Exercise #1
Explain the following nmap scan types:
TCP Connect Scan: Default scan, makes a full TCP connection (3 way handshake is completed) to discover open ports. Sends a RST packet after final ACK to kill connection.
TCP SYN Scan: Sends SYN packet and gets back a SYN ACK to discover open ports (partial 3 way handshake, kills connection before final ACK) , used when nmap has access to elevated privileges. Also known as a half open scan
TCP FIN Scan: Sends TCP packets with FIN flag set. If port is closed, the target responds with RST.
TCP Null Scan: Does not set any bits, closed ports will respond with RST.
TCP XMAS: sets FIN, PSH, and URG flags. Closed ports respond with RST.
FIN,NULL, XMAS are used to identify operating system
TCP ACK scan: only sends ACK packets, used to map out firewall rulesets.

Cyber Kill Chain:
The cyber kill chain maps out the cycle of an attacker getting into a system
The idea of the kill chain is to stop the attacker somewhere on the chain

Where do vulnerabilities come from? Why do systems have vulnerabilities?

Sources of Insecurity:
Standards
Requirements
Architecture
Design
Implementation
Configuration
Operations
People
Mindset

Security is not often the top of mind for organizations

Configuration Security
The configuration of a network is probably the number one source of access for a hacker
No easy way to view configurations for completeness - misconfigurations ar therefore hidden

IP Address Spoofing: Attacker doesn't want actions traced back, very easy and little can be done to stop it

Ways to try to stop:
Egress Filtering: Stopping and monitoring the flow of information outbound from on network to another - rarely done (stopping packets from leaving networks)
Ingress Filtering: used to ensure incoming packets are actually from the networks from which they claim to originate (stopping packets from coming into network)

Session Hijacking: Take control of one side of a TCP connection - a marriage of sniffing and snooping

Exercise #2: Since you can only hijack the telnet session once (or any TCP connection once), how can you establish Command and Control with the target?
Create a reverse shell with that hijacking

Why does the original connection fail?
The sequence and ack numbers are out of wack due to the session hijacking. The client and server tries to resynchronize, there is a few attempts at retransmission before the connection fails (in wireshark these are red and black packets)

How else can the attacker take someone offline?
Vulnerability attack: Send a few crafted messages to target app that has vulnerability
•Malicious messages called the “exploit”
•Remotely stopping or crashing services

Connection Flooding: overwhelming connection queue with SYN flood
Bandwidth flooding attack: Overwhelming communication link with packets

Exercise #3:
What are 2 methods to mitigate a SYN Flood:

1. Using SYN Cookies - generating a unique cookie and sending it in the SYN-ACK and wait for the ACK before opening the connection
2. Recent Connection Cache: a small cache of recent connections - typical system reservers about 25% of the connections to be only used by the recently used connections

Exercise #4:
Aside from SYN Flood, name and describe another type of DDOS attack.
UDP Flood: large number of UDP packets are sent to a targeted server with the aim of overwhelming that device's ability to process and respond.

DDoS is a generic term for "sending lots of junk" to a target. It can be done with a lot of protocols.
Attacker controls a bunch of bots that attack a particular victim.
Where do bots come from? From hacked systems. Back in the day, it could be a hacked

computer. But today, IoT devices do outnumber computers.
It can be done with any protocol.
Using the DNS Protocol:
One of the biggest DDoS attacks was done with the DNS protocol (UDP).
Attacker will send a DNS request to a server to get a response. The response goes to the victim. The maximum size of a reply is 512 bytes max. A DNS request can vary, but it can be 60 to 80 bytes.
Attacker can send a packet 70 bytes in size, but then the DNS response can be up to 512 bytes in size.
This is an amplification attack: Attacker sends something small, and server amplifies it.
This is a reflection attack: Attacker sends to DNS server, the DNS server is the one "attacking" the victim

DNS Amplification Attack: sends forged DNS requests with spoofed source IP addresses to DNS servers

Exercise #5
Assuming that your browser and the DNS servers has not been on the Internet for a while, what are the steps (in terms of DNS) that occur when you want to visit the site:
https://www.nytimes.com/section/science

Exercise A: Describe Three types of Denial of Service Attacks and explain a mitigation strategy for each.