l.SI110 Learning Objectives

1. The Cyber Battlefield----------

➢ Information Assurance

- **Explain** the DoD Information Assurance (IA) Model ("Pillars of IA")". **(CIANA)**
    - **C**onfidentiality
    - **I**ntegrity
    - **A**vailability
    - **N**on-repudiation
    - **A**uthentication
- **Describe** cyber attacks in terms of compromise to the pillars of IA.
    - **C** - Protection of information from disclosure to unauthorized individuals, systems, or entities. EX: Target credit card breach
    - **I** - Protection of information, systems, and services from unauthorized modification or destruction. EX: Stuxnet
    - **A** - Timely, reliable access to data and information services by authorized users. EX: DDOS Attacks
    - **N** - The ability to correlate, with high certainty, a recorded action with its originating individual or entity. EX: Unauthorized manipulation of transaction logs.
    - **A**- The ability to verify the identity of an individual or entity. EX: RSA security breach.

➢ Digital Data

- **Define** terms such as bit, byte, ASCII, hex.
    - Bit - individual unit
    - Byte - 8 Bits, making two hex digits
    - Hex - 4 bits to translate to numerical/alphabetical 0-9 a-f

hex	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
4-bit	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

    - ASCII - plain text rendered from hex.
- **Convert** between binary and decimal number representations.
    - Binary to Decimal - http://youtu.be/UUqtjb8WEUs
    - Decimal to Binary - http://youtu.be/qWxiXU02ZQM
- **Use** tools to determine a file's type by examining its digital content.
    - Tables provided on a test will help you determine the correct header for the appropriate file format / extension. Use the next bullet to define the appropriate terms.
- **Explain** what is meant by the terms "file type", "file format", "file header", and "filename extension", and **explain** how a filename extension is used and abused.
    - File type - the kind of data stored in a file; how the bytes in a file are intended to be interpreted, e.g., as text, as an image, as CPU instructions

    - File Format - the encoding used to represent the information stored in a file, e.g., an image could be stored using the JPG, GIF, or PNG format (or others).
    - File extension - the suffix portion of a file name, which in correct practice is used to indicate the file format.
    - File Header - is a short sequence of data at the head, or beginning, of the file data. This can readily be recognized when viewing a file in a hex editor.
    - Filename extensions can be abused to make a malicious file appear as something it is not by renaming the extension from a malicious file type to a normal .jpg or .doc format to fool the user.

➢ The Physical Computer

- **Describe** a computer as a device that manipulates digital data through input, processing, and output.
    - device that can read in data, process data, output data, and, optionally, store data.
- **Name** the major physical components of a computer, **describe** their function, **remove** them from and **reassemble** them into a working computer.
    - CPU - this stands for Central Processing Unit. It is essentially the brain of the computer.
    - Memory (RAM) - this is the CPU's short term memory, it can only really compute with values it has loaded into RAM, because the CPU itself can only remember a very small number of things. When the power goes off, anything stored in RAM is losurned off.
    - Peripherals - These component computer but ars. I know longer know what a peripheral is.
    - Hard Drive (HD) - this is the computer's long-term memory. Things stored here are remembereD even after the power's been te not a part of the core architecture of your computers are attached to the computer in some way to increase the capabilities of yo. These are things like webcams, printers, scanners, and many others.
    - Look at the dissection lab to learn more about the placement and identification of each item. http://www.usna.edu/CS/si110/lec/l04/lec.html
- **Explain** program launch and the CPU fetch-decode-execute cycle.
    - You tell the computer to do something, for example: launch a program.
    - The instructions are copied to temporary memory(RAM).
    - Temporary memory talks to the CPU and as each of the instructions are sent, the CPU decodes what should be done.
    - The CPU executes the instructions and repeats the fetch (from RAM), decode, execute cycle.
    - When all parameters of the instructions have been met, the cycle is complete.

