Section 5: Securing Individual Systems

47.Denial of Service

DOS
Three big groups:

```
1. Volume Attacks (Doesn't do anything wrong, just a lot of it.)
        1. Ping Flood
        2. UDP Flood

2. Protocol Attack (Does bad things to the protocol to create confusion)
        1. SYN Flood/TCP SYN Attack

3. Application Attack
        1. Slow Loris Attack

        *Amplification attacks:
                1. Smurf Attack (Spoofs Websites IP address)
```

DDOS - (Malware forms a botnet to attack) aka - A bunch of computers with malware on them that are called 'Zombies' are under the control of one computer.

Quick Review:

```
- Denial of Service Attacks prevent others from accessing a system
- Distributed Denial of Service uses multiple systems to attack a single
host.
- Denial of Service attacks can broadly be broken down into volumetric,
protocol, and application attacks
```

48.Host Threats

```
1. Spam - Unsolicited Email

2. Phishing and Spear Phishing - Unsolicited Email that is trying to get
information out of you
        1. Spear Phishing - Get the potential victims name and uses that to
get information

3. Spim - To recieve unsolicited things via instant messaging

4. Vishing - The unsolicited use of voice to get info out of you

5. Clickjacking - When you go onto a website and you are lead to accidently
```

click something bad (download malware, authorize something)

6. Typo Squatting and Domain Hijacking - Takes andvante of someone will make a typo when going to a popular domain

1. Domain Hijacking - They steal your domain name of your website and often try to randsom the original domain owner

7. Privilege Escalation - people getting privileges and uses them to do bad things

Quick Review:

- Phishing is unsolicited emails that typically request information from you
- Vishing is voice-based (Voice+Phishing) solicitations requesting information about you that is confidential
- Be able to recognize all of these threats

49.Man in the Middle

Man in the middle attack is a third party that is sneaking into a conversation between people.
The number one thing for MITM attacks is garnering information

Two big parts to MITM Attack
1. Third-party interception between a two-party conversation
2. Uses the information to the third parties advantage

Wireless man-in-the-middle Attack:

802.11:

- Isolation is beneficial to protect people from this
- WPA is susceptible to hacking still but encryption helps prevent this
- WEP is totally Susceptible to hacking and man-in-the-middle

Bluetooth:

- Susceptible to attack
- Relies on short distances and short connection duration to prevent attacks

NFC (Near Field Communication):

- Relies on extremely close distances

Wired Man-in-the-middle attack:

Spoofing: (making something in the attackers address look like its the vicitms e.g. MAC Spoofing, IP Spoofing, DNS, etc)

```
        - Ettercap (finds all host on the network)
                - Allows spoofing by 'Poisionings'
                - Grabs data and looks through it
- MAC spoofing = Port stealing
- IP Spoofing = ARP Poisioning (Very Noisy)
- DHCP Spoofing
* Typosquatting
* Domain Highjacking
```

Manipulating Man in the Middle data:

```
- Replay attack: Get username and a hash, replay it later and login anytime you want, also impact certificates
- Downgrade attack: Webpages (weaken a conversation by downgrading to a less secure communication method)
- Session hijacking: Inject information into the middle of a conversation. (Very Difficult)
        - Firesheep (old session jacking tool)
```

Quick Review:

- To start a man in the middle attack one must 'get in the middle'
- Once an attack is succesful you must use all information obtained
- The type of network can make the man in the middle attack easier or more difficult

---

50.System Resiliency

1. Scalability: e.g. Being able to add servers to take care of demand
2. Elasticity: e.g. Being able to scale up and down

*Cloud based services allow us to do these things easily.

3. Redundancy
   Distributive Allocation: Redundancy, still more than one, but in different parts of the country incase there are weather conditions etc.

