Brief Introduction

Information security, sometimes shortened to infosec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection, recording or devaluation, although it may also involve reducing the adverse impacts of incidents.

Goals of Security

The CIA triad is put into pratice through various security mechanisms and controls. Every security technique, practice, and mechanism put into place to protect systems and data relates in some fashion to ensuring confidentiality, integrity, and availability.

The CIA Triad

Confidentiality:

Keeping systems and data from being accessed, seen, read to anyone who is not authorized to do so.

Integrity:

Protect the data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.

Availability:

Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.

Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO/IEC 27000:2009)

Auditing & Accountability

Basically keep tracking of everthing, like, who's been logging in when are they loggin in whose access this data.

Non-Repudiation

Anyone can validate the authenticity of a message as well as the source of the message.

---

1. Securing Individual Systems

Denial-of-Service (DoS)

Prevents others from accessing a system / comprimising the availability.

Attack Types

- **Volumetric Attack**
    - Ping Flood
    - UDP Flood
- **Protocol Attack**
    - SYN Flood/TCP SYN Attack
- **Application Attack**
    - SlowLoris Attack - *(tries to keep many connections to the target web server open and hold them open as long as possible)*
- **Amplification Attack** Generate a high volume of packets to flood the target website without alerting the intermediary, by returning a large reply to a small request. The basic defense against these attacks is blocking spoofed-source packets.
- **Smurf Attack** - flooded with spoofed ping messages.

Distributed-Denial-of-Service (DDoS)

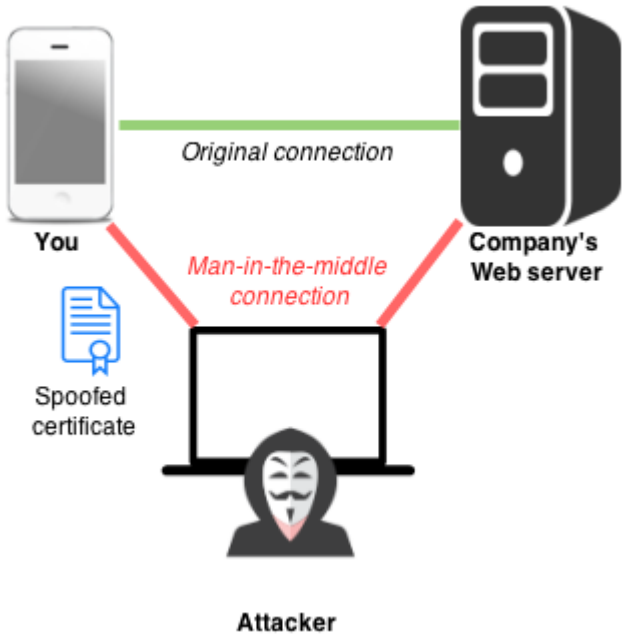
Uses multiple systems to attack a single host - Generally controlled by **BotNets**, which is a type of malware that uses remotely controlled malicious software to control a large range of computers.

Host Threats

- **Spam**
- **Phishing & Spear Phishing** - The difference between both is that Spear Phishing is for targeted individuals with some type of information about the victim embeded.
- **Spim** - Phishing through instant messaging

- **Vishing** - Unsolicited use of voice to get sensitive information
- **Click Jacking** - malicious click bait sites that forces you type your PII or download some malicious software.
- **Typo squatting** - Mistype URL's (i.e. - facebook.corn)
- **Domain Hijacking** - the act of changing the registration of a domain name without the permission of its original registrant, or by abuse of privileges on domain hosting and registrar software systems.
- **Privilege Escalation**

Man-in-the-Middle Attack



- Third-party intercepting between a two-party conversation
- Uses the information to the third party's advantage
- Wireless MITM
    - 802.11
    - Bluetooth
- Wired MITM
    - Spoof MAC address, IP address, ARP, DNS...
- Typosquatting - *(i.e facebook.corn / wikipdia.org)*
- Domain Hijacking
- Replay atack - when an attacker detects a data transmission and fraudulently has it delayed or repeated
- Downgrade attack - is a cryptographic attack that makes it change the encrypted connection to the older one (i.e. cleartext).

- Session Hijacking - Inject information on middle of connection

System Resiliency

Generally they handle risks better, adding technologies and processes to enable the system recovery easily.

Scalability

Adding more resources to take care the demand (manually added)

Elasticity

The resources grow on demand as they required (i.e. IaaS)

Redundancy - Distributed Allocation

Is a form of distributive allocation.

- Mass storage
- Redundant systems
- Redundant networks

You can create more than one copy of non-OS critical data so that if one copy dies, another copy is ready to go to keep the systems up and running.

Non-persistance

Is data that is collected but will not be saved on restart.

- Snapshots - take the current state of something (i.e binary level) and store. A snapshot reverts to known state.
- Virtualization
- Revert/rollbacks tools - The rollback method bring the system back to a previous state. (i.e. Bad Driver, broken Updated etc).
- Live boot

RAID - (Redudant Array of Independent Disks)

Different levels of RAID arrays or combination is for:

- Improve disk access.
- Improve fault tolerance and data integrity.
- Or both

Features	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
Minimum # Drives	2	2	3	4	4
Data Protection	No Protection	Single-drive failure	Single-drive failure	Two-drive failure	Up to one disk failure in each sub-array
Read Performance	High	High	High	High	High
Write Performance	High	Medium	Low	Low	Medium
Read Performance (degraded)	N/A	Medium	Low	Low	High
Write Performance (degraded)	N/A	High	Low	Low	High
Capacity Utilization	100%	50%	67% - 94%	50% - 88%	50%
Typical Applications	High end workstations, data logging, real-time rendering, very transitory data	Operating system, transaction databases	Data warehousing, web serving, archiving	Data archive, backup to disk, high availability solutions, servers with large capacity requirements	Fast databases, application servers

RAID 0

- **Has no data integrity.**
- **Improves speed** - data striping(divide the data into pieces in X hard drives); RAID0 speeds up performance but has no integrity, because if one of these hard drives fail, the data is lost.

RAID 1

- **Has data integrity** - but doesn't have performance ; slow process because the data processed in all hard drives.

RAID 5

- **Has disk striping with parity** - parity information is spread across all disks evenly; 1/n of the total disk space available is used for parity. You can only loose one drive and keep the data, the problem is if you loose more than one drive.

RAID 6

- **Disk parity with double distributed parity** - Same as RAID 5 but has one more parity which you can loos two drives and keep your data safe.

RAID 0+1 (01)

- **Disk striping with mirroring** - combines both RAID levels 0 and 1 for performance and redundancy; a mirror of two striped arrays.

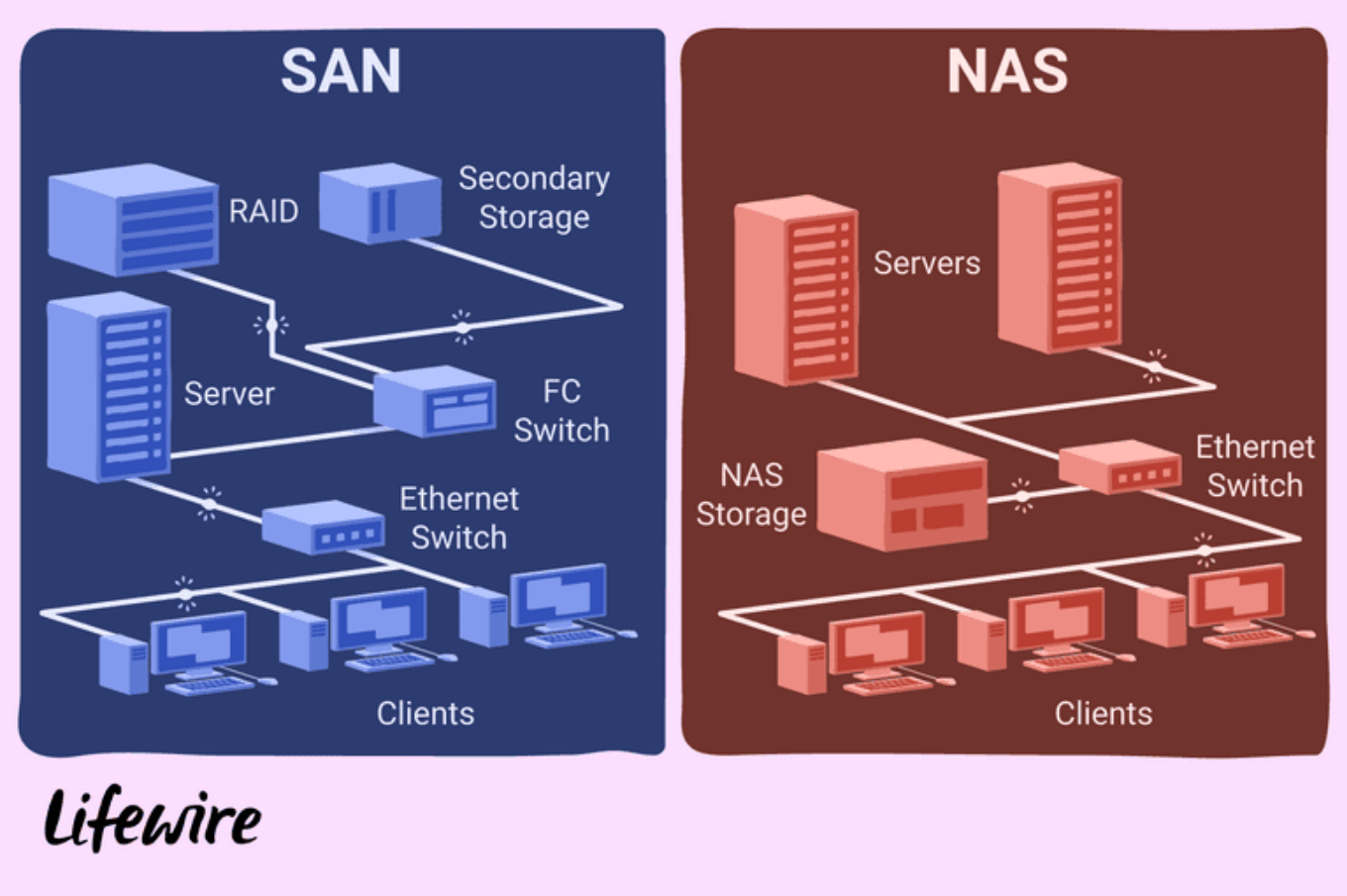
RAID 1+0 (10)

- **Disk mirroring with striping** - combines both RAID level 0 and 1 for performance and redundancy; a strip of two mirrored arrays.

- **The most common RAID styles includes 0, 1, 5 and 10.**
- **RAID 1 and RAID 0 requires at least 2 drives.**
- **RAID 5 requires 3 or more drives and RAID 10 requires 4 drives.**

NAS and SAN

Storage area networks and network-attached storage both provide networked storage solutions. A NAS is a single storage device that operates on data files, while a SAN is a local network of several devices.



Network Attached Storage (NAS)

- Runs over a standard network
- Shows up as normal shares on network
- Good for small environments
- **File-level**

Storage Area Networks (SAN)

- **SAN runs on block-level storage**
- Fibre Channel (FC) or iSCSI
- Expensive implementation

Physical Hardening

Policies can control how system hardware acts or reacts to an action.

- Removable media controls
- **Data Execution Prevention (DEP)** DEP is refer to Windows, in generic term is *Executable space protection*; DEP is almost always on by default on Windows.

🛑 DEP should be always be on, quietly protecting systems from buffer overflows. **The need to turn off DEP is rare**.

- Disabling Ports (can be done in the BIOS); Turn off legacy non-active ports to avoid vulnerable entry point.

RFI and EMI

Electromagnetic Interference (EMI)

Is a disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction.

- Shielded twisted pair (STP) cable.
- Creating a distance between the device generating the EMI, or shield the emanating device or media.

Radio Frequency Interference (RFI)

RFI is EMI that transmits in the **radio frequency** range. (i.e. 802.11, cellular WAN radio bands)...

- Both 802.11 and cellular WANs almost always have automatic channel-hopping features that automatically tune devices to the least congested channel.

Electrostatic discharge (ESD)

Discharge of an electrical current through the air, arcing from a point of a relative positive charge to a point of a relative negative charge.

- Protect equipment by shielding it in protective cases
- Only use properly grounded power supplies
- Anti-ESD wrist strap

Host Hardening

- **Disabling Unecessary Services** - i.e. SSH server, Apache server...
- **Default Passwords** - Simply avoid default passwords and use good password methodologies.
- **Disabling Unecessary Accounts** - i.e. Windows default guest account, Duplicate accounts...
- **Patch Management**
    1. Monitoring patches
        - Might not get reminders
    2. Testing the patches on Sandbox
    3. Evaluating
    4. Deploying the patch
        - Scheduling
    5. Document what is patched

Anti-Malware

- Training for users
- Procedures
    - Best practices
- Monitoring
- IDS
- Third-party anti-malware tools

Host Firewalls

- **Whitelist**
    - Defines all the applications a user is allowed to install
- **Blacklist**
    - Blocked programs

Data & System Security

- Data integrity
- Speed/performance quick access
- High availability

Solutions to secure data:

RAID

- Provides Good integrity
- Provides Good speed
- Affordable

Clustering - Distributive allocation

The primary rationale for server clusters is protection against outages and downtime. There are three main reasons for server clustering. They are availability, scalability, and reliability. The key to a protected IT infrastructure lies in redundancy.

- Good method to protect not only Data, but system resources
- Clustering is Expensive

Load Balancing

Refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.

- Distributes work loads across multiple machines

Virtualize the serves

- Scalability
- High-availability comes from elasticity
- Snapshots
- Affordable

Disk Encryption

Usage:

- Mobile and Portable devices
    - Laptops, smartphones, tablets
- Desktop Systems with limited security

TPM - Trusted Platform Module

Microchip built into a computer hardware that is used to store cryptographic information(public/private key). *(i.e **BitLocker** 1.2+)*; The OS relies on this **hardware of root trust** to check for low-level changes at boot up.

examples of disk encryption TPM and non-TPM:

- BitLocker (for Windows - TPM)
- PGP Disk (non-TPM)
- TrueCrypt (non-TPM)
- FileVault (for macOS - non-TPM)

🛑 **BitLocker is a built-in Windows Utility Drive Encryption Tool; must have a recovery key to access the data.**

Secure Boot - TPM

During the boot process, the TPM and UEFI generate reports about the process and can send those reports to a remote system, like a central authentication server. This process is called **remote authentication** / remote attestation.

Hardware / Firmware Security

- **Full Disk Encryption (FDE)**

    - i.e. Windows - BitLocker

- **Self-encrypting Drive (SED)**

Hardware Security Module (HSM)

Is any type of hardware that's designed to do security work. For ATMs, Web Servers, or other applications that perform an unusually high amount of key handling, it's usually a good idea to offload this work to other hardware.

Secure OS Types

- **Server OS** [RedHat Server, Windows Server etc]
- Built-in functionality
- Connections
- **Workstation** [Linux Ubuntu, Windows 10 etc]
    - Desktop version
    - Workhorse
- **Embedded Systems** [Routers, CCTVs etc]
    - Appliance
    - Their own OS
- **Kiosk** [i.e. Big Touch Screens on Museums, Mall etc]
    - Limited function
- **Mobile OS**
    - Apple iOS
    - Android OS

🛑 *Picking an OS based on least functionality is a good security practice.*

Secure Peripherals

- Keyboards, USB flash drivers, printers, monitors and so on.
- Patch!
- Disable unecessary ports
- Avoid backdoors

Bluetooth Security

Bluejacking - When bad actors connects with any Device that have Bluetooth enable by default.

Bluesnarfing - When the attacker steals data from the target device by connecting to an unsuspecting user's device.

Types of bluetooth:

- Class1 is 328' foot
- Class2 is 33' foot
- Class3 is 3' foot

🛑 *Most Mobile phones and Bluetooth headsets are class2 - range upto 33'*

802.11

Many peripherals can connect to an 802.11 network as a host. Printers and multifunction devices (MFDs) are very commonly connected with 802.11.

Malwares

Viruses do things to files and propagates, Malware collect keystrokes and information

Virus

- Piece of malicious software
- Attach to other files
- Propagate
- Spread to other devices
- Active

Adware

- Web-centric
- Programs that pop-up unecessary advertisment

Spyware

- Hide from system
- Tracking your web brownsing
- Stealing cookies

Trojans

- Standalone programs that must be installed **disguised** in programs
- Deliver payload without users knowledge
- Backdoor access

RAT - Remote Access Trojan

- Mimic the behavior of legitimate remote control
- Can hide in common 'inofensive' programs like games
- Backdoor access

Ransomware - Crypto-Malware

- Uses some form of encryption to lock a user out of a system.
- Usually encrypting the boot drive
- Then forces the user to pay money to get the system decrypted
- Can devastate systems

Logic Bomb

- Are triggered by an event *(i.e. erasing file shares or disk storage at a certain time or date)*
- Can devastate systems

Rootkit

- Piece of software that escalates privileges to execute other things on computer
- Hard to detect

Backdoor

- Piece of software that work on obfuscating an remote access.

Polymorphic Malware

- Changes his own code to confuse the digital signature of anti-malware programs
- Hard to detect and destroy

Armored Virus

- Design to make harder the detection by anti-malware programs.
- Hard to detect and destroy

Keylogger

- Record keystrokes
- Inject scripts

Analyzing Output

Anti-Malware

- Almost all anti-malware tools include a point scanner and a mass storage scanner.

Host-based Firewall

- Inbound rules / outbound rules
- All host based firewalls are basically they exclude everybody, so it is called an **implicity deny** *(not programs gets in or out)*
- The output is really an Access Control List
- Use of Least privilege and whitelisting

🛑 **False positive** - scan results identify a file that may not actually harm a system or is allowed on the system. (i.e. you just downloaded the Cain & Abel to crack some passwords on your assessment, probably Windows Defender will try to block it out).

File Integrity Check

Verify the integrity of file is in good order and ready to run.

