



ANALISI DELL'ASSET

"HARRY POTTER: FAWKES"

*Processo di penetration testing ed overview della
documentazione consegnata*

Professore:

Arcangelo Castiglione

Studente:

Simone Masullo (0522501369)

HARRY POTTER: FAWKES

- L'asset analizzato consiste in una macchina virtuale presente su VulnHub;
- È possibile scaricare la macchina al link:
<https://www.vulnhub.com/entry/harrypotter-fawkes,686/>;



ANALISI DELL'ASSET HARRY POTTER: FAWKES

- Non sono state fornite informazioni preliminari sull'asset target, si è dunque proceduto ad un'analisi di tipo **black-box**;
- Maggiori informazioni sulle regole di ingaggio sono presenti al **Capitolo 2: "Engagement Highlights"** del Penetration Testing Report.

Indice

1	Executive Summary	5
2	Engagement Highlights	8
2.1	Identificazione del committente	8
2.2	Accordo di non divulgazione	8
2.3	Informazioni preliminari	9
2.4	Tecniche e strumenti consentiti	9
2.5	Periodo di attività	9
2.6	Budget stimato	10
2.7	Risultati attesi	10
2.8	Test plan	11
3	Vulnerability Report	13
4	Remediation Report	16
4.1	Messa in sicurezza del software server_hogwarts . . .	16
4.2	Autenticazione al server FTP	17
4.3	Sostituzione del protocollo FTP	17
4.4	Aggiornamento degli applicativi	17
4.5	Miglioramento della politica di controllo degli accessi	18

ANALISI DELL'ASSET HARRY POTTER: FAWKES

- Le vulnerabilità da cui è affetto l'asset, così come le debolezze che comportano problemi alla sicurezza dello stesso, vengono presentate nel Penetration Testing Report. In particolare:
 1. per una visualizzazione sommaria consultare il **Capitolo 3: "Vulnerability Report"**;
 2. Per una visualizzazione in grafici e tabelle visualizzare il **Capitolo 5: "Findings Summary"**;
 3. Per la visualizzazione di maggiori dettagli tecnici relativi alle vulnerabilità, visualizzare il **Capitolo 6: "Detailed Summary"**.

Indice

1	Executive Summary	
2	Engagement High	
2.1	Identificazione	
2.2	Accordo di non	
2.3	Informazioni pr	
2.4	Tecniche e stru	
2.5	Periodo di attiv...	
2.6	Budget stimato	10
2.7	Risultati attesi	10
2.8	Test plan	11
3	Vulnerability Report	13
4	Remediation Report	16
4.1	Messa in sicurezza del software server_hogwarts	16
4.2	Autenticazione al server FTP	17
4.3	Sostituzione del protocollo FTP	17
4.4	Aggiornamento degli applicativi	17
4.5	Miglioramento della politica di controllo degli accessi	18

4.6	Formazione del personale	18
4.7	Implementazione di sistemi di sicurezza avanzati	19
5	Findings Summary	20
5.1	Descrizione delle vulnerabilità riscontrate	20
5.2	Descrizione delle debolezze riscontrate	31
5.3	Suddivisione delle vulnerabilità per severity	31
5.4	Vulnerability breakdown	31
5.4.1	Vulnerabilità del container	32
5.4.2	Vulnerabilità di Fawkes	33
5.5	Valutazione dei rischi	33

6	Detailed Summary	38
----------	-------------------------	-----------

ANALISI DELL'ASSET HARRY POTTER: FAWKES

- Suggerimenti su possibili rimedi da applicare per mitigare o risolvere le vulnerabilità esposte sono consultabili attraverso il **Capitolo 4: "Remediation Report"**;
- Si precisa che le informazioni presenti sono da prendere unicamente come suggerimenti e, come tali, vanno affiancati ad un'attività di analisi svolta da un appropriato **team di remediation**;
- Il penetration tester incaricato dell'analisi resta a disposizione per ulteriori approfondimenti e supporto al team di remediation.