➢ Operating Systems

- **Define** the purpose of an Operating System (OS) and these core services it provides: access control; and filesystem, process, and user account management.
    - An Operating System (OS) is a Program (or collection of Programs) that manages the physical computer and the Programs that run on it (Programs managing Programs).
    - Filesystem - the OS manages all the different storage-related peripherals, like hard drives, flash drives, DVD's, etc. The OS can create, modify, read and destroy files on behalf of other Programs.

    - Process - The important thing here is that the OS manages the Programs as they execute, scheduling when each Program gets to use the CPU to progress in its execution.
    - User account management - the OS ensures that users log in properly, and that they can only access the things they're supposed to.
- **Describe** how the shell is the OS interface for both users and programs, and contrast it with the GUI and API interfaces.
    - Shell - OS interface for USERS and PROGRAMS. The shell allows commands for the OS to be entered as plain text strings.
    - GUI - "graphical user interface", basically this is the stuff you click on or use your fingers on a touch screen to interact with.
    - API - Application Programming Interface. It is a very direct way for an executing Program to ask the OS to do something on its behalf. The API is an interface exclusively for Programs.
- **Explain** the concept of absolute and relative filesystem pathnames.
    - Absolute pathnames can be identified by a base directory such as C:\
    - Relative pathnames can be identified by a home directory that does not include a colon such as \desktop\foo.txt
    - These can be used when executing the change directory (cd) command in the windows shell.
- **Describe** the distinction between a program and a process.
    - Program- An executable file
    - Process- An actively open and executing program/ executable file
- **Explain** the role of the OS with respect to security as relates to user accounts, logins, and file/process ownership and access permissions.
    - Program - a set of CPU instructions stored in a file. After loaded into RAM, a Program is called a process.
    - program - a text file written in a programming language
    - process - A program file loaded into RAM, in some state of execution; an "executing instance of a program".
- **Explain** the significance of an Administrator ("root") account.
    - Administrators have the highest level of privileges. Normal users are sometimes restricted from executing large-scale commands, while administrators can facilitate control of the system or network as a whole.
- **Perform** basic OS and network related tasks in both Windows and UNIX.
    - Reference the Windows / Unix Dictionary for different commands. Familiarize yourself with the tables provided to ensure that you can identify the different commands in each system.
    - http://rona.academy.usna.edu/~si110/resources/windowsunixdictionary.html

➢ Programs

- **Explain** the concepts of data types, expressions and variables, and correctly **use** them to modify the behavior of simple programs.
    - Numbers - Simplest expression. Evaluates itself. Used in math functions and arithmetic
    - Variables - defined names to store values. Helpful in javascript to create functions and strings to be acted upon. ex: var n= .25 The variable *n* is defined as .25
    - Strings - used to represent sequences of characters.

- Given a simple code example involving branching and loops, **explain** how the code inputs, processes, and outputs data.
    - Reference the homeworks and previous exams to see how questions about processes could be asked. Usually in the form of "What does this script do?" or "How would you make this script do *x*?" http://www.usna.edu/CS/si110/lec/l09/lec.html
- **Discuss** the implications on program execution of unexpected data input by a user.
    - When a program is written with 'holes' it can allow for the user to sometimes 'break' or otherwise bypass intended functions by inputting data outside of the parameters required. Such as "Enter a number between 1 and 10" and they input a character, rather than a number. If the program is written improperly it would allow this and cause a malfunction in the code. Look at previous exams and how the code would be adjusted to combat this, along with what sort of reactions different scripts would have. http://www.usna.edu/CS/si110/lec/l10/lec.html

