Table of Contents

Course 1 – Foundations of Cybersecurity | Instructor Toni

Week 1 – Welcome to the Exciting World of Cybersecurity

1. Cybersecurity (or security)
    a. The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.
2. Threat Actor- Any person or group who presents a security risk
3. Benefits of Cybersecurity
    a. Protects against external and internal threats
    b. Meets regulatory compliance
    c. Maintains and improves business productivity
    d. Reduces expenses
    e. Maintains brand trust
4. Common job titles
    a. Security analysts or specialist
    b. Cybersecurity analyst or specialist
    c. Security operations center (SOC) analyst
    d. Information security analyst
5. **Security Analysts** are responsible for monitoring and protecting information and systems
    a. Responsibilities
        i. Protecting computer and network systems
        ii. Installing prevention software
        iii. Conducting periodic security audits
6. Common Cybersecurity Terminology
    a. Compliance- process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches
    b. Security frameworks- guidelines used for building plans to help mitigate risks and threats to data and privacy
    c. Security controls- safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture
    d. Security posture- an organization's ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization
    e. Threat actor/Malicious attacker- any person or group who presents a security risk. This risk can relate to computer, applications, networks, and data
    f. Internal threat- a current or former employee, an external vendor, or a trust partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor *intentionally* engages in risky activities, such as unauthorized data access
    g. Network security- practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization's network
    h. Cloud security- the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of Cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud
    i. Programming- a process that can be used to create a specific set of instructions for a computer to execute tasks. They include:
        i. Automation of repetitive tasks

    ii. Reviewing web traffic
    iii. Alerting suspicious activity
7. **Transferable skills**- Skills from other areas that can apply to different careers
    a. Communication
    b. Problem-solving
    c. Time management
    d. Growth mindset
    e. Diverse perspectives
8. **Technical skills**- Skills that require knowledge of specific tools, procedures, and policies
    a. Programming languages
    b. Security information and event management (SIEM) tools
    c. Intrusion detection systems (IDSs)
    d. Threat landscape knowledge
    e. Incident response
9. **Personally Identifiable Information (PII)-** Any information used to infer an individual's identity
10. **Sensitive Personally Identifiable Information (SPII)-** A specific type of PII that falls under stricter handling guidelines
11. **Digital forensic investigator-** identify, analyze, and preserve criminal evidence within networks, computers, and electronic devices

Week 2 – The Evolution of Cybersecurity

1. **Computer virus-** Malicious code written to interfere with computer operations and cause damage to data and software
    a. Worm- a type of virus that can multiply on its own
    b. Brain Virus- Track illegal copies of medical software and prevent pirated licenses, infected the computer once the pirated software was inserted, spread globally over a couple of months
    c. Morris Worm- crawled the web, installed itself on computer, continued to re-install itself, costs millions of dollars in disruptions, **led to the development of computer emergency response teams commonly referred to as computer security incident response teams (CSIRTs).**
2. **Malware-** Software designed to harm devices or networks, primary purpose is to obtain money or an intelligence advantage that can be used against a person/organization/territory I.E. Love Letter- steal login credentials, "love letter for you", infected 45 million computers globally, social engineering attack
    a. Viruses: Malicious code written to interfere with computer operations and cause damage to data, software, and hardware. A virus attaches itself to programs or documents, on a computer. It then spreads and infects one or more computers in a network.
    b. Worms: Malware that can duplicate and spread itself across systems on its own.
    c. Ransomware: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
    d. Spyware: Malware that's used to gather and sell information without consent. Can be used to access devices. Allows threat actors to collect personal data such as private emails, texts, voice and image recordings, and locations.
3. **Social engineering-** A manipulation technique that exploits human error to gain private information, access, or valuables. Reasons for effectiveness:
    a. Authority: Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
    b. Intimidation: Threat actors use bullying tactics. Includes persuading and intimidating victims into doing what they're told.

   c. Consensus/Social proof: Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate.
   d. Scarcity: Used to imply that goods or services are in limited supply.
   e. Familiarity: Establish a fake emotional connection with users that can be exploited.
   f. Trust: Establish an emotional relationship with users that can be exploited over time. Use this relationship to develop trust and gain personal information.
   g. Urgency: Persuades others to respond quickly and without questioning.
4. **Phishing-** The use of digital communications to trick people into revealing sensitive data or deploying malicious software
   a. Business Email Compromise (BEC): A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
   b. Spear phishing: A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
   c. Whaling: A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
   d. Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
   e. Smishing: The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.
5. Equifax Breach
   a. 2017
   b. Credit report agency
   c. Over 143 million customer records were stolen, and the breach affected approximately 40% of all Americans
      i. PII, SSN, Birthdates, Driver's License #'s
6. Introduction to the eight CISSP security domains
   a. Security and Risk Management
      i. Defines security goals and objectives, risk mitigation, compliance, business continuity, and the law (ex. HIPAA)
   b. Asset Security
      i. Secures digital and physical assets. Also related to the storage, maintenance, retention, and destruction of data.
      ii. I.E., ensuring that company servers are configured to securely store, maintain, and retain SPII
   c. Security Architecture and Engineering
      i. Optimizes data security by ensuring effective tools, systems, and processes are in place
      ii. I.E., configuring a firewall
   d. Communication and Network Security
      i. Manage and secure physical networks and wireless communications.
      ii. I.E., tasked with monitoring employee interactions
   e. Identity and Access Management
      i. Keeps data secure by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications
      ii. I.E., Installing and implementing key card access to a building
   f. Security Assessment and Testing
      i. Conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities

    ii. I.E., conducting user audits of permissions (access to payroll for authorized personnel)
g. Security Operations
    i. Conducting investigations and implementing preventative measures
    ii. I.E., receive an alert that an unknown device has been plugged into the network and you are responsible for investigating in accordance with your company's policies
h. Software Development Security
    i. Secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services
    ii. I.E., working with software development teams in order to ensure proper security is implemented into the software development cycle (new mobile app and consulting on the proper creation of a password for a user)

7. Attack Types
    a. Password
        i. attempt to access password-secured devices, systems, networks, or data. Forms include:
            1. brute force
            2. rainbow table
        ii. Falls under Communication and Network Security domain
    b. Social Engineering
        i. a manipulation technique that exploits human error to gain private information, access, or valuables. Forms include:
            1. phishing
            2. smishing
            3. vishing
            4. spear phishing
            5. whaling
            6. social media phishing
            7. business email compromise (BEC)
            8. watering hole attack
            9. USB (universal serial bus) baiting
            10. physical social engineering
        ii. Falls under Security and Risk Management domain
    c. Physical
        i. security incident that affects not only digital but also physical environments where the incident is deployed. Forms include:
            1. malicious USB cable
            2. malicious flash drive
            3. card cloning and skimming
        ii. Falls under the Asset Security domain
    d. Adversarial Artificial Intelligence
        i. Technique that manipulates AI to conduct attacks more efficiently
        ii. Falls under both Communication and Network Security and the Identity and Access Management Domains
    e. Supply-Chain
        i. targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed. A security breach can happen at any point in the supply chain between vendors.

ii. Falls under Security and Risk Management, Security Architecture and Engineering, and Security Operations domains

f. Cryptographic
   i. affects secure forms of communication between a sender and intended recipient. Forms include:
      1. birthday
      2. collision
      3. downgrade
   ii. Falls under the Communication and Network Security domain

8. Threat Actor Types
   a. Advanced Persistent Threats
      i. have significant expertise accessing an organization's network without authorization. Tends to research their targets in advance and can remain undetected for an extended period of time. Intentions and motivations include:
         1. Damaging critical infrastructure, such as the power grid and natural resources
         2. Gaining access to intellectual property, such as trade secrets or patents
   b. Insider Threats
      i. Abusing authorized access to obtain data that may harm the organization. Intentions and motivations can include:
         1. sabotage
         2. corruption
         3. espionage
         4. unauthorized data access or leaks
   c. Hacktivists
      i. Threat actors that are driven by a political agenda. Abusing digital technology to accomplish goals, which may include:
         1. demonstrations
         2. propaganda
         3. social change campaigns
         4. fame
   d. Hacker
      i. Any person who uses computer to gain access to computer systems, networks, or data.
      ii. Three main categories
         1. Authorized- ethical hacker, follows code of ethics and adhere to the law to conduct organizational risk evaluations
         2. Semi-authorized- considered researcher, search for vulnerabilities but don't take advantage of the vulnerabilities they find
         3. Unauthorized- unethical, malicious threat actors who do not follow or respect the law, goal is to collect and sell confidential data for financial gain
      iii. Multiple types that fall into one of three categories
         1. to learn and enhance their hacking skills
         2. to seek revenge
         3. to exploit security weaknesses by using existing malware, programming scripts and other tactics

Week 3 – Protect Against Threats, Risks, and Vulnerabilities

1. Security Framework
   a. Guidelines used for building plans to help mitigate risk and threats to data and privacy
   b. Purposes

        i. Protect PII
        ii. Securing financial information
        iii. Identifying security weaknesses
        iv. Managing organizational risks
        v. Aligning security with business goals
    c. Components
        i. Identifying and documenting security goals
            1. goal to align with EU's General Data Protection Regulation (GDPR)
                a. GDPR- data protection law established to grant European Citizens more control over their personal data
            2. data analyst may be assigned to find where in their organization's policies are not compliant with the GDPR
        ii. Setting guidelines to achieve security goals
            1. organization's need to develop new policies for how to handle data requests from individual users
        iii. Implementing strong security processes
            1. a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests
            2. I.E., when someone attempts to update or delete their profile information
        iv. Monitoring and Communicating Results
            1. monitoring your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer
    d. Allows analysts to work alongside other members of the security team to document, implement, and use the policies and procedures that have been created
    e. **Compliance** is the process of adhering to internal standards and external regulations
2. Security Control
    a. Safeguards designed to reduce specific security risks
        i. I.E., company guideline requiring all employees to complete a privacy training to reduce risk of data breaches
3. CIA Triad
    a. A foundational model that helps inform how organizations consider risk when setting up systems and security policies
        i. Confidentiality- Only authorized users can access specific assets or data
        ii. Integrity- Data is correct, authentic, and reliable
        iii. Availability- Data is accessible to those who are authorized to access it
4. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
    a. NIST is a U.S.-based agency that develops multiple voluntary compliance frameworks that organizations worldwide can use to help manage risk
    b. A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk
        i. Built for managing short and long-term risk
    c. Disgruntled employees can be the greatest threat to the CIA Triad
5. NIST Risk Management Framework (RMF)
6. Federal Energy Regulatory Commission – North American Electric Reliability Corporation (FERC-NERC)
    a. Applies to organizations that work with electricity in the U.S and North American power grid
    b. Legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined in the FERC

7. Federal Risk and Authorization Management Program (FedRAMP)
    a. U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services/product offerings
    b. Involved with government sector and third-party cloud providers
8. Center for Internet Security (CIS)
    a. Nonprofit with areas of emphasis on
        i. Controls used to safeguard systems and networks against attacks
        ii. Helping organizations establish a better plan of defense
        iii. Provides actionable controls that security professional follow if an incident occurs
9. General Data Protection Regulation (GDPR)
    a. European Union (E.U.) general data regulation that protects the processing of E.U. residents' data and their right to privacy in and out of E.U. territory
    b. If a breach occurs, E.U. citizens must be informed within 72 hours
10. Health Insurance Portability and Accountability Act (HIPAA)
    a. U.S. federal law established in 1996 to protect patient health information
    b. Governed by three rules:
        i. Privacy
        ii. Security
        iii. Breach notification
    c. Organizations storing patient data have a legal obligation to inform patients of breach if patient Protected Health Information (PHI) is exposed
        i. relates to past, present, or future physical or mental health/condition of an individual
11. International Organization for Standardization (ISO)
    a. Created to establish international standards related to technology, manufacturing, and management across borders
    b. helps improve processes and procedures for staff retention, planning, waste, and services
12. System and Organizations Controls (SOC type 1, SOC type 2)
    a. Developed by American Institute of Certified Public Accountants (AICPA)
    b. series of reports that focus on an organization's user access policies at different organizational levels such as:
        i. Associate
        ii. Supervisor
        iii. Manager
        iv. Executive
        v. Vendor
        vi. Others
    c. Used to assess an organization's financial compliance and levels of risk
13. **To keep up to date with changes to frameworks, consult Gramm-Leach-Bliley Act and Sarbanes-Oxley Act.**
14. United States Presidential Executive Order 14028
    a. Joe Biden's executive order related to improving the nation's cybersecurity to remediate the increase in threat actor activity
    b. include ties to U.S. critical infrastructure
15. Security Ethics
    a. Guidelines for making appropriate decisions as a security professional
    b. Ethical principles in security
        i. Confidentiality
        ii. Privacy protections- Safeguarding personal Information from unauthorized use

iii. Laws- Rules that are recognized by a community and enforce by a governing entity
1. You must remain unbiased and conduct your work honestly, responsibly, and with the highest respect for the law
2. Be transparent and just, and rely on evidence
3. Ensure constant investment in the conducted work so all issues can be appropriately and ethically addressed
4. Stay informed and strive to advance your skills so you can contribute to the cyber landscape

c. United States standpoint on counterattacks
i. No counterattacking, only defend
ii. Only authorized U.S. personnel of the federal government or military are allowed to counterattack

d. International standpoint on counterattacks
i. International Court of Justice (ICJ) states a person/group can counterattack if:
1. will only affect the party that attacked first
2. direct communication asking the initial attacker to stop
3. does not escalate the situation
4. effects can be reversed

Week 4 – Cybersecurity Tools and Programming Languages

1. Log
a. A record of events that occur within an organization's systems
2. Tools
a. Security Information and Event Management (SIEM) "Sim"
i. An application that collects and analyzes log data to monitor critical activities in an organization
ii. Examples:
1. Splunk- data analysis platform
2. Splunk Enterprise- retain, organize, analyze data
3. Chronicle- cloud native for search and analysis

b. Playbook
i. A manual that provides details about any operational action
ii. Chain of Custody
1. process of documenting evidence possession and control during an incident lifecycle
2. document who, what, where, and why you have collected evidence

iii. Protecting and Preserving Evidence
1. understanding what fragile and volatile digital evidence is
2. consult Order of Volatility
a. sequence outlining the order of data that must be preserved from first to last
b. considers which data may be lost if power goes off

c. Network Protocol Analyzer (packet sniffer)
i. A tool designed to capture and analyze data traffic within a network
1. TCPdump
2. Wireshark

3. Linux
a. Open-Source operating system
b. Common use: Examining logs
4. Structured Query Language (SQL)
a. A programming language used to create, interact with, and request information from a database

5. Python
    a. Used to perform tasks that are repetitive and time-consuming, and that require a high level of detail and accuracy
6. Operating System
    a. The interface between computer hardware and the user
7. Web Vulnerability
    a. unique flaw in a web application that a threat actor could exploit by using malicious code or behavior, to allow unauthorized access, data theft, and malware deployment
8. Antivirus Software
    a. program used to prevent, detect, and eliminate malware and viruses/anti-malware
9. Encryption- makes data unreadable and difficult to decode for an unauthorized user, **main goal is to ensure confidentiality of private data**
    a. Cryptographic encoding- converting plaintext into secure ciphertext
10. Penetration testing
    a. act of participating in a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes
11. Options for creating your portfolio
    a. Documents folder
        i. Subfolders containing: resume, education, portfolio documents, cybersecurity tools, programming
    b. Google Drive or Dropbox
    c. Google Sites
    d. Git repository
        i. Sites like: GitLab, Bitbucket, GitHub
    e. Portfolio Projects:
        i. Drafting a professional statement
        ii. Conducting a security audit
        iii. Analyzing network structure and security
        iv. Using Linux commands to manage file permissions
        v. Applying filters to SQL queries
        vi. Identifying vulnerabilities for a small business
        vii. Documenting incidents with an incident handler's journal
        viii. Importing and parsing a text file in a security-related scenario
        ix. Creating or revising a resume

Course 2 – Manage Security Risks | Instructor Ashley

Week 1 – Security Domains

1. Security Posture
    a. An organization's ability to manage its defense of critical assets and data, and react to change
2. CISSP Domains – Expanded Review
    a. Security and Risk Management
        i. Focused on defining **(elements)** security goals and objectives, risk mitigation, compliance, business continuity, legal regulations, and professional and organizational ethics
            1. Risk Mitigation
                a. The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach
            2. Business Continuity

        a. An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans
    ii. Information Security (InfoSec)- refers to a set of processes established to secure information
        1. Incident response
        2. Vulnerability Management
        3. Application security
        4. Cloud security
        5. Infrastructure security
b. Asset Security
    i. Focused on securing digital and physical assets. Also related to the storage, maintenance, retention, and destruction of data
    ii. Conducting a security impact analysis, establishing a recovery plan, and managing data exposure
c. Security Architecture and Engineering
    i. Focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data
    ii. Shared Responsibility
        1. All individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security
    iii. Additional Principles
        1. Threat modeling
        2. Least privilege
        3. Defense in depth
        4. Fail securely
        5. Separation of duties
        6. Keep it simple
        7. Zero trust
        8. Trust but verify
d. Communication and network security
    i. Focused on managing and securing physical networks and wireless communications
e. Identity and Access Management (IAM)
    i. Focused on access and authorization to keep data secure, by making sure users follow established policies to control and manage assets
    ii. Overall, the goal is to reduce the overall risk to systems and data
    iii. Four main components:
        1. Identification- who you are via ID card/biometric data
        2. Authentication- verification process of someone's identity
        3. Authorization- relates to level of access/role in organization
        4. Accountability- recording of the user's activity I.E., login attempts
    iv. Principle of Least Privilege- granting only the minimal access and authorization require to complete a task
f. Security Assessment and Testing
    i. Focused on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities
    ii. Emphasizes the importance of conducting security audits to monitor for and reduce probability of a data breach
g. Security Operations
    i. Focused on conducting investigations and implementing preventative measures

        ii. How you carry out investigations in the instance of a breach
        iii. Involves strategies such as:
            1. Training and awareness
            2. Reporting and documentation
            3. Intrusion detection and prevention
            4. SIEM tools
            5. Log management
            6. Incident management
            7. Playbooks
            8. Post-breach forensics
            9. Reflecting on lessons learned
    h. Software Development Security
        i. Focused on using secure coding practices
            1. recommended guidelines used to make secure applications and features
3. Threat
    a. Any circumstance or event that can negatively impact assets
    b. Example- Social Engineering
        i. A manipulation technique that exploits human error to gain private information, access, or valuables
4. Risk
    a. Anything that can impact the confidentiality, integrity, or availability of an asset
    b. “likelihood of a threat occurring”
    c. Low-Risk Asset
        i. Information that would not harm the organization’s reputation or ongoing operations, and would not cause financial damage if compromised
    d. Medium-Risk Asset
        i. Information that’s not available to the public and may cause some damage to the organization’s finances, reputation, or ongoing operations
        ii. I.E. Early release of company’s quarterly earnings
    e. High-Risk Asset
        i. Information protected by regulations or laws, which if compromised would have a sever negative impact on an organization’s finances, ongoing operations, or reputation
        ii. I.E. SPII, PII, Intellectual property
5. Vulnerability
    a. A weakness that can be exploited by a threat
    b. I.E. Outdated firewall/software application, weak passwords, un-protected confidential data, people
6. Ransomware
    a. A malicious attack where threat actors encrypt an organization’s data and demand payment to restore access
7. Layers of the web
    a. Surface
        i. layer that most people use, accessed via typical search engine
    b. Deep
        i. need authorization to access
    c. Dark
        i. accessed via special software
8. Key impacts of threats, risks, and vulnerabilities

a. Financial
b. Identity Theft (think PII)
c. Reputation

9. NIST Risk Management Framework (RMF) – 7 Steps
    a. Prepare
        i. Activities that are necessary to manage security and privacy risks before a breach occurs
    b. Categorize
        i. Used to develop risk management processes and tasks
    c. Select
        i. Choose, customize, and capture documentation of the controls that protect an organization
        ii. I.E., keep the playbook up to date
    d. Implement
        i. Implement security and privacy plans for the organization
    e. Assess
        i. Determine if established controls are implemented correctly
        ii. Identify potential weaknesses to current controls
    f. Authorize
        i. Being accountable for the security and privacy risks that may exist in an organization
    g. Monitor
        i. Be aware of how systems are operating
10. Risk Management – Protecting your assets
    a. Examples of digital assets: SSN, birth dates, bank account numbers, mailing addresses
    b. Examples of physical assets: payment kiosks, servers, desktop computers, office spaces
    c. Strategies to manage risk:
        i. Acceptance- accepting a risk to avoid disrupting business continuity
        ii. Avoidance- creating a plan to avoid the risk altogether
        iii. Transference- transferring risk to a third party to manage
        iv. Mitigation- lessening the impact of a known risk
    d. Common Risk Management Frameworks:
        i. NIST RMF
        ii. Health Information Trust Alliance (HITRUST)
11. Most common threats, risks, and vulnerabilities
    a. Threats
        i. Insider threats- staff members or vendors abuse their authorized access
        ii. Advanced Persistent Threats (APTs)- threat actor maintain unauthorized access to a system
    b. Risks (anything that can impact the CIA triad of an asset)
        i. External risk
            1. anything outside the organization
        ii. Internal risk
            1. current or former employee, vendor, or trust partner
        iii. Legacy systems
            1. old systems not accounted for or update, but can still impact assets, outdated workstations or old mainframe systems
        iv. Multiparty risk
            1. outsourcing work to third-party vendors can give access to intellectual property
        v. Software compliance/licensing
            1. patches not installed in a timely manner

c. Vulnerabilities (a weakness that can be exploited by a threat)
    i. ProxyLogon
        1. pre-authenticated vulnerability affecting Microsoft Exchange servers, deploy malicious code from a remote location
    ii. ZeroLogon
        1. Microsoft's NetLogon authentication protocol
    iii. Log4Shell
        1. allows attackers to run Java code on someone else's computer or leak sensitive information, enables remote attacker to control devices connected to internet
    iv. PetitPotam
        1. Windows New Technology Local Area Network (LAN) Manager (NTLM), allows LAN-based attacker to initiate an authentication request
    v. Security logging and monitoring failures
        1. insufficient logging and monitoring capabilities that result in attackers exploiting vulnerabilities without the organization knowing it
    vi. Server-side request forgery
        1. allows attacker to manipulate a server-side application into accessing and updating backend resources, allowing threat actors to steal data