Non-persistence ("isn't permenant")
1. Snapshot: keep a copy of a system in its current state at a binary level
2. Known State: Getting back to one small aspect of a machine.
3. Rollback: Zeros in on a small part of a system e.g. Drivers
4. Live CD: aka bootable drive (e.g. kali live)

Quick Review:

- Elasticity is the ability to expand and contract your network system depending on demand
- Redundancy is a form of distributive allocation

- Non-persistence is data that is collected but will not be saved on restart
- A snapshot reverts to known state, rolls back to known configuration, and can store non-persistent data

---

51.RAID

RAID (Redundant Array of Independent Disks)
"Instead of using one hard drive, use multiple hard drives that act as one that are going to do one of two things:"
1. Provides Data Integrity
2. Improves Access

RAID VERSIONS

```
1. RAID 0 (AKA STRIPING) - Increases the speed at which you can get data. **Speed with no data integrity**
        1. Disperses a piece of data across multiple drives
        2. Downside to striping is that if you lose one drive, you lose all your data

2. RAID 1 (AKA Mirroring) **Data Integrity with no speed (Slows things down)**
        1. Requires an even number of drives and data is copied to two drives

*"Parity" is introduced to allow both speed and data integrity

        Example:
                - Data has three pieces as an equation (1 + 2 = 3)
                - If any part of the data is lost the lost piece can be figured out (x + 2 = 3)

3. RAID 2 (RAID 3 AND 4 ALSO USED A DEDICATED PARITY DRIVE)
        1. Minimum of 3 drives
                1. Drive 1 - Half of the data
                2. Drive 2 - The other half of the data
                3. Drive 3 (Dedicated Parity Drive) - Parity Calculation

4. RAID 5
        1. Requires 3 drives minimum (Parity is distributed to all drives)
        2. Downside is that you can afford to lose one drive, but you cannot lose more than one

5. RAID 6
        1. Requires a minimum of 4 drives (parity is distributed and two
```

```
paritiys are made on two drives)
        2. We are able to lose 2 drives without losing any data

6. Hybrid RAID
        *Two most common types to combine:

        1. RAID 0+1 (aka RAID 01)
                1. minimum of 4 hard drives
                2. Mirroring to two drives and then striping them (Mirrored
Stripes)

        2. RAID 1+0 (aka RAID 10)
                1. 4 drives
                2. Striped data that gets mirrored (Striped Mirrors)

7. Proprietary RAID

        1. e.g. Synology hybrid Raid
                1. Accessed through a web page
                2. Box full of drives

        2. e.g. Storage Spaces
```

FOR THE EXAM REMEMBER:

Different levels of raid do two or a combination of two things
1. Increase Disk access
2. Improve fault tolerance/Data integrity

Quick Review:

- RAID arrays enable you to speed up data access, protect data or both
- The most common RAID styles includes 0, 1, 5, & 10
- RAID 1 & RAID 0 requires at least 2 drives
- RAID 5 requires 3 or more drives
- RAID 10 Requires 4 drives

NAS and SAN

NAS - Network Area Storage
SAN - Storage Area Network

- Robust dedicated systems that only share data

NAS Network Area Storage (Smaller of the two)
1. File based sharing protocol

2. Runs an operating system
3. Runs over standard network
4. Shows up as normal shares on the network (Runs Common protocols)

NAS BOX:

SANs Storage Area Networks
1. SAN provides block level storage
2. Ran on Fibre Channel (FC) (Host bus Adapter on your computer ---> Runs to a FC Switch ---> Runs to FC Controller in the server room) *Super expensive
3. iSCSI (eye-skuh-zee) - "poor mans version of SAN tech"
1. Allows you to connect to existing devices on top of your existing network and allows you to work at an iSCSI Block level
In an iSCSI Network you have a
1. Initiator
2. Target

Quick Review:
- NAS is File Level
- SAN is Block level
- SANs will either use Fibre Channel or iSCSI

53. Physical Hardening

1. Removable Media Controls (Not including USB, Mainly Optical Media'CD Rom')
    - In windows you can configure a local media policy (Can be set as a whole or for individual users)
2. DEP (Data Execution Prevention)
    1. DEP by default is a good thing.
3. Disabling Ports (Serial Ports, Parallel Ports, USB ports)
    1. Make changes in the BIOS

QUICK REVIEW:

- Policies Can control how system hardwar acts or reacts to an action
- Disabling ports can be done in the BIOS
- Turn off legacy non-active ports to avoid vulnerable entry point

---

54.RFI, EMI and ESD

Radiation that is emitted from electronic devices:

```
1. RFI - Radio Frequency Interference
2. EMI - Electro Magnetic Interference (AKA Electromagnetic Pulse)

*What can we do about radiation?
        1. Move stuff away from what is causes the interferance
        2. Shield our devices
        3. Use Separate Circuits
```

Electricity:

```
1. ESD - Electro Static Discharge
        *How to avoid it:
                1. Try to keep everything at the same potential
                2. ESD Wrist Strap
                3. USBs come with anti ESD in them
```