Indice

1	Executive Summary	5
2	Engagement Highlights	8
2.1	Identificazione del committente	8
2.2	Accordo di non divulgazione	8
2.3	Informazioni preliminari	9
2.4	Tecniche e strumenti consentiti	9
2.5	Periodo di attività	9
2.6	Budget stimato	10
2.7	Risultati attesi	10
2.8	Test plan	11
3	Vulnerability Report	13
4	Remediation Report	16
4.1	Messa in sicurezza del software server_hogwarts	16
4.2	Autenticazione al server FTP	17
4.3	Sostituzione del protocollo FTP	17
4.4	Aggiornamento degli applicativi	17
4.5	Miglioramento della politica di controllo degli accessi	18

VULNERABILITÀ E RISCHI

- Per una più dettagliata visione delle vulnerabilità che affliggono il sistema in analisi si rimanda al documento - accluso alla presentazione - **Penetration Testing Report**.
- In figura vengono presentati un diagramma che mostra la distribuzione delle vulnerabilità identificate in base alla loro gravità (5.1) e la matrice dei rischi per la sicurezza dell'asset (5.2).

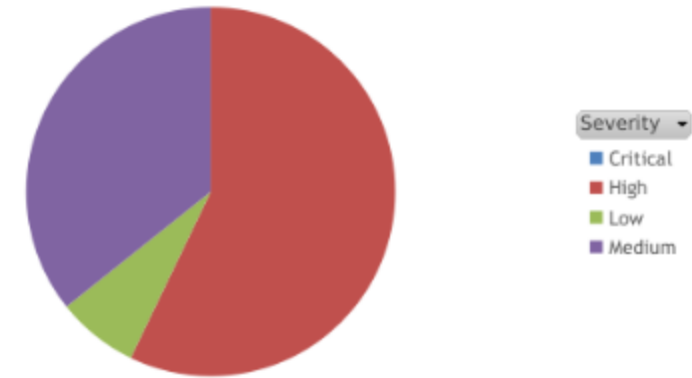


Figura 5.1: Diagramma delle vulnerabilità

Occorrenza	1 - Catastrofico	2 - Critico	3 - Serio	4 - Minore
A) Frequente	0	0	1	1
B) Probabile	1	1	0	1
C) Occasionale	0	0	0	0
D) Remoto	3	1	3	1
E) Improbabile	1	2	2	0

Figura 5.2: Hazard Risk Assessment matrix

SOLUZIONI E MITIGAZIONI

- Attualmente l'asset presenta un **rischio alto**. Le mitigazioni proposte possono ridurre il rischio fino a raggiungere un **livello basso**. Tali mitigazioni consistono in:
 1. Abilitazione dell'**autenticazione** per l'accesso al server FTP;
 2. Messa in sicurezza del software in esecuzione sulla porta 9898 tramite adeguati **controlli sull'input** dell'utente;
 3. Sostituzione dei **protocolli che trasmettono dati in chiaro** (FTP) con le relative versioni sicure (SFTP) che fanno uso di cifratura;
 4. Costante **aggiornamento degli applicativi e del sistema operativo** degli host;
 5. Miglioramento della politica di controllo degli accessi, tenendo conto del **principio del privilegio minimo**;
 6. Garantire un'adeguata **formazione del personale** al fine di evitare azioni che possano mettere a rischio la sicurezza dell'asset.

ANALISI DELL'ASSET

HARRY POTTER: FAWKES

- L'altro documento accluso alla presentazione è il **Documento di Replicabilità** nel quale è possibile trovare dettagli su tutti gli strumenti e le tecniche utilizzati durante il processo di analisi;
- Seguendo i passi illustrati nel documento dovrebbe essere possibile replicare esattamente - salvo risultati legati al momento esatto dell'esecuzione delle operazioni - gli output riportati;
- Di seguito verrà riportata una presentazione dettagliata del processo di analisi ed alcuni estratti del documento.

ANALISI DELL'ASSET HARRY POTTER: FAWKES

Il documento è diviso in capitoli. In ogni capitolo viene illustrata una diversa fase del processo di analisi svolto. In particolare il processo di analisi prevede sei fasi:

1. Information Gathering;
2. Target Discovery;
3. Enumerating Target;
4. Vulnerability Mapping;
5. Target Exploitation;
6. Post-exploitation.

