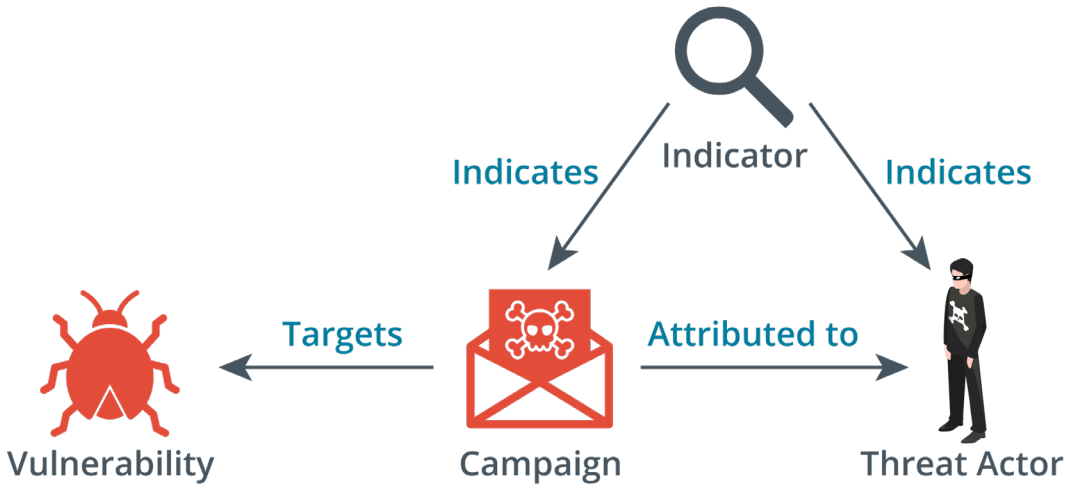
- **Closed/proprietary -** The threat research and cti data is made available as a paid subscription to a commercial threat intelligence platform.
- **Vendor websites -** This is proprietary threat intelligence that is not provided at a cost but is provided as a general benefit to customers e.g microsoft's security intelligence blog.
- **Public/private information sharing centers -** In many critical industries, **information sharing and analysis centers (isacs)** have been set up to share threat intelligence and promote best practice.
- **Open source intelligence (OSINT) -** Some companies operate threat intelligence services on an open-source basis earning income from consultancy
- **Other threat intelligence research resources include -** Academic journals, conferences, request for comments (RFC) and social media

8.8 Threat Data Feeds

There Are Various Ways That A Threat Data Feed Can Be Implemented.

Structured Threat Information Expression (Stix) - Describes Standard Terminology For Iocs And Ways Of Indicating Relationships Between Them.



Trusted automated exchange of indicator information (taxii) - Protocol provides a means for transmitting cti data between servers and clients.

Automated indicator sharing (ais) - Is a service offered by the dhs for companies to participate in threat intelligence sharing. ais is based on the stix and taxii standards and protocols.

Threat map - A threat map is an animated graphic showing the source, target and type of attacks detected by a cti platform.

File/code repositories - such a repository holds signatures of known malware code.

Vulnerability databases & feeds - Another source of threat intelligence is identifying vulnerabilities in os, software applications and firmware code. vulnerability databases include the common vulnerabilities and exposure (CVE).

Artificial Intelligence - Ai is the science of creating machine systems that can simulate or demonstrate a similar general intelligence capability to humans.

Predictive analysis - This refers to when a system can anticipate an attack and possibly identify the threat actor before the attack is fully realized.

8.9 Vulnerability Response & Remediation

Vulnerability scanning - This is an automated activity that relies on a database of known vulnerabilities such as the CVE.

Web app vulnerability scanners are specialized automated tools designed to identify vulnerabilities such as XSS and SQL injection attacks in websites and other web-based applications.

This category of tools is frequently referred to as the Dynamic Application Security Testing (DAST) tools.

True Positive	False Positive	True Negative	False Negative
Normal or xpected activity is correctly identified	Normal or xpected activity is incorrectly identified as abnormal	Abnormal or unexpected activity is correctly identified	Abnormal or unexpected activity is incorrectly identified as normal or expected
GOOD	PROBLEMATIC	GOOD	DANGEROUS

Vulnerability Scanning & Assessments

- **System Configuration -** Identify issues related to security configurations, compliance and nonconformance.
- **Vulnerability Assessment -** Identify host attributes and known Common Vulnerabilities and Exposures (CVE)
- **Penetration Testing -** Evaluate the security of a target by identifying and providing proof of concept of flaws and vulnerabilities by performing compromise exploitation.

Vulnerability Analysis - This focuses on analyzing the results gotten from vulnerability scans and assessments to determine the level of risk associated with each identified vulnerability.

Very useful for prioritizing vulnerabilities.

