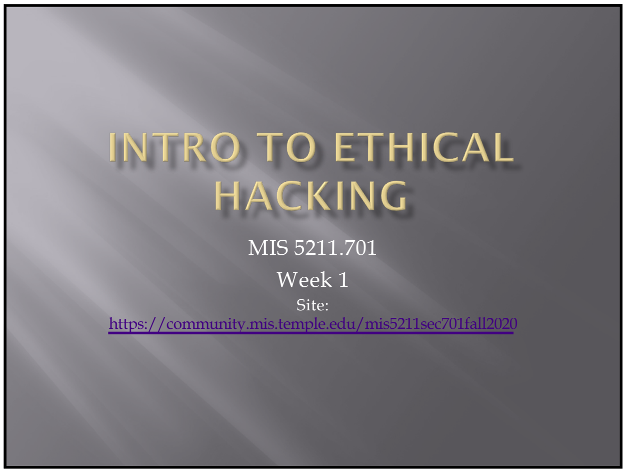


INTRO TO ETHICAL HACKING

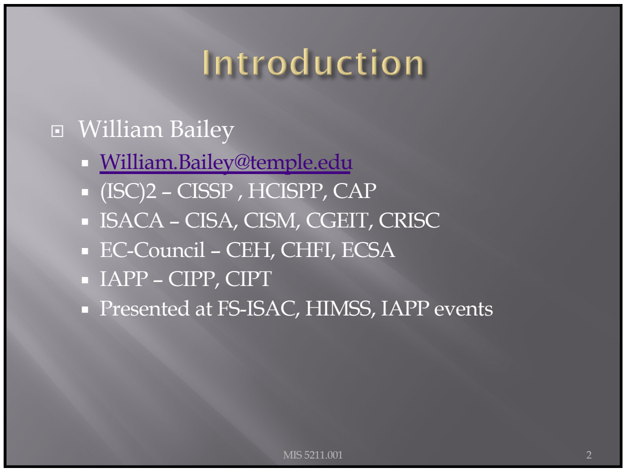
MIS 5211.701

Week 1

Site:

https://community.mis.temple.edu/mis5211sec701fall2020

1

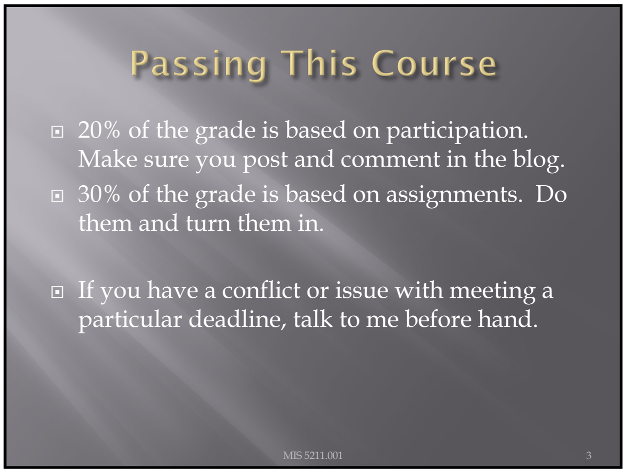


Introduction

- William Bailey
  - William.Bailey@temple.edu
  - (ISC)2 – CISSP , HCISPP, CAP
  - ISACA – CISA, CISM, CGEIT, CRISC
  - EC-Council – CEH, CHFI, ECSA
  - IAPP – CIPP, CIPT
  - Presented at FS-ISAC, HIMSS, IAPP events

MIS 5211.001 2

2

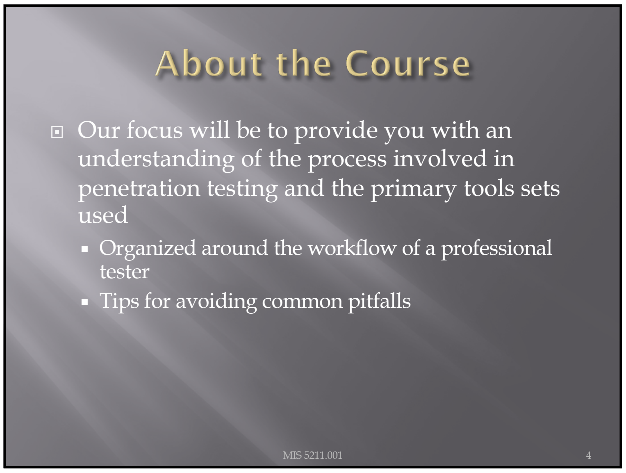


Passing This Course

- 20% of the grade is based on participation. Make sure you post and comment in the blog.
- 30% of the grade is based on assignments. Do them and turn them in.
- If you have a conflict or issue with meeting a particular deadline, talk to me before hand.

MIS 5211.001 3

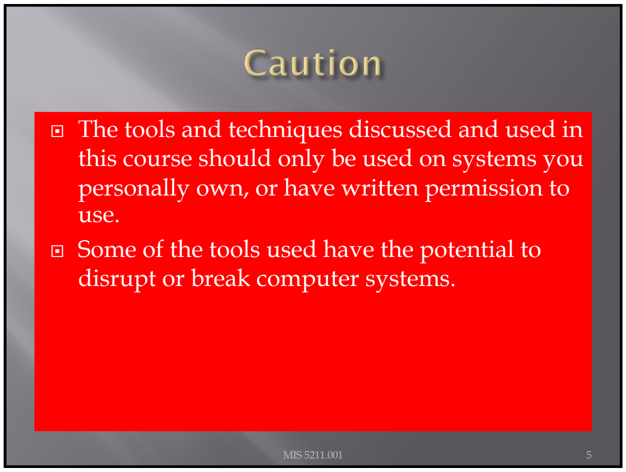
3



About the Course

- Our focus will be to provide you with an understanding of the process involved in penetration testing and the primary tools sets used
  - Organized around the workflow of a professional tester
  - Tips for avoiding common pitfalls

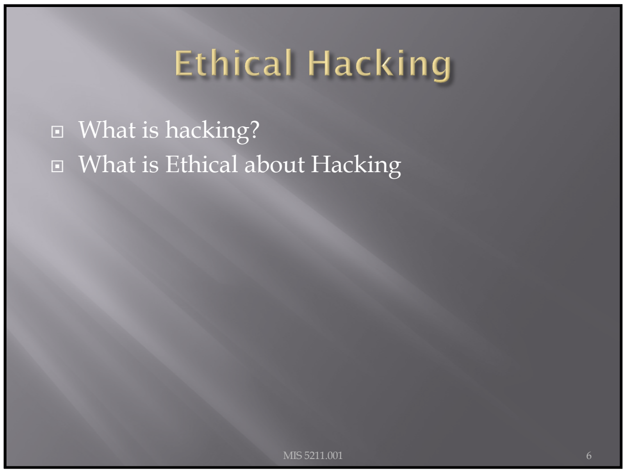
4



Caution

- The tools and techniques discussed and used in this course should only be used on systems you personally own, or have written permission to use.
- Some of the tools used have the potential to disrupt or break computer systems.

