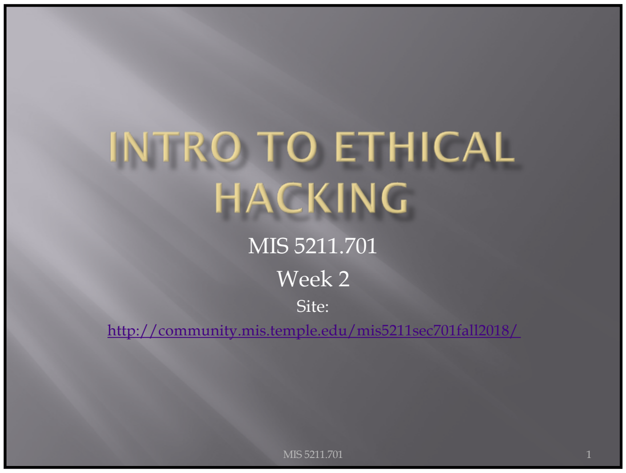


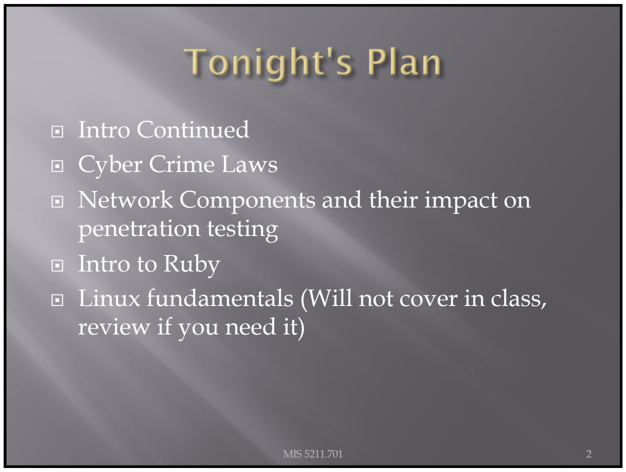
INTRO TO ETHICAL HACKING

MIS 5211.701

Week 2

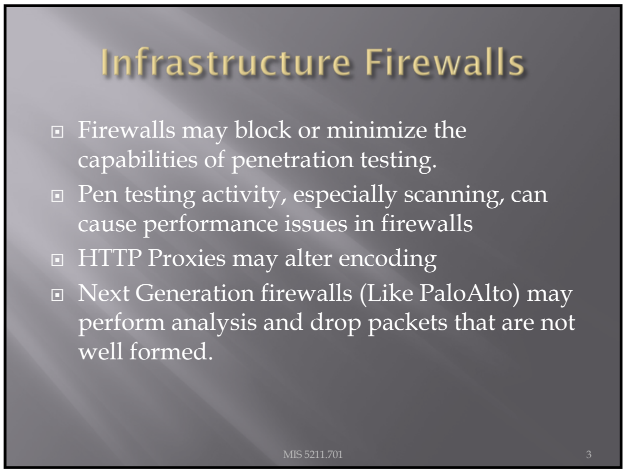
Site:

http://community.mis.temple.edu/mis5211sec701fall2018/



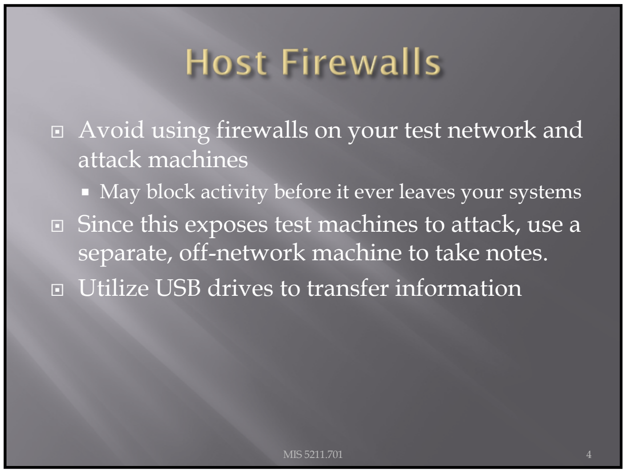
Tonight's Plan

- Intro Continued
- Cyber Crime Laws
- Network Components and their impact on penetration testing
- Intro to Ruby
- Linux fundamentals (Will not cover in class, review if you need it)



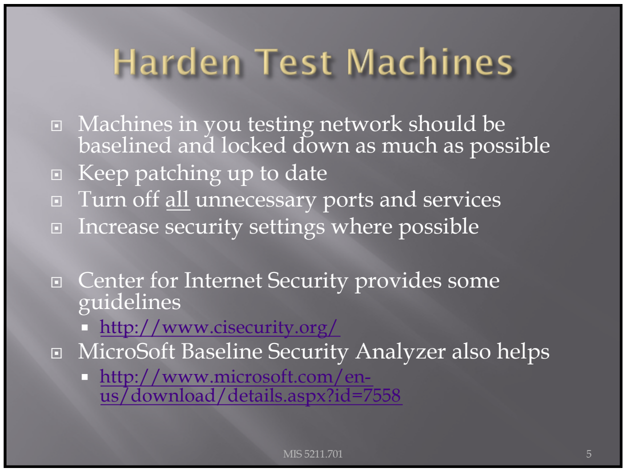
Infrastructure Firewalls

- Firewalls may block or minimize the capabilities of penetration testing.
- Pen testing activity, especially scanning, can cause performance issues in firewalls
- HTTP Proxies may alter encoding
- Next Generation firewalls (Like PaloAlto) may perform analysis and drop packets that are not well formed.



Host Firewalls

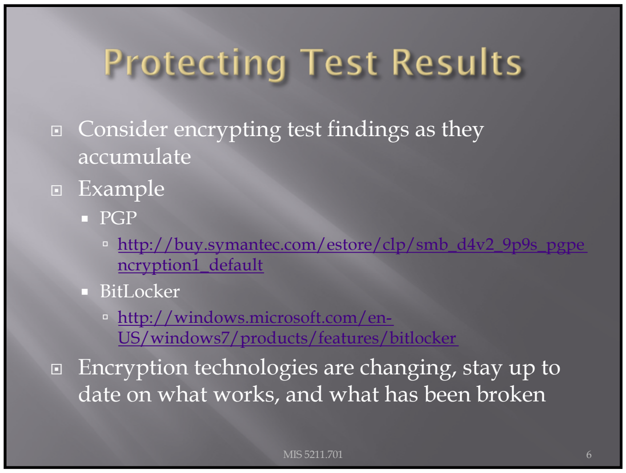
- Avoid using firewalls on your test network and attack machines
  - May block activity before it ever leaves your systems
- Since this exposes test machines to attack, use a separate, off-network machine to take notes.
- Utilize USB drives to transfer information



Harden Test Machines

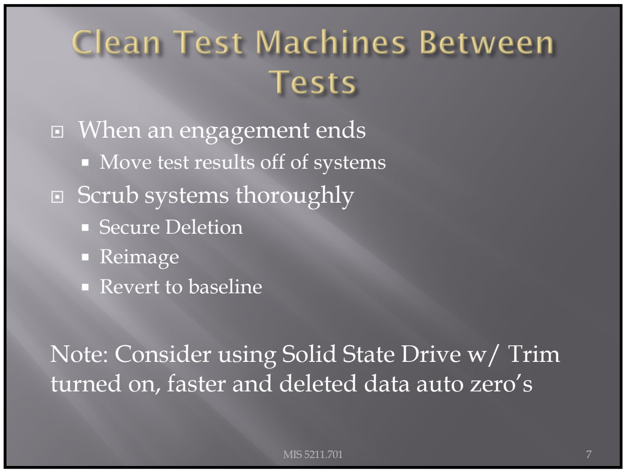
- Machines in you testing network should be baselined and locked down as much as possible
- Keep patching up to date
- Turn off all unnecessary ports and services
- Increase security settings where possible

- Center for Internet Security provides some guidelines
  - http://www.cisecurity.org/
- MicroSoft Baseline Security Analyzer also helps
  - http://www.microsoft.com/en-us/download/details.aspx?id=7558



Protecting Test Results

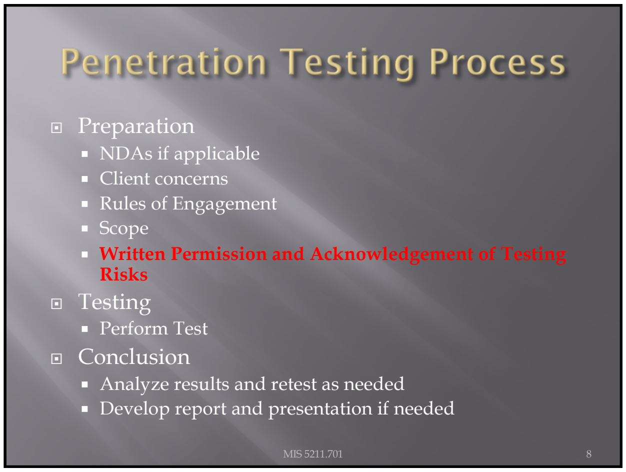
- Consider encrypting test findings as they accumulate
- Example
  - PGP
    - http://buy.symantec.com/estore/clp/smb_d4v2_9p9s_pgpencryption1_default
  - BitLocker
    - http://windows.microsoft.com/en-US/windows7/products/features/bitlocker
- Encryption technologies are changing, stay up to date on what works, and what has been broken



Clean Test Machines Between Tests

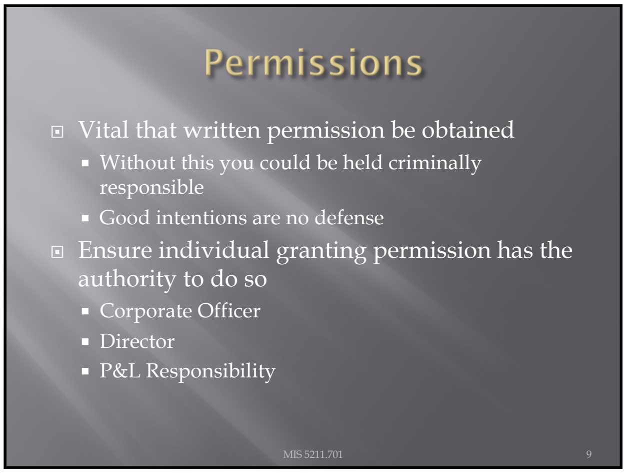
- When an engagement ends
  - Move test results off of systems
- Scrub systems thoroughly
  - Secure Deletion
  - Reimage
  - Revert to baseline

Note: Consider using Solid State Drive w/ Trim turned on, faster and deleted data auto zero's



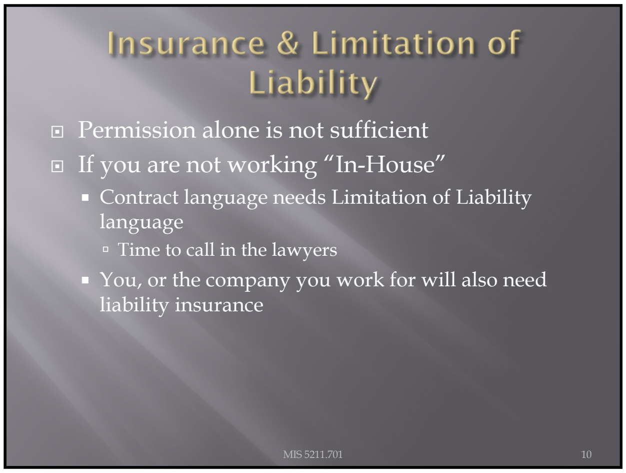
Penetration Testing Process

- Preparation
  - NDAs if applicable
  - Client concerns
  - Rules of Engagement
  - Scope
  - **Written Permission and Acknowledgement of Testing Risks**
- Testing
  - Perform Test
- Conclusion
  - Analyze results and retest as needed
  - Develop report and presentation if needed