Indice

Introduzione	9
1 Information gathering	12
1.1 Information gathering passivo	12
1.2 Information gathering attivo	14
2 Target discovery	15
2.1 Ottenimento dell'indirizzo IP	15
2.2 OS Fingerprinting	18
3 Enumerating target	19
3.1 Verifica della presenza di firewall	19
3.2 Analisi dei servizi erogati	20
3.2.1 Porta 9898	22
4 Vulnerability mapping	23
4.1 Analisi automatica	23
4.1.1 Nessus - basic network scan	23
4.1.2 Nessus - web application tests	25
4.2 Analisi tramite nmap	26

MACCHINA UTILIZZATA DAL PENTESTER

- L'intero processo di penetration testing è stato effettuato utilizzando una macchina su cui è montato un sistema **Kali Linux v2024.1**;
- Molti dei tool utilizzati durante il processo di analisi sono installati di default in tale sistema. In ogni caso, viene specificata la versione di ognuno degli strumenti al fine di garantire la replicabilità esatta del risultato.

STRUMENTI E VERSIONI

```
(kali㉿kali)-[~]  
$ cat /etc/os-release  
PRETTY_NAME="Kali GNU/Linux Rolling"  
NAME="Kali GNU/Linux"  
VERSION_ID="2024.1"  
VERSION="2024.1"  
VERSION_CODENAME=kali-rolling  
ID=kali  
ID_LIKE=debian  
HOME_URL="https://www.kali.org/"  
SUPPORT_URL="https://forums.kali.org/"  
BUG_REPORT_URL="https://bugs.kali.org/"  
ANSI_COLOR="1;31"
```

Figura 1: Informazioni sul Sistema Operativo della macchina del pentester

Nome del tool	Versione
nmap [25]	v7.94 SVN
Nessus [23]	v10.7.4 (#55) LINUX
OWASP ZAP [26]	v2.15.0
Nikto [24]	v2.5
dirb	v2.22
gobuster	v3.6
file	v5.45
strings	v2.42
Ghidra [6]	v11.1.1
gdb [5]	v13.2
metasploit-framework [9]	v6.4.16-0kali1
ropper [27]	v1.13.8
linux-smart-enumeration [8]	v4.14nw

INFORMATION GATHERING

- La prima fase di un processo di penetration testing prevede la raccolta di informazioni sull'asset in analisi;
- Le informazioni possono essere raccolte in maniera *passiva* - ovvero interrogando servizi di terze parti - o in maniera *attiva* - ovvero interrogando l'asset stesso;
- Si premette che in un sistema "fittizio" come quello in analisi, potrebbe non aver senso tentare di raccogliere informazioni in una fase preliminare. Si è comunque proceduto a tale attività a scopo didattico.

INFORMATION GATHERING PASSIVO

- È stata effettuata una query utilizzando la funzionalità Google Dork.
- Query utilizzata: Harry Potter: Fawkes +vulnhub ;
- Risultati ottenuti: pagina di download della macchina virtuale e walkthrough presenti in rete.