Basically to check if the file isn't:

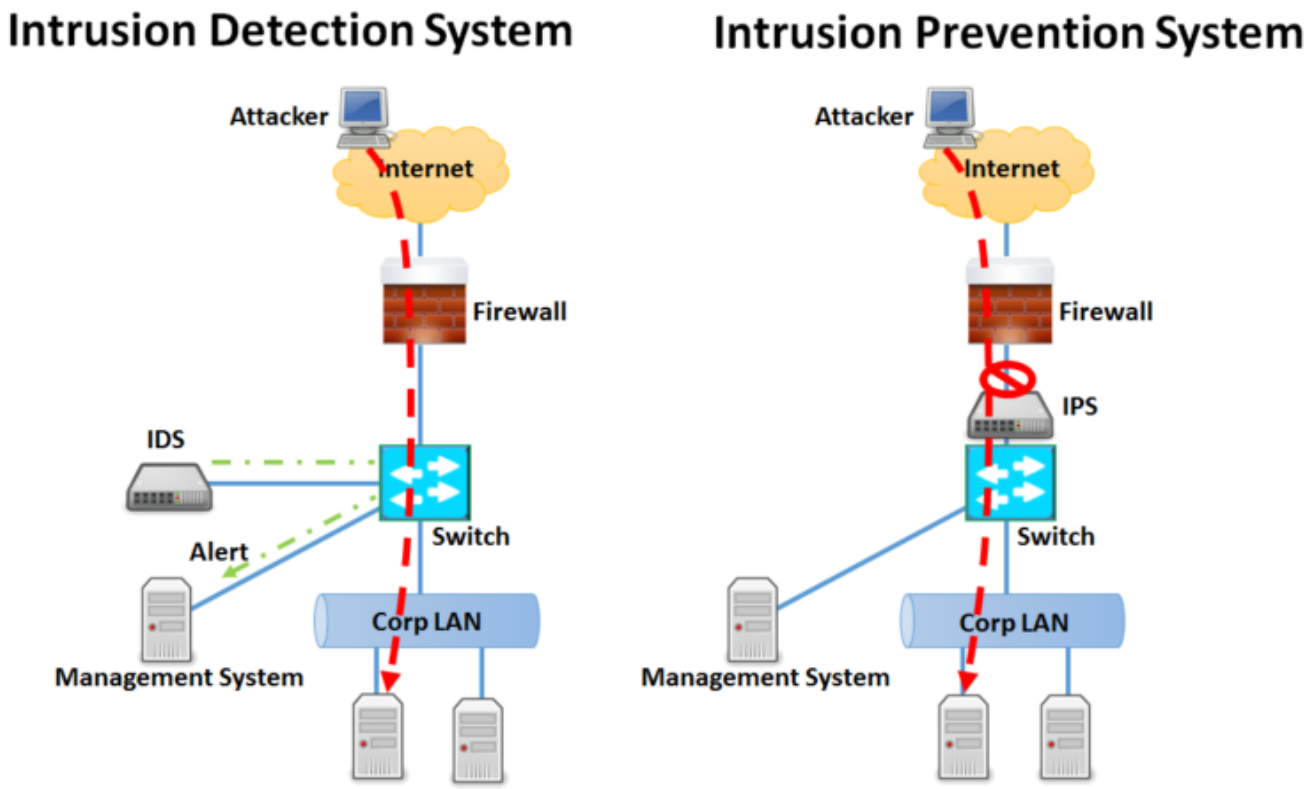
- corrupted
- tampered
- version and date

🛑 *To create a file integrity check, you can Generate a hash from source code - checksum. If somebody tamper the file or change from source code, the output hash will be different.*

Application Whitelisting

Everything about software management, application whitelisting, the main job - it's to make sure that users are running the right applications on each individual systems.

IDS and IPS



Intrusion Detection Systems (IDS)

- Lives inside the Network
- Watches within the network traffic
- Sends alerts on suspicious activity

Intrusion Prevention System (IPS)

- Active IDS
- IPS is usually close to the edge the network
- Action to prevent will occur at the IPS device

🛑 **IDS: notifies | IPS: acts to stop | Firewall: filters**

Automation Strategies

Automation is often used with various scans and updates based on configurable trigger.

- Repetitive
- Consistent
- Template restoration
- Continuous monitoring network devices (i.e. SNMP)
- Automatic update from OS
- Monitoring host for application whitelists
- Application Development - continuous integration tools like fuzzing, static testing
- Built-in tools vs Shell Scripting to Automate (Powershell(Windows) , Bash(Linux) ..)

Media Sanitization | Data Destruction

Clearing/Clear

Clear means to tell the device through user commands inherent to the massa storage device to sanitize the data. *(i.e. send commands to a hard drive to erase data)*

🛑 Can be done with commands such as erase, format and delete (these methods are not final)

Purge

Purging will process the device to remove data from the drive, the device might will no longer be usable. Means to use anything other than an internal command to sanitize the data on the media. *(i.e. Degausser: machine with a strong magnetic field that destroys/purge the data from massa storage devices)*

purge also means that the device is basically not useful anymore

Crypto Erase

In case you lost the keys to encrypted device.

Destroy / Data Destruction

Ruin the media in such a way tha it is no longer functional.

- Mass storage device
- Tape media
- Floppy disks
- Paper

Methods:

- Burning
- Pulping
- Shredding
- Pulverizing

---

2. Tools

OS Utilities - Command Line (Linux & Windows)

ping

can be handful for DNS checks (up / or down) | is a DNS tool to resolves web addresses to an IP address.

```
ping www.google.com

PING www.google.com (172.217.168.164): 56 data bytes
64 bytes from 172.217.168.164: icmp_seq=0 ttl=55 time=25.981 ms
64 bytes from 172.217.168.164: icmp_seq=1 ttl=55 time=25.236 ms
--- www.google.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 25.236/25.608/25.981/0.373 ms
```

🛑 In Windows you need to add a **-t** flag to keep running.

Most useful switches for Ping command - Windows:

Switch	Description
-a	Resolve address to hostnames
-f	Set don't fragment flag in packet (IPv4 only)
-4	Force using IPv4
-6	Force using IPv4

netstat

get info on host system TCP / UDP connections and status of all open and listening ports and routing table.

- Who you talking to?
- Who trying talking to you?

```
netstat -a (server)
netstat -n (host)
```

tracert | traceroute

traceroute - how packets get from host to another endpoint. Traceroute is helpful to see what routers are being hit, both internal and external.

- tracert - Windows
- traceroute - Linux

arp

address resolution protocol - caches of ip-to-ethernet

ipconfig (Windows)

show all IP configuration on Windows-only systems.

Useful switches:

Switch	Description
/all	Exhaustive listing of virtually every IP and Ethernet setting (MAC address etc)
/release	Release the DHCP IP address lease
/renew	Renews the DHCP IP address lease
/flushdns	Clears the host's DNS cache
/displaydns	Displays the host's DNS cache

ifconfig

equivalent to ipconfig for UNIX/Linux OS.

iwconfig

similar to ifconfig, but is dedicated to the wireless network interface.

ip addr

show / manipulate routing, network devices, interfaces and tunnels.

Show all the ip configuration, mac address, ipv6 etc.

nslookup

query Internet name servers interactively; check if the DNS server is working

```
nslookup www.certifiedhacker.com

output:
```

```
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Name:   certifiedhacker.com
Address: 162.241.216.11 inslookup www.certifiedhacker.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Name:   certifiedhacker.com
Address: 162.241.216.11
```

dig

DNS lookup tool - Functions like nslookup, but allows for further functionality.

```
dig www.certifiedhacker.com

output:
; <<>> DiG 9.11.14-3-Debian <<>> certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15708
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 2048
; COOKIE: 70bd915b07b3fd08757c9ad65e5d6f3e549d5787b59e97cb (good)
;; QUESTION SECTION:
;certifiedhacker.com.           IN      A

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A       162.241.216.11

;; Query time: 419 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Mar 02 15:40:29 EST 2020
;; MSG SIZE  rcvd: 92
```

netcat

TCP/IP swiss army knife; you can make any type of connection and see the results from a command line. With nc you can connect to anything on any port number or you can make your system listen on a port number. Can be an agressive tool for recon.

Network Scanners

Useful for collect and inventory the hosts on a network, and is useful for reconnaissance of your system.

Nmap

The Best way to query a system to check if they have open ports, services, system versions, service versions etc.

Zenmap is a GUI version of Nmap.

```
nmap -v -A -T5 scanme.nmap.org

...
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 156515DA3C0F7DC6B2493BD5CE43F795
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
...
```

Angry IP Scanner (GUI) - for Windows

Does a good job using simple protocols, mainly ping, to query a single IP address or an address range.

Protocol Analyzers

Protocol Analyzers collect and inventory the network traffic.

Sniffer - Some type of software that grab all the data that is going in and out of particular interface.

Why Protocol Analyze?

- Count all the packets coming through over a certain time period to get a strong ideas to your network utilization.
- Inspect packets for single protocols to verify they are working properly.
- Monitor communication between client and a server to look for problems.

- Look for servers that aren't authorized on the network.
- Find systems broadcasting bad data.
- Find problems in authentication by watching each step of the process.

Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level.

With Wirehsark you can inspect and detect ARP poisonings, Rogue DHCP servers, Broadcast Storm etc.

🛑 Broadcast Storm - when a NIC (or port on a switch) sends large amounts of broadcast traffic, thereby crippling network resources.

tcpdump

Another popular protocol analyzer option for UNIX/Linux.

SNMP - Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

- SNMP v1 - does not support encryption
- SNMP v2 - added basic encryption
- SNMP v3 - added TLS encryption

SNMP uses Port 161

Logging

There are two types of events (Network and Non-network events).

Non-Network Logs

- Operation System Events
    - Host starting
    - Host shutdown
    - Reboot
    - Service starting, stopping, and failling
    - OS Updates
- Applications Events
    - Application Installation
    - Application starts, stops or crashes
- Security Events

    - Logons
    - Logons successes and failures

Generic Log Structure:

- Date and Time
- Process/Source/ID
- Account associated/System
- Event Number
- Event Description
- Network Logs

Network Events

- O.S. / System-Level
    - Remote logon fail/not
    - Events on Shared Applicaton/Resources
        - Activity on Web Server (i.e. Apache)
        - Activity on Firewall
- Application-Level

Centralized vs Descentralized Log Management

Descentralized log management - In environments such as very small networks and don't have large infrastructure or in isolated network segments, descentralized log management is usually the norm.

Centralized log management - means that the log files from different machines are automatically sent to a centralized logging facility or server, such as a syslog server, administrators review logs from a centralized loogging facility on the network. Enterprise correlate them into one unifed management interface, so the administrator can look for trends or events.

Centralized

- Uses a Central repository
    - Drag on system
- Use SNMP Systems
    - Pulls informaton needed and generates graphs and charts

🛑 Monitoring-as-a-Services (MaaS)

SIEM - Security Information and Event Management

Collects data points from network, including **log files, traffic captures, SNMP messages, and so on**, from every host on the network. **SIEM can collect all this data into one centralized location and correlate it for analysis to look for security and performance issues, as well negative trends all in real time.**

Continuos Monitoring

Is a proactive way of ensuring that the network administrator receives all the different logs and other data points throughout the network from all network devices and all systems, on a constant basis. This data is continually fed into.

Auditing

Important part of ensuring accountability on the network. Examines the logs and other data points of certain events and construct a time frame and event sequence surrounding an incident.

Auditing also consists of other activities, such as:

- Performing Network Sniffing traffic analysis
- Password Cracking
- Vulnerability Assessment
- Penetration Test
- Compliance Audits

Auditing can reveal weak security configurations

Trend Analysis

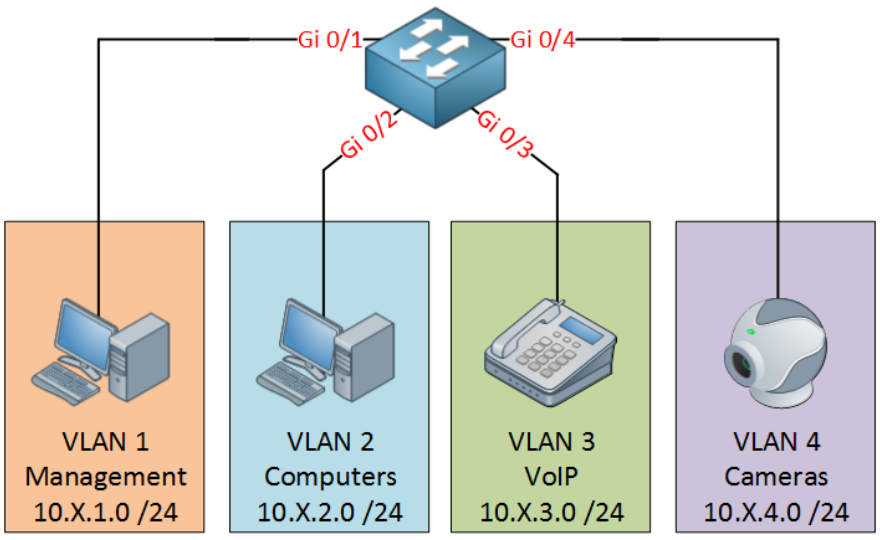
Enables network administrator to correlate different data sources and data points from various places in the network, such as log files, IDS logs, wireless and wired sniffing as well as other event sources, and seek to identify on-going trends in both performance and security. The goal is find patterns that can indicate a emerging issue.

---

3) Networks and Infrastructure - Basics

Switches

A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses **MAC addresses** to forward data at the **data link layer of the OSI model.**

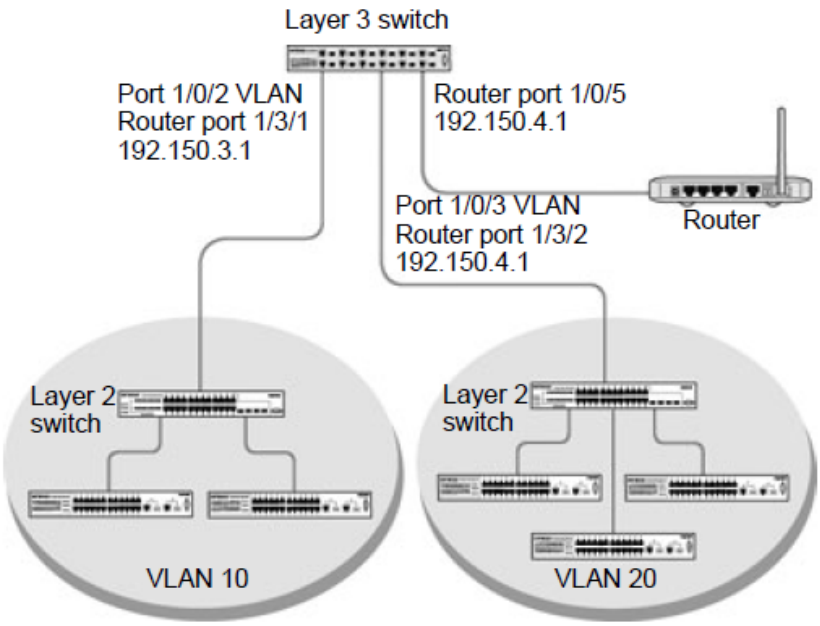


- Filter & forward data based on **MAC address**
- Where VLANs are set up
- **STP (Spanning Tree Protocol)** prevents bridge loop / loop floods

🛑 **Bridge Loop/Switching Loop** - A switching loop or bridge loop occurs in computer networks when there is more than one Layer 2 path between two endpoints. The loop creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port, the switch or switches will repeatedly rebroadcast the broadcast messages flooding the network.

VLANs

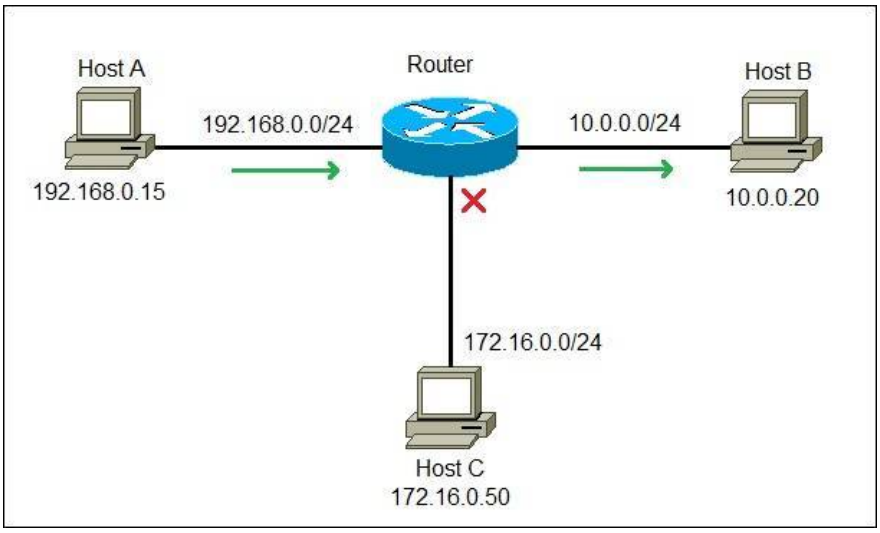
A virtual LAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.



- Provides layer 2 separation of networks
- **Flood guarding**
  - **STP (Spanning Tree Protocol) - enable**

Routers

Router is a networking device which helps in routing the data packets between home network & other networks.



- Filter & forward based on **IP address**
- Allocates IP addresses to the devices connected to it using a DHCP server.
- It performs NAT (Network Address Translation)

🛑 *Generally operates in the Network layer*

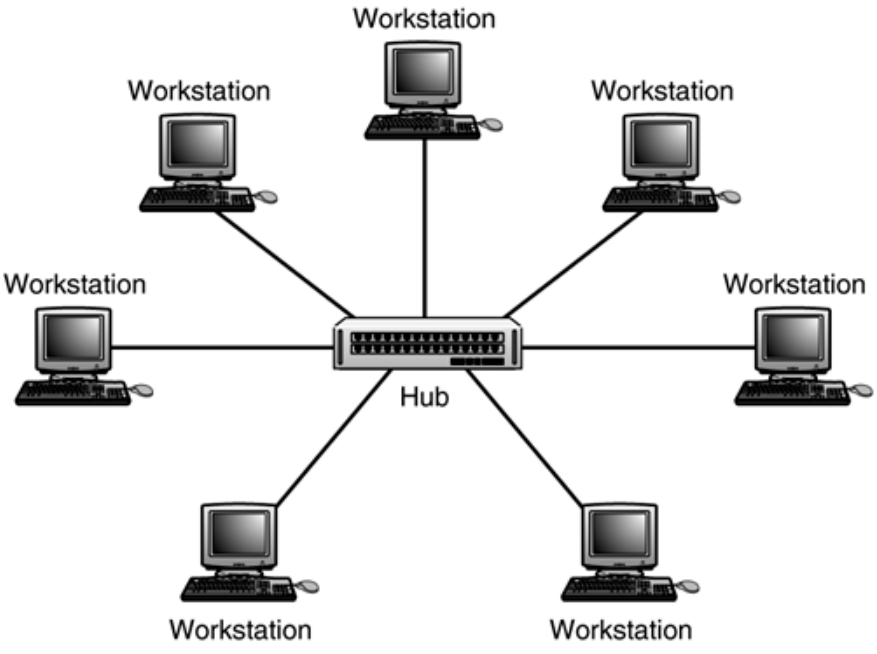
🛑 A firewall is a piece of software that is commonly run on a gateway router which protects us from the evils of the Internet, so it can forward and filter based on port numbers, based on IP addresses, URL's, all kinds of different stuff. **So we would call this a network firewall because the gateway is running the firewall software** and protecting us from the evil of the Internet.

Network Topologies - Basics

The actual organization of a network in terms of how is the data moving around and the best way to do it.

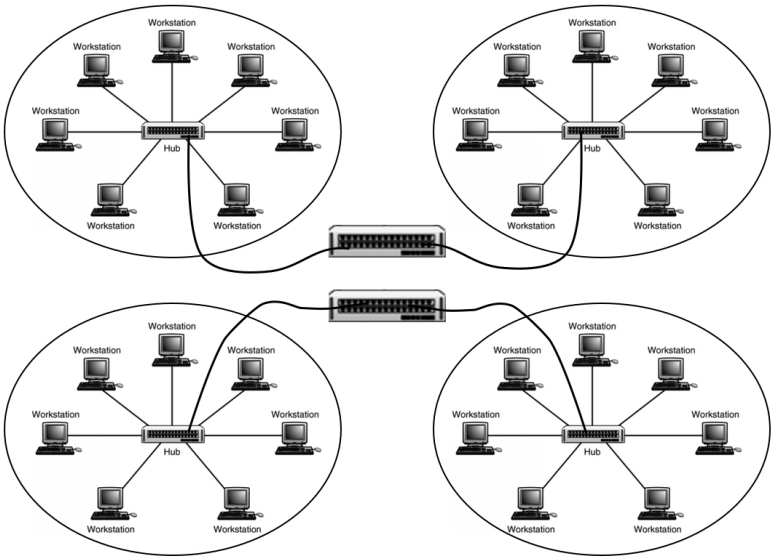
LAN - Local Area Network

- A LAN is a network that has a logical and physical borders that a computer can broadcast

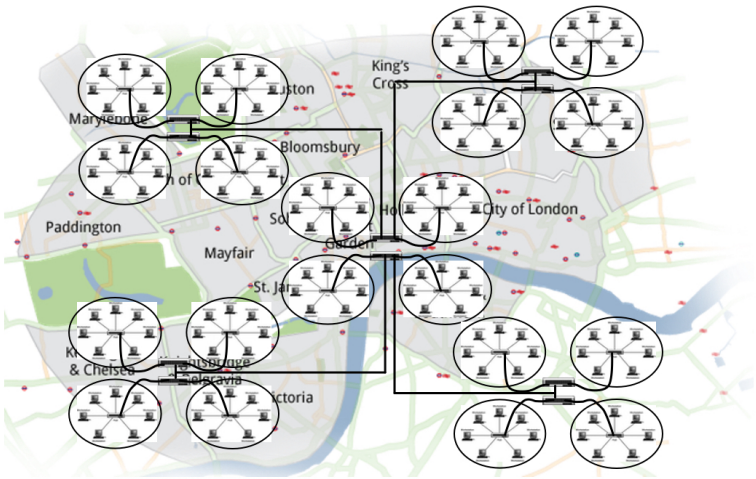


WAN - Wide Area Network

- WAN is a multiple LANs or additional WANs with routing functionality for interconnectivity.