➢ The Web

- **Describe** the World-Wide-Web ("web") as a client-server system involving the HTTP protocol.
    - The World Wide Web is the vast global collection of servers and clients (aka browsers) communicating over the Internet using the HTTP protocol (or HTTPS). The Web is an example of a client-server system.
- **Explain** the components of a URL.
    - Protocol - The portion before the double slash. usually HTTP or HTTPS3
    - Server - The 'bulk' of the URL. Where the data is being extracted from. Starting from the double slash and continuing until the next slash. for example www.google.com
    - Path - The file path in which the data will be located. Anything following first single slash. for example, the bolded and underlined text below. www.google.com**/Users/crazy/awesome.txt**
- Given a simple HTML file, **describe** how it will be rendered by a browser.
    - Know the simple HTML commands and what each means. Know styling and links, embedded images. Page 3, question 6 of the homework below is a great reference which we all had issues with. http://rona.academy.usna.edu/~si110/lec/l12/hw/hw.pdf
- **Describe** client-server interaction for a static web page, and the processing done by the browser on the data it receives.
    - The browser requests the page, reads the source data, then renders the page. HTML will be rendered as a whole, while Javascript will be rendered sequentially.
- **Describe** client-server interaction for a dynamic web page that involves user input to a form and server-side scripts.
    - After the page is rendered, the user will be prompted with a form or pop-up message. When the user inputs the data, the javascript will execute the necessary actions to redirect the user to the appropriate outputs. When the javascript is executed in the web page itself it is client side, if the code is executed server side, the HTML will reference a script outside of the page and the URL will show a question mark, followed by the input.
- **Discuss** tradeoffs between client-side and server-side scripts, and **explain** why client-side input validation is weaker than server-side.
    - As seen above, client side is weaker because the scripts are ran on the client's browser. If you look at passwords, the script would reveal the redirect, thus

allowing the user to bypass the need for the password input. On server side scripting, with proper encryption, the user would be forced to use the proper password, which the server would decrypt and send the user on their way.

- **Explain** how an email containing HTML with embedded scripts is a risk to security.
    - Embedding scripts into HTML in an email is risky because it allows the sender to put malicious scripts into their message that would go unnoticed until the user opened the email. Most email clients disable scripting to protect their users. Most cases of these malicious attacks are Phishing.
- **Explain** how cookies are used by both the web browser and the webserver.
    - Browser - The browser stores cookies related to different web pages for authorization.
    - Server - Maintains a record to validate that the users requesting access have the right cookies to view certain content.
- **Explain** how reflection, injection attack, and cross-site scripting work and why they may fail.
    - Very broad, can be seen here: http://www.usna.edu/CS/si110/lec/l18/lec.html

➢

    - Transport - a client needs to send a bunch of bytes to the server (its request), and then waits around and ultimately receive a bunch of bytes Networks
        a. **Explain** the basic functioning of the Internet in terms of hosts, packets, routers and IP addresses.
            i. Host - computer connected to a network.
            ii. IP Adress - On the Internet, hosts are identified by their IP Addresses. They may or may not have a name as well, but always an IP Address. ex: 192.168.1.1
            iii. Packets - Information travels around the Internet like notes being passed in class. This message chunk+address is called a packet. Each packet gets passed from one host to another
            iv. Routers - The intermediate packet-passing hosts in this process are called routers. Hosts normally live at the end points of communication, and routers live along the communication routes in the middle. A router uses a packet's IP Address to choose a neighbour host that gets the packet closer to the recipient (destination IP Address), and passes the packet on to that neighbour.
        b. **List** the layers in the protocol stack of the TCP/IP Model. **Describe** each layer in terms of its function and the hardware devices used. **Contrast** TCP and UDP transport.
            i. Application - The Application Layer is about programs running on different hosts that want to communicate from the server (the server's response). The server needs the reverse. This is the service browsers and web servers need the Transport Layer to provide. the Transport Layer has to on one side break the request/response message up into small pieces and wrap each piece up with an address to form a packet, and on the other side reconstitute the received packets into a full message.
    - Internet - responsible for routing packets the Internet from the source host to the destination host through the various networks that make up the Internet.