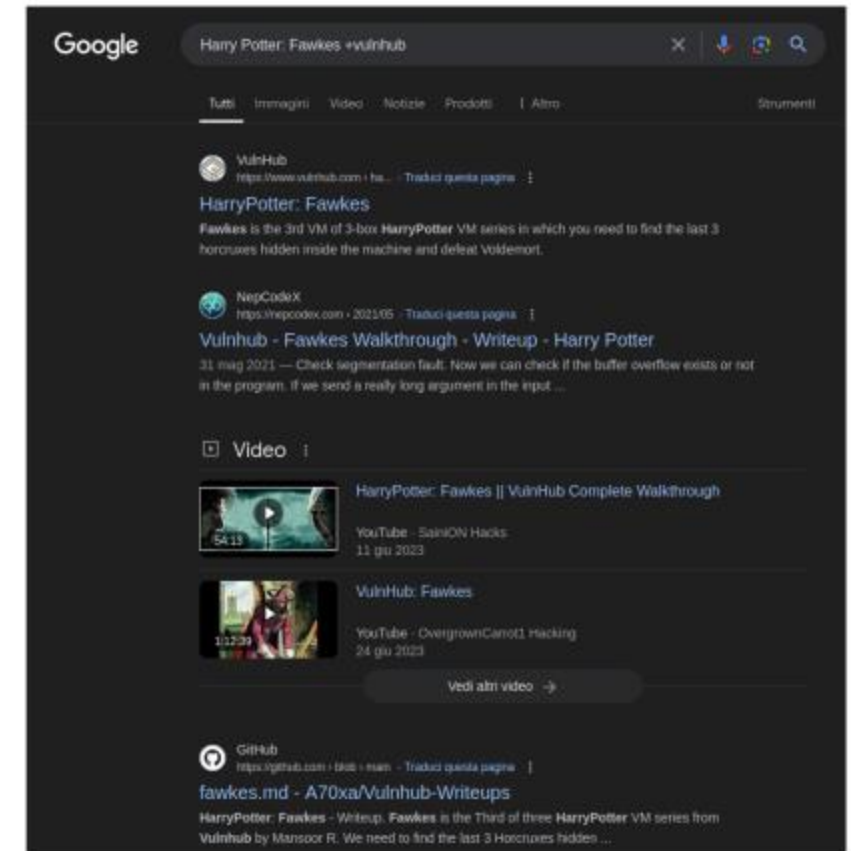


Figura 1.1: Risultato della query con Google dork

INFORMATION GATHERING ATTIVO

- Non essendo presente un indirizzo IP pubblico a cui inviare richieste non è stato possibile ottenere informazioni preliminari in maniera attiva.

TARGET DISCOVERY TRAMITE NMAP

- Viene sfruttato lo strumento **nmap** per ottenere la lista degli host attivi sulla rete;
- Trattandosi di una rete fittizia, sono presenti solo tre tipologie di host:
 1. la macchina del pentester;
 2. la macchina target;
 3. host virtuali creati dall'hypervisor VirtualBox.

```
(root@kali) ~/home/kali
nmap -sS 10.0.2.4/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 05:16 EDT
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.000056s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
631/tcp   open  ipp
7070/tcp  open  realserver
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.000056s latency).
All 1000 scanned ports on 10.0.2.3 (10.0.2.3) are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:24:31:FD (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.10 (10.0.2.10)
Host is up (0.00012s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
9898/tcp  open  monkeycom
MAC Address: 08:00:27:7D:C5:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4 (10.0.2.4)
Host is up (0.000020s latency).
All 1000 scanned ports on 10.0.2.4 (10.0.2.4) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 2.25 seconds
```

Figura 2.2: Risultato della scansione tcp syn di nmap

OS FINGERPRINTING TRAMITE NMAP

- Tramite lo stesso strumento viene effettuato OS Fingerprinting sulla macchina target.

```
(root@kali) ~ [/home/kali]
nmap -O 10.0.2.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 08:06 EDT
Nmap scan report for 10.0.2.10 (10.0.2.10)
Host is up (0.00032s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
9898/tcp  open  monkeycom
MAC Address: 08:00:27:7D:C5:F9 (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 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
```

Figura 2.3: OS Fingerprinting tramite nmap

ANALISI DEI SERVIZI ATTIVI

- Sempre sfruttando **nmap** vengono visualizzati i servizi attivi sulla macchina target e le relative versioni;
- Il comando utilizzato è: `nmap -sV 10.0.2.10 -p- -T5`;
- Un prospetto riassuntivo del risultato di tale operazione è riportato nella tabella di seguito.

Porta	Servizio	Versione
21	ftp	vsftpd 3.0.3
22	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80	http	Apache httpd 2.4.38 ((Debian))
2222	ssh	OpenSSH 8.4 (protocol 2.0)
9898	?	?