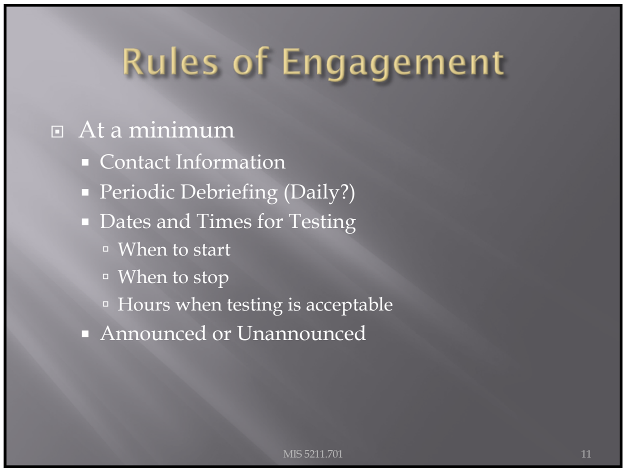
Permissions

- Vital that written permission be obtained
  - Without this you could be held criminally responsible
  - Good intentions are no defense
- Ensure individual granting permission has the authority to do so
  - Corporate Officer
  - Director
  - P&L Responsibility



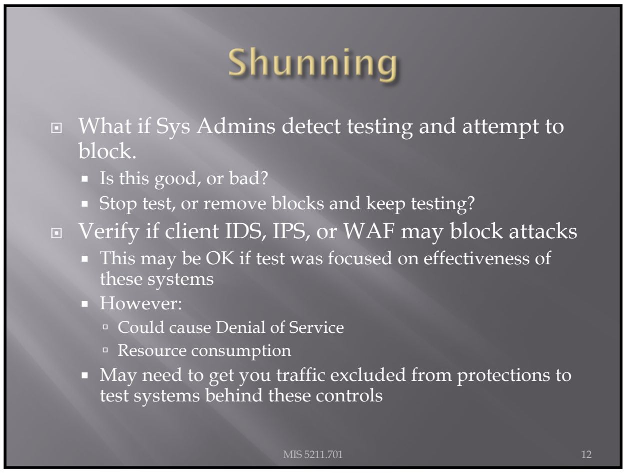
Insurance & Limitation of Liability

- Permission alone is not sufficient
- If you are not working "In-House"
  - Contract language needs Limitation of Liability language
    - Time to call in the lawyers
  - You, or the company you work for will also need liability insurance



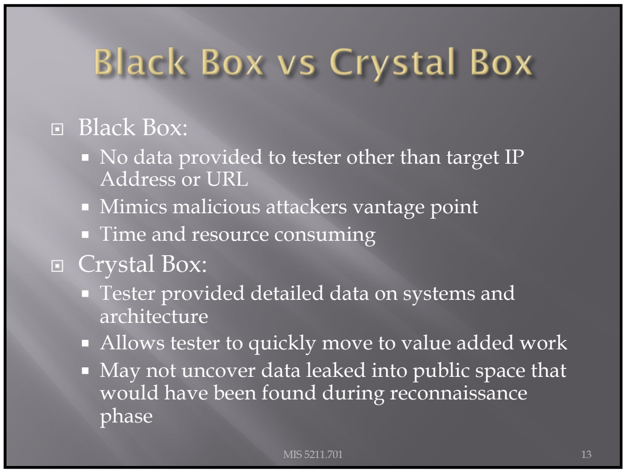
Rules of Engagement

- At a minimum
  - Contact Information
  - Periodic Debriefing (Daily?)
  - Dates and Times for Testing
    - When to start
    - When to stop
    - Hours when testing is acceptable
  - Announced or Unannounced



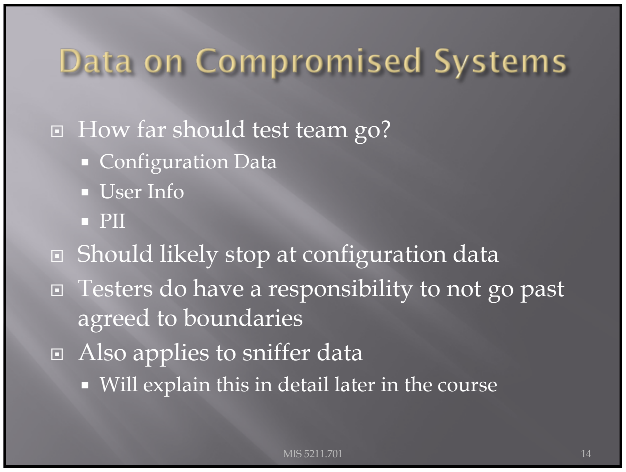
Shunning

- What if Sys Admins detect testing and attempt to block.
  - Is this good, or bad?
  - Stop test, or remove blocks and keep testing?
- Verify if client IDS, IPS, or WAF may block attacks
  - This may be OK if test was focused on effectiveness of these systems
  - However:
    - Could cause Denial of Service
    - Resource consumption
  - May need to get you traffic excluded from protections to test systems behind these controls



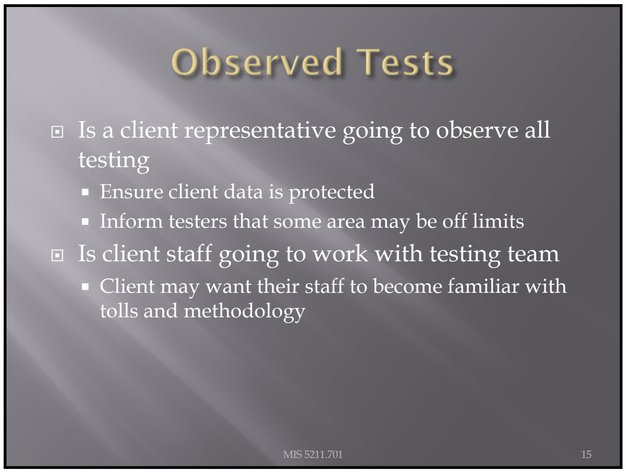
Black Box vs Crystal Box

- Black Box:
  - No data provided to tester other than target IP Address or URL
  - Mimics malicious attackers vantage point
  - Time and resource consuming
- Crystal Box:
  - Tester provided detailed data on systems and architecture
  - Allows tester to quickly move to value added work
  - May not uncover data leaked into public space that would have been found during reconnaissance phase



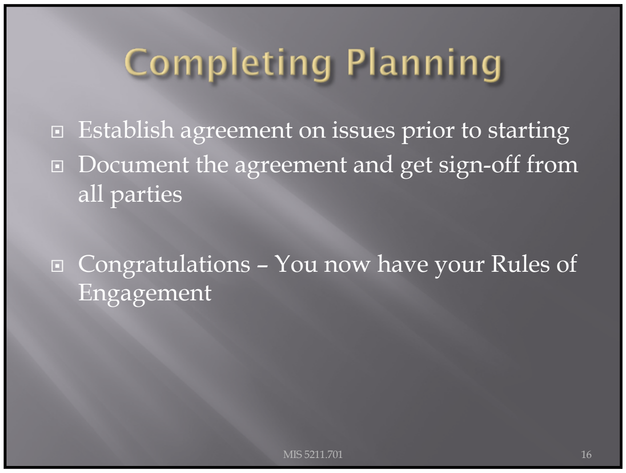
Data on Compromised Systems

- How far should test team go?
  - Configuration Data
  - User Info
  - PII
- Should likely stop at configuration data
- Testers do have a responsibility to not go past agreed to boundaries
- Also applies to sniffer data
  - Will explain this in detail later in the course



Observed Tests

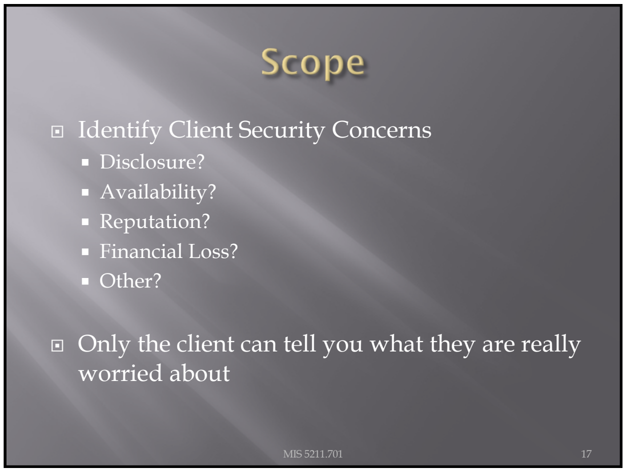
- Is a client representative going to observe all testing
  - Ensure client data is protected
  - Inform testers that some area may be off limits
- Is client staff going to work with testing team
  - Client may want their staff to become familiar with tolls and methodology



Completing Planning

- Establish agreement on issues prior to starting
- Document the agreement and get sign-off from all parties

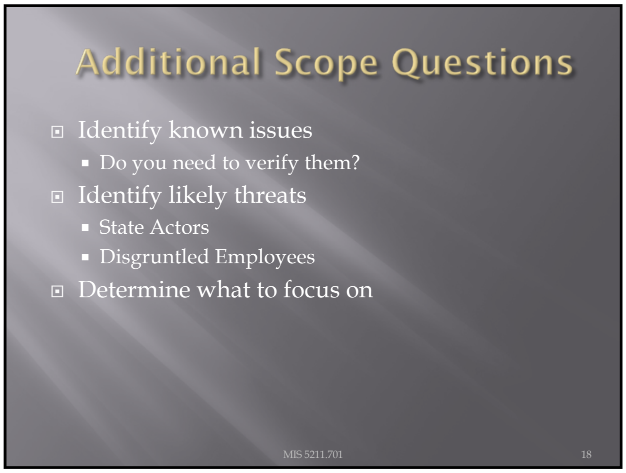
- Congratulations – You now have your Rules of Engagement



Scope

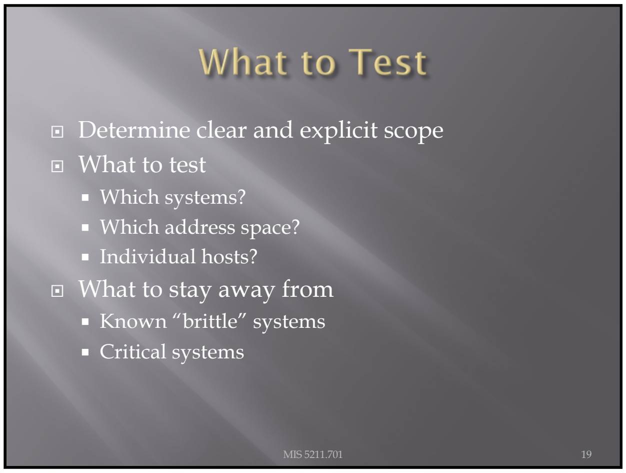
- Identify Client Security Concerns
  - Disclosure?
  - Availability?
  - Reputation?
  - Financial Loss?
  - Other?