    - Link - Actually getting the packet between hosts within the same network is the job of the Link Layer.
    - Physical - The lowest layer is the easiest of these to understand: The Physical layer is wires and radio waves.
- For each of the following protocols: **describe** its purpose, **state** the protocol stack layer it uses, and **identify** commands or tools that use the protocol: HTTP(S), DNS, DHCP, SSH, RDP, SMB, SSL/TLS, TCP, UDP, ICMP, ARP. **Relate** ports, services, and protocols.

2. network address, usually written as a dotted quad. Example: 255.255.255.0 specifies a 24 bit network prefix, i.e., a network where all hosts have the same values for the first 3 components of their dotted quads.
3. Network address - A network prefix expressed as a dotted quad. Example: 131.122.88/24 defines a network address where the first 24 bits in an IP address are identical. A gateway router uses the network address to decide if a packet must be forwarded to a different network.
4. Broadcast address - the address at which all hosts on a local network will be recipients. Packets sent to a broadcast address are not routable, i.e., they will never leave the local network.
5. Private address - an IP address that cannot be routed to, from a host outside a gateway router.
6. MAC address - (Media Access Control) the address used at the Link Layer of the TCP

Service	Protocol	Port	TCP/UDP	Tools
"ping", check if node is alive	ICMP	--*	--	ping
World Wide Web	HTTP	80	TCP	browsers
Secure Web	HTTPS	443	SSL/TLS	browsers
Name Resolution	DNS	53	UDP	nslookup
Secure Remote Shell	SSH	22	TCP	ssh (PuTTY)
Remote Desktop (Windows)	RDP	3389	TCP	rdesktop (a UNIX tool)
Secure Remote File Transfer	SFTP	22**	TCP	WinSCP
Dynamic Host Configuration***	DHCP	67/68****	UDP	built in Windows DHCP client, dhclient
Network file & printer sharing	SMB	445	TCP	the file browser's "map network drive"

+ You only need to memorize the ports that are highlighted
* Ping doesn't use the Transport Layer, so there's no associated port
** Same port as SSH because it actually uses SSH
*** Means you can join a network "on the fly" and get assigned an IP Address and find a DNS serverPort
**** 67 is for the server, 68 is for the client

/IP protocol stack for sending a packet to an a

- **Describe** the Domain Name System (DNS) and security issues with name resolution.
    - Phonebook of the internet
    - From a security perspective it's crucial that DNS works properly. If the name bankwithallmymoney.com gets resolved incorrectly to an IP address owned by a bad guy, I could be in trouble. He could put up a dummy web page that looks just like bankwithallmymoney.com's, but which isn't and he could perhaps steal my password ... and then my money.
- **Describe** each of the following: IP Address, subnet mask, network address, broadcast address, private address, MAC address, BSSID, ESSID.
    - Subnet mask - A 32-bit value that encodes the number of prefix bits in adjacent (i.e., physically connected) hosts. Every physical hardware network interface device has a unique MAC address "burned into" its circuitry at manufacture.
    - BSSID - (Basic Service Set ID) the MAC address of a base station, used to identify it to host stations.