Week 2 – Security Frameworks and Controls

1. Security Frameworks - Review
    a. Guidelines used for building plans to help mitigate risk and threats to data and privacy
    b. Examples such as HIPAA for medical professionals
2. Controls – Review
    a. Safeguards designed to reduce specific security risks
    b. Examples such as multi-factor authentication to access medical records
    c. Three common types:
        i. Encryption
        ii. Authentication
        iii. Authorization- Granting access to specific resources within a system
    d. Physical: gates/fences/locks, security guards, cctv, access cards/badges
    e. Technical: firewalls, MFA, antivirus software
    f. Administrative: separation of duties, authorization, asset classification
3. Cyber Threat Framework (CTF)
    a. developed by the U.S. government to provide "a common language for describing and communicating information about cyber threat activity
    b. helps cybersecurity professionals analyze and share information more efficiently
4. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001
    a. "ISO/IEC 27001"
    b. family standards enabling organization to manage security of assets, and information to 3rd parties
    c. Outlines requirements for information security management system, best practices, and controls
5. CIA Triad – Review
    a. A model that helps inform how organizations consider risk when setting up systems and security policies
    b. Confidentiality
        i. only authorized users can access specific assets or data
    c. Integrity
        i. data is correct, authentic, and reliable
    d. Availability

        i. data is accessible to those who are authorized to access it
6. NIST Cybersecurity Framework (CSF)
    a. A voluntary framework, consists of standards, guidelines, and best practices to manage cybersecurity risk
    b. helps organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes
    c. Five Elements
        i. Identify
            1. management of cybersecurity risk and its effect on an organization's people and assets
            2. "relates to monitoring systems and devices in an organization's internal network to help security teams manage potential cybersecurity risks and their effects"
        ii. Protect
            1. strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats
        iii. Detect
            1. identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections
        iv. Respond
            1. Making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process
            2. "investigating an incident to determine how the threat occurred, what was affected, and where the attack originated"
        v. Recover
            1. the process of returning affected systems back to normal operation
7. NIST S.P. 800-53
    a. A unified framework for protecting the security of information systems within the federal government
8. Open Web Applications Security Project (OWASP)
    a. Core Principles
        i. Minimize attack surface area
        ii. Least privilege
        iii. Defense in depth- organization should have multiple security controls in many ways
        iv. Separation of duties- no one should be given so many privileges that they can abuse the system
        v. Keep security simple
        vi. Fix security issues correctly
    b. Additional Principles
        i. Establish secure defaults- optimal security state is also its default state for users
        ii. Fail securely- when a control fails/stops, it should default to its most secure option
        iii. Don't trust services- outside partners have different security policies, don't explicitly trust
        iv. Avoid security by obscurity- "security of an app. should not rely on keeping the code secret"
9. Security Audit (Internal)
    a. A review of an organization's security controls, policies, and procedures against a set of expectations
    b. Basic Checklist
        i. Identify the scope of the audit
        ii. Complete a risk assessment
        iii. Conduct the audit
        iv. Create a mitigation plan
        v. Communicate results to stakeholders
    c. Questions for an audit

i. what is the audit meant to achieve?
ii. which assets are most at risk?
iii. are current controls sufficient to protect those assets?
iv. what controls and compliance regulations need to be implemented?

d. Factors that affect audits
   i. industry type
   ii. organization size
   iii. ties to the applicable government regulations
   iv. a business' geographical location
   v. a business decision to adhere to a specific regulatory compliance
e. Purpose
   i. Identify organizational risk
   ii. Assess controls
   iii. Correct compliance issues
f. Common elements
   i. (P) Establishing the scope and goals
      1. assets that will be assessed
      2. who are the stakeholders
      3. who is this audit for
      4. how the audit will help the organization achieve its desired goals
      5. how often an audit should be performed
      6. include an evaluation of organizational policies, protocols, and procedures to make sure they are working as intended and being implemented by employees
   ii. (P)Conducting a risk assessment
      1. often completed by managers or stakeholders
      2. may provide input from team level
   iii. Completing a controls assessment
      1. closely reviewing an organization existing assets
      2. evaluating potential risks to those assets
      3. controls:
         a. Administrative- human component
         b. Technical- hardware/software used to protect assets
         c. Physical- measures put in place to physically protect assets
   iv. Assessing compliance
      1. which regulations are they bound to follow/adhere to?
   v. Communicating results
      1. summarizes scope and goals
      2. lists existing risks
      3. notes how quickly those risks need to be addressed
      4. identified compliance regulations

Week 3 – Introduction to SIEM Dashboard and Tools

1. Common log sources
   a. Firewall
      i. record of attempted or established connections for incoming traffic from the internet
      ii. includes outbound request to the internet from with the network
   b. Network
      i. record of all computers and devices that enter and leave the network

        ii. records connections between devices and services on the network
    c. Server
        i. record of events related to services such as websites, emails, or file shares
        ii. includes actions such as login, password, and username requests
2. Metrics
    a. key technical attributes, such as response time, availability, and failure rate, which are used to assess the performance of a software application
3. Security Orchestration, Automation, and Response (SOAR)
    a. collection of applications, tools, and workflows using automation to respond to security events
    b. handling common security-related incidents with the use of SIEM tools
4. Different types of SIEM tools
    a. Self-hosted
        i. ideal when organization is responsible for maintaining physical control
    b. Cloud-hosted
        i. ideal for organizations that don't need to maintain physical control
    c. Hybrid
5. Splunk Enterprise
    a. self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time
6. Splunk Cloud
    a. cloud-hosted tool used to collect, search and monitor log data
7. Chronicle
    a. cloud-native tool designed to retain, analyze, and search data
8. Suricata
    a. open-source network analysis and threat detection software
    b. developed by the Open Information Security Foundation (OISF)
        i. dedicated to maintaining open-source use of Suricata project
9. Splunk
    a. Security posture dashboard
        i. designed for Security Operations Centers (SOCs)
        ii. displays last 24 hours of organization's notable security-related events and trends
    b. Executive summary dashboard
        i. analyzed and monitors overall health of organization over time
        ii. provides high-level insights to stakeholders
    c. Incident review dashboard
        i. suspicious patterns that can occur in the event of an incident
        ii. highlights higher risk items that need immediate review by an analyst
        iii. provides timeline leading up to incident
    d. Risk analysis dashboard
        i. identify risk for each object
        ii. shows change in risk-related activity or behavior
        iii. used to analyze the potential impact of vulnerabilities in critical assets
10. Chronicle
    a. Allows you to collect and analyze data according to:
        i. a specific asset
        ii. a domain name
        iii. a user

        iv. an IP address
    b. Enterprise insights dashboard
        i. highlights recent alerts
        ii. identifies suspicious domain names in logs know as Indicators of Compromise (IOC)
        iii. monitor login or data access attempts related to a critical asset
    c. Data ingestion and health dashboard
        i. number of event logs/log sources/success rates of data being processed into chronicle
        ii. ensure that log sources are correctly configured and received without error
    d. IOC matches dashboard
        i. indicates top threats, risks, and vulnerabilities to the organization
        ii. observe domain names, IP addresses, and device IOCs over time to identify trends
        iii. search for additional activity associated with an alert
    e. Main Dashboard
        i. high-level summary of information related to the organization's data ingestion
        ii. access a timeline of security events to identify threat trends across log sources
    f. Rule detections dashboard
        i. statistics related to incidents with the highest occurrences/severities/detections over time
        ii. access list of all alerts triggered by a specific detection rule
        iii. helps manage recurring incidents and establish mitigation tactics to reduce organization's risk
    g. User sign in overview dashboard
        i. provides information about user access behavior across the organization
        ii. access a list of all user sign-in events to identify unusual user activity

Week 4 – Phases of Incident Response Playbooks and Incident Response

1. Playbook
    a. Manual that provides details about any operational action
    b. Ensure that people follow a consistent list of actions in a prescribed way
    c. Clarifies what tools should be used to respond to security incidents
    d. Often updated when:
        i. a failure is identified, such as an oversight in the outlined policies and procedures
        ii. there is a change in industry standards, such as changes in laws or regulatory compliance
        iii. the cybersecurity landscape changes due to evolving threat actor tactics and techniques
    e. **usually devised from the organization's business continuity plan**
    f. Used for:
        i. Open attacks
        ii. Privacy incidents
        iii. Data leaks
        iv. Denial of service attacks
        v. Service alerts
2. Incident Response
    a. An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach
    b. Six Phases
        i. (1) Preparation
            1. sets foundation for successful incident response
            2. procedures for each role of an incident response
        ii. (2) Detection and Analysis
            1. detect and analyze events using appropriate tools and strategies

iii. (3) Containment
    1. prevent further damage and reduce immediate impact of incident
    2. high-priority for organization
iv. (4) Eradication and Recovery
    1. complete removal of incidents artifacts in order to return to normal operation
    2. restore affected environment
v. (5) Post Incident Activity
    1. documenting incident, informing leadership, ensure that the organization is better prepared to handle future security events
    2. perform full-scale analysis
    3. "security teams may conduct a full-scale analysis to determine the **root cause** of an incident and use what they learn to improve the company's overall security posture"
vi. (6) Coordination
    1. Reporting/recording incidents and sharing findings throughout the incident response process along with sharing with other coworkers

Course 3 – Networks and Network Security | Instructor Chris

Week 1 – Intro to Networks, Network Communication, Local/Wide Network Communication

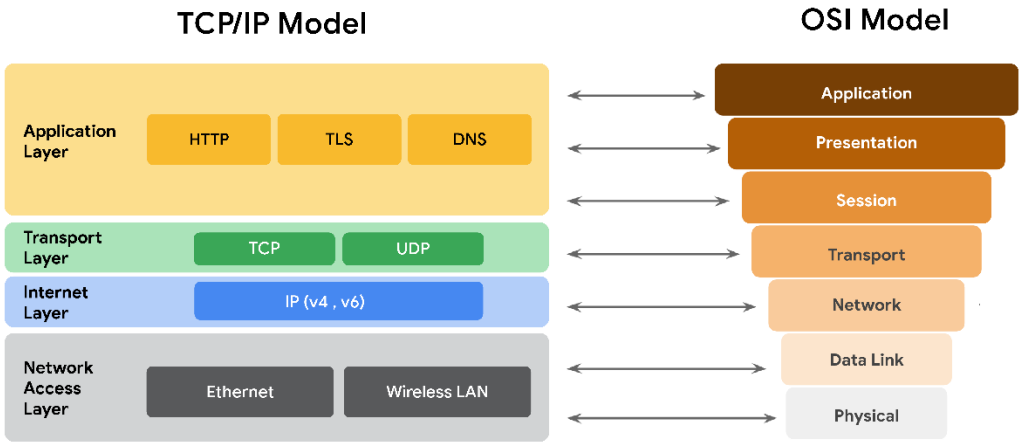
1. Network- A group of connected devices
2. Local Area Network (LAN)
    a. A network that spans a small area like an office building, a school, or a home
3. Wide Area Network (WAN)
    a. A network that spans a large geographic area like a city, state, or country
4. Network tools
    a. Hub
        i. network device that broadcasts information to every device on the network
    b. Switch
        i. device that makes connections between specific devices on a network by sending and receiving data between them
        ii. **"When a switch receives a data packet, it reads the MAC address of the destination device and maps it to a port."**
    c. Router
        i. network device that connects multiple networks together
    d. Modem
        i. device that connects your router to the internet and brings internet access to the LAN
        ii. usually interfaces with an internet service provider
    e. Virtualization Tools
        i. pieces of software that perform network operations
5. Cloud Computing
    a. the practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices
    b. Cloud Network
        i. A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet
    c. Services providers offer:
        i. on-demand storage
        ii. processing power

iii. analytics

d. Three main categories of Cloud Service Providers (CSP)
    i. Software as a Service (SaaS)
        1. software suites operated by the CSP that a company can use remotely without hosting the software
    ii. Infrastructure as a Service (IaaS)
        1. use of virtual computer components offered by the CSP
        2. virtual containers and storage that are configured remotely through the CSP's API
    iii. Platform as a Service (PaaS)
        1. tools that application developers can use to design custom applications for their company
        2. used for a company's specific business needs
e. Software-defined Networks (SDN)
    i. consists of virtual network devices and services
    ii. provides virtual switches, routers, firewalls, etc.
f. Three Main Benefits of cloud computing and software-defined networks
    i. Reliability
        1. available cloud services/resources are
        2. how secure the connections are
        3. how effective the services are running
    ii. Cost
        1. much less expensive than having to purchase your own physical infrastructure
    iii. Scalability
        1. only pay for what you need according to business' growth model

6. Data Packet
    a. A basic unit of information that travels from one device to another within a network
    b. Contains: | Header | Body | Footer |
        i. Header- ip address, MAC address, protocol number
        ii. Body- Intended message/content
        iii. Footer- Signature/end of packet
7. Bandwidth
    a. The amount of data a device receives every second
8. Speed
    a. The rate at which data packets are received or downloaded
9. Packet Sniffing
    a. The practice of capturing and inspecting data packets across a network
10. Transmission Control Protocol (TCP)
    a. An internet communication protocol that allows two devices to form a connection and stream data
11. Internet Protocol (IP)
    a. A set of standards used for routing and addressing data packets as they travel between devices on a network.
12. Port
    a. A software-based location that organizes sending and receiving of data between devices on a network
    b. Common Port Numbers:
        i. 25 – email
        ii. 443 – secure internet communication
        iii. 20 – large file transfers

13. TCP/IP Model
    a. A framework used to visualize how data is organized and transmitted across the network
    b. Four Layers:
        i. **4. Application**- protocols determine how the data packets will interact with receiving devices
        3. Transport- protocols to control the flow of traffic across a network, status of connection
        2. Internet- IP addresses attached to data packets indicating the location of the sender/receiver
        1. Network Access- Creation of packets and their transmission across a network



    c. TCP/IP Layers in-depth
        i. Application
            1. similar to the application/presentation/session layers of the OSI model
            2. responsible for making network requests or responding to requests
            3. common protocols:
                a. HTTP 80
                b. SMTP 25
                c. SSH 22
                d. FTP 20data 21cmd
                e. DNS 53
        ii. Transport
            1. responsible for reliably delivering data between two systems or networks
            2. TCP/UDP are the two protocols at this layer
                a. TCP
                    i. Ensures data is reliably transmitted to the destination service
                    ii. contains port number of intended destination service which resides in the TCP header of a TCP/IP packet
                b. UDP
                    i. used by applications not concerned with reliability of the transmission
                    ii. used for real time applications such as video streaming
        iii. Internet
            1. referred to as the “network” layer
            2. ensures delivery to the destination host potentially residing on a different network
            3. determines which protocol is responsible for delivering the data packets
            4. common protocols
                a. Internet Protocol (IP)
                    i. data packets to correct destination and relies on TCP/UDP

ii. allows communication between two networks

b. Internet Control Message Protocol (ICMP)

i. shares error information and status updates of data packets

ii. reports info. about packets that were dropped or disappeared in transit

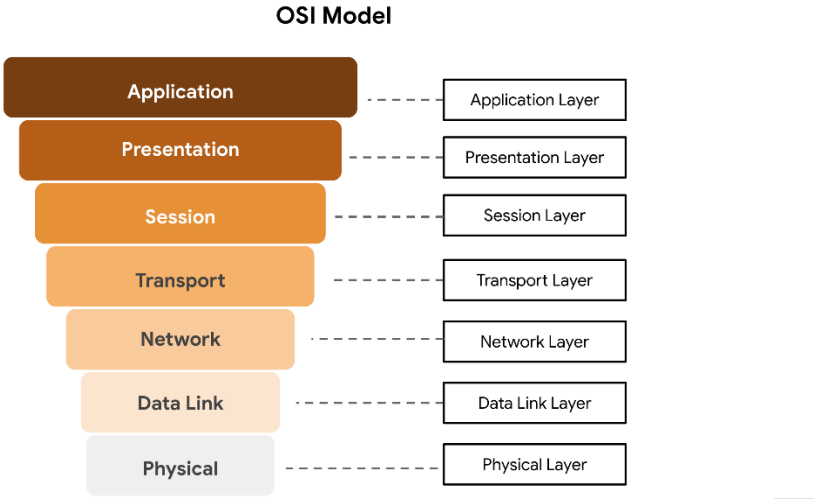
iv. Network Access

1. Known as the “data link” layer
2. organizes sending and receiving data frames within a single network
3. corresponds to the physical hardware involved
4. hubs, modems, cables, and wiring
5. ARP (Address Resolution Protocol)

a. mapping IP addresses to MAC addresses on the same physical network

14. OSI Model In-Depth

a. describes the seven layers computers use to communicate and send data over the network



b. Layer 7: Application

i. processes that directly involve the user

ii. includes all of the networking protocols that software applications use to connect a user to the internet

iii. “user connection to the network via applications and requests”

iv. Protocols: HTTP, HTTPS, SMTP, DNS

c. Layer 6: Presentation

i. data translation and encryption for the network

ii. adds to and replaces data with formats that can be understood by layer 7

iii. format standardization

iv. uses encryption such as SSL

1. encrypts data between web servers and browsers as part of websites using HTTPS

d. Layer 5: Session

i. when a connection is established between two devices

ii. terminate the session once transmission is complete

iii. authentication, reconnection, and setting checkpoints during a data transfer

iv. respond to requests for service from layer 6 and sends requests to layer 4

e. Layer 4: Transport

i. responsible for delivering data between devices

ii. handles speed of data transfer, flow of the transfer, and breaking down of data into smaller segments for easier transport
iii. Protocols: TCP, UDP

f. Layer 3: Network
i. receiving frames from layer 2 and delivering them to the intended destination
1. intended destination found based on address residing in frame of the data packet
ii. includes IP address

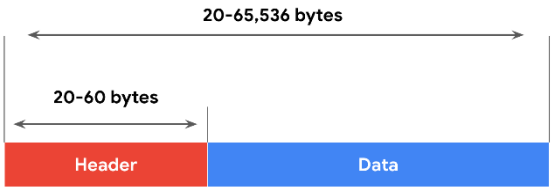
g. Layer 2: Data Link
i. organizes sending and receiving data packets within a single network
ii. involves switches on a local network and network interface cards on local devices
iii. Protocols:
1. Network Control Protocol (NCP) 524
2. High-Level Data Link Control (HDLC)
3. Synchronous Data Link Protocol (SDLC)

h. Layer 1: Physical
i. hardware involved in network transmission
ii. involves hubs, modems, cables, and wiring
iii. data packet needs to be translated into stream of 0s and 1s

15. Internet Protocol (IP) Address
a. A unique string of characters that identifies the location of a device on the internet
i. “Each device on the internet has a unique IP address, just like every house on a street has its own mailing address.”
b. Two types of IP Addresses
i. IP version 4 (IPv4)
ii. IP Version 6 (IPV6)
c. **“A Public IP Address is assigned by an internet service provider that is shared by all devices on a local area network”**

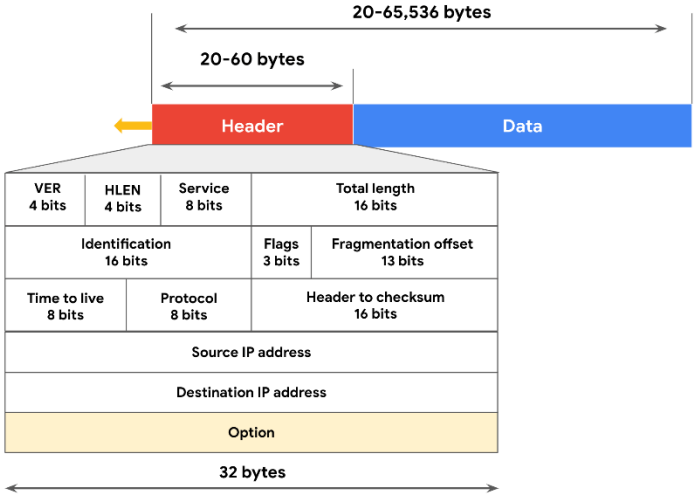
16. MAC Address
a. A unique alphanumeric identifier that is assigned to each physical device on a network

17. Format of an IPv4 Packet
a. Basic View



i. Header includes IP routing information that devices use to direct the packet
ii. Format of an IP packet is determined by the IPv4 Protocol

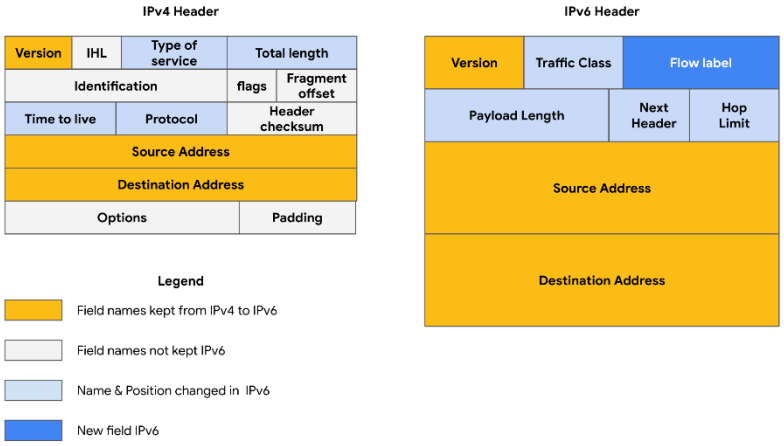
b. In-Depth View of Header



c. There are 13 fields within the header of an IPv4 packet
   i. **Version**: tells receiving devices what protocol the packet is using
   ii. **IP Header Length (HLEN)**: packet's header length, indicates where packet header ends and data segment begins
   iii. **Type of Service (TOS)**: prioritization of packet delivery to maintain quality of service on the network and provides this information to the router
   iv. **Total Length**: length of the entire IP packet including the header and data, max size of an IPv4 packets is 65,535 bytes
   v. **Identification**: if larger than 65,535 bytes then packets are divide/fragmented into smaller IP packets, provides unique identifier for all fragments of the original IP packet so it can be reassembled once they reach their destination
   vi. **Flags**: provides routing device with more information whether the original packet has been fragmented and if there are more in transit
   vii. **Fragmentation Offset**: tells routing devices where in the original packet the fragment belongs
   viii. **Time to Live (TTL)**: prevents data packets from being forwarded by routers indefinitely, contains a counter that is set by the source, counter is decremented by one as it passes through each router along its path, when TTL reaches zero then the router holding the packet will discard it and return an ICMP Time Exceeded error message to the center
   ix. **Protocol**: tells receiving device which protocol will be used for the data portion of the packet
   x. **Header Checksum**: contains a checksum used to detect corruption of the IP header in transit
   xi. **Source IP Address**: IP address of the sending device
   xii. **Destination IP Address**: IP address of the receiving device
   xiii. **Options**: allows for security options to be applied to the packet if the HLEN value is greater than five, communicates these options to the routing device

18. Difference Between IPv4 and IPv6
    a. IPv4 is made of 4 bytes ='ing 4.3 billion possible addresses

b. IPv6 is hexadecimal and 16 bytes =’ing 340 undecillion addresses (340 x 10^{36})



Week 2 – Intro to Network Protocols and System Identification

1. Network Protocols
    a. A set of rules used by two or more devices on a network to describe the order of delivery and the structure of the data
2. Three categories of network protocols
    a. Communication
        i. Transmission Control Protocol (TCP)
            1. “three-way handshake process”
                a. SYN -> server
                SYN/ACK -> sender
                ACK -> server
                b. Occurs at transport layer
        ii. User Datagram Protocol (UDP)
            1. does not establish a connection between devices before a transmission
            2. used for internet gaming transmissions
            3. occurs at transport layer
        iii. Hypertext Transfer Protocol (HTTP) 80
            1. communication between clients and web servers
            2. occurs at the application layer
        iv. Domain Name System (DNS) 53
            1. translates internet domain names into IP address
            2. occurs at the application layer
    b. Management Protocols
        i. Simple Network Management Protocol (SNMP) 161/162
            1. monitoring and managing devices on a network
            2. can reset a password on a network device or change its baseline configuration
            3. can send requests to network devices for a report on how much of the network’s bandwidth is in use
            4. occurs at application layer
        ii. Internet Control Message Protocol (ICMP)
            1. used by devices to tell each other about data transmission errors across the network
            2. quick way to troubleshoot network connectivity and latency issuing “ping” command

3. occurs at the internet layer

c. Security Protocols
   i. Hypertext Transfer Protocol Secure (HTTPS) 443
      1. like HTTP, but secure
      2. uses secure sockets layer/transport layer security (SSL/TLS) encryption
      3. occurs at application layer
   ii. Secure File Transfer Protocol (SFTP) 22
      1. used to transfer files from one device to another over a network
      2. uses SSH through TCP port 22 and Advanced Encryption Standard (AES)
      3. often used with cloud storage

3. Network Address Translation
   a. Replacing a private source IP address with a public IP address and performing the reverse operation for responses

Private IP Addresses	Public IP Addresses

• Assigned by network admins
• Unique only within private network
• No cost to use
• Address ranges:
  ◦ 10.0.0.0-10.255.255.255
  ◦ 172.16.0.0-172.31.255.255
  ◦ 192.168.0.0-192.168.255.255
	• Assigned by ISP and IANA
	• Unique address in global internet
	• Costs to lease a public IP address
	• Address ranges:
	  ◦ 1.0.0.0-9.255.255.255
	  ◦ 11.0.0.0-126.255.255.255
	  ◦ 128.0.0.0-172.15.255.255
	  ◦ 172.32.0.0-192.167.255.255
	  ◦ 192.169.0.0-233.255.255.255

