JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Passive Recon: Netstat

THREAT MANAGEMENT

Netstat

- Built-in utility in Windows, Linux, MacOS, and Unix operating systems
- Provides active TCP and UDP connections
- Identify process using a connection
- Provides statistics on sent/received data
- Route table information

netstat -a

- Provides active TCP and UDP connections filtered by TCP, UDP, ICMP, IP, IPv6, and more

```
Last login: Wed Sep 20 20:05:22 on ttys000
[Jasons-MacBook-Pro:~ hacking$ netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  10.40.8.249.54305      hyp01-packet-res.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54304      17.173.65.216.https    ESTABLISHED
tcp4       0      0  10.40.8.249.54302      usdal4-vip-bx-00.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54300      ec2-34-226-108-2.https ESTABLISHED
tcp4       0      0  10.40.8.249.54299      nyc28.ff.avast.c.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54298      mia27.ff.avast.c.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54296      a184-24-97-43.de.http  ESTABLISHED
tcp4       0      0  10.40.8.249.54295      a104-93-80-197.d.https ESTABLISHED
tcp4       0      0  10.40.8.249.54294      adobe.com.ssl.d1.https ESTABLISHED
tcp4       0      0  10.40.8.249.54293      a104-93-68-42.de.https ESTABLISHED
tcp4       0      0  10.40.8.249.54292      ec2-52-35-208-52.https ESTABLISHED
tcp4       0      0  10.40.8.249.54291      17.248.141.48.https    ESTABLISHED
tcp4       0      0  10.40.8.249.54290      ec2-52-35-208-52.https ESTABLISHED
tcp4       0      0  10.40.8.249.54289      adobe.com.ssl.d1.https ESTABLISHED
```


netstat -o

- Identify process using a connection

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49688        DESKTOP-1TI5NVD:49689  ESTABLISHED     1936
  TCP    127.0.0.1:49689        DESKTOP-1TI5NVD:49688  ESTABLISHED     1936
  TCP    192.168.66.129:55899   msnbot-65-52-108-222:https  ESTABLISHED     3684
  TCP    192.168.66.129:55902   msnbot-65-52-108-222:https  ESTABLISHED     1336
  TCP    192.168.66.129:55991   23.102.4.253:https     TIME_WAIT       0
  TCP    192.168.66.129:56000   134.170.58.123:https   ESTABLISHED     1336
```


netstat -e

- Ethernet statistics on sent/received data

```
Interface Statistics

                           Received            Sent

Bytes                    3019189716      2539479229
Unicast packets            22644273        11242559
Non-unicast packets               0               0
Discards                          0               0
Errors                            0               3
Unknown protocols                 0
```


netstat -r

- Displays route table information

```
Jasons-MacBook-Pro:~ hacking$ netstat -r
Routing tables

Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            10.40.8.1          UGSc          260       50     en0
10.40.8/21         link#6             UCS             0        0     en0
10.40.8.1/32       link#6             UCS             1        0     en0
10.40.8.1          1c:5e:c:64:e6:89   UHLWIir       274     2098     en0    749
10.40.8.249/32     link#6             UCS             0        0     en0
127                localhost          UCS             0        0     lo0
localhost          localhost          UH             25   902604     lo0
169.254            link#6             UCS             0        0     en0
172.16.145/24      link#16            UC              1        0  vmnet2
192.168.63         link#15            UC              1        0  vmnet1
192.168.66         link#17            UC              2        0  vmnet8
192.168.66.129     0:c:29:74:67:55     UHLWI           0        0  vmnet8    670
```