Vulnerability Severity Levels

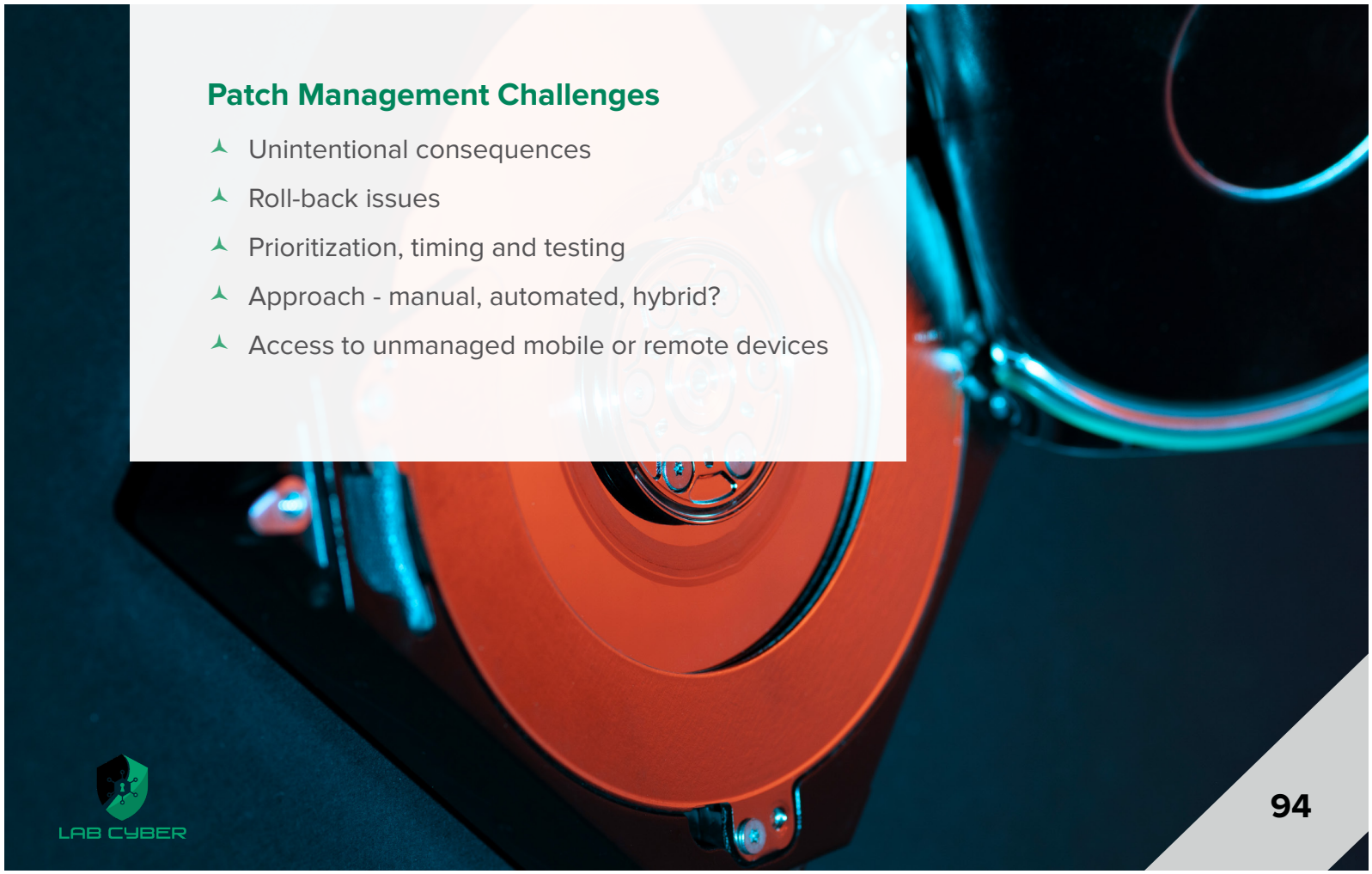
- **High -** This can also be critical levels and such vulnerabilities have the potential to cause significant damage and require immediate attention.
- **Medium -** Could result in adverse consequences eventually and should be prioritized based on their potential impact on the organization.
- **Low -** Have limited impact and should be remediated as part of ongoing vulnerability management efforts.

Patch Management - This is the process of identifying, acquiring, installing and verifying patches (updates)

The time from when an exploit first becomes active to the time it becomes insignificant is known as the **Window of Vulnerability.**

Patch Classifications

CRITICAL	DEFINITION	DRIVERS	FEATURE PACKS
Fixes for critical non- security related issues.	Updates to virus and definition files	For software components that control or regulate a	Provides new product functionality for the next product release
SECURITY	**SERVICE PACKS**	**UPDATE ROLLUPS**	**UPDATES**
Provides a fix for a product- specific, security-related vulnerability	Provides a cumulative set of security updates, hotfixes and design change or features	Provides a cumulative set of security updates, hot fixes and updates in one package	Provides fixes that address non-critical, non-security bugs



Patch Management Challenges

- Unintentional consequences
- Roll-back issues
- Prioritization, timing and testing
- Approach - manual, automated, hybrid?
- Access to unmanaged mobile or remote devices

SECTION 9

EVALUATE NETWORK SECURITY CAPABILITIES

9.1 Bench Marks & Secure Configuration Guides

Although frameworks provide a "high-level" view of how to plan its services, they generally don't provide detailed implementation guidance.

At a system level, the deployment of servers and applications is covered by benchmarks and secure configuration guides.

Center For Internet Security (CIS)

A non profit organization that publishes the well-known (the cis critical security controls).

They also produce benchmarks for different aspects of cybersecurity e.g benchmarks for compliance with it frameworks include pci dss and iso 27000.

There are also product-focused benchmarks such as windows desktop, windows server, macos and web & email servers.

Os/Network Appliance Platform/ Vendor-Speci ic Guides

Operating System (OS) best practice configuration lists the settings and controls that should be applied for a computing platform to work in defined roles such as workstation, server, network switch/router etc.

Most vendors will provide guides, templates and tools for configuring and validating the deployment of network appliances and operating systems and these configurations will vary not only by vendor but by device and version as well.

- Department of Defense Cyber Exchange Provides Security Technical Implementation Guides (STIGs) with Hardening Guidelines for a Variety of Software and Hardware Solutions.
- National Checklist Program (NCP) by NIST provides Checklists And Benchmarks for A Variety of Operating Systems and Applications.

Application Servers

Most Application Architectures use a Client/Server Model which Means Part of The Application is a Client Software Program Installed and run on Separate Hardware to the Server Application Code.

Attacks can Therefore be Directed at The Client, Server or The Network Channel Between Them.

Open Web Application Security Project (OWASP)

A Non Profit Online Community That Publishes Several Secure Application Development Resources Such As The Owasp Top 10 That Lists The Most Critical Application Security Risks.

9.2 Hardening Concepts

Network equipment, software, and operating systems use default settings from the developer or manufacturer which attempt to balance ease of use with security. Unfortunately these default configurations are an attractive target for attackers as they usually include well-documented credentials, allow simple passwords and use insecure protocols which increase the likelihood of successful cyberattacks. Therefore, it's crucial to change these default settings to improve security.

Hardening refers to the methods used to improve a device's security by changing its default configuration. There are various ways for hardening switches, routers, server hardware and operating systems.

Switches & Routers

- Change default credentials
- Disable unnecessary services and interfaces
- Use secure management protocols such as SSH and HTTPS instead of Telnet or HTTP
- Implement Access Control Lists
- Configure port security
- Enforce strong password policies

Server Hardware and Operating Systems

- Change default credentials
- Disable unnecessary services
- Apply security patches and updates
- Use firewalls and intrusion detection systems
- Secure configuration
- Enable logging and monitoring
- Use Antivirus and Antimalware solutions
- Enforce physical security

9.3- Wi-Fi Authentication Methods

Wi-Fi Authentication Comes In Three Types - Open, Personal And Enterprise.