55.Host Hardening

1. Disable Unnessary Services
2. Default Passwords (Don't use default passwords) - All things have a default password
3. Disabling Unnessary Accounts
4. Patch Management
   Process (Enterprise Environment)
    1. Monitor (Being aware of patches that are coming out)

1. Might not get reminders
2. Test the patch
1. Deploy in sandbox environment first
3. Evaluate
4. Deploy the patch
1. Watch for scheduling issues
5. Document

5. Anti Malware
    1. Training for users
    2. Procedures
        1. Best practices
    3. Monitoring
        1. Watching security logs/network flow diagrams
        2. check DNS
    4. IDS (Intrusion detection systems)
    5. 3rd Party anti malware tools
6. Host Firewalls
    1. Firewalls work on an application-level basis
        1. white-list or black-list applications

QUICK REVIEW

- Host hardening strengthens the IT infrastructure
- Be sure all users, updates, firewalls, etc are being monitored
- IDS (Intrusion Detection System) can help detect threats to the hosts

---

56.Data and System Security

1. Data Integrity
2. Speed/Quick Access
3. High Availability

RAID

- Provides good integrity
- provides good speed
- is very affordable

Clustering
1. Instead of having one computer do a job, you have two or more computers performing the same job.
2. Very Expensive

Load balacing
1. Distributing the work load

Virtualize the servers
1. Bring server back from a snapshot
2. Still can use RAID and Clustering

QUICK REVIEW:

- Clustering is a good method to protect not only data but system resources, but its expensive
- Load balancing distributes work loads across multiple machines
- Virtualization servers is a cost effective way to secure data

---

57.Disk Encryption

```
1. Could Slow system down
```

Usage:

```
1. Mobile and portable devices
        1. laptops, smartphones, tablets


2. Desktop systems with limited security
```

Encryption tools (Two Groups):

```
1. TPM (Trusted Platform Module) Support
        1. You have a chip burned into the device which holds a full blown
public private key and there is no way to get it out
        2. Turned on at the system/BIOS level


2. Those that dont use TPM
```

Encryption tools:
PGP (Pretty good privacy)
TrueCrypt
BitLocker (Windows Environment)
FileVault (MAC Environment) - MACs don't use TPM

QUICK REVIEW:

- Disk Encryption can be a valuable tool for mobile devices, and other devices in areas without adequate physical Security
- Disk Encryption can be broken into two groups: TPM & non-TPM
- Two examples of disk encryption programs are BitLocker (Windows) and FileVault(Mac)

58.Disk Encryption

FDE (Full Disk Encryption) - Encrypts Mass storage
1. Uses software or Firmware based tools

SDE (Self Encrypting Hard Drive)

Secure Boot:
TPM (Trust Platform Model)
TPM2.0 (Inlcudes Secure Boot) (Good on Embedded Systems (Cars, etc)
- Your OS checks the Quality of everything in it (Everything must be signed) each time the system boots

```
Hardware Root of Trust provided by manufacture
        - Secures the supply chain
```

HSM (Hardware Security Model) - Used only in places where there is a lot of signing going on. (Sever Type Situations)
1. Hardware whos only job is to check signage and make sure everything is okay
- Seen often on webservers

QUICK REVIEW:

- BitLocker is a built-in Windows Utility Drive Encryption Tool; must have a recovery key to access the data
- Windows TPM chip is used by BitLocker and Secure boot and is activated in the BIOS
- Turn off legacy non-active ports to avoid vulnerable entry point.

59.Secure OS Types

What types of OS do I use in a particular Situations?

Types:

```
1. Server OS
        1. Designed to support servers
        2. Built in functionality
        3. Connections

2. WorkStation
        1. Desktop Version
        2. Workhorse systems

3. Embedded Systems
        1. Appliance
        2. Have their Own OS

4. Kiosk
        1. Limited Function
```

5. Mobile OS
    1. Apple IOS
    2. Android

When am I going to use these different OSes?

For the exam think two things:

1. Which one of the operating systems have the least amount of functionality to do the job it needs to do?
2. Secure Configurations: (Trusted Operating Systems)

Quick Review:

- The main OS types are server, workstation, embedded (appliance), kiosk, mobile
- Mobile OSes are custom designed for phones and cameras and have built-in GUI and security
- Picking an OS based on least functionality is a good security practice

---

60.Securing Peripherals

*Printers, keyboards, mice, cameras, smart phones, etc.

1. Wired vs. Wireless Periferals

   1.Bluetooth
   - Bluejacking: Making a connection to use a resource
   - Blue snarfing: Grabbing and stealing data

   Bluetooth comes in three different classes:
    1. Class 1 is 328'(distance)
    2. Class 2 is 33' (distance)
    3. Class 3 is 3' (distance)

    - Most mobile phones and Bluetooth headsets are class 2 (Range up to 33ft)

   2.802.11
   - WPS (Wireless protected setup) (Very Vulnerable)

   - Hidden Wifi (SD cards can have Wifi and can be plugged into a periferal device)

Displays/Monitors - USB Ports on the display is a security issue.

RUBBER DUCK - A USB that has a bunch of functionality that can be plugged in to do things

- Avoid Backdoors
- Turn off unneeded ports

- Patch updates

QUICK REVIEW:

- Bluetooth Connections are not very secure
- Watch out for Hidden Wi-Fi and SD Wi-Fi card
- Keep all devices patched and up-to-date

61.Malware

Types:

1. Virus: A piece of software that gets on your computer

1. Attach to other files
2. Propogate
3. Spread to other devices
4. Viruses Activate

2. Adware: Ad popups

3. Spyware: Some form of malware that you don't see but it's doing things in the background

4.Trojan Horse/RATs: runs on your system and it does something nice, but its doing something back in the background

- RATs (Remote Access Trojans) - Doesn't do bad things until someone in a remote location does something to activate it far away

5. Randomware/Cryptomalware

6. Logic Bomb - Program that is sitting on a computer and has to activate, but they trigger because there is an action that takes place.

7. RootKit/Backdoor

1. Rootkit - Software that escalates privileges to execute other things on computer (Difficult to detect and remove)
2. Backdoor - Piece of software that has an intentionally derived way to get into something

8.PolyMorphic malware, Keylogger, and Armored Viruses

- Polymorphic malware
  - Changes itself to avoid anti malware programs

- Armored Viruses are hard for anti-malware to detect

```
                                - Designed to make it hard for the anti
malware people to figure out whats going on (Prevents Reverse engineering)

                        - Keylogger: Logs keystrokes
```

Quick Review:

- Viruses do things to files and propogate, Malware collects Keystrokes and information
- Ransomware and logic bombs can devastate systems
- Polymorphic and armored malware are hard to detect and destroy

---

62. Analyzing Output

1. Anti-Malware/Anti-virus

   How do we set it up?
   1. Realtime setting (Anything coming in and out of the network card is being scanned)
   2. There is a problem and the storage needs to be scanned

   Anti-malwares often output log files
   Updates: Anti-malware auto updates to ensure protection
2. Host-Based Firewall: Any firewall installed on an individual host
   1. Output is in the form of an ACL or Rules list
   2. All host based firewalls have an Implicit Deny, you build your whitelist
   3. Remember you output is an ACL
   4. You're using Least privledge
   5. White list that builds up over time
3. File Integrity:
   1. File integrity check verifys that a file is in good order and ready to run.
      1. checks that the file Isnt corrupted
      2. hasn't been tampered with
      3. the file is the version and date that is expected
         *SystemFileChecker (sfc /scannow) - Windows tool which checks the core files which make up the windows OS
      - If the file is good, Hash it and all of its attributes.
      - Windows makes an extra copy of all critical files (sfc looks at the backup copies and compares)

   *A log is always generated by all file integrity checkers
4. Application Whitelist
   1. You don't want people installing unwanted stuff.
   2. Licensing/Inventory

3. Standardization (Same versions of everyting (e.g. office applications/web browsers)) - Standardization tools exist

Quick Review:

- False Positive - Scan results identify a file that may not actually harm a system or is allowed on the system
- Host-based firewalls are set up as implicit deny buy default; access is controlled by an ACL whitelist
- File integrity check verifies the file isn't corrupted, and that the version and date match expection

---

63.IDS and IPS

```
*Firewall is the first line of defense in protecting the network

IDS (Intrusion Detection System)
        - Inside the network
        - Watches within the network traffic
        - Sends alerts on suspicious activity

IPS (Intrustion Prevention System) - ('Active' IDS)
        - It's close to the edge of the network - inband
        - watches network traffic
        - Stops suspicious activity
```

*Know Firewall vs. IDS Vs. IPS

Quick Review:

- Intrusion detection systems detect and report possible attacks to the administrators
- Intrusion prevention systems run inline with network and act to stop detected attacks
- A firewall filters
- An IDS notifies
- An IPS acts to stop

64.Automation Strategies

Automation is used specifically for two features:
1. Repetitive - Allows us to do something at a very specific time everytime like clockwork
2. Consistent - Does something the exact way every time

Scenarios:
1. You have a classroom with 24 computers and at the end of the day you need to restore the systems.
2. Continuous monitoring of network devices
3. Automatic updates of Operating Systems
4. Monitoring application Whitelists
5. Application Development

*Built in tools vs Shells

Quick Review:

- Know the different types of automation strategies
- Automation is repetitive and consistent
- Automatino is oftern used with various scans and updates based configurable trigger
- PowerShell is a built in windows tool to write custom built scripts to automate task

---

65.Data Destruction

Three levels

```
1. Clearing: To use some internal command within the mass storage device to make the data go away (DRIVE IS REUSABLE)
        - Wiping Programs: wipes from beginning of the drive until the end of the drive

2. Purge: e.g. degouser - uses magnetation to destroy the drive (DRIVE IS NOT REUSABLE)
        - Crypto Erase: Hard drive that is encrypted, just destroy the key and the drive is useless now because it can't be recovered

4. Destroy: ruin the media in a way that is no longer functional (Life is more than harddrives, tape, paper, floppy disks)
        1. Burning
        2. Pulping (Soak paper in water and grind it up)
        3. Shredding (Literally shredding a Hard drive or other)
        4. Pulverizing
```

Quick Review:

- Clearing can be done with commands such as erase, format, and delete; these methods are not final
- Purging will process the devie to remove data from the drive, the device will no longer be usable
- destroying will ruin the data and physical medis; this includes paper, tape, electronic data, etc

---

QUIZ

Question 1:

Which host threat might appear as an email message that addresses you by name and uses some other personal information, like an account number, to request additional personal information?

- Phishing
- Spam
- Vishing
- Spear phishing

Question 2:

Which of the following are methods to store non-persistent data?

- Snapshot
- Revert to known state
- Rollback to known configuration
- Live boot media
- All of the above

Question 3:

Which of the following RAID levels require only two drives?

- ○ RAID 10
- ○ RAID 5
- ◉ RAID 0
- ○ RAID 6

Question 4:

Which of the following storage technologies operates at the block level?

- ○ NAS
- ○ LAN
- ○ WAN
- ◉ SAN

Question 5:

System hardware should be protected as a standard practice with which of the following?

- [x] Disabling legacy ports
- [ ] Using USB devices
- [ ] Booting servers only when disconnected from the network
- [ ] None of the above

Question 6:

Which type of interference is NOT due to radiation emission?

- [ ] Electromagnetic interference (EMI)
- [x] Electrostatic discharge (ESD)
- [ ] Radio frequency interference (RFI)
- [ ] Shielded Ethernet cable

Question 7:

True or false: It is not a good idea to change default username and password.

- [ ] True
- [x] False

Question 8:

True or false: Before encrypting a drive, it is vital to obtain a key and keep it in a safe place.

- (●) True
- ( ) False

Question 9:

FDE and SDE are both from which of the following?

- (●) Hardware security & disk encryption
- ( ) Boot logon security
- ( ) Certificate of trust
- ( ) Backup recovery methods

Question 10:

What software is made to run computers with particular attention to providing a secure computing environment?

- (●) Trusted operating systems
- ( ) Safe mode
- ( ) FDE
- ( ) RAID 10 enabled

Question 11:

When working with peripherals, what are some of the considerations to factor in?

- What connection type will be best match for usage and security
- If Bluetooth is enabled, what class the device is
- How to update the firmware
- (selected) All the above

Question 12:

What is a form of malware that locks you out of your system until you pay someone to unlock it?

- Trojan
- Spyware
- (selected) Ransomware
- Adware

Question 13:

A whitelist is a list of applications that are allowed to run on a system. This list can be created in which location(s)?

- Host firewall
- Group policy
- Local machine
- Proxy server
- **All of the above**

Question 14:

Which of the following answers describe automation strategies?

- Continuous monitoring with alerts
- Triggers based on thresholds or baselines
- Load balancing
- Firewall configurations
- **All of the above**

Question 15:

Which of the following will destroy the media for future uses?

- Delete
- Shred
- Format
- All of the above