Basic Networking

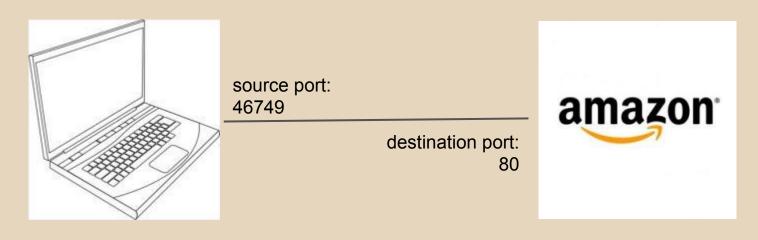
GTFO Security

outline

- basic networking
 - o ports
 - examples
 - tools
- packets
 - basics
 - examples
 - tools

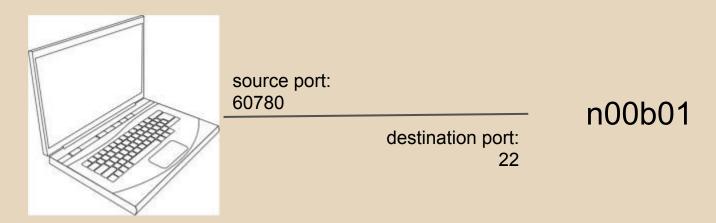
Ports

- A computer has 65535 ports.
- When two computers communicate, they connect through ports.
- Example: connecting to the web



Ports

Example: connecting to the n00bs



- Destination ports are standardized
- Source ports are randomized (mostly)

Ports

- More examples
 - o HTTPS 443
 - o FTP 23
 - PostgreSQL 5432
- Ports communicate information between computers.
- We call this a connection.

Illustration of Ports

Destination	Source
nc -l 9000	nc <destination> 9000 type something</destination>
nc -l 8000 > myfile	nc <destination> 8000 < /etc/passwd</destination>
netstat -apn grep 7000 nc -l 7000 netstat -apn grep 7000	netstat -apn grep 7000 nc <destination> 7000 netstat -apn grep 7000</destination>
sudo lsof -i -n grep 5000 nc -l 5000 sudo lsof -i -n grep 5000	sudo lsof -i -n grep "nc " nc <dest> 5000 sudo lsof -i -n grep "nc "</dest>

netstat

```
ieee8023@ieee8023-ThinkPad-T60: ~
ieee8023@ieee8023-ThinkPad-T60:~$ netstat -apn | head
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address
                                            Foreign Address
                                                                     State
                                                                                 PID/Program name
tcp
                                                                     LISTEN
                  0 127.0.0.1:631
                                            0.0.0.0:*
tcp
                 0 127.0.0.1:8089
                                            0.0.0.0:*
                                                                     LISTEN
                                                                                 7707/banshee
tcp
                 0 0.0.0.0:8000
                                                                     LISTEN
                                                                                 10360/nc
                                            0.0.0.0:*
             0 192.168.8.117:45252
                                            74.125.93.189:443
                                                                     ESTABLISHED 5111/firefox
tcp
             0 192.168.8.117:51040
                                            158.121.104.22:443
                                                                     ESTABLISHED -
tcp
                 0 192.168.8.117:47585
                                            74.125.113.106:80
                                                                     ESTABLISHED 5111/firefox
tcp
                  0 192.168.8.117:50941
                                            74.125.226.223:80
                                                                     ESTABLISHED 5111/firefox
tcp
                  0 192.168.8.117:50802
                                            74.125.226.203:80
                                                                     ESTABLISHED 5111/firefox
tcp
ieee8023@ieee8023-ThinkPad-T60:~$ s
```

- Shows listening ports / established conections
- Invoke using -apn
- Protocol UDP / TCP
- Address <IP> : <port>
- State LISTEN / ESTABLISHED / SYN_SENT / SYN_RECEIVED

lsof

```
ieee8023@ieee8023-ThinkPad-T60: ~
ieee8023@ieee8023-ThinkPad-T60:~$ lsof -i -n -P
COMMAND
            PID
                           FD
                                TYPE DEVICE SIZE/OFF NODE NAME
                    USER
           4958 ieee8023
gvfsd-htt
                                IPv4 75373
                                                      TCP 192.168.0.61:35099->91.189.89.31:80 (CLOSE WAIT)
firefox
           5111 ieee8023
                                IPv4 286523
                           28u
                                                      TCP 192.168.8.117:40855->72.14.204.189:443 (ESTABLISHED)
firefox
           5111 ieee8023
                           29u
                                IPv4 286563
                                                      TCP 192.168.8.117:40856->72.14.204.189:443
firefox
           5111 ieee8023
                           30u
                                IPv4 289230
                                                  0t0 TCP 192.168.8.117:40857->72.14.204.189:443
          5111 ieee8023
firefox
                           55u
                                                  0t0 TCP 192.168.8.117:40858->72.14.204.189:443
                                IPv4 289301
firefox
          5111 ieee8023
                           62u
                                IPv4 286331
                                                  0t0 TCP 192.168.8.117:35077->74.125.226.213:443 (ESTABLISHED)
firefox
          5111 ieee8023
                                IPv4 286053
                                                  0t0 TCP 192.168.8.117:46169->74.125.226.118:443 (ESTABLISHED)
                           63u
firefox
           5111 ieee8023
                           69u
                                IPv4 286483
                                                      TCP 192.168.8.117:38732->74.125.226.196:443 (ESTABLISHED)
          11641 ieee8023
                                                       TCP 192.168.8.117:53989->74.125.115.109:993 (ESTABLISHED)
                            3u
                               IPv4 289311
nc
```

- Shows listening ports / established connections
- Command that opened / accepted port
- PID of process
- User owner of process
- Node TCP / UDP
- Name Source IP : Port -> Destination IP : Port (Status)

netcat (nc)

- Connect Mode
 - Connects to remote port
 - Syntax: nc <dest_ip> <port>
- Listen mode
 - Opens port for raw data transfer
 - Syntax: nc -l <port>
- Piping to / from netcat
 - Can transfer files
 - Can be used as remote shell

Packets

Packets

- Data is sent in packets
 - UDP single burst of packets
 - TCP constant stream of packets
- Format of packets determined by protocols
 - Packets wrapped in several different protocols
- Types of packets
 - SYN begins connections
 - ACK acknowledgement to receive ACK
 - FIN connection finished
 - RST reset (close) connection
 - Data is sent over all of these

Packets

- We can inspect packets for various contents
 - Destination IP / Source IP
 - Destination port / Source port
 - Protocol
 - Data
- Some packets use encrypted protocols and cannot be inspected

Packet Sniffing

- Packets sniffers inspect all packets coming to / from machine
- Can also inspect packets to / from other machines
 - Promiscuous mode
 - Hubs
 - Span port on routers
- Tools
 - tcpdump
 - Wireshark

tcpdump

- Command line Linux tool
- Powerful syntax for filtering packets
- Examples
 - tcpdump src port not 22 and dst port not 22
 - tcpdump dst citizensbank.com
- Useful to pipe to file

Wireshark

- Powerful GUI tool for packet sniffing
- Easy to use
- Can filter on live output
- Filtering syntax similar to tcpdump