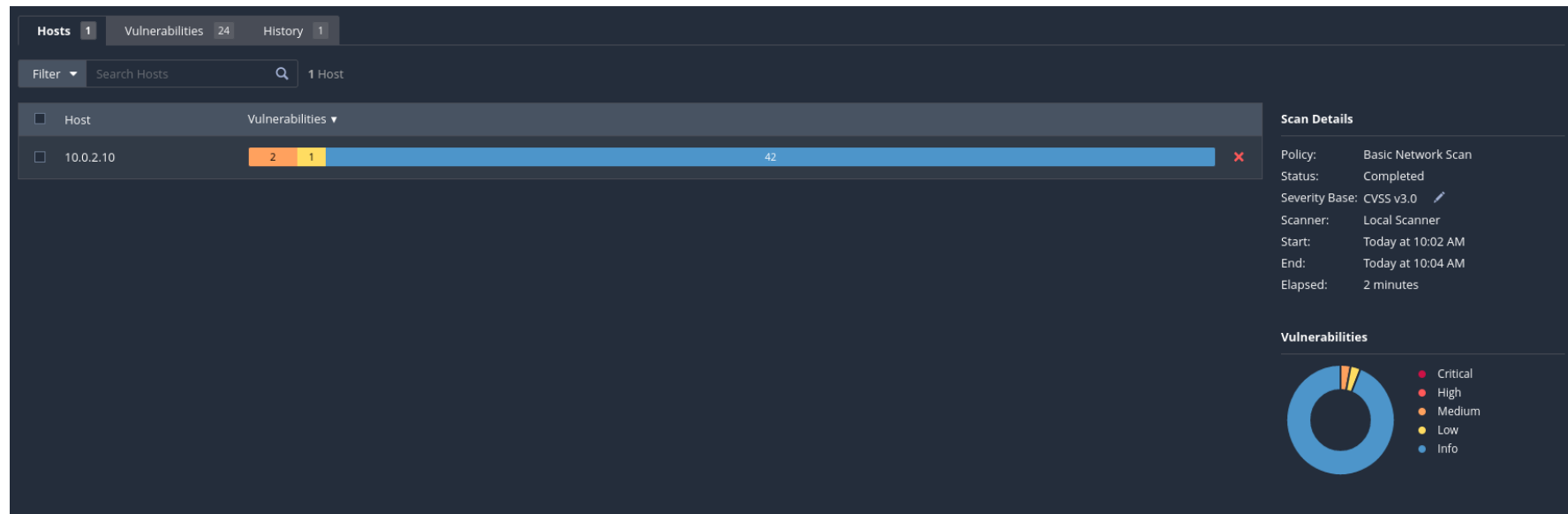
Tabella 3.1: Servizi erogati e relative versioni

RICERCA DI VULNERABILITÀ

- La ricerca di vulnerabilità è stata effettuata con diverse modalità e strumenti;
- Sono state adottate tecniche *automatiche* e *manuali*;
- Di seguito vengono riportate le tecniche utilizzate, illustrate con maggiore dettaglio nel documento di replicabilità.

RICERCA DI VULNERABILITÀ TRAMITE NESSUS

- Il primo strumento utilizzato per la ricerca di vulnerabilità è **Nessus**, del quale viene sfruttata la modalità "Basic Network Scan";
- Il processo ha restituito due vulnerabilità di gravità *media* ed una vulnerabilità di gravità *bassa*.



