اقرأ باسم ربك

جامعة الملك عبدالعزيز

King Abdulaziz University

CYBERSECURITY

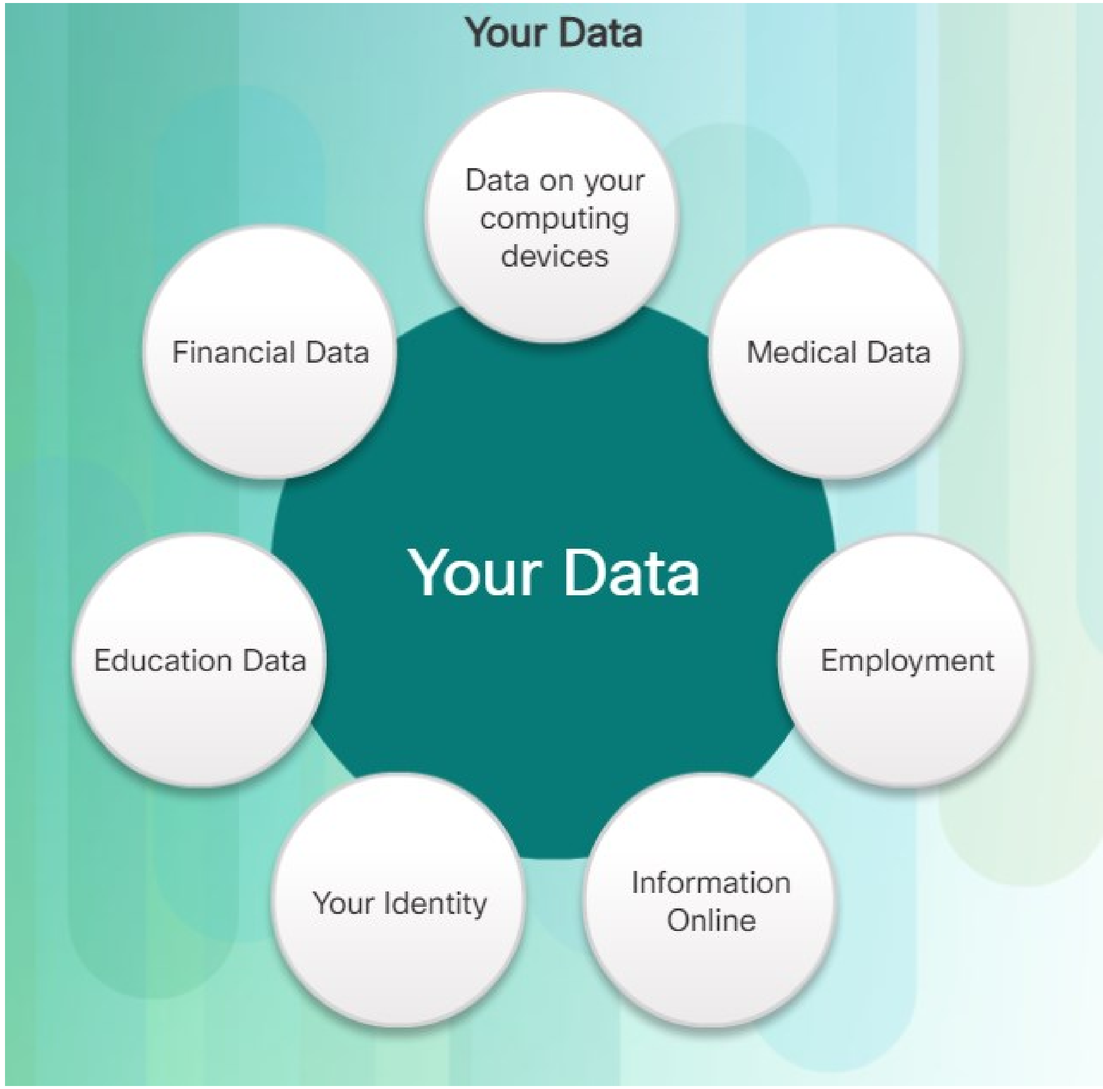
Prof. Yasser Mostafa Kadah – www.k-space.org

What is Cybersecurity?

- Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm
- On a personal level, you need to safeguard your identity, your data, and your computing devices
  - Online vs. offline identity
  - You should take care when choosing a username or alias for your online identity
  - Username should not include any personal information. It should be something appropriate and respectful. This username should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.
- At the corporate level, it is everyone's responsibility to protect the organization's reputation, data, and customers
- At the state level, national security, and the safety and well-being of the citizens are at stake.

Your Data: Medical Records as Example

- Every time you go to the doctor's office, more information is added to your EHR
  - Prescription from your family doctor, physical health, mental health, medical history, family information
- Medical devices, such as fitness bands, use cloud platform for transfer, storage and display of clinical data like heart rate, blood pressure and blood sugar
  - Enormous amount of clinical data that could become part of EHR



Targets

- Your online credentials are valuable to give thieves access to your accounts for profit
- Long-term profits can be made through stealing personal identity
  - As medical costs rise, medical identity theft is also on rise where identity thieves can steal medical insurance identity and use its medical benefits for themselves

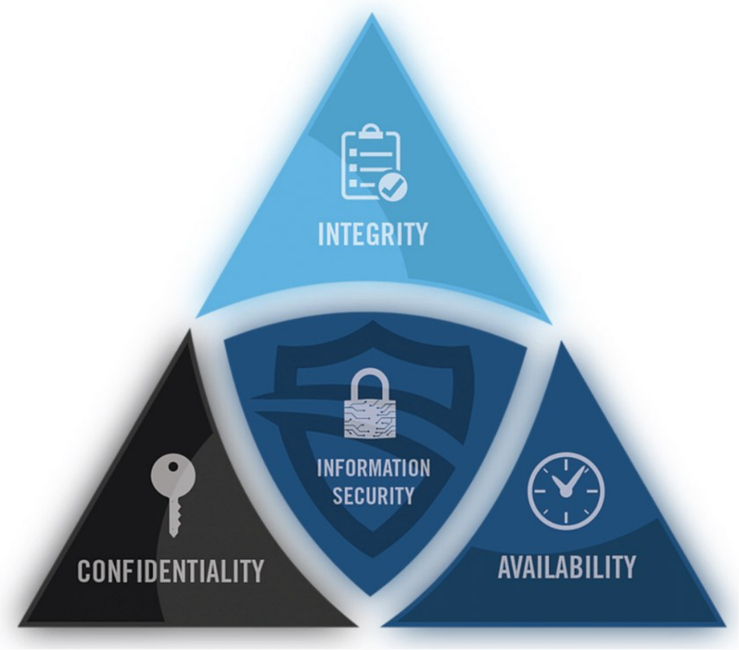
Types of Data

- Traditional Data
  - Corporate data includes personnel information, intellectual properties, and financial data. The personnel information includes application materials, payroll, offer letters, employee agreements, and any information used in making employment decisions. Intellectual property, such as patents, trademarks and new product plans, allows a business to gain economic advantage over its competitors. This intellectual property can be considered a trade secret; losing this information can be disastrous for the future of the company. The financial data, such as income statements, balance sheets, and cash flow statements of a company gives insight into the health of the company.

- Internet of Things and Big Data
  - With the emergence of the Internet of Things (IoT), there is a lot more data to manage and secure. IoT is a large network of physical objects, such as sensors and equipment that extend beyond the traditional computer network.