- Only the client can tell you what they are really worried about



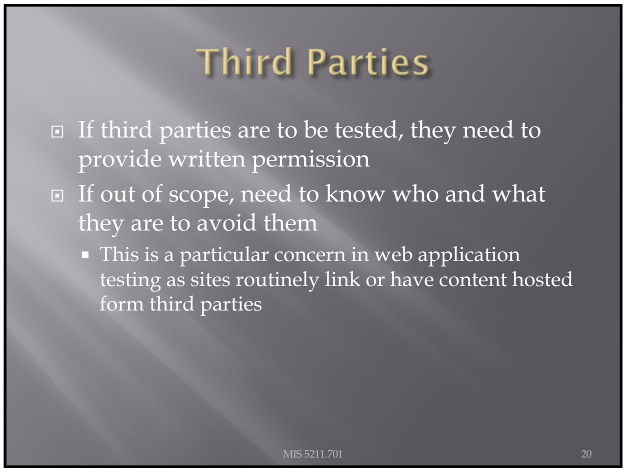
Additional Scope Questions

- Identify known issues
  - Do you need to verify them?
- Identify likely threats
  - State Actors
  - Disgruntled Employees
- Determine what to focus on



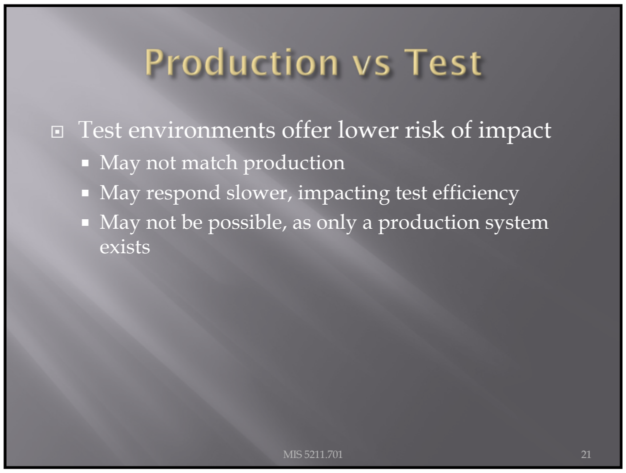
What to Test

- Determine clear and explicit scope
- What to test
  - Which systems?
  - Which address space?
  - Individual hosts?
- What to stay away from
  - Known “brittle” systems
  - Critical systems



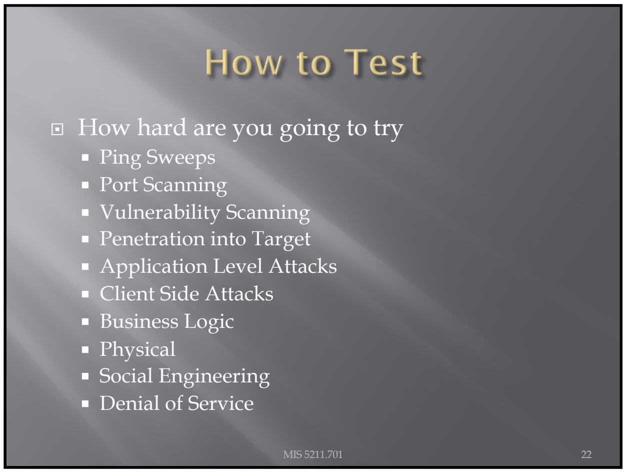
Third Parties

- If third parties are to be tested, they need to provide written permission
- If out of scope, need to know who and what they are to avoid them
  - This is a particular concern in web application testing as sites routinely link or have content hosted form third parties



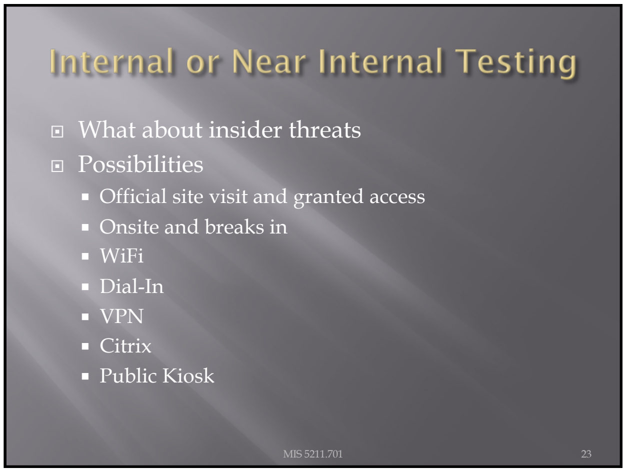
Production vs Test

- Test environments offer lower risk of impact
  - May not match production
  - May respond slower, impacting test efficiency
  - May not be possible, as only a production system exists



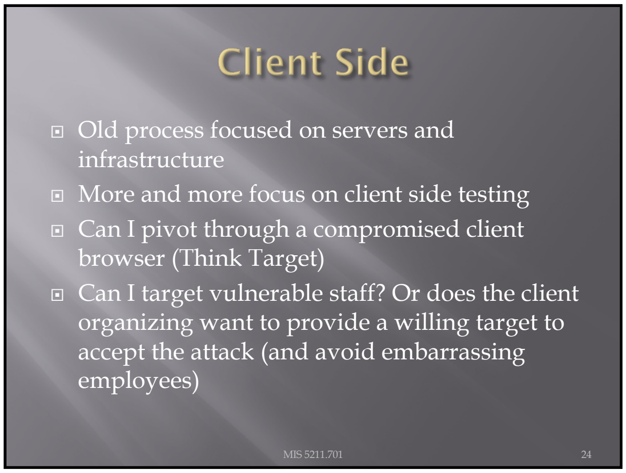
How to Test

- How hard are you going to try
  - Ping Sweeps
  - Port Scanning
  - Vulnerability Scanning
  - Penetration into Target
  - Application Level Attacks
  - Client Side Attacks
  - Business Logic
  - Physical
  - Social Engineering
  - Denial of Service



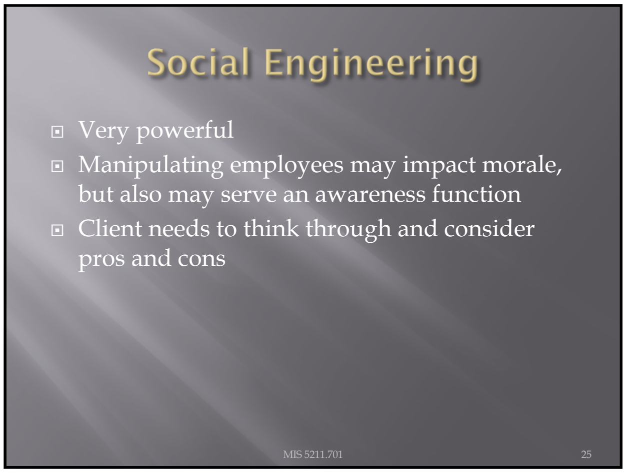
Internal or Near Internal Testing

- What about insider threats
- Possibilities
  - Official site visit and granted access
  - Onsite and breaks in
  - WiFi
  - Dial-In
  - VPN
  - Citrix
  - Public Kiosk



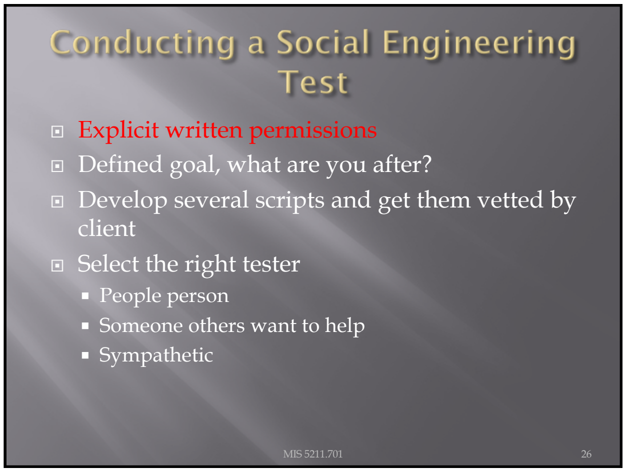
Client Side

- Old process focused on servers and infrastructure
- More and more focus on client side testing
- Can I pivot through a compromised client browser (Think Target)
- Can I target vulnerable staff? Or does the client organizing want to provide a willing target to accept the attack (and avoid embarrassing employees)



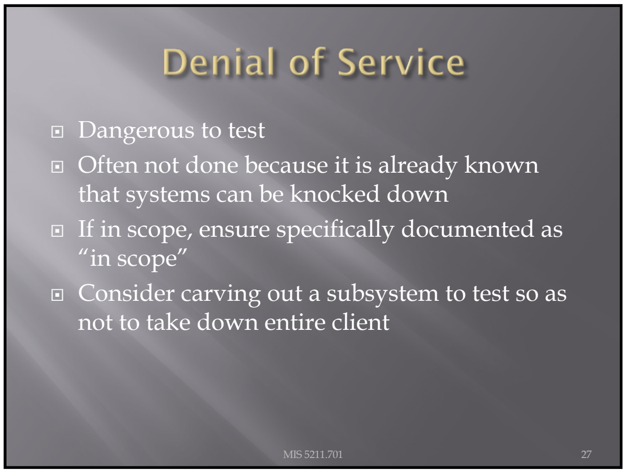
Social Engineering

- Very powerful
- Manipulating employees may impact morale, but also may serve an awareness function
- Client needs to think through and consider pros and cons



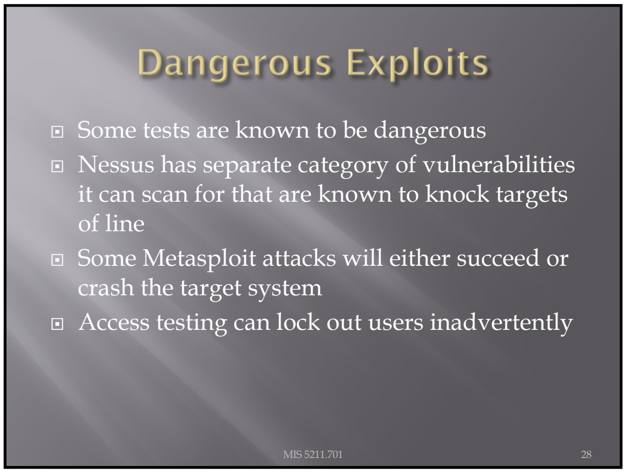
Conducting a Social Engineering Test

- Explicit written permissions
- Defined goal, what are you after?
- Develop several scripts and get them vetted by client
- Select the right tester
  - People person
  - Someone others want to help
  - Sympathetic



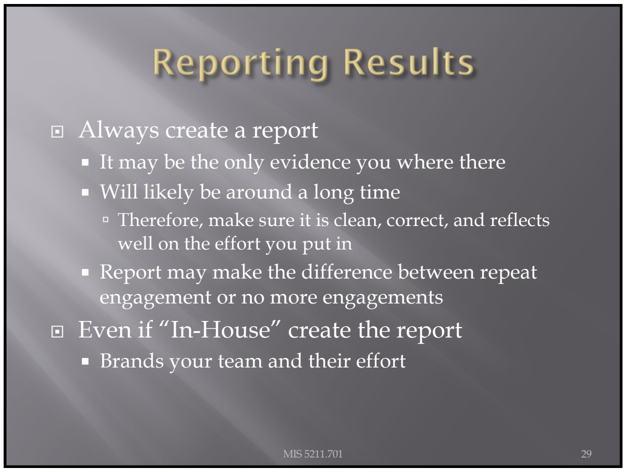
Denial of Service

- Dangerous to test
- Often not done because it is already known that systems can be knocked down
- If in scope, ensure specifically documented as “in scope”
- Consider carving out a subsystem to test so as not to take down entire client