Within The Personal Category, There Are Two Methods:

- Pre-Shared Key Authentication (PSK)
- Simultaneous Authentication Of Equals (SAE)

WPA2 pre-shared key authentication - In WPA2, pre-shared key (PSK) authentication uses a passphrase to generate the key for encryption.

The passphrase length is typically between 8 and 63 ASCII characters and is then converted to a 256-bit HMAC value.

Wpa3 personal authentication - WPA3 also uses a passphrase like WPA2 but it changes the method by which this secret is used to agree on session keys. this scheme is called password authenticated key exchange (PAKE)

Wi- i protected setup (WPS) - This is a feature of both WPA and WPA2 that allows enrollment in a wireless network based on an 8-digit pin.

It is vulnerable to brute force attacks and is set to be replaced by the easy connect method in WPA3 which uses quick response (qr) codes of each device.

Open authentication and captive portals - Open authentication means that the client is not required to authenticate however it can be combined with a secondary authentication mechanism via a browser.

When the client launches the browser, the client is redirected to a **captive portal** or splash page where they will be able to authenticate to the hotspot provider's network.

Enterprise/ieee 802.1x authentication - When a wireless station requests to join the network, its credentials are passed to an aaa server on the wired network for validation.

Once authenticated, the aaa server transmits a master key (mk) to the station and then both of them will derive the same pairwise master key (pmk) from the mk.

Extensible authentication protocol (eap) - This defines a framework for negotiating authentication mechanisms rather than the details of the mechanisms themselves.

Eap implementations can include smart cards, one-time passwords and biometric identifiers.

PEAP, EAP-TTLS and EAP-FAST- in protected extensible authentication protocol (PEAP), an encrypted tunnel is established between the supplicant and authentication server but only a server-side public key certificate is required.

EAP with flexible authentication via secure tunneling (EAP-FAST) - is also similar to PEAP but instead of a server side certificate, it uses a protected access credential (PAC) which is generated for each user from the authentication server's master key.

Radius federation - most implementations of EAP use a radius server to validate the authentication credentials for each user.

Radius federation means that multiple organizations allow access to one another's users by joining their radius servers into a radius hierarchy or mesh.

Rogue access points & evil twins - a rogue access point is one that has been installed on the network without authorization.

A rogue wap masquerading as a legitimate one is called an evil twin. an evil twin might have a similar ssid as the real one or the attacker might use some dos technique to overcome the legitimate wap.

A rogue hardware WAP can be identified through physical inspections. there are also various wi-fi analyzers that can detect rogue waps including inssider and kismet

Disassociation and replay attacks - a disassociation attack exploits the lack of encryption in management frame traffic to send spoofed frames.

One type of disassociation attack injects management frames that spoof the MAC address of a single victim causing it to be disconnected from the network.

Another variant broadcasts spoofed frames to disconnect all stations.

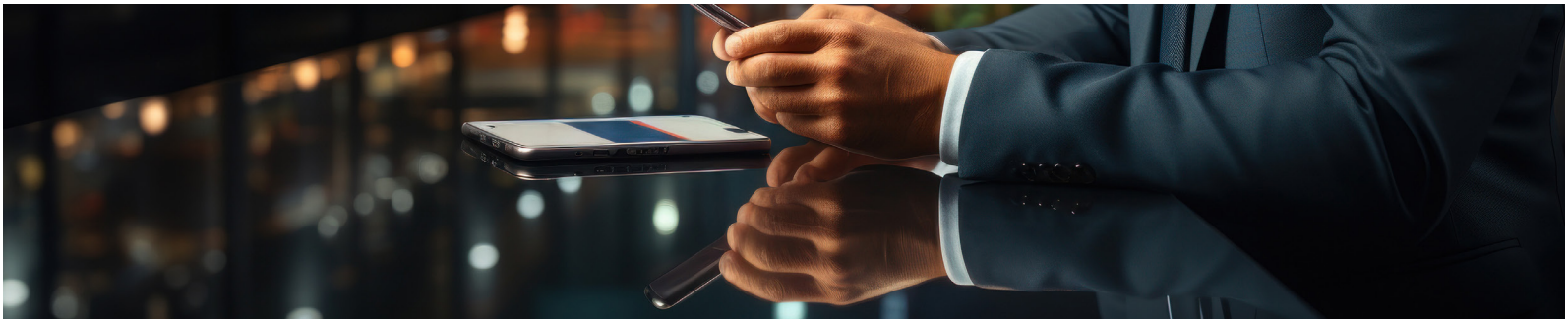
Jamming Attacks - A Wi-Fi Jamming Attack can be Performed by Setting up a WAP with a Stronger Signal.

The Only Way To Defeat This Attack Is To Either Locate The Offending Radio Source And Disable It Or To Boost The Signal From The Legitimate Equipment.

9.4 Network Access Control

Network Access Control (NAC) not only authenticates users and devices before allowing them access to the network but also checks and enforces compliance with established security policies. By evaluating the operating system version, patch level, antivirus status, or the presence of specific security software, NAC ensures that devices meet a minimum set of security standards before being granted network access.

NAC also can restrict access based on user profile, device type, location, and other attributes, to ensure users and devices can only access the resources necessary to complete their duties. NAC plays a crucial role in identifying and quarantining suspicious or noncompliant devices.



NAC and virtual local area networks (VLANs) work together to improve and automate network security. One of the primary ways NAC integrates with VLAN protections is through dynamic VLAN assignment. Dynamic VLAN assignment is a NAC feature that assigns a VLAN to a device based on the user's identity attributes, device type, device location, or health check results.

Agent vs Agentless Configurations

NAC can enforce security policies using agent-based and agentless methods.