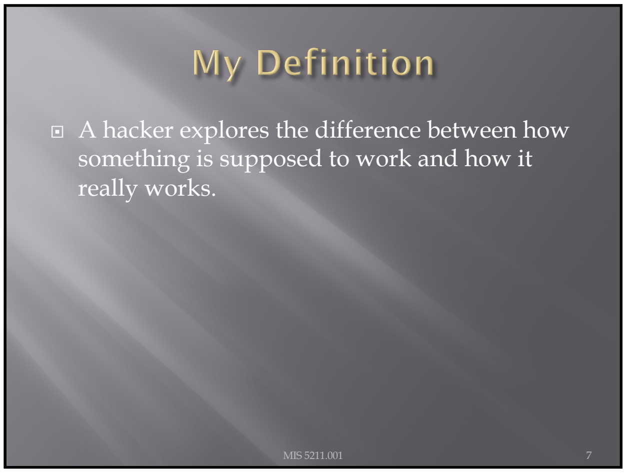
5



Ethical Hacking

- What is hacking?
- What is Ethical about Hacking

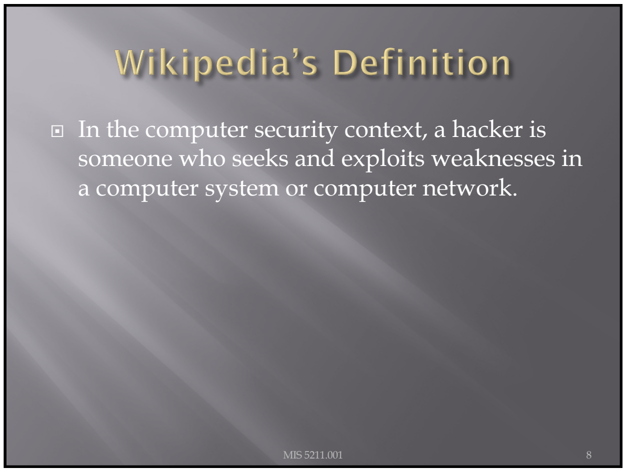
6



My Definition

- A hacker explores the difference between how something is supposed to work and how it really works.

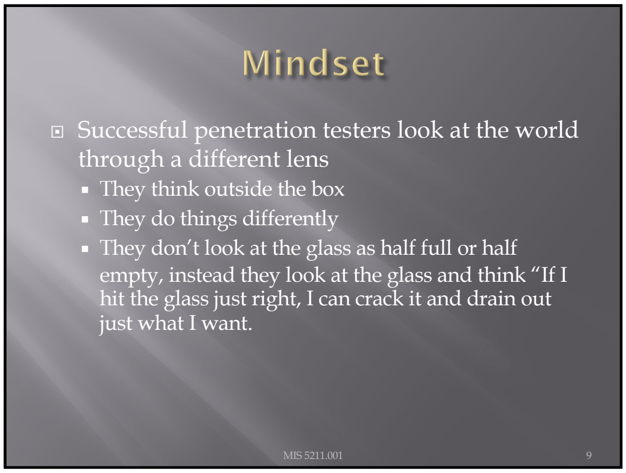
7



Wikipedia's Definition

- In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network.

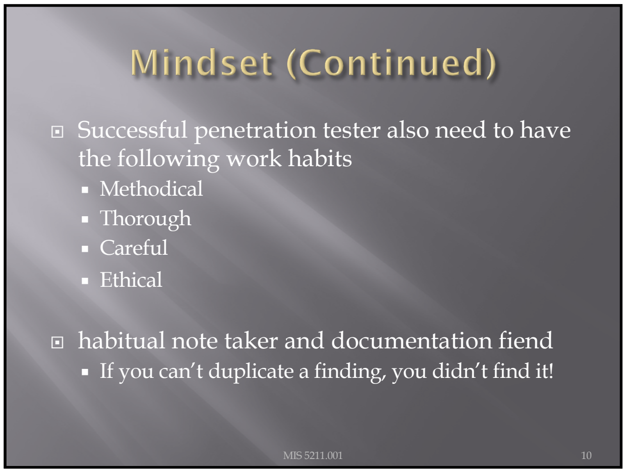
8



Mindset

- Successful penetration testers look at the world through a different lens
  - They think outside the box
  - They do things differently
  - They don't look at the glass as half full or half empty, instead they look at the glass and think "If I hit the glass just right, I can crack it and drain out just what I want.

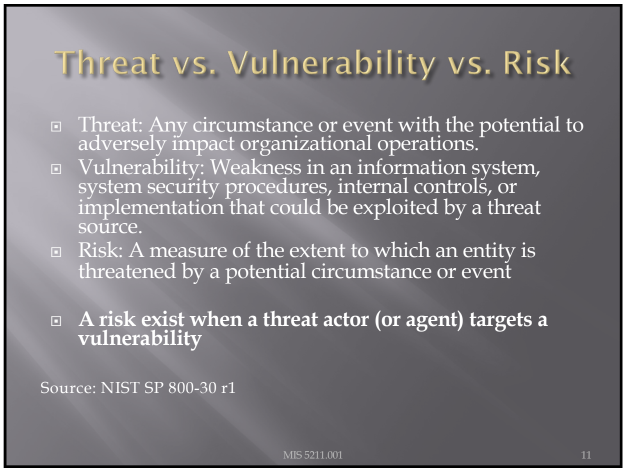
9



Mindset (Continued)

- Successful penetration tester also need to have the following work habits
  - Methodical
  - Thorough
  - Careful
  - Ethical
- habitual note taker and documentation fiend
  - If you can't duplicate a finding, you didn't find it!