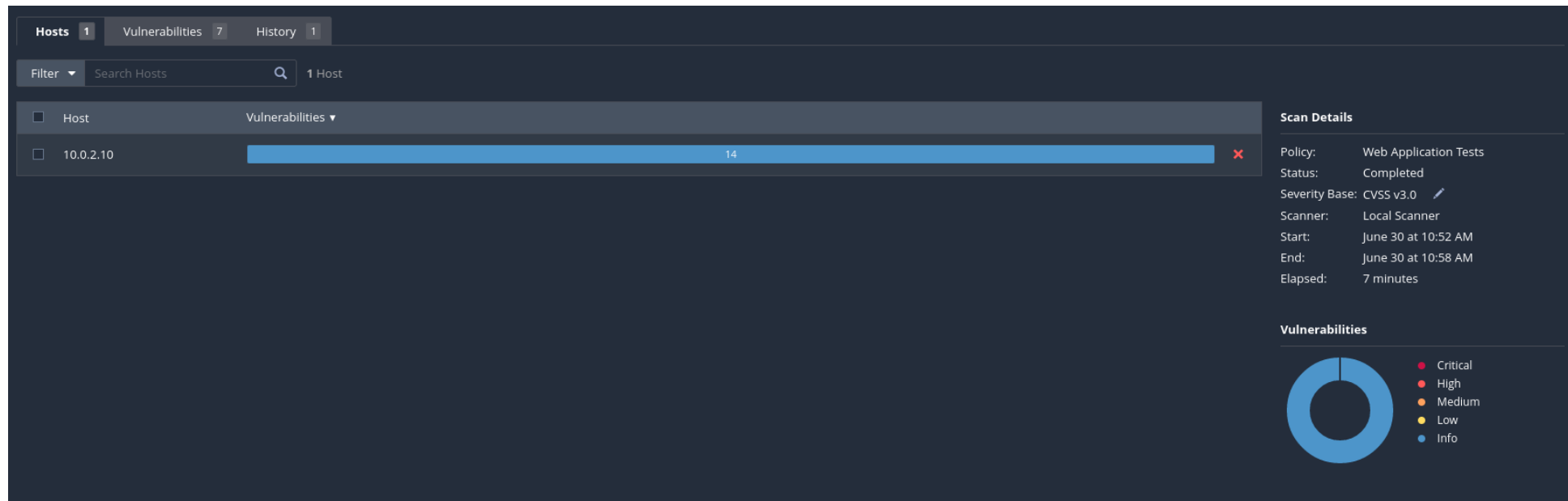
RICERCA DI VULNERABILITÀ TRAMITE NESSUS

- In particolare sono state identificate le vulnerabilità:
 - **Medium (5.9)** - CVE-2023-48795
 - **Low (-n/a-)** - CVE-1999-0524

Nota: la vulnerabilità CVE-2023-48795 viene conteggiata due volte poiché presente su due porte che sfruttano il servizio OpenSSH.

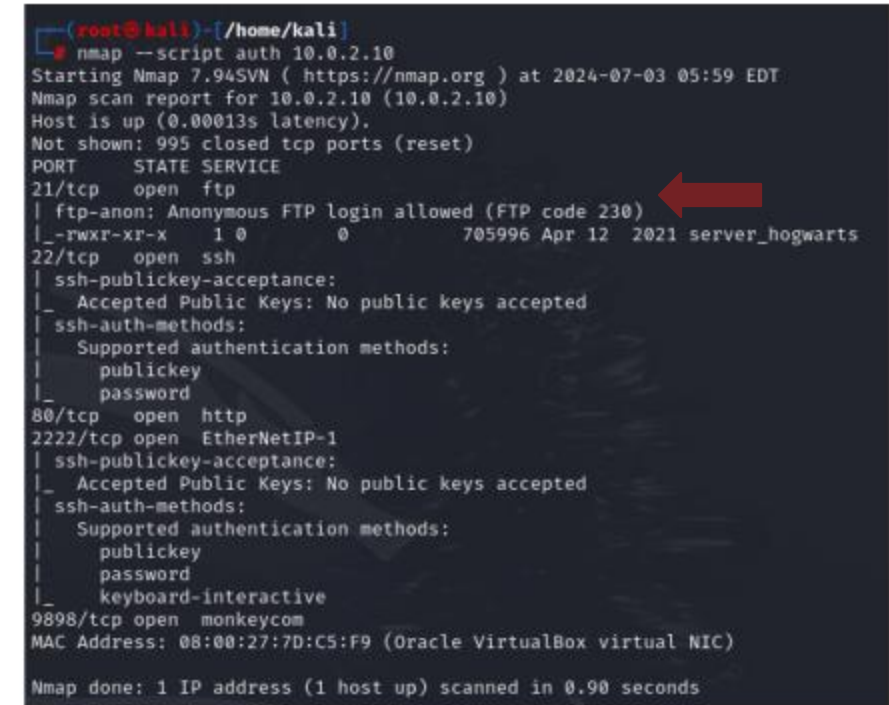
RICERCA DI VULNERABILITÀ TRAMITE NESSUS

- Sempre tramite il tool **nessus** si è poi proceduto ad utilizzare la modalità "Web Application Tests";
- Quest'ultima non ha riportato alcuna vulnerabilità.