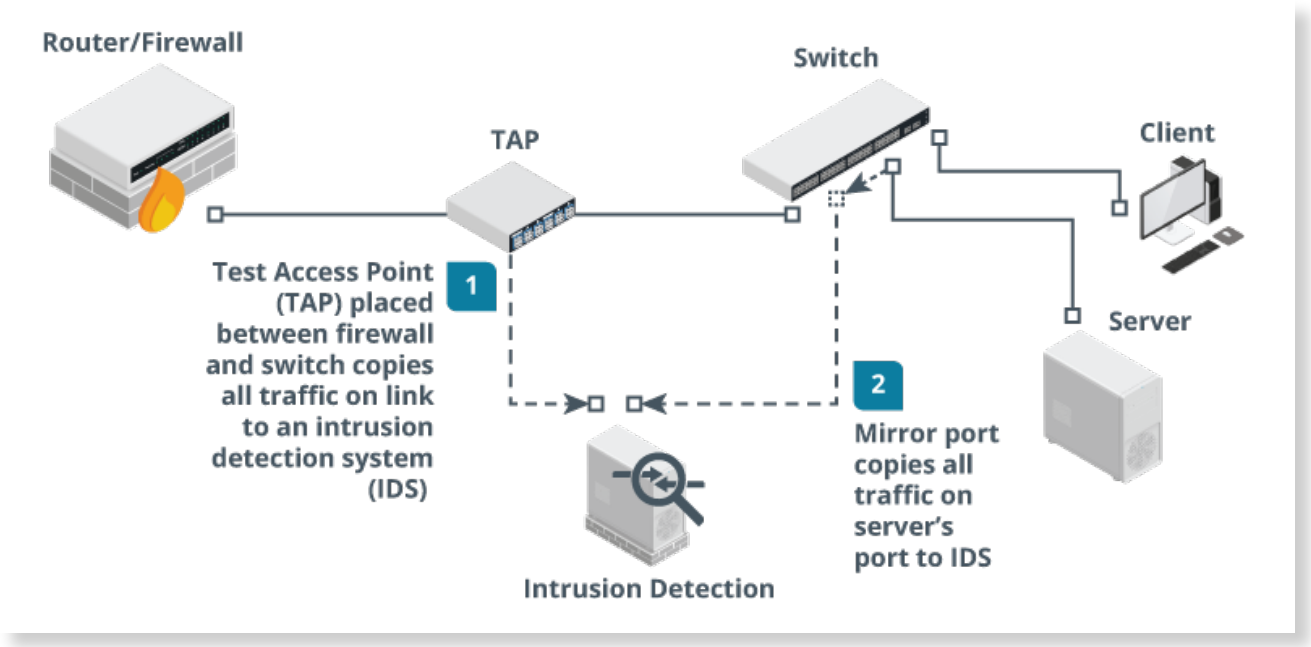
In an agent-based approach, a software agent is installed on the devices that connect to the network. This agent communicates with the NAC platform, providing detailed information about the device's status and compliance level. An agent-based NAC implementation can enable features such as automatic remediation, where the NAC agent can perform actions like updating software or disabling specific settings to bring a device into compliance with mandatory security configurations.

In contrast, an agentless NAC approach uses port-based network access control or network scans to evaluate devices. For example, agentless NAC may use DHCP fingerprinting to identify the type and configuration of a device when it connects, or it might perform a network scan to detect open ports or active services.

9.5 Network Security Monitoring

Network-based intrusion detection systems - An IDS is a means of using software tools to provide real-time analysis of either network traffic or system and application logs. a network-based ids captures traffic via a packet sniffer referred to as a sensor. when traffic matches a detection signature, it raises an alert but will not block the source host.

Taps & port mirrors - Typically the packet capture sensor is placed inside a firewall or close to an important server and the idea is to identify malicious traffic that has managed to get past the firewall. depending on network size and resources, one or just a few sensors will be deployed to monitor key assets and network paths.



Network-based intrusion prevention systems (IPS) - An ips provides an active response to any network threat.

Typical responses to a threat can include blocking the attacker's ip address (shunning), throttling the bandwidth to attacking hosts and applying complex firewall filters.

Next generation firewall (NGFW) - HGFW is a product that combines application-aware filtering with user account-based filtering and the ability to act as an ips.

Uni ied threat management (UTM) - This refers to a security product that centralizes many types of security controls - firewall, antimalware, spam filtering, VPN etc into a single appliance. The downside is that this creates a single point of failure that can affect the entire network. they can also struggle with latency issues if they are subject to too much network activity.

Content/url filter - A firewall typically has to sustain high loads of traffic which can increase latency and even cause network outages. a solution is to treat security solutions for server traffic differently from that of user traffic.

A Content Filter Is Designed To Apply A Number Of User-Focused Filtering Rules Such As Applying Time-Based Restrictions To Browsing.

Content filters are now implemented as a class of product called secure web gateway (SWG) which can also integrate filtering with the functionality of data loss prevention.

Host-based IDS - a host-based ids (HIDS) captures information from a single host. the core ability is to capture and analyze log files but more sophisticated systems can also monitor OS kernel files, monitor ports and network interfaces.

One other core feature is file integrity monitoring (FIM). FIM software will audit key system files to make sure they match the authorized versions.

Web Application Firewall (WAF) - a WAF is designed to specifically protect software running on web servers and their back-end databases from code injection and dos attacks. they use application-aware processing rules to filter traffic and perform application-specific intrusion detection.

9.6 Web Filtering

Its primary function is to block users from accessing malicious or inappropriate websites, thereby protecting the network from potential threats.

Web filters analyze web traffic, often in real time, and can restrict access based on various criteria such as URL, IP address, content category, or even specific keywords.

Agent-Based Web Filtering

Agent-based web filtering involves installing a software agent on desktop computers, laptops, and mobile devices. The agents enforce compliance with the organization's web filtering policies.

Agents communicate with a centralized management server to retrieve filtering policies and rules and then apply them locally on the device.

Centralized Web Filtering

A centralized proxy server plays a crucial role in web content filtering by acting as an intermediary between end users and the Internet.

When an organization routes Internet traffic through a centralized proxy server, it can effectively control and monitor all inbound and outbound web content.

The primary role of the proxy in web content filtering is to analyze web requests from users and determine whether to permit or deny access based on established policies.