10

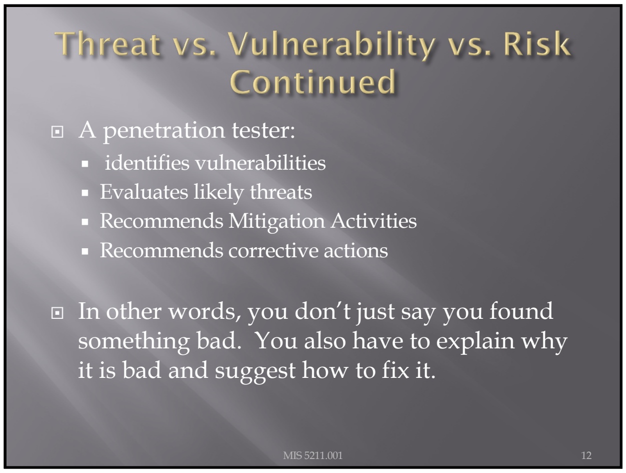


Threat vs. Vulnerability vs. Risk

- Threat: Any circumstance or event with the potential to adversely impact organizational operations.
- Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
- Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event
- **A risk exist when a threat actor (or agent) targets a vulnerability**

Source: NIST SP 800-30 r1

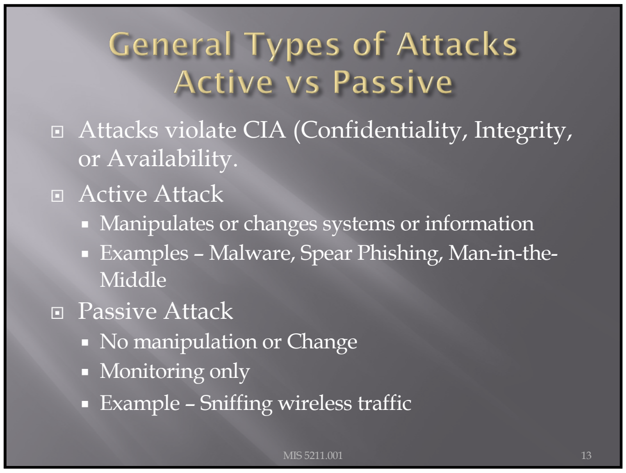
11



Threat vs. Vulnerability vs. Risk Continued

- A penetration tester:
  - identifies vulnerabilities
  - Evaluates likely threats
  - Recommends Mitigation Activities
  - Recommends corrective actions
- In other words, you don't just say you found something bad. You also have to explain why it is bad and suggest how to fix it.

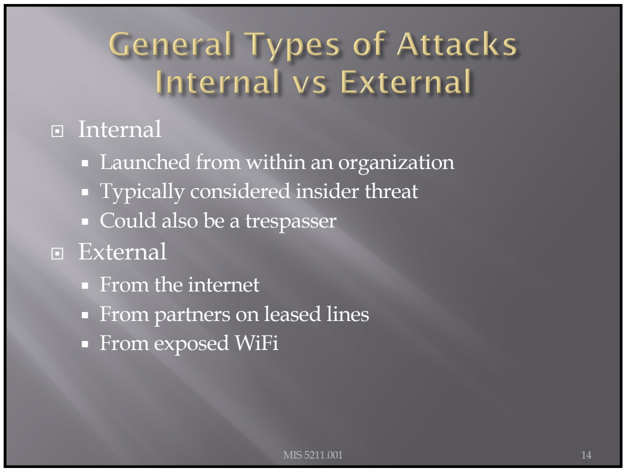
12



General Types of Attacks Active vs Passive

- Attacks violate CIA (Confidentiality, Integrity, or Availability.
- Active Attack
  - Manipulates or changes systems or information
  - Examples – Malware, Spear Phishing, Man-in-the-Middle
- Passive Attack
  - No manipulation or Change
  - Monitoring only
  - Example – Sniffing wireless traffic

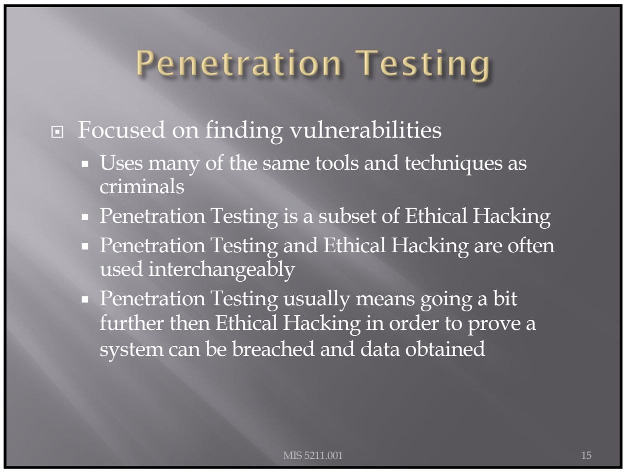
13



General Types of Attacks Internal vs External

- Internal
  - Launched from within an organization
  - Typically considered insider threat
  - Could also be a trespasser
- External
  - From the internet
  - From partners on leased lines
  - From exposed WiFi

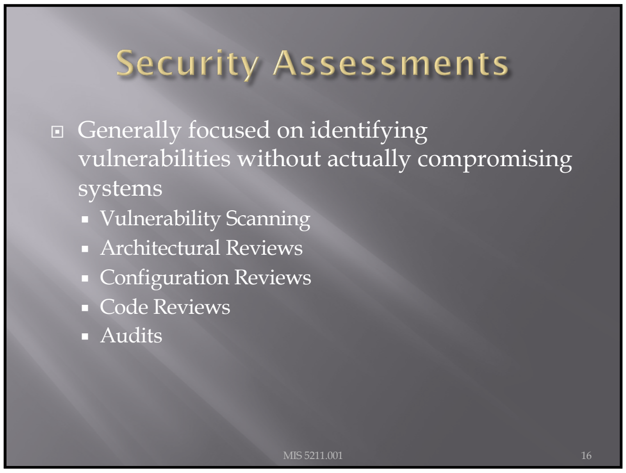
14



Penetration Testing

- Focused on finding vulnerabilities
  - Uses many of the same tools and techniques as criminals
  - Penetration Testing is a subset of Ethical Hacking
  - Penetration Testing and Ethical Hacking are often used interchangeably
  - Penetration Testing usually means going a bit further then Ethical Hacking in order to prove a system can be breached and data obtained