4. Additional Protocols
   a. Dynamic Host Control Protocol (DHCP)
      i. application layer protocol
      ii. assigns a unique IP address and provides the addresses of the appropriate DNS server and default gateway for each device
      iii. Server Port: UDP 67
      Client Port: UDP 68
   b. Address Resolution Protocol (ARP)
      i. MAC address is permanent
      ii. internet layer protocol in the TCP/IP model
      iii. translates IP address that are found in data packets into the MAC address of the hardware device
      iv. matching IP and MAC addresses are kept in an ARP cache
      v. no specific port numbers
   c. Telnet 23
      i. application layer protocol
      ii. allows communications between devices and servers
      iii. sends all information in clear text and command line prompt

iv. used to connect to local or remote devices
v. uses TCP port 23

d. Secure Shell (SSH) 22
   i. like telnet but secure
   ii. provides secure authentication and encrypted communication

e. Post Office Protocol (POP) 110 or 995
   i. application layer
   ii. manages and retrieves email from a mail server
   iii. Unencrypted, plaintext: TCP/UDP 110
   Encrypted, SSL/TLS: TCP/UDP 995
   iv. when using, mail has to finish downloading on a local device before it can be read
   v. does not allow a user to sync emails

f. Simple Mail Transfer Protocol (SMTP) 587
   i. works with Message Transfer Agent (MTA)
      1. searches DNS servers to resolve email addresses to IP addresses
   ii. Unencrypted emails: TCP/UDP 25
   TLS Encrypted emails: TCP/UDP 587
   high-volume spam: TCP 25
   iii. helps to filter out spam by regulating how many emails a source can send at a time

g. Summary Table

Protocol	Port
DHCP	UDP port 67 (servers) UDP port 68 (clients)
ARP	none
Telnet	TCP port 23
SSH	TCP port 22
POP3	TCP/UDP port 110 (unencrypted) TCP/UDP port 995 (encrypted, SSL/TLS)
IMAP	TCP port 143 (unencrypted) TCP port 993 (encrypted, SSL/TLS)
SMTP	TCP/UDP port 587 (encrypted, TLS)

5. IEEE 802.11 (Institute of Electrical and Electronics Engineers) (WiFi)
   a. A set of standards that define communication for wireless LANs
   b. WiFi Protected Access (WPA)
      i. wireless security protocol for devices to connect to the internet
   c. Wired Equivalent Privacy (WEP)
      i. first and oldest form of wireless security standards
      ii. high-risk security protocol
   d. WiFi Protected Access (WPA)
      i. developed in 2003 to improve upon WEP
      ii. intended to be a transitional measure
      iii. uses Temporal Key Integrity Protocol (TKIP)
      iv. includes a message integrity check

e. WPA2
    i. second version of WPA
    ii. released in 2004
    iii. uses Advanced Encryption Standard (AES)
    iv. uses Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP)
        1. provides encapsulation and ensures message authentication and integrity
    v. considered security standard for all WiFi transmission today
    vi. vulnerable to KRACK attacks
    vii. WPA2 Personal
        1. useful for home networks
        2. global passphrase needs to be applied to each individual computer and access point in a network
    viii. WPA2 Enterprise
        1. best for business applications
        2. initial setup is more complicated than personal mode
        3. offers individualized and centralized control over WiFi access to a business network
            a. network admin can grant/remove user access at any time
        4. users never have access to encryption keys
            a. prevents potential attackers from recovering network keys on individual comps.
f. WPA3
    i. created in 2018
    ii. addresses authentication handshake vulnerability to KRACK attacks
    iii. uses Simultaneous Authentication of Equals (SAE)
        1. password-authenticated, cipher-key-sharing agreement
        2. prevents attackers from downloading data from wireless network connections
    iv. increased encryption (128-bit), Enterprise version offering optional 192-bit encryption

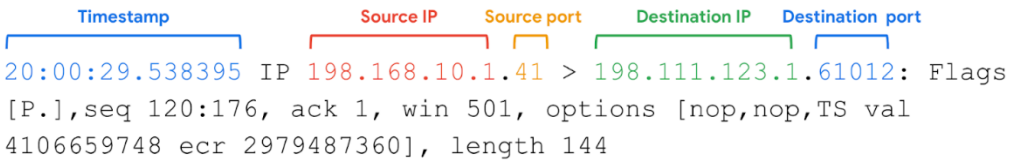
6. Port Filtering
    a. A firewall function that blocks or allows certain port numbers to limit unwanted communication
7. Cloud-based firewalls
    a. software firewalls that are hosted by a cloud service provider
8. Stateful
    a. A class of firewall that keeps track of information passing through it and proactively filters out threats
9. Stateless
    a. A class of firewall that operates based on predefined rules and does not keep track of information from data packets
10. Next Generation Firewall (NGFW)
    a. deep packet inspection
    b. intrusion protection
    c. threat intelligence
11. Virtual Private Network (VPN)
    a. A network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you are using a public network like the internet
    b. Provides Encapsulation
        i. process performed that protects your data by wrapping sensitive data in other data packets
12. Security Zone
    a. A segment of a network that protects the internal network from the internet
    b. involves Segmentation

        i. security technique that divides the network into segments
    c. Uncontrolled
        i. any network outside of the organization's control
    d. Controlled
        i. a subnet that protects the internal network from the uncontrolled zone
        ii. Areas
            1. Demilitarized zone (DMZ)
                a. contains public-facing services that can access the internet
                b. acts as barrier to internal network
            2. Internal network
                a. contains private servers and data
            3. Restricted zone
                a. protects highly-confidential information
        iii. Common flow of zones:
        Internet <-> Firewall <-> DMZ <-> Firewall <-> Internal Network <-> Firewall <-> Restricted Zone
13. Subnetting
    a. subdivision of a network into logical groups called subnets
    b. "like a network inside a network"
14. Classless Inter-Domain Routing notation for subnetting (CIDR)
    a. method of assigning subnet masks to IP addresses to create a subnet
    b. Example: IP Address 198.51.100.0/24
        i. encompasses all IP address between 198.51.100.0 -> 198.51.100.255
    c. Benefits
        i. create a network within their own network without requesting another network IP address from their internet service provider
15. Proxy Server
    a. server that fulfills the requests of a client by forwarding them to other servers
    b. sits between the internet and the rest of the network
    c. used to block unsafe websites within an organization
    d. Types:
        i. Forward Proxy
            1. regulates and restricts a person's access to the internet
            2. receives outgoing traffic from an employee, approves it, then forwards it on to the dest.
        ii. Reverse Proxy
            1. regulates and restricts the internet's access to an internal server
            2. accept traffic from external parties, approve it, and forward it to the internal servers
        iii. Email Proxy
            1. filters spam email by verifying whether a sender's address was forged
            2. reduces risk of phishing attacks that impersonate people known to the organization

Week 3 – Intro to Network Intrusion Tactics, DoS Attacks, and Network Attack/Defense Tactics

1. Attacks can harm an organization by
    a. leaking valuable or confidential information
    b. damaging an organization's reputation
    c. impacting customer retention
    d. costing money and time
2. Types of Attacks
    a. Network Interception

        i. Packet Sniffing
            1. use hardware or software tools to capture and inspect data in transit
        ii. inserting malicious code modifications or altering the message
    b. Backdoor
        i. weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms
        ii. DoS Attack
            1. targets a network or server and floods it with network traffic
3. Impacts of Attacks on an Organization
    a. Financial
    b. Reputation
    c. Public Safety
4. Distributed Denial of Service Attack (DDoS)
    a. A type of denial-of-service attack that uses multiple devices or servers in different locations to flood the target network with unwanted traffic
5. Syn (synchronize) flood attack
    a. DoS attack that simulates a TCP connection and floods a server with SYN packets
6. Internet Control Message Protocol (ICMP) Flood
    a. DoS attack performed by an attacker repeatedly sending ICMP packets to a network server
7. Ping of Death
    a. DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB
8. Network Protocol Analyzer A.K.A “packet sniffer”
    a. Most common analyzers:
        i. SolarWinds NetFlow Traffic Analyzer
        ii. ManageEngine OpManager
        iii. Azure Network Watcher
        iv. Wireshark
        v. tcpdump
    b. tcpdump
        i. command-line network protocol analyzer
        ii. output example:



        iii. Timestamp: formatted as hours, minutes, seconds, fractions of a second
        iv. Source IP: packet’s origin provided by its source IP address
        v. Source port: port number where the packet originated
        vi. Destination IP: IP address of where the packet is being transmitted to
        vii. Destination port: port number where the packet is being transmitted to
        viii. Common Uses:
            1. Establish a baseline for network traffic patterns and network utilization metrics
            2. Detect and identify malicious traffic

3. Create customized alerts to send the right notifications when network issues or security threats arise
4. Locate unauthorized instant messaging (IM), traffic, or wireless access points

9. Botnet
    a. a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder”
10. Passive Packet Sniffing
    a. where data packets are read in transit
11. Active Packet Sniffing
    a. where data packets are manipulated in transit
12. Protecting yourself from malicious packet sniffing
    a. VPN Tunnel
    b. Ensure websites you use are “HTTPS”
    c. Avoid using unprotected WiFi
13. IP Spoofing
    a. A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network
    b. Common Spoofing Attacks:
        i. On-Path
            1. malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit
            2. when a hacker intercepts the communication between two devices or servers that have a trusted relationship
            3. referred to as a “meddler-in-the middle attack)
        ii. Replay
            1. when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time
        iii. Smurf (combination of DoS and IP spoofing attack)
            1. when an attacker sniffs an authorized user’s IP address and floods it with packets
14. Network Interface Card (NIC)
    a. Piece of hardware that connects the device to a network
    b. reads data transmission, and if it contains the device’s MAC address, it accepts the packet and send it to the device to process the information based on the protocol
    c. Can be set to **promiscuous mode**
        i. accepts all traffic on the network, even the packets not addressed to the NIC’s device

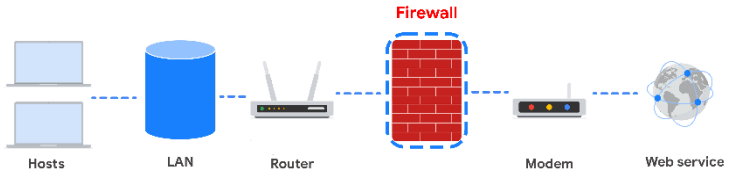
Week 4 – Security Hardening for Operating Systems, Networks, and Cloud

1. Security Hardening
    a. The process of strengthening a system to reduce its vulnerability and attack surface
2. Penetration Test
    a. A simulated attack that helps identify vulnerabilities in systems, networks, websites, apps, and processes
3. Operating System (OS)
    a. acts as an intermediary between software applications and computer hardware
4. OS Hardening
    a. Patch Update
        i. A software and operating system update that addresses security vulnerabilities within a program or product
    b. Baseline Configuration (Baseline Image)

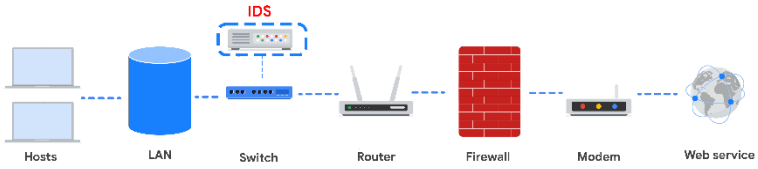
        i. A documented set of specifications within a system that is used as a basis for future builds, releases, and updates
    c. Multi-factor Authentication (MFA)
        i. A security measure which requires a user to verify their identity in two or more ways to access a system or network
        ii. Categories of MFA
            1. Something you know
            2. Something you have
            3. Something unique about you
5. Brute Force Attacks
    a. trial-and-error process of discovering private information
    b. two types:
        i. Simple brute Force: when attackers try to guess a user's login credentials
        ii. Dictionary: attackers use a list of commonly used passwords and stolen credentials
6. Assessing Vulnerabilities
    a. Virtual Machines (VMs)
        i. software versions of physical computers
        ii. provide an additional layer of security to rune code in an isolated environment
        iii. provides ability to "revert" to a previous state of the machine
    b. Sandbox Environment
        i. allows you to execute software or programs separate from your network
        ii. can be stand-alone physical computers not connected to a network
7. Prevention Measures
    a. Salting and Hashing
        i. converts information into a unique value that can then be used to determine its integrity
        ii. one-way function (impossible to decrypt and obtain the original text)
        iii. adds random characters to hashed passwords, increasing length and complexity of hash values
    b. Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA)
        i. requires a user to verify their identity in two or more ways to access a system/network
        ii. combination of authentication factors:
            1. username and password
            2. fingerprints
            3. facial recognition
            4. one-time password (OT)
        iii. 2FA is similar to MFA, except 2FA uses only two forms of verification
    c. CAPTCHA and reCAPTCHA
        i. "Completely Automated Public Turing test to tell Computers and Humans Apart"
        ii. asks you to complete a test to prove you're human
        iii. reCAPTCHA is the google free version of CAPTCHA
    d. Password Policies
        i. standardized password policies throughout the business
        ii. guidelines on how complex a password should be
        iii. login limit attempts and password renewal frequency
8. Network Security Hardening
    a. Port Filtering
        i. a firewall function that blocks or allows certain port numbers to limit unwanted communication
    b. Network Access Privilege

c. Encryption
d. Tasks performed:
    i. Firewall rules maintenance
    ii. Network log analysis
    iii. Patch updates
    iv. Server backups
e. Network log analysis
    i. the process of examining network logs to identify events of interest

9. Network Security Applications
    a. Firewall
        i. allows or blocks traffic based on a set of rules
        ii. only NGFWs can inspect the payload of the packet



    b. Intrusion Detection System (IDS)
        i. monitors system activity and alerts on possible intrusions
        ii. based on the signature of malicious traffic
        iii. can sniff data packets as they move across the network
        iv. can also detect anomalies that could be the sign of malicious activity
        v. when anomaly is discovered, it sends an alert to the network admin who can investigate further
        vi. **does not stop an attack, only alerts of one**



    c. Intrusion Prevention System (IPS)
        i. monitors system activity for intrusive activity and **takes action to stop the activity**
        ii. searches for signatures of known attacks and data anomalies
        iii. sits behind the firewall in the network architecture
        iv. if it breaks, the connection between private network and internet breaks
        v. limitation- possibility of false positives, can results in legitimate traffic being dropped
    d. Full-Packet Capture Devices

e. Summary of Network Security Applications

Key takeaways

Devices / Tools	Advantages	Disadvantages
Firewall	A firewall allows or blocks traffic based on a set of rules.	A firewall is only able to filter packets based on information provided in the header of the packets.
Intrusion Detection System (IDS)	An IDS detects and alerts admins about possible intrusions, attacks, and other malicious traffic.	An IDS can only scan for known attacks or obvious anomalies; new and sophisticated attacks might not be caught. It doesn't actually stop the incoming traffic.
Intrusion Prevention System (IPS)	An IPS monitors system activity for intrusions and anomalies and takes action to stop them.	An IPS is an inline appliance. If it fails, the connection between the private network and the internet breaks. It might detect false positives and block legitimate traffic.
Security Information and Event Management (SIEM)	A SIEM tool collects and analyzes log data from multiple network machines. It aggregates security events for monitoring in a central dashboard.	A SIEM tool only reports on possible security issues. It does not take any actions to stop or prevent suspicious events.

10. Cloud Hardening
    a. Identity Access Management (IAM)
        i. Collection of processes and technologies that helps organizations manage digital identities in their environment
        ii. authorizes how users can use different cloud resources
    b. Configuration
        i. each service must be carefully configured to meet security and compliance requirements
    c. Attack Surface
        i. consider any possible entry point into the cloud network
    d. Zero-Day Attacks
        i. an exploit that was previously unknown
        ii. CSPs are more likely to know about a zero-day attack before a traditional IT organization
    e. Visibility and Tracking
        i. admins must have access to every data packet crossing the network
        ii. CSPs pay for third-party audits to verify how secure a clod network is
    f. Things change fast in the cloud
        i. connection configurations might need to be changed based on the CSP's updates
    g. Shared Responsibility Model
        i. CSP must take responsibility for security involving the cloud infrastructure, including physical data centers, hypervisors, and host operating systems
    h. Overall:
        i. the security team, and the cloud service provider are responsible for ensuring the safety of cloud networks
        ii. Misconfigured cloud serviced are a common source of cloud security issues

Course 4 – Linux and SQL | Instructor Kim

Week 1 – The Wonderful World of Operating Systems and the User Interface

1. Common Operating Systems
    a. Window and MacOS
        i. Windows was introduced in 1985

1. closed-source: source code is not shared freely

ii. MacOS was introduced in 1984

1. partial open-source

b. Linux

i. Released in 1991

ii. completely open-source

c. ChromeOS

i. launched in 2011

ii. partially open-source

iii. derived from Chromium OS

iv. used in education field

d. Android and iOS

i. mobile operating systems

ii. Android was introduced in 2008

1. open-source

iii. iOS was introduced in 2007

1. partial open-source

2. Operating systems and vulnerabilities

a. Legacy Operating System

i. outdated but still being used

ii. can be vulnerable to security issues because they're no longer supported or updated

b. Other vulnerabilities

i. Microsoft Security Response Center

1. https://msrc.microsoft.com/update-guide/vulnerability

ii. Apple Security Updates

1. https://support.apple.com/en-us/HT201222

iii. Common Vulnerabilities and Exposures (CVE) Report for Ubuntu (distribution of Linux)

1. https://ubuntu.com/security/cves

iv. Google Cloud Security Bulletin

1. https://cloud.google.com/support/bulletins

3. Requests to the operating system

a. "The user communicates with the operating system via an interface"

b. Booting the computer

i. when you turn on a computer, either a BIOS or UEFI microchip is activated

1. Basic Input/Output System (BIOS)

2. Unified Extensible Firmware Interface (UEFI)

a. replaces BIOS on more modern systems

ii. Bootloader

1. software program that boots the operating system

2. once operating system has finished booting, the computer is ready for use

c. Completing a task

i. four-part process

1. User
    a. initiates the process
2. Application
    a. software program the users interact with to complete a task
3. Operating System
    a. receives user's request from the application
    b. interprets the request and direct its flow
    c. sends request to applicable components of the hardware
4. Hardware
    a. where the processing is done to complete the tasks initiated by the user
    b. when complete, results are sent through the OS to the application so it can be read by the user

ii. Example: Downloading a file from an internet browser
1. User decides they want to download a file they found online, clicks download button
2. internet browser communicates this action to the OS
3. OS sends the request to download the file to the appropriate hardware for processing
4. hardware begins downloading the file, OS sends this info to the internet browser application, internet browser then informs the user when the file has been downloaded

4. OS Resource Allocation
    a. "It is necessary for the OS to handle resource and memory management to ensure the limited capacity of the computer system is used where it is needed most"
5. Virtualization Technology
    a. Virtual Machine (VM)
        i. Virtual version of a physical computer
        ii. using software to create virtual representations of various physical machines
        iii. uses allocated RAM (Random Access Memory) in order to create new virtual machines
    b. Benefits
        i. Security
            1. isolated/sandbox environment
        ii. Efficiency
            1. open multiple virtual machines at once and switch easily between them
            2. many virtual machines can be hosted on the same physical machine
    c. Managed with a hypervisor
        i. helps manage multiple virtual machines
        ii. connects the virtual and physical hardware
        iii. helps with allocating share resources of the physical host machine to the virtual machine
        iv. Kernel-Based Virtual Machine (KVM)
            1. open-source hypervisor supported by most major Linux distributions
            2. built into the Linux kernel
                a. can be used to create virtual machines on any machine running a Linux operating system without the need for additional software

   d. Other Forms
      i. some do not need operating systems
         1. multiple virtual servers can be created from a single physical server
         2. virtual networks created to more efficiently use the hardware of a physical network
6. GUI versus CLI
   a. User Interface
      i. allows the user to control the functions of the operating system
   b. Graphical User Interface (GUI)
      i. interface that uses icons on the screen to manage different tasks on the computer
      ii. Basic components:
         1. Start menu
         2. Task bar
         3. Desktop with icons and shortcuts
         4. Search for files or programs from the start menu
   c. Command-Line Interface (CLI)
      i. text-based user interface that uses commands to interact with the computer
      ii. allows users to enter commands that can perform multiple tasks simultaneously
7. Advantages of a CLI in Cybersecurity
   a. Efficiency
      i. can be used more quickly when you know how to manage the interface
      ii. can accept multiple requests at one time
   b. History File
      i. records a history file of all the commands and actions in the CLI
      ii. may be able to trace an attacker's actions

Week 2 – All about Linux, Linux Distributions, and "The Shell"

1. Linux
   a. An open-source operating system
   b. in the early 1990s, two different people were working separately on projects to improve computer engineering, first person was Linus Torvalds, at the time UNIX operating system was already in use, Linus wanted to improve it and make it open source and accessible to anyone- this was the introduction of the Linux kernel. At the same time Richard Stallman started working on GNU- an operating system based on UNIX. Stallman shared Torvalds' goal of creating software that was free and open to anyone. After working on GNU for a few years, the missing element for the software was a kernel. Together they made what is commonly referred to as Linux.
   c. There are over 600 distributions of Linux
   d. Security Analysts use Linux for three common use cases:
      i. To examine different types of logs to identify what is going on in a system
      ii. To verify access and authorization in an identity and access management system
      iii. To use digital forensic tools to investigate what happened following an event
2. Components of Linux
   a. User
      i. the person interacting with a computer
      ii. initiating the task
   b. Applications
      i. a program that performs a specific task
      ii. Package Manager
         1. tool that helps users install, manage, and remove packages or applications

        2. piece of software that can be combined with other packages to form an application
    c. Shell
        i. the command-line interpreter
        ii. allows users to give text-based commands and receive responses
        iii. translator between you and your computer
    d. Filesystem Hierarchy Standard (FHS)
        i. the component of the Linux OS that organizes data
        ii. specifies the location where data is stored in the operating system
        iii. directory
            1. file that organizes where other files are stored
            2. contains files or other directories
        iv. defines how directories, directory contents, and other storage is organized
    e. Kernel
        i. the component of the Linux OS that manages processes and memory
        ii. communicates with the hardware to execute the commands sent by the shell
        iii. unique to the Linux OS and is critical for allocating resources in the system
        iv. controls all major functions of the hardware
        v. open-source, anyone can modify it to build new Linux distributions
    f. Hardware
        i. physical components of the computer
        ii. peripheral devices
            1. hardware components that are attached and controlled by the computer system
            2. not core components and can be added/removed freely (monitors, printers, keyboard)
        iii. Internal
            1. Components required to run the computer
                a. Central Processing Unit (CPU)
                b. Random Access Memory (RAM)
                c. Hard Drive
3. Linux Distributions
    a. Distribution = different version / “flavor” of the Linux OS
    b. Parent Distributions
        i. Red Hat Enterprise Linux (CentOS)
        ii. Slackware (SUSE)
        iii. Debian (Ubuntu and KALI LINUX)
    c. More In-Depth on Different Distributions
        i. Ubuntu
            1. open-source, user-friendly
            2. widely used in security and other industries
            3. has CLI and GUI
            4. Debian-derived
            5. widely used for cloud computing
        ii. Parrot
            1. open-source commonly used for security
            2. Debian-derived
            3. known to have a user-friendly GUI along with its own CLI
        iii. Red Hat Enterprise
            1. subscription-based built for enterprise use

2. offers a dedicated support team for customers to call about issues

iv. CentOS

1. open-source distribution closely related to Red Hat
2. uses source code published by Red Hat to provide a similar platform
3. supported through the community