Centralized Web Filtering Techniques

- **URL Scanning -** Where the proxy server examines the URLs requested by users.
- **Content Categorization -** Classifies websites into categories
- **Block Rules -** Uses the proxy server to implement block rules based on various factors such as the website's URL, domain, IP address and even specific keywords within the web content.
- **Reputation-Based Filtering -** This leverages continually updated databases that score websites based on their observed behavior and history.

SECTION 10

ASSESS ENDPOINT SECURITY CAPABILITIES

10.1 Endpoint Security

Hardening - this is the process of putting an os or application in a secure configuration however hardening must be balanced against the access requirements and usability in a particular situation.

The essential principle is of least functionality meaning the system should run only the protocols and services required by legit users and no more. Interfaces, services and application service ports not in use should be disabled.

Patch Management - on residential and small networks, hosts can be configured to auto-update either by the windows update process or in Linux with the commands yum-cron or apt unattended-upgrades depending on the package manager used by the distribution.

Patches can become incompatible with a particular application and cause availability issues. update repositories can also be infected with malware that can then be spread via automatic updates.

Anti-virus (a-v)/ anti-malware - first generation of anti-virus scanned for only viruses but today they can perform generalized malware detection. While a-v software remains important, signature-based detection is widely regarded to be insufficient for the prevention of data breaches.

Host-based intrusion Detection/Prevention (hids/hips) - HIDS provide threat detection via logs and file system monitoring. other products may also monitor ports and network interfaces and process data and logs generated by specific applications such as http or ftp.

Endpoint Protection Platform (EPP) - An EPP is a single agent performing multiple security tasks, including malware/intrusion detection and prevention but also other features such as firewall, web content filtering and file/message encryption.

Sandboxing - this is a technique that isolates an untrusted host or app in a segregated environment to conduct tests. sandbox offers more than traditional anti-malware solutions because you can apply a variety of different environments to the sandbox instead of just relying on how the malware might exist in your current configuration.

10.2 Segmentation

This is the division of an enterprise into security zones based on function, performance and security requirements.

Security zones are enforced by firewall ingress and egress access control lists

Security Zones

- **Untrusted -** The organization has no control
- **Screened Subnet -** Has connections to both trusted and untrusted networks
- **Trusted -** The organization has complete control
- **Enclave -** Is a restricted network within a trusted network
- **Air Gapped -** Does not connect to any untrusted network
- **Physically Isolated -** Does not connect to any other network
- **Wireless -** Supports wireless transmissions
- VPN - Designed to facilitate secure communications over a public circuit

Micro-Segmentation - This is a method of creating zones within data centers and cloud environments to isolate workloads from one another and secure them individually.

It allows for the implementation of a zero trust protect surface environments.

A protect surface is made up of the network's most critical and valuable data, assets and applications.

North-South traffic is one that flows into and out of a data center or cloud while East-West refers to traffic within a data center or cloud.

Isolation - This is when zones, devices, sessions or even components need to be segregated so as not to cause harm or be harmed.

Virtualization - creates multiple environments from a single physical hardware system.

Logical - A VLAN divides a single existing network into multiple logical network segments which can be restricted.

10.3 Mobile Device Management

Mobile Device Deployment Models Include

- **Bring Your Own Device (BYOD) -** the mobile device is owned by the employee and will have to meet whatever security profile is required. it's the most common model for employees but poses the most difficulties for security managers.
- **Corporate Owned Business Only (COBO) -** the device is owned by the company and may only be used for company business
- **Corporate Owned, Personally-Enabled (COPE) -** the employee may use it to access personal email ,social media accounts and for some personal web browsing.
- **Choose Your Own Device (CYOD) -** very similar to cope except that here, the employee is given a choice of device from a list.
- **Enterprise Mobility Management (EMM) -** this is a class of management software designed to apply security policies to the use of mobile devices and apps in an enterprise.
- **Mobile Device Management (MDM) -** sets device policies for authentication, feature use (camera and microphone) and connectivity. MDM also allows device resets and remote wipes.
- **Mobile Application Management (MAM) -** sets policies for apps that can process corporate data and prevents data transfer to personal apps.

IoS in the enterprise - In apple's ios ecosystem, third-party developers can create apps using apple's software development kit available only on macos.

Corporate control over IoS devices and distribution of corporate and b2b apps is facilitated by participating in the device enrollment program, the volume purchase program and the developer enterprise program.

Android in the enterprise - Android is open source meaning there is more scope for vendor-specific versions and the app model is far more relaxed.

The sdk is available on linux, windows and macos.

Mobile access control systems - If a threat actor is able to gain access to a smartphone, they might be able to gain access to plenty of confidential data as well as cached passwords for email, social media etc.

Smartphone authentication - Access control can be implemented by configuring a screen lock that can be bypassed using a password, pin or swipe pattern. Some devices also support biometrics like fingerprint readers.

Screen lock - The screen lock can also be configured with a lockout policy. For example, the device can be locked out for a period of time after a certain number of incorrect password attempts.

Context-aware authentication - Smartphones now allow users to disable screen locks when the device detects it is in a trusted location (home) however an enterprise may seek more stringent access controls to prevent misuse of a device.

For example, even if a device has been unlocked, the user might need to reauthenticate in order to access the corporate workspace.

Remote wipe - If the phone is stolen, it can be set to factory defaults or cleared of any personal data with the use of the remote wipe feature. it can also be triggered by several incorrect password attempts.

In theory, the thief could prevent the remote wipe by ensuring the phone cannot connect to the network then hacking the phone and disabling its security.

Full device encryption & external media - in ios, there are various levels of encryption:

- All user data on the device is always encrypted but the key is stored on the device. It's this key that is deleted in a remote wipe to ensure the data is inaccessible.
- Email data and any apps using the "data protection" option are subject to a second round of encryption using a key derived from the user's credential.

Location services - location services make use of two systems:

- **Global positioning system (gps) -** Means of determining the device's latitude and longitude based on information received from satellites via a gps sensor.
- **Indoor positioning system (ips) -** Works out a device's location by triangulating its proximity to other radio sources such as cell towers and wi-fi access points.

Geofencing and camera /microphone enforcement - Geofencing is the practice of creating a virtual boundary based on real-world geography and can be a useful tool for controlling the use of camera or video functions or applying context-aware authentication.

GPS tagging - This is the process of adding geographical identification metadata such as latitude and longitude, photographs, sms messages, video and so on.