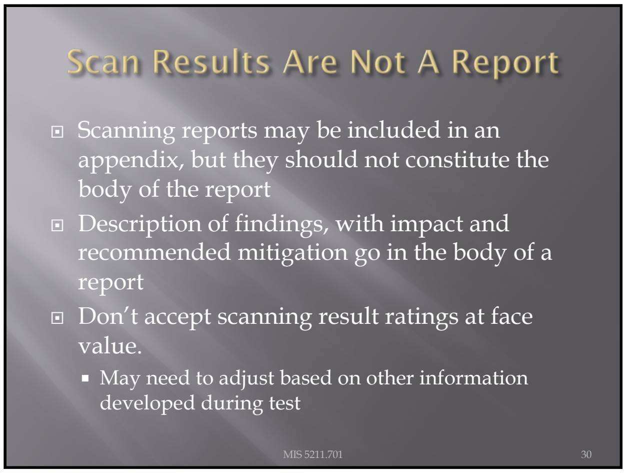
Dangerous Exploits

- Some tests are known to be dangerous
- Nessus has separate category of vulnerabilities it can scan for that are known to knock targets of line
- Some Metasploit attacks will either succeed or crash the target system
- Access testing can lock out users inadvertently



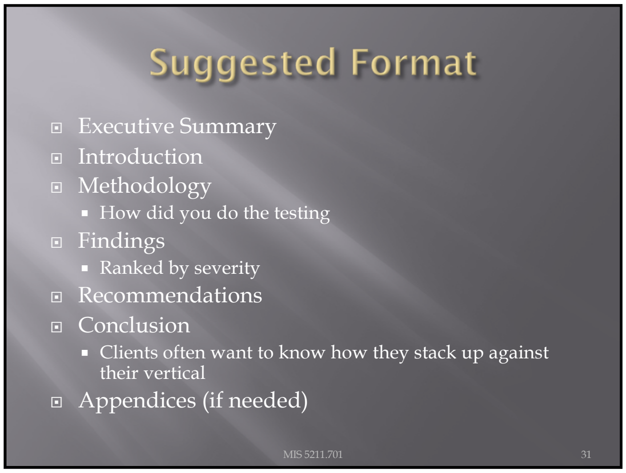
Reporting Results

- Always create a report
  - It may be the only evidence you where there
  - Will likely be around a long time
    - Therefore, make sure it is clean, correct, and reflects well on the effort you put in
  - Report may make the difference between repeat engagement or no more engagements
- Even if "In-House" create the report
  - Brands your team and their effort



Scan Results Are Not A Report

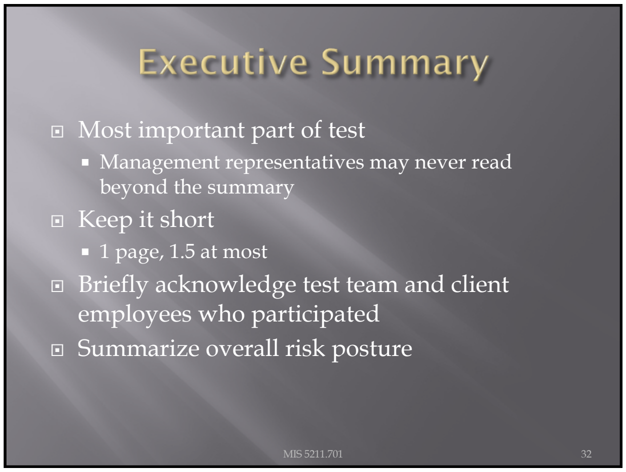
- Scanning reports may be included in an appendix, but they should not constitute the body of the report
- Description of findings, with impact and recommended mitigation go in the body of a report
- Don't accept scanning result ratings at face value.
  - May need to adjust based on other information developed during test



Suggested Format

- Executive Summary
- Introduction
- Methodology
  - How did you do the testing
- Findings
  - Ranked by severity
- Recommendations
- Conclusion
  - Clients often want to know how they stack up against their vertical
- Appendices (if needed)

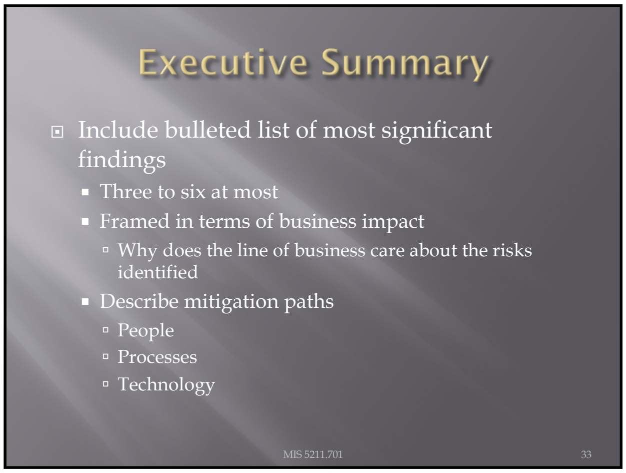
MIS 5211.701 31



Executive Summary

- Most important part of test
  - Management representatives may never read beyond the summary
- Keep it short
  - 1 page, 1.5 at most
- Briefly acknowledge test team and client employees who participated
- Summarize overall risk posture

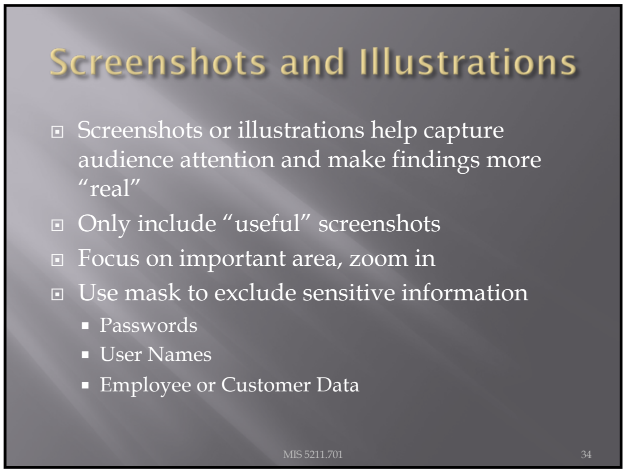
MIS 5211.701 32



Executive Summary

- Include bulleted list of most significant findings
  - Three to six at most
  - Framed in terms of business impact
    - Why does the line of business care about the risks identified
  - Describe mitigation paths
    - People
    - Processes
    - Technology

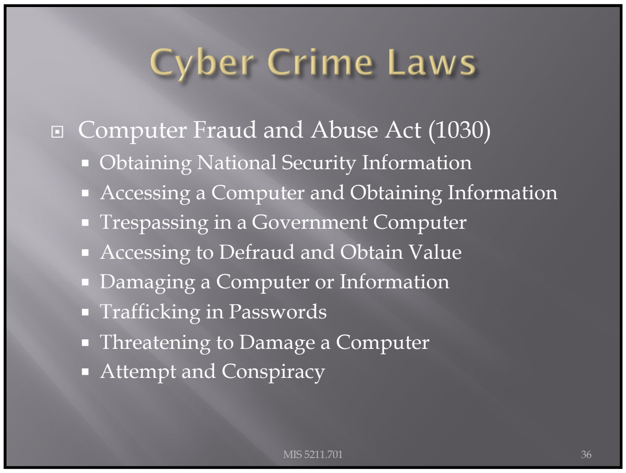
MIS 5211.701 33



Screenshots and Illustrations

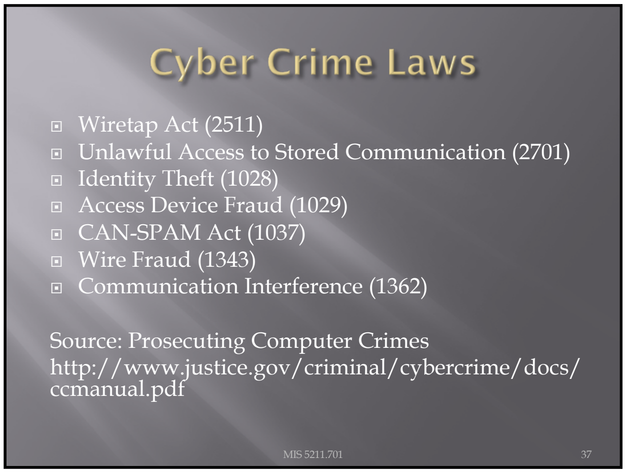
- Screenshots or illustrations help capture audience attention and make findings more "real"
- Only include "useful" screenshots
- Focus on important area, zoom in
- Use mask to exclude sensitive information
  - Passwords
  - User Names
  - Employee or Customer Data

Legal



Cyber Crime Laws

- Computer Fraud and Abuse Act (1030)
  - Obtaining National Security Information
  - Accessing a Computer and Obtaining Information
  - Trespassing in a Government Computer
  - Accessing to Defraud and Obtain Value
  - Damaging a Computer or Information
  - Trafficking in Passwords
  - Threatening to Damage a Computer
  - Attempt and Conspiracy

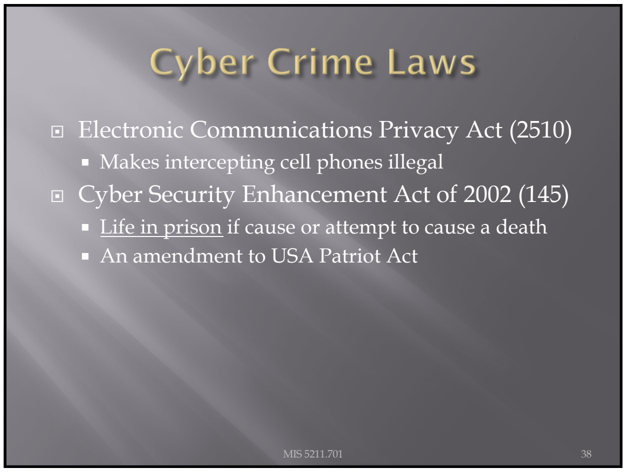


Cyber Crime Laws

- Wiretap Act (2511)
- Unlawful Access to Stored Communication (2701)
- Identity Theft (1028)
- Access Device Fraud (1029)
- CAN-SPAM Act (1037)
- Wire Fraud (1343)
- Communication Interference (1362)

Source: Prosecuting Computer Crimes
http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

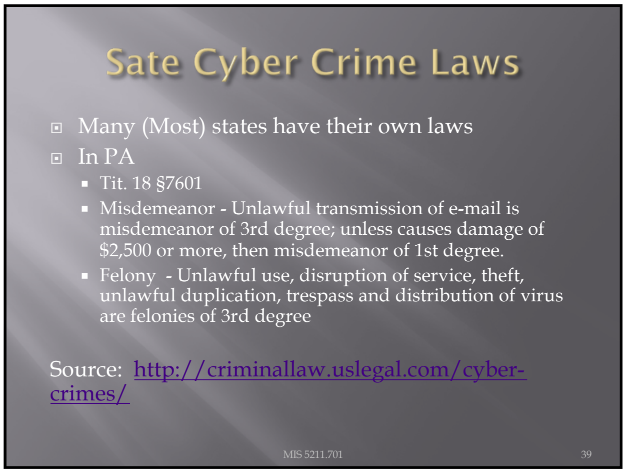
MIS 5211.701 37



Cyber Crime Laws

- Electronic Communications Privacy Act (2510)
  - Makes intercepting cell phones illegal
- Cyber Security Enhancement Act of 2002 (145)
  - Life in prison if cause or attempt to cause a death
  - An amendment to USA Patriot Act