4. KALI LINUX
    a. Trademark of Offensive Security
    b. Debian-derived
    c. Most commonly involved with penetration testing
    d. Common Tools
        i. Metasploit- exploit vulnerabilities on machines
        ii. Burp Suite- explore vulnerabilities on web applications
        iii. John the Ripper- password guessing
    e. Digital Forensics
        i. The practice of collecting and analyzing data to determine what has happened after an attack
        ii. Forensic Tools in KALI LINUX
            1. tcpdump
            2. Wireshark
            3. Autopsy- analyzing hard drives and smart phones
5. Package Managers
    a. Package
        i. piece of software that can be combined with other packages to form an application
        ii. may include files necessary for an application to be installed, including dependencies which are supplemental files used to run an application
    b. Types:
        i. Red Hat Package Manager (RPM) uses files with a .rpm file extension
            1. I.E., “Package-Version-Release_Architecture.rpm”
        ii. Debian-derived Linux uses dpkg with a .deb file extension
            1. I.E., “Package_Version-Release_Architecture.deb”
6. Package Management Tools
    a. Allows you to work with packages through the Shell
    b. Two Notable Tools:
        i. Advanced Package Tool (APT)
            1. used with Debian-derived distributions
            2. run from the command-line interface to manage, search, and install packages
        ii. Yellowdog Updater Modified (YUM)
            1. used with Red Hat-derived distributions
            2. run from the command-line to manage, search, and install packages
            3. “YUM” works with .rpm files
7. Lab Activity: Install software in a Linux distribution
    a. Ensure “apt” installed
        i. apt
    b. Install and Uninstall the Suricata Application
        i. sudo apt install suricata
        <enter>
        suricata
        sudo apt remove suricata

<enter>
suricata

c. Install tcpdump Application
    i. sudo apt install tcpdump
d. List the Installed Applications
    i. apt list –installed
e. Reinstall the Suricata Application
    i. sudo apt install suricata
    <enter>
    apt list –installed

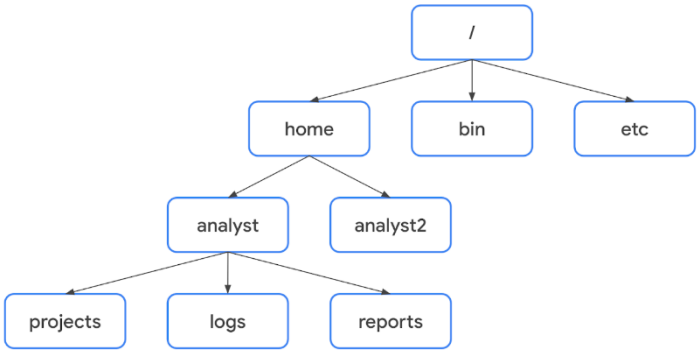
8. Shell
    a. command-line interpreter
    b. translator between you and the computer system
    c. "**communicates with the kernel to execute commands"**
    d. when a command is entered into a shell, the shell executes many internal processes to interpret your command, and send it to the kernel then returns your results
    e. Types:
        i. Bourne-Again Shell (bash) $
        ii. C Shell (csh)
        iii. Korn Shell (ksh) $
        iv. Enhanced C shell (tcsh)
        v. Z shell (zsh) %
9. Input and Output in the shell
    a. Standard Input
        i. Information received by the OS via the command line
    b. Standard output
        i. Information returned by the OS through the shell
    c. Standard error
        i. Error messages returned by the OS through the shell

Week 3 – Navigate Linux File System, Bash Manage File Content, Authenticate/Authorize Users

1. Security Analysts must be able to:
    a. Work with server logs
    b. Navigate, manage, and analyze files remotely
    c. Verify and configure users and group access
    d. Give authorization and set file permissions
2. Bash
    a. The default shell in most Linux distributions
3. Argument (Linux)
    a. Specific information needed by a command
4. **All commands in Linux are <u>case sensitive</u>**
5. FHS is important because everything is considered a file in the eyes of a Linux OS
6. Root Directory
    a. The highest-level directory in Linux
7. Example of a root-branching directory
    a. /home/analyst
    first "/" means root directory
    then "home" sub-directory

second “/” means it’s branching out again
“analyst” sub-directory reached

8. Core Commands in Bash
    a. pwd: prints the working directory onto the screen
    b. ls: displays the names of files and directories in the current working directory
    c. cd: navigates between directories
    d. cat: displays the content of a file
    e. head: displays just the beginning of a file, by default 10 lines
        i. if you want a certain number of lines besides 10, specify with -n
            1. example: “head -n 5” for the first 5 lines of the item you are head’ing
    f. tail: display the last lines of a file, by default 10 lines
        i. you can use “tail” to read the most recent information in a log file
    g. less: returns the content of a file one page at a time
        i. space bar: move forward one page
        ii. b: move back one page
        iii. down arrow: move forward one line
        iv. up arrow: move back one line
        v. q: quit and return to the previous terminal window
9. FHS Expanded (how directories, directory contents, and other storage is organized in the operating system)



    a. A file’s location can be described by a file path
        i. location of a file or directory
    b. Standard FHS Directories:
        i. /home: each user in the system gets their own
        ii. /bin: stands for “binary”, contains binary files and other executables
            1. executables are files that contain a series of commands a computer need to function
        iii. /etc: location of system’s configuration files
        iv. /tmp: location of temporary files, commonly used by attackers because anyone in the system can modify data in these files
        v. /mnt: stands for “mount”, stores media such as USB drive and hard drives
    c. User-Specific Subdirectories
        i. under home are subdirectories for specific users
            1. each user has their own personal subdirectories
        ii. Note: when the path leads to a subdirectory below the user’s home directory, the user’s home directory can be represented as the tilde “~” thus “/home/analyst/logs” = “~/logs”
        iii. Absolute File Path: full file path
        iv. Relative File Path: path that starts from a user’s current directory

1. Note: relative file paths can use a dot "." to represent the current directory or two dots ".." to represent the parent of the current directory

10. Find what you need with Linux
    a. grep: searches a specified file and returns all lines in the file containing a specified string
        i. example: grep OS updates.txt
            <cmd> <argument> <argument>
    b. | (piping): send the standard output of one command as standard input to another command
        i. example: ls /home/analyst/reports | grep users
    c. find: searches for directories and files that meet specified criteria
        i. example: "find /home/analyst/project" searches for everything starting at the projects directory
        ii. -name: (case-sensitive), -iname (not case sensitive)
            1. example: finding all files in the projects directory that contain the world "log"
                find /home/analyst/projects -name "*log*"
                find /home/analyst/projects -iname "*log*"
        iii. -mtime: finding files within a certain time frame
            1. example: "find /home/analyst/project -mtime -3" returns all files and directories in the projects directory that have been modified within the past three days
            2. "-mtime +1" indicates all files or directories last modified more than one day ago
            3. "-mtime -1" indicates all files/directories last modified less than one day ago
        iv. -mmin: used for searching on minutes rather than days
11. Create and modify directories and files with Linux
    a. mkdir: creates a new directory
    b. rmdir: removes, or deletes, a directory (built in warning that directory may not be empty)
    c. touch: creates a new file
    d. rm: removes, or deletes, a file
    e. mv: moves a file or directory to a new location
        i. example: "mv email_policy.txt /home/analyst/drafts/"
            moves the text file to that new specified directory
    f. cp: copies a file or directory into a new location
        i. example: "cp vulnerabilities.txt /home/analyst/projects/"
            copies the text file to that new specified directory
12. "nano" command
    a. text editor for files
    b. example command: "nano vulnerabilities.txt"
    c. to save the changes made: ctrl + o, <enter>
    d. to exit after changes saved: ctrl + x
13. Standard output redirection with ">" and ">>"
    a. use of ">" and ">>" can redirect standard output
    b. ">" overwrites your existing file
    c. ">>" adds your content to the end of the existing file
14. Permissions
    a. The type of access granted for a file or directory
    b. remember: "authorization is the concept of granting access to specific resources in a system"
    c. Three types of permission in Linux
        i. read- content of file can be read, that's it
            1. if a directory, it's the ability to ready all contents in the directory including both files and their subdirectories

   ii. write- allows modifications of the content of the file
      1. if a directory, same concept as the read directory permission
   iii. execute- means the file can be executed if it's an executable
      1. directory execute access means you can enter into a directory and access its files
d. Types of owners in Linux:
   i. User: owner of the file
   ii. Group: a larger group that the owner is a part of
   iii. Other: all other users on the system
e. File permission "labels" in Linux
   i. 10-character string: "drwxrwxrwx"
      1. d: indicates files type (directory)
      2. "-" instead of "d": file
      3. 1st "rwx": user permissions (in this case, read, write, execute privs)
      4. 2nd "rwx": group permissions (in this case, same permissions as user)
      5. 3rd "rwx": other permissions (in this case, same permissions as user)

15. Options to displaying file permissions
   a. modify the behavior of the command
   b. ls -l: displays permission to files and directories
   c. ls -a: displays hidden files
   d. ls -la: displays permissions to files and directories, including hidden files
16. Change permissions (chmod)
   a. chmod: changes permissions on files and directories, stands for "change mode"
   b. example: chmod g+w, o-r access.txt
      grants write permission to group, removes read permission from other group to the "access.txt" file
   c. add all permissions to a text file
      i. chmod u+rwx,g+rwx,o+rwx textfile.txt
   d. remove all permissions to a text file
      i. chmod u-rwx,g-rwx,o-rwx textfile.txt
   e. using the "=" sign for changing permissions
      i. example: set read permissions for a text file for user, group and other:
         chmod u=r,g=r,o=r textfile.txt
   f. Summary table

Character	Description
u	indicates changes will be made to user permissions
g	indicates changes will be made to group permissions
o	indicates changes will be made to other permissions
+	adds permissions to the user, group, or other
-	removes permissions from the user, group, or other
=	assigns permissions for the user, group, or other

17. Root User (or superuser)
   a. A user with elevated privileges to modify the system
   b. Problems with logging in as root
      i. Security risks
      ii. Irreversible mistakes

iii. Accountability

18. sudo
    a. temporarily grants elevated permissions to specific users
    b. used to manage authorization and authentication
    c. “super user do”
    d. must be granted sudo access via sudo file
19. Commands requiring responsible use of sudo
    a. useradd
        i. adds a user to the system
            1. example: “sudo useradd salesrep7”
        ii. -g: sets the user’s default group, also called their primary group
            1. example: “sudo useradd -g security fgarcia” adds fgarcia as a new user and assigns their primary group to be security
        iii. -G: adds the user to additional groups, also called supplemental or secondary groups
            1. example: “sudo useradd -G finance,admin fgarcia” adds fgarcia as a new user and adds them to the existing finance and admin groups
    b. userdel
        i. deletes a user from the system
        ii. example: “sudo userdel salesrep7”
    c. usermod
        i. modifies existing user accounts
        ii. -g: changes the primary group of an existing user
            1. example: “sudo usermod -g executive fgarcia” changes fgarcia primary group to the executive group
        iii. -a -G: appends the user to an existing group
            1. example: “sudo usermod -a -G marketing fgarcia” adds fgarcia to the supplemental marketing group
            2. “-a -G” ensures that the new groups are added but existing groups aren’t replaced
        iv. -d: changes the user’s home directory
            1. example: “sudo usermod -d /home/garcia_f fgarcia” changes fgarcia’s home directory to “/home/garcia_f”
        v. -l: changes the user’s login name
        vi. -L: locks the account so the user can’t log in
    d. userdel
        i. deletes a user from the system
        ii. example: “sudo userdel fgarcia”
        iii. -r: must be used in order to delete the files in the user’s home directory
            1. example: “sudo userdel -r fgarcia”
    e. chown
        i. changes ownership of a file or directory
        ii. can use to change user or group ownership
        iii. example “change user owner of “access.txt” file to fgarcia
        “sudo chown :<insert new owner> access.txt”
            1. must enter “:” before “<insert new owner>” to designate it as a group name
20. Linux Community and In-House Resources
    a. consider Unix/Linux stack exchange
        i. https://unix.stackexchange.com/

b. man
    i. displays information on other commands and how they work
    ii. find information about “usermod”
        1. man usermod
c. whatis
    i. displays the description of a command on a single line
d. apropos
    i. searches the manual page descriptions for a specified string
    ii. example: apropos -a change password
        1. output is limited to the most relevant commands
    iii. “used to search for a command even if they **do not** know the specific command name”

Week 4 – Intro to SQL/Databases, SQL Queries/Filters/Joins

1. Database Basics
    a. Database
        i. an organized collection of information or data
        ii. accessed by multiple people simultaneously
        iii. stores massive amounts of data
    b. Relational Database
        i. a structured database containing tables that are related to each other
    c. Primary Key
        i. a column where every row has a unique entry
    d. Foreign Key
        i. a column in a table that is a primary key in another table
        ii. allows a connection between two tables
    e. SQL (Structured Query Language)
        i. a programming language used to create, interact with, and request information from a database
    f. Query
        i. a request for data from a database table or a combination of tables
    g. SQL Filtering vs Linux Filtering
        i. Accessing SQL
            1. Linux: via the command line
                a. example: enter “sqlite3”
        ii. Differences in filtering
            1. Structure
                a. SQL separates each record separated into columns
                b. Linux prints the data as a line of text without organization
                c. Overall, SQL is more readable
            2. Joining Tables
                a. SQL allows joining multiple tables together when returning data
                b. Linux doesn’t have this joining functionality
            3. Best Uses
                a. Databases needing multiple columns = SQL
                b. Large text files = Linux
2. SQL Basics
    a. SELECT
        i. indicates which columns to return
    b. FROM

i. indicates which table to query
ii. Example:
SELECT employee_id, device_id
FROM employees;
1. note: “;” must be placed at the end of a statement

c. ORDER BY
i. sequences the records returned by a query based on a specified column or columns
ii. can be either ascending or descending
iii. Example:
SELECT customerid, city, country
FROM customers
ORDER BY city;
iv. default ascending numeric order is smallest to largest
v. default ascending alphabetic character goes a->z
vi. using DESC for descending
1. Example:
SELECT customerid, city, country
FROM customers
ORDER BY city DESC;
vii. You can also sort by multiple items I.E., “ORDER BY country, city;”

3. Filtering Basics
a. Filtering
i. selecting data that match a certain condition
b. Operator
i. a symbol or keyword that represents an operation
ii. I.E., “country = ‘USA’”
c. WHERE
i. indicates the condition for a filter
d. example so far:
SELECT *
FROM log_in_attempts
WHERE country = ‘USA’;
e. “%” wildcard filter
i. substitutes for any number of other characters
ii. example
Filter for ‘East%’ returns
East-120
East-290
East-435
f. “_” wildcard filter
i. only substitutes for one other character

g. Wildcard Example Table:

Pattern	Results that could be returned
'a%'	apple123, art, a
'a_'	as, an, a7
'a__'	ant, add, a1c
'%a'	pizza, Z6ra, a
'_a'	ma, 1a, Ha
'%a%'	Again, back, a
'_a_'	Car, ban, ea7

h. LIKE (it's an operator, similar to the "=" sign)
   i. must be used with WHERE to search for a pattern in a column
   ii. example:
   SELECT *
   FROM log_in_attempts
   WHERE country LIKE 'US%';

4. Common Data Types
   a. String
      i. everything is treated as text
   b. Numeric
      i. just numbers, can be used with mathematical operations
   c. Date and Time
5. More Common Operators

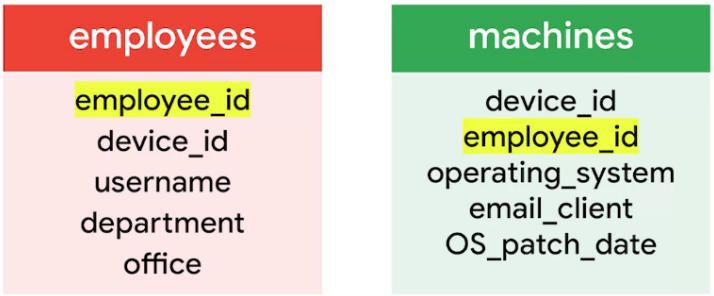
operator	use
<	less than
>	greater than
=	equal to
<=	less than or equal to
>=	greater than or equal to
<>	not equal to

   a. example query using greater than:
   SELECT firstname, lastname, birthdate
   FROM employees
   Where birthdate > '1970-01-01';

6. BETWEEN
   a. filters for numbers of dates within a range
      i. example:
      SELECT *
      FROM machines
      WHERE OS_patch_date BETWEEN '2021-03-01' AND '2021-09-01';
   b. numbers do not require quotation marks within the query
7. AND
   a. specifies that both conditions must be met simultaneously

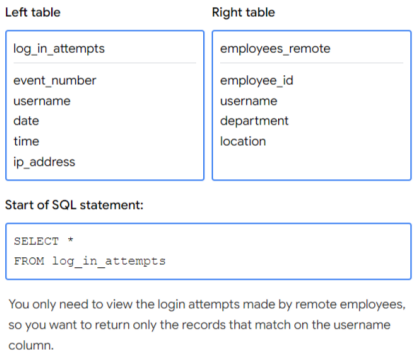
i. example:
SELECT *
FROM machines
WHERE operating_system = 'OS1' AND email_client = 'Email Client 1';

8. OR
   a. specifies that either condition can be met
   b. example:
   SELECT *
   FROM machines
   WHERE operating_system = 'OS1' OR operating_system = 'OS3';
9. NOT
   a. negates a condition
   b. example:
   SELECT *
   FROM machines
   WHERE NOT operating_system = 'OS3';
   c. can also use "WHERE operating_system **<>** 'OS3';
   or
   "WHERE operating_system **!=** 'OS3'
10. Combining Logical Operators
   a. example:
   SELECT firstname, lastname, email, country
   FROM customers
   WHERE NOT country = 'Canada' AND NOT country = 'USA';
11. Joining Tables in SQL
   a. example tables for referring to a column involving two tables:



   "employees" table with "employee_id" column = employees.employee_id
   b. INNER JOIN
      i. returns rows matching on a specified column that exists in more than one table
      ii. used when the primary key of the **first table** is used as a foreign key in the **second table**
      iii. example:
      SELECT username, office, operating_system
      FROM employees
      INNER JOIN machines ON employees.employee_id = machines.employee_id;

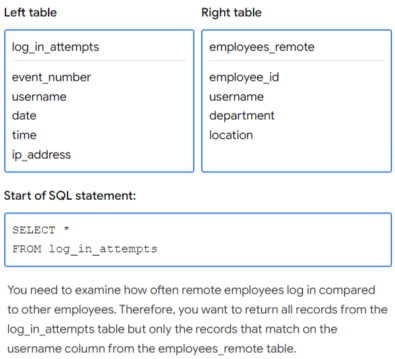
iv. Scenario Example:



c. Three Outer Joins (replaces “INNER JOIN”):

i. LEFT JOIN

1. returns all of the records on the first table, but only returns rows of the second table that match on a specified column
2. example query:
   Select *
   FROM employees
   LEFT JOIN machines ON employees.device_id = machines.device_id

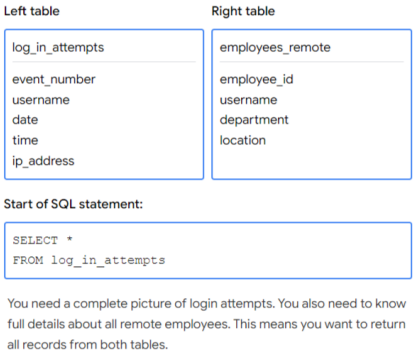


ii. RIGHT JOIN

1. returns all of the records of the second table, but only returns rows from the first table that match on a specified column
2. example query:
   Select *
   FROM employees

RIGHT JOIN machines ON employees.device_id = machines.device_id

iii. FULL OUTER JOIN
   1. returns all records from both tables
   2. example query:
      Select *
      FROM employees
      FULL OUTER JOIN machines ON employees.device_id = machines.device_id



12. Aggregate SQL Functions
   a. functions that perform a calculation over multiple data points and returns the result
   b. COUNT: returns a single number that represents the number of rows returned from your query
      i. example:
         SELECT COUNT(firstname)
         FROM customers
         WHERE country = 'USA';
   c. AVG: returns a single number that represents the average of the numerical data in a column
   d. SUM: returns a single number that represents the sum of the numerical data in a column

Course 5 – Assets, Threats, and Vulnerabilities | Instructor Da'Queshia

Week 1 – Introduction to Digital and Physical Assets, Risk and Asset Security

1. Risk
   a. anything that can impact the confidentiality, integrity, or availability of an asset
2. Security Risk Planning consists of:
   a. Assets
      i. an item perceived as having value to an organization

   b. Threats
      i. any circumstance or event that can negatively impact assets
   c. Vulnerabilities
      i. a weakness that can be exploited by a threat
3. Likelihood x Impact = Risk
   a. calculated to help:
      i. prevent costly and disruptive events
      ii. identify improvements that can be made to systems and processes
      iii. determine which risks can be tolerated
      iv. prioritize the critical assets that require attention
4. Risk Factors (broad) to be concerned with in the field:
   a. Threats
   b. Vulnerabilities
5. Categories of threat
   a. threat = circumstances or events that can negatively impact assets
   b. two types of threats
      i. intentional
      ii. unintentional
6. Categories of vulnerability
   a. vulnerability = weakness that can be exploited by threats
   b. two categories
      i. technical (I.E., misconfigured software)
      ii. human (I.E., forgetful employee who loses their access card in the parking lot
7. Asset Management
   a. the process of tracking assets and their risks that affect them
   b. why it matters / examples of assets
      i. digital assets such as customer data or financial records
      ii. information systems that process data, like networks or software
      iii. physical assets which can include facilities, equipment, or supplies
      iv. intangible assets such as brand reputation or intellectual property
   c. Asset Inventory
      i. a catalog of assets that need to be protected
   d. Asset Classification
      i. the practice of labeling assets based on sensitivity and importance to an organization
      ii. labeling usually involves:
         1. what you have
         2. where it is
         3. who owns it
         4. how important it is
      iii. levels of asset classification
         1. Public
            a. shared with anyone
         2. Internal-Only
            a. shared with anyone inside the organization along with business partners
         3. Confidential
            a. accessed by those only working on a specific project
            b. disclosure may lead to a significant negative impact on an organization

4. Restricted
    a. highly sensitive and must be protected
    b. need-to-know
    c. payment information

8. States Of Data
    a. In Use
        i. data being accessed by one or more users
    b. In Transit
        i. data traveling from one point to another
    c. At Rest
        i. data not currently being access
        ii. usually stored on a physical device
9. Information Security (InfoSec)
    a. the practice of keeping data in all states away from unauthorized users
10. Cloud-Based Services – a review
    a. SaaS: Software as a Service
        i. front-end applications that users access via a web browser
        ii. service providers host, manage, and maintain all of the back-end
        iii. examples: gmail, slack, zoom
    b. PaaS: Platform as a Service
        i. back-end application development tools that clients can access online
        ii. devs use these resources to write code and build, manage, and deploy their own apps
        iii. examples: google app engine platform, heroku, VMware cloud foundry
    c. LaaS: Infrastructure as a Service
        i. customers given remote access to a range of back-end systems
        ii. includes data processing servers, storage, networking resources
        iii. examples: google cloud platform, microsoft azure
    d. cloud responsibility model
        i. identity and access management
        ii. resource configuration
        iii. data handling
    e. security challenges
        i. misconfiguration
            1. ***biggest concern***
            2. customers are responsible for configuring their own security environment
        ii. cloud-native breaches
            1. most likely to occur due to misconfigured services
        iii. monitoring access might be difficult
            1. depends on the client and level of service
        iv. meeting regulatory standards
            1. particularly in industries required by law to follow HIPPA, PCI DSS, and GDPR
    f. cloud security resources
        i. U.K.'s National Cyber Security Center
            1. https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model
        ii. Cloud Security Alliance (organization dedicated to creating secure cloud environments)
            1. https://cloudsecurityalliance.org/

iii. CompTIA Cloud+ (program designed to teach foundational skills of a cloud security specialist)
1. https://www.comptia.org/blog/your-next-move-cloud-security-specialist