GPS tagging is highly sensitive personal information and potentially confidential organizational data also.

Content management - Containerization allows the employer to manage and maintain the portion of the device that interfaces with the corporate network. a container can also enforce storage segmentation where the container will be associated with a directory.

rooting & jailbreaking

- **Rooting -** Associated with android devices and typically involves using custom firmware
- **Jailbreaking -** Associated with ios and is accomplished by booting the device with a patched kernel
- **Carrier unlocking -** For either ios or android and it means removing the restrictions that lock a device to a single carrier.

Rooting or jailbreaking mobile devices involves subverting the security measures on the device to gain super administrative access to it but also has the side effect of permanently disabling certain security features.

10.4 Secure Mobile Device Connections

Personal area networks (pans) - These enable connectivity between a mobile device and peripherals. Ad hoc (peer-to-peer) networks between mobile devices or between mobile devices and other computing devices can also be established

For corporate security, these peer-to-peer functions should generally be disabled.

Ad hoc wi-fi and wi-fi direct - An ad hoc network involves a set of wireless stations establishing peer-to-peer connections with one another rather than using an access point.

Wi-fi directly allows one-to-one connections between stations though one of them will serve as a soft access point.

Tethering and hotspots - A smartphone can share its internet connection with other devices via wi-fi making it a hotspot.

Where the connection is shared by connecting the smartphone to a pc via usb or bluetooth, it can be referred to as tethering.

Bluetooth connection methods

- **Device discovery -** Allows the device to connect to any other bluetooth devices nearby.
- **Authentication & authorization -** Use of a simple passkey to “pair” connecting devices
- Malware

Bluetooth connection methods - Discoverable devices are vulnerable to **bluejacking,** where the spammer sends unsolicited messages to the device.

Bluesnarfing refers to using an exploit in bluetooth to steal information from someone else’s phone.

Infrared & rfid connection methods - infrared has been used for pan but it’s use in modern smartphones and wearable technology focuses on two other uses:

- **Ir blaster -** This allows the device to interact with an ir receiver and operate a device such as a tv as though it were the remote control.
- **Ip sensor -** These are used as proximity sensors and to measure health information (heart rate & blood oxygen levels).

Radio frequency id (rfid) is a means of encoding information into passive tags which can easily be attached to devices, clothing and almost anything else.

Skimming involves using a fraudulent rfid reader to read the signals from a contactless bank card

Microwave radio connection methods - Microwave radio is used as a backhaul link from a cell tower to the service provider's network and these links are important to 5g where many relays are required and provisioning fiber optic cable backhaul can be difficult.

A microwave link can be provisioned in two modes:

- **Point-to-point (p2p) -** Microwave uses high gain antennas to link two sites and each antenna is pointed directly at the other. It's very difficult to eavesdrop on the signal as an intercepting antenna would have to be positioned within the direct path.
- **Point-to-multipoint (p2m) -** Microwave uses smaller sectoral antennas each covering a separate quadrant. P2m links multiple sites to a single hub and this can be cost-efficient in high density urban areas.

SECTION 11

ENHANCE APPLICATION SECURITY CAPABILITIES

11.1 DNS Security, Directory Services & Snmp

DNS Security - to ensure dns security on a private network, local DNS servers should only accept recursive queries from local authenticated hosts and not from the internet.

Clients should be restricted to using authorized resolvers to perform name resolution. DNS footprinting means obtaining information about a private network by using its DNS server to perform a zone transfer (all the records in a domain) to a rogue DNS.

Security Extensions (DNSSEC) - These Help to Mitigate against spoofing And Poisoning Attacks by Providing a Validation Process For DNS responses.

Secure Directory Services - a network directory lists the subjects (users, computers and services) and objects (directories and files) available on the network plus the permissions subjects have over objects.

Most Directory Services Are Based on The Lightweight Directory Access Protocol (LDAP) Running over Port 389.

Authentication Referred To As Binding To The Server Can Be Implemented By:

- **No Authentication -** Anonymous Access Is Granted
- **Simple Bind -** The Client Must Supply Its Distinguished Name And Password In Plaintext
- **Simple Authentication And Security Layer (Sasl) -** The Client And Server Negotiate The Use Of A Supported Authentication Mechanism Such As Kerberos.
- **Ldap Secure (Ldaps) -** The Server Is Installed With A Digital Certificate Which It Uses To Setup A Secure Tunnel For The User Credential Exchange. Ldaps Use Port 636.

Generally Two Levels Of Access To The Directory Can Be Granted Which Are Read-Only Access (Query) And Read/Write Access (Update) And Is Implemented Using An Access Control Policy.

Time Synchronization - Many Network Applications Are Time Dependent And Time Critical. The **Network Time Protocol (Ntp)** Provides A Transport Over Which To Synchronize These Time Dependent Applications

Ntp Works Over Udp On Port 123.

NTP has Historically Lacked Any Sort Of Security Mechanism but There Are Moves to Create a Security Extension For the Protocol Called **Network Time Security**.

Simple Network Management Protocol (SNMP) Security - This Is a Widely used Framework For Management And Monitoring And Consists of an SNMP Monitor and Agents. The agent is a Process (Software Or Firmware) running on a Switch, Router, Server or other SNMP-Compatible network device.

This Agent Maintains a Database Called a Management Information Base (MIB) that Holds Statistics Relating to The activity Of the Device. The Agent Is also Capable Of Initiating a Trap Operation Where It Informs The Management System Of a Notable Event Like port failure.

11.2 Secure Application Operations Protocols

HTTP enables clients to request resources from an HTTP server. The server acknowledges the request and responds with the data or an error message.

HTTP is a **stateless** protocol which means the server preserves no information about the client during a session.

Transport Layer Security - Secure Sockets Layer (SSL) was developed by Netscape in the 1990s to address the lack of security in HTTP and was quickly adopted as a standard named Transport Layer Security (TLS).

To implement TLS, a server is assigned a digital certificate signed by some trusted CA. The certificate proves the identity of the server and validates the server's public/private key pair.

The server uses its key pair and the TLS protocol to agree mutually supported ciphers with the client and negotiate an encrypted communications session.