Information Security Guideline: CIA Triad

- Confidentiality, integrity and availability, known as the CIA triad is a guideline for information security for an organization
  - Confidentiality ensures the privacy of data by restricting access through authentication encryption
  - Integrity assures that the information is accurate and trustworthy
  - Availability ensures that the information is accessible to authorized people



Types of Attackers

- Amateurs (script kiddies)
  - Attackers with little or no skill, often using existing tools or instructions found on Internet to launch attacks
    - Some of them just curious, while others trying to demonstrate their skills and cause harm (even with basic tools, still devastating)
- Hackers
  - White hat attackers discover weaknesses so that security of these systems can be improved
  - Black hat attackers take advantage of any vulnerability for illegal personal, financial or political gain
  - Gray hat attackers are somewhere between white and black hat attackers
- Organized Hackers
  - Highly sophisticated and organized, and they may even provide cybercrime as service to other criminals
  - Hacktivists make political statements to create awareness to issues that are important to them
  - State-sponsored attackers gather intelligence or commit sabotage on behalf of their government

Script kiddie

White hat

Grey hat

Black hat

Hacktivist

State sponsored Hacker

Finding Security Vulnerabilities

- Security vulnerabilities are any kind of software or hardware defect that can be exploited by malicious users to exploit it
  - Exploit: term used to describe a program written to take advantage of a known vulnerability
  - Attack: act of using an exploit against a vulnerability
  - Goal of attack: gain access to a system, data it hosts or to specific resource
- Software vulnerabilities result from errors in operating system or application codes
  - Goal of software updates is to stay current and avoid exploitation of vulnerabilities
- Hardware vulnerabilities are often introduced by hardware design flaws
  - Specific to device models and not generally exploited through random compromising attempts

Categorizing Software Security Vulnerabilities

- Buffer overflow – data are written beyond the limits of a buffer allocated to an application
  - By changing data beyond the boundaries of a buffer, application accesses memory allocated to other processes and can lead to system crash, data compromise, or provide escalation of privileges
- Non-validated input – data coming into the program could have malicious content
  - Force program to behave in an unintended way (for example, allocation of buffers of incorrect and unexpected sizes)
- Race conditions – output of an event depends on ordered or timed outputs
  - For example, multiprocessor computer accessing/changing same memory location by different processors
- Weaknesses in security practices – improper authentication, authorization, and encryption
  - Developers should not attempt to create their own security algorithms because it will likely introduce vulnerabilities and should use security libraries that have already created, tested, and verified
- Access-control problems – process of controlling who does what
  - Ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it,
  - Many security vulnerabilities are created by the improper use of access controls

Physical Access

- Nearly all access controls and security practices can be overcome if the attacker has physical access to target equipment
- For example, no matter what you set a file’s permissions to, the operating system cannot prevent someone from bypassing the operating system and reading the data directly off the disk
- To protect the machine and the data it contains, physical access must be restricted and encryption techniques must be used to protect data from being stolen or corrupted

Types of Malicious Software (Malware)

- Malware is any code that can be used to steal data, bypass access controls, or cause harm to, or compromise a system
- Spyware: malware designed to track and spy on the user (activity trackers, keystroke collection, and data capture)
  - Modifies security settings and often bundles itself with legitimate software or with Trojan horses
- Adware – Advertising supported software is designed to automatically deliver advertisements
  - Some adware is designed to only deliver advertisements but it is also common for adware to come with spyware
- Bot (robot) – malware designed to automatically perform action, usually online
  - Malicious bots are botnets where several computers are infected with bots programmed to quietly wait for commands provided by attacker
- Ransomware – malware designed to hold a computer system or the data it contains captive until a payment is made
  - Works by encrypting data in the computer with a key unknown to user or taking advantage of specific system vulnerabilities to lock down the system
  - Ransomware is spread by a downloaded file or some software vulnerability

Types of Malicious Software (Malware)

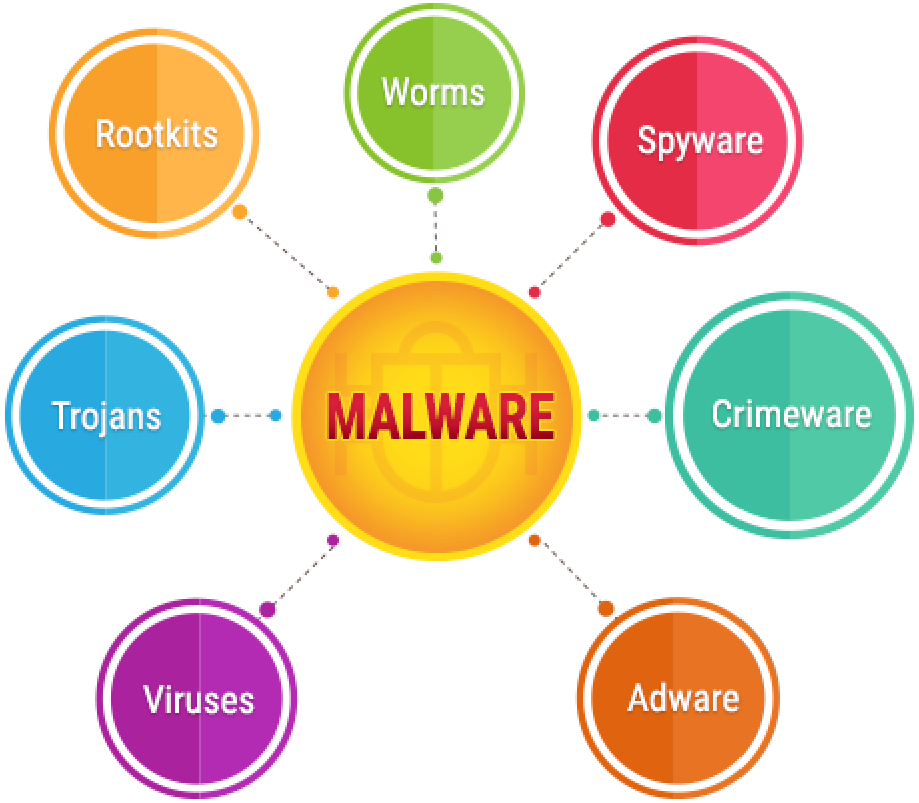
- Virus – malicious executable code that is attached to other executable legitimate programs
  - Most viruses require end-user activation and can activate at a specific time or date
  - Viruses can be destructive, such as those that modify or delete data
  - Viruses can also be programmed to mutate to avoid detection
  - Most viruses are now spread by USB drives, optical disks, network shares, or email
- Trojan horse - malware that carries out malicious operations under guise of desired operation
  - Malicious code exploits the privileges of user that runs it
  - Often, Trojans are found in image files, audio files or games (differs from virus because it binds itself to non-executable files)
- Worms – malicious codes that replicate themselves by independently exploiting vulnerabilities in networks
  - Whereas a virus requires a host program to run, worms can run by themselves and slow down networks
  - Other than the initial infection of a host, worm is able to spread very quickly over the network
  - Worms share similar patterns, an enabling vulnerability, a way to propagate themselves, and they all contain a payload
  - Responsible for some of the most devastating attacks on the Internet (e.g., Code Red work in 2001)

Types of Malicious Software (Malware)

- Man-In-The-Middle (MitM) – allows attacker to take control over device without user’s knowledge
  - With that access, attacker can intercept and capture user information before relaying it to its intended destination
  - Many malwares exist to provide attackers with MitM capabilities, widely used to steal financial information
- Man-In-The-Mobile (MitMo) – A variation of MitM used to take control over a mobile device
  - When infected, mobile device can be instructed to exfiltrate user-sensitive information and send it to the attackers
  - ZeuS, an example MitMo, allows attackers quietly to capture 2-step verification SMS messages sent to users.
- Scareware – malware designed to persuade the user to take a specific action based on fear
  - Scareware forges pop-up windows that resemble operating system dialogue windows that convey forged messages stating the system is at risk or needs the execution of a specific program to return to normal operation
  - If the user agrees and clears the mentioned program to execute, his or her system will be infected with malware
- Rootkit – malware designed to modify operating system to create backdoor
  - Attackers then use the backdoor to access the computer remotely
  - Most rootkits take advantage of software vulnerabilities to perform privilege escalation and modify system files
  - Common for rootkits to modify system forensics and monitoring tools, making them very hard to detect
  - Often, computer infected by rootkit must be wiped and reinstalled