11. Types of Risk Categories
    a. Damage
    b. Disclosure
    c. Loss of Information
12. Elements of a Security Plan
    a. Policies
        i. set of rules that reduces risk and protects information
    b. Standards
        i. references that inform how to set policies
    c. Procedures
        i. step-by-step instructions to perform a specific security task
13. Compliance
    a. the process of adhering to internal standards and external regulations
14. Regulations
    a. rules set by a government or other authority to control the way something is done
15. NIST Cybersecurity Framework (CSF) – review
    a. a voluntary framework that consists of standards, guidelines, best practices to manage cybersecurity risk
    b. three main components:
        i. Core
            1. set of desired cybersecurity outcomes that help orgs. customize their security plan
            2. Five Functions:
                a. Identify (most important)
                b. Protect
                c. Detect
                d. Respond
                e. Recover
        ii. Tiers
            1. way of measuring the sophistication of an organization's cybersecurity program
            2. Four Tiers
                a. 1 (passive) – barely passing minimum standards, limited set of security controls have been implemented
                b. 2
                c. 3
                d. 4 (adaptive)- indication that a function is being performed at an exemplary standard
        iii. Profiles
            1. pre-made templates of the NIST CSF
            2. tailored to address the specific risks of an organization/industry
            3. helps develop a baseline for cybersecurity plans
16. Implementing the CSF
    a. **Create a current profile**: outline the specific needs of your business
    b. **Perform a risk assessment**: id which of your current ops are meeting business and regulatory standards
    c. **Analyze and prioritize existing gaps**: anything that places the businesses' assets at risk
    d. **Implement a plan of action**: will help achieve your organization's goals and objectives
    e. *note*: always consider current risk, threat, and vulnerability trends when using the NIST CSF

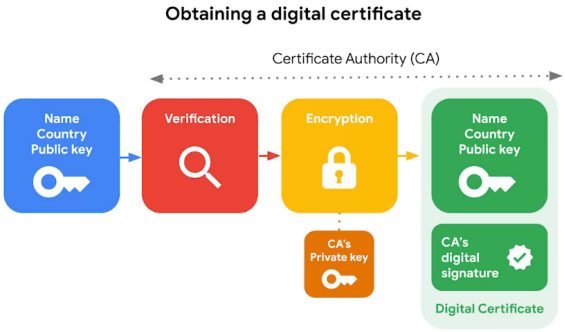
Week 2 – Safeguard Information, Encryption Methods, Authentication/Authorization/Accounting

1. Security Controls
    a. safeguards designed to reduce specific security risks
    b. Three types:
        i. Technical
            1. encryption, digital security means
        ii. Operational
            1. people-based
        iii. Managerial
            1. policies, standards, and procedures
2. Information Privacy
    a. the protection of unauthorized access and distribution of data
3. Data Owner
    a. the person that decides who can access, edit, use, or destroy their information
4. Data Custodian
    a. anyone or anything that's responsible for the safe handling, transport, and storage of information
5. Principle of Least Privilege
    a. security concept in which a user is only granted the minimum level of access and authorization required to complete a task or function
    b. fundamental security control that supports confidentiality, integrity, and availability (CIA)
    c. limiting access reduces risk
        i. limiting access to sensitive information
        ii. reducing the chances of accidental data modification, tampering, or loss
        iii. supporting system monitoring and administration
6. Determining Access and Authorization
    a. ask the questions
        i. who is the user
        ii. how much access do they need to a specified resource?
    b. most common types of user accounts
        i. Guest: provided to external users who need to access an internal network
        ii. User: assigned to staff based on their job duties
        iii. Service: granted to applications or software that needs to interact with other network software
        iv. Privileged: elevated permissions or administrative access
7. Auditing Account Privileges
    a. three common approaches:
        i. Usage Audit
            1. review which resources each account is accessing and what the user's doing with it
            2. helps identify whether a user has permissions that may need to be revoked
        ii. Privilege Audit
            1. known to help combat "privilege creep"
            2. assess whether a user's role is in alignment with the resources they have access to
        iii. Account Change Audit
            1. I.E., multiple attempts to change an account password
            2. ensures that all account changes are made by authorized users
8. The Data Lifecycle
    a. Collect

   b. Store
   c. Use
   d. Archive
   e. Destroy
9. Data Governance
   a. set of processes that define how an organization manages information
   b. includes policies that specify how to keep data private, accurate, available, and secure
   c. policies commonly categorize individuals into a specific role
      i. Data Owner: person that decides who can access/edit/use/destroy their information
      ii. Data Custodian: anyone or anything that's responsible for the safe handling, transport, and storage of information
      iii. Data Steward: the person or group that maintains and implements data governance policies set by an organization
   d. "Data Governance Policy"
      i. security plans including a specific policy that outlines how information will be managed across the organization
   e. As a data custodian you are responsible for ensuring that data isn't damaged, stolen, or misused.
10. Legally Protected Information
   a. PII
      i. information used to infer an individual's identity
      ii. information that can be used to contact or locate someone
   b. PHI (Protected Health Information)
      i. regulated by the Health Insurance Portability and Accountability Act (HIPAA)
         1. defines PHI as "information that relates to the past, present, or future physical/mental health/condition of an individual"
      ii. has similar definition in the EU but regulated by the GDPR
   c. SPII (Sensitive PII)
      i. specific type of PII that falls under stricter handling guidelines
      ii. S = "sensitive"
      iii. should only be accessed on a need-to-know basis
      iv. I.E., bank account number or login credentials
11. Information Security vs. Information Privacy
   a. privacy: refers to the protection of unauthorized access and distribution of data
      i. providing people with control over their personal information and how it's shared
   b. security (InfoSec): refers to the practice of keeping data in all states away from unauthorized users
      i. protecting people's choices and keeping their information safe from potential threats
12. Notable Privacy Regulations
   a. General Data Protection Regulation (GDPR)
      i. set by European Union (EU)
      ii. puts data owners in total control of their personal information
      iii. regards name, address, phone number, financial information, and medical information
      iv. note: a US based company that handles EU data is subject to GDPR provisions
   b. Payment Card Industry Data Security Standard (PCI DSS)
      i. aims to secure credit and debit card transactions against data theft and fraud
   c. Health Insurance Portability and Accountability Act (HIPAA)
      i. prohibits disclosure of a person's medical information without their knowledge and consent
13. Security Assessment vs. Audit

a. Audit: review of an organization's security controls, policies, and procedures against a set of expectations
    i. performed once a year (usually)
b. Assessment: check to determine how resilient current security implementations are against threats
    i. performed once every three to six months

14. Cryptography
    a. the process of transforming information into a form that unintended readers can't understand
15. Cipher
    a. an algorithm that encrypts information
16. Cryptographic Key
    a. a mechanism that decrypts ciphertext
17. Brute Force Attack
    a. a trial-and-error process of discovering private information
18. Public Key Infrastructure (PKI)
    a. an encryption framework that secures the exchange of information online
    b. The Two-Step Process:
        i. Exchange of encrypted information, asymmetric or symmetric
            1. Asymmetric Encryption
                a. the use of a public and private key pair for encryption and decryption of data
            2. Symmetric Encryption
                a. the use of a single secret key to exchange information
        ii. Establish trust using a system of digital certificates
            1. Digital Certificate
                a. a file that verifies the identity of a public key holder
                b. example of gaining trusted cert:

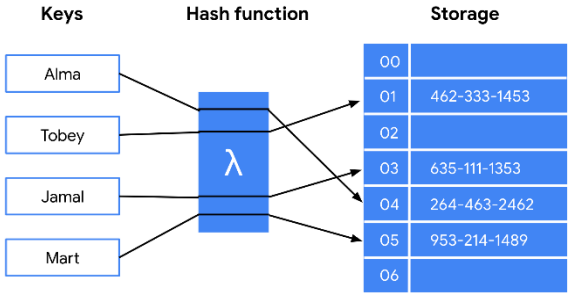


19. Approved Encryption Algorithms
    a. Symmetric
        i. Triple DES (3DES)
            1. "block cipher" by way of converting plaintext into ciphertext "blocks"
            2. traces back to Data Encryption Standard (DES)
                a. developed in 1970s
                b. one of the earliest symmetric encryption algorithms generating 64-bit keys
            3. uses 192-bit encryption
        ii. Advanced Encryption Standard (AES)
            1. one of the most secure symmetric algorithms
            2. generates 128/192/256-bit keys
            3. brute forcing an AES 128-bit key would take billions of years
    b. Asymmetric

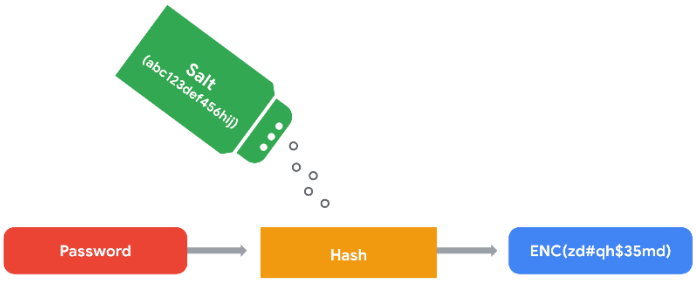
   i. Rivest Shamir Adleman (RSA)
      1. named after its three creators who developed it at MIT
      2. produces a public and private key pair
      3. key sizes: 1024, 2049, 4096
      4. used to protect highly sensitive data
   ii. Digital Signature Algorithm (DSA)
      1. standard introduced by NIST in early 1990s
      2. 2048-bit key length
      3. used as a complement to RSA in PKI

20. OpenSSL
    a. open-source command line tool used to generate public and private keys
    b. commonly used by computers to verify digital certs exchanged as part of PKI
    c. no longer recommended due to the Heartbleed Bug of 2014
21. Kerchoff's Principle
    a. cryptography should be designed in such a way that all the details of an algorithm, except for the private key, should be knowable without sacrificing its security
       i. example: you can access all the details about how AES works yet it's still unbreakable
22. Decrypting with a Caesar Cipher in Linux Bash
    example: openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute
    breakdown:
    openssl AES-256-CBC: reverses the encryption of the file with a secure symmetric cipher
    -pbkdf2: option used to add extra security to the key
    -a: indicates desired coding for the output
    -d: indicates decrypting
    -in: specifies the input file
    -out: specifies the output file
    -k: specifies the password (password is ettubrute in this example case)
23. Hash Function
    a. an algorithm that produces a code that can't be decrypted
    b. example hash function: sha256sum newfile.txt
24. Non-Repudiation
    a. the concept that the authenticity of information can't be denied
25. Origins of Hashing
    a. originally created as a way to quickly search for data
       i. meant to represent data of any size as small, fixed-size values, or digests
    b. Earliest hash function was Message Digest 5, also known as MD5
       i. developed by Professor Ronald Rivest of MIT
       ii. converts data into a 128-bit value

c. Example of how plaintext gets turned into hash values:



26. Hash Collisions
    a. an instance when different inputs produce the same hash value
    b. can be used to carry out collision attacks to fraudulently impersonate authentic data
27. Next Generation Hashing (NIST Approved)
    a. Secure Hashing Algorithms (SHA)
        i. Five functions make up the SHA family:
            1. SHA-1 (160-bit)
            2. SHA-224
            3. SHA-256
            4. SHA-384
            5. SHA-512
28. Secure Password Storage
    a. passwords are stored in a database mapped to a username, server receives a request for authentication that contains the credentials supplied by the user, looks up username in the database and compares password with the password inputted
    b. hashing would prevent a hacker from gaining these passwords because the store password would not be human-readable
29. Rainbow Tables
    a. file of pre-generated hash values and their associated plaintext
    b. like a dictionary of weak passwords
    c. hacker's will steal hashes and compare them against all possible table values
30. Salting
    a. additional safeguard used to strengthen hash functions
    b. salt- a random string of characters that's added to data before it's hashed
    c. helps produce a more unique hash value, thus resilient to rainbow table attacks

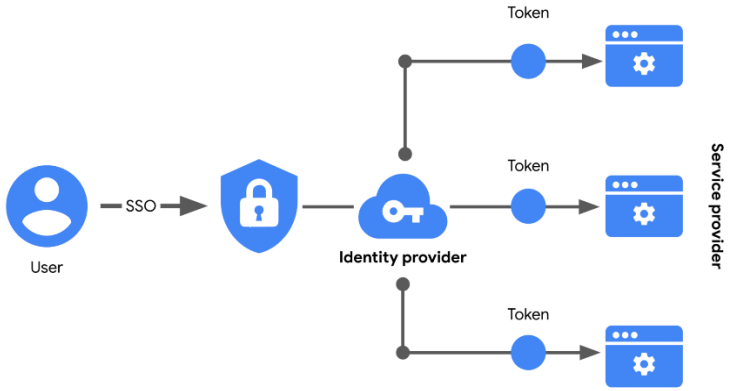


31. Access Controls
    a. security controls that manage access, authorization, and accountability of information
32. AAA Framework

a. Authentication
    i. “Who are you?”
    ii. Factors of authentication:
        1. Knowledge: something the user knows
            a. username/password
        2. Ownership: something the user possesses
            a. one-time passcode (OTP) sent via SMS
        3. Characteristic: something the user is
            a. fingerprints or facial scans
    iii. Single Sign-On (SSO)
        1. a technology that combines several different logins into one
        2. three reasons this is a good solution:
            a. improves the user experience by eliminating the number of usernames and passwords people have to remember
            b. companies can lower costs by streamlining how they manage connected services
            c. improves overall security by reducing the number of access points an attacker is able to target
    iv. Multi-Factor Authentication (MFA)
        1. a security measure which requires a user to verify their identity in two or more ways to access a system or network
b. Authorization
    i. Basic Auth
        1. the technology used to establish a user’s request to access a server
    ii. OAuth
        1. an open-standard authorization protocol that shares designated access between apps
        2. uses API tokens
            a. a small block of encrypted code that contains information about a user
            b. serve as an additional layer of encryption
c. Accounting
    i. practice of monitoring the access logs of a system

33. SSO Functionality Explained
    a. automated how trust is established between a user and a service provider
    b. uses third-parties to prove that a user is who they claim to be
    c. done via exchange of encrypted access tokens between the identity provider and the service provider
    d. token exchange relies on two protocols:
        i. Lightweight Directory Access Protocol (LDAP): transmitting information on-premises
        ii. Security Assertion Markup Language: transmitting information off-premises (cloud)

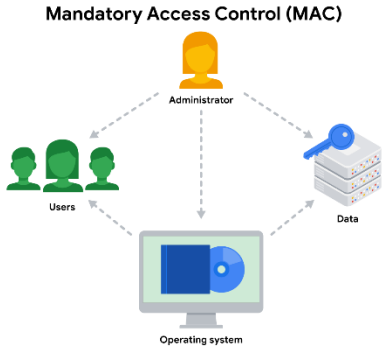
e. example of SSO use when connecting a user to multiple applications with one access token:



f. limitations
    i. a lost or stolen password could expose information across multiple services
        1. solution = MFA

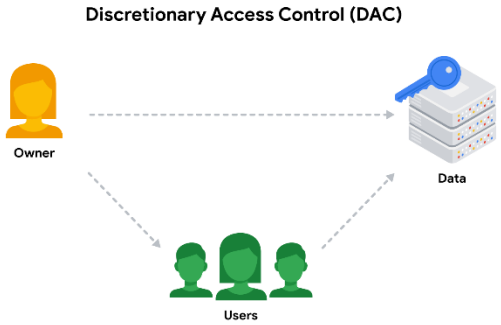
34. Session
    a. a sequence of network HTTP basic auth requests and responses associated with the same user
    b. involves two main functions:
        i. Session ID
            1. a unique token that identifies a user and their device while accessing the system
        ii. Session Cookie
            1. a token that websites use to validate a session and determine how long that session should last
35. Session Hijacking
    a. an event when attackers obtain a legitimate user's session ID
36. Identity and Access Management (IAM)
    a. a collection of processes and technologies that helps organizations manage digital identities in their environment
    b. both AAA and IAM systems are designed to:
        i. authenticate users
        ii. determine their access privileges
        iii. track their activities within a system
    c. it ensures the **right user** is granted access to the **right resources** at the **right time** for the **right reasons**
37. User Provisioning
    a. process of creating and maintaining a user's digital identity
    b. removing a user's access rights when they should no longer have them
38. Granting Authorization

a. Mandatory Access Control (MAC)



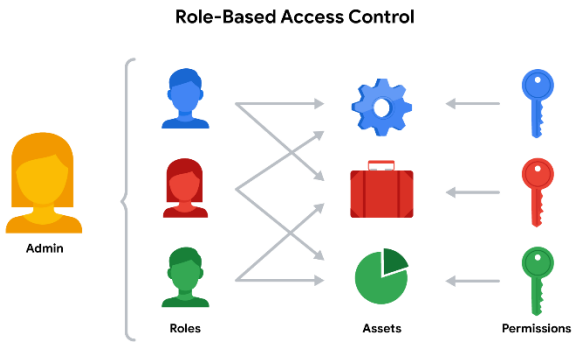
   i. strictest of the three frameworks
   ii. based on a strict need-to-know basis
   iii. access to information granted manually by central authority or system administrator
   iv. applied in law enforcement, military and government agencies
   v. also known as “non-discretionary” control because access isn’t given at the discretion of the data owner

b. Discretionary Access Control (DAC)



   i. applied when a data owner decides appropriate levels of access
   ii. example: owner of a google drive folder shares editor, viewer, or commentor access with others

c. Role-Based Access Control (RBAC)



   i. determined via user’s role within an organization
   ii. example: user in marketing department has access to user analytics but not network admin

39. Resource for staying informed on the identity and access management industry
   a. https://idpro.org/

Week 3 – Flaws in the System, Identity System Vulnerabilities, Cyber Attacker Mindset

1. Term Review
    a. Vulnerability- a weakness that can be exploited by a threat
    b. Exploit- a way of taking advantage of a vulnerability
    c. Example of vulnerability/exploit relationship
        i. A house has windows that are weak to rock (vulnerability), a theft who is trying to break in will smash the windows with a rock (exploit)
2. Vulnerability Management
    a. The process of finding and patching vulnerabilities
    b. Four steps:
        i. Identify vulnerabilities
        ii. Consider potential exploits
        iii. Prepare defenses against threats
        iv. Evaluate those defenses
3. Zero-Day
    a. An exploit that was previously unknown
4. Defense In Depth
    a. A layered approach to vulnerability management that reduces risk
    b. Five Layers
        i. Perimeter Layer
            1. usernames and passwords/user authentication layer
        ii. Network Layer
            1. authorization
            2. I.E. Firewalls
        iii. Endpoint Layer
            1. laptop, desktop, server
            2. I.E. Anti-virus software
        iv. Application Layer
            1. all interfaces used to interact with technology
            2. I.E. MFA
        v. Data Layer
            1. any information that's stored, in transit, or in use
            2. I.E. Asset classification
5. Exposure
    a. a mistake that can be exploited by a threat
6. Common Vulnerabilities and Exposures list (CVE List)
    a. An openly accessible dictionary of known vulnerabilities and exposures
    b. Created by MITRE
        i. a collection of non-profit research and development centers
        ii. sponsored by U.S. Government
    c. offer standard way of identifying and categorizing vulnerabilities and exposures
7. Anyone can report to the CVE
    a. must go through a strict vetting process via CVE Numbering Authority (CNA)
        i. an organization that volunteers to analyze and distribute information on eligible CVEs
    b. CVE List Criteria
        i. Independent of other issues
        ii. Recognized as a potential security risk

    iii. Submitted with supporting evidence
    iv. Only affect one codebase (one program source code)
8. Common Vulnerability Scoring System (CVSS)
    a. a measurement system that scores the severity of a vulnerability
    b. used by the NIST National Vulnerabilities Database
9. Open Web Application Security Project (OWASP)
    a. a nonprofit foundation that works to improve the security of software
10. OWASP “Top 10”
    a. published since 2003 as a way to spread awareness of the web’s most targeted vulnerabilities
    b. updated every few years as technologies evolve
11. OWASP Top 10 Vulnerabilities
    a. Broken Access Control
        i. limits what user can do in a web application
    b. Cryptographic failures
        i. happens with weak hashing algorithms or failure to properly encrypt sensitive data
    c. Injection
        i. when malicious code is inserted into a vulnerable application
        ii. common target would be a website’s login form in order to steal credentials
    d. Insecure Design
        i. applications should be resilient to attack
    e. Security Misconfiguration
        i. when security settings aren’t properly set or maintained
        ii. example: when businesses deploy equipment using default settings
    f. Vulnerable and Outdated Components
        i. refers to application development
    g. Identification and Authentication Failures
        i. when applications fail to recognize who should have access and what they’re authorized to do
    h. Software and Data Integrity Failures
        i. when updates or patches are inadequately reviewed before implementation
        ii. likely to lead to a “supply chain attack”
        iii. refer to https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
    i. Security Logging and Monitoring Failures
        i. must be able to log and trace back events
    j. Server-Side Request Forgery (SSRF)
        i. when attackers manipulate the normal operations of a server to read or update other resources on that server
12. Information vs Intelligence
    a. Information: refers to the collection of raw data or facts about a specific subject
    b. Intelligence: analysis of information to produce knowledge or insights that can be used
13. Information Security (InfoSec)
    a. practice of keeping data in all states away from unauthorized users
14. Using OSINT to generate intelligence:
    a. provide insights into cyber attacks
    b. detect potential data exposures
    c. evaluate existing defenses

    d. identify unknown vulnerabilities
15. OSINT Tools
    a. VirusTotal- Analyze suspicious files, domains, URLs, and IP addresses
        i. https://www.virustotal.com/gui/home/upload
    b. MITRE ATT&CK- knowledge base of adversary tactics and techniques based on real-world observation
        i. https://attack.mitre.org/
    c. OSINT Framework- web-based interface where you can find OSINT tools for any kind of source/platform
        i. https://osintframework.com/
    d. Have I been Pwned- used to search for breached email accounts
        i. https://haveibeenpwned.com/
16. Vulnerability Assessment
    a. the internal review process of an organization's security systems
    b. 4 steps:
        i. Identification
        ii. Vulnerability Analysis
        iii. Risk Assessment
        iv. Remediation
17. Vulnerability Scanner
    a. software that automatically compares known vulnerabilities and exposures against the technologies on the network, can help find misconfigurations or programming flaws
18. Performing Scans
    a. Should be non-intrusive
    b. External vs Internal
        i. External
            1. test the perimeter layer outside of the internal network
            2. analyze outward facing systems like websites and firewalls
        ii. Internal
            1. examines organization's internal systems such as application software
    c. Authenticated vs Unauthenticated
        i. Authenticated
            1. test a system by logging in with a real user account or even with an admin account
            2. used to check for vulnerabilities like broken access controls
        ii. Unauthenticated
            1. simulate external threat actors that do not have access to your business or resources
            2. I.E. Analyzing file shares within the organization that are used to house internal-only documents, unauthenticated users should receive "access denied" results
    d. Limited vs Comprehensive
        i. Limited
            1. analyzes particular devices on a network
        ii. Comprehensive
            1. analyzes all devices connected to a network, including operating systems and user databases and more
19. Patch Update
    a. software and operating system update that addresses security vulnerabilities within a program
    b. usually contains bug fixes that address common security vulnerabilities and exposures
20. Common Update Strategies
    a. Manual

i. Advantages
    1. strategies of control
ii. Disadvantages
    1. can be forgotten or disregarded entirely

b. Automatic (Recommended by The Cybersecurity and Infrastructure Security Agency (CISA)
i. Advantages
    1. deployment process is simplified
    2. systems and software stay current with the latest, critical patches
ii. Disadvantages
    1. if patches are not thoroughly tested by the vendor, can result in instability and performance problems in end-user experience