        - ESSID - (Extended Service Set ID) a character string identifying an ESS. Example: usna-wap.
- Appropriately **use** these commands and tools and **explain** their output: ipconfig/ifconfig, netstat, arp, ping, traceroute, nmap, nslookup, netcat.
        - ipconfig / ifconfig - IP for windows, IF for unix; use these to identify your IP address and IP configurations.
        - netstat - Displays information on current port usage (-a shows "all")
        - arp - The Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.
        - ping - Check whether host with name/IP Address is alive
        - traceroute - tracert (windows) Determine route taken by packets to given host
        - nmap - discover hosts and services on a computer network, thus creating a "map" of the network.
        - nslookup - Translates domain names to IP addresses and vice versa
        - Optional second argument specifies what nameserver to use.
        - netcat - lets you send and receive tcp/udp traffic between two hosts.
- **Describe** the purpose of encryption on a wireless network, and compare WEP, WPA, WPA2.
        - We can't effectively control who transmits on and receives our wireless network's frequency, so anyone within range can listen in on 802.11 traffic or broadcast 802.11 traffic. We cannot: control who can join our network, nor provide privacy (Confidentiality Pillar of Cyber Security) from people who have not joined our network but are none-the-less snooping (i.e., listening to the radio traffic).
        - The most common solution to both these problems is to encrypt (encode) the data you broadcast in such a way that only the people you want on the network can decrypt (decode). To join/scramble/unscramble one needs a "key".
        - WEP - (Wired Equivalent Privacy), the oldest of the three methods. This uses a weak (by today's standards) encryption method and a 40-bit key.
        - WPA - (Wifi Protected Access), which uses the same encryption method as WEP, but uses a stronger 128-bit key.
        - WPA2 - (Wifi Protected Access 2) is the strongest of the three encryption methods. This uses a strong 256-bit key for the encryption and is currently considered the best protection for wireless networks.

7. Security Tools----------

➢ Firewalls

- **Relate** use of a firewall to the pillars of IA.
        - **C**onfidentiality - By filtering the port access, information that is stored in certain areas on a server can be protected from unauthorized access.
        - **I**ntegrity - Blocking access to ports such as SSH allows for no unauthorized changes to network systems.
        - **A**vailability - By implementing firewalls, malicious attacks on the server can be hindered and prevented. For example: DDoS.
        - **N**on-repudiation - No unauthorized changes by anyone who shouldn’t be there. By blocking certain ports, illegal escalation of privileges can be prevented.
        - **A**uthentication - Certain IPs can be filtered for each port, making authentication easy.
- **Describe** a firewall's role in implementing decisions concerning tradeoffs between service and security.

- A firewall is a device or program that filters network traffic in order to control access to services; many routers have firewall programs built into them. A firewall is configured with a set of rules, called an Access Control List (ACL), which the firewall uses on each and every packet to determine whether to forward (allow) the packet to its destination or drop (deny) the packet (i.e. filter it out).
- Must filter enough malicious activity out, while still allowing for proper function. If you build a house with no door, nobody can get in to rob you, but you can't get out to get food. Or air.

➢ Authentication and Cryptography

- **Describe** and **contrast** symmetric encryption, asymmetric encryption and hashing and **explain** their roles in protecting the Pillars of IA.
  - Symmetric encryption - a cryptosystem using a key shared between the communicating parties, and otherwise kept secret. The same key is used to encrypt and decrypt. Example: AES.
  - Asymmetric encryption - (public key cryptography) a cryptosystem using public/private key pairs. Plaintext encrypted with one of the two keys can only be decrypted with the other key. Example: RSA.
  - Hashing - (cryptographic hashing) a technique that computes an output value (a "hash") from input data (the "message", or "key"), by applying a hash function. When the hash function has certain properties, hashing is a tool that provides Integrity. Hashing is also often used in password authentication.
- **Explain** and actually **use** representative symmetric encryption and hashing techniques that are done "by hand" (e.g., Vigenere Cipher, Rubik's Hash).
  - Reference http://www.usna.edu/CS/si110/lec/l27/lec.html for explanations and practice in Ceasar, Vigenere, and Rubik's hashing. Focus on what previous tests have asked!
- **Identify** the user's vs. the technology's responsibilities in situations where cryptography is used (e.g., HTTPS).
  - User - Verification of certificates provided, ensuring that their own system is updated.
  - Tech - Verification of user's data, management and security of all data and password hashes.
- **Describe** common tools such as AES and MD5,**relate** their use to Information Assurance.
  - MD5 - takes a sequence of bytes of any length and produces from it a 128-bit (16 byte) hash value, which is invariably written as a string of 32 hex digits.
  - AES - (Advanced Encryption Standard) is a symmetric key (i.e. there is a single, shared secret key) encryption algorithm for encrypting digital data. It is a 128-bit block cipher, i.e., it always operates on 128 input bits at a time, although it has several variants with different key sizes.
  - These provide confidentiality of user's passwords by saving the encrypted value, then encrypting the input, then matching the two. This could be applied to many other pillars as well.
- **Discuss** authentication by password, password attacks, hashing, salt, and password strength.
  - A very common application of hashing is password checking. Suppose there's a server you login to from time to time. It's undesirable to store your password on the server's hard drive. There are tricks that might allow people to see that file and, once they do, they'd have your password and be able to log in as you. So instead,