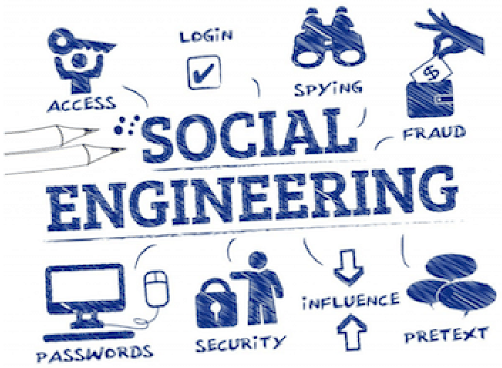
Symptoms of Malware

- Regardless of the type of malware a system has been infected with, these are common malware symptoms:
  - There is an increase in CPU usage
  - There is a decrease in computer speed
  - The computer freezes or crashes often
  - There is a decrease in Web browsing speed
  - There are unexplainable problems with network connections
  - Files are modified
  - Files are deleted
  - There is a presence of unknown files, programs, or desktop icons
  - There are unknown processes running
  - Programs are turning off or reconfiguring themselves
  - Email is being sent without the user's knowledge or consent



Social engineering

- Access attack that attempts to manipulate individuals into performing actions or divulging confidential information
  - Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses
  - Attacker calls authorized employee with urgent problem that requires immediate network access
  - Attacker appeals to employee's vanity or greed, or invoke authority using name-dropping techniques
- Several types of social engineering attacks
  - Pretexting: attacker calls individuals and lies to them in attempt to gain access to privileged data (e.g., attacker pretending to need personal or financial data in order to confirm identity of recipient)
  - Tailgating: attacker quickly follows authorized person into secure location to gain physical access
  - Something for Something (quid pro quo): attacker requests information in exchange for something, like a gift



Password Cracking

- Social engineering
  - Attacker manipulates a person who knows the password into providing it
- Brute-force attacks
  - Attacker tries several possible passwords in an attempt to guess the password
  - Example: if password is 4-digit number, attacker would have to try every one of 10000 combinations
  - Brute-force attacks usually involve word-list file containing list of words taken from a dictionary and try each word and common combinations
  - Because brute-force attacks take time, complex passwords take much longer to guess
- Network sniffing
  - By listening and capturing packets sent on the network, attacker may be able to discover password if it is being sent unencrypted (in plain text) or using a password cracking tool if encrypted

Phishing

- Malicious party sends fraudulent email disguised as being from legitimate, trusted source
  - Message intent is to trick the recipient into installing malware on their device, or into sharing personal or financial information
  - Example: email forged to look like it was sent by retail store asking the user to click link to claim prize where link may go to fake site asking for personal information, or install a virus

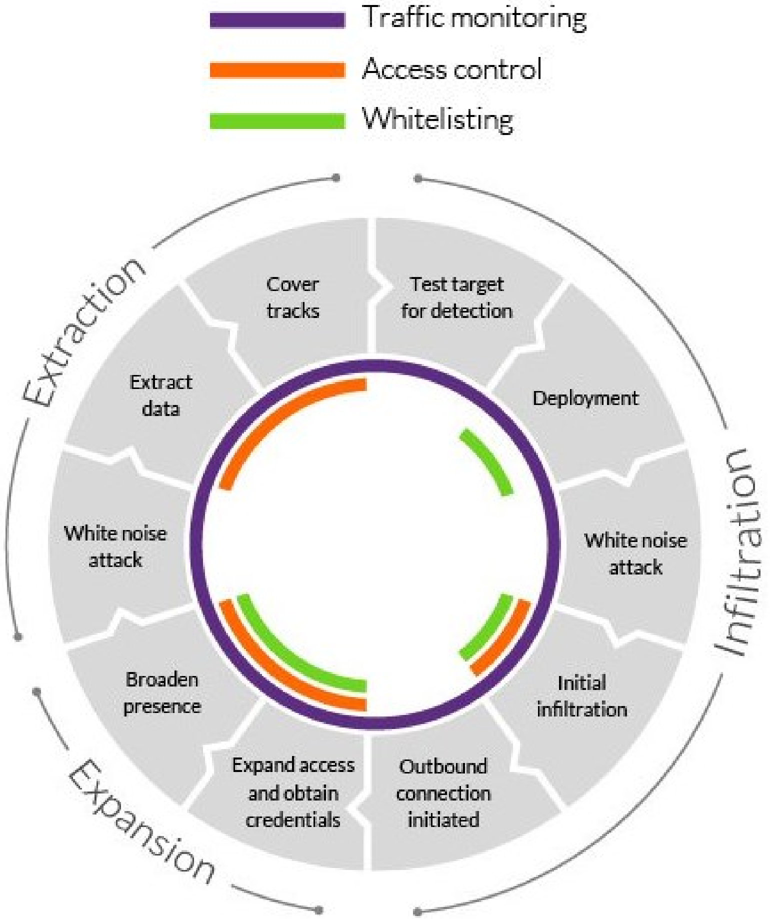
- Spear phishing is highly targeted phishing attack
  - While phishing and spear phishing both use emails to reach the victims, spear phishing emails are customized to specific person where attacker researches target's interests before sending email
  - Example: attacker learns target person is interested in cars and looking to buy specific model of car and joins same car discussion forum where target is member, forges car sale offering and sends email to the target that contains link for pictures of car that installs malware when clicked

Vulnerability Exploitation

- Step 1. Gather information about the target system
  - This could be done in many different ways such as port scanner or social engineering where goal is to learn as much as possible about target computer
- Step 2. One of the pieces of relevant information learned in step 1 might be the operating system, its version, and a list of services running on it
- Step 3. When the target's operating system and version is known, the attacker looks for any known vulnerabilities specific to that version of OS or other OS services
- Step 4. When a vulnerability is found, the attacker looks for a previously written exploit to use. If no exploits have been written, the attacker may consider writing an exploit
- Example: attacker using whois, a public Internet database containing information about domain names and their registrants, then uses nmap tool, a popular port scanner, to probe ports of target computer to learn about which services are running on that computer

Advanced Persistent Threats (APTs)

- They consist of multi-phase, long term, stealthy and advanced operation against specific target
- APT is well funded (complexity and skill level required)
  - Target organizations or nations for business or political reasons
- Usually related to network-based espionage, APT's purpose is to deploy customized malware on one or multiple of target's systems and remain undetected
- With multiple phases of operation and several customized types of malware that affect different devices and perform specific functions, individual attacker often lacks skill-set, resources or persistence to carry out APTs

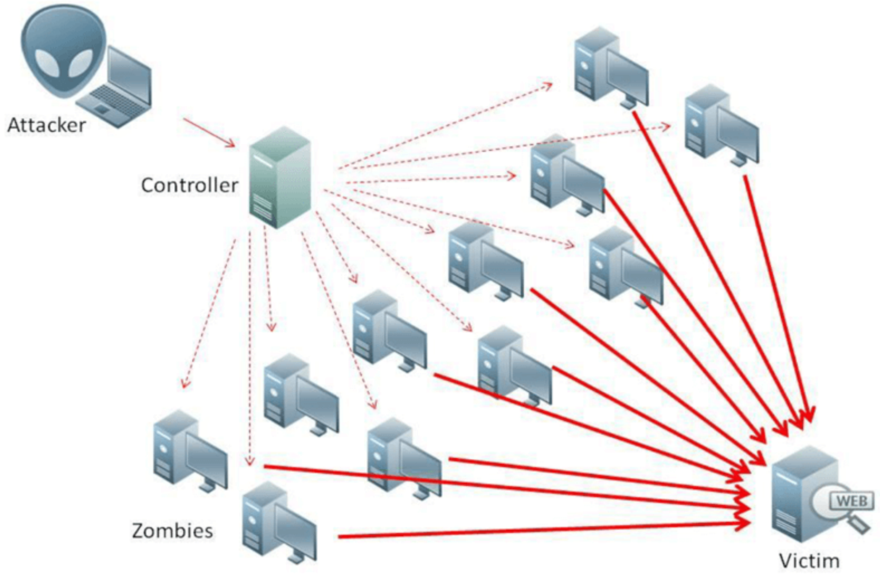


Denial-of-Service (DoS) Attack

- Type of network attack that results in some sort of interruption of network service to users, devices, or applications
- Two major types of DoS attacks
  - Overwhelming Quantity of Traffic: when network, host, or application is sent an enormous quantity of data at a rate which it cannot handle and causes slowdown in transmission or response, or crash of device or service
  - Maliciously Formatted Packets: when maliciously formatted packet is sent to host or application and receiver is unable to handle it, such as packets containing errors that cannot be identified by application, and causes receiving device to run very slowly or crash
- DoS attacks are considered major risk because they can easily interrupt communication and cause significant loss of time and money and they are relatively simple to conduct, even by unskilled attacker