21. End-of-Life Software
    a. older software is still useful while the manufacturer no longer supports it
    b. upgrade = completely new version s of hardware of software that can be purchased
22. Penetration Test
    a. simulated attack that helps identify vulnerabilities in a system, networks, websites, etc.
    b. Red Team Test: simulates attacks to identify vulnerabilities
    c. Blue Team Test: focuses on defense and incident response to validate an organization's security
    d. Purple Team Test: collaborative, focusing on improving security posture of the organization by combining elements of red and blue team exercises
    e. Strategies
        i. Open-box Testing
            1. when the tester has the same privileged access that an internal developer would have
            2. aka internal, full knowledge, white-box, clear box
        ii. Closed-Box Testing
            1. when tester has little to no access to internal systems- similar to malicious hacker
            2. aka external, black-box, zero knowledge
        iii. Partial Knowledge
            1. tester has limited access and knowledge of internal system
            2. aka gray-box
    f. Skills needed for pen testing
        i. network and application security
        ii. experience with operating systems
        iii. vulnerability analysis and threat modeling
        iv. detection and response tools
        v. programming languages
        vi. communication skills
    g. Bug Bounty Programs
        i. giving freelance pen testers financial rewards for finding and reporting vulnerabilities in their products
23. Security Hardening
    a. the process of strengthening a system to reduce its vulnerabilities and attack surface
24. Simulating threats
    a. applying an attacker mindset by proactively and or reactively making the system safer
    b. Proactive Simulation: assume the role of an attacker by exploiting vulnerabilities and breaking through defenses
        i. I.E. "Red Team Exercise"

    c. Reactive Simulation: role of a defender responding to an attack
        i. I.E. “Blue Team Exercise”
25. Vulnerability Scanner- Example
    a. Identification: a vulnerable server is flagged b/c it’s running an outdated OS
    b. Vulnerability Analysis: Research is done on the outdated OS and its vulnerabilities
    c. Risk Assessment: After doing due diligence, the severity of each vulnerability is scored and the impact of not fixing it is evaluated
    d. Remediation: The information that you’ve gather can be used to address the issue
26. https://nvd.nist.gov/ to remain current on common vulnerabilities
27. Threat Actor Types (someone who presents a security risk)
    a. Competitor: rival companies who pose a threat because they might benefit from leaded information
    b. State Actors: government intelligence agencies
    c. Criminal Actors: organized groups of people who make money from criminal activity
    d. Insider Threats: any individual who has or had authorized access
    e. Shadow IT: individuals who use technologies that lack IT governance
        i. example: when an employee uses their personal email to send work-related communications
28. Types of Hackers
    a. Unauthorized hackers
    b. Authorized, or ethical, hackers
    c. Semi-Authorized hackers
29. Advanced Persistent Threat (APT)
    a. when a threat actor maintains unauthorized access to a system for an extended period of time
    b. associated with nation states and state-sponsored actors
    c. concerned with surveilling a target to gather information
30. Access Points
    a. Direct access- physical access to the system
    b. Removable media- portable hardware, USB flash drives
    c. Social media platforms- content sharing
    d. Email- personal and business accounts
    e. Wireless networks- on premises
    f. Cloud Services- provided by third-party organizations
    g. Supply chains- third-party vendors that can present a backdoor into systems
31. Attack Vectors
    a. the pathways attackers use to penetrate security defenses
32. Practicing an attacker mindset
    a. Identify a target
    b. Determine how the target can be accessed
    c. Evaluate the attack vectors that can be exploited
    d. Find the tools and methods of attack
33. Defending Attack Vectors
    a. Educating users
    b. Applying principle of least privilege
    c. Using the right security controls and tools
    d. Building a diverse security team
34. Brute Force Attack: A matter of trial and error
    a. Simple brute force
        i. attackers guess a user’s login credentials, trying multiple combinations until they get it right

   b. Dictionary attack
      i. attackers use a list of commonly used credentials to access a system
   c. Reverse brute force
      i. similar to dictionary attack, but starting with a single credential and try it in various systems
   d. Credential stuffing
      i. attackers use stolen login credentials from previous data breaches to access user accounts at another organization
      ii. specialized type is called “pass the hash”
         1. attackers reuse stolen, unsalted hashed credentials to trick an authentication system into creating a new authenticated user session on the network
35. Tools of the trade (brute force)
   a. Aircrack-ng
   b. Hashcat
   c. John the Ripper
   d. Ophcrack
   e. THC Hydra
36. Brute force prevention measures
   a. Hashing and salting
   b. Multi-factor authentication
   c. CAPTCHA
   d. Password policies

Week 4 – Social Engineering, Malware, Web-Based Exploits, Threat Modeling

1. Social Engineering
   a. a manipulation technique that exploits human error to gain private information, access, or valuables
2. Stages of Social Engineering
   a. prepare
   b. establish trust
   c. use persuasion tactics
   d. disconnect from the target
3. Preventing social engineering
   a. implementing managerial controls
   b. staying informed of trends
   c. sharing your knowledge with others
4. Common types of social engineering
   a. Baiting
      i. tempts people into compromising their security
      ii. USB baiting- relies on someone finding an infected USB and plugging it into their device
   b. Phishing
      i. use of digital communications to trick people into revealing sensitive data
      ii. typically performed via email
   c. Quid Pro Quo
      i. type of baiting used to trick someone into believing they’ll be rewarded in return for sharing access, information, or money
      ii. impersonating a loan officer at a bank and call customers offering them a lower interest rate if they provide their account details to claim the deal
   d. Tailgating
      i. unauthorized people follow an authorized person into a restricted area

        ii. also known as piggybacking
    e. Watering Hole
        i. when a threat actor compromises a website frequently visited by a specific group of users
5. Encouraging caution of social engineering
    a. Stay alert
    b. Be cautious
    c. Control curiosity
6. Phishing
    a. the use of digital communications to trick people into revealing sensitive data or deploying malicious software
7. Phishing Kit
    a. a collection of software tools needed to launch a phishing campaign
    b. Three main tools
        i. malicious attachments
        ii. fake data-collection forms
        iii. fraudulent web links
8. Review of terms
    a. Smishing- user of text messages to obtain sensitive information or to impersonate a known source
    b. Vishing- exploitation of electronic voice communication
    c. Spear Phishing- subset of email phishing in which specific people are purposefully targeted
    d. Whaling- category of spear phishing aimed at high-ranking executives
    e. Angler Phishing- when attackers impersonate customer service representatives on social media
9. Phishing security measures
    a. anti-phishing policies
    b. employee training resources
    c. email filters
    d. intrusion prevention systems
10. Malware- software designed to harm devices or networks
11. Types of Malware
    a. virus
        i. malicious code written to interfere with computer operations and cause damage to data and software
        ii. must be activated to start infection
    b. worm
        i. malware that can duplicate and spread itself across systems on its own
        ii. uses an infected device as a host
        iii. doesn’t need an action to trigger replication
    c. trojan
        i. malware that looks like a legitimate file or program
        ii. disguised as files or trusted applications
    d. ransomware
        i. type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access
        ii. attackers will make themselves known to the target
    e. spyware
        i. malware that’s used to gather and sell information without consent
        ii. A type of PUA

iii. commonly hidden in bundleware

f. Adware
    i. type of legitimate software that is sometimes used to display digital advertisements in applications
        1. Potentially Unwanted Application (PUA)
            a. malicious adware
            b. bundled with legitimate programs

g. Scareware
    i. type of malware that employs tactics to frighten users into infecting their own device
    ii. comes in emails and fake pop-ups

h. Fileless Malware
    i. does not need to be installed because it uses legitimate programs already installed to infect a person's computer
    ii. resides in memory where the malware never touches the hard drive
    iii. can get into operating system or hide within trusted applications

i. Rootkit
    i. malware that provides remote, administrative access to a computer
    ii. often spread by two components:
        1. dropper- type of malware that comes packed with malicious code which is deliver and installed onto a target system
            a. often disguised as a legitimate file or executable, if the user opens the dropper program, its malicious code is executed and hides itself on the target system
        2. loader- type of malware that downloads strains of malicious code from an external source and installs them onto a target system

j. Botnet
    i. short for "robot network"
    ii. collection of computers infected by malware under the control of a single "bot-herder"

k. Cryptojacking
    i. a form of malware that installs software to illegally mine cryptocurrencies

l. Signs of infection
    i. slowdown
    ii. increased cpu usage
    iii. sudden system crashes
    iv. fast draining batteries
    v. unusually high electricity costs

12. Web-Based Exploits
    a. malicious code or behavior that's used to take advantage of coding flaws in a web application
13. Injection Attack
    a. malicious code inserted into a vulnerable application
14. Cross-Site Scripting (XSS)
    a. an injection attack that inserts code into a vulnerable website or web application
    b. usually exploits JavaScript and HTML
    c. three types:
        i. reflected
            1. an instance when malicious script is sent to a server and activated during the server's response
        ii. stored

1. an instance when malicious script is injected directly on the server

iii. Document Object Model (DOM)-based

1. an instance when malicious script exists in the webpage a browser loads
2. a malicious script can be seen in the URL

15. SQL Injection
    a. an attack that executes unexpected queries on a database
    b. categories
        i. In-band
            1. uses the same communication channel to launch the attack and gather the results
            2. example: search box of a retailer's website that lets customers find products to buy, an attacker could enter a malicious query that would be executed in the database
        ii. Out-of-band
            1. uses a different communication channel to launch the attack and gather the results
            2. example: attacker uses a malicious query to create a connection between a vulnerable website and a database they control, the separate channel allows them to bypass any security controls in place on the website's server
        iii. Inferential
            1. when an attacker is unable to directly see the results of the attack, results interpreted by the behavior of the system
            2. example: attacker performs an SQL injection attack on the login form of a website that causes the system to respond with an error message, attacker can figure out the database's structure based on the error
16. Preventing SQL Injection
    a. Prepared Statement
        i. a coding technique that executes SQL statements before passing them onto the database
    b. Input Sanitization
        i. removes user input which could be interpreted as code
    c. Input Validation
        i. ensures user input meets a system's expectations
17. Threat Modeling
    a. the process of identifying assets, their vulnerabilities, and how each is exposed to threats
18. Six Steps of Threat Modeling
    a. Define the scope
    b. Identify threats
        i. creating an Attack Tree- a diagram of mapping threats to assets
    c. Characterize the environment
    d. Analyze threats
    e. Mitigate risks
    f. Evaluate findings
19. PASTA
    a. a popular threat modeling framework that's used across many industries
    b. **P**rocess for
       Attack
       Simulation and
       Threat
       Analysis
    c. Three goals:

        i. Improve security goals
        ii. Document potential risks
        iii. Prepare fixes
20. PASTA threat model framework (7 Steps) (risk centric)
    a. Define business and security objectives
    b. Define the technical scope
    c. Decompose the application
    d. Perform a threat analysis
    e. Perform a vulnerability analysis
    f. Conduct attack modeling (Attack Tree)
    g. Analyze risk and impact
21. STRIDE
    a. threat-modeling framework developed by Microsoft
    b. used to identify vulnerabilities in six specific attack vectors:
        i. spoofing
        ii. tampering
        iii. repudiation
        iv. information disclosure
        v. denial of service
        vi. elevation of privilege
22. Trike
    a. open-source methodology and tool
    b. commonly used to focus on security permissions, application use cases, and privilege models
23. Visual, Agile, and Simple Threat (VAST)
    a. part of automated threat-modeling platform called ThreatModeler
    b. used as a way of automating and streamlining threat modeling assessments
24. Asking the right questions about threat modeling
    a. What are we working on?
    b. What kinds of things can go wrong?
    c. What are we doing about it?
    d. Have we addressed everything?
    e. Did we do a good job?

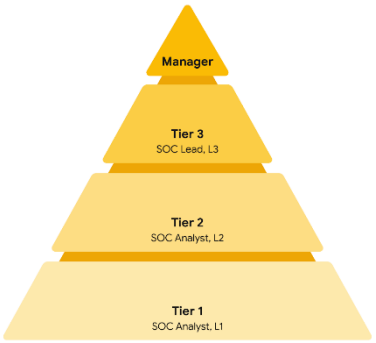
Course 6 – Sound the Alarm: Detection and Response | Instructor Dave

Week 1 – The Incident Response Lifecycle, Incident Response Operations and Tools

1. Incident
    a. an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies
2. Event
    a. an observable occurrence on a network, system, or device
3. The NIST Incident Response Lifecycle
    a. Preparation
    b. Detection and Analysis
    c. Containment, Eradication, and Recovery
    d. Post-Incident Activity
4. The 5 W's of an Incident

a. who triggered the incident
b. what happened
c. when the incident took place
d. where the incident took place
e. why the incident occurred

5. Incident handler's journal
    a. a form of documentation used in incident response
6. Computer Security Incident Response Teams (CSIRT)
    a. a specialized group of security professionals that are trained in incident management and response
    b. goals
        i. manage incidents
        ii. provide services and resources for response and recovery
        iii. prevent future incidents from occuring
    c. Roles
        i. Security Analyst
            1. monitors an environment for any security threats including
                a. analyzing and triaging alerts
                b. performing root-cause investigations
                c. escalating or resolving alerts
        ii. Technical Lead (ops lead)
            1. manages all technical aspects of the incident response process, such as applying software patches or updates
            2. creates and implements the strategies for containing, eradicating, and recovering from the incident
            3. collaborates with other teams to ensure incident response priorities align with business priorities such as reducing disruptions for customers and returning to normal operations
        iii. Incident Coordinator
            1. coordinates with relevant departments during a security incident
            2. lines of communication are open and clear
            3. all personnel are made aware of the incident status
            4. tracks and manages the activities of all teams involved in the response team
    d. Requires the 3 C's
        i. Command- having the appropriate leadership and direction to oversee the response
        ii. Control- ability to manage technical aspects during incident response, like coordinating resources and assigned tasks
        iii. Communication- ability to keep stakeholders informed
7. SOC organization



    a. Tier 1 SOC Analyst (L1)

        i. monitoring, reviewing, and prioritizing alerts based on criticality or severity
        ii. creating and closing alerts using ticketing systems
        iii. escalating to Tier 2 or Tier 3
    b. Tier 2 SOC Analyst (T2)
        i. more experienced analysts
        ii. receives escalated tickets form L1 for deeper investigation
        iii. configures and refines security tools
        iv. reports to the SOC Lead
    c. Tier 3 SOC Lead (L3)
        i. highly experienced professionals
        ii. manages operation of their team
        iii. explores methods of detection by performing advanced detection techniques
        iv. malware and forensics analysis
        v. reports to the SOC manager
    d. SOC Manager
        i. hires, trains, and evaluates SOC team members
        ii. creates performance metrics and manages the performance of the SOC team
        iii. develops reports related to incidents, compliance, and auditing
        iv. communicates findings to stakeholders such as executive management
    e. Other roles
        i. Forensic Investigators
            1. commonly L2s and L3s
            2. collects, preserves, and analyzes digital evidence to determine what happened
        ii. Threat Hunters
            1. L3s
            2. works to detect, analyze, and defend against new and advanced cybersecurity threats using threat intelligence
8. Incident Response Plan
    a. a document that outlines the procedures to take in each step of incident response
9. Elements of an Incident Plan
    a. Incident response procedures
    b. System Information
    c. Other documents
10. Tools for incident response
    a. detection and management
    b. documentation
        i. playbooks
        ii. incident handler’s journals
        iii. policies
        iv. plans
        v. final reports
    c. investigative
11. word processor tools
    a. Google Docs
    b. OneNote
    c. Evernote
    d. Notepad++

12. Intrusion Detection System (IDS)
    a. an application that monitors system and network activity and produces alerts on possible intrusions
13. Intrusion Prevention Systems (IPS)
    a. same as IDS but can take action to stop the activity
14. IDS and IPS tools
    a. Snort
    b. Zeek
    c. Kismet
    d. Sagan
    e. Suricata
15. Detection Tool Overview

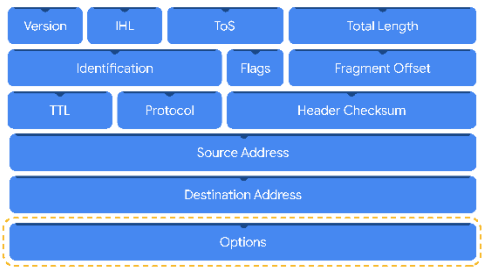
Capability	IDS	IPS	EDR
Detects malicious activity	✓	✓	✓
Prevents intrusions	N/A	✓	✓
Logs activity	✓	✓	✓
Generates alerts	✓	✓	✓
Performs behavioral analysis	N/A	N/A	✓

16. Detection Categories
    a. true positive- correct detection of an attack
    b. true negative- no malicious activity exists and no alert is triggered
    c. false positive- flagged as malicious activity, but it wasn't
    d. false negative- there was malicious activity, but IDS/IPS/EDR failed to detect it
17. Endpoint Detection and Response
    a. application that monitors an endpoint for malicious activity
    b. installed on any endpoint like device, computer, phone, tablet etc.
    c. collects endpoint activity data to perform behavioral analysis to identify threat patterns
    d. examples: Open EDR, Bitdefender, FortiEDR
18. SIEM Process
    a. collect and aggregate data
        i. the process of consolidating log data into a centralized place
    b. normalize data
        i. take raw data, clean it up, make it human readable
        ii. data must be transformed into a single format so it's easily processed by the SIEM
    c. analyze data
        i. done with a type of detection logic such as a set of rules and conditions
19. SIEM Advantages
    a. access to event data and real-time activity
    b. monitoring, detecting, and alerting
    c. log storage
20. Security Orchestration, Automation, and Response (SOAR)
    a. a collection of applications, tools, and workflows that uses automation to **respond** to security events
21. Example log format and what each component means
    a. April 3 11:01:21 server sshd[1088]: Failed password for user nuhara from 218.124.14.105 port 5023
       host = server
       process = sshd

source_user = nuhara
source ip = 218.124.14.105
source port = 5023

Week 2 – Understanding Network Traffic, Capturing/Viewing Traffic, Packet Inspection

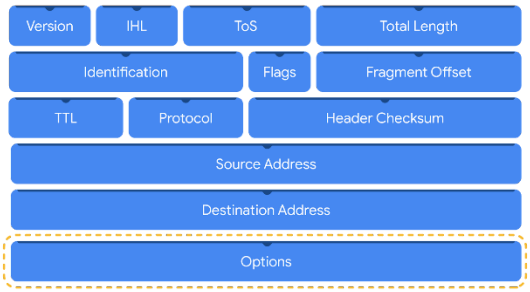
1. Network Traffic
    a. the amount of data that moves across a network
2. Indicators of Compromise (IOC)
    a. observable evidence that suggests signs of a potential security incident
    b. they provide a way to identify an attack
3. Data exfiltration
    a. unauthorized transmission of data from a system
4. Command and Control (C2)
    a. when malicious actors can use protocols and ports that are not commonly associated to maintain communications between the compromised system and their own machine
5. Lateral Movement
    a. an attacker has infiltrated a network, they spend time exploring it in order to expand and maintain their access, they look for valuable assets such as proprietary code and financial records
6. Temporal Patterns
    a. observe what the baseline network traffic is during work hours in order to gauge future intrusions
7. Network Operations Center (NOC)
    a. organizational unit that monitors the performance of a network and responds to any network disruption
    b. responsible for maintaining network performance, availability, and uptime
8. Network Protocol Analyzer
    a. A.K.A. “packet sniffer”
    b. used to analyze network communications manually in detail
    c. examples are tcpdump and Wireshark
9. Defensive Measures
    a. prevent attacker access
    b. monitor network activity
    c. protect assets
    d. detect and stop the exfiltration
10. Components of a packet – review
    a. Header
        i. contains information such as ethernet header, ip header, tcp header, source and dest. address



    b. Payload
        i. immediately follows the header and contains the actual data being delivered
    c. Footer
        i. known as the trailer

   ii. provides error-checking information to determine if the data has been corrupted
   iii. most protocols, such as Internet Protocol (IP), do not use footers

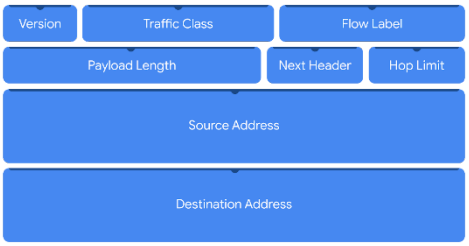
11. Packet Capture (P-cap)
    a. a file containing data packets intercepted from an interface or a network
12. Different types of P-caps
    a. Libpcap
       i. packet capture library designed to be used by Unix-like systems (Linux and MacOS)
       ii. used by tcpdump
    b. WionPcap
       i. open-source packet capture for devices running Windows OS
       ii. considered older file format
    c. Npcap
       i. library designed by the port scanning tool Nmap
       ii. common in Windows OS
    d. PCAPng
       i. modern file format
       ii. can simultaneously capture packets and store data
       iii. ng = “next generation”
13. IPv4 Header Breakdown – Review



    a. Version
       i. which internet protocol is being use (IPv4 or IPv6)
    b. IHL
       i. Internet Header Length
    c. TOS
       i. packet priority for delivery
       ii. whether this packet should be treated differently
    d. Total Length
       i. includes length of the entire packet including the headers and the data
    e. Identification, Flags, Fragment Offset
       i. related to data fragmentation (when an IP packet gets broken up into chunks, transferred over the wire, then re-assembled at the destination)
    f. Time to Live (TTL)
       i. how many times the packet can be routed before it gets dropped
    g. Protocol
       i. TCP = 6
    h. Header Checksum
       i. used to determine any errors
    i. Source IP Address

j. Destination IP Address
k. Options (not required)

14. IPv6 Header Breakdown



a. Version
    i. IP version (IPv6)
b. Traffic Class
    i. similar to IPv4 TOS field
    ii. provides information about the packet's priority or class to help with packet delivery
c. Flow Label
    i. flow = sequence of packets sent from a specific source
d. Payload Length
    i. specifies length of the data portion of the packet
e. Next Header
    i. type of header that follows the IPv6 header such as TCP
f. Hop Limit
    i. Same as IPv4's TTL
g. Source Address
h. Destination Address

15. Wireshark
    a. Comparison Operators

Operator type	Symbol	Abbreviation
Equal	==	eq
Not equal	!=	ne
Greater than	>	gt
Less than	<	lt
Greater than or equal to	>=	ge
Less than or equal to	<=	le

    b. "contains" operator
        i. used to filter packets that contain an exact match of a string of text
        ii. example:
            http contains "moved"
    c. "matches" operator
        i. used to filter packets based on the regular expression (regex) that's specified
    d. filter for protocols
        i. just input the protocol in the toolbar like "dns" or "http" (without the quotations)
    e. filtering for source or destination ip examples:
        ip.addr == 172.21.224.2

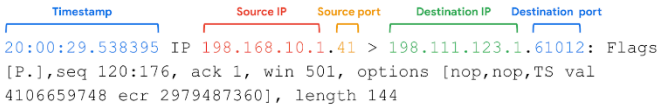
ip.src == 10.10.10.10
ip.dst == 4.4.4.4

f. filter for MAC address example:
eth.addr == 00:70:f4:23:18:c4

g. filter for ports examples:
udp.port == 53
tcp.port == 25

h. following a stream
   i. lets you filter for packets specific to a protocol
   ii. stream = conversation/exchange of data between devices using a protocol