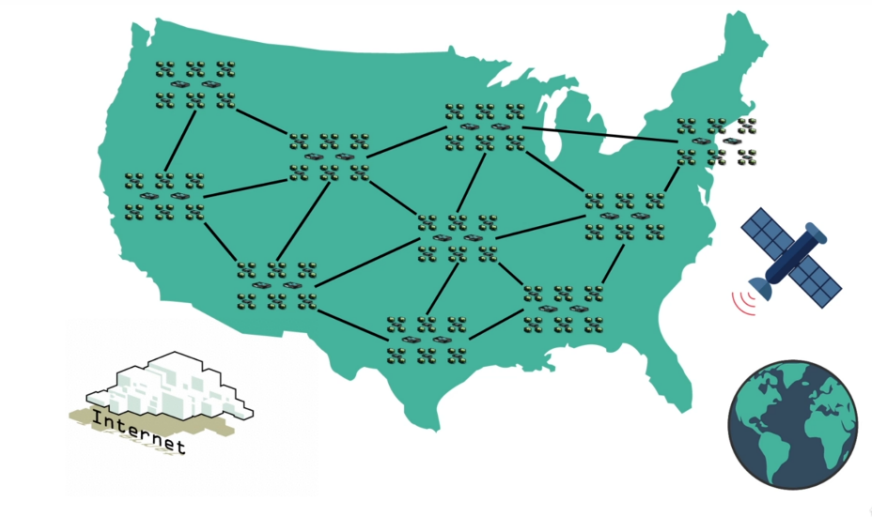
MAN - Metropolitan Area Network



Internet

Connecting WANs through WANs until complete the entire world = Internet.

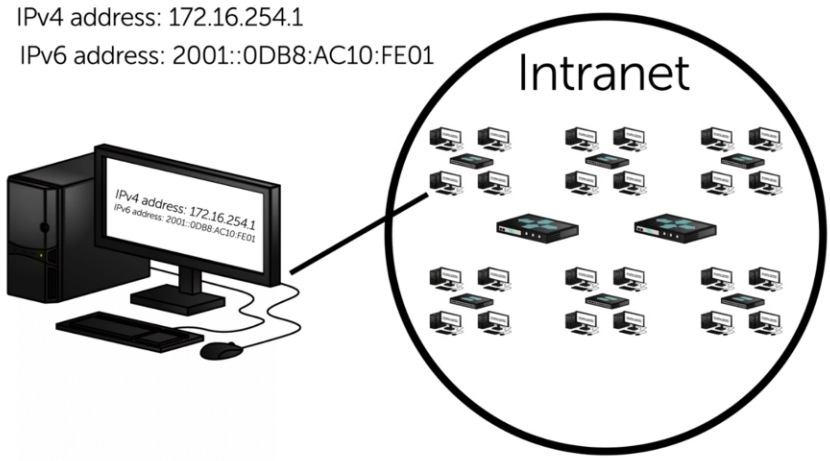
- The protocol which runs the internet is TCP/IP
- As long you're using legitimate IPv4 address or IPv6



Intranet

If you're using the TCP/IP stack and making your own LAN or WAN = Intranet.

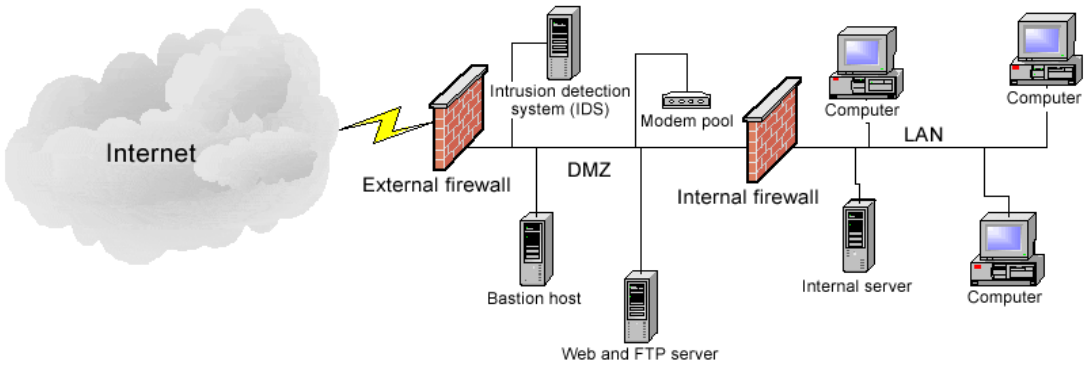
- Intranet is a private network which still runs TCP/IP



🛑 **Extranet**: example of some vendor who need to access the Intranet network.

Network Zones - Concepts

- **LAN** - the core of your network.
- **VLAN** - physical device that designate separate broadcast domains....
- **DMZ** - Demilitarized Zone: Perimeter network, isolating untrusted network from LAN area. DMZ is a firewall configuration used to secure hosts on a network segment, in most DMZs the hosts on the DMZ are connected behind a Firewall that is connected to a public network(internet).



- **Wireless Network** - Basically a LAN connected to an Wireless Access Point (WAP).
- **Guest Network** - i.e. Coffee Shop network.
- **Virtualization**
- **Airgap** - Simply means a disconnect to provide real isolation and the use of a completely separate internet from the world; Private internet.

Network Access Controls

- Wireless Network
- Remote Access
- VPN Access

PPP - Point-to-Point Protocol

In computer networking, Point-to-Point Protocol (PPP) is a data link layer (layer 2) communications protocol between two routers directly without any host or any other networking in between. It can provide connection authentication, transmission encryption, and compression.

- Transport layer protocol
    - Initiate connection
    - Get address information
    - Make connection
- Poor authentication mechanisms:
    - PAP - password authentical protocol (passwords in the clear)
    - CHAP - Challenge handshake authentication protocol - (use of hashing)

EAP - Extensible Authentication Protocol

Developed initially as an extension to the authentication part of PPP. EAP is only an extension for the protocol that having a connection, and was created as a better authentication method to PPP.

- **EAP - MD5**
    - basically MSCHAP
    - Takes those passwords and hashes them into MD5 hash

- **EAP - PSK**
    - Uses pre-determined symmetric keys
    - Similar to WPA and WPA-2
- **EAP - TLS**
    - Cand handle an entire TLS
    - Needs server and client certificates
- **EAP - TTLS**
    - Uses the TLS exchange method
    - Only requires server certificates

Protocols that Encapsulates the EAP

- **802.1X** - Full blown authentication standard that allows us to make connections between some type of client system. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
- *Early EAP adaptations*:
    - **LEAP** (Cisco) - LEAP is weak nowdays
    - **PEAP** (Microsoft) - PEAP is weak nowdays

Network Firewalls - Concepts

Stateful Firewall

Can watch traffic streams from end to end. They are aware of communications paths; Can implement varios IPSec functions (tunnels and encryption); Can tell what stage a TCP connection is in (open, open sent, synchronized SYN ACK or established).

- Are better at identifying unauthorized and forged communications.

Stateless Firewall

They watch network traffic and restrict / block packets based on source and destination address or static values **(ACL Rules)**.

- Typically faster and perform better under havier traffic loads.

Packet-filtering

- Inspect data packets (drop or forward), such as the destination and originiation IP address, packet type, port number and other surface-level information.

Circuit-level firewall

- Quickly approve or deny traffic; verify transmission protocol (TCP) handshake (session).

Application-level Firewall

- Filter traffic based on user group, group membership, application or services (works at layer 7 OSI - also called proxy firewall as well)

Proxy Servers

A box/piece of software running on a computer acts an intermediary between two different devices having a session.

- Application-specific
  - Web proxy
  - FTP proxy
  - VOIP proxy

Forward Proxy - Client

The proxy simply forward the requests of respective client.

- [Client -> **Proxy** -> Firewall -> Internet -> Server]
- **Hides the client**
- Provides:
  - Caching
  - Content filtering
  - Acts similar to firewall (block based on URL, content filtering and so on).

Reverse Proxy - Server

Like a forward but complete reverse.

- [Client <- Internet <- Firewall <- **Proxy** <- Server]
- **Hides the servers**
- Provides
  - High security
  - Protect the servers
  - Handle DoS attacks
  - Load balancing
  - Caching
  - Encryption acceleration

Honeypots

Emulate a web server, vulnerable machine purposely to attack; Inviting target to keep away from targets.

- Benefit to see how threat actors, what techniques they're using, what vulnerabilities are they look for, what ports, and so on.
- Log all information (port information and the origin IP address)

- Usually located in the DMZ to get close to the source but still isolated to capture the traffic.

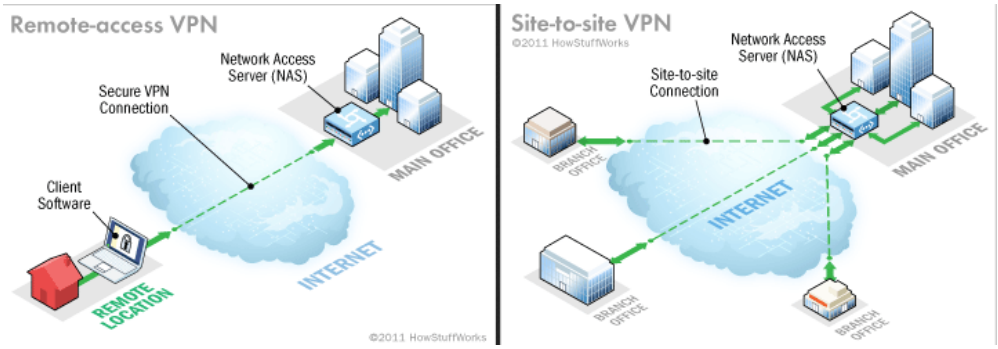
Honeynet

A honeynet is a vulnerable and **simulated computer network** using a decoy server. **By design, honeynets are not authorized for any authentic uses. If a honeynet is accessed, a fair assumption is that the person accessing it is a bad actor.**

VPN - Virtual Private Networks

Organizations use virtual private networks (VPNs) to create an end-to-end private network connection (tunnel) over third-party networks such as the Internet or extranets. The tunnel eliminates the distance barrier and enables remote users to access central site network resources. The **IP Security (IPsec) protocol** provides a framework for configuring secure VPNs and is commonly deployed over the Internet to connect branch offices, remote employees, and business partners. Secure site-to-site VPNs, between central and remote sites, can be implemented using the IPsec protocol. IPsec can also be used in remote-access tunnels for telecommuter access.

The two types of VPN - **Remote Access** and **Site-to-Site**



- A **remote-access** VPN is created when VPN information is not statically set up, but instead allows for dynamically changing information and can be enabled and disabled. Consider a telecommuter who needs VPN access to corporate data over the Internet. The telecommuter does not necessarily have the VPN connection set up at all times. The telecommuter's PC is responsible for establishing the VPN, each host typically has Cisco VPN client software.

- A **site-to-site** VPN is created when connection devices on both sides of the VPN connection are aware of the VPN configuration in advance.

VPN Setup Steps

1. Protocol to set up tunnel
2. Protocol to handle authentication and encryption

Early VPNs Protocols

- **PPTP** - Point-to-Point tunneling Protocol
    - Oldest VPN protocol
    - Uses PPP for tunnel
    - Password only

    - **TCP port 1723**
    - Weak encryption

- **L2TP** - Layer 2 Tunneling Protocol
    - Cisco proprietary
    - SImilar to PPTP
    - L2TP tunnel
    - IPsec encryption
    - **UDP ports 500, 1701, 4500**
    -

- 'Pure' **IPsec**
    - uses IPsec for tunneling and encryption
    - Great for IPv6
    - **UDP ports 500, 4500**

- **SSL** and **TLS**
    - **TCP port 443**
    - Often works within a web browser
    - TUN/TAP (virtual network driver) tunnel
    - TLS encryption

- **OpenVPN**
    - Unique tunnel
    - Encryption based on SSL/TLS protocol
    - **TCP port 1194**, but can be changed

IPSec - IP Security

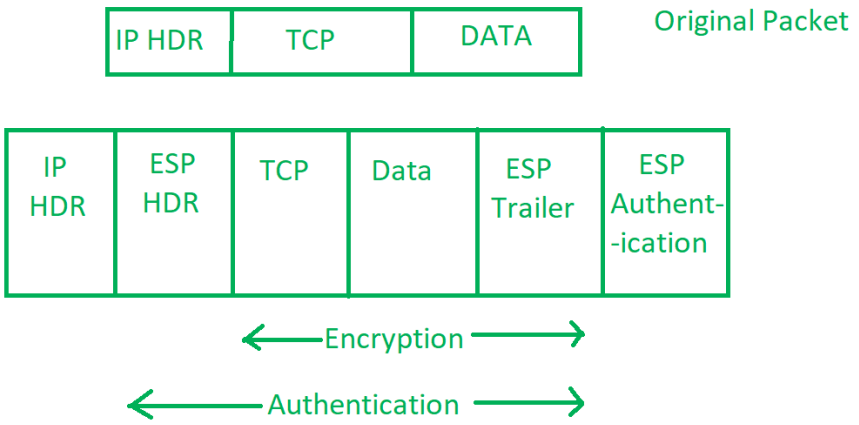
Is a suite of protocols developed to ensure the integrity, confidentiality and authentication of data communications over an IP network.

🛑 IPSec works at the IP layer

IPSec Components

1. **Encapsulating Security Payload (ESP)** – It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH)** – It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

3. **Internet Key Exchange (IKE)** – It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. **The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange.** ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.



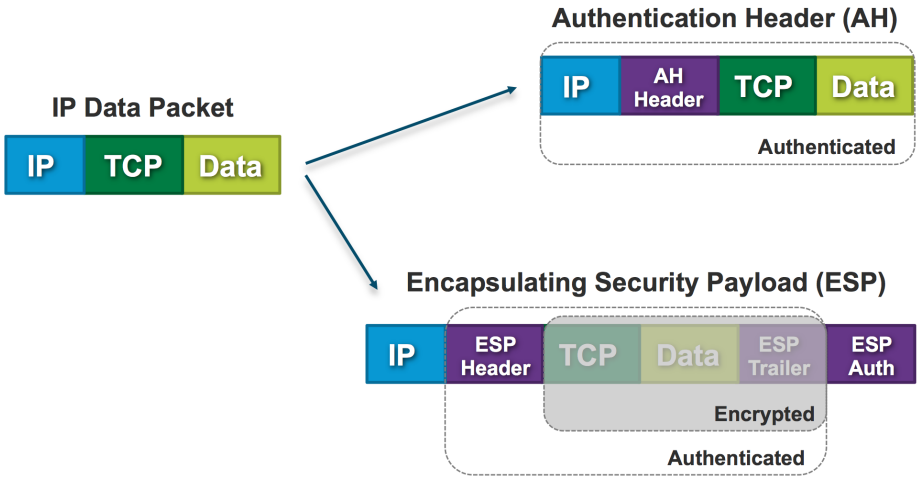
Tunnel Mode and Transport Mode

When IPsec protects traffic, it has a couple of services and modes to choose from.

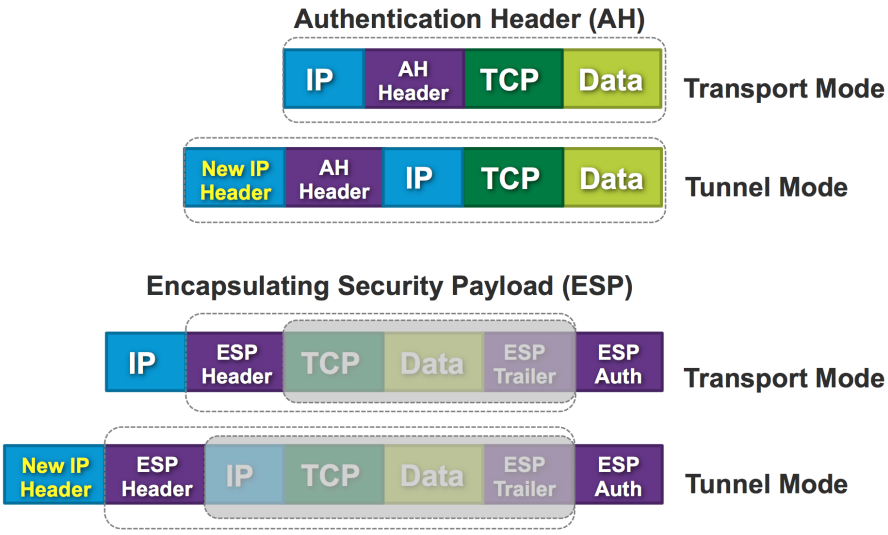
Transport mode - preserving original IP header. Typically used in combination with GRE or other encapsulating protocols. (Host-to-Host)

Tunnel mode - encapsulating entire IP datagram within a new header, essentially tunneling the packet. (The gateway creates the tunnel)

1. *Some TCP data will be sent over:*



2. *And now about how those IP protocols fit in the two modes.*



The last mode is what is typically used with crypto map based IPsec VPNs.

Use of IPSec

- **VPNs**
  - Pure IPsec (using tunneling mode)
  - IPSec with L2TP (add a tunnel layer)
- **RADIUS and TACACS+**
- **IPSec with IPv6**
- **Using IPSec with Non-security protocols / Encrypting Unsecured Protocols**
  - i.e. IPsec over Telnet

NIDS and NIPS

Network Intrusion Detection Systems (NIDs) and **Network Intrusion Prevention Systems (NIPS)** look at attacks coming into the network at large instead of into a host. Attacks could be in the form of malformed network traffic or excessive amounts of traffic.

Prevention vs Detection

NIDS is a **passive** device and focuses on detection alone, making it a **detection control**. It detects network traffic issues and alerts and administrator to these issues, also logging the events in the process.

NIPS is /**inline**(Active) device and focuses not only on detecting network attacks, but preventing them. (block things from router)

Detection

NIDS/NIPS solutions act very much like firewalls in that they inspect packets.