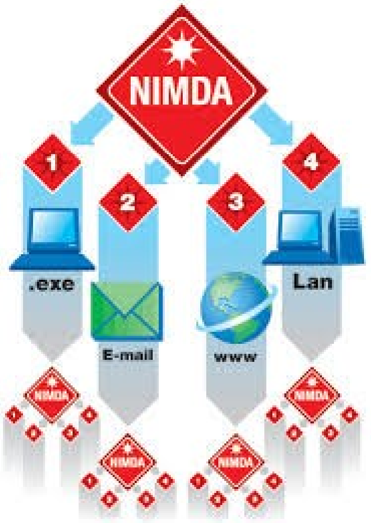
Distributed Denial-of-Service (DDoS) Attack

- Similar to DoS attack but originates from multiple, coordinated sources
- As an example, a DDoS attack could proceed as follows:
  - An attacker builds network of infected hosts, called botnet
  - Infected hosts are called zombies and are controlled by handler systems
  - Zombie computers constantly scan and infect more hosts, creating more zombies
  - When ready, hacker instructs handler systems to make botnet of zombies carry out DDoS attack.



Blended Attack

- Attacks that use multiple techniques to compromise a target
  - By using several different attack techniques at once, attackers have a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes, revealing more complex malware
- Most common type of blended attack uses spam email messages, instant messages or legitimate websites to distribute links where malware is secretly downloaded to computer
- Another common blended attack uses DDoS combined with phishing emails
  - First, DDoS is used to take down a popular bank website and send emails to the bank's customers, apologizing for the inconvenience and directing users to a forged emergency site where their real login information can be stolen
- Many of the most damaging computer worms are better categorized as blended
  - Nimbda worm used email attachments, file downloads from compromised web server, and Microsoft file sharing (e.g., anonymous shares) as propagation methods



Data Breach Impact Reduction

- No set of security practices is 100% efficient and breach is likely to happen
  - Companies and organizations must also be prepared to contain the damage
  - Impact of a breach is not only related to technical aspects, stolen data, damaged databases, or damage to intellectual property, but also damage extends to the company's reputation
- Responding to data breach is a very dynamic process with several important measures
  - Communicate the issue to employees and customers to create transparency, which is crucial in this case
  - Be sincere and accountable in case the organization is at fault
  - Provide details and explain why the situation took place and what was compromised and also take care of the costs of identity theft protection services for affected customers
  - Understand what caused and facilitated the breach including, if necessary, hiring forensics experts
  - Apply what was learned from forensics investigation to ensure similar breaches do not happen again
  - Ensure all systems are clean, no backdoors were installed, and nothing else has been compromised
  - Educate employees, partners, and customers on how to prevent future breaches

Protecting Your Computing Devices

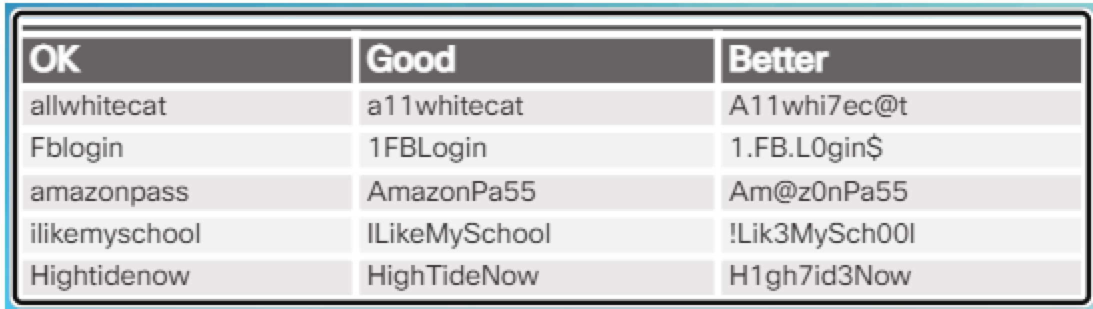
- Keep the Firewall On
  - Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your personal or company data
- Use Antivirus and Antispyware
  - Antivirus software is designed to scan your computer and incoming email for viruses and delete them
- Manage Your Operating System and Browser
  - Hackers are always trying to take advantage of vulnerabilities in operating systems and web browsers
  - Set the security settings on your computer and browser at medium or higher and update operating system including your web browsers and regularly download and install the latest software patches and security updates from the vendors
- Protect All Your Devices
  - All computing devices should be password protected to prevent unauthorized access and stored information should be encrypted
  - If any one of your devices is compromised, criminals may have access to all your data through your cloud-storage such as Google drive
- IoT devices pose an even greater risk than your other computing devices
  - If vulnerabilities are found in firmware, the IoT device is likely to stay vulnerable because they do not receive updates
  - Often designed to have internet access through customer's local network, which makes them very likely to be compromised to allow access to customer's local network and data (unless connected to isolated network for only IoT devices)

Using Wireless Networks Safely

- Wireless networks allow devices to connect to network by way of Service Set Identifier (SSID)
- Preset SSID and default password for the browser-based administrative interface should be changed
  - Hackers will be aware of this kind of default access information.
  - Optionally, wireless router can also be configured to not broadcast the SSID, which adds additional barrier to discover network
- Encrypt wireless communication by enabling wireless security and the WPA2 encryption feature on wireless router
- Use a trusted VPN service to prevent the unauthorized access to your data while using the wireless network
- Away from home, public Wi-Fi hot spot allows access to online information and surf the Internet
  - However, it is best to not access or send any sensitive personal information over public wireless network
  - Verify whether device is configured with file and media sharing and requires user authentication with encryption
  - To prevent someone from intercepting your information (known as “eavesdropping”) while using public wireless network, use encrypted VPN tunnels and services to make your information not decipherable even if a data transmission is intercepted
- Mobile devices with Bluetooth wireless protocol allows devices to connect and share information
  - Exploited by hackers to eavesdrop, establish remote access controls, distribute malware, and drain batteries

Password Guidelines

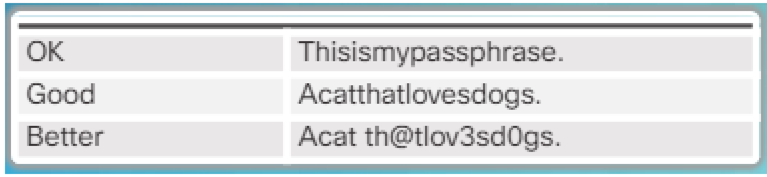
- Using unique and strong passwords for each online account to avoid being vulnerable to hacking
  - Using the same password for all online accounts is like using same key for all your locked doors, if an attacker was to get your key, he would have the ability to access everything you own
  - If criminals get your password through phishing for example, they will try to get into your other online accounts
  - If you only use one password for all accounts, they can get into all your accounts, steal or erase all your data, or decide to impersonate you.
- Problem: many online accounts with many passwords may be too much to remember
  - One solution to avoid reusing passwords or using weak passwords is to use a password manager.
  - Password manager stores and encrypts all your different and complex passwords and then helps you to log into your online accounts automatically with one master password to access password manager
- Tips for choosing a good password:
  - Do not use dictionary words or names in any languages
  - Do not use common misspellings of dictionary words
  - Do not use computer names or account names
  - If possible, use special characters, such as ! @ # $ % ^ & * ( )
  - Use a password with ten or more characters



OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

Using Passphrase Rather Than Password

- Easier to create long passphrase than password, because it is in form of sentence rather than word
  - The longer length makes passphrases less vulnerable to dictionary or brute force attacks, and easier to remember
- Tips in choosing a good passphrase:
  - Choose a meaningful statement to you
  - Add special characters, such as ! @ # $ % ^ & * ( )
  - The longer the better
  - Avoid common or famous statements, for example, lyrics from a popular song

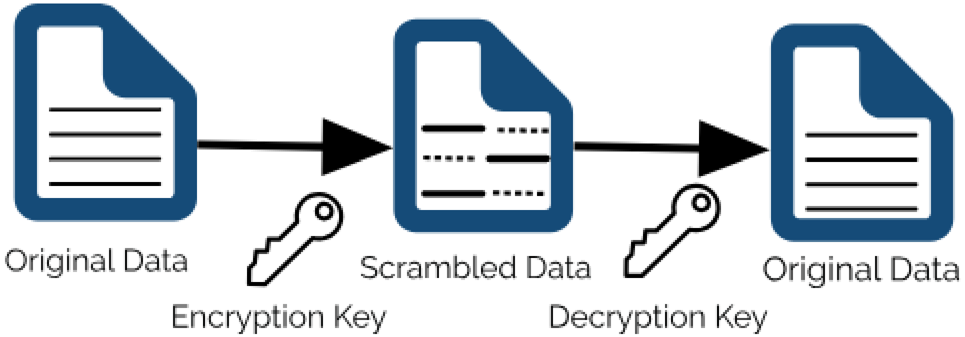


OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

- Improved password guidelines from National Institute for Standards and Technology (NIST)
  - 8 characters minimum in length, but no more than 64 characters
  - No common, easily guessed passwords, such as password, abc123
  - No composition rules, such as having to include lowercase and uppercase letters and numbers
  - Improve typing accuracy by allowing the user to see the password while typing
  - All printing characters and spaces are allowed
  - No password hints
  - No periodical or arbitrary password expiration
  - No knowledge-based authentication, such as information from secret questions, marketing data, transaction history

Data Encryption

- Encryption is process of converting information into form that unauthorized party cannot access or read
  - Only trusted, authorized person with secret key can decrypt data and access it in its original form
  - Encryption itself does not prevent someone from intercepting the data but can only prevent unauthorized access of contents
- Malicious applications may infect your computer or mobile device and steals potentially valuable information, such as account numbers and passwords, and other official documents
  - That kind of information can lead to identity theft, fraud, or ransom
- Software programs are used to encrypt files, folders, and even entire drives.
  - Encrypting File System (EFS) is Windows feature that is directly linked to a specific user account
  - Only user that encrypted data will be able to access it after it has been encrypted using EFS



Data Backup

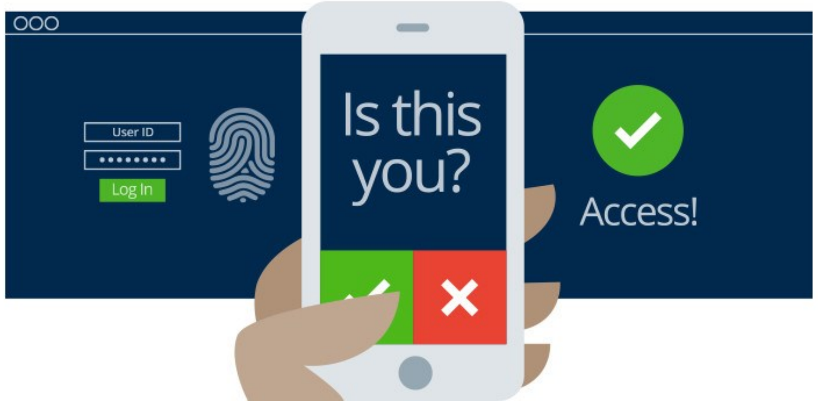
- Many ways where data may be lost
  - Erasing important data by mistake, hard drive failure, computers stolen
- Having backup may prevent loss of irreplaceable data
  - For proper backup, additional storage location is needed (on network, secondary location, or cloud)
  - Data must be copied to that location regularly and automatically
- By storing backup of data locally, you have total control of data
  - One can use network attached storage device (NAS), external hard drive, CDs/DVDs, or even tapes
  - Problem: you are totally responsible for cost and maintenance of storage device equipment
- If you subscribe to cloud storage service, cost depends on storage space needed
  - With cloud storage service, you have access to backup data as long as you have access to account
  - Need to be more selective about data being backed up due to cost of storage and data transfers
- Benefit of storing backup at alternate location is safety in event of fire, theft or other catastrophes other than storage device failure

Permanent Deletion of Data

- When you move file to trash and delete it permanently, file is only inaccessible from operating system
  - Anyone with right forensic tools can still recover file due to magnetic trace left on hard drive
- To erase data so that it is no longer recoverable, data must be overwritten with ones and zeroes multiple times
- To prevent recovery of deleted files, you may need to use tools specifically designed to do just that
  - SDelete from Microsoft, claims to have the ability to remove sensitive files completely
  - Shred for Linux and Secure Empty Trash for Mac OSX are some tools that claim to provide similar service
- Only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device
  - It has been the folly of many criminals in thinking their files were impenetrable or irrecoverable
- Besides storing data on your local hard drives, your data may also be stored online in the cloud
  - Those copies will also need to be deleted
- When you need to delete your data or get rid of hard drive or computer, make sure that you safeguarded data to keep them from falling into the wrong hands

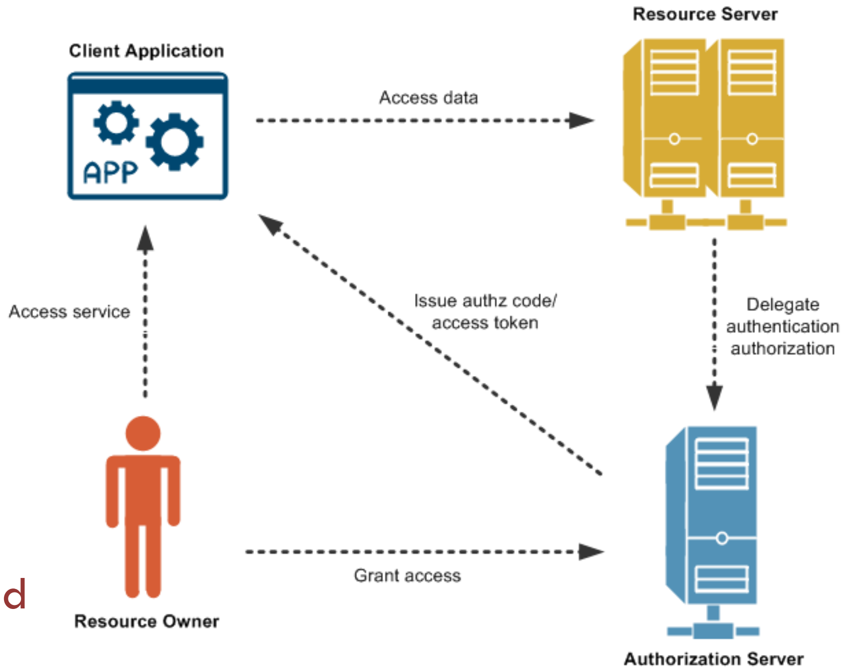
Two/Multiple Factor Authentication

- Popular online services use two or multiple factor authentication to add extra layer of security for account logins
- Besides the username and password, or personal identification number (PIN) or pattern, two factor authentication requires second token
  - Physical object - credit card, ATM card, phone, or fob
  - Biometric scan - fingerprint, palm print, as well as facial or voice recognition
- Even with two factor authentication, hackers can still gain access to your online accounts through attacks such as phishing attacks, malware, and social engineering