16. TCPdump
    a. command-line network protocol analyzer
    b. traffic data is stored to a packet capture (p-cap) file
    c. breakdown of tcpdump syntax: sudo tcpdump [-i interface] [option(s)] [expression(s)]
    sudo tcpdump: begins the command running permissions as sudo
    -i: parameter specifies the network interface, "-i any" means sniffing traffic on all network interfaces
    [option] [expression]: ways to further filter traffic in order to isolate a certain type of packet
    d. "[option]" expanded, **case sensitive**
       i. -w: write or save the sniffed network packets to a packet capture file instead of printing it
       sudo tcpdump -i any -w packetcapture.pcap
       ii. -r: read a packet capture file by specifying the file name as a parameter
       sudo tcpdump -r packetcapture.pcap
       iii. -v: verbosity (level of detail) of the data capture
       sudo tcpdump -r packetcapture.pcap -v
       iv. -c: controls how many packets tcpdump will capture ("-c 1" will print out one packet)
       sudo tcpdump -i any -c 3
       v. -n: disables automatic mapping of numbers to names, best practice for sniffing
       sudo tcpdump -r packetcapture.pcap -v -n
       vi. -nm: doesn't resolve both hostnames or ports
    e. expression
       i. ability to use boolean operators like "and", "or", or "not"
       ii. example: reads the file "packetcapture.pcap" and combine "ip and port 80" using "and"
       sudo tcpdump -r packetcapture.pcap -n 'ip and port 80'
    f. interpreting output of tcpdump



       i. timestamp: displayed in hours, minutes, seconds, and fractions of a second
       ii. source ip: ip of packet's origin
       iii. source port: port of packet's origin
       iv. destination ip: self-explanatory
       v. destination port: self-explanatory

17. Comparison of Wireshark vs tcpdump
    a. Wireshark only
       i. uses a GUI
       ii. offers more features such as advanced filtering and colorizing

iii. requires more system resources

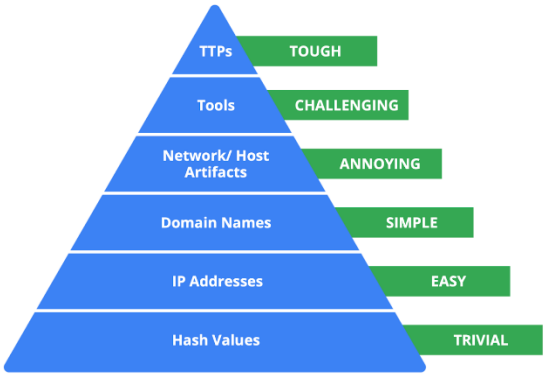
b. tcpdump only
   i. uses a command-line interface
   ii. is lightweight and uses fewer system resources

c. both
   i. network protocol analyzers
   ii. open-source and available for free
   iii. filter for a specified protocol

Week 3 – Incident Detection/Verification, Response & Recovery, Post-Incident Actions

1. Challenges in the detection and analysis phase
   a. impossible to detect everything
   b. high volumes of alerts
2. Methods of detection
   a. threat hunting
      i. combines technology with a human element to discover hidden threats left undetected by usual detection tools
      ii. proactive search for threats on a network
      iii. uncovering malicious activity that was not identified by detection tools
   b. threat intelligence
      i. evidence-based threat information that provides context about existing or emerging threats
      ii. found in private or public sources:
         1. Industry Reports- details about attacker's tactics, techniques, and procedures (TTP)
         2. Government Advisories- similar to industry reports, includes details about attacker's TTP
         3. Threat Data Feeds- provides a stream of threat-related data that can be used to help protect against sophisticated attackers (APTs)
         4. Cyber Deception- techniques that deliberately deceive malicious actors with the goal of increasing detection and improving defensive strategies
            a. honeypots- decoy that's vulnerable to attacks with the purpose of attracting potential intruders I.E., fake file labeled "Client Credit Card Information"
3. Indicators of Compromise (IoC)
   a. observable evidence that suggests signs of a potential security incident
   b. they chart specific pieces of evidence that are associated with an attack
   c. identifies the who and what of an attacked after it's taken place
4. Indicators of Attack (IoA)
   a. series of observed events that indicate a real-time incident
   b. they focus on identifying the behavioral evidence of an attacker, including their methods and intentions
   c. finding the why and how of an ongoing or unknown attack

5. Pyramid of Pain

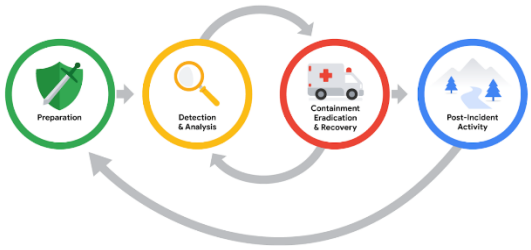


   a. captures the relationship between indicators of compromise and the level of difficulty that malicious actors experience when indicators of compromise are blocked by security teams
6. Pyramid of Pain levels explained
   a. Hash values
      i. corresponds to known malicious files
      ii. often used to provide unique references to specific samples of malware
   b. IP addresses
      i. self-explanatory
   c. Domain names
      i. web address such as www.google.com
   d. Host Artifacts
      i. observable evidence created by malicious actors on a host
      ii. example: the name of a file created by malware
   e. Tools
      i. software that's used by a malicious actor to achieve their goal
      ii. example: attackers can use password cracking tools like John the Ripper
   f. TTPs
      i. behavior of a malicious actor
      ii. refers to the high-level overview of the behavior
      iii. provides detailed descriptions of the behavior relating to the tactic
7. Crowdsourcing
   a. practice of gathering information using public input and collaboration
   b. used by threat intelligence platforms
8. Open-Source Intelligence (OSINT)
   a. collection and analysis of information from publicly available sources
   b. Tools for crowdsourced investigation of IoCs
      i. Jotti Malware Scan
      ii. Urlscan.io
      iii. CAPE Sandbox
      iv. MalwareBazaar
9. Benefits of Documentation
   a. transparency
   b. standardization
   c. clarity
10. Chain of Custody
   a. the process of documenting evidence possession and control during an incident lifecycle

    b. establishes:
        i. integrity
        ii. reliability
        iii. accuracy
11. Best practices of documentation
    a. Know your audience
        i. consider their needs
        ii. consider technical literacy (SOC Manager vs CEO)
    b. Be concise
        i. establish purpose immediately
    c. Update regularly
        i. in order to keep up with the evolving threat landscape
12. Playbook (review)- a manual that provides details about any operational action
    a. three types:
        i. non-automated
        ii. automated
        iii. semi-automated
13. Triage
    a. the prioritizing of incidents according to their level of importance or urgency
    b. process:
        i. Receive and Assess
            1. usually from an IDS
            2. ask questions like
                a. Is the alert a false positive?
                b. Was this alert triggered in the past?
                c. Is the alert triggered by a known vulnerability?
                d. What is the severity of the alert?
        ii. Assign Priority
            1. consider the following realms:
                a. functional impact- data being encrypted (ransomware), network uptime
                b. Information impact- possibility of stolen sensitive data, effects beyond org
                c. recoverability- consider whether it is possible, not-recoverable = less priority
        iii. Collect and Analyze
            1. gather enough information to make an informed decision to address the problem
            2. determining whether this needs escalation
        iv. Benefits of triage
            1. resource management
            2. standardized approach
    c. other questions to ask:
        i. Is there anything out of the ordinary?
        ii. Are there multiple failed login attempts?
        iii. Did the login happen outside of normal working hours?
        iv. Did the login happen outside of the network?
14. Containment (review)- the act of limiting and preventing additional damage caused by an incident
15. Eradication (review)- the complete removal of the incident elements from all affected systems
16. Recovery (review)- the process of returning affected systems back to normal operations
17. Business Continuity Planning

a. a document that outlines the procedures to sustain business operations during and after a significant disruption and helps organizations ensure that critical business functions can resume

18. Site Resilience
    a. the ability to prepare for, respond to, and recover form disruptions
    b. three types of recovery sites:
        i. hot sites- fully operational facility that is a duplicate of an organization's primary environment
        ii. warm site- contains a fully updated and configured version of the hot site, not fully operational
        iii. cold site- equipped with some of the necessary infrastructure required to operate
19. Post-Incident Activity Phase
    a. the process of reviewing an incident to identify areas for improvement during incident handling
    b. involves final report
        i. documentation that provides a comprehensive review of an incident
20. Post-Incident Review



    a. Lessons Learned Meeting (a.k.a "post-mortem")
        i. ask questions like:
        What happened?
        What time did it happen?
        Who discovered it?
        How did it get contained?
        What were the actions taken for recovery?
        What could have been done differently?
    b. Recommendations
        i. security teams can identify errors in response actions, gaps in processes and procedures, and/or ineffective security controls
    c. Final Report
        i. Executive Summary
        ii. Timeline
        iii. Investigation
        iv. Recommendations

Week 4 – Overview of Logs, IDSs, and SIEMs

1. The primary purpose of logs during incident investigation
    a. to provide a record of event details
2. Log details:
    a. date
    b. time
    c. location
    d. action
    e. names
3. Log types:
    a. network

   b. system
   c. application
   d. security (IDS/IPS)
   e. authentication
4. Industries requiring special log retention
   a. public sector industries
   b. healthcare industries
   c. financial services industries
5. Specific log details:
   a. timestamps
   b. system characteristics
   c. action
6. Commonly used log formats
   a. Syslog
   b. JavaScript Object Notation (JSON)
   c. eXtensible Markup Language (XML)
   d. Comma Separated Values (CSV)
   e. CEF
7. JSON
   a. file format used to store and transmit data
   b. known for being lightweight and easy to read and write
   c. used for transmitting data in web technologies and in cloud environments
   d. included JavaScript components like
      i. key-value pair- set of data representing two linked items
         example: “Alert” : ”Malware”
      ii. commas- used to separate data
      iii. double quotes- used to enclose text data (numbers are not enclosed in double quotes)
      iv. curly brackets- enclose an object, an object contains multiple properties
      v. square brackets- used to enclose an array I.E., a list of objects
8. Syslog
   a. Three main capabilities:
      i. Log format
      ii. Protocol
      iii. Service
   b. example log entry:
      <236>1 2022-03-21T01:11:11.003Z virtual.machine.com evntslog - ID01 [user@32473 iut="1" eventSource="Application" eventID="9999"]
      This is a log entry!

      Timestamp- YYYY-MM-DD format, “T” is used to separate the date and time, “z” = timezone
      Hostname- virtual.machine.com
      Application- eventlog
      Message ID- ID01
      Structured-data- contains additional logging information enclosed in square brackets
      Message- detailed log message about the event
      Priority (PRI)- indicated urgency of the logged event contained in angle brackets
9. XML

a. native file format used in Windows systems
b. used for storing and transmitting data
c. uses Tags, Elements, Attributes
d. Tags
    i. stores and identifies data
    ii. are pairs that must contain a start tag and end tag
    iii. start tag is <tag> while close tag is </tag>
e. Elements
    i. include both the data contained inside of a tag and the tags itself
    ii. must contain at least one root element
    example:
    <Event>
      <EventID>4688</EventID>
      <Version>5</Version>
    </Event>
    (<event> is the root element containing two child elements)
f. Attributes
    i. used to provide additional information about elements
    ii. included as second part of the tag itself used with single or double quotes

10. CSV
    a. position of data corresponds to its field name, all comma separated
11. CEF (Common Event Format)
    a. uses key-value pairs to structure data and identify fields and their corresponding values
    b. CEF syntax is as follows:
    Sep 29 08:26:10 host CEF:1|Security|threatmanager|1.0|100|worm successfully stopped|10|src=10.0.0.2 dst=2.1.2.2 spt=1232

    Syslog Timestamp: Sep 29 08:26:10
    Syslog Hostname: host
    Version: CEF:1
    Device Vendor: Security
    Device Product: threatmanager
    Device Version: 1.0
    Signature ID: 100
    Name: worm successfully stopped
    Severity: 10
    Extension: written in key value pairs
12. Host-based intrusion detection system (HIDS)
    a. an application that monitors the activity of the host on which it's installed
    b. usually installed on an endpoint
    c. monitors inbound and outbound traffic
    d. can monitor file systems, system resource usage, user activity
13. Network-based intrusion detection system (NIDS)
    a. an application that collects and monitors network traffic and network data
14. Signature Analysis
    a. a detection method used to find events of interest
    b. when monitoring activity, a signature specified the rules used by an IDS

15. Detection techniques
    a. Signature-based
        i. detection method that is used to find events of interest
        ii. signature- patter that is associated with malicious activity
        iii. advantages
            1. low rate of false positives, very efficient at detection known threats
        iv. disadvantages
            1. signatures can be evaded, attackers can make slight modifications to their code
            2. signatures require updates
            3. inability to detect unknown threats, relies on pre-existing attacks
    b. Anomaly-based
        i. two phases
            1. training- baseline of normal or expected behavior must be established
            2. detection- current system activity is compared against the baseline
        ii. disadvantages
            1. high rate of false positives
            2. pre-existing compromise, bad if existence of an attacker during training phase
16. Components of a NIDS Rule
    a. Action
        i. determines the action to take if the rule criteria is met
        ii. alert, pass, or reject
    b. Header
        i. source and destination IP addresses
        ii. source and destination ports
        iii. protocols
        iv. traffic direction
        v. example:
        tcp 10.120.170.17 any -> 133.113.202.181 80
        protocol, source ip, source port, traffic direction, destination ip, destination port
    c. Rule Options
        i. example: (msg: “This is a message’;sid: 123456;rev:1;)
        Message
        Signature ID
        Revision
17. Suricata format type
    a. EVE JSON – Extensible Event Format JavaScript Object Notation
    b. Log types
        i. Alert logs
        ii. Network telemetry logs
            1. network traffic flows, what’s happening on the network
18. Suricata Overview
    a. it is an open-source IDS, IPS, and Network Analysis Tool
    b. features
        i. IDS
        ii. IPS
        iii. Networking Security Monitoring (NSM)
            1. helps keep networks safe by producing and saving relevant network logs

2. can analyze live network traffic, existing packet capture files, create/save full or conditional packet captures

c. Rules
   i. Signature Analysis
      1. three components:
         a. Action- describes action taken if activity matches signature (alert, pass, drop, reject)
         b. Header- includes network traffic information
         c. Rule Options- different options to customize signatures

d. Configuration File
   i. used to configure the settings of an application
   ii. located in “suricata.yaml”
e. Log Files
   i. two log files Suricata generates when alerts are triggered
      1. eve.json- standard Suricata log file, contains information and metadata about events and alerts stored in JSON format
      2. fast.log- records minimal alert information including basic IP address and port details about network traffic, basic logging and alerting, not suitable for incident response

19. SIEM Tools in the modern-day industry
    a. Splunk
    b. Chronicle
20. SIEM Process Review – Three steps
    a. Collect and aggregate data
    b. Normalize data
    c. Analyze data
21. Log Ingestion
    a. the process of collecting and importing data from log sources into a SIEM tool
22. Log Forwarders
    a. software that automates the process of collecting and sending log data to a remote SIEM
23. Query for logs in Splunk
    a. Search Processing Language (SPL)- Splunk’s query language
    b. example: index=main fail
       index=main: command telling splunk to retrieve events from an index called main
       fail: tell splunk to return any event that contains the term fail
    c. Piping can be used in SPL
    d. “chart count by host” = creates a chart according to the count or number of events, “by host” tells splunk to list the events by host
       example: index=main fail | chart count by host
    e. Wildcard
       i. using “*” with the search term “index=main fail*” means we get all items that have the term “fail” in the log included “failure” and “failed”
24. Query for logs in Chronicle
    a. YARA-L- computer language used to create rules for searching through ingest log data
    b. types of searches:

i. UDM search- normalized data
ii. Raw log search

c. common fields in a UDM search
i. Entities
1. also known as nouns
2. all UDMs must contain at least one entity
3. must include something like hostname, username, and IP address of the event
ii. Event metadata
1. basic description of an event, type of event it is, timestamps
iii. Network metadata
1. information about network-related events and protocol details
iv. Security results
1. security-related outcome of events
2. “virus detected and quarantined”

d. example UDM search using event metadata field to locate events relating to user logins:
metadata.event_type = “USER_LOGIN”
---
metadata.event_type- contains information about the event type
USER_LOGIN- searches for events relating to authentication

e. Raw Log Search
i. searching through raw/unparsed logs
ii. takes longer than structured search
iii. supports regular expressions

Course 7 – Automate Cybersecurity Tasks with Python | Instructor Angel

Week 1 – Intro to Python, Core Python Components, Conditional and Iterative Statements

1. Python Overview
a. Advantages of Python
i. resembles human language
ii. less code
iii. easy to read
iv. standard guidelines
v. online support
vi. built-in code
b. uses an **interpreter**
i. a computer program that translates python code into runnable instructions line by line
c. its use in cybersecurity (automation)
i. log analysis
ii. malware analysis
iii. access control list management
iv. intrusion detection
v. compliance checks
vi. network scanning
2. comment
a. a not programmers make about the intention behind their code

b. example:
```
# Print Hello Python
print (“Hello Python!”)
```

3. print()
    a. outputs a specified object to the screen
4. Python Environments
    a. notebooks
        i. online interface for writing, storing, and running code
        ii. allows documentation about the code
        iii. appears in a code cell or markdown cell
        iv. common notebook environments
            1. Jupyter Notebook
            2. Google Colaboratory
        v. code cells
            1. meant for wwriting and running code
            2. a play button is located within the cell
        vi. markdown cells
            1. meant for describing the code
            2. allows formatting text in the markdown language
            3. used for formatting plain text in text editors and code editors
            4. example: indicating text should be in a certain header style
    b. Command Line
5. String Data
    a. data consisting of an ordered sequence of characters
    b. always counted as text
6. Numeric Data
    a. Float Data
        i. data consisting of a number with a decimal point
        ii. dividing two integer values or two float values results in float output when using “/”
        iii. using “//” to divide two floats will return a result rounded down to the nearest whole number
    b. Integer Data
        i. data consisting of a number that does not include a decimal point
    c. Boolean Data
        i. data that can only be on of two values: either true or false
        ii. example:
```
# determine boolean values
print(10<5)
print(9<12)
-yields-
False
True
```
    d. List Data
        i. data structure that consists of a collection of data in sequential form
        ii. example:
```
# print a list
print([“dtanaka”, “mabadi”, “aestrada”])
```

-yields-
['dtanaka', 'mabadi', 'aestrada']

7. Tuple
    a. just like a list, but contents of a tuple cannot be changed
    b. place in-between parenthesis rather than brackets
8. Dictionary
    a. data that consists of one or more key-value pairs
    b. each key is mapped to a value
    c. a ":" is placed between the key and value
    d. commas separate key-value pairs
    e. placed within curly brackets "{ }"
    f. example:
    { 1: "East",
      2: "West",
      3: "North",
      4: "South" }
9. Set
    a. data that consists of an unordered collection of unique values
    b. no two values in a set can be the same
    c. elements in a set are always placed within curly brackets and separated by a comma
    d. can be of any data type
    e. example:
    {"jlanksy", "drosas", "nmason"}
10. Variable
    a. a container that stores data
    b. example:
    device_id = "h32rb17"
    print(device_id)
    print("m50pi21")
    -yields-
    h32rb17
    m50pi21
11. type()
    a. returns the data type of its input
    b. example:
    device_id = "h32rb17"
    data_type = type(device_id)
    print(data_type)
    -yields-
    <class 'str'>
12. Type Error
    a. results from using the wrong data type
13. Assigning variable to variables
    a. example:
    username = "nzhao"
    old_username = username
    username = "zhao2"

```
print("Previous username:", old_username)
print("Current username:", username)
-yields-
Previous username: nzhao
Current username: zhao2
```

14. Conditional Statement
    a. a statement that evaluates code to determine if it meets a specified set of conditions
15. if
    a. starts a conditional statement
    b. example:

```
if failed_attempts > 5:
  print(“Account locked”)
```

16. Operators
    a. >
    b. <
    c. >= (greater than or equal) to
    d. <= (less than or equal to)
    e. == (whether two object match)
    f. != (not equal)
17. else statement
    a. precedes a code section that only evaluates when all conditions that precede it within the conditional statement evaluate to False
    b. example:

```
operating_system = “OS3”
if operating_system == “OS2”:
  print(“Updates needed”)
else:
  print(“No updates needed”)
-Yields-
No updates needed
```

18. elif statement
    a. when you have multiple alternative actions that depend on new conditions
        i. precedes a condition that is only evaluated when previous conditions evaluate to false
        ii. when it reaches an elif statement that evaluates to true, it won’t check the other elif statements
        iii. example:

```
if status == 200:
   print("OK")
elif status == 400:
   print("Bad Request")
elif status == 500:
   print("Internal Server Error")
else:
  print(“check other status”)
```

19. and operator
    a. requires both conditions on either side of the operator to evaluate to true

b. example:
```
if status >= 200 and status <= 226:
  print("successful response")
```

20. or operator
    a. requires only one of the conditions on either side of the operator to evaluate to true
    b. example:
```
if status == 100 or status == 102:
  print("informational response")
```
21. not operator
    a. example:
```
if not(status >= 200 and status <= 226):
  print("check status")
```
22. in operator
    a. used to check if a value is listed within a prescribed list
    b. example:
```
approved_list = ["johnny", "matt", "kelly"]
username = "matt"
if username in approved_list:
  print("User is authorized")
else:
  print(User is not authorized")
```
23. Iterative Statement
    a. code that repeatedly executes a set of instructions
24. for loop
    a. example:
```
for i in [1,2,3,4]:
  print(i)
```
explanation:
"for" signals the beginning of a for loop
"i" is the variable to iterate through, only used within the loop
25. range()
    a. generates a sequence of numbers
    b. example:
range(0,10) **<------- 10 is excluded**
-yields-
0,1,2,3,4,5,6,7,8,9
    c. range(10) generates the same as above, but it automatically starts at 0
example:
```
for i in range(10)
  print("Cannot connect to the destination.")
```
-yields-
Cannot connect to the destination.
Cannot connect to the destination.
Cannot connect to the destination.
Cannot connect to the destination.
Cannot connect to the destination.
Cannot connect to the destination.

Cannot connect to the destination.
Cannot connect to the destination.
Cannot connect to the destination.
Cannot connect to the destination.

d. range can also have a third value, being an increment number
example:
```
for i in range(0, 5, 1):
  print(i)
```
-yields-
0
1
2
3
4

26. while loop
    a. an iterative loop that continues only based on a condition
    example:
    ```
    time = 0
    while time <= 10:
      print(time)
      time = time + 2
    ```
27. break statement
    a. breaks from the loop if the condition is met
    b. example:
    ```
    computer_assets = [“laptop1”, “desktop20”, “smartphone03”]
    for asset in computer_assets:
      if asset == “desktop20”:
        break
      print(asset)
    ```
28. continue statement
    a. use it to skip back to the top of the loop if a certain condition is met
    b. example:
    ```
    computer_assets = [“laptop1”, “desktop20”, “smartphone03”]
    for asset in computer_assets:
      if asset == “desktop20”:
        continue
      print(asset)
    ```
    -yields-
    laptop1
    smartphone03

Week 2 – Intro to Functions, Working with Functions, Learning from the Python Community

1. Function
    a. a section of code that can be reused in a program
2. Built-in Functions
    a. functions that exist within Python and can be called directly
3. User-defined Functions
    a. functions that programmers design for their specific needs

4. def
    a. place before a function name to define a function
    b. example:
    ```
    # define a function
    def greet_employee():
      print("Welcome! You're logged in.")