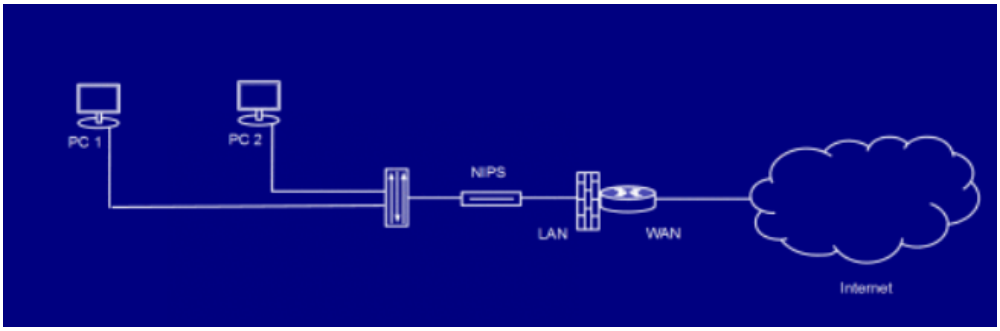
There's 4 types of detection methods:

- **Behavioral/Anomaly** - Comparing traffic with a baseline of patterns considered normal for the network
- **Signature** - Preconfigured Signature-based
- **Rule** - Preconfigured rules in a ruleset - like firewall
- **Heuristic - (Anomaly and Signature)**

Sensors: In-band & Out-of-Band

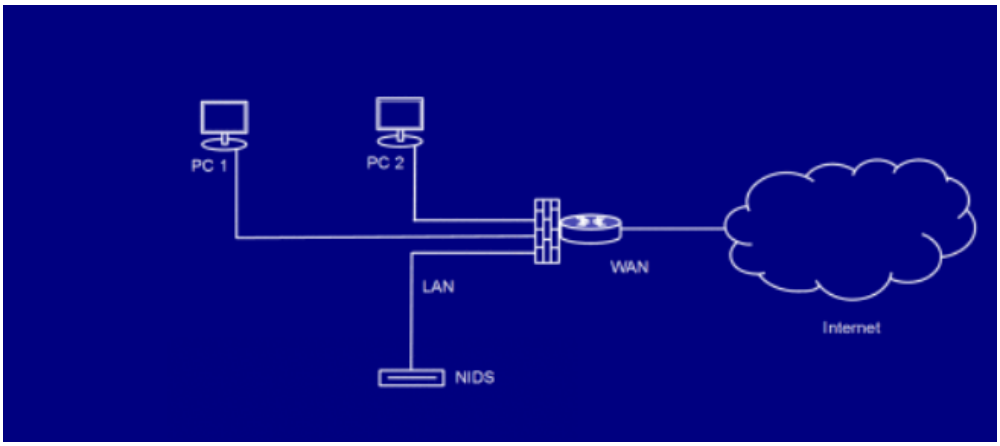
NIPS

- NIPS sensor must be installed **in-band** to your network traffic



NIDS

- NIDS sensor, being **passive**, is normally installed **out-of-band**



Devices

Network Tap

Is a device that you can insert anywhere along a run to grab packets.

Port Mirror

Also called a Switch Port Analyzer, or SPAN in Cisco Devices, is a special port on a managed switch configured to listen for all data going in and out of the switch. Unlike a network tap, port mirroing is convenient and easily changed to reflect any changes in your NIDS/NIPS monitoring stragegy.

SIEM - Security Information and Event Management

SIEM tools aggregate and correlate data, allowing you to organize it into valuable information. You can get to the time sequence of an event in all the logs quickly, have alerts and the ability to notify you based on a configurable trigger.

- **Aggregation** - Collecting data from disparate sources and organizing the data into a single format. Any device within a SIEM system that collects data is called collector or an aggregator.
- **Correlation** - is the logic that looks at data from disparate sources and can make determinations about events taking place on your network. (could be in-band or out-of-band, depending on the placement of the NIDS/NIPS)
    - Alerts - for notification if something goes bad
    - Triggering - Exceeding thresholds
- **Normalization** - will actually create multiple tables / organize in such a way that the data can become more efficient and allows our analysis and reports tools to work better.
- **WORM - Write Once Read Many**: The concept being is that log files are precious, and a lot of times you might want to look at them in an archival way, so that we can use optical media like WORM drives to store them.

Tools

- **Splunk**
- **ArcSight**
- **ELK - Elastic Search, Log Stash and Kibana (openSource)**

Network - Part 2, Beyond the Basics

802.11

IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands.

Table 1: IEEE 802.11 Standards

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s

Wireless Access Point (WAP) - Concepts

- Wireless Access Point is a Bridge between **802.11** and **Ethernet**.
- Every WAP have MAC address
- **SSID (Service Set identifier)** associated to the MAC address on a WAP is known as **BSSID - (Basic Service Set Identifier)**
- When a large network is connected multiple WAP's through a **Common Ethernet Broadcast Domain** - turns out **ESSID - (Extended Service Set Identifier)**

WEP - Wireless Equivalency Privacy

- 64/128 bit RC4 ICV

RC4 - Rivest Cipher 4 Stream Cipher Algorithm
ICV - Integrity Check Value

🛑 *Very old and insecure.*

WPA - Wi-Fi Protected Access

- Enterprise
    - TKIP + RADIUS
    - 64/128 bit RC4 MIC
- Personal
    - TKIP + PSK
    - 64/128 bit RC4 MIC

TKIP - Temporal Key Integrity Protocol
PSK - Pre-Shared key
MIC - Message Integrity Check

WPA2 - Wi-Fi Protected Access v2

- **802.11i** IEEE standard
- Enterprise
    - CCMP + RADIUS
    - 128 bit AES MIC
- Personal
    - CCMP + PSK
    - 128 bit AES MIC

CCMP - Cipher Block Chaining Message Code Protocol
AES - Advanced Encryption System

Vulnerabilities with Wireless Access Points

Rogue Access Point

Unauthorized access point plugged into a wired one. *(Can be accidental)*

Evil Twin Attack

Is a Rogue AP tha is broadcasting **the same (or very similar) SSID**.

802.11 Jammer

Jamming is a form of intentional interference on wireless networks, designed as a DoS attack. This type of attack by overpowering the signals of a legitimate wireless AP, typically using a rogue AP with its transmit power set to very high levels.

Deauthentication Attack

Deauthenticates clients from the network to grab the authentication information performing a man-in-the-middle attack.

Cracking WEP, WPA, WPA2 and WPS

WEP

- **IV Attack** - Initialization Vector is vulnerable to cracking.
    - Aircrack can grab WEP keys and crack them.
- WEP is the oldest security standard 802.11

WPA/WPA2

- WPA/WPA2 uses 4-way handshake
- WPA is vulnerable to a dictionary attack
- Can be cracked at the initial connection between the WPA/WPA2 client and the access point during the 4-way handshake
- Aircrack can grab WPA handshakes on authentication time and crack the PSK's (if they are common/weak).

WPS

Wi-Fi Protected Setup (WPS) - is a push button configuration, which enables the router WPS enable to another WPS device (wireless printers are the most common).

- 8 digit key is actually only 7 digits, 2^7
- Key exchange is the first processed in 4-bit and 3-bit
- Can be cracked using Reaver
- *The new generation of WPS enabled device can detect an attack and shut off.*
- **WPS Attack Prevention**:
    - Get rid of older routers
    - Firmware updates
    - Upgrade to newer wireless routers

Hardening 802.11 Networks

- Survey installation issues
- Maintaining existing wireless networks
- Monitoring
- Define how to defend wireless clients

Site Survey & Installation

- **Survey Tools**
    - Find SSIDs
    - Find MAC addresses
    - Band, channels, and signals
    - Document everything around 802.11 device
- **Maintanance Wireless Networks**
    - Good Documentation
        - SSIDs
        - MAC addresses associated to
            - WAPS
            - AP locations
            - Heatmaps
    - **Scanning**
- **WIDS** - Wireless Intrusion Detection System - *listen to what is going on inside the wireless network and help detect potential threats, or any abnormality.*
    - Monitors wireless radios
    - Watches for rogue access points
    - Knows MAC address of authorized equipment
    - Watches working protocols
- *Good Practice:*
    - AP isolation enabled
    - 802.1X is more robust

Fat vs. Thin Access Points

Thick Client

- Good for small environments
- Management console to configure security controls
- ACLs
- White/black listing
- Encryption
- Manage individually
- Also called controller-based AP

Thin Client

- Good for big environments. *(i.e A building with multiple floors and hundreds of users might rely on one good switch (with a redundant backup) to control dozens of thin access points)*
- Act as a repeater taking the wireless signal and pushing it ot a managed access control (AC) switch that handles encryption and other security. Also called **Standalone AP**

Antenna Types

Higher dB = better

- Omnidirecitonal Signals goes on every direction.
- Dipole
- Directional
    - Long individual beam
- Patch Graphic
    - Half Omni (i.e stick to the wall the get one side signals)

Antenna Placement Examples

Antennas should be centrally located throughout different areas of the facility so that hey can adequately span all areas of coverage within a facility, without being too close to exterior walls or the roof whenever possible.

- Stadium like = **Omnidirectional Antenna**
- Outdoors = **Dipole Antenna**
- Shooting long distances *(one building to another)* = **Directional Antenna**

Band Selection - 2.4 vs 5 GHz

The higher the frequency of a wireless signal, the shorter its range. **2.4 GHz wireless networks, therefore, cover a larger range than 5 GHz networks. In particular, signals of 5 GHz frequencies do not penetrate solid objects as well as 2.4 GHz signals, and this limits the reach of 5 GHz frequencies inside homes.**

2.4 GHz

- Longer range
- Penetrate walls easily

5 GHz

- Faster choice
- Automated channels
- Wider Channels = better

Virtualization - Concepts

- Virtual version of host hardware
- Multiple virtual servers on one box/physical device
- Hardware consolidation and reduced energy consumption
- System Recovery

Types

- **Type 2** - Runs on top of host OS
- **Type 1** - Runs directly on top of hardware, independent of host OS. *(i.e bootable Linux thumbdrive)*
- **Cloud-based Virtualization**
    - IaaS (i.e. AWS, MS Azure)

Virtualization Benefits

- Security Feature
- Patch management
- Centralized hardware maintenance
- Resilient and high availability
- Great for testing everything and sandboxing environment
- Snapshots and backups
- Network Separation

Virtual Threats

- VM sprawl - the out-of-control creation of VMs outside of security controls.
- VM escape - when a user inside a VM finds a way to break out the VM and get into the underlying hypervisor/host OS.

Virtualization Hardening

- Remove remnant data
- Make good policies
- Define user privileges
- Patch everything!
- CASB - Cloud Access Security Brokers: Intermediary between your infrastructure(in-house stuff) and the cloud; Make sure policies are controlled; watches for malware;

Containers

- Containers are self-contained applications that can communicate with network resources that have been explicity allowed
- Runs isolated instances of programs and services
- Can depend on each other, and can be configured to communicate with each other on a single host
- Runs a single program and all its dependencies, when the programs exists

IaaS - Infrastructure-as-a-Service

- Basically virtual machines hosted by a cloud provider's infrastructure; Users simply connect to them via RDP (remote desktop protocol) or another secure remote connection protocol and use the as they would any other computer.
    - *i.e: AWS, Microsoft Azure, Digital Ocean, Google Cloud.*

PaaS - Platform-as-a-Service

- Offers a computing platform, such as Web application server or database server with easy setup focusing on quick deployment; Enables you to access a software development platform without the need

to host it yourself.
    - *i.e: Heroku*

SaaS - Software-as-a-Service

- SaaS is a subscription based license; Access applications via subscription;
    - *i.e: Microsoft Office 365, Dropbox storage, Google Docs*

Cloud Deployment Models

- Private Cloud
    - A group of virtual machines that only the organization can access.
- Public Cloud
    - Amazon S3, Microsoft Azure - Open for business
- Community Cloud
    - Is make up of infrastructure from several different entitites wich may be cloud providers, business partners, and so on. (members only type of thing)
- Hybrid Cloud
    - Any combination of the cloud models described above
- Virtual Desktop Environment (VDE)
    - Remote Access to a Remote System that **is not virtualised**
- Virtual Desktop Integration (VDI)
    - The actual virtualized environment in the cloud

Static Hosts - Concepts

Intelligent device designed to do a specific task or process

- WAP
- Switch
- Router
- Printer
- **ICS** - Industrial Control Systems
    - HVAC - Heating Ventilation, and Air Conditioning
- **SCADA** - Supervisory Control and Data Acquisition
    - Pretty much ICS with more funcionality

Securing Static Hosts

- Change default passwords
- Turn off unnecessary services
- Monitoring security and firmware updates
- **Defense in depth**
    - Network Segmentation - VLANs with Firewalls; VPN to connect a pipeline securely.

Mobile Connectivity

- **SATCOM** - Sattelite communication phone
- **Bluetooth**
- **NFC** - Near Field Communication: Almost/Physical contact with another device *(there's no security envolved when activated)* - Easy connection
- **ANT/ANT+** - Very simple form of wireless communication; slow and protected; (i.e Odometers, Heart Rate Monitors, Bikes)
- **Infrared** - Most Androids, communication Transmitter.
- **USB**, USB OTG (On-the-Go)
- **Wi-Fi** and **Tethering**
    - ADHOC, Wi-Fi Direct (Easy connection)
    - Tethering - Wired and Wireless Tethering: acts like a router

Deploying Mobile Devices

COBO - Corporate Owned, Business Only

- Company owned
- Company devices what to do with that device
- What applications are on that device
- What encryption is used?
- What wireless is connected?

COPE - Corporate Owned, Personally Enabled

- Everyone has the same device
- Great control because everyone has same device on environment
- People will still want to use their own devices
- Learning curve

CYOD - Choose Your Own Device

- Users get to choose from a list af approved devices
- Less of learning curve

BYOD - Bring Your Own Device

- User get to choose to bring their own devices, based on their experiences
- Learning curve is decreased
- Very heavy device management

- Mobile application management

Mobile Enforcement

Sideloading

Installation of third-party applications that is different from original Application Store (Google Play, Apple Store)

Carrier Unlocking

Rooting/Jailbreaking

- Root Access
    - Install custom firmware
- Root Access Issues
    - Auto updates disabled
    - Trouble accessing the store
    - Exposure to malware

Things to Avoid on Mobile

To achieve this topics you will need a good policy

- Firmware OTA updates (over-the-air) - turn off
- Camera use - can be use to take pictures of confidential information etc.
- SMS/MMS - high cost
- External Media
- Recording Mic/GPS tagging
- Payment Methods - when your bank account is connected to the phone

Mobile Device Management - MDM

- **Content Management**
    - Applications Management
    - Databases
    - Documents
- **Geolocation**
    - Knows the location of that device
- **Geofencing**
    - Geolocation with geographic trigger
- **Push notification services**
    - Applications will push notifications if you want

- **Passwords and PINs**
    - Require use of passwords and PINs
    - Can recover passwords
- **Biometrics**
    - Fingerprints
    - Facial Recognition
    - Vocal Recongnition
    - Can lock and unlock devices
    - Use to configure applications
- **Screen Locks**
    - Make sure your screen is locked
- **Remote Wipe**
    - Great when the device is lost

Mobile Application Management - MAM

- Versioning
- Updates
- Patches

Context-aware authentication

- Where are they right know?
- What OS are they using?
- What time/day are they trying to authenticate?

Storage segmentation

- Dedicating a storage space for our applications

Full Device Encryption

- Encrypt the entire storage of the device

🛑 - *Some companies provides **MDM solutions** (i.e Google - Android: What applications people can install, security policies and so on)*

Physical Controls

Deterrent Physical Controls

- Outside light, Parking Lot Lighting
- Signage (i.e Restricted Area)
- Security Guards

Preventive Physical Controls

- **External**
    - Fences, Gates, Barricades, K ratings(designed to stop vehicles)
    - Mantrap (some type of entry system, consisting of 2 doors)
    - Cabling systems - (Using AirGap ; VPNs or VLANs)
- **Internal**
    - Safe for Important documents
    - Locked cabinets
    - Faraday cages - to protect sensitive eletronic equipment
    - Locks
        - Key management system (where the keys are stored? who is in possession of those keys?...)
- Individual Workstation
    - Cable Locks
    - Screen filters

Detective Physical Controls

- Alarms
- Cameras
- Motion detectors
- Infrared detectors
- Log Files - can be important in terms of tracking

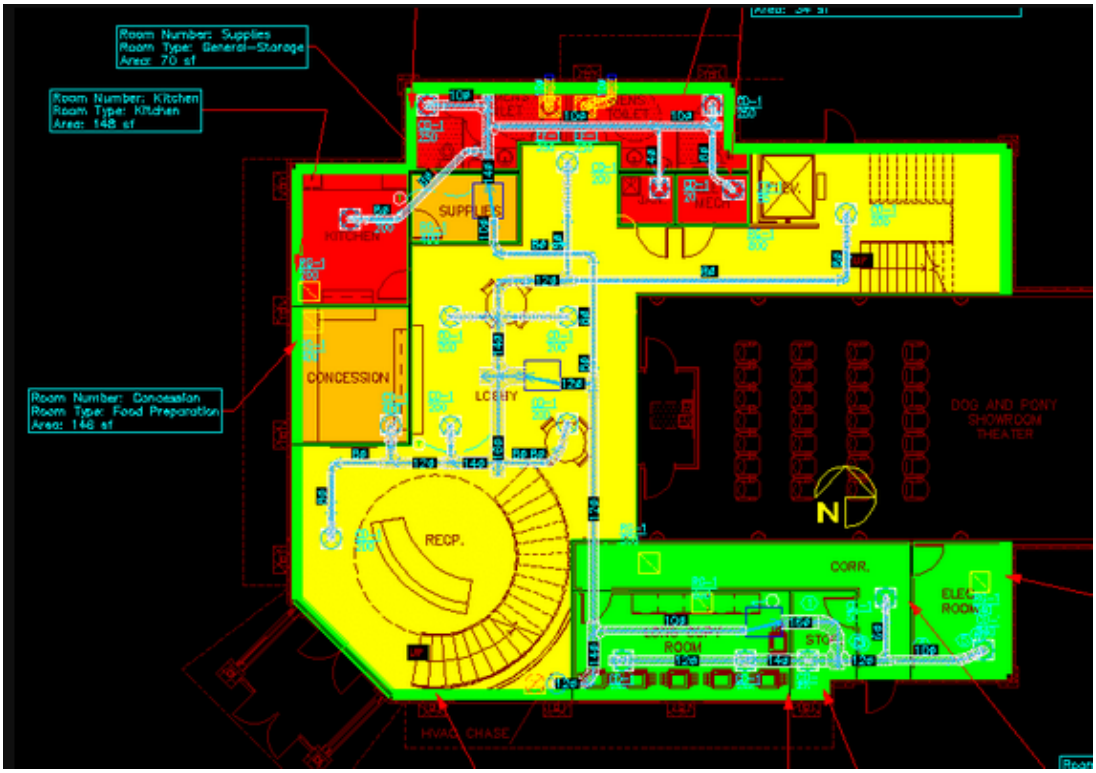
Compensating & Corrective Physical Control

Temporary fixes when these controls are weakened.
i.e - If the outside fence in some way got a big hole, you need to place a security guard on that location until the fences got fixed.