15

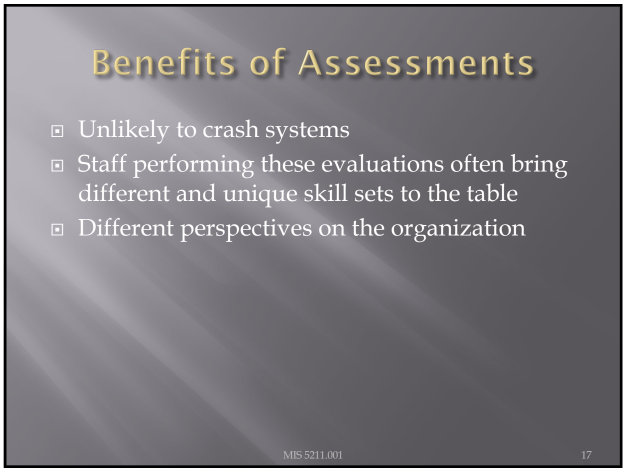


Security Assessments

- Generally focused on identifying vulnerabilities without actually compromising systems
  - Vulnerability Scanning
  - Architectural Reviews
  - Configuration Reviews
  - Code Reviews
  - Audits

MIS 5211.001 16

16

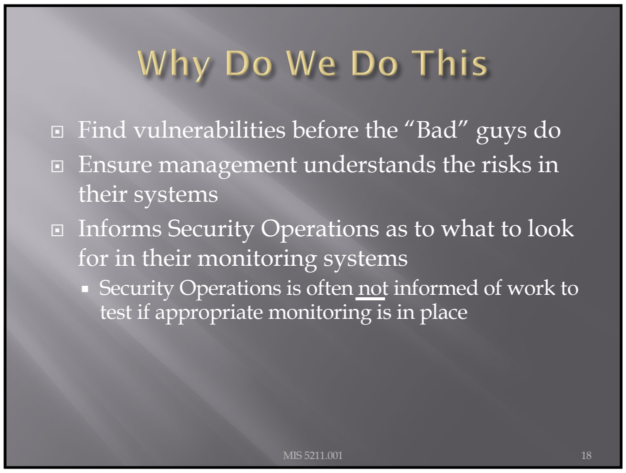


Benefits of Assessments

- Unlikely to crash systems
- Staff performing these evaluations often bring different and unique skill sets to the table
- Different perspectives on the organization

MIS 5211.001 17

17

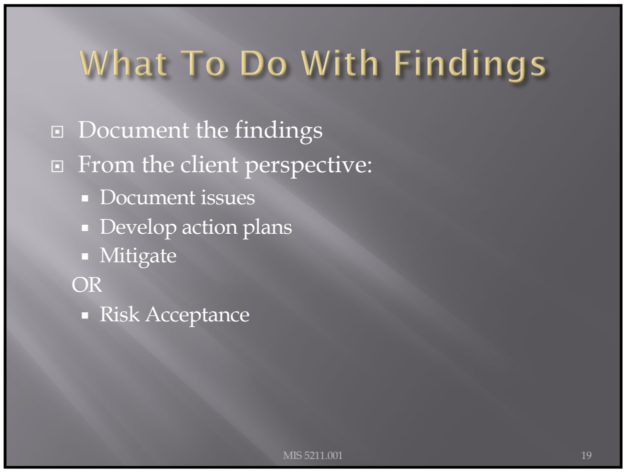


Why Do We Do This

- Find vulnerabilities before the "Bad" guys do
- Ensure management understands the risks in their systems
- Informs Security Operations as to what to look for in their monitoring systems
  - Security Operations is often not informed of work to test if appropriate monitoring is in place

MIS 5211.001 18

18

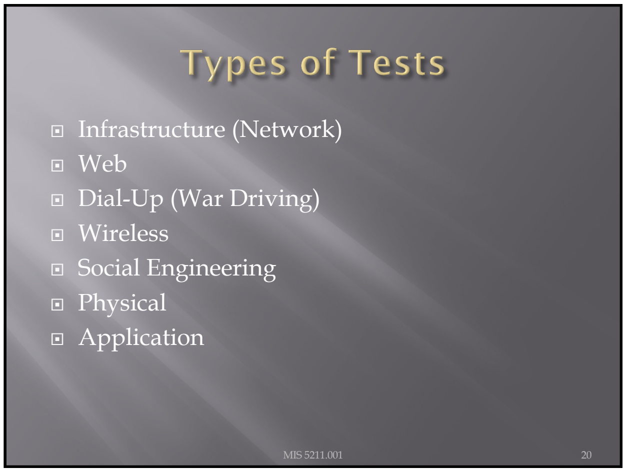


What To Do With Findings

- Document the findings
- From the client perspective:
  - Document issues
  - Develop action plans
  - Mitigate

  OR
  - Risk Acceptance

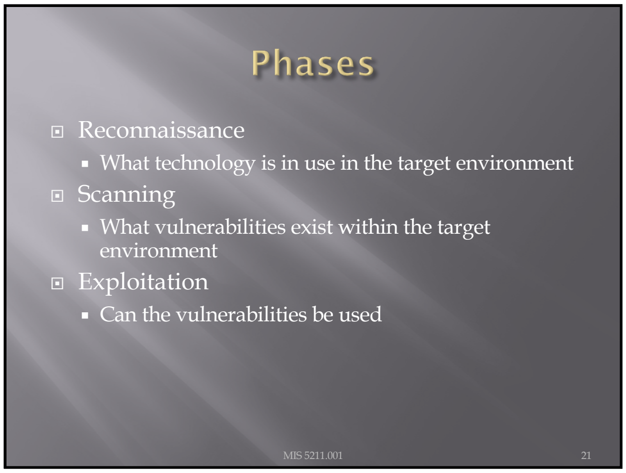
19



Types of Tests

- Infrastructure (Network)
- Web
- Dial-Up (War Driving)
- Wireless
- Social Engineering
- Physical
- Application

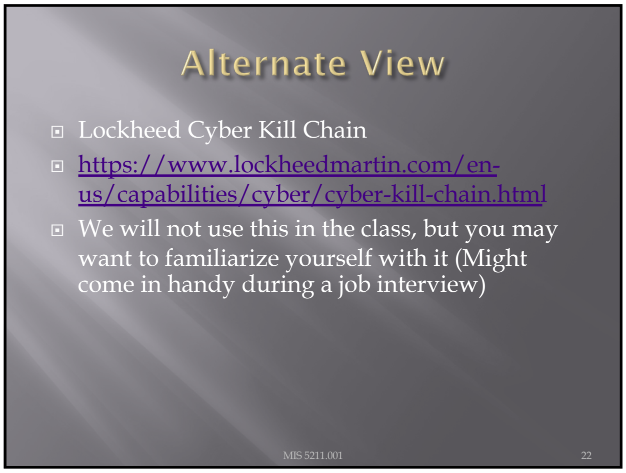
20



Phases

- Reconnaissance
  - What technology is in use in the target environment
- Scanning
  - What vulnerabilities exist within the target environment
- Exploitation
  - Can the vulnerabilities be used