RICERCA DI VULNERABILITÀ TRAMITE NMAP

- Utilizzando l'**nmap scripting engine (NSE)** sono state cercate ulteriori vulnerabilità;
- Il comando **nmap --script vuln 10.0.2.10** non ha restituito alcun risultato;
- Il comando **nmap --script auth 10.0.2.10** ha evidenziato la possibilità di effettuare accesso anonimo al servizio FTP erogato tramite la porta 21. Tale possibilità rappresenta una debolezza, identificata in **CWE-284: Improper Access Control**.



```
(root@kali)~[/home/kali]
# nmap --script auth 10.0.2.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 05:59 EDT
Nmap scan report for 10.0.2.10 (10.0.2.10)
Host is up (0.00013s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r-- 1 0 0 705996 Apr 12 2021 server_hogwarts
22/tcp    open  ssh
| ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
| ssh-auth-methods:
| Supported authentication methods:
| publickey
| password
|_ keyboard-interactive
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
| ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
| ssh-auth-methods:
| Supported authentication methods:
| publickey
| password
|_ keyboard-interactive
9898/tcp  open  monkeycom
MAC Address: 08:00:27:7D:C5:F9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
```

Figura 4.4: Controllo sulle credenziali di autenticazione tramite nmap

RICERCA DI VULNERABILITÀ MANUALE

- Sono state effettuate diverse query sul sito https://cve.mitre.org/cve/search_cve_list.html utilizzando come parametro i servizi e le versioni identificati precedentemente tramite nmap. Tali query hanno evidenziato le seguenti vulnerabilità:

- **High (7.8)** - CVE-2018-7566
- **High (7.8)** - CVE-2018-8781
- **High (7.8)** - CVE-2019-0211
- **High (7.5)** - CVE-2021-30047
- **High (7.5)** - CVE-2019-0215
- **High (7.5)** - CVE-2019-0217
- **Medium (6.7)** - CVE-2019-20908
- **Medium (6.7)** - CVE-2023-51385
- **Medium (5.5)** - CVE-2023-51384
- **Medium (5.3)** - CVE-2019-0220

RICERCA DI VULNERABILITÀ WEB

- Sono stati utilizzati i seguenti tool specifici per la ricerca di vulnerabilità su applicazioni web: **nikto**, **owasp zap**, **dirb**, **gobuster**.
- Nessuno dei tool elencati ha riportato vulnerabilità, né ha evidenziato un rilascio di informazioni sensibili e non accessibili normalmente tramite l'applicazione.

ACCESSO ANONIMO AL SERVER FTP

- Sfruttando la possibilità di effettuare accesso anonimo al server FTP è stato ottenuto il file **server_hogwarts**. Si è più tardi proceduto a verificare che tale file fosse l'eseguibile relativo al server sulla porta 9898.
- Effettuando reverse engineering tramite il tool **ghidra** è stato possibile verificare la presenza di una debolezza nell'utilizzo di funzioni che non controllano la taglia dell'input.
- Sfruttando la debolezza identificata si è proceduto con un attacco di tipo *buffer overflow* per l'esecuzione di uno shellcode che aprisse un terminale remoto sulla macchina host.

OTTENIMENTO DI UNA REMOTE SHELL

- Dalla remote shell aperta ci si è resi conto di essere in un ambiente containerizzato.
- Si è dunque passati alla fase di post-exploitation per tentare di effettuare privilege escalation e di ottenere accesso anche all'host principale.