we'd like the server to store something that it can use to verify your password, but which nobody can use to figure out your password. We can use a hash function!
    - Hashing allows for the passwords to be encrypted and then matches the hashed value to the stored file.
    - Salt is added before hashing to add another layer of random security, to prevent decryption.
    - Online Attacks. In this setting, the attacker does not possess a password-hash file, but actually tries to login with many different passwords. Most systems take a long time (in computer terms) to respond to a login — especially an incorrect login. This limits the effectiveness of this kind of attack.
    - Offline Attacks. In this scenario, things are a lot more dire, because someone has stolen the password file. Because the attacker has his own copy of the password file, he doesn't have to try logging into a real system to check whether he's found the password. He simply hashes his guessed password and checks if it matches a hash in the file. This means he can check millions — potentially billions — of passwords per second.
    - Server Responsibilities:
        a. Use Hashing
        b. Use Salt
        c. Secure the Password File
    - Client Responsibilities
        a. Choose Unusual Passwords
        b. Choose Long Passwords
        c. Choose Complex Passwords (uppercase, lowercase, number, special character)
        d. Do Not reuse a password from another account
- **Discuss** two-factor authentication.
    - Use two forms of ID. Password and a physical item or another ID code. IE: Smart Card
- **Explain** the workings of attacks such as frequency analysis, chosen plaintext, and man-in-the-middle.
    - Frequency analysis - based on analysing the frequencies of letters in the ciphertext to get information about what key value produced that ciphertext. If you can deduce the key, you can decrypt the message. Cracks the ceasar cipher.
    - Chosen plaintext - Trick someone into using their code to send a message of yours so you not only have the message, but the ciphertext as well. there are three strings — the key, the plaintext and the ciphertext — and knowing any two is enough to get the third.
    - Man-in-the-middle - an attack where the threat intercepts and forwards messages without his presence known by the communicating parties.
- **Describe** the purpose of Public Key Infrastructure (PKI) and how it works; **relate** PKI to man-in-the-middle attacks.
    - Public keys allow people to encrypt a message meant for only one user to read, so that when it is in transit, men-in-the-middle cannot grab it from the air. It is encrypted by person A with B’s public key, so that B can read it by using his private key.
- **Explain** the guarantee that comes with a valid certificate, **describe** reasons a certificate may be invalid, and how user actions with respect to certificates can affect security.

- Messages you receive can only be read by you and can only have come from the actual sender
- Message you send can only be read by the receiver and the receiver will know it could only have come from you.
- A certificate may be invalid if the signing authority cannot be verified, it is out of date, or something about it is suspicious.

8. Cyber Operations----------

➢ Digital Computer Forensics

- For a given activity, **state** the forensic evidence it leaves behind and where it can be found.
  - Website visits:
    a. Date/Time/IP entry in the sites server log
    b. Can be found in browser history
  - Message board attack:
    - Date/Time/IP entry in the server log
    - Can be found in web server log
- **Describe** and **use** MD5 in digital forensics.
  - (Message Digest Algorithm) a cryptographic hash function; an MD5 hash is 16 bytes long.