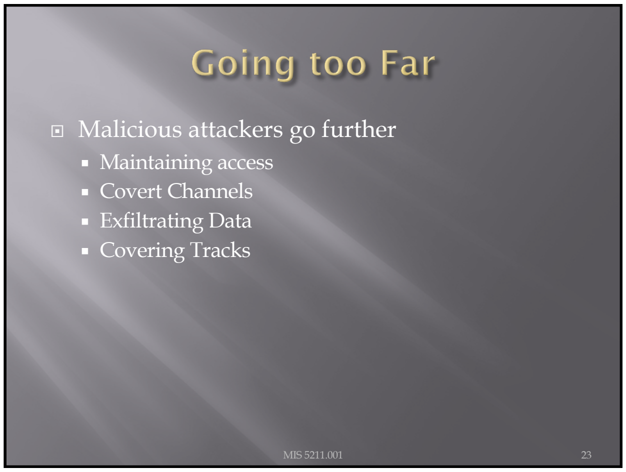
21



Alternate View

- Lockheed Cyber Kill Chain
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- We will not use this in the class, but you may want to familiarize yourself with it (Might come in handy during a job interview)

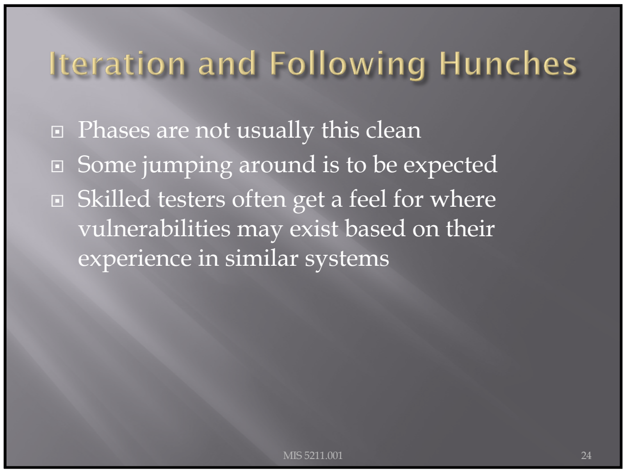
22



Going too Far

- Malicious attackers go further
  - Maintaining access
  - Covert Channels
  - Exfiltrating Data
  - Covering Tracks

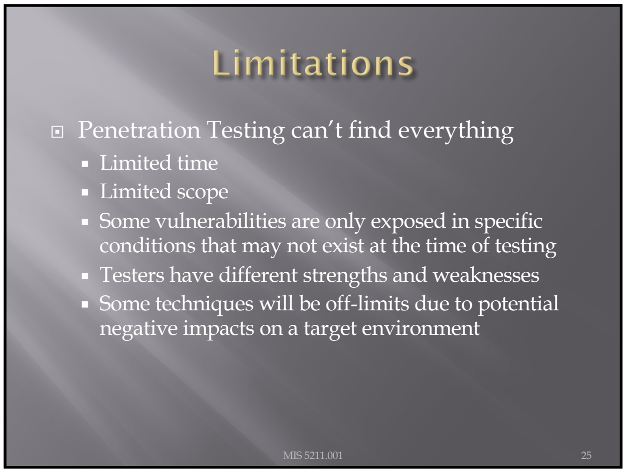
23



Iteration and Following Hunches

- Phases are not usually this clean
- Some jumping around is to be expected
- Skilled testers often get a feel for where vulnerabilities may exist based on their experience in similar systems

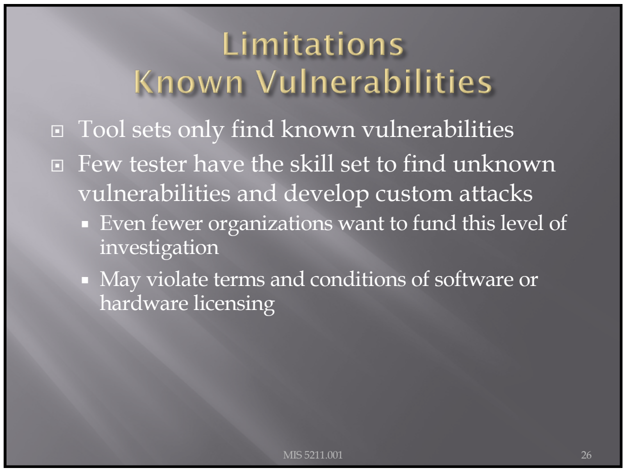
24



Limitations

- Penetration Testing can’t find everything
  - Limited time
  - Limited scope
  - Some vulnerabilities are only exposed in specific conditions that may not exist at the time of testing
  - Testers have different strengths and weaknesses
  - Some techniques will be off-limits due to potential negative impacts on a target environment

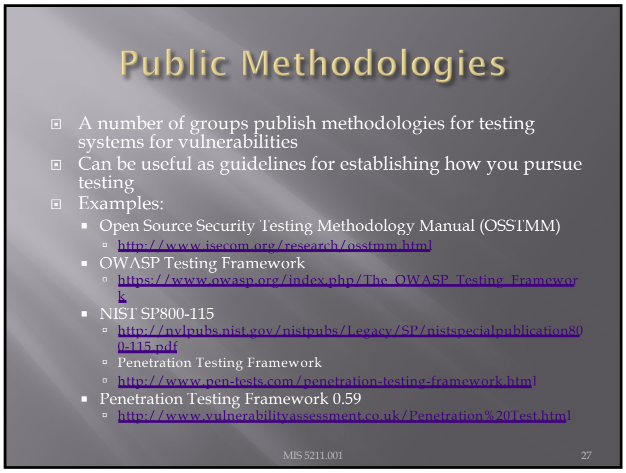
25



Limitations
Known Vulnerabilities

- Tool sets only find known vulnerabilities
- Few tester have the skill set to find unknown vulnerabilities and develop custom attacks
  - Even fewer organizations want to fund this level of investigation
  - May violate terms and conditions of software or hardware licensing

