Exercise #1: List Three Tools that were discussed in the last lecture

1. Maltego
2. Cree.py
3. Mxtoolbox

traceroute: maps the path of network traffic from one point to another
traceroute to nyu:

```
7  lag-65.nyquny9101r.netops.charter.com (68.173.202.94)  20.008 ms  23.386 ms  21.190 ms
8  lag-25-10.nycmny837aw-bcr00.netops.charter.com (107.14.19.22)  40.832 ms  18.746 ms
lag-15-10.nycmny837aw-bcr00.netops.charter.com (66.109.6.76)  22.141 ms
9  lag-1.pr2.nyc20.netops.charter.com (66.109.9.5)  19.566 ms  19.829 ms  22.274 ms
10  * *
11  209.66.118.177.idia-282827-zyo.zip.zayo.com (209.66.118.177)  25.919 ms  22.067 ms  19.946 ms
12  *
13  *
14  * *
15  ngfw-palo-vl3090.net.nyu.edu (128.122.254.254)  24.233 ms  15.750 ms  16.282 ms
```

15: shows that nyu is using ngfw palo alto firewalls, and vl3090 can mean the vlan #.
You can search for known ngfw palo alto vulnerabilities.
Why is this info out here?

1. It could be an accident
2. It could be chosen - honeypot
3. Troubleshooting purposes

Shodan - IoT search engine

DNS Zone Transfer: process of replicating a DNS zone's resource records (mapping domain names to IP addresses) from one DNS server to another
Horrible practice today
Brute Force Forward DNS - trying to guess DNS names
firewall.example.com, vpn.example.com, etc

Split DNS: main technique to stop this. External DNS has info on DMZ servers. Internal DNS has info on internal servers. Prevents leakage of internal DNS information

TCP Header: Source Port, Dst Port, Seq #, Ack #

Port Scanning finds what services are running on ports
If a port is open and a SYN packet is sent, and and a synack is sent back
If a port is closed and a SYN packet is sent, a TCP rst is sent back. You can also get an ICMP destination unreachable back. This can mean network error or firewall blocking.

Sending a TCP syn packet, you can get 4 potential responses:

1. Get a SYNACK == Port Open
2. get TCP rst == port closed
3. icmp destination unreachable == network error or firewall rejecting packets
4. No response : network error, firewall dropping packets

DROP vs REJECT:
Drop == no response
Reject == send ICMP destination unreachable. "Nice" method
Drop would probably be better security, but reject is better for troubleshooting if you're internal to a network

Exercise #2:
Explain the three steps in the TCP 3-way handshake
5. The client initiates the connection by sending a SYN packet. It contains the initial sequence number for the client.
6. The server responds with a SYN ACK. It has its own sequence number and an ACK number that is the client's sequence number plus one.
7. The client responds with an ACK and the connection is ready to start.

Hping - runs on all unix like systems, windows version
faster than scapy
Can be used to write scripts implementing low level packet manipulation very quickly

TCP Connect scan - This type of scan is the most reliable, although it is also the most detectable. It is easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK, whereas closed ports respond with an RST/ACK. Uses standard connect() system call.
TCP SYN scan - This type of scan is known as half open because a full TCP three-way connection is not established. This type of scan was originally developed to be stealthy and evade IDS systems although most now detect it. Open ports reply with a SYN/ACK, whereas closed ports respond with a RST/ACK.
TCP FIN scan - This type of scan sends a FIN packet to the target port. Closed ports should send back an RST. This technique is usually effective only on UNIX devices.
TCP NULL scan - a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST.

TCP XMAS - port scan that has toggled on the FIN, URG, and PSH flags. Closed ports should return an RST.

XMAS, FIN, NULL scans are usually used to identify the operating system.

TCP ACK scan - This scan attempts to determine firewall access control list (ACL) rule sets or identify if stateless inspection is being used. If a RST packet returned, it means the port is ether open or closed. If an ICMP destination unreachable, communication administrative prohibited message is returned, the port is considered to be filtered.

ACK scan: purpose is to map out firewall rulesets and determine if ports are filtered or unfiltered

FTP Proxy “bounce attack” scans – bounce an attack off a poorly configured FTP server
Version Scanning – tries to determine the version number of the program listening on the port
Fragmented Scans – can get around some router ACL packet filters that do not examine the port number in fragmented packets.
TCP Sequence Prediction – useful in spoofing attacks

Exercise #3:
What information can obtained from a nmap SYN scan, and how does nmap perform it?
Nmap can figure out which ports are open when a SYN ACK is sent back

UDP Scanning:
Every UDP port scanned takes one second.

Exercise #4:
In UDP scanning, what are the three responses and the meaning of each?
Port Open: send a probe, get a response
Port is Closed: UDP probe is sent, icmp destination unreachable is sent back (not to be confused with the TCP response with that. That means a firewall is in the way)
No Response: Network issues, filter (blocked by firewall), transmission error

Exercise # A
Explain the difference between a TCP SYN scan and a TCP connect scan:
A SYN scan sends a syn packet to a target port. If the port is open, it responds with a SYN-ACK. If it is closed, a TCP rst is sent. If an ICMP destination unreachable is sent, then very likely a firewall is blocking it. If no response is sent, then there may be a network error. In a SYN scan, the sender sends a RST packet to end the connection.
In a connect scan, the full handshake is completed with the sender sending the SYN, the SYN/ACK being sent by the target, and the ACK being sent by the sender. It then closes the connection with a FIN.

SYN scans are more useful generally, but connect scans can be used if administrative privileges aren't available.