Lab 2 - Due Jun 22 (5% bonus for early submission)
Exercise #1 : List three topics that we discussed

1. Risk Management
2. Qualitative vs Quantitative risk assessment
3. Mat Honan hack

Why teach how to hack into systems?
Most important tools: nmap for scanning network, nessus for finding vulnerabilities, metasploit for exploits.
These tools only work on known vulnerabilities.
Tomorrow - 06-10 is patch tuesday (second tuesday of the month) - security patch

For a pentest there must be:

1. Written permission from someone authorized to give that permission - CISO, CIO, CEO for example
2. Scoping/Rules of Engagement - outlines: which systems are being targeted, which are not, IP address range, etc. What you are allowed/not allowed to do. Who are points of contact - if you accidentally do something wrong, who do you call?

General Assumption: bypassing protection is illegal, no matter what

Emanation Eavesdropping: radio waves to find info about sender

Why do hacks occur:
Fame: Not so much now
Money
War
There is research every year to figure it out - right now mostly for money. Could change.

The Cyber Kill Chain:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives

Lab 2

Expands on lab 1 to sniff packets. Use scapy - sniff() to capture packets.
Q1: Can you sniff() to capture packets?
Q2: Spoof ICMP echo request packets
Q3: Traceroute program: sends out icmp echo requests with incrementing TTL.
Challenges for this portion: How do you know that you reached the destination?
if IP addr == destination
How do you handle if a node does not respond?
Q4: spoof icmp echo replies
sniff icmp echo request as attacker and also send the icmp echo reply
1. ping 1.2.3.4 - host unreachable is the normal response, the attacker/program needs to reply back anyway with icmp echo reply
2. ping 10.9.0.99 - host unreachable due to non-existing host on subnet, with program running, there is also host unreacable/timeout
1. This is because if the host is on the same subnet, there is an ARP request first.
3. ping 8.8.8.8 - normal icmp echo reply, with program running there will be 2 replies per ping
Q5: extra credit: Q4.3 with ARP cache poisoning

Scapy sniff() caveat:
filter must be set correctly
Must be careful that scapy does not pull in what it just sent out - must exclude packets scapy sent out

Reconnaissance - Information Gathering

Finding information about the target.
IP address, network topology, domain names, user account names, operating systems/software being used, security policies, etc.

Public information from public databases, dumpster diving, social engineering, DNS or searching services, physical break ins
Changing caller-ID is easy to do

Google hacking: making google searches more useful
"site:" searches within only a given domain
"intitle:"
"inurl:"

Exercise #2: How would you find a file on nyu.edu with the string: this file was generated by nessus
site:nyu.edu “this file was generated by nessus”

https://www.exploit-db.com/google-hacking-database

Edgar Database - sec.gov
Publicly traded companies

Maltego
Cree.py - open source intelligence gathering application
Can gather from Twitter

Exercise #3: What are some ways you would obtain information from a company using public sources?

1. Browse social media like LinkedIn
2. OSINT framework
3. theHarvester: gathers names, emails, IPs, subdomains, URLs

MXtoolbox: check DNS records
Robtex

Exercise #4: What is the difference between whois and DNS, and what information can you obtain from each?
whois: who owns the domain, who registered, contact details
DNS: translates domain names into IP address

Exercise A: Explain three methods used for network reconnaissance and provide a security measure to mitigate the risks (if possible) associated with each method.