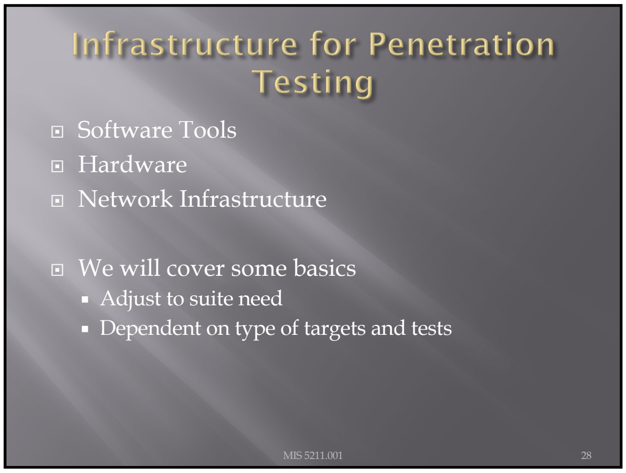
26



Public Methodologies

- A number of groups publish methodologies for testing systems for vulnerabilities
- Can be useful as guidelines for establishing how you pursue testing
- Examples:
  - Open Source Security Testing Methodology Manual (OSSTMM)
    - http://www.isecom.org/research/osstmm.html
  - OWASP Testing Framework
    - https://www.owasp.org/index.php/The_OWASP_Testing_Framework
  - NIST SP800-115
    - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
    - Penetration Testing Framework
    - http://www.pen-tests.com/penetration-testing-framework.html
  - Penetration Testing Framework 0.59
    - http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

27



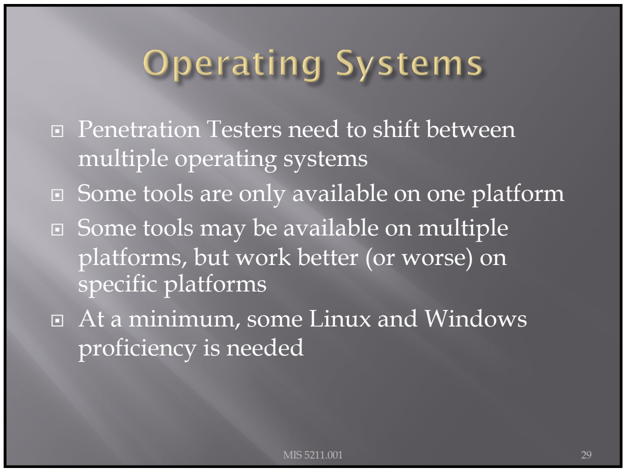
Infrastructure for Penetration Testing

- Software Tools
- Hardware
- Network Infrastructure

- We will cover some basics
  - Adjust to suite need
  - Dependent on type of targets and tests

MIS 5211.001 28

28

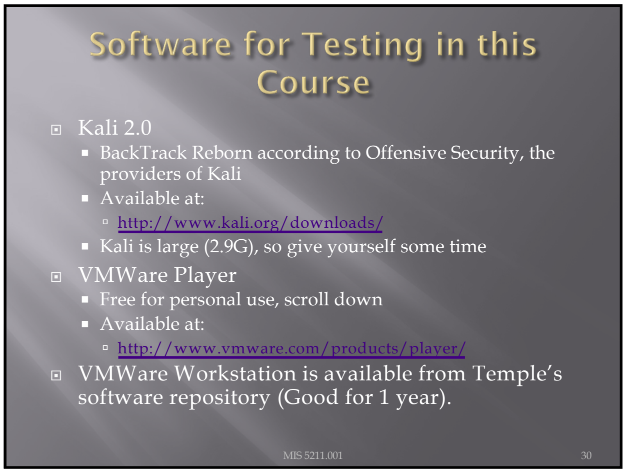


Operating Systems

- Penetration Testers need to shift between multiple operating systems
- Some tools are only available on one platform
- Some tools may be available on multiple platforms, but work better (or worse) on specific platforms
- At a minimum, some Linux and Windows proficiency is needed

MIS 5211.001 29

29

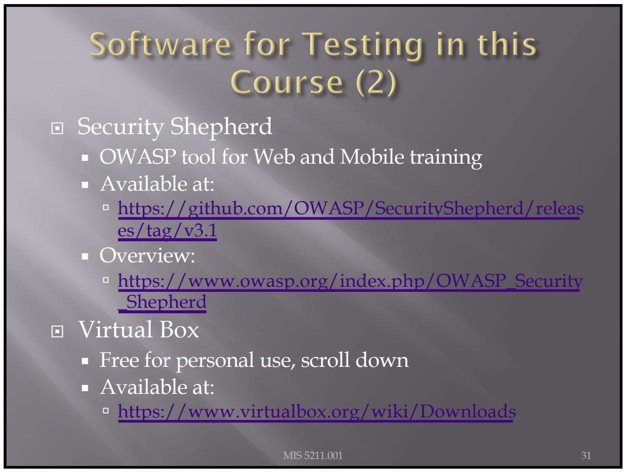


Software for Testing in this Course

- Kali 2.0
  - BackTrack Reborn according to Offensive Security, the providers of Kali
  - Available at:
    - http://www.kali.org/downloads/
  - Kali is large (2.9G), so give yourself some time
- VMWare Player
  - Free for personal use, scroll down
  - Available at:
    - http://www.vmware.com/products/player/
- VMWare Workstation is available from Temple's software repository (Good for 1 year).

MIS 5211.001 30

30

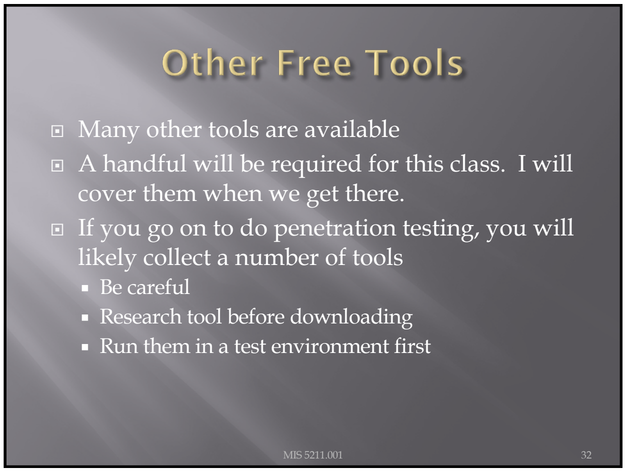


Software for Testing in this Course (2)

- Security Shepherd
  - OWASP tool for Web and Mobile training
  - Available at:
    - https://github.com/OWASP/SecurityShepherd/releases/tag/v3.1
  - Overview:
    - https://www.owasp.org/index.php/OWASP_Security_Shepherd
- Virtual Box
  - Free for personal use, scroll down
  - Available at:
    - https://www.virtualbox.org/wiki/Downloads