MIS 5211.701 38

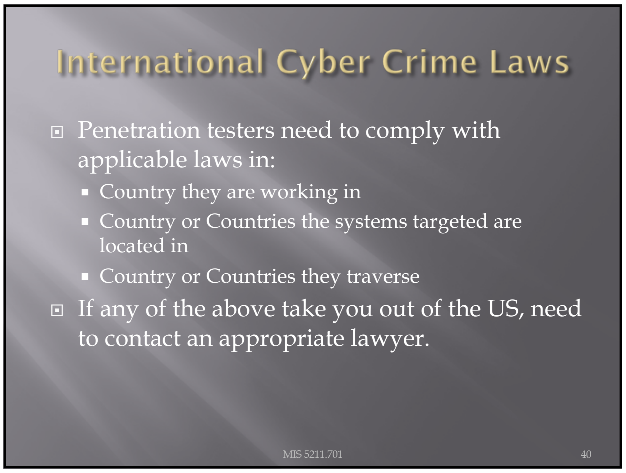


Sate Cyber Crime Laws

- Many (Most) states have their own laws
- In PA
  - Tit. 18 §7601
  - Misdemeanor - Unlawful transmission of e-mail is misdemeanor of 3rd degree; unless causes damage of $2,500 or more, then misdemeanor of 1st degree.
  - Felony - Unlawful use, disruption of service, theft, unlawful duplication, trespass and distribution of virus are felonies of 3rd degree

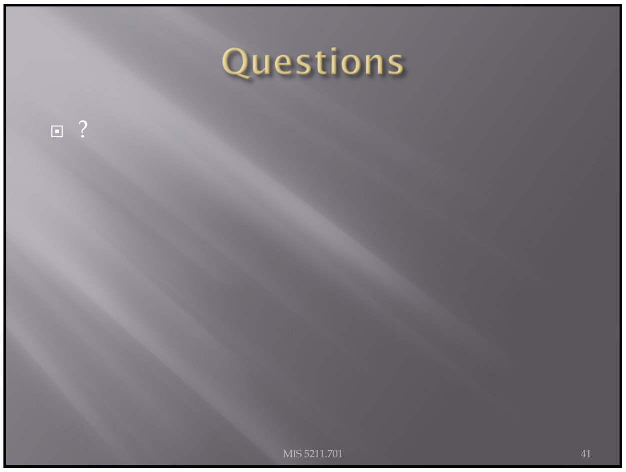
Source: http://criminallaw.uslegal.com/cyber-crimes/

MIS 5211.701 39



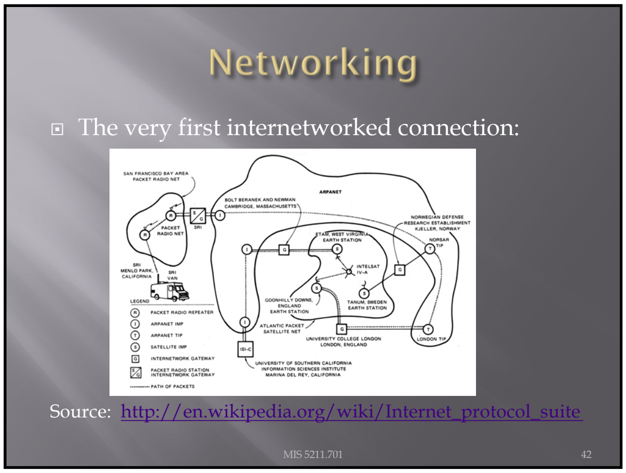
International Cyber Crime Laws

- Penetration testers need to comply with applicable laws in:
  - Country they are working in
  - Country or Countries the systems targeted are located in
  - Country or Countries they traverse
- If any of the above take you out of the US, need to contact an appropriate lawyer.



Questions

- ?



Networking

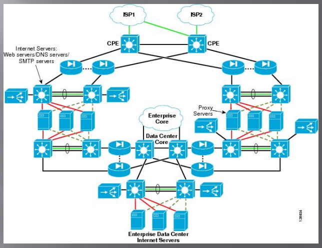
- The very first internetworked connection:

SAN FRANCISCO BAY AREA PACKET RADIO NET
ARPANET
BOLT BERANEK AND NEWMAN CAMBRIDGE, MASSACHUSETTS
R
R
PACKET RADIO NET
S G
SRI
I
NORWEGIAN DEFENSE RESEARCH ESTABLISHMENT KJELLER, NORWAY
ETAM, WEST VIRGINIA EARTH STATION
NORSAR TIP
I
G
S
T
INTELSAT IV-A
G
SRI MENLO PARK, CALIFORNIA
SRI VAN
S
S
GOONHILLY DOWNS, ENGLAND EARTH STATION
TANUM, SWEDEN EARTH STATION
I
ATLANTIC PACKET SATELLITE NET
G
T
UNIVERSITY COLLEGE LONDON LONDON, ENGLAND
LONDON TIP
ISI-C
UNIVERSITY OF SOUTHERN CALIFORNIA INFORMATION SCIENCES INSTITUTE MARINA DEL REY, CALIFORNIA
LEGEND
R PACKET RADIO REPEATER
I ARPANET IMP
T ARPANET TIP
S SATELLITE IMP
G INTERNETWORK GATEWAY
S G PACKET RADIO STATION INTERNETWORK GATEWAY
PATH OF PACKETS

Source: http://en.wikipedia.org/wiki/Internet_protocol_suite

Networking

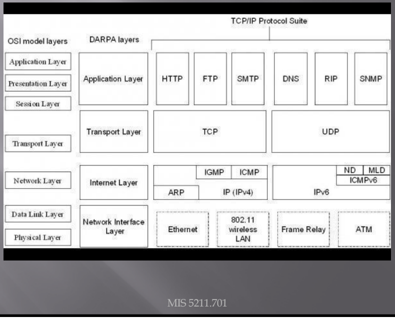
- Today



Source:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/2_Topolo.html

Internet Protocol Suite

- How Data fits together:



OSI model layers	DARPA layers	TCP/IP Protocol Suite
Application Layer Presentation Layer Session Layer	Application Layer	HTTP FTP SMTP DNS RIP SNMP
Transport Layer	Transport Layer	TCP UDP
Network Layer	Internet Layer	IGMP ICMP ARP IP (IPv4) ND MLD ICMPv6 IPv6
Data Link Layer Physical Layer	Network Interface Layer	Ethernet 802.11 wireless LAN Frame Relay ATM

A word about Ports

- Ports – logical assignment to packets of data
- Used to distinguish between different services that run over transport protocols such as TCP and UDP
- IANA Registry:

http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1

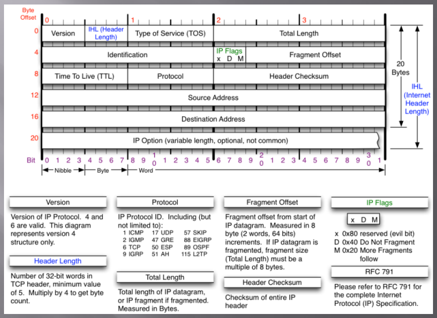
Protocols

- What we will cover
  - IP
  - ICMP
  - UDP
  - TCP
  - ARP

IP Protocol

- Internet Protocol
  - Primary protocol of the Internet Layer of the Internet protocol
  - Three main functions
    - For outgoing packets – Select the next hop host (Gateway)
    - For incoming packets – Capture the packet and pass up the protocol stack as appropriate
    - Error detection

IP Protocol



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

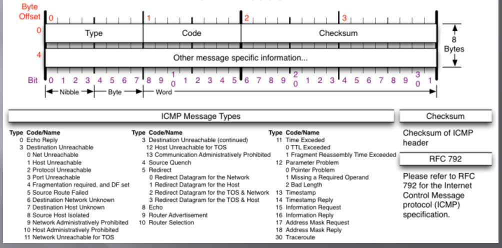
Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Source: http://nmap.org/book/tcpip-ref.html

ICMP Protocol

- Internet Control Message Protocol
  - Used by network devices to communicate status
  - Not "typically" used to exchange data
  - Does not have a "port" assignment
  - Not usually accessed by end-users accept for:
    - ping
    - traceroute

ICMP Protocol



ICMP Message Types

Type Code/Name
0 Echo Reply
3 Destination Unreachable
0 Net Unreachable
1 Host Unreachable
2 Protocol Unreachable
3 Port Unreachable
4 Fragmentation required, and DF set
5 Source Route Failed
6 Destination Network Unknown
7 Destination Host Unknown
8 Source Host Isolated
9 Network Administratively Prohibited
10 Host Administratively Prohibited
11 Network Unreachable for TOS

Type Code/Name
3 Destination Unreachable (continued)
12 Host Unreachable for TOS
13 Communication Administratively Prohibited
4 Source Quench
5 Redirect
0 Redirect Datagram for the Network
1 Redirect Datagram for the Host
2 Redirect Datagram for the TOS & Network
3 Redirect Datagram for the TOS & Host
8 Echo
9 Router Advertisement
10 Router Selection

Type Code/Name
11 Time Exceded
0 TTL Exceeded
1 Fragment Reassembly Time Exceeded
12 Parameter Problem
0 Pointer Problem
1 Missing a Required Operand
2 Bad Length
13 Timestamp
14 Timestamp Reply
15 Information Request
16 Information Reply
17 Address Mask Request
18 Address Mask Reply
30 Traceroute

Checksum

Checksum of ICMP header

RFC 792

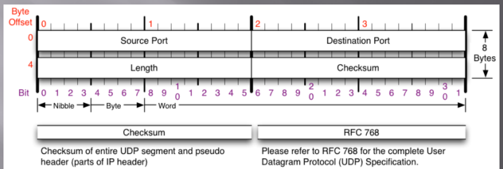
Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Source: http://nmap.org/book/tcpip-ref.html

UDP Protocol

- User Datagram Protocol
  - Simple transmission model with limited mechanisms
  - No guarantee of delivery
  - No acknowledgement of receipt
  - Does include checksum and port numbers

UDP Protocol



Checksum

Checksum of entire UDP segment and pseudo header (parts of IP header)

RFC 768

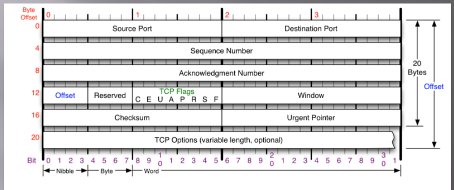
Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.