SSL/TLS Version - A server can provide support for legacy clients meaning a TLS 1.2 server could be configured to allow clients to downgrade to TLS 1.1 or 1.0

TLS 1.3 was approved in 2018 and the ability to perform downgrade attacks was mitigated by preventing the use of unsecure features and algorithms from previous versions.

Cipher Suites - This is a set of algorithms supported by both the client and server to perform the different encryption and hashing operations required by the protocol.

Prior to TLS 1.3, a cipher suite would be written like this

ECDHE-RSA-AES128-GCM-SHA256

This means that the server can use Elliptic Curve Diffie-Hellman Ephemeral mode for a session key agreement, RSA signatures, 128-bit AES-GCM (Galois Counter Mode) for symmetric bulk encryption and 256-bit SHA for HMAC functions.

TLS 1.3 uses simplified and shortened suites

TLS_AES_256_GCM_SHA384

Only ephemeral key agreement is supported in 1.3 and the signature type is supplied in the certificate so the cipher suite only lists the bulk encryption key strength and mode of operation (AES_256_GCM) plus the cryptographic hash algorithm (SHA384).

11.3 File Transfer, Email & Video Services

FTP - File Transfer Protocol is the most popular protocol for transferring files across networks because it is very efficient and has wide cross-platform support but has no security mechanism.

SSH FTP (SFTP) & FTP over SSL (FTPS) - SFTP addresses the lack of security by encrypting the authentication and data transfer between client and server. SFTP uses port 22.

Explicit TLS (FTPES) - Use the AUTH TLS command to upgrade and insecure connection established on port 21 to a secure one.

Implicit TLS (FTPS) - Negotiates an SSL/TLS tunnel before the exchange of any FTP commands. This mode uses the secure port 990 for the control connection.

Email Services: These use two types of protocols:

- The Simple Mail Transfer Protocol (SMTP) which specifies how mail is sent from one system to another.
- A mailbox protocol stores messages for users and allows them to download them to client computers or manage them on the server.

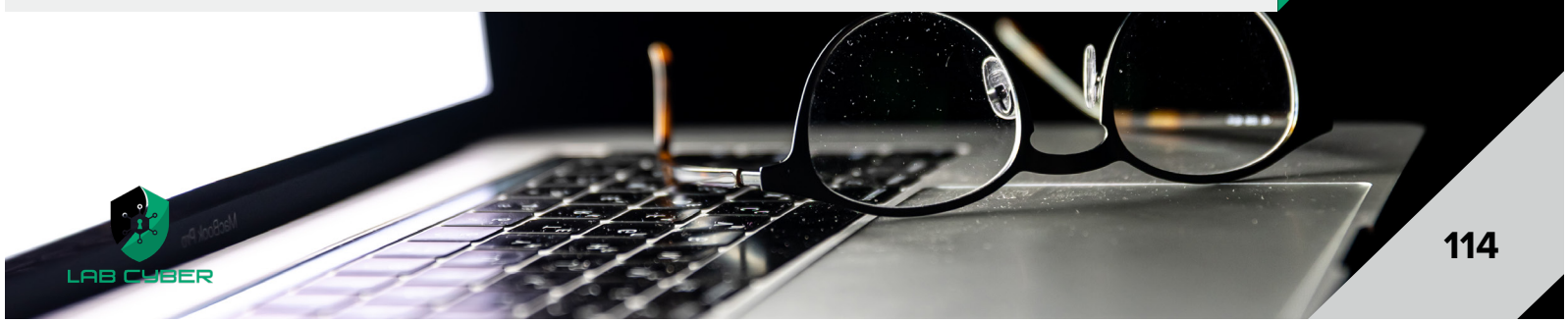
Secure SMTP (SMTPS) - communications can be secured using TLS and there are two ways to do this:

- **STARTTLS -** This command will upgrade an existing unsecure connection to use TLS. Also referred to as explicit TLC or opportunistic TLS.
- **SMTPS -** This establishes the secure connection before any SMTP commands are exchanged. Also referred to as implicit TLS.

Typical SMTP configurations use the following ports and secure services:

- **Port 25 -** Used for message relay between SMTP servers or Message Transfer Agents (MTA)
- **Port 587 -** Used by mail clients to submit messages for delivery by an SMTP server
- **Port 465 -** Some providers and mail clients use this port for message submission over implicit TLS (SMTPS)

Secure POP (POP3S) - The Post Office Protocol v3 is a mailbox protocol designed to store the messages delivered by SMTP on a server.



Secure IMAP (IMAPS) - The Internet Message Access Protocol v4 (IMAP4) supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously.

Secure/Multipurpose Internet Mail Extensions (S/MIME) - Is a means of applying both authentication and confidentiality on a per-message basis.