MIS 5211.001 31

31

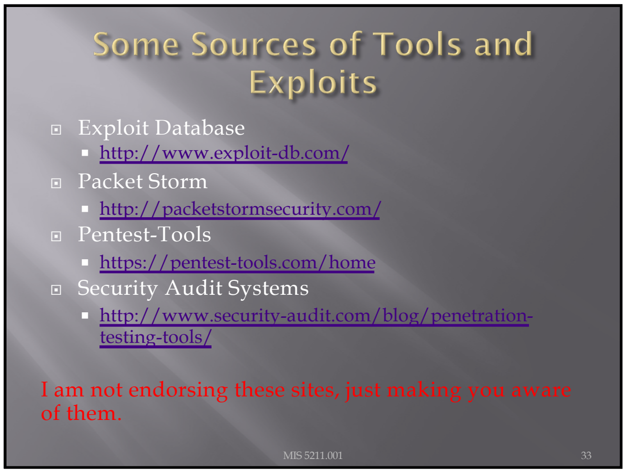


Other Free Tools

- Many other tools are available
- A handful will be required for this class. I will cover them when we get there.
- If you go on to do penetration testing, you will likely collect a number of tools
  - Be careful
  - Research tool before downloading
  - Run them in a test environment first

MIS 5211.001 32

32



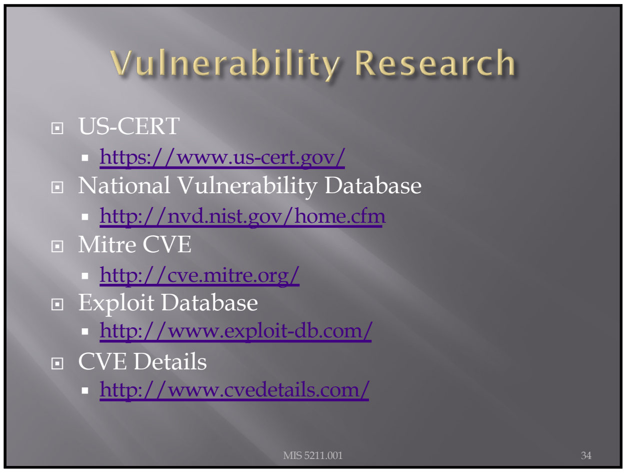
Some Sources of Tools and Exploits

- Exploit Database
  - http://www.exploit-db.com/
- Packet Storm
  - http://packetstormsecurity.com/
- Pentest-Tools
  - https://pentest-tools.com/home
- Security Audit Systems
  - http://www.security-audit.com/blog/penetration-testing-tools/

I am not endorsing these sites, just making you aware of them.

MIS 5211.001 33

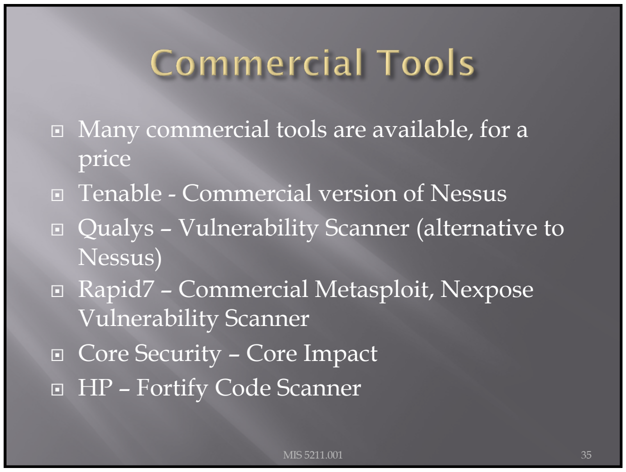
33



Vulnerability Research

- US-CERT
  - https://www.us-cert.gov/
- National Vulnerability Database
  - http://nvd.nist.gov/home.cfm
- Mitre CVE
  - http://cve.mitre.org/
- Exploit Database
  - http://www.exploit-db.com/
- CVE Details
  - http://www.cvedetails.com/

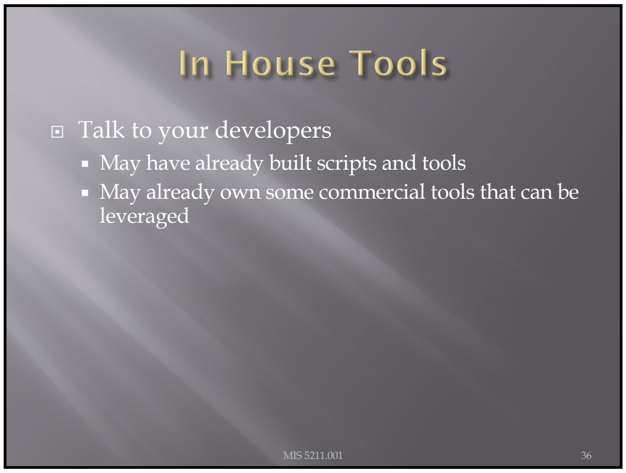
34



Commercial Tools

- Many commercial tools are available, for a price
- Tenable - Commercial version of Nessus
- Qualys – Vulnerability Scanner (alternative to Nessus)
- Rapid7 – Commercial Metasploit, Nexpose Vulnerability Scanner
- Core Security – Core Impact
- HP – Fortify Code Scanner

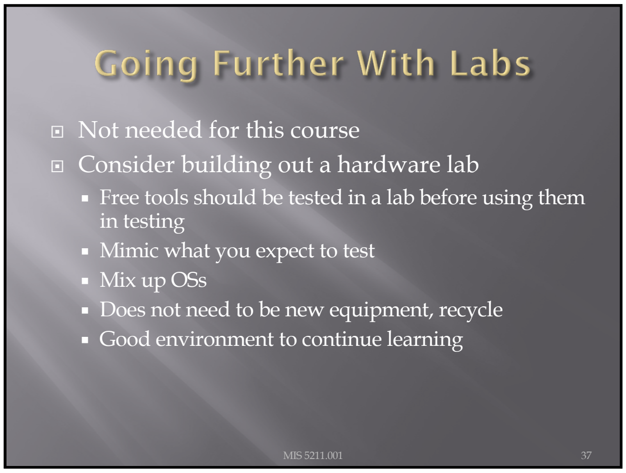
35



In House Tools

- Talk to your developers
  - May have already built scripts and tools
  - May already own some commercial tools that can be leveraged

