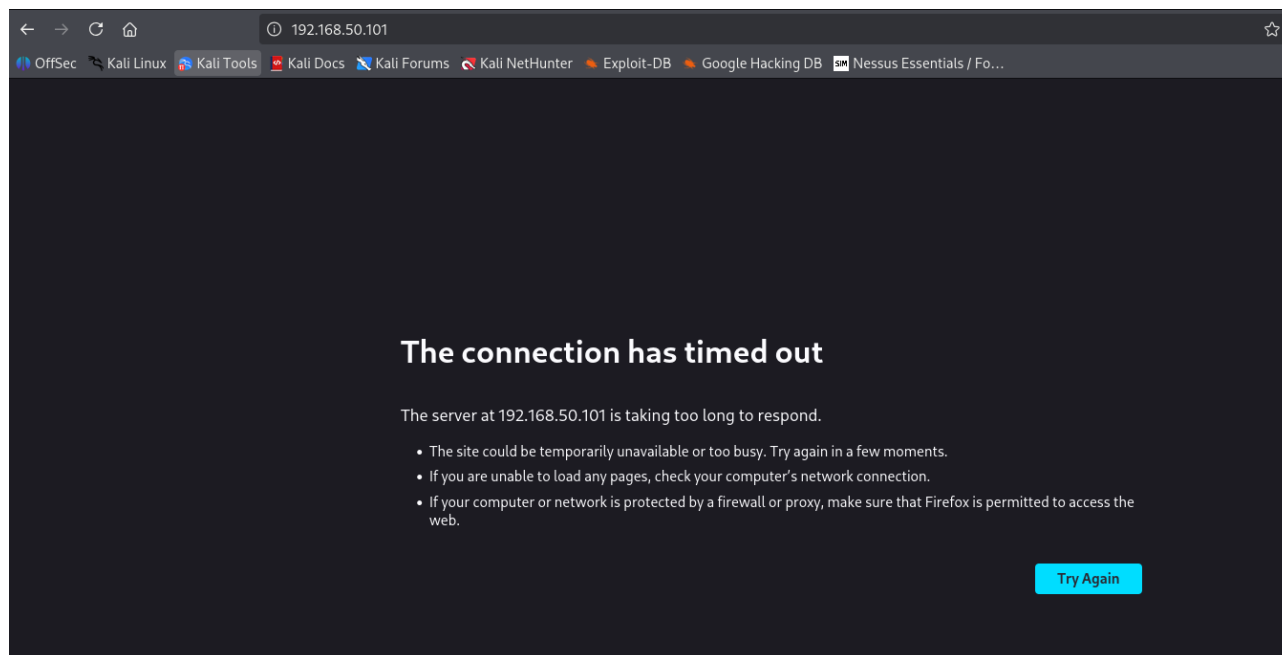
Remediation

Da Metasploitable ho impostato una regola di firewall con IPTABLES per bloccare tutte le richieste in entrata sulla porta 80, e poi ho salvato la regola.

```
root@metasploitable:~/msfadmin# sudo iptables -I INPUT -p tcp --dport 80 -j DROP
```

```
root@metasploitable:~/msfadmin# sudo iptables-save > /etc/network/interfaces.d/iptables.rules
```

Successivamente la pagina non sarà più raggiungibile.



Lo scan di nmap conferma che lo stato della porta 80 è filtrato.

```
(kali@kali)~$ nmap -sV -p 80 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:19 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00084s latency).

PORT      STATE      SERVICE VERSION
80/tcp    filtered  http

MAC Address: 08:00:27:E4:29:4E (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 13.74 seconds
```