11.4 Email Security

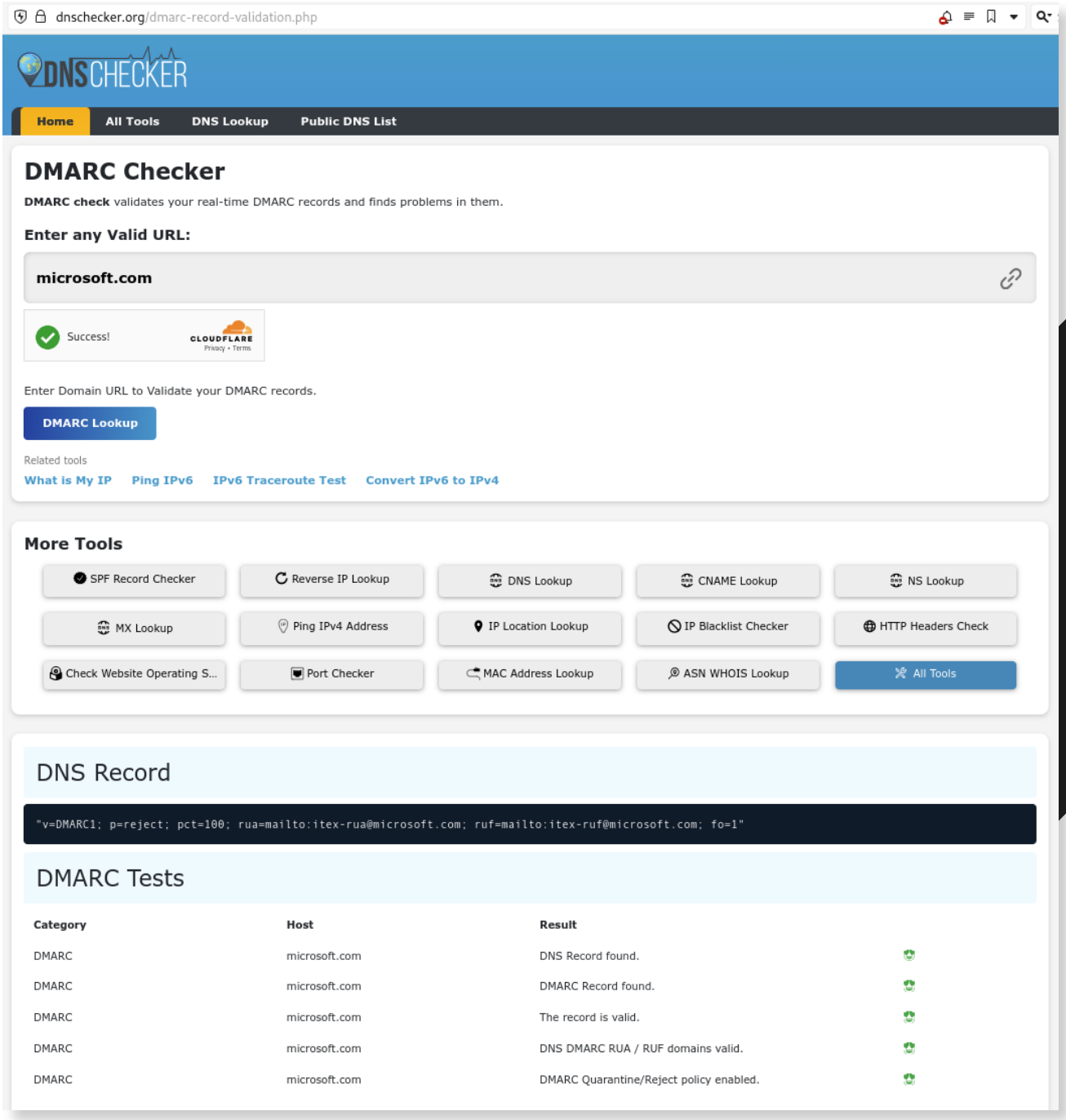
Sender Policy Framework (SPF) - Is an email authentication method that helps detect and prevent sender address forgery commonly used in phishing and spam emails.

SPF works by verifying the sender's IP address against a list of authorized sending IP addresses published in the DNS TXT records of the email sender's domain.

DomainKeys Identified Mail (DKIM) - Leverages encryption features to enable email verification by allowing the sender to sign emails using a digital signature, The receiving email server uses a DKIM record in the sender's DNS record to verify the signature and the email's integrity.

Domain-based Message Authentication, Reporting & Conformance (DMARC) - Uses the results of SPF and DKIM checks to define rules for handling messages, such as moving messages to quarantine or spam, rejecting them outright or tagging the message.

An email gateway - Is the control point for all incoming and outgoing email traffic. It acts as a gatekeeper, scrutinizing all emails to remove potential threats before they reach inboxes. Email gateways utilize several security measures, including anti-spam filters, antivirus scanners, and sophisticated threat detection algorithms to identify phishing attempts, malicious URLs, and harmful attachments.



The combined use of SPF, DKIM, and DMARC significantly enhances email security by making it much more difficult for attackers to impersonate trusted domains, which is one of the most common tactics used in phishing and spam attacks.

11.5 Secure Coding Techniques

Input Validation - malicious input could be crafted to perform an overflow attack or some type of script or SQL injection attack. To mitigate this, there should be routines to check user input and anything that does not conform to what is required must be rejected.

Normalization and Output Encoding - normalization means that a string is stripped of illegal characters or substrings and converted to the accepted character set. this ensures that the string is in a format that can be processed correctly by the input validation routines.

Output encoding means that a string is re-encoded safely for the context in which it is being used.

Server-side versus Client-side Validation - a web application can be designed to perform code execution and input validation locally (on the client) or remotely (on the server). The main issue with client-side validation is that the client will always be more vulnerable to some sort of malware interfering with the validation process.

Main issue with server-side validation is that it can be time-consuming as it may involve multiple transactions between the server and client. Client-side validation is usually restricted to informing the user that there is some sort of problem with the input before submitting it to the server. relying on client-side validation only is poor programming practice.

Web Application Security In Response Headers

A Number Of Security Options Can Be Set In The Response Header

- **Http Strict Transport (HST) -** Forces Browser to Connect Using HTTPS Only, Mitigating Downgrade Attacks Such as SSL Stripping.
- **Content Security Policy (CSP)** - Mitigates Clickjacking, Script Injection And Other Client-Side Attacks.
- **Cache Control -** Sets Whether The Browser can Cache Responses. Preventing Caching Of Data Protects Confidential And Personal Information Where The Client Device Might Be Shared By Multiple Users.

Data Exposure And Memory Management - Data Exposure is a Fault that allows Privileged Information such as a Password or Personal Data to be Read without being Subject to the appropriate access controls.

A Well-Written application must be able to Handle Errors and Exceptions Gracefully. Ideally the Programmer should have Written a **Structured Exception Handler (SEH)** to dictate what the application should then do.

The Error Must Not Reveal Any Platform Information Or Inner Workings Of The Code To An Attacker.

Secure Code Usage - A Program May Make Use Of Existing Code In The Following Ways:

- **Code Reuse -** using a block of code from elsewhere in the same application or from another application to perform a different function.
- **Third-Party Library -** using a binary package (such as a dynamic link library) that implements some sort of standard functionality such as establishing a network connection.
- **Software Development Kit (SDK) -** using sample code or libraries of pre-built functions from the programming environment used to create the software.
- **Stored Procedures -** Using a Pre-Built Function to Perform a database query.

Unreachable code and dead code

Unreachable code is a part of application source code that can never be executed (if ... then conditional logic that is never called because the conditions are never met).

Dead code is executed but has no effect on the program flow (a calculation is performed but the result is never stored as a variable or used to evaluate a condition).

Static code analysis - this is performed against the application code before it is packaged as an executable process. The software will