PRIVILEGE ESCALATION VERTICALE

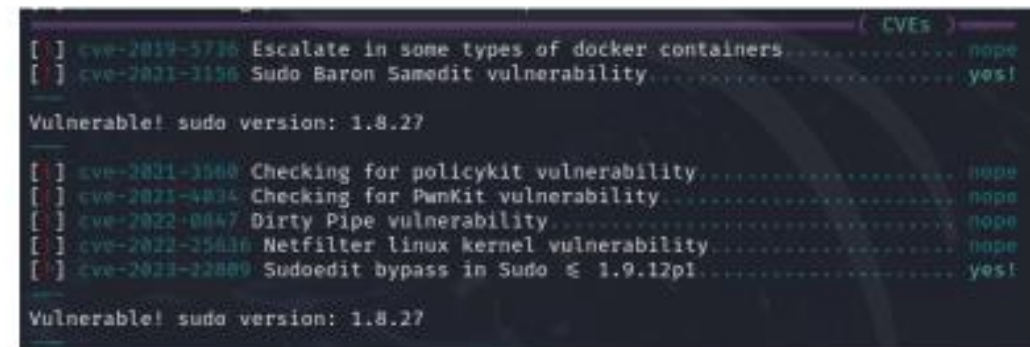
- Analizzando il sistema su cui è stata ottenuta una shell remota è stato possibile verificare che:
 - è presente un file contenente le credenziali (in chiaro) dell'utente **harry**;
 - l'utente **harry** ha accesso a tutti i comandi come *super user* senza necessità di effettuare autenticazione;
 - le conversazioni relative al protocollo FTP sono trasmesse in chiaro ed è dunque possibile ottenere informazioni sensibili analizzandole.

ANALISI DEL TRAFFICO DI RETE

- Tramite l'analisi del traffico di rete è stato possibile leggere le credenziali di accesso di un altro utente, **neville**.
- Tali credenziali hanno consentito l'accesso via ssh al sistema host - con hostname Fawkes.

PRIVILEGE ESCALATION (FAWKES)

- Utilizzando il tool **linux-enumerating-service (nse)**, il programma **sudo** presente sulla macchina Fawkes è risultato soggetto a due vulnerabilità:
 - **High (7.8)** - CVE-2021-3156
 - **High (7.8)** - CVE-2023-22809



```
( CVEs )
[ ] cve-2019-5736 Escalate in some types of docker containers.....nope
[ ] cve-2021-3156 Sudo Baron Samedit vulnerability.....yes!

Vulnerable! sudo version: 1.8.27

[ ] cve-2021-3560 Checking for policykit vulnerability.....nope
[ ] cve-2021-4434 Checking for PwnKit vulnerability.....nope
[ ] cve-2022-0847 Dirty Pipe vulnerability.....nope
[ ] cve-2022-25636 Netfilter linux kernel vulnerability.....nope
[ ] cve-2023-22809 Sudoedit bypass in Sudo < 1.9.12pl.....yes!

Vulnerable! sudo version: 1.8.27
```

Figura 6.11: Vulnerabilità della versione di sudo identificate da lse

PRIVILEGE ESCALATION VERTICALE (FAWKES)

- Sfruttando un exploit reperibile all'URL https://github.com/worawit/CVE-2021-3156/blob/main/exploit_nss.py è stato possibile ottenere privilegi di *root* sulla macchina Fawkes.
- Sono state aperte delle backdoor sfruttando eseguibili generati dal tool **msfvenom** per proseguire con l'attività di analisi.
- Non sono stati sfruttati altri tool per la creazione di backdoor poiché necessaria l'installazione di software adeguato sulla macchina host. Si è cercato di mantenere quanto più inalterato possibile il sistema presente sulla macchina.
- Le backdoor aperte sono state tutte documentate e successivamente chiuse. Maggiori informazioni sono disponibili sul documento di replicabilità.

CONCLUSIONI

- Sono state illustrate in maniera sommaria le vulnerabilità che affliggono l'host in analisi;
- È possibile porre rimedio a tali vulnerabilità senza necessità di sostenere costi eccessivi;
- Tramite le azioni di mitigazione esposte è possibile abbassare di molto il rischio per la sicurezza dell'asset;
- Le fasi di target exploitation e post-exploitation hanno avuto lo scopo principale di mostrare come un attaccante possa ottenere privilegi massimi sull'asset. Per tale motivo è necessario adottare le mitigazioni proposte il prima possibile.

GRAZIE PER L'ATTENZIONE