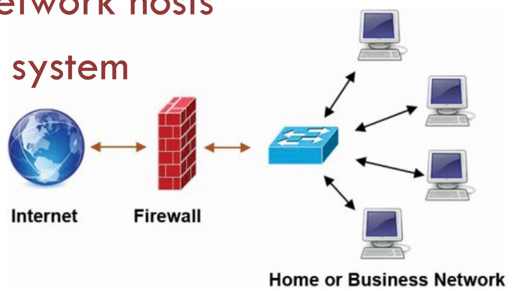
Open Authorization (OAuth)

- Open standard protocol that allows end user's credentials to access third party applications without exposing user's password
  - OAuth acts as middle man to to allow end users access to third party applications
- For example, say you want to access web application XYZ, and you do not have user account for accessing this web application but XYZ has option to allow you to log in using credentials from social media website ABC and so you access the website using social media login
  - For this to work, application 'XYZ' is registered with 'ABC' and is approved application
  - When accessing XYZ, you use user credentials for ABC then XYZ requests access token from ABC on your behalf
    - Access granted to XYZ without knowing your user credentials
    - Interaction is totally seamless for the user
  - Using secret tokens prevents malicious application from getting your information and your data



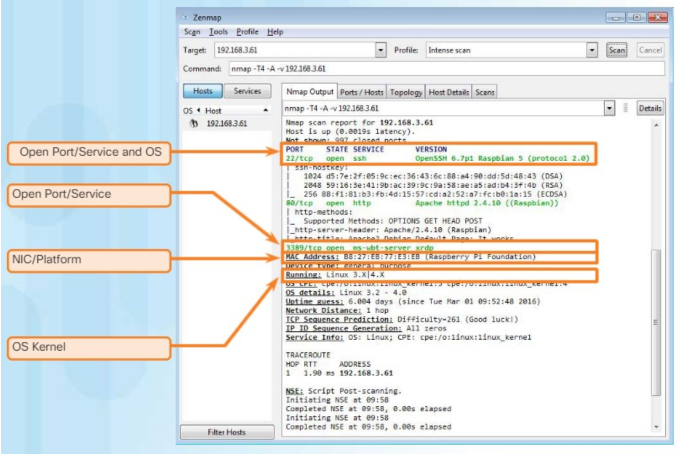
Firewall

- In computer networking context, firewall is designed to control, or filter, which communications are allowed in and which are allowed out of device or network
  - Can be installed on single computer with purpose of protecting that computer (host-based firewall)
  - Can be stand-alone network device that protects entire network of computers and all of the host devices on that network (network-based firewall)
- As computer and network attacks became more sophisticated, new types of firewalls were developed
  - Network Layer Firewall – filtering based on source and destination IP addresses
  - Transport Layer Firewall –filtering based on source and destination data ports, and based on connection states
  - Application Layer Firewall –filtering based on application, program or service
  - Context Aware Application Firewall – filtering based on the user, device, role, application type, and threat profile
  - Proxy Server – filtering of web content requests like URL, domain, media, etc.
  - Reverse Proxy Server – placed in front of web servers to protect, hide, offload, and distribute access to web servers
  - Network Address Translation (NAT) Firewall – hides or masquerades the private addresses of network hosts
  - Host-based Firewall – filtering of ports and system service calls on a single computer operating system



Port Scanning

- Process of probing a computer, server or other network host for open ports
  - In networking, each application running on device is assigned identifier called port number that is used on both ends of transmission so that right data is passed to correct application
- Port-scanning can be used maliciously as reconnaissance tool to identify operating system and services running on computer or host, or can be used harmlessly by network administrator to verify network security policies on network
- For the purposes of evaluating your own computer network's firewall and port security, you can use a port-scanning tool like Nmap to find all the open ports on your network
  - Port-scanning can be seen as a precursor to network attack and therefore should not be done on public servers on the Internet, or on company network without permission
- Nmap port-scan of computer on local network report any services that are running (e.g., web services, mail services, etc.) and port numbers with scanning of port generally resulting in one of three responses
  - Open or Accepted – The host replied indicating a service is listening on the port.
  - Closed, Denied, or Not Listening – The host replied indicating that connections will be denied to the port.
  - Filtered, Dropped, or Blocked – There was no reply from the host.
- Port-scan of network from outside runs against your firewall or router's public IP address
  - To discover your public IP address, use search engine such as Google with query "what is my ip address"



Target: 192.168.3.61 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.3.61

OS Host
192.168.3.61

nmap -T4 -A -v 192.168.3.61

```
Nmap scan report for 192.168.3.61
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE        VERSION
22/tcp   open  ssh            OpenSSH 6.7p1 Raspbian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 d5:7e:2f:05:9c:ec:36:43:6c:88:a4:90:dd:5d:48:43 (DSA)
|   2048 59:16:3e:41:9b:ac:39:9c:9a:58:ae:a5:ad:b4:3f:4b (RSA)
|_  256 88:f1:81:b3:fb:4d:15:57:cd:a2:52:a7:fc:b0:1a:15 (ECDSA)
80/tcp   open  http           Apache httpd 2.4.10 ((Raspbian))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.10 (Raspbian)
|_http-title: Apache2 Debian Default Page: It works
3389/tcp open  ms-wbt-server xrdp
MAC Address: B8:27:EB:77:E3:EB (Raspberry Pi Foundation)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Uptime guess: 6.004 days (since Tue Mar 01 09:52:48 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.90 ms 192.168.3.61

NSE: Script Post-scanning.
Initiating NSE at 09:58
Completed NSE at 09:58, 0.00s elapsed
Initiating NSE at 09:58
Completed NSE at 09:58, 0.00s elapsed
```

Security Appliances

- Today there is no single security appliance or piece of technology that will solve all network security needs
  - Because there is variety of security appliances and tools that need to be implemented, it is important that they all work together
  - Security appliances are most effective when they are part of a system.
- Security appliances can be stand-alone devices, like router or firewall, card that can be installed into network device, or module with its own processor and cached memory
- Security appliances can also be software tools that are run on network device
- Security appliances fall into these general categories
  - Routers - many firewall capabilities besides just routing functions, including traffic filtering, the ability to run an Intrusion Prevention System (IPS), encryption, and VPN capabilities for secure encrypted tunneling
  - Firewalls - all the capabilities of an ISR router as well as advanced network management and analytics
  - IPS - dedicated to intrusion prevention
  - VPN - server and client technologies designed for secure encrypted tunneling
  - Malware/Antivirus - comes in next generation routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers
  - Other Security Devices – web and email security appliances, decryption devices, client access control servers, and security management systems

Detecting Attacks in Real Time

- When hacker exploits flaw in piece of software before creator can fix it, it is known as a zero-day attack
- Due to sophistication and enormity of zero-day attacks found today, it is becoming common that network attacks will succeed and that successful defense is measured by how quickly network can respond to attack
  - Ideal goal: ability to detect attacks as they happen in real-time and stop attack immediately or within minutes
  - Unfortunately, many organizations are unable to detect attacks until days or even months after they occur
- Real Time Scanning from Edge to Endpoint
  - Detecting attacks in real time requires actively scanning for attacks using firewall and IDS/IPS network devices
  - Next generation client/server malware detection with connections to online global threat centers must also be used
  - Active scanning devices/software must detect network anomalies using context-based and behavior analyses
- DDoS Attacks and Real Time Response
  - Extremely difficult to defend against because attacks originate from hundreds or thousands of zombie hosts and attacks appear as legitimate traffic
  - Regularly occurring DDoS attacks cripple Internet servers and network availability and timely response is crucial