    # call a function
    greet_employee()
    -yields-
    Welcome! You're logged in.
    ```
5. parameter (python)
    a. an object that is included in a function definition for use in that function
    b. accepted into the parenthesis when defining a function
    c. example:
    ```
    # greet employees by name
    def greet_employee(name):
      print("Welcome! You're logged in", name)

    greet_employee("Charley Patel")
    -yields-
    Welcome! You're logged in Charley Patel
    ```
    d. example for multiple parameters:
    ```
    def greet_employee(first_name, last_name):
      print("Welcome! You're logged in", first_name, last_name)

    greet_employee("Kiara", "Carter")
    -yields-
    Welcome! You're logged in Kiara Carter
    ```
6. argument
    a. the data brought into a function when it is called
7. return statement
    a. a python statement that executes inside a function and sends information back to the function call
    b. return is used to return information from a function
    c. example:
    ```
    # Return information from a function
    def calculate_fails(total_attemps, failed_attempts):
      fail_percentage = failed_attempts / total_attempts
      return fail_percentage

    calculate_fails(4,2)

    if (percentage >= .5):
      print("Account locked.")
    -yields-
    Account locked.
    ```
8. global variable

    a. variable that is available through the entire program
    b. assigned outside of a function definition
9. local variable
    a. variable assigned within a function
    b. cannot be called or accessed outside of the body of a function
10. max()
    a. returns the largest numeric input passed into it
    b. example:
    a = 3
    b = 9
    c = 6
    print(max(a,b,c))
    -yields-
    9
11. min()
    a. returns the smallest numeric input passed into it
12. sorted()
    a. sorts the components of a list
13. Library
    a. a collection of modules that provide code users can access in their programs
14. Module
    a. a python file that contains additional functions, variables, classes, and any kind of runnable code
15. Python Standard Library
    a. an extensive collection of usable python code that often comes packaged with python
    b. example modules
        i. re- searching for patters in log files
        ii. csv- working with .csv files
        iii. glob- interacting with the command line
        iv. os- interacting with the command line
        v. time- working with timestamps
        vi. datetime- working with timestamps
        vii. statistics- functions used when calculating statistics related to numeric data
            1. median() is a function in the statistics module
16. importing an entire module
    a. “import statistics” to import the statistics module
17. importing specific functions from a module
    a. example:
    from statistics import mean, median
18. External Libraries
    a. libraries external to python such as Beautiful Soup (bs4) (for parsing HTML files) and NumPy (numpy) for arrays and mathematical computations
    b. to install an external library such as numpy
        i. %pip install numpy
    c. after a library is installed, you can import it directly into python via import via “import numpy”
19. Style Guide
    a. a manual that informs the writing, formatting, and design of documents
20. PEP 8 Style Guide

a. a resource that provides stylistic guidelines for programmers working in python
b. “Python Enhancement Proposals”

Week 3 – Working with Strings, Lists and Algorithms, REGEX

1. str()
    a. converts the input object into a string
    b. example
    new_string = str(123)
    print new_string
    -yields-
    “123”
2. len()
    a. returns the number of elements in an object
    b. example:
    print(len(“Hello”))
    -yields-
    5
3. String Concatenation
    a. the process of joining two strings together
    b. example:
    print(“Hello” + “world”)
    -yields-
    Helloworld
4. Method
    a. a function that belongs to a specific data type
    b. .upper()
        i. returns a copy of the string in all uppercase letters
        ii. example
        print(“Hello”.upper())
        -yields-
        HELLO
    c. .lower()
        i. returns a copy of the string in all lowercase letters
5. Index
    a. a number assigned to every element in a sequence that indicates its position
    b. uses bracket notation for extracting a part of the string
    c. `0 1 2 3 4`
    `h e l l o`
    d. example:
    “HELLO”[1]
    -yields-
    ‘E’
6. Slicing
    a. “HELLO”[1:4] (1 is the first character included, including up to just before the 4th character)
    -yields-
    ELL
7. .index() method
    a. finds the first occurrence of the input in a string and returns its location

   b. example:
      print("HELLO".index("E"))
      -yields-
      1
8. Finding substring with .index()
   a. substring = continuous sequence of characters within a string ("llo" being a substring of "hello"
   b. can be used to find the index of a first occurrence of a substring
      i. example:
         tshah_index = "tsnow, tshah, bmoreno – updated".index("tshah")
         print(tshah_index)
         -yields-
         7
9. Immutable
   a. cannot be changed after it is created and assigned a value
10. List Concatenation
   a. combining two lists into one by placing the elements of the second list directly after the elements of the first list
   b. example:
      my_list = ["a', "b", "c", "d", "e"]
      number_list = [1, 2, 3, 4]
      print(my_list + number_list)
      -yields-
      ['a', 'b', 'c', 'd', 'e', 1, 2, 3, 4]
11. Changing an element in a list
   a. example:
      my_list = ["a", "b", "c", "d", "e"]
      my_list[1] = 7
      print(my_list)
      -yields-
      ['a', 7, 'c', 'd', 'e']
12. .insert()
   a. adds an element in a specific position inside a list
   b. example:
      my_list = ["a', "b", "c", "d", "e"]
      my_list.insert(1,7) (1 is the position where we want to insert the new information)
      print(my_list)
      -yields-
      my_list = ["a", 7, "b", "c", "d", "e"]
13. .remove()
   a. removes the first occurrence of a specific element in a list
   b. example:
      my_list.remove("d")
14. Algorithm
   a. set of rules that solve a problem
15. Example with building an algorithm to extract the first three numbers of a list of ip addresses
   a. IP = ["198.567.xx.xx", "198.501.xx.xx", "180.664.xx.xx", "192.668.xx.xx", "184.690.xx.xx"]
   b. Solution-based steps

i. use string slicing to extract the first 3 digits from one IP address
ii. use a loop to apply that solution to every IP address on the list

c. Writing the first chunk of code to extract the first 3 digits of a single IP address:
```
address = “198.567.xx.xx”
# extract the first three characters of an IP address
print(address[0,3])
-yields-
198
```
d. Building from the previous solution to go even further:
```
networks = []
for address in IP:
  networks.append(address[0:3])
print(networks)
-yields-
[‘198’, ‘198’, ‘192’, ‘184’]   <-----the product we were looking for
```

16. .append()
    a. adds input to the end of a list
17. Regular Expression (regex)
    a. a sequence of characters that forms a pattern
18. Regular Expression Symbols
    a. +
        i. represents one or more occurrences of a specific variables
        example:
        “a+” **matches**
        -“a”
        -“aaa”
        -“aaaaa”
        ii. example:
        “Device IDs:
        a37rz87
        io2aap4
        32rb5a2
        9aaa95y”
        -yields-
        [“a”, “aa”, “a”, “aaa”]
    b. .
        i. matches to all characters, including symbols
    c. \d
        i. matches to all single digits [0-9]
        ii. example:
        re.findall(“\d”, “h32rb17)
        -yields-
        [‘3’, ‘2’, ‘1’, ‘7’]
        iii. using +:
        re.findall(“\d+”, “h32rb17)
        -yields-
        [‘32’, ‘17’]

iv. using *:
re.findall("\d*", "h32rb17)
-yields-
['', '32', '', '', '17', '']

v. using { } to indicate a specific number of repetitions:
re.findall("\d{2}", "h32rb17 k825t0m c2994eh")
-yields-
['32', '17', '82', '29', '94']

vi. specifying a range with { }:
#first number in brackets represents min reps needed, second represents max number of reps
re.findall("\d{1,3}", "h32rb17 k825t0m c2994eh")
-yields-
['32', '17', '825', '0', '299', '4']

d. \s
   i. matches to all single spaces

e. \x
   i. matches to the period of a character

f. \w
   i. matches with any alphanumeric character but it doesn't match symbols
   ii. example:
   "\w" **matches**
   "1"
   "k"
   "i"

g. combining + and \w
   i. example:
   "\w+" **matches**
   "192"
   "abc123"
   "security"

h. practice expression
   i. Which string matches with the regular expression "b\wa+b"?
      1. answer = "bkaaab" because...
      first character must be "b"
      the symbol "\w" is used to match any alphanumeric character including k
      "+" specifies that there should be one or more occurrences of the character it follows
      (in this case it's "a")
      finally, the string must end with a "b"

i. practice expression
   i. user1@email.com
   \w+ @ \w+ \. \w+
   ii. # Extract email addresses
   import re
   email_log = """Email received June 2 from user1@email.com.
   Email received June 2 from user2@email.com.
   Email rejected June 2 from invalid_email@email.com."""
   print(re.findall("\w+@\w+\.\w+",email_log))

j. re.findall(parameter, parameter)
   i. returns a list of matches to a regular expression
   ii. first parameter string containing the regex pattern
   iii. second parameter is the string you're searching through

19. Construct a pattern with Regex
   a. take the following string:
   employee_logins_string = "1001 bmoreno: 12 Marketing 1002 tshah: 7 Human Resources 1003 sgilmore: 5 Finance"
   b. break down what you're searching for into smaller components
   c. identify where \w+, :, \s, and \d+ can be applied respectively
   d. therefore:
   import re
   pattern = "\w+:\s\d+"
   employee_logins_string = "1001 bmoreno: 12 Marketing 1002 tshah: 7 Human Resources 1003 sgilmore: 5 Finance"
   print(re.findall(pattern, employee_logins_string))
   -yields-
   ['bmoreno: 12', 'tshah: 7', 'sgilmore: 5']

Week 4 – Python for Automation, Working with Files in Python, Debugging Python Code

1. with
   a. parameter
   b. handles errors and manages external resources
   c. will manage resources by closing the file after exiting the "with" statement
2. open(,)
   a. first argument is the file you want to open
   b. second argument indicated what you want to do with the file
      i. r = read
      ii. w = write
      iii. a = append
   c. opens a file in python
3. .read()
   a. converts files into strings
4. as
   a. assigns a variable that references another object
5. combine the 3 previous in order to open a text file via python
   a. example:
   with open("login_attempts.txt", "r") as file:
    file_text = file.read()
   print(file_text)
   -yields-
   elarson
   eraab
   eraab
   bmoreno
   tshah
   etc.
6. writing files in python

a. uses either “w” or “a” as the second argument of open()
   example:
   with open(“update_log.txt”, “w”) as file:
   -yields-
   it will open the file so it’s contents can be replaced
b. “w” can also be used to create a file that doesn’t exist yet
c. appending to new files with “a”
   i. example:
      with open(“update_log.txt”, “a”) as file:
      -yields-
      it will open update_log.txt so that new information can be appended to the end
   ii. full example of using append:
      line = “jrafael, 192.168.243.140,4:56:27,True”
      with open(“access_log.txt, “a”) as file:
       file.write(line)

7. Parsing
   a. the process of converting data into a more readable format
8. .split()
   a. converts a string into a list
   b. separates the string based on a specified character that’s passed as an argument
      i. if you do not pass an argument into .split(), it will separate via every white space
   c. separates the string based on a specific character
   d. example:
      with open(“login_attempts.txt”, “r”) as file:
       file_text = file.read()
      print(file_text.split())
9. using .split() to files
   a. used with the .read() method
   b. example: opening “update_log.txt”, reading the contents into “updates” variable, and splits the string in the “updates” variable into a list by creating a new element at each whitespace-
      with open(“update_log.txt”, “r”) as file:
       updates = file.read()
      updates = updates.split()
10. .join()
   a. concatenates the elements of an iterable into a string
   b. unique syntax compared to .split() and .index()
   c. you must pass the list that you want to concatenate into a string in as an argument
      example use:
      approved_users = ["elarson", "bmoreno", "tshah", "sgilmore", "eraab"]
      print("before .join():", approved_users)
      approved_users = ",".join(approved_users)
      print("after .join():", approved_users)
      -yields-
      before .join(): ['elarson', 'bmoreno', 'tshah', 'sgilmore', 'eraab']
      after .join(): elarson,bmoreno,tshah,sgilmore,eraab
11. using .join() on files

a. example:

```
with open("update_log.txt", "r") as file:
  updates = file.read()
updates = updates.split()
```

12. parsing algorithm in python
    a.
```
# open, read, and split a text file
with open("login_attempts.txt", "r") as file:
  file_text = file.read()
usernames = file_text.split()
print(usernames)

# create a function that counts a user's failed login attempts
def login_check(login_list, current_user):
  counter = 0
  for i in login_list:
    if i == current_user:
      count = counter + 1
    if counter > = 3:
      return "You have tried to login three or more times. Your account has been locked."
    else:
      return "You can log in!"

login_check(usernames, "elarson")
```

13. Types of errors
    a. syntax errors
        i. I.E., forgetting to add a colon after defining a function
    b. logic errors
        i. when logic used in code produces unintended results
        ii. may not produce error messages
        iii. code will not do what you expect it to do, but is still valid to the interpreter
    c. exceptions
        i. error that involves code that cannot be executed even though it is syntactically correct
        ii. example: including a variable that hasn't been assigned or a function that hasn't been defined
        iii. "IndexError"
            1. when you place an index in bracket notation that does not exist in the sequence being referenced
        iv. "TypeError"
            1. using the wrong data type
            2. performing a mathematical calculation by adding a string to an integer
        v. "FileNotFound"
            1. trying to open a file that does not exist in the specified location
14. Debugging Strategies
    a. Debuggers
        i. running in an "Integrated Development Environment" (IDE)
            1. application for writing code that provides editing assistance and error correction tools
        ii. software tool that helps to locate the source of an error and assess its causes
    b. Using print statements throughout your code

Course 8 – Put it to Work: Prepare for Cybersecurity Jobs | Instructor Dion

Week 1 – Event and Incident Detection, Your Impact on Data Protection

1. Security Mindset
    a. the ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data
2. Classifying Different Types of Data
    a. Public
        i. does not need extra security protections
        ii. already accessible to the public
        iii. poses a minimal risk to the organization if view or shared by others
    b. Private
        i. higher security level
        ii. information that should be kept from the public
        iii. could pose a serious risk to an organization
        iv. I.E., email addresses, employee identification numbers, organization's research data
    c. Sensitive
        i. must be protected from everyone who does not have authorized access
        ii. includes PII, SPII, and PHI
        iii. I.E., banking account numbers, usernames and password, SSNs, passport number
    d. Confidential
        i. important for an organization's ongoing business operations
        ii. often has limits on the number of people who have access to it
        iii. involves signing of a non-disclosure agreement
        iv. I.E., trad secrets, financial records, sensitive government data
3. Asset Classification
    a. labeling assets based on the sensitivity and importance to an organization
    b. ranges from low- to high-level
    c. Public = low-level asset
    d. Sensitive = high-level asset
4. Examples of Customer Data
    a. credit card numbers
    b. social security numbers
    c. emails
    d. usernames
    e. passwords
5. Business Continuity Plan
    a. a document that outlines the procedures to sustain business operations during and after a significant disruption
    b. created alongside a disaster recovery plan to minimize the damage of successful security attacks
    c. four essential steps
        i. Conduct a business impact analysis
            1. focus on possible effects a disruption of business functions can have on an organization
        ii. Identify, document, and implement steps to recover critical business functions and processes
            1. creating actionable steps toward responding to a security event
        iii. Organize a business continuity team
            1. bringing various members of the organization to help execute the continuity plan
            2. members of team are usually cybersecurity, IT, HR, communications, and operations

iv. Conduct training for the business continuity team
    1. the team considers different risk scenarios and prepares for security threats

6. Disaster recovery plan
    a. allows an organization's security team to outline the steps needed to minimize the impact of a security incident
    b. steps to the plan include:
        i. implementing recovery strategies to restore software
        ii. implementing recovery strategies to restore hardware functionality
        iii. Identifying applications and data that might be impacted after a security incident has taken place
7. Examples of the potential impact of a security incident involving **malicious code**
    a. Financial consequences
    b. Loss of assets
    c. Operational downtime

Week 2 – Escalation in Cybersecurity, To Escalate or Not to Escalate, Timing is Everything

1. Incident Escalation
    a. the process of identifying a potential security incident, triaging it, and handing it off to a more experience team member
2. Essential skills to escalate security incidents
    a. Attention to detail
        i. can make the difference between escalating an incident to the right or wrong person
        ii. can help prioritize which incidents need to be escalated with more or less urgency
    b. Ability to follow an organization's escalation guidelines or processes
3. Notification of breaches
    a. countries have breach notification laws
        i. requires companies and government entities to notify individuals of security breaches involve potential release of PII
4. Low-level security issues
    a. issues that do not result in the exposure of PII
    b. can include the following:
        i. an employee having one failed login attempt on their account
        ii. an employee downloading unapproved software onto their work laptop
5. Types of incidents:
    a. Malware Infection
        i. an incident type that occurs when malicious software designed to disrupt a system infiltrates an organization's computer or network
    b. Unauthorized Access
        i. an incident type that occurs when an individual gains digital or physical access to a system or application without permission
    c. Improper Usage
        i. an incident type that occurs when an employee of an organization violates the organization's acceptable use policies
        ii. **should always be escalated out of caution**
6. Recognize roles and responsibilities during escalation
    a. Data owners
        i. person that decides who can access, edit, use, or destroy their information
        ii. accountable for the classification, protection, access, and use of company data
    b. Data controllers

        i. determine the procedure and purpose for processing data
        ii. focuses on collecting the personal information of customers
        iii. determines how that data is used
        iv. ensures the data is used, stored, and processed in accordance with relevant security regulations
    c. Data processors
        i. report directly to the data controller
        ii. responsible for processing the data on behalf of the data controller
        iii. typically a vendor and is often tasked with installing security measures to help protect the data
    d. Data custodians
        i. assign and remove access to software or hardware
        ii. responsible for implementing security controls for the data they are responsible for, granting and revoking access to that data, creating policies regarding how that data is store and transmitted
        iii. notified when data security controls need to be strengthened
    e. Data protection officers (DPOs)
        i. responsible for monitoring the internal compliance of an org's data protection procedures
        ii. they advise the security team on the obligations required by the org's data protection standards and procedures
        iii. conducts assessments to determine whether or not the security measures in place are properly protecting the data as necessary
        iv. notified when set standards or protocols have been violated
7. Escalation Policy
    a. a set of actions that outline who should be notified when an incident alert occurs and how that incident should be handled
8. Escalation tips
    a. familiarize yourself with the escalation policy of an organization you work for
    b. follow the policy at all times
    c. ask questions

Week 3 – Understand Your Stakeholders, Communicate for Impact, Dashboard Communication

1. Stakeholders in cybersecurity
    a. Risk Managers
        i. identify risks
        ii. manage the response to security incidents
        iii. notify the legal department
        iv. inform the organization's public relations team
    b. Chief Executive Officer (CEO)
        i. financial and managerial decisions
        ii. report to shareholders
        iii. manage operations
    c. Chief Financial Officer (CFO)
        i. manage financial operations
        ii. costs of tools and strategies
    d. Chief Information Security Officer (CISO)
        i. develop an organization's security architecture
        ii. conduct risk analysis and system audits
        iii. create security and business continuity plans
    e. Operation Managers
        i. oversee security professionals

        ii. work directly with analysts
        iii. responsible for daily maintenance of security operations
2. When escalating possible security threats/risks/vulnerabilities, be mindful of
    a. what you communicate
    b. who you communicate to
3. Communications should
    a. be precise
    b. avoid unnecessary technical terms
    c. have a clear purpose
4. Security story details
    a. what the security challenge is
    b. how it impacts the organization
    c. possible solutions to the issue
5. Communicate the story
    a. email
    b. document
    c. visual representation
    d. incident management or ticketing systems
6. Communicate effectively with stakeholders
    a. get to the point
        i. what do I want this person to know?
        ii. why is it important for them to know it?
        iii. when do they need to take action?
        iv. how do I explain the situation in a nontechnical manner?
    b. follow the protocols
    c. communicate with impact
    d. communication methods
        i. instant messaging
        ii. emailing
        iii. video calling
        iv. phone calls
        v. sharing a spreadsheet of data
        vi. sharing a slideshow presentation
    e. **Information that is communicated to stakeholders is <u>sensitive.</u>**
7. Visual Dashboard
    a. a way of displaying various types of data quickly in one place
    b. used to communicate security events to stakeholders
    c. can contain a chart vs charts, graphs, and tables
    d. Google Sheets and Apache OpenOffice are examples of way to make visual dashboards
    e. when to usual a visual report is situational based on availability of data

Week 4 – Reliable Sources Go a Long Way, Build Your Cybersecurity Network

1. Security Websites and Blogs
    a. CSO Online
        i. news, tips, and ideas
    b. Krebs on Security
        i. in-depth security blog
    c. Dark Reading

        i. for security professionals, IoT, application security, mobile and cloud
2. Cybersecurity Community
    a. Security organizations and conferences
        i. attending conferences and joining organizations in order to learn from seasoned professionals
    b. Find the right organization
        i. reacting to security incidents vs preventing them from happening
        ii. forensic security vs data logging
        iii. aspirations of being a CISO one day
    c. Begin the search
        i. such as “incident response cybersecurity conferences in my area”
    d. Use social media
        i. search on LinkedIn
            1. “Incident response cybersecurity groups”
            2. “Organizations for cybersecurity analysts”
    e. Be aware of social engineering
    f. Mailing lists for security
        i. Cybersecurity & Infrastructure Security Agency (CISA) offers two mailing lists to join
            1. a list focused on security threat information, best practices for cybersecurity, and analysis from CISA’s domestic and international security partners
            2. a list providing weekly summaries of new vulnerabilities that might pose a risk to an organization’s network
3. engaging with the cybersecurity community in a meaningful way
    a. use social media to follow or read posts of leaders in a security industry
        i. I.E., CISOs of major companies
    b. connect with security professionals working in the industry you’re interested in
    c. social media filters
        i. people
        ii. #cybersecurity
        iii. connect via LinkedIn
        iv. events
        v. groups
    d. internet search engine, type: “cybersecurity industry associations’

Week 5 – Find/Prepare for a Job in Cybersecurity, Job Interviews, Answer Interview Questions

1. Initial Cybersecurity Roles
    a. Security Analyst
        i. monitoring networks
        ii. developing strategies
        iii. researching IT security trends
    b. Information Security Analyst
        i. Creating plans
        ii. Implementing security measures
    c. SOC Analyst
        i. Ensuring security incidents are handled rapidly
        ii. Following established policies and procedures
2. Job searching sites
    a. ZipRecruiter
    b. Indeed

    c. Monster Jobs
    d. LinkedIn
3. What to add to your resume
    a. programming languages
    b. Linux line-command
    c. security mindset
    d. frameworks and controls
    e. SIEM tools
    f. packet sniffers
    g. Transferable and technical Skills
        i. detail oriented
        ii. collaborative
        iii. written and verbal communication skills
    h. Summary Statement
        i. brief
        ii. strengths
        iii. skills
    i. Skills
    j. Work Experience
    k. Education
4. Resume tips
    a. no spelling or grammatical errors
    b. two pages long
    c. 10 years or less of work experience
5. Prepare for an interview
    a. revie the job description and your resume
    b. practice speaking about experiences and skills
    c. Dress professionally and feel comfortable
    d. take a few deep breaths
    e. remind yourself of all the preparation you've done
6. Background Interview
    a. questions about your education, work experience, skills, and abilities
    b. ask questions to help you decide if the team and company culture are a good match for you
7. Technical Interview
    a. answer confidently and concisely
    b. it's ok to say you don't know
8. Research the organization
    a. mission
    b. vision
    c. core values
    d. company culture
9. Why you?
    a. skills
    b. experience
    c. work ethic
    d. goals
10. Rapport

    a. a friendly relationship in which the people involved understand each other's ideas and communicate well with each other

11. Questions to ask the interviewer:
    a. What is the biggest challenge I could face going into this role
    b. How would I be expected to meet that challenge?
    c. What would you say is the best part of working for this company?
    d. What does a typical day look like for an analyst?
    e. What is the potential for growth in this role?
    f. *What is the biggest challenge for a new person in this role?
    g. *In what ways can I contribute to the success of the team and the organization?
    h. *What qualities or traits are most important for working well with the team and other stakeholders?
12. STAR Method
    a. a technique used to answer behavioral and situation interview questions
    b. Situation, Task, Action, Result
13. Elevator Pitch
    a. a brief summary of your experience, skills, and background
    b. must be:
        i. short
        ii. persuasive
        iii. who you are
        iv. why you care
        v. qualifications
        vi. skills
    c. avoid
        i. rambling
        ii. sounding ingenuine (robotic)
        iii. speaking too quickly
        iv. search for elevator pitch examples
14. Parts of an elevator pitch
    a. Provide an introduction
    b. Describe your career interests and transferable skills
    c. Express your excitement
    d. Communicate your interest in the company
15. Tips for interviewing remotely
    a. Test your technology
    b. Practice communicating through video
    c. Create a professional background
    d. Dress appropriately
    e. Look at the interviewer when speaking
    f. Sign in early