Source: http://nmap.org/book/tcpip-ref.html

TCP Protocol

- Transmission Control Protocol
  - Sometimes called TCP/IP
  - Provides **reliable**, **ordered** and **error checked** delivery of a stream of data (or Octets) across local area networks, intranets, and public internet
- This is the protocol used for HTTP, HTTPS, SMTP, POP3, IMAP, SSH, FTP, Telnet, and others

TCP Protocol



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

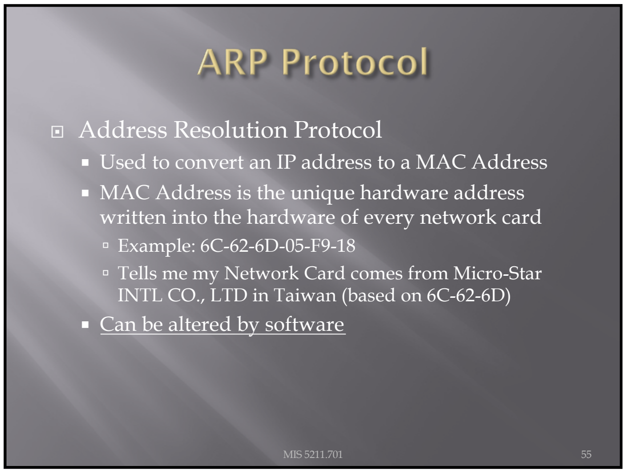
Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

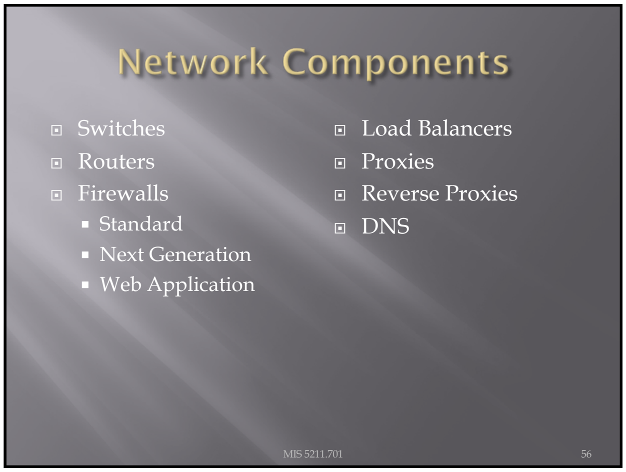
Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Source: http://nmap.org/book/tcpip-ref.html



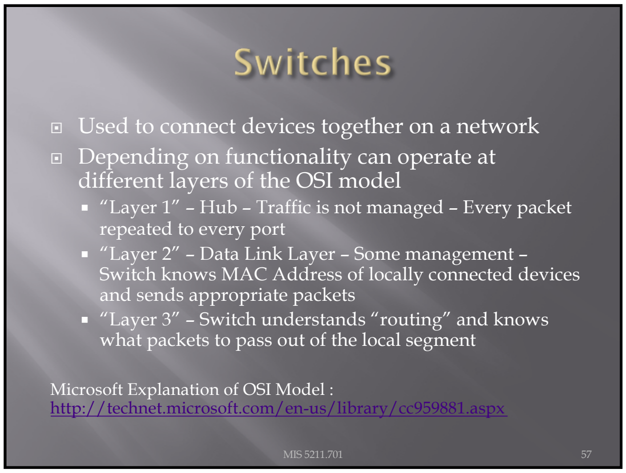
ARP Protocol

- Address Resolution Protocol
  - Used to convert an IP address to a MAC Address
  - MAC Address is the unique hardware address written into the hardware of every network card
    - Example: 6C-62-6D-05-F9-18
    - Tells me my Network Card comes from Micro-Star INTL CO., LTD in Taiwan (based on 6C-62-6D)
  - Can be altered by software



Network Components

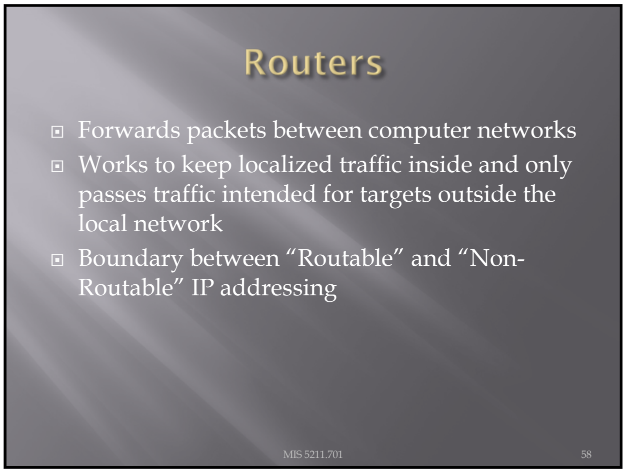
- Switches
- Routers
- Firewalls
  - Standard
  - Next Generation
  - Web Application
- Load Balancers
- Proxies
- Reverse Proxies
- DNS



Switches

- Used to connect devices together on a network
- Depending on functionality can operate at different layers of the OSI model
  - "Layer 1" – Hub – Traffic is not managed – Every packet repeated to every port
  - "Layer 2" – Data Link Layer – Some management – Switch knows MAC Address of locally connected devices and sends appropriate packets
  - "Layer 3" – Switch understands "routing" and knows what packets to pass out of the local segment

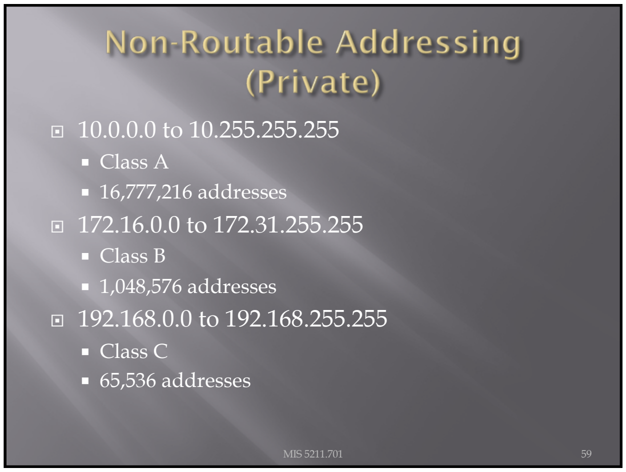
Microsoft Explanation of OSI Model : http://technet.microsoft.com/en-us/library/cc959881.aspx



Routers

- Forwards packets between computer networks
- Works to keep localized traffic inside and only passes traffic intended for targets outside the local network
- Boundary between "Routable" and "Non-Routable" IP addressing

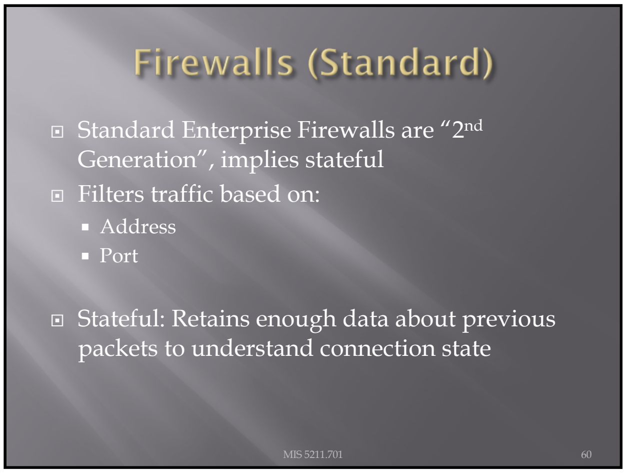
MIS 5211.701 58



Non-Routable Addressing (Private)

- 10.0.0.0 to 10.255.255.255
  - Class A
  - 16,777,216 addresses
- 172.16.0.0 to 172.31.255.255
  - Class B
  - 1,048,576 addresses
- 192.168.0.0 to 192.168.255.255
  - Class C
  - 65,536 addresses

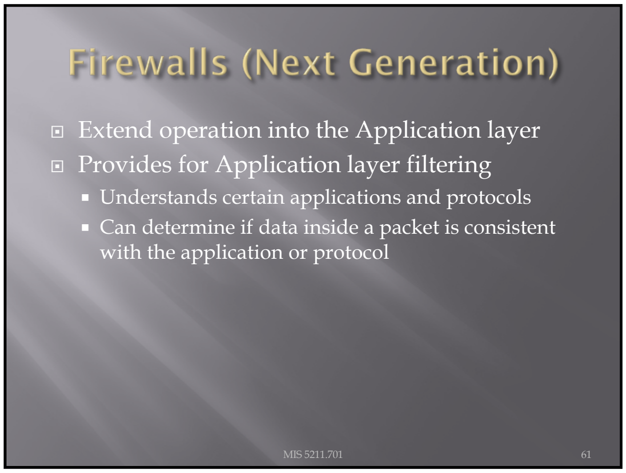
MIS 5211.701 59



Firewalls (Standard)

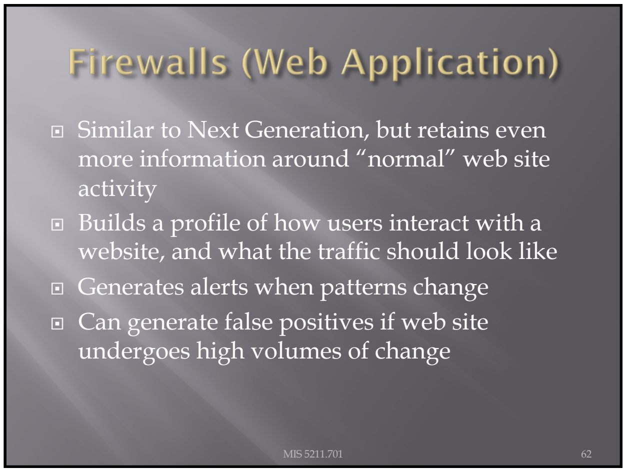
- Standard Enterprise Firewalls are "2nd Generation", implies stateful
- Filters traffic based on:
  - Address
  - Port
- Stateful: Retains enough data about previous packets to understand connection state

MIS 5211.701 60



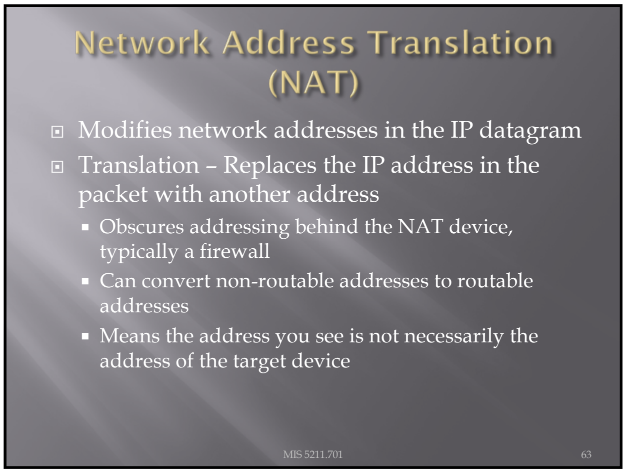
Firewalls (Next Generation)

- Extend operation into the Application layer
- Provides for Application layer filtering
  - Understands certain applications and protocols
  - Can determine if data inside a packet is consistent with the application or protocol



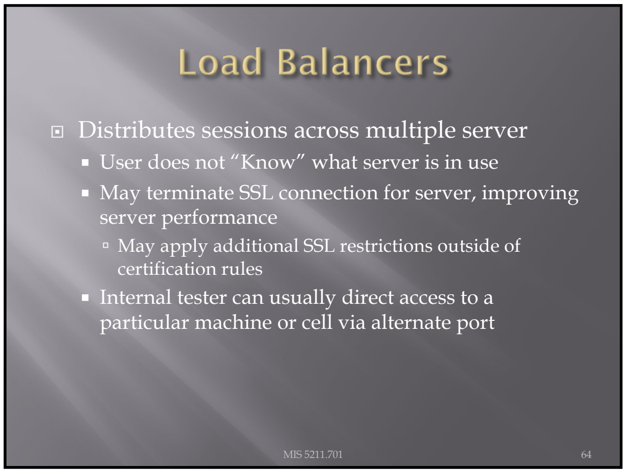
Firewalls (Web Application)