Protection Against Malware

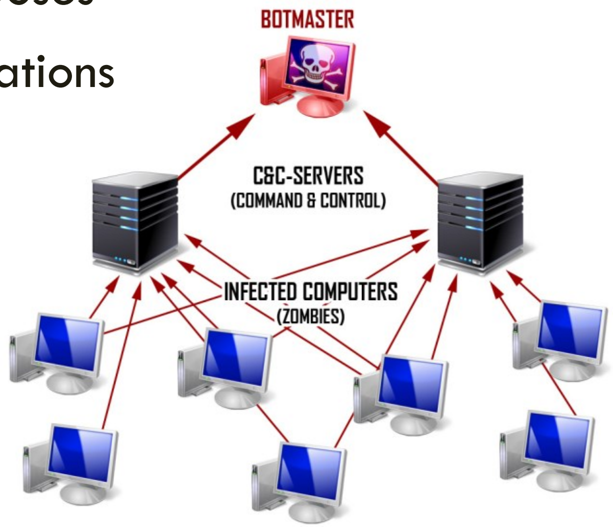
- To provide defense against the constant presence of zero-day attacks, as well as advanced persistent threats (APT) that steal data over long periods of time, one solution is to use an enterprise-level advanced malware detection solution that offers real-time malware detection
- Network administrators must constantly monitor the network for signs of malware or behaviors that reveal the presence of an APT
  - Cisco has an Advanced Malware Protection (AMP) Threat Grid that analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts
  - This provides global view of malware attacks, campaigns, and their distribution
  - AMP is client/server software deployed on host endpoints, as a standalone server, or on other network security devices

Cybersecurity Best Practices

- Many professional organizations published lists of security best practices
  - Perform Risk Assessment – Knowing the value of what you are protecting will help in justifying security expenditures.
  - Create a Security Policy – Create a policy that clearly outlines company rules, job duties, and expectations.
  - Physical Security Measures – Restrict access to networking closets, server locations, as well as fire suppression.
  - Human Resource Security Measures – Employees should be properly researched with background checks.
  - Perform and Test Backups – Perform regular backups and test data recovery from backups.
  - Maintain Security Patches and Updates – Regularly update server, client, and network device operating systems and programs.
  - Employ Access Controls – Configure user roles and privilege levels as well as strong user authentication.
  - Regularly Test Incident Response – Employ an incident response team and test emergency response scenarios.
  - Implement a Network Monitoring, Analytics and Management Tool - Choose a security monitoring solution that integrates with other technologies.
  - Implement Network Security Devices – Use next generation routers, firewalls, and other security appliances.
  - Implement a Comprehensive Endpoint Security Solution – Use enterprise level antimalware and antivirus software.
  - Educate Users – Educate users and employees in secure procedures.
  - Encrypt data – Encrypt all sensitive company data including email.

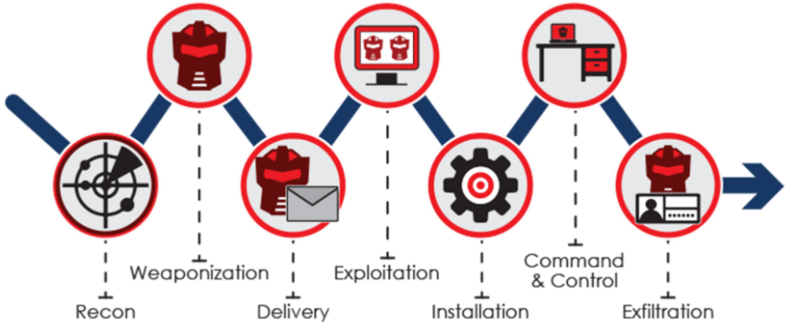
Botnet

- Botnet is group of bots, connected through the Internet, with the ability to be controlled by a malicious individual or group
  - Bot computer is typically infected by visiting website, opening an email attachment, or opening infected file
- Botnet can have tens of thousands, or even hundreds of thousands of bots
  - These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute force password attacks
  - Botnets are typically controlled through command and control server
- Cyber criminals often rent out Botnets for fee to third parties for nefarious purposes
- Botnet traffic filter can be used to inform global security community of their locations



Cyber Kill Chain

- Stages of cyber attack developed by Lockheed Martin as framework for incident detection and response
  - Stage 1. Reconnaissance - Attacker gathers information about the target
  - Stage 2. Weaponization - Attacker creates an exploit and malicious payload to send to the target
  - Stage 3. Delivery - Attacker sends the exploit and malicious payload to the target by email or other method
  - Stage 4. Exploitation - Exploit is executed
  - Stage 5 Installation - Malware and backdoors are installed on the target
  - Stage 6. Command and Control - Remote control of the target is gained through command-and-control channel or server
  - Stage 7. Action - Performing target malicious actions or execute more attacks on other devices from within network
- To defend against the Kill Chain, network security defenses are designed around stages of Kill Chain
  - Attack indicators at each stage of the Kill Chain
  - Security tools are needed to detect the attack indicators at each of the stages?
  - Gaps in the company’s ability to detect an attack?
- According to Lockheed Martin, understanding the stages of Kill Chain allowed them to put up defensive obstacles, slow down the attack, and ultimately prevent the loss of data

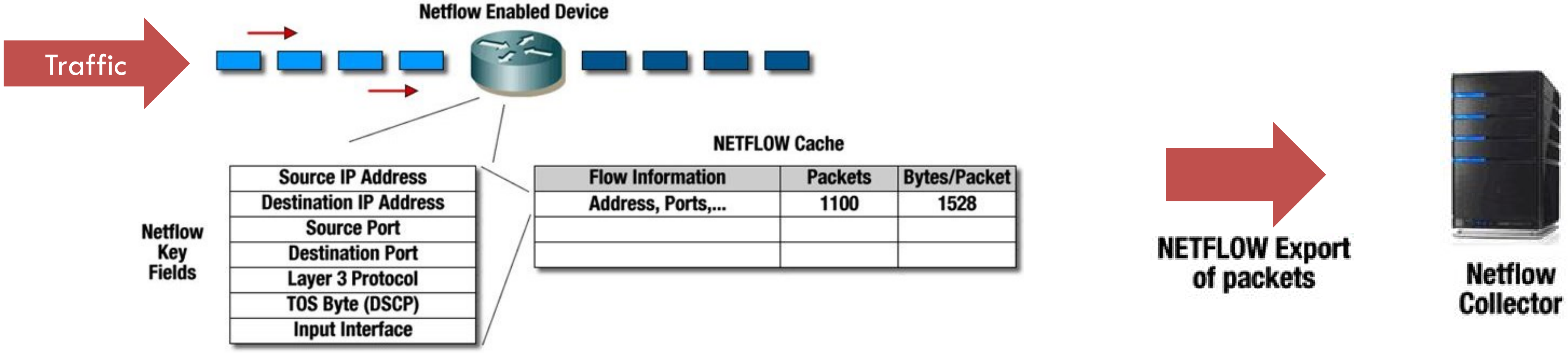


Behavior-Based Security

- Form of threat detection that does not rely on known malicious signatures, but instead uses informational context to detect anomalies in the network
  - Behavior-based detection involves capturing and analyzing flow of communication between user on local network and local, or remote destination
  - These communications, when captured and analyzed, reveal context and patterns of behavior which can be used to detect anomalies and can help discover presence of attack by change from normal behavior
- Honeypots is behavior-based detection tool that first lures attacker in by appealing to attacker's predicted pattern of malicious behavior, and then, when inside the honeypot, network administrator can capture, log, and analyze attacker's behavior
  - This allows administrator to gain more knowledge and build better defense
- Cisco's Cyber Threat Defense Solution Architecture is security architecture that uses behavior-based detection and indicators, to provide greater visibility, context, and control
  - Goal is to know who, what, where, when, and how attack is taking place and . This security architecture uses many security technologies to achieve this goal

NetFlow

- NetFlow technology is used to gather information about data flowing through network
  - Like phone bill for network traffic that shows who and what devices are in your network, as well as when and how users and devices accessed your network
  - NetFlow is an important component in behavior-based detection and analysis where switches, routers, and firewalls equipped with NetFlow can report information about data entering, leaving, and travelling through the network
  - Information is sent to NetFlow Collectors that collect, store, and analyze NetFlow records
  - NetFlow is able to collect information on usage through many different characteristics of how data is moved through the network to establish baseline behaviors on more than 90 different attributes.