36

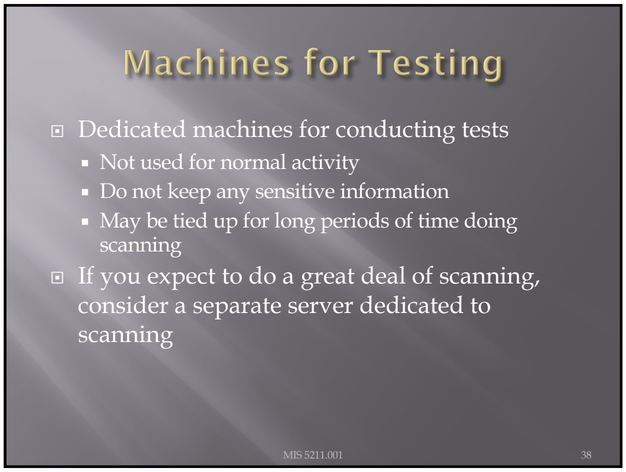


Going Further With Labs

- Not needed for this course
- Consider building out a hardware lab
  - Free tools should be tested in a lab before using them in testing
  - Mimic what you expect to test
  - Mix up OSs
  - Does not need to be new equipment, recycle
  - Good environment to continue learning

MIS 5211.001 37

37

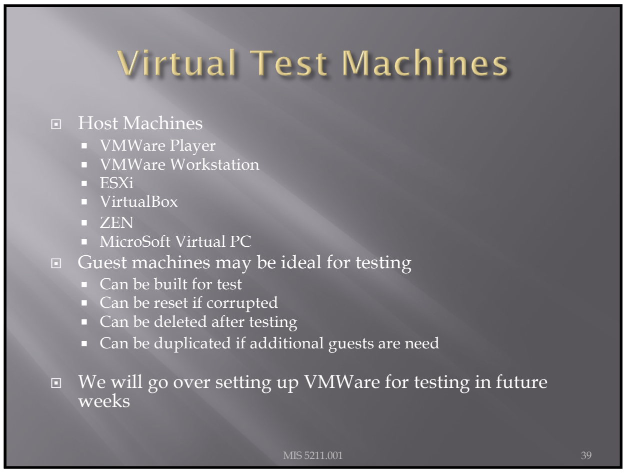


Machines for Testing

- Dedicated machines for conducting tests
  - Not used for normal activity
  - Do not keep any sensitive information
  - May be tied up for long periods of time doing scanning
- If you expect to do a great deal of scanning, consider a separate server dedicated to scanning

MIS 5211.001 38

38

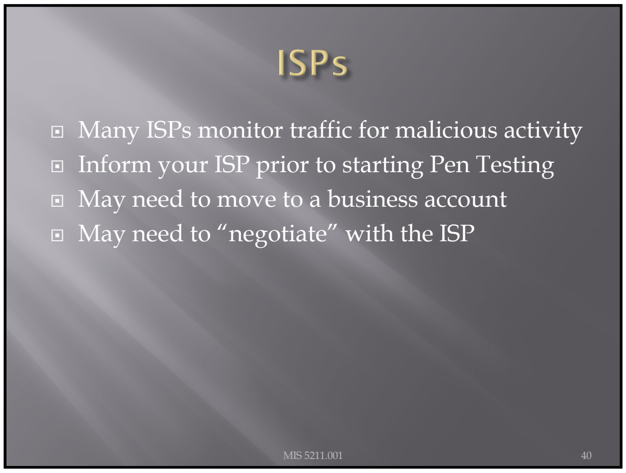


Virtual Test Machines

- Host Machines
  - VMWare Player
  - VMWare Workstation
  - ESXi
  - VirtualBox
  - ZEN
  - MicroSoft Virtual PC
- Guest machines may be ideal for testing
  - Can be built for test
  - Can be reset if corrupted
  - Can be deleted after testing
  - Can be duplicated if additional guests are need
- We will go over setting up VMWare for testing in future weeks

MIS 5211.001 39

39

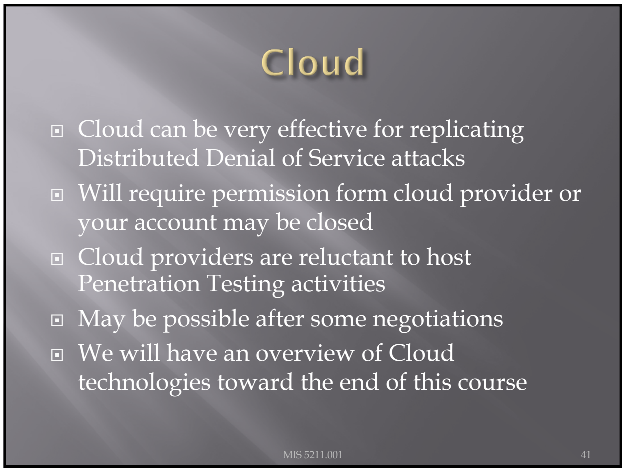


ISPs

- Many ISPs monitor traffic for malicious activity
- Inform your ISP prior to starting Pen Testing
- May need to move to a business account
- May need to "negotiate" with the ISP

MIS 5211.001 40

40

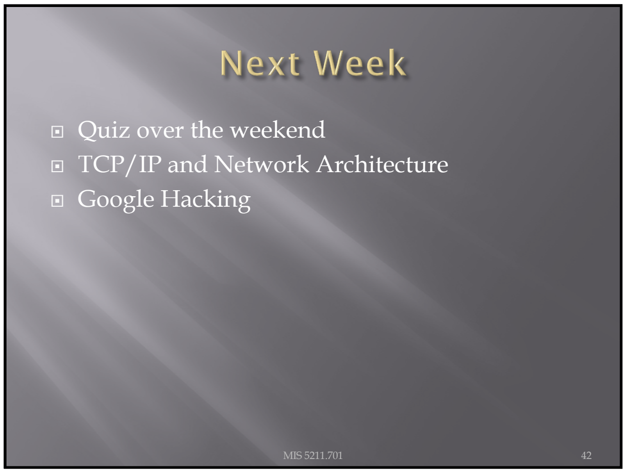


Cloud

- Cloud can be very effective for replicating Distributed Denial of Service attacks
- Will require permission form cloud provider or your account may be closed
- Cloud providers are reluctant to host Penetration Testing activities
- May be possible after some negotiations
- We will have an overview of Cloud technologies toward the end of this course

MIS 5211.001 41

41



Next Week

- Quiz over the weekend
- TCP/IP and Network Architecture
- Google Hacking

MIS 5211.701 42

42

Questions

?

MIS 5211.701

43

43