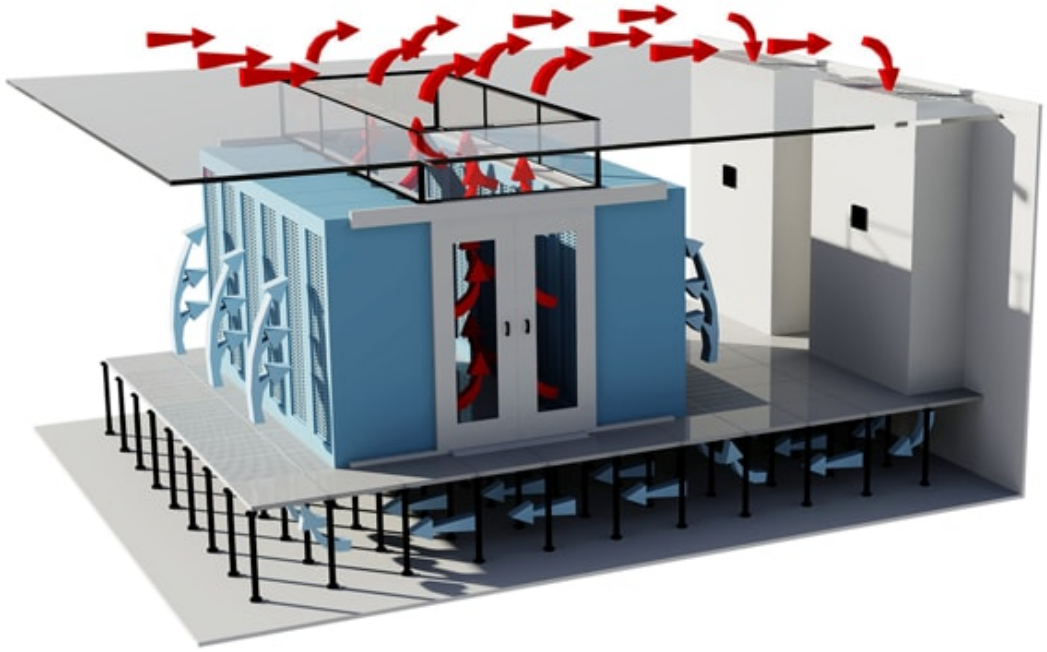
HVAC - Heating, Ventilation, and Air Conditioning

- Office Environment - room temperature, humidity
- Server Rooms - Super sophisticated HVAC's systems; Make sure keep cool and dry
- **Infrared Camera** - we can determine heats more easily

- **Zone-based HVAC**



- **Hot & Cold aisles** - Used in server rooms, HVAC use either hot and cold aisles a contained system to vent hot air out and away from ther server racks; Layout of data centers inteligently and efficiently. Aisles of equipment racks are set up such that there are alternating hot and cold aisles.



- MAC filtering is a good idea on system controllers of HVAC

- **Remote Monitoring** - VPN access, 802.1X

Fire Suppression

Types of Fires and Appropriate Fire Extinguishers

Class	Type	Contains
A	Ordinary(Wood, Paper)	Foam, Water
B	Liquids(Gases, oil)	CO2, Foam, Powder
C	Electrical (eletronic equipment)	CO2
D	Combustible metals (sodium, magnesium)	Powder

FM200 is a special extinguisher liquid that is great because it can stops fires, but can still save the electrical equipment; "Gold Standard" for fire suppression on server rooms.

Class C is best extinguisher for suppress fire on Server Room, but it may ruin some electronics due to the corrosive powder inside.

Protocols Security

SSH protocol

- Key exchange algorithms
- Designed to run in a tunneling mode (encrypted); And then can provide their own encryption (AES, DES...)
- Runs on Port 22

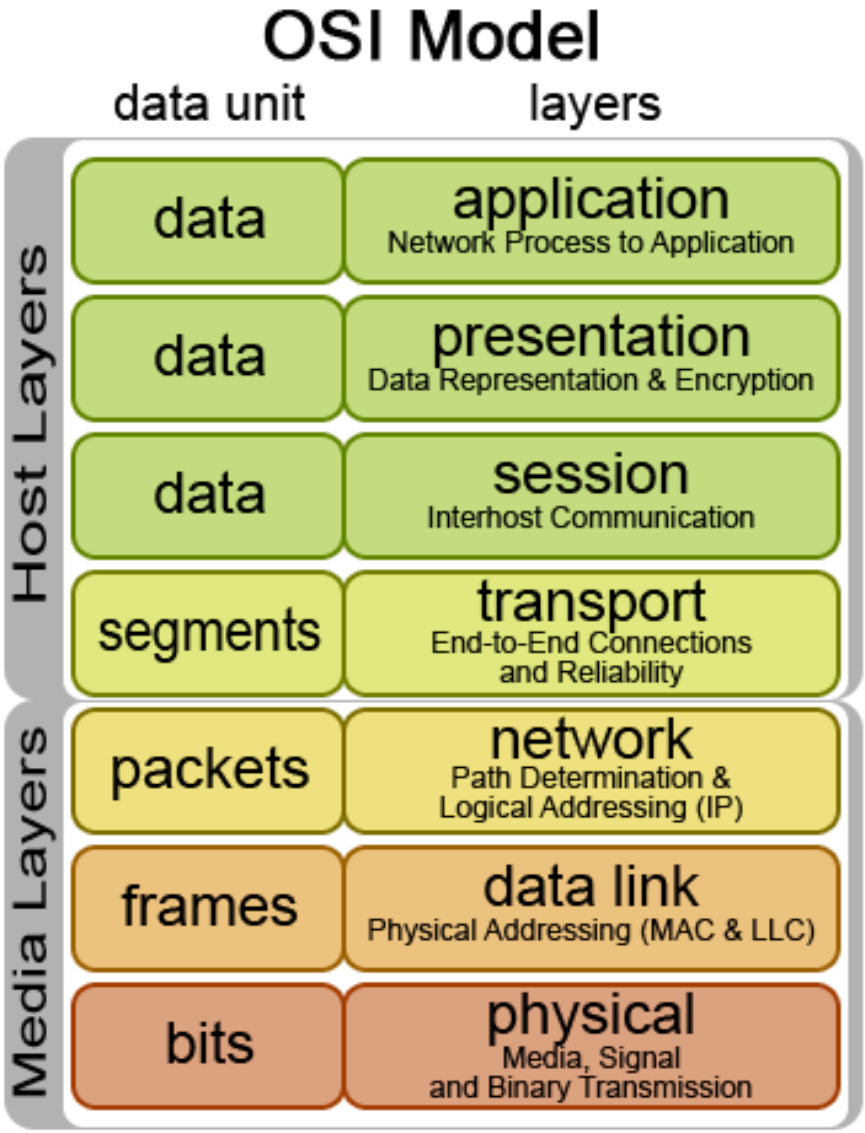
- Almost any encrypted application or protocol number do some kind of key exchange.

HTTP over TLS = HTTPS

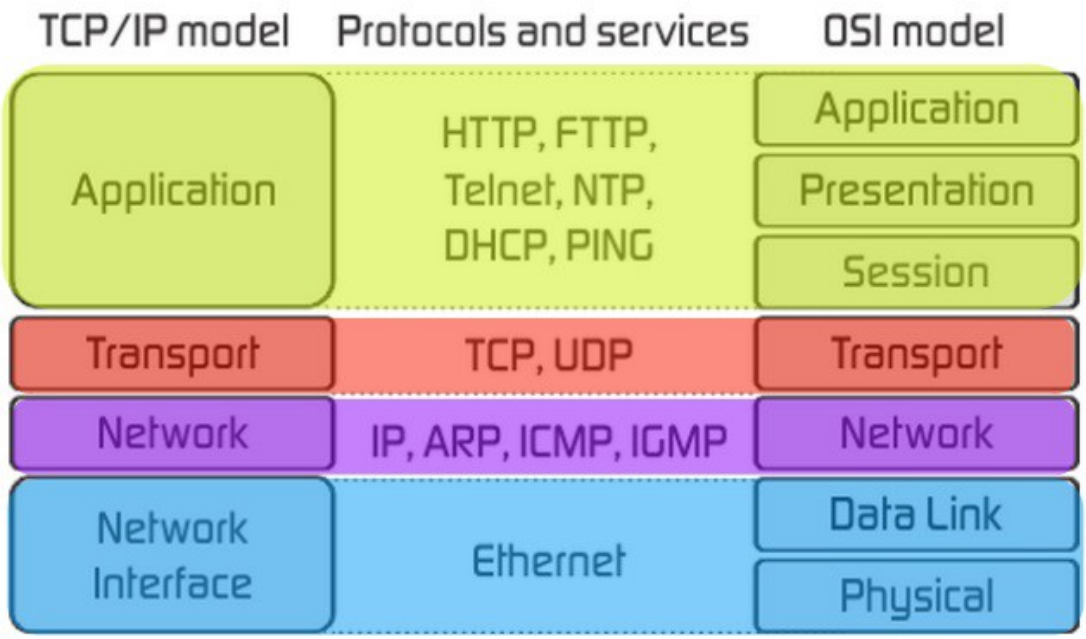
Unencrypted HTTP running TLS encryption

- TLS encryption is a protocol that you can plug it into different types of applications
- Runs on Port 443

Network Models



TCP/IP MODEL vs OSI MODEL



IP Addressing

Private **IPv4** address range

32-bit address with 4 octets

10.0.0.0 - 10.255.255.255
172.16.0.0 - 173.31.255.255
192.168.0.0 - 192.168.255.255

IPv6 Address

128-bit address

Link local: **FE80** - generated automatically by individual hosts

Internet addresss: 2000:0BD8:A388:0000:0000:A2E8:3844:1337

- Very common within the IPv6 wolrd to have more than one IP address

Transport Protocols

TCP - connection oriented; lots of packets being set; three-way handshake is the cornerstone of TCP

UDP - connectionless, sends lots of packets. Have no acknowledgement.

ICMP - supporting protocol handling ARP and Ping.

File Transfer Protocols

Port	Description
20	FTP Data / FTPS

Port	Description
21	FTP Control / FTPS
22	SSH - Secure Shell Remote Login Protocol / SCP - Secure Copy / SFTP(Secure FTP)
25	SMTP - Simple Mail Transfer Protocol (sends email)
53	DNS
67, 68	DHCP uses UDP
69	TFTP - Trivial File Transfer Protocol runs on UDP
110	POP (receives email)
137, 138, 139	NETBios Protocol
143	IMAP (receives email)
161, 162	SNMP - Simple Network Management Protocol
389	LDAP - Light Weight Directory Access Protocol
445	SMB
465, 587	SMTP over SSL/TLS encrypted
993	IMAP over TLS/TLS
995	POP over TLS/SSL
3389	RDP - Remote Desktop protocol (TCP)

SSL and TLS

Secure Socket Layer (**SSL**) and Transport Layer Security (**TLS**), they are protocols that are designed to make secure connections between two points.

- SSL and TLS originally designed for Secure Websites (**HTTPS**)
- TLS is more robust and new solution for secure connection than SSL
- SSL/TLS is not only for HTTPS, you can see in e-mails, VPNs, all over the internet.

  - **Making a Secure Connection**
    - *Client Hello - Body/Example (from Wireshark):*
      - **Symmetric Encryption** (i.e AES 128 GCM)
      - **Key Exchange** (i.e ECDHE)
      - **Authentication** (i.e RSA certs)
      - **HMAC** (hash-based message authentication code) (i.e SHA 256)

DNS - Domain Name System

- DNS is a nonsecure protocol

DNSSEC

DNSSEC is not encryption, is an authentication tool to avoid spoof and replay attack.

- Uses PKE (publick key encryption)
- Adds Integrity and Authentication
- Avoid Replay Attacks and Spoofing

E-mail (SMTP, POP, IMAP)

🛑 SMTP, POP and IMAP is not secure.

SMTP over TLS/SSL

- Encrypt the connection to the server
- Uses port **465** or **587**

IMAP over TLS/SSL

- Creates a TLS encrypted tunnel
- Uses port **993**

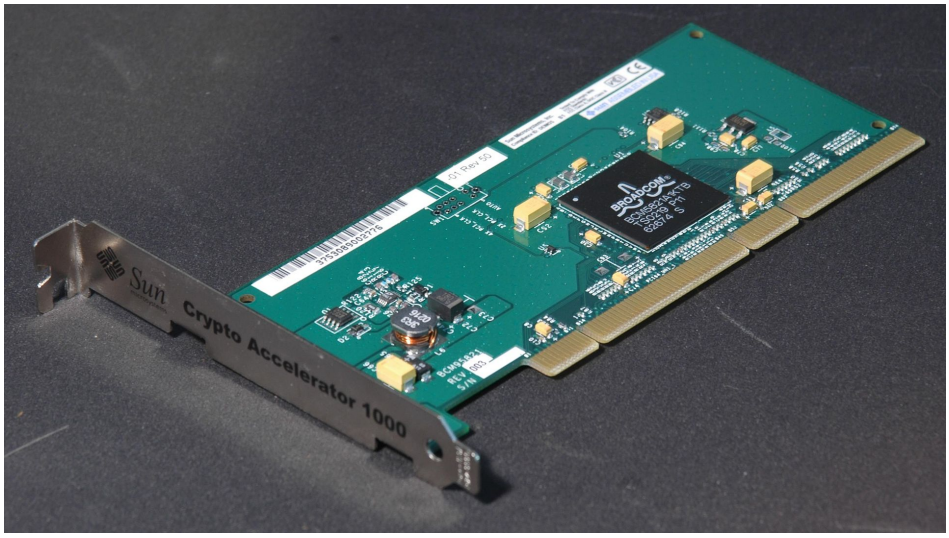
POP over TLS/SSL

- Creates a TLS encrypted tunnel
- Uses port **995**

Protecting Servers

SSL Accelerator

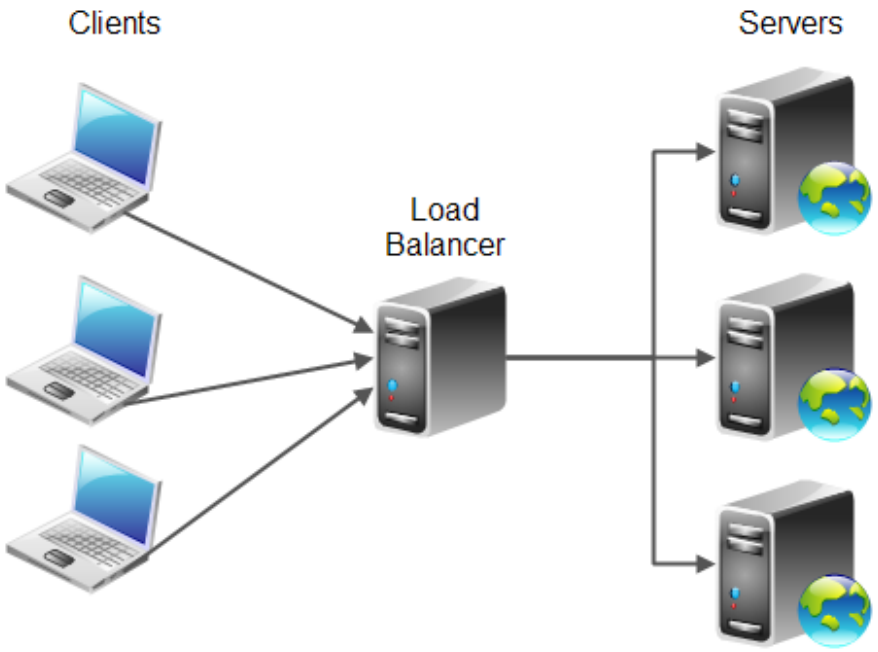
- Dedicated card placed behind the gateweay router between the internet, to handle all SSL/TLS encryption & decryption going across the network.
- Can be done on a dedicated machine



Load Balancer

- Load balancer is actually a proxy because he takes all the incoming requests for the Web site and then distributes it around to the servers

- Enhance security and efficiency

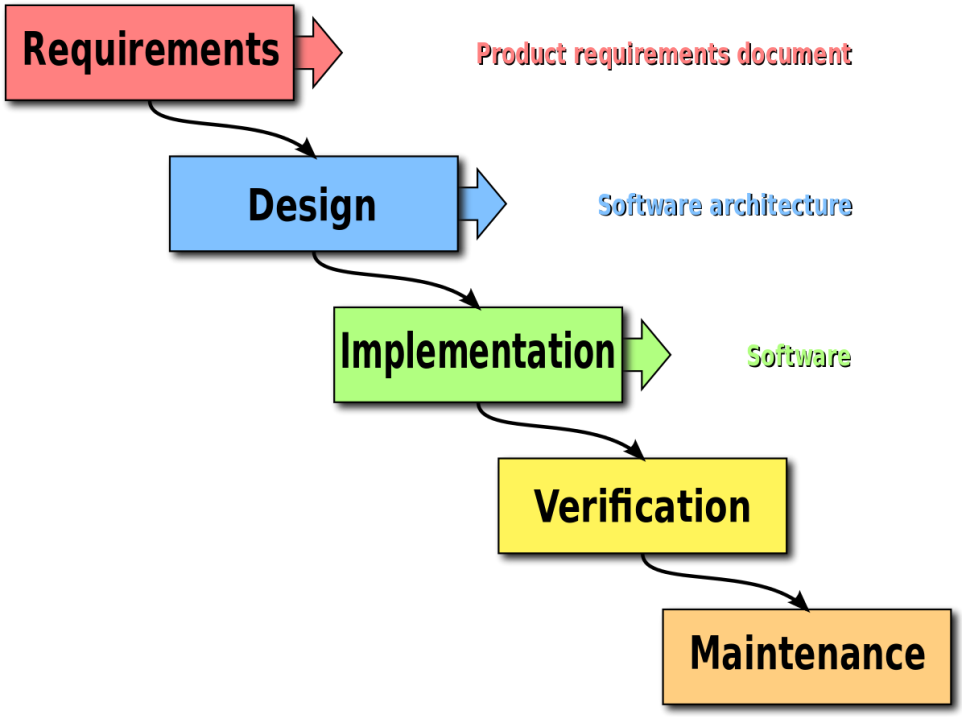


DDoS Mitigator

- A box that can detect when denial of service attacks are coming through.
- Will send an alert to emergency response services which assist in traffic flow to the site under attack
- Act like a proxy for websites

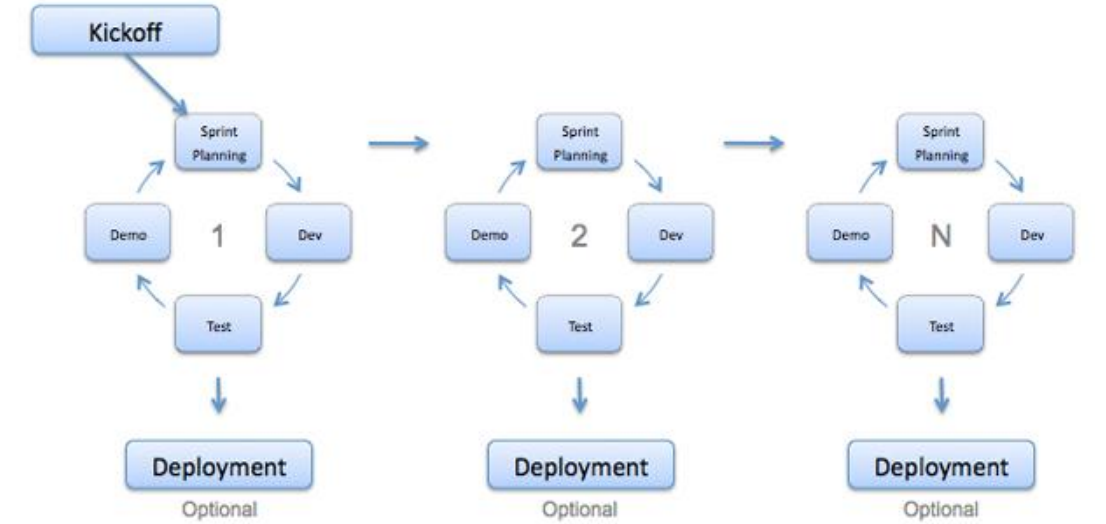
Secure Code Development

Waterfall Model



Agile

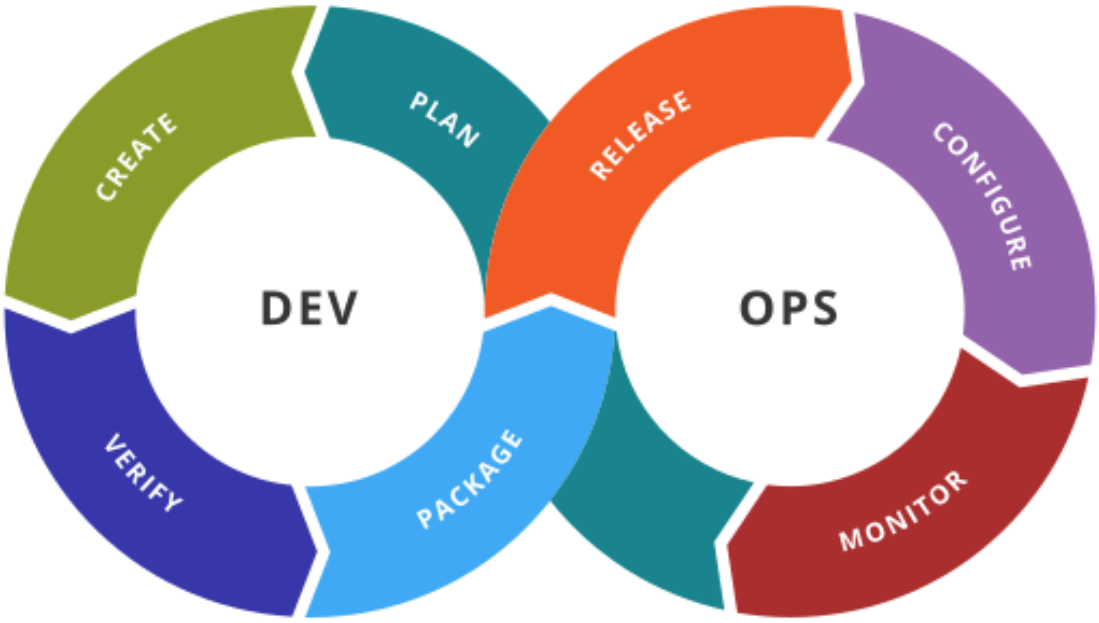
- Created to be better than Waterfall Model
- Sprints (small, rapid, measurable deliverables)
- Scrum



DevOps

Benefits of DevOps:

- Speed
- Rapid Delivery
- Reliablity
- Scale
- Improved Collaboration
- Security



Securing DevOps

- **Run Security Automation Tools** to speed up security testing and eliminate human errors. Security testing like fuzzing.
- **Add strict Change Management and Version Controls** to ensure faults aren't introduced into the application.
- **Introduce Security Concerns and Requirements** at the planning stage to ensure strong security integration.
- **Integrity measurement** shows honesty, morality, and quality of the application.
- **Baselining** defines security objectives that the application must meet.
- **Immutable systems** are systems that once deployed are never upgraded, changed, or patched. They are simply replaced. This is easy to do in a **VM environment**.
- **Infrastructure as Code (IaC)** means to use preset definition files as opposed to manual configurations to set up servers. IaC prevents accidental vulnerabilities due to flawed server configurations.

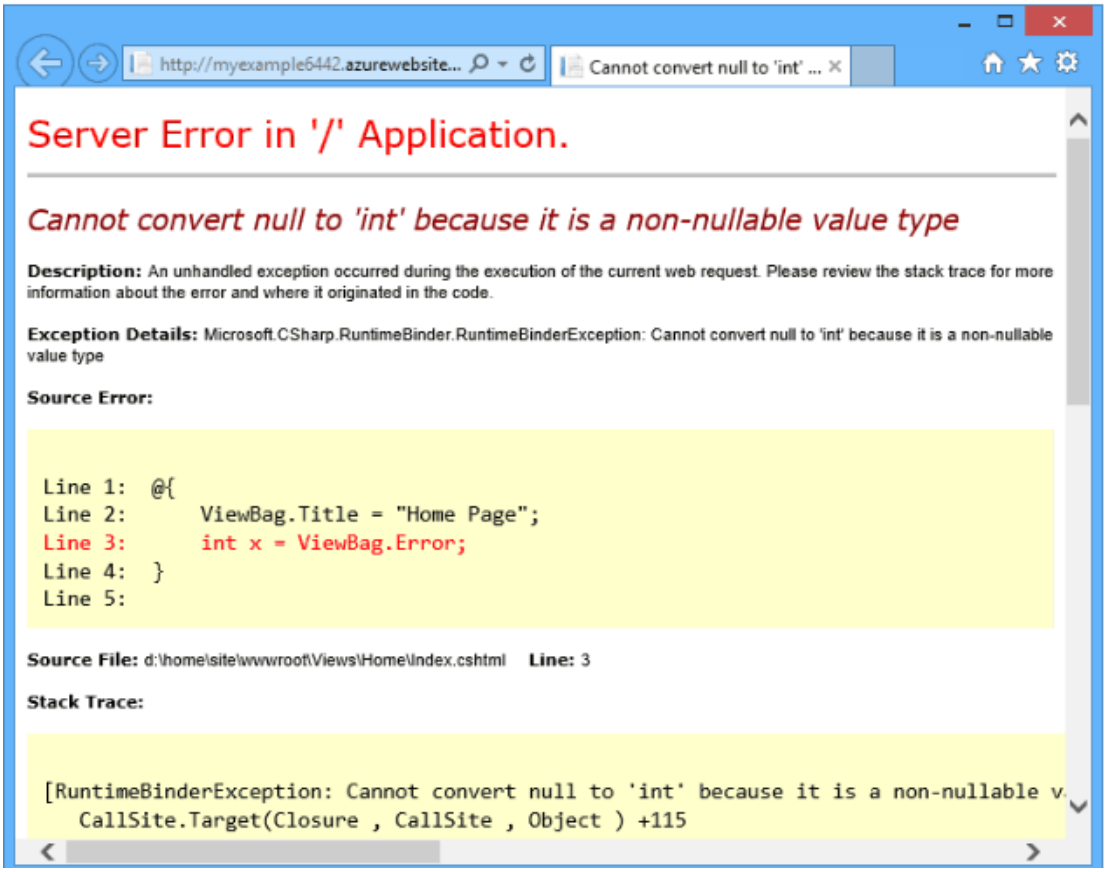
Secure Code Techniques

Compiled vs. Runtime code

Compile-time is the instance where the code you entered is converted to executable. Run-time is the instance where the executable is run.

Error Handling

Proper Error Handling: isn't going to stop all errors, but it will prevent errors from apperaring on the user interface for easy viewing for attackes / bad actors.



Input Validation

Proper Input Validation: helps prevent these types of attacks: **command insertion, cross-site scripting, buffer overflows, and SQL injection**.

Normalization

Is a database term meaning to store and organize data so that it exists in one form only. For example, a user database has the three tables shown. (name table, zip code table etc).

Stored Procedures

Stored Procedures harden web apps; Is a piece of code, custom written by devs of the app and stored in the Database. **This code only respond to a specific query format defined by the eveloper, this can prevent SQL injection or common bad queries used by attackers.**

Encryption / Code signing

Code signing means to sign an individual executable/interpred code digitally so that users have confidence the code they run is the actual code from the developer.

Obfuscation

To make harder an attacker reverse-engineer the code (i.e Minifying Javascript)

Code reuse / Dead Code

Get rid of dead code inside the web app. (i.e Commented unecessary code)

Server-side vs. Client-side

In general, a server-side platform is more secure than a client-side platform, but client-side is generally faster and may receive big chunks of code to the client, to prevent that you can use encryption.

Memory Management

Watch out the memory leaks to avoid buffer overflow attack and code reuse.

Third-party libraries

Weaknesses of third-party libraries can result on bad actor exploring this. To avoid this type of risk, maintain patch updates, stay on top of any announcements, check the dependencies of the third-party libraries using OWASP dependency checker.

Data Exposure

If you have data that is a part of your app some of that data has risk of exposure. And our job as developers is to reduce if not eliminate any risk of that data exposure especially if it's personally identifiable information or personal health information. We almost always today go through aggressive encryptions any time.

Code Quality & Testing

- **Static Code Analysis**

    - Look for standard types of errors
    - They don't run the code

- **Dynamic Code Analysis**

    - Actually runs the code
    - Looks for logic errors
    - Look for Security holes
    - Memory Leak
    - Database querying

- **Staging**

    - **Stress Test** - aggressive test of issues such as multiple user simultaneous inputs, multiple server data syncing ...
    - **Sandboxing** - test the systems, almost always virtual machines (VMs), that enable developers to run the application aggressively.

- **Model Verification** - **Model** defines how developers expect some feature of the final code to perform. **Model Verification** match the application to the aspect of the model.(i.e -This button drive the user to the home or not?)

- **Production** - When the testing are done and it's time to pull the application online and running. (expose to the public / internet). The process of moving an application from the development environment to the production environment is called **provisioning**. The process of remove an application from the production is called **desprovisioning**.

---

4) Identity and Access Management

Identification and AAA

Identification, authentication, authorization, and accounting work together to manage assets securely.

Identification

The information on credentials identifies the user.

Authentication

- **Authentication Factors:**
    - Something you **know** (password)
    - Something you **have** (smart card)
    - Something you **are** (fingerprint)
    - Something you **do** (android pattern)
    - **Somewhere** you are (geolocation)
    - *Multi-factor authentication generally uses two of this examples (Something you Know and Something you Have), never on same category*

- **Trusts and Federated Authentication**:
  - **Trust Relationship** - Active Directory DS
  - **Transitive Trust** - The organization trusts another entity because they are trusted by someone else that the organization trusts.
  - **Federated System** - Common authentication and credentials database that multiple entities use and share. (Active Directory: Different Domains could be used in other domains in the same forest).

Authorization

- **Permissions**: Applied to resources
- **Rights** / **Privileges**: Assign at system level
- **Authorization strategies**:
  - Least privileged
  - Separation of Duties

Authorization Models

- **Mandatory Access Control (MAC)**:
  - Labelling
  - Used on old systems (i.e. Top Secret Gov. information)
- **Discretionary Access Control (DAC)**:
  - Owner of the data defines access
  - Roles
- **Role-based Access Control (RBAC)**:
  - Access to resources is defines by a set of rules
  - by Groups (i.e. Admin Groups --> Rights and Perms | Sales Group --> Rights and Perms)

🛑 **Access is defined by ACL, Access Control List.**

🛑 **Implicity deny prevents access unless specifically permitted.**

Password Security

- **Complexity**
  - Length and character requirements
- **Expiration**
  - Reset and time triggers
- **Password history**
  - Reusage and retention

Password Security

Password Policy (Local Security Policy - Windows)

- **Enforce Password History**: determine the number of new unique passwords [1-24]
- **Maximum Password Age**: Password age [1-999 days]
- **Minimum Password Age**: Limit until request password change [1-998 days]
- **Maximum Password Lenght**: [1-20 characters]
- **Password Complexity:**
    - Not contain user account name or parts of full name
    - At least 6 characters lenght
    - At least three of four categories:
        - Uppercase [A-Z]
        - Lowercase [a-z]
        - Base 10 digits [0-9]
        - Non-alphabetic characters [!,@,#,$,...]

Account Lockout Policy

- **Account Lockout Duration**: Time (in minutes) for a locked-out account [0-99,999]
- **Account Lockout Threshold**: Number of failed logon attempts [0-999]
- **Reset Account Lockout Duration**: Period of time that must elapse before the account lockout counter is reset to 0 bad logon attempts. [1-99,999]

Group Policy Objects (AD DS)

Set of rules that allow an administrator granular control over the configuration of objects in Active Directory, including user accounts, operation systems, applications and other AD objects. Can apply over multiple domains, groups and OU's.

Linux - File Permissions

Linux has three permissions and they can be set for the owner, group or other.

r = read - open a file, view a file.
w = write - edit a file, add or delete files for directories.
x = execute - run a file, execute a program or script, CD to a different directory.

Owner	Group	Other
rwx	rwx	rwx

- Viewing the permissions on Linux command-line:

```
ls -l
-rwxrwxr-x 1 user user 31337 Feb 11 13:13 File
```

Using `chmod` - to change file modes or Access Control Lists

- Clear out the permissions of the **File** to have no read, write and execute permissions on **Other**:
  (The flag equals to nothing[o=] deny the permissions)

```
ls -l
-rwxrwxr-x 1 user user 31337 Feb 11 13:13 File

chmod o= File

ls -l
-rwxrwx--- 1 user user 31337 Feb 11 13:13 File
```

- Giving **read** and **write** permissions to **Group**:

```
ls -l
-rwx---r-- 1 user user 31337 Feb 11 13:13 File

chmod g=rw File

ls -l
-rwxrw-r-- 1 user user 31337 Feb 11 13:13 File
```

- Giving **all permissions** to everybody(Owner,Group and Other):

```
ls -l
-rwx---r-- 1 user user 31337 Feb 11 13:13 File

chmod a=rwx File

ls -l
-rwxrwxrwx 1 user user 31337 Feb 11 13:13 File
```

Using `chmod` on oldschool way:

The chmod command will take the octal value and combine them to associate the permissions on three different positions for the Owner, Group and Other/Everyone. This boils down to a simple binary rule: 0 = off | 1 = on.

Octal	Binary	Permissions
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x

Octal	Binary	Permissions
6	110	rw-
7	111	rwx

If you want to give all permissions to a group for example, the number will be 7 (4 + 2 + 1).

Read	Write	Execute
r--	-w-	--x
4	2	1

Examples:

- Giving **read, write and execute** permission to everybody:

```
ls -l
-rwx---r-- 1 user user 31337 Feb 11 13:13 File

chmod 777 File

ls -l
-rwxrwxrwx 1 user user 31337 Feb 11 13:13 File
```

- Giving all permissions to the **owner**, read and write to **group** and no permissions to **other/everyone**:

```
ls -l
-r-x---r-- 1 user user 31337 Feb 11 13:13 File

chmod 760 File

ls -l
-rwxrw---- 1 user user 31337 Feb 11 13:13 File
```

Linux - File Ownership using `chown` -- change file owner and group

```
ls -l
-rwxrwxrwx 1 user001 user001 31337 Feb 11 13:13 File

sudo chown root File

ls -l
-rwxrwxrwx 1 root user001 31337 Feb 11 13:13 File
```

The chown command requires sudo

Linux - Changing the Password using `passwd`

```
sudo passwd
```

Windows - NTFS File & Folder Permissions

NTFS permissions are granted to users and groups on folders and files.

NTFS Permissions - Folder

- **Full Control** - Anything
- **Modify** - Read, Write and Delete Files and Subfolders
- **Read/Execute** - See contents and Run Programs
- **List** Folder Contents - See Contents of Folders and Subfolders
- **Read** - View Contents and Open data files
- **Write** - Write to Files and Create new files and folders

NTFS Permissions - File

- **Full Control** - Anything
- **Modify** - Read, Write and Delete files
- **Read/Execute** - Open and Run the file
- **List** Folder Contents - Open the file See Contents of Folders and Subfolders
- **Read** - Open the file
- **Write** - Open and Write to the file

🛑 *Deny is stronger than allow*

Moving and Copying NTFS Objects

1. **Copy and Move** from drive X: to Y: - will take the NTFS permissions of the **destination** drive.
2. **Copy** from drive X: to the same drive X: - **will loose the NTFS permissions.**
3. **Move** from drive X: to the same drive X: - **will inheritance the NTFS permissions**

User Account Management

Continuous Access Monitoring

Monitoring all users account activity

- Track Log on and Log off activity
- Track file access

🛑 - Shared Accounts = Bad!!!
🛑 - Multiple Accounts = Use different user/pass.
🛑 - Use least privilege - enough necessary to accomplish task.

- 🛑 - Monitor and log activity of users with multiple accounts. (Log everything)
- 🛑 - Avoid default usernames on user accounts.

Triple AAA - Authentication, Authorization and Accounting

Two most popular protocols of triple AAA is RADIUS and TACACS+, providing centralized **Authentication**, **Authorization** and **Account management and registry logging** for computers to connect and use a **network service** securely.

RADIUS or TACACS+ server resides on a remote system and responds to queries from clientes such as VPN clients, wireless access points, routers and switches.

How RADIUS and TACACS+ works:

- The server authenticates **username and password** [authentication]
- Determine if a user is **allowed to connect** to the client [authorization]
- **Log** the connection [accounting]

RADIUS - Remote Authentication Dial-In User Service

used for network access

1. **Radius Server**: Get the stack of usernames and passwords (can be MySQL, AD/DS, etc.)
2. **Radius Client**: The Gateway between users and servers
3. **Radius Supplicant**: The person that want to authenticate

RADIUS can use up to 4 different ports:

- **1812**
- **1813**
- **1645**
- **1646**

TACACS+ - Terminal Access Controller Access-Control System Plus

Is really good to manage a big number of network devices.

Provide the same as RADIUS but the service decouple the authorization from the authentication. Manages the authorization better than RADIUS.

Uses TCP Port 49

Authentication Methods

PAP - Password Authentication Protocol

Is the oldest authentication method. PAP sends username and password **in the clear / plaintext**

CHAP - Challenge Handshake Authentication Protocol

Uses a hash value of challenge message to authenticate

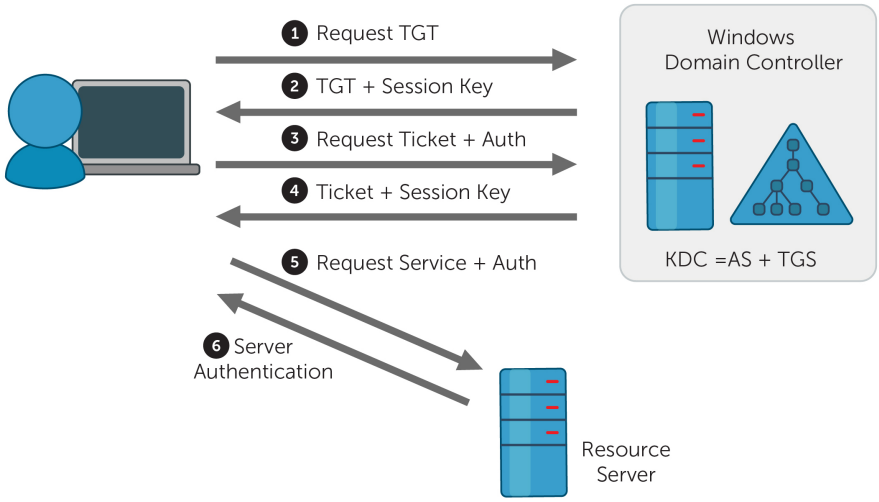
NTLM - NT LAN Manager for Windows

Similar to the CHAP; uses a challenge hashed message with a different process than CHAP

Kerberos - for AD/DS

1. Authenticator (Encrypted with user's password)
2. TGT (Encrypted with KDC's key) [ticket-grant-ticket]
3. Resource Ticket (Encrypted with Resource's key by the KDC and issued to the user)
4. Resource Ticket used by Client to access the resources

Uses Port 88



SAML - Security Assertion Markup Language

Used exclusive for **Web Application**

LDAP - Lightweight Directory Access Protocol

Query Directories: Structured language that allows one computer to go into somebody's directory and query, update...

Uses TCP/UDP Port 389

Single Sign-On

- **LAN**: Windows Active Directory is dominant for **security SSO**
- **SAML**: SSO for **Web Application** / used to manage multiple apps using a single account

---

5) Risk Management

Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Defining Risk

Vulnerability: A weakness; System flaw

Threat: Exploit vulnerabilities to harm assets.

Risk: The likelihood of a THREAT exploiting a VULNERABILITY, resulting in a loss.

Formulas:
threats x vulnerability = risk
threats -> vulnerability = risk

1) Asset:

Is a part of an IT infrastructure that has a value. You can measure value either tangibly or intangibly. A gateway router is an example of an asset with tangible value, if it fails, you can easily calculate the cost to replace the router.

Example of assets:

Asset	Info.
Servers	The computers that offer shared resources
Workstations	The computers users need to do their job
Data	The stored, proprietary information an organization needs to operate
Applications	Specific programs an organization needs to use
Personnel	The people who work in an organization
Wireless access	Wireless access to the network
Internet services	The public or private-facing resources an organization provides to customers, vendors, or personnel via the Web or the Internet applications

2) Probability

Probability means the likelihood - over a defined period of time - of someone or something damaging assets.

Quantitative likelihood: based on numbers and data, can be more easy to measure anually.

Qualitative likelihood: is more subjective like (low/medium/high).

3) Threat actors

A threat actor can be a malicious person, such as a hacker accessing corporate secrets.

The exam cover six types of threat actor:

- Hacktivists
- Script Kiddies
- Insiders
- Competitors
- Organized Crime
- Nation State/APT

Risk Assessment

1) Vulnerability Assessment

- NIST SP 800-30
- CVE (Common Vulnerabilities and Exposures)
- Nessus scanner
- Penetration Testing

2) Threat Assessment

- **Environmental**: Natural disasters outside the control of humans
- **Manmade**: Any threat that is not environmental
- **Internal**: Threat generated by internal sources, usually an insider to the organization
- **External**: Threat generated from outside your infrastructure

Risk Response

After identified and analyzed risk, you must decide how to responde to the risks produced as a result of the analysis.

1) Risk Mitigation

Is an attempt to reduce the risk, or at least minimize its effects on an asset.

2) Risk Transference

Or Risk Sharing, deals with risk by sharing with third-party. Example buying insurance to protect against natural disasters.

3) Risk Acceptance

Means the organization has implemented controls and some risk remains. (residual risk). Remember that risk can never be completely eliminated.

4) Risk Avoidance

Means thtat the organization could choose not to participate in activities that cause unnecessary or excessive risk.

Risk Frameworks

- NIST - Risk Management Framework SP 800-37
- ISACA Risk IT Framework

Security Controls

The cornerstone of IT security is understanding security controls and how to apply them.

1. **Administrative Control** (People -> IT Security)
    - Laws
    - Policies
    - Guidelines
    - Best Practices
2. **Technical Control** (IT Systems -> IT Security)
    - Computer stuff
    - Firewalls
    - Password links
    - Authentication
    - Encryption
3. **Physical Control** (Physical World)
    - Gates
    - Guards
    - Mantraps
    - Keys

Activity Phase Control Types

1. **Deterrent control**: Deters the actor from **attempting** the threat. *(Warning Sign, SSH Banner)*
2. **Preventive control**: Deters the actor from **performing** the threat. *(Fence, Server Locks, Password Complexity)*
3. **Detective control**: Recognizes an actor's threat. *(Background check, CCTV, IDS)*
4. **Corrective**: Mitigates the impact of a manifested threat. *(Backups)*
5. **Compensating**: Provides alternative fixes to any of the above functions

*Most of security controls are **preventive** phase controls*

Interesting Security Controls

- Mandatory Vacation
- Job Rotation
- Multi-person Control

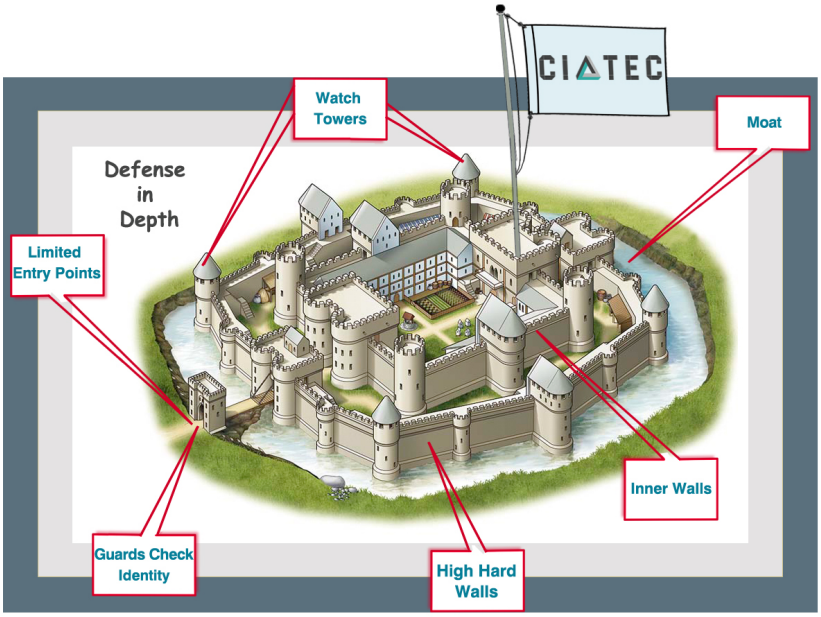
- Separation of Duties
- Principle of Least Privilege

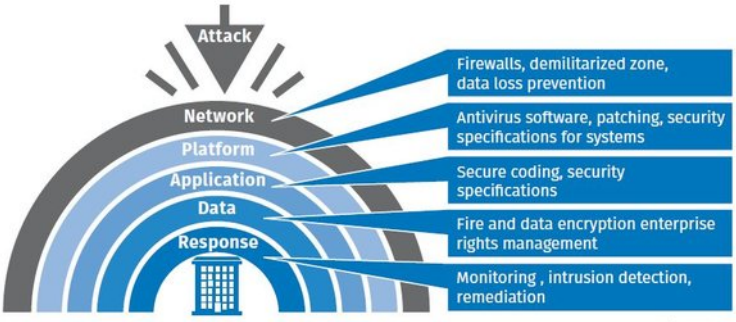
Defense in Depth

Every IT infrastructure might be looked at as a series of concentric shells. The location of these shells depends on the types of threats you are mitigating.

Defense in Depth uses **administrative, physical and technical controls**.

Physical defense in depth





Source: http://www.tsidata.com/defense-in-depth/ *Figure 1 - Defense in Depth*

Redundancy

Repeating the same controls at various intervals.

Diversity

Try different set of security controls in a random pattern.

- **Vendor Diversity**: Uses several vendors to supply equipament and services.

IT Governance

Influences how the organization conducts IT security.

In its most core function is to actually make the right set of security controls.

1. Laws and Regulations

- HIPAA (Health Insurance Portability and Accountability - USA)

2. Standards

- **Governament Standards**: NIST, ISO
- **Industry Standards**: PCI-DSS (Payment Card Industry Data Security Standard)

3. Best Practices
4. Common-Sense

Policies

Document that defines how we're going to be doing something. Define Roles and Responsabilities.

Organizational Standards

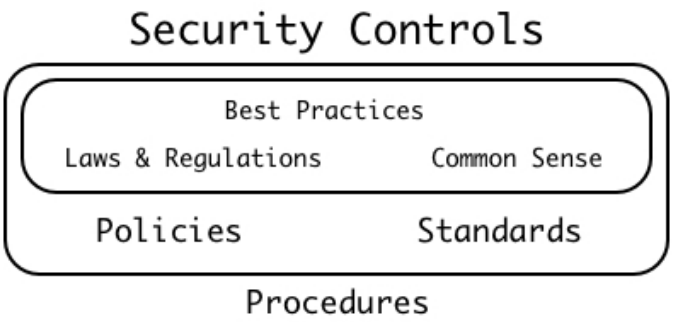
Have much more detail than policies. Define the acceptable level of performance policy.

The security controls come from the policies and standards.

Procedures

Step by step process of how to do something.

Security controls, Policies and standards help define and build the **Procedures**.



Security Policies

The Acceptable Use Policy (AUP):

Defines what a person can or can not do when using company assets and equipament. *(The paper you sign before entry a job position)*.

Data Sensitivity and Classification Policies:

Define the importance or nature of the data. *(i.e. Applying labels on the Government, they use Top Secret, Classified, etc)*.

Access Control Policies:

- How people get access to data or resources
- What type of data do users have access to.
- Data access and classification restrictions *(It cover a lot of things based on the job type)*.

Password Policy:

- Password recovery
- Password retention
- Bad login attempt
- Password reuse
- Complexity

Care and Use of Equipament

How you maintain company equipament.

Privacy Policy:

Are often for customers; defines how your data or usage will be shared with other resoruces. *(i.e. Services like Facebook etc)*.

Personnel Policies:

- Background Check
- Mandatory Vacation
- Job Rotation
- Separation of Duties
- Multi-person Control

Risk Management Frameworks

A framework is a description of a complex process, concentranting on major steps and the flows between the steps. **Describes the major steps and flows of the complex process of applying security controls in an organized and controlled fashion.**

Frameworks come from a variety of sources including:

- **Regulatory**
- **Non-Regulatory**
- **National**
- **Industry Standards (Best Practices)**

Popular RMF

National Standard and Regulatory:

- NIST SP 800-37

Non-Regulatory:

- ISACA IT Infrastructure

International Standard:

- ISO 27000

NIST Risk Management Framework:

Quantitative Risk Assessment

Is based on objective data -typically, numerical data; Exact values, for instance, can be used to describe impact or loss of an asset.

Asset Value (AV)

When valuing an asset, consider not only the replacement cost, but also the revenue the asset generates, as this will be lost as well if the asset is not available.

Example:

Asset	Cost	Repair	Revenue	= Total
Router	€600	€500 x day	€2000 x day	€3100

Exposure Factor (EF)

The percentage of an asset that could be lost during a negative event. Realistically, you will not always lose 100% (1) of the asset; you may lose only 20% (0.2) or 50% (0.5) for example.

Example:

Incident	Exposure Value
Flood	1 (100%)

Single Loss Expectancy (SLE)

Is the value that's computed simply by multiplying the asset's value by the exposure factor (percentage of loss).

Formula:
Single Loss Expectancy = Asset Value x Exposure Factor
SLE = AV x EF

Example (using data below):

AV	x EF	= SLE
€3100	1	€3100

SLE = €3100 (AV) x 1 (EF) = €3100

Annualized Rate of Occurrence (ARO)

How many times per year you would expect a particularly negative event to occur, resulting in a loss of the asset. **This value relates more to likelihood than impact.**

Example: Flood on Server room, base on data: one flood in about 10 years, 1/10 (0.1). [SLE x ARO = ALE]

Annualized Loss Expectancy (ALE)

Essentially looks at the amount of loss from the SLE and determines how much loss the organization could realistically expect in a one-year period.

Formula:
ALE (Annualized loss expectancy) = SLE x ARO
SLE x ARO = ALE

Business Impact Analysis

Designed to mitigate the effects of an incident, **not to prevent an incident**.

- Determine mission process. *(make sure servers are up)*
- Identify critical systems.
- Single point-of-failure. *(using Defense-in-Depth...)*
- Identify resource requirements.
- Identify recovery priorities. *(prioritize most important steps to kepp whatever essential function running)*

Types of Impact

- Property
- Safety / Life / People
- Finance (Credit, Cash flows...)
- Reputation
- Privacy

Privacy Impact Assessment (PIA) and Privacy Threshold Assessment (PTA)

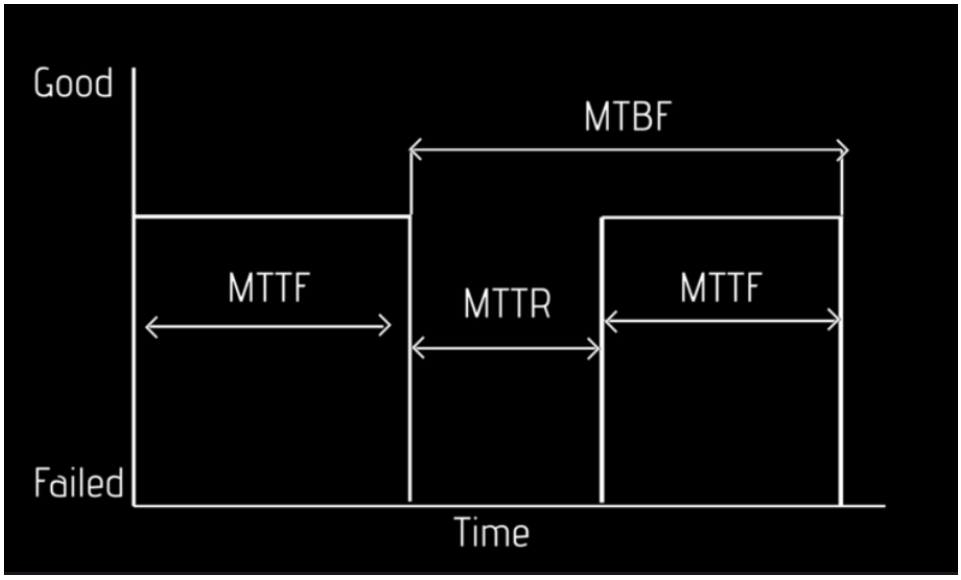
PIA: Determine the impact on the privacy of the individuals who data is beign stored; and ensure that the organization has sufficient security controls applied to be within compliance of applicable laws or standards.

To create a **(PIA) - Privacy Impact Assessment**, the organization needs to perform a **(PTA) - Privacy Threshold Assessment** on its infrastructure to locate **personal information**, what personal info. is stored and from whom the personal info is collected.

PTA and PIA - in order to understand the impact of the loss of personal information can do to a particular business.

Calculating Impact

Determine how long the particular equipament going to last. (qualitative)



- **MTTF = Mean Time to Failure**
- **MTTR = Mean Time to Repair**
- **MTBF = Mean Time Between Failure**

Recovery Time Objective (RTO):

- Maximum amount of time that a resource may remain unavailable before an unacceptable impact on other system resources occurs.

Recovery Point Objective (RPO):

- Defines de amount of time that will pass between an incident and recovery from backup.

Recovery priorities help define what needs to be addressed to maintain business continuity.

Organizing Data

The first step to dealing with data security is **organization**.

- Analyze individual chuncks of data (such as databases, files, access control lists..)
- Determine the importance - **the sensitivity of data.**

Data Sensitivity | Labeling

- **Public Data**: Has no restrictions. (stills needs integrity and availability)
- **Confidential Information**: Limited to authorized viewing as agreed by the parties involved.
- **Private Information**:social security number, passport number, PII - Peronally identifiable information...
- **Proprietary Information**: Information owned by a company that gives a certain competitive advantages. (i.e. The secret formula of Coca-Cola).
- **PHI - Protected Health Information**: Not only Health information, PII may include on PHI.

Data Roles

- **Owner of the data / Data Owner**: Legally responsible for the data, can be entity responsible.
- **Steward / Custodian**: Maintain the accuracy and integrity of data.
- **Privacy Officer**: Ensures data adhere to privacy policies and procedures.

User Roles

- **Users**: Assigned standard permissions to complete tasks. | Must understand how system functions works and have proper security training to recognize common issues (Malware, etc).
- **Privileged Users**: Increased access and control over the data or system. (i.e. a Normal user can run anti-malware software, but the privileged can updated then).
- **Executive Users**: Concentrates on strategic decisions including policy review, incident response and disaster recovery.
- **System Administrator**: Has complete direct control over the data or system. (Can remove or add users, applying permissions, and doing system maintance...)

- **Data Owner | System Owner**: People or organizations who have legal ownership of this particular data set or particular system.

Security Training

Onboarding:

New hires or contractors

- Background check
- NDA (Non-disclosure agrement)
- Standard Operation Procedures
- Specialized Issues (i.e. Clean Desk)
- Rules of Behavior (i.e. Good AUP)
- General Security Policies (i.e. Personal Email, Social network...)

Offboarding:

When the employee leaves the company

- Disable accounts (never delete an account)
- Return Credentials
- Exit interview
- Knowledge transfer

Personnel Management Controls

- **Mandatory Vacation**:
    - Required
    - Prevents collusion
    - Dependency issues
    - Makes fraud harder
- **Job Rotation**:
    - Redundancy and Backup
    - Allows for cross-training
    - Makes fraud harder
- **Separation of Duties**:
    - Requires dual execution *(at least two people to do a sensitive function)*
- **Multi-Person control**:
    - Moren than one person required in a task/function

Role-Based Data Controls

- **System Owner**:

    - Management level role
    - Maintains security of the system
    - Defines a system administrator
    - Works with all **Data Owners** to ensure data security

- **System Administrator**:

    - Day-to-day administration of a system
    - Implement security controls

- **Data Owner**:

    - Defines the sensitivity of the data
    - Defines the protection of the data
    - Works with **System Owner** to protect data
    - Defines access to the data

- **User**:

    - Accesses and uses the assigned data responsibly
    - Monitors and reports security breaches

- **Privileged**:

    - Has special access to data beyond the typical user
    - Works closely with **System Administrators** to ensure data security

- **Executive User**:

    - **Read only** access but can look at all business data

Third-Party Risk / Agreements

Business Partnership Agreement (BPA):

Most common used in private sector.

- Primary entities
- Time frame
- Financial issues
- Management

Service Level Agreement (SLA):

Used in private sector.

- Agreement between who is getting the service and service provider
- Service to be provided
- Minimum up-time
- Response time (contacts)
- Start and End date

Interconnection Security Agreement (ISA):

Is a technical Agreement used on public sector.

- Statement of Requirements
    - *Why are we interconnecting?*
    - *What system is interconnecting?*
- System secuirty considerations
    - *What information is interconnecting?*
    - *Where is this information going?*
    - *What services are involved?*
    - *What encryption is needed?*
- Topological drawing
- Signature authoring
    - Time frame for the interconnection
    - Technical and security reviews from them

Memorandum of Understanding/Agreement (MOU / MOA):

Agreement used in public sector.

- The purpose of the interconnection
- Relevant authorities *(Who is on charge?)*
- Specify the responsabilities
    - Downtime
    - Billing
- Define the terms of the agreement
    - Cost
- Termination/reauthorization

---

6) Cryptography and PKI

Cryptography is the practice of disguising information in a way that looks random

Obfuscation

Hidden sensitive data - providing confidentiality

Classic Algorithms - by Substituition

- **Caesar Cipher** (ROT1-25) - *The earliest known and simples ciphers*
- **Vigenère Cipher** *(Employs the Caesar cipher as one element of the encryption process + the key)*

Kerkchoff Principle

The crypto algorithm should be public and the key is the secret.

Where to **Encrypt & Decrypt**?

- **Data-at-Rest**: Resides in storage
- **Data-in-Transit**: Transport / Network
- **Data-in-Process**: RAM & CPU

Symmetric Encryption

- Fast
- One Single Key / Session Key to encryption and decryption
- Primary way to encrypt data
- Ephemeral Key
    - Temporary
    - Provides perfect forward secrecy

Asymmetric Encryption

- Slow
- Uses a Key pair **(Public Key and Private Key)**
    - Public Key - encrypt
    - Private Key - decrypt

Cryptosystem

Defines key properties, communication requirements for the key exchange; actions through encryption and decryption process.

(Ex: Using asymetric encryption to exchange Session keys after that communicate using Symmetric encryption.)

Symmetric CryptoSystems

Algorithm	Block or Streaming	Block Size	Rounds	Key Size	Notes
DES	Block	64-bit	16	56 bits	Uses five modes of operation: ECB, CBC, CFB, OFB and CTR.
Blowfish	Block	64-bit	16	32-448 bits	Public domain algorithm.
Twofish	Block	128-bit	16	128, 192 and 256 bits	Public domain algorithm.
3DES	Block	64-bit	16	168 bits (56 x 3)	Repeats DES process 3 times.
AES	Block	128-bit	10, 12, or 14	128, 192 or 256 bits	Encryption standard for the US Gov.

Algorithm	Block or Streaming	Block Size	Rounds	Key Size	Notes
RC4	Streaming	N/A	1	40-2048 bits	Used in WEP, SSL and TLS; largely deprecated in current technologies.

Rounds: Repeating the XOR/left-shift iteration X times.

Block modes

- **ECB** - Eletronic Code Block *(deprecated because nowdays is a week method that always produces the same output results with same input)*

All block modes below uses IV, which ensures the output block is uniquely different

- **CBC** - Cipher Block Chaining
- **CFB** - Cipher Feedback
- **OFB** - Output Feedback
- **CTR** - Counter

*A **Binary Block** is a plaintext converted into 16-bit, 64-bit or 128-bit binary ciphertext.*

Asymmetric Algorithms

RSA

Rivest Shamir and Edelman - Asymmetric algorithm, **generates the private and public key**.