Source IP Address
Destination IP Address
Source Port
Destination Port
Layer 3 Protocol
TOS Byte (DSCP)
Input Interface

Flow Information	Packets	Bytes/Packet
Address, Ports,...	1100	1528

Security Playbook

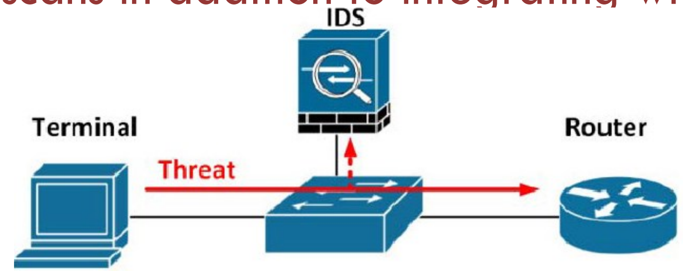
- Technology is constantly changing and this means cyberattacks are evolving too
  - New vulnerabilities and attack methods are discovered continuously and attacks are targeting critical networks and data
  - Organizations should have plans to prepare for, deal with, and recover from a breach
- The best way to prepare for a security breach is to prevent one
  - There should be guidance on identifying cybersecurity risks to systems, assets, data, and capabilities, protecting system by implementation of safeguards and personnel training, and detecting cybersecurity event as soon as possible
- When security breach is detected, appropriate actions should be taken to minimize its impact and damage
- After breach is contained and compromised systems and services are restored, security measures and processes should be updated to include lessons learned during breach and compiled into security playbook to accomplish several tasks
  - Detect malware infected machines
  - Detect suspicious network activity
  - Detect irregular authentication attempts
  - Describe and understand inbound and outbound traffic
  - Provide summary information including trends, statistics, and counts
  - Provide usable and quick access to statistics and metrics
  - Correlate events across all relevant data sources

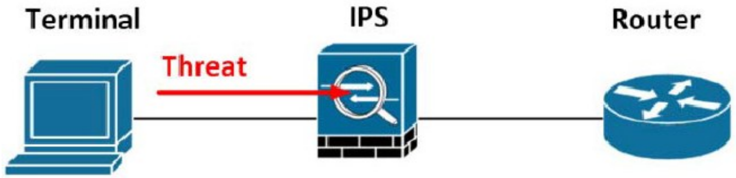
Tools for Incident Prevention and Detection

- SIEM – Security Information and Event Management (SIEM) system is software that collects and analyzes security alerts, logs and other real time and historical data from security devices on network
- DLP – Data Loss Prevention Software (DLP) is software or hardware system designed to stop sensitive data from being stolen from or escaping a network
  - Focus on file access authorization, data exchange, data copying, user activity monitoring, and more
  - Designed to monitor/protect data in three different states: data in-use, data in-motion and data at-rest
    - Data in-use focus on client, data in-motion refers to data as it travels through network, and data at-rest refers to data storage
- Cisco ISE and TrustSec – Cisco Identity Services Engine (Cisco ISE) and Cisco TrustSec enforce access to network resources by creating role-based access control policies that segment access to the network (guests, mobile users, employees) without added complexity
  - Traffic classification is based on user or device identity

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

- IDS is either dedicated network device, or one of several tools in server or firewall that scans data against a database of rules or attack signatures, looking for malicious traffic
  - If match is detected, IDS will log detection, and create an alert for network administrator
  - IDS does not take action when match is detected so it does not prevent attacks from happening
  - Job of the IDS is merely to detect, log and report
- Scanning performed by IDS slows down network (known as latency)
  - To prevent against network delay, IDS is usually placed offline, separate from regular network traffic
  - Data are copied or mirrored by switch and then forwarded to IDS for offline detection
  - IDS tools can be installed on top of host computer operating system, like Linux or Windows
- IPS has ability to block or deny traffic based on positive rule or signature match
  - Ability to perform real-time traffic and port analysis, logging, content searching and matching, and can detect probes, attacks, and port scans in addition to integrating with other tools for reporting, performance and log analysis





Legal Issues in Cybersecurity

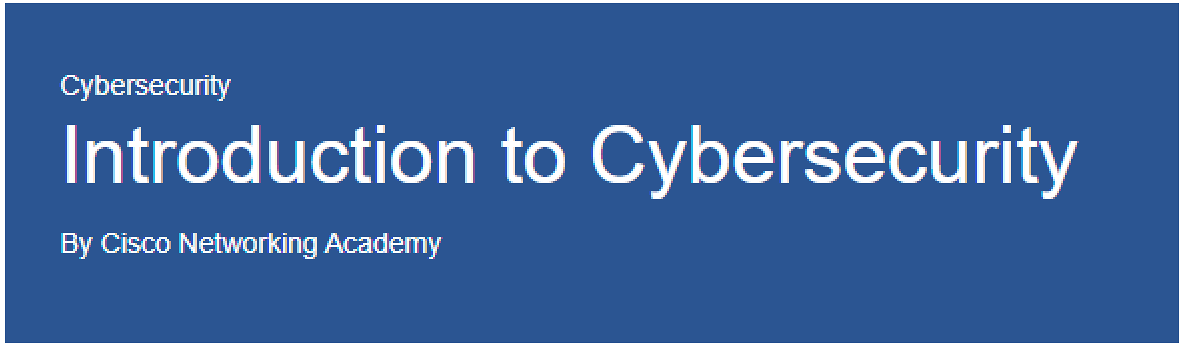
- Cybersecurity professionals must have same skills as hackers in order to protect against attacks
  - One difference between hacker and cybersecurity professional is that cybersecurity professional must work within legal boundaries
- Personal Legal Issues
  - You do not even have to be an employee to be subject to cybersecurity laws
  - In your private life, you may have opportunity and skills to hack another person's computer or network, but this is illegal
  - Most hackers leave tracks, whether they know it or not, and these tracks can be followed back to hacker
- Cybersecurity professionals develop many skills which can be used for good or evil
  - Those who use skills within legal system to protect infrastructure, networks, and privacy are always in high demand
- Corporate Legal Issues
  - Most countries have some cybersecurity laws in place that may have to do with critical infrastructure, networks, and corporate and individual privacy
  - Businesses are required to abide by cybersecurity laws
  - In some cases, if you break cybersecurity laws while doing your job, it is the company that may be punished and you could lose your job, while in other cases, you could be prosecuted, fined, and possibly sentenced
  - In general, if you are confused about whether an action or behavior might be illegal, consult legal department to assess your situation before you do something illegal

Ethical Issues in Cybersecurity

- In addition to working within the confines of the law, cybersecurity professionals must also demonstrate ethical behavior
- Personal Ethical Issues
  - A person may act unethically and not be subject to consequences because action may not have been technically illegal
  - This does not mean that such behavior is acceptable given that ethical behavior is fairly easy to ascertain
- Corporate Ethical Issues
  - There are many ethical areas in cybersecurity that are not covered by laws
  - Doing something that is technically legal still may not be ethical thing to do because so many areas of cybersecurity are not (or not yet) covered by laws.
- Many IT professional organizations developed codes of ethics for persons in the industry
  - CyberSecurity Institute (CSI), Information Systems Security Association (ISSA), andAssociation of Information Technology Professionals (AITP)

Reference

- https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity



Cybersecurity

Introduction to Cybersecurity

By Cisco Networking Academy