- Similar to Next Generation, but retains even more information around “normal” web site activity
- Builds a profile of how users interact with a website, and what the traffic should look like
- Generates alerts when patterns change
- Can generate false positives if web site undergoes high volumes of change



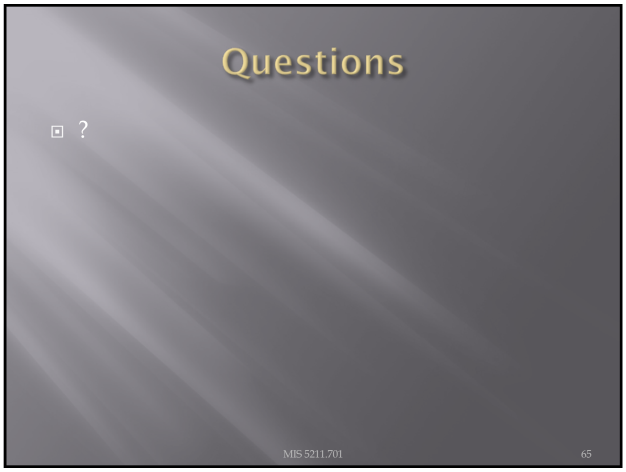
Network Address Translation (NAT)

- Modifies network addresses in the IP datagram
- Translation – Replaces the IP address in the packet with another address
  - Obscures addressing behind the NAT device, typically a firewall
  - Can convert non-routable addresses to routable addresses
  - Means the address you see is not necessarily the address of the target device



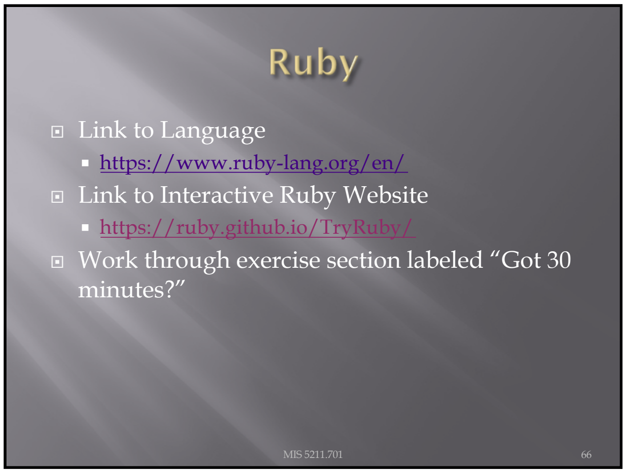
Load Balancers

- Distributes sessions across multiple server
  - User does not "Know" what server is in use
  - May terminate SSL connection for server, improving server performance
    - May apply additional SSL restrictions outside of certification rules
  - Internal tester can usually direct access to a particular machine or cell via alternate port



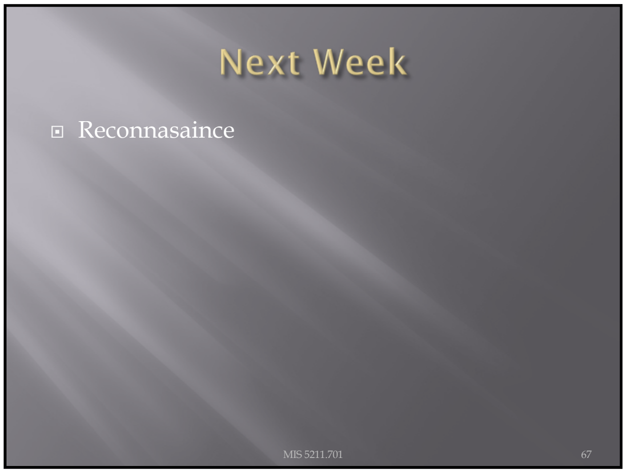
Questions

- ?



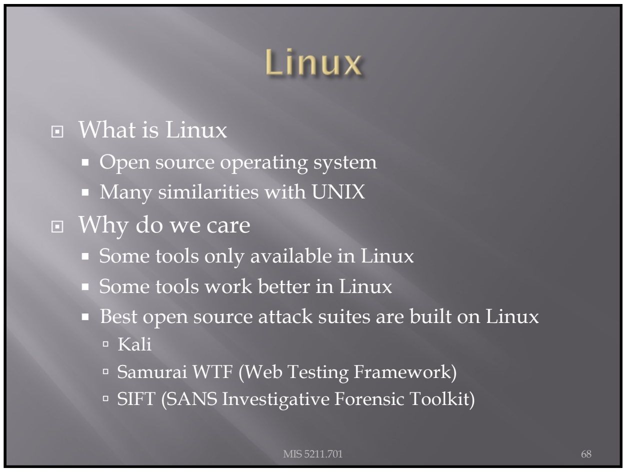
Ruby

- Link to Language
  - https://www.ruby-lang.org/en/
- Link to Interactive Ruby Website
  - https://ruby.github.io/TryRuby/
- Work through exercise section labeled "Got 30 minutes?"



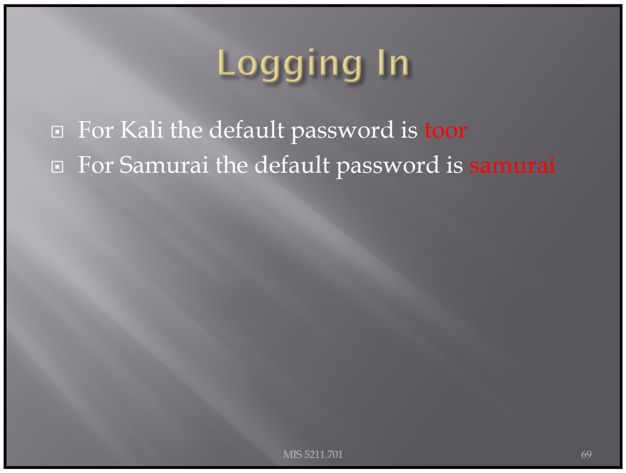
Next Week

- Reconnasaince



Linux

- What is Linux
  - Open source operating system
  - Many similarities with UNIX
- Why do we care
  - Some tools only available in Linux
  - Some tools work better in Linux
  - Best open source attack suites are built on Linux
    - Kali
    - Samurai WTF (Web Testing Framework)
    - SIFT (SANS Investigative Forensic Toolkit)



Logging In

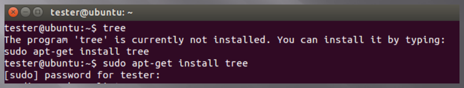
- For Kali the default password is toor
- For Samurai the default password is samurai

root

- "root" is the base admin account on a Linux system.
- Should not be used for routine operations

SUDO

- Used to execute commands that require root privilege
- Requires user to supply their password, not the root password



```
tester@ubuntu:~$ tree
The program 'tree' is currently not installed. You can install it by typing:
sudo apt-get install tree
tester@ubuntu:~$ sudo apt-get install tree
[sudo] password for tester:
```

Changing Passwords (passwd)

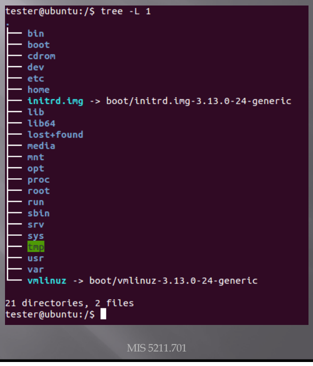
- "passwd" command is used to change passwords
- Any user can change their password by typing passwd at the command prompt.
- Will be prompted to enter new password twice
- "root" or sudo user can change others passwords with command:

passwd [login_name]

Changing Accounts

- "su" command allows you to jump to another user account (with appropriate password of course)
- "whoami" command tells you who you are logged in as

Linux File System



```
tester@ubuntu:/$ tree -L 1
.
├── bin
├── boot
├── cdrom
├── dev
├── etc
├── home
├── initrd.img -> boot/initrd.img-3.13.0-24-generic
├── lib
├── lib64
├── lost+found
├── media
├── mnt
├── opt
├── proc
├── root
├── run
├── sbin
├── srv
├── sys
├── tmp
├── usr
├── var
└── vmlinuz -> boot/vmlinuz-3.13.0-24-generic

21 directories, 2 files
tester@ubuntu:/$ 
```

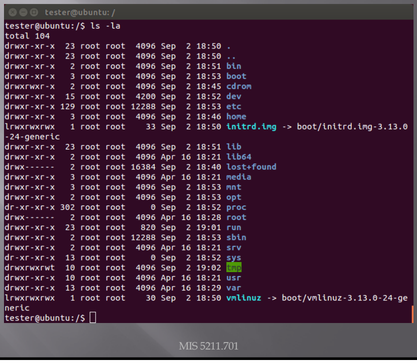
Navigating File System

- Command cd [directory_name] changes directory
- Command cd.. Moves up one level
- Command pwd tells you were you are
- Command cd by itself takes you to your home directory

Viewing Directories

- Command ls lists directory content
- Flags
  - -l – details including permissions
  - -a – shows all files
- When in doubt use command "man ls", this gives you the manual or man page for the command

Output from ls -la

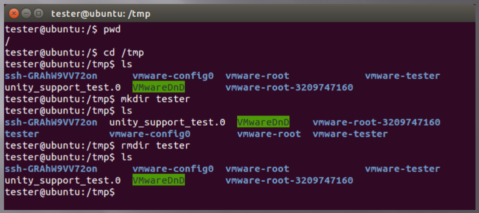


```
tester@ubuntu:/$ ls -la
total 104
drwxr-xr-x  23 root root  4096 Sep  2 18:50 .
drwxr-xr-x  23 root root  4096 Sep  2 18:50 ..
drwxr-xr-x   2 root root  4096 Sep  2 18:51 bin
drwxr-xr-x   3 root root  4096 Sep  2 18:53 boot
drwxrwxr-x   2 root root  4096 Sep  2 18:45 cdrom
drwxr-xr-x  15 root root  4200 Sep  2 18:52 dev
drwxr-xr-x 129 root root 12288 Sep  2 18:53 etc
drwxr-xr-x   3 root root  4096 Sep  2 18:46 home
lrwxrwxrwx   1 root root    33 Sep  2 18:50 initrd.img -> boot/initrd.img-3.13.0
-24-generic
drwxr-xr-x  23 root root  4096 Sep  2 18:51 lib
drwxr-xr-x   2 root root  4096 Apr 16 18:21 lib64
drwx------   2 root root 16384 Sep  2 18:40 lost+found
drwxr-xr-x   3 root root  4096 Apr 16 18:21 media
drwxr-xr-x   3 root root  4096 Sep  2 18:53 mnt
drwxr-xr-x   2 root root  4096 Sep  2 18:53 opt
dr-xr-xr-x 302 root root     0 Sep  2 18:52 proc
drwx------   2 root root  4096 Apr 16 18:28 root
drwxr-xr-x  23 root root   820 Sep  2 19:01 run
drwxr-xr-x   2 root root 12288 Sep  2 18:53 sbin
drwxr-xr-x   2 root root  4096 Apr 16 18:21 srv
dr-xr-xr-x  13 root root     0 Sep  2 18:52 sys
drwxrwxrwt  10 root root  4096 Sep  2 19:02 tmp
drwxr-xr-x  10 root root  4096 Apr 16 18:21 usr
drwxr-xr-x  13 root root  4096 Apr 16 18:29 var
lrwxrwxrwx   1 root root    30 Sep  2 18:50 vmlinuz -> boot/vmlinuz-3.13.0-24-ge
neric
tester@ubuntu:/$ 
```

Make and Remove Directories

- Command mkdir creates directory
- As before man mkdir gives you the manual
- Command rmdir removes directory

Make and Remove Directories

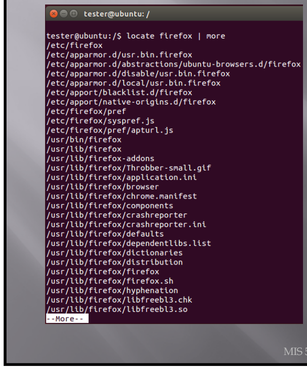


```
tester@ubuntu:/$ pwd
/
tester@ubuntu:/$ cd /tmp
tester@ubuntu:/tmp$ ls
ssh-GRAhW9VV72on       vmware-config0  vmware-root              vmware-tester
unity_support_test.0  VMwareDnD       vmware-root-3209747160
tester@ubuntu:/tmp$ mkdir tester
tester@ubuntu:/tmp$ ls
ssh-GRAhW9VV72on  unity_support_test.0  VMwareDnD    vmware-root-3209747160
tester            vmware-config0        vmware-root  vmware-tester
tester@ubuntu:/tmp$ rmdir tester
tester@ubuntu:/tmp$ ls
ssh-GRAhW9VV72on       vmware-config0  vmware-root              vmware-tester
unity_support_test.0  VMwareDnD       vmware-root-3209747160
tester@ubuntu:/tmp$
```

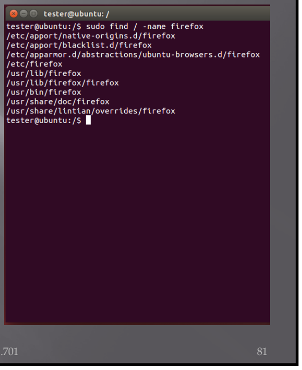
Locate and Find

- Command locate checks an index on system to look for common items
- Command find searches file system
- On my test implementation, find required sudo privileges

Locate and Find



```
tester@ubuntu:/$ locate firefox | more
/etc/firefox
/etc/apparmor.d/usr.bin.firefox
/etc/apparmor.d/abstractions/ubuntu-browsers.d/firefox
/etc/apparmor.d/disable/usr.bin.firefox
/etc/apparmor.d/local/usr.bin.firefox
/etc/apport/blacklist.d/firefox
/etc/apport/native-origins.d/firefox
/etc/firefox/pref
/etc/firefox/syspref.js
/etc/firefox/pref/apturl.js
/usr/bin/firefox
/usr/lib/firefox
/usr/lib/firefox-addons
/usr/lib/firefox/Throbber-small.gif
/usr/lib/firefox/application.ini
/usr/lib/firefox/browser
/usr/lib/firefox/chrome.manifest
/usr/lib/firefox/components
/usr/lib/firefox/crashreporter
/usr/lib/firefox/crashreporter.ini
/usr/lib/firefox/defaults
/usr/lib/firefox/dependentlibs.list
/usr/lib/firefox/dictionaries
/usr/lib/firefox/distribution
/usr/lib/firefox/firefox
/usr/lib/firefox/firefox.sh
/usr/lib/firefox/hyphenation
/usr/lib/firefox/libfreebl3.chk
/usr/lib/firefox/libfreebl3.so
--More--
```

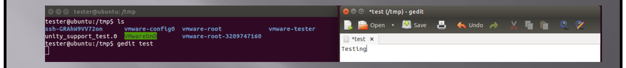


```
tester@ubuntu:/$ sudo find / -name firefox
/etc/apport/native-origins.d/firefox
/etc/apport/blacklist.d/firefox
/etc/apparmor.d/abstractions/ubuntu-browsers.d/firefox
/etc/firefox
/usr/lib/firefox
/usr/lib/firefox/firefox
/usr/bin/firefox
/usr/share/doc/firefox
/usr/share/lintian/overrides/firefox
tester@ubuntu:/$
```

Editing Files

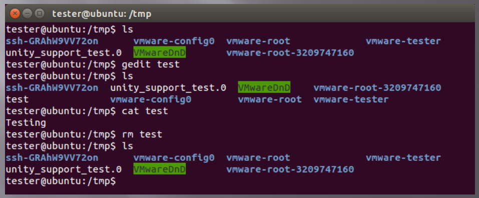
- Lots of choices, lets keep it simple
- Command gedit opens a text editor
- Command gedit test opens an existing file named test. If no such file exists, the file is created
- Edit as wish, save when done

Editing Files



```
tester@ubuntu:/tmp$ ls
ssh-GRAhW9VV72on      vmware-config0  vmware-root            vmware-tester
unity_support_test.0  VMwareDnD       vmware-root-3209747160
tester@ubuntu:/tmp$ gedit test
```

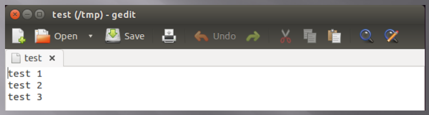
```
Testing
```



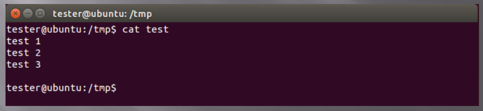
```
tester@ubuntu:/tmp$ ls
ssh-GRAhW9VV72on      vmware-config0  vmware-root            vmware-tester
unity_support_test.0  VMwareDnD       vmware-root-3209747160
tester@ubuntu:/tmp$ gedit test
tester@ubuntu:/tmp$ ls
ssh-GRAhW9VV72on  unity_support_test.0  VMwareDnD    vmware-root-3209747160
test              vmware-config0        vmware-root  vmware-tester
tester@ubuntu:/tmp$ cat test
Testing
tester@ubuntu:/tmp$ rm test
tester@ubuntu:/tmp$ ls
ssh-GRAhW9VV72on      vmware-config0  vmware-root            vmware-tester
unity_support_test.0  VMwareDnD       vmware-root-3209747160
tester@ubuntu:/tmp$
```

Viewing Files

- Command cat shows content of a file



```
test 1
test 2
test 3
```



```
tester@ubuntu:/tmp$ cat test
test 1
test 2
test 3

tester@ubuntu:/tmp$
```

Looking at Output

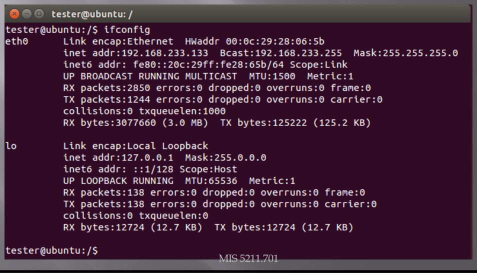
- Output often larger then screen
- Commands less and more
- Work similarly
  - less requires you hit q when done to return to command prompt
  - more dumps to command prompt when last screen is completed

Miscellaneous Commands

- Command ps shows running processes
  - Lots of switches to refine results
- Command CTRL-z interrupts running com
- Command bg restores interrupted command to run in background
- Command & tells job to run in background from the beginning
- Command jobs shows jobs running
- Command fg moves job to foreground

Network

- Command ifconfig shows network configuration. Similar to ipconfig in windows

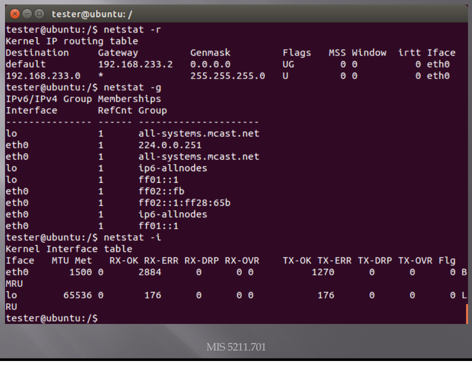


```
tester@ubuntu:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:28:06:5b
          inet addr:192.168.233.133  Bcast:192.168.233.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:65b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2850 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1244 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3077660 (3.0 MB)  TX bytes:125222 (125.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12724 (12.7 KB)  TX bytes:12724 (12.7 KB)

tester@ubuntu:/$
```

Netstat

- Netstat prints information about the Linux networking subsystem. The type of information printed is controlled by the first argument, as follows:
  - (none) – By default, netstat displays a list of open sockets. If you don't specify any address families, then the active sockets of all configured address families will be printed.
  - --route , -r – Display the kernel routing tables. See the description in route(8) for details. netstat -r and route -e produce the same output.
  - --groups , -g – Display multicast group membership information for IPv4 and IPv6.
  - --interfaces, -I – Display a table of all network interfaces.
  - --masquerade , -M – Display a list of masqueraded connections.
  - --statistics , -s – Display summary statistics for each protocol.

Netstat



```
tester@ubuntu:/$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.233.2   0.0.0.0         UG        0 0          0 eth0
192.168.233.0   *               255.255.255.0   U         0 0          0 eth0
tester@ubuntu:/$ netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      all-systems.mcast.net
eth0            1      224.0.0.251
eth0            1      all-systems.mcast.net
lo              1      ip6-allnodes
lo              1      ff01::1
eth0            1      ff02::fb
eth0            1      ff02::1:ff28:65b
eth0            1      ip6-allnodes
eth0            1      ff01::1
tester@ubuntu:/$ netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500 0      2884      0      0 0          1270      0      0      0 B
MRU
lo        65536 0       176      0      0 0           176      0      0      0 L
RU
tester@ubuntu:/$
```

grep

- grep searches the named input FILEs for lines containing a match to the given PATTERN. By default, grep prints the matching

Grep w/ netstat and ps

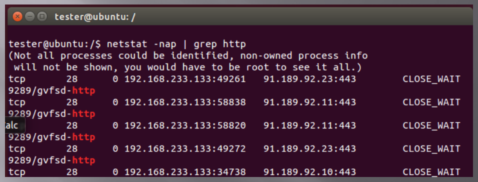
- Try grep with netstat to see what is using http

netstat -nap | grep http

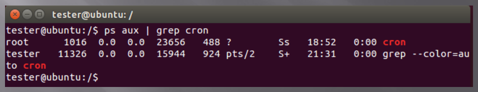
- Try grep with ps to see if cron is running

ps aux | grep cron

Grep w/ netstat and ps



```
tester@ubuntu:/$ netstat -nap | grep http
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        28      0 192.168.233.133:49261   91.189.92.23:443        CLOSE_WAIT
9289/gvfsd-http
tcp        28      0 192.168.233.133:58838   91.189.92.11:443        CLOSE_WAIT
9289/gvfsd-http
alc        28      0 192.168.233.133:58820   91.189.92.11:443        CLOSE_WAIT
9289/gvfsd-http
tcp        28      0 192.168.233.133:49272   91.189.92.23:443        CLOSE_WAIT
9289/gvfsd-http
tcp        28      0 192.168.233.133:34738   91.189.92.10:443        CLOSE_WAIT
```



```
tester@ubuntu:/$ ps aux | grep cron
root      1016  0.0  0.0  23656   488 ?        Ss   18:52   0:00 cron
tester   11326  0.0  0.0  15944   924 pts/2    S+   21:31   0:00 grep --color=au
to cron
tester@ubuntu:/$
```

Going Further

- Get VMWare and a Linux ISO
  - Kali
  - http://www.kali.org/downloads/
  - Ubuntu
  - http://www.ubuntu.com/download/desktop
- Give it a try
- All examples here where created in a clean, plain vanilla Ubuntu install