➢ Malware

- **Classify** various types of malware.
  - Virus - A computer virus is a computer program that can replicate itself and "infect" a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, or even the whole hard drive.
    a. Macro - A virus written in a macro language for a separate application, such as a word processor. Some programs allow macro programs to be embedded in documents (Microsoft Office products), this provides a unique vector for viruses.
    b. Cross-site Scripting: Up and coming virus type, virus executed by your web browser.
    c. Program virus: This is the most traditional virus, a stand-alone executable program attached to some other file (which usually looks benign).
    d. Boot sector: A virus that starts every time computer boots. This can be mitigated by setting this area on the disk to read-only, so that only the Administrator can override.
  - Worm - A computer worm is a self-replicating, self-propagating program that uses networking mechanisms to spread itself. This is a virus with the added functionality of spreading across a network without any help from a user.
  - Trojan - a program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes exploiting legitimate authorizations of a system entity that invoked the program. In contrast to viruses, Trojans don't try to propagate — they don't try to replicate themselves or send themselves to other machines. In fact, "trojan" refers to the mechanism by which the malware is delivered not really to the malware itself. Once malware is delivered via a trojan, in might be used to gain access to other hosts, but not usually via the same trojan mechanism.

- **Describe** malware as an attack vector that in most cases depends on both a vulnerability and a user action; **define** "zero day".
    - Zero-day Attack - An attack that makes use of a zero-day exploits against a zero-day vulnerability. A single attack mission may make use of multiple zero-day attacks.
    - Zero-day exploit - An exploit that exploits a zero-day vulnerability
    - Zero-day vulnerability - A vulnerability that is unknown to cyber security professionals (cyber security researchers, cyber domain penetration testers, software/hardware vendors) at large.

➢ Phases of Cyber Attack

- **Describe** the phases of a cyber attack, **relating** them to the pillars of IA.
    - Infiltration - Find a back door into the network
    - Escalating Privileges - Finding ways to reach admin or root status
        a. Password guessing
        b. Code injection (buffer overflows, sql, trojans)
    - Attack - erase data, steal data, modify data, escalate more, steal and sell passwords

➢ Computer Network Attack (CNA) and Computer Network Defense (CND)

- **Give examples** of defense-in-depth.
    - DID - Redundant defense measures to defend a network
        a. Multiple firewalls
        b. DMZ / Perimeter network
        c. Sandboxing
        d. Monitor logs
        e. Monitor traffic

➢ Case Studies

- **Use** knowledge of the Cyber Battlefield, Models and Tools, and Cyber Operations to **analyze** case studies to **identify** technical and human security failures.

➢ **Estonia 2007**

- DDOS attack to Estonia's Networks
    - Destroyed availability for media, government infrastructure and banking.
- 2 Sources of attack:
    - Script Kiddies - novice javascript that follows instructions.
    - Botnet (zombies) - ping attacks (from all over the world) to Estonia's servers.
- Solutions
    - Tried to shut down all the traffic coming from Russia, then the world.
        a. These Firewalls were useless since it dropped signals from outside networks also.
    - Blocked all IPs at the source of computers all over the world.
        a. They needed help from foreign countries to make sure that the IPs were safe to allow access.

➢ **RSA Labs on Lockheed Martin - March 2011**

- RSA company produced one-time-password keys for Lockheed Martin employees.
- Spear Phishing attack with an excel attachment.
    - "Zero Day" exploit was launched: no known defense (no patch available)
    - Allowed to install Trojan (backdoor entry) which also provided later access.
    - Escalated privileges, found secrets, found seeds (foundation of system).
    - Encrypted secrets - exfiltrated through file access.
    - Deleted and covered tracks.

    a. RSA needed to replace 40 million devices

- **Lockheed Martin - May 2011**
  - A keylogger was installed in employee's computer.
    - Grabbed username/password - one-time-password code.
  - Recreated individual one-time-passwords to maintain access.
  - Lockheed Martin claimed that nothing was stolen.
  - Solution
    - Vigilance of traffic entering and leaving network.