ECC

Elliptic Curve Cryptography - Can create a smaller key than RSA, provides the same security with increased performance (more faster).

Diffie-Hellman

- **Does not** use Public or Private keys
- Uses key exchange protocol
- Diffie Hellman groups help by defining the size or type of key structure to use:

Diffie Hellman Groups

Group	Size
Group 1	768-bit modulus
Group 2	1024-bit modulus
Group 5	1536-bit modulus
Group 14	2048 bit modulus
Group 19	256-bit elliptic curve

Group	Size
Group 20	384-bit elliptic curve
Group 21	521-bit elliptic curve

PGP - Pretty Good Privacy

Uses both asymmetric and symmetric keys for a wide variety of operations uses web-of-trust instead PKI.

PGP Certificates

- Symantec Corp.
    - Enterprise $olution
    - Encrypts Massa storage
    - Signing
    - Disk Encryption
    - BitLocker
    - FileVault
    - Enterprise Cloud Solutions
- OpenPGP
    - Free
    - Encrypted email
    - PKI Support
    - S/MIME
- GPG (GNU Privacy Guard)
    - Free Toolset
    - File and Disk encryption

Hashing

One-way encryption providing integrity.

Hash	Algo.
MD5	128 bit hash
SHA-1	160 bit hash

SHA-1 and MD5 has the same cryptographic flaws, that can cause hash collision.

SHA-2 Family

SHA-256 | minor version: SHA-224
SHA-512 | minor version: SHA-384

SHA-3

Uses a hash function called Keccack and has the same length of SHA-2.

SHA-1 and SHA-2 have been replaced by the latest iteration of SHA known as SHA-3.

RIPEMD

RACE Integrity Primitives Evaluation Message Digest.

- Not very common
- Open Standard
- 128, 168, 256, 320 bit digests

HMAC

Hash Message Authentication Code - Used in conjunction with symmetric key both to authenticate and verify integrity of the message.

- Provides message integrity
- Requires each side of the conversation to have the same key
- It is based on standard hashes (SHA-1, MD5, etc)

Steganography

The art of hide information inside the data (hide data within data), and can be encrypted.

Certificates and Trust

- Certificates include a public key and at least one digital signature.

Digital Signature

- To create a digital signature for a document, you hash the document using your private key. Others can verify your digital signature with your public key.

Web of Trust

- Web of Trust uses a web of mutually trusting peers.
- Requires a lots of maintenance

PKI - Public Key Infrastructure

Is a system consisting of hardware, software, policies and procedures that creates, manage, distributes, uses, store and revoke **DIGITAL CERTIFICATES.**

PKI is the way we do internet. Uses a hierarchical structure with root servers.

- Certificate Authority (CA): Issues the certificates (Verisign, Thawte, etc).

CRL - Certificate Revocation List

A list of serial numbers of certificates that have been revoked or are no longer valid, therefore should not be relied on.

- Downside it is slow and old.

OCSP - Online Certificate Status Protocol

Is a more modern version of CRL that are used today, have a better performance.

Common Types of Digital Certificates:

- **PKCS-7**: is a way to store certificates as individual files.
- **PKCS-12**: stores the certificates and the private keys as packages.
- **X.509**

Cryptographic Attacks

- Brute Force
- Dictionary Attack
- Rainbow Table (dictionary of hashes)
- Collision Attack
- Replay Attack

Salt

Salt is an arbitrary value, usually created by the application or OS storing passwords, added to the end of the password before it is hashed, making cracking harder.

Example:

```
> Password: 123456
> Salt (arbitrary): aksfle3t

> Concatenated with Salt: 123456aksfle3t

> Salted password (SHA-256):
02FCD2C88B089D2E1816070FFF8B80E13242264DA14233A57821CDAF4DDA45DF
```

Keystretching

Combine a very long salt and a huge number of hashing iterations to make cracking even more harder.

Two most popular Key derivation functions

- PBKDF2 (Password-Based Key Derivation Function 2) algorithm
- BCrypt algorithm

Example:

```
PBKDF2

Password:
123456

Hash:
rYoSDg62evyzhE1+lWBa9A==:YaeMu71c8KU3H0RYFPle0Q==

-------------------------

BCrypt

Password:
123456

Hash:
$2b$10$vES9mCPsE10//vOc1u01XeUVmJrZyHGMPaRfo39OIUoJ2g7iPtDnu
```

---

7) Testing the Infrastructure

Vulnerability Scanning Tools

- traceroute/tracert
- Advanced IP scanner
- Nmap
- MBSA - Microsoft Baseline Security Analyzer (determine the security state of a system by assessing missing security updates and less-secure security settings; report good information for vulnerability assessment)

Vulnerability Scanning Assessmentk

The purpose of Vulnerability Scanning is to identify vulnerabilities cause by lack of security controls, common misconfigurations, and so on.

Credential vs Non-credential Vulnerability Assessments

A **Credential Vulnerability Asssessment** basically means you've got usernames and passwords as a part of your assessment. **Non-credential** you don't touch on usernames and passwords on assessments.

Intrusive vs. Non-intrusive

Almost all vulnerability assessments are **non-intrusive**. Scanning systems, gather information and identifying vulnerabilities are different than corrupt the entire database.

Vulnerability Assessment Tools

- Nessus by Tenable
- Nexpose by Rapid7
- OpenVAS (Opensource)

Principles of Social Engineering

- **Authority**
  - Impersonate or imply a position of authority
- **Intimidation**
  - Frighten by threat
- **Consensus**
  - To convince of a general group agreement
- **Scarcity**
  - To describe a lack of something
- **Familiarity**
  - To imply a closer relationship
- **Trust**
  - To assure reliance on their honesty and integrity
- **Urgency**
  - To call for imediate action

Social Engineering Attacks

- **Phishing**
- **Spear Phishing** - Directed towards a specific person or company
- **Vishing** - Uses Voice calls/telephone system to get private information
- **Hoax** - Warns someone that something bad is happening when its not
- **Watering Hole Attack** - An attempt to infect websites that a group of end users would normally go to gain access to their information or network
- **Whaling** - Spear phishing tha targets senior management and executives
- **Tailgating** - *(i.e leave computer unlocked, door etc)*
- **Shoulder Surfing** 👀
- **Dumpster Diving**

Web Application Attacks

- **Common Log Format (CLF)** - Standard type of logs that every single type of web server generates.

```
127.0.0.1 - - [28/OCT/2012/13:12:44 - 0500] "GET /CertifiedHacker.png
HTTP/1.0" 200 42213
    |      |             |                    |
|     |
  HOST    IDENT     DATE & TIME            REQUEST
STATUS BYTES
```

IDENT - If the IdentityCheck directive is enabled and the client machine runs ident, then this is the identity information reported by the client.

GET - Request HTTP method command
STATUS - status, 200 = Everything is ok
BYTES - the number of bytes in the object returned to the client, excluding all HTTP headers.

Common Web Application Attacks

- **Cross-site scripting (XSS)** - Client-side script injected into trusted web site
- **XML injections** - Used to manipulate or compromise the logic of an XML application or service (i.e change the price of a product on ecommerce)

Attacking Applications

- **Code Injection**
- **Comand Injection**
- **SQL injection (queries)**
    - inner join
    - select from
    - insert into
- **LDAP injection (queries info)**
    - based on X.500 protocol
        - DC = Domain Component
        - OU = Organizational Unit
        - CN = Common Name
- **Buffer Overflow** - overflows the input directly to the memory
- **Integer Overflow** - overflow an input variable (i.e typing a large number on calculate forcing an error)

Applications Vulnerabilities

- **Race Condition**
- **Improper Input Handling**
- **Improper Error Handling**
- **Memory/buffer vulnerability**
    - Memory Leak
    - Integer Overflow
    - Buffer Overflow
- **Pointer deference**
- **Resource exhaustion**
- **Weak cipher suites and implementations**
- **DLL injection**

Pentesting / Penetration Testing

A penetration test will actually try to grab the data itself. A vulnerability assessment at no time will ever actually try to grab the data.

Pentesting Process

1. Reconnaissance
2. Scanning

3. Gaining Access
4. Maintaining Access
5. Expanding to other systems
6. Avoid Detection

Principles

- Authorization
    - Define the targets
    - Attack model
        - White box - have extensive knowledge about the target
        - Black box - attacker know nothing about the target
        - Gray box - somewhere between the two
- Discover Vulnerabilities
    - Reconnaissance
        - Passive Discovery
        - Semi-passive discovery
        - Active discovery
    - Try to get Information
- Exploit vulnerabilities
    - Pivotting
    - Persistance
    - Privilege Escalation

---

8) Incident Response & Forensics

Incident Response Process

Preparation

- The big plan
- Who's doing what
- Organize types of incidents that might happen

Reporting

- What reports go to whom?
- Escalation

Identification

- Recognize what incident has ocurred
- Report from users
- Check the monitoring tools you use
- Watch alerts and logs
- Assess the impact

- Define who's involved

Containment

- Mitigate the damage
- Stop the attack
- Segregate the network
- Shutdown the system
- Turn off a service

Eradication

- Remove the malware
- Close off vulnerabilities
- Add new controls

Recovery

- Restore from backups
- Pull from snapshots
- Hire replacemente personnel
- Monitor to ensure good operation

Documentation

- Document the incident
- What failed?
- What worked?

Incident Response Plan

CIRT-Cyber incident response team

- A group of people whose job is to response to all incident
- Full or part time - or both
- IT Security Team
- IT Department
- Human Resources
- Legal
- Public Relations

Document incident types / Category definitions

- Physical access
- Malware Phishing
- Social engineering
- Data access

Roles and Responsabilities

- Users

- Help Desk
- Human Resources
- Database manager
- Incident Hotline
- IR manager/ IR officer
- IR team

Reporting Requirements / Escalation

- Determine Severity
- Based on severity have a clear chain of escalation
- Informing law enforcement

Practice

- Annual scenario drills

Digital Forensics

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.

Chain of Custody

The whole idea of hcina of custody is to show good integrity of the evidence itself.

- Gathering Evidence - data is of high integrity

Chain of Custody Process

1. Define the Evidence
2. Document collection method
3. Data/time collected
4. Person(s) handling the evidence
5. Function of person handling evidence (qualified person)
6. All locations of the evidence (i.e inital collection, moved to law enforcement...)

Order of Volatility

*The order of volatility is a process that **enumerates when, where, and how to gather the data/evidence before the data changes or disappears**.*

- **Memory**
    - Caches
    - Routing tables
    - ARP tables
- **Data on the Disk**

    - Optical, flash drives
    - Cache files, temp files
    - Write blocks enabled tools
- **Remotely logged data**
    - Web site data
    - Remote file server logs
    - Backups
- **Backups**
    - Trends
    - Low volatility takes time to gather data

Forensic Data Acquisition

Checklist of issues you should consider when you're performing Digital Forensics.

1. Capture the system image
2. Netwrok traffic and logs
3. Capture video
    - Security cameras
    - Record time offset
4. Take Hashes
5. Take screenshots
6. Interview witnesses
7. Track man hours

Contingency Planning

Attempts to mitigate adverse incidents to preserve business continuity.

- How do we recover from a specific type of a disaster?
- What to do for keep the **Business Continuity** going?

Disaster Recovery - Evacuation Plan

- **Backup Sites**
    - **Cold site**
        - It takes weeks to bring online
        - Basic office spaces (i.e building, chairs, AC...)
        - No operational equipment
        - Cheapest recovery site
    - **Warm site**
        - It takes days to bring online
        - Operational equipment but little or no data
    - **Hot site**
        - It take hours to bring online
        - Real-time synchronization
        - Almost all data ready to go - often just a quick update
        - Very expensive

- **Distance & Location** - different backup sites
- **Internet requirements**
- **Housing & entertainment**
- **Legal Issues**

Order of Restoration

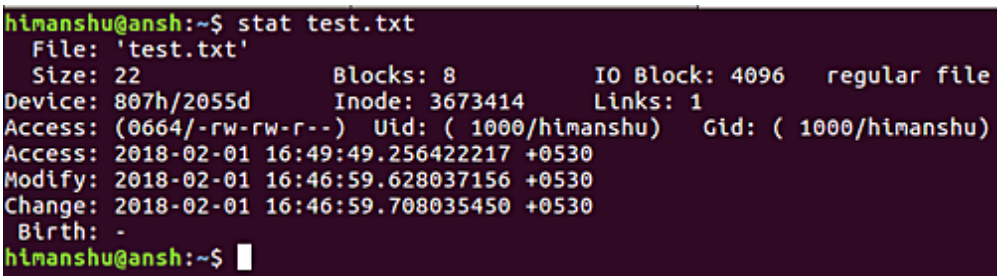
- Power
- Wired LAN (is open and running)
- ISP link (running)
- Active Directory/DNS/DHCP server (up and cooking)
- Account servers
- Sales and account workstations
- Production servers
- Production workstation
- Wireless access
- Peripherals (Printers, Camers, Scanners, faxes...)

Annual exercises
Failover - simpe means the process of making recovery site happen.
Alternative Processing Sites - different types of processing sites
Alternative business practices
After action reports - A clear and detailed documentation of everything that happened so that if it ever happens again you'll be ready to handle any form of business contingency planning.

🛑 Through planning and practice is what makes recovery plans successful when disasters occur

Backups

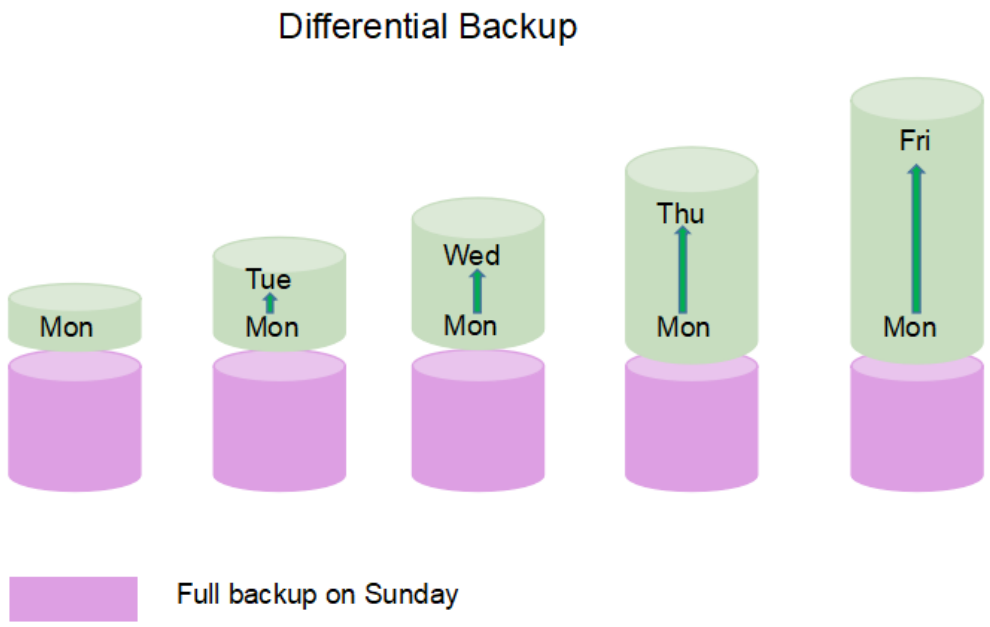
- `stat` **Linux** command - stat can return the status of an entire file system, the status of the first hard disk and so on.



- Archive attribute - **Windows** - if something is created or changed

Differential Backup

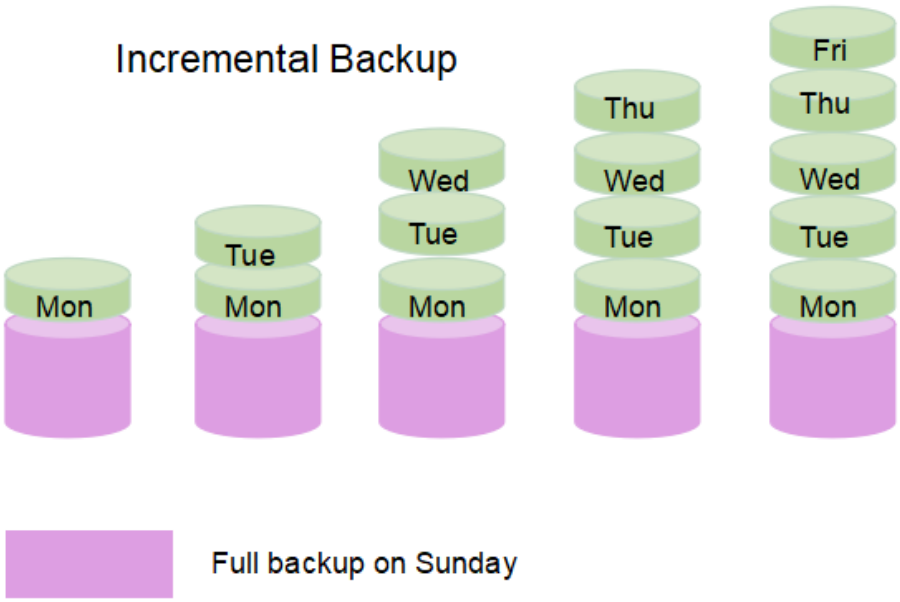
- Backup all the changes since the last full backup



- *Differential there are less backup sets but they get bigger.*

Incremental Backup

- Only backs up changes made from last backup



- *Incremental more backup sets but smaller.*

Snapshots

Snapshots typically under virtual machines and they are an absolute perfect way of making a copy of something that's happened in the past.

What Media

- External hard-drive
- Tape
- Cloud

Offsite Backup

Remote backup is good for disasters in general.

Cloud Backup

Cloud backups work beautifully, however, they have one big downside and that is they take up a tremendous amount of time to get the initial backups going.

List of Common Ports

Port	Description
20	File Transfer Protocol - FTP Data
21	File Transfer Protocol - FTP Control
22	SSH - Secure Shell Remote Login Protocol / SCP / SFTP
23	Telnet
25	SMNTP - Simple Mail Transfer Protocol
49	TACACS+ - Login Host Protocol
53	DNS - Domain Name System
67	DHCP - Bootp-server (Outgoing DHCP)
68	DHCP - Bootp-client (Incoming DHCP)
69	TFTP - Trivial File Transfer Protocol
80	HTTP
88	Kerberos - Secure Encrypted Login
110	POP3 - Post Office Protocol (Email)
119	NNTP - Network News Transfer Protocol
123	NTP - Network Time Protocol
137, 138, 139	NETBios Protocol
143	IMAP 4 - Internet Message Access Protocol (Email)
161, 162	SNMP - Simple Network Management Protocol
389	LDAP - Lightweight Directory Access Protocol
443	HTTPS - HTTP over TLS/SSL
445	SMB
464	Kerberos

Port	Description
465	SMTP/SMTPS over SSL
500	ISAKMP - Internet Security Association and Key Management Protocol - IPSec
514, 6514	SysLog Servers & SysLog TCP over TLS
636	LDAP over SSL
860	iSCSI - Internet Small Computer Systems Interface
993	IMAP 4S - IMAP over TLS/SSL (Email)
995	POP3 over SSL
989, 990	FTP - FTP Data and Control over TLS/SSL
1194	OpenVPN
1645, 1646	RADIUS
1812, 1813	RADIUS
1701	L2TP - Layer 2 Tunneling Protocol (IPSec - used in VPN)
1723	PPTP - Point-to-Point Tunneling Protocol - VPN
3389	RDP - Remote Desktop Protocol
5060, 5061	SIP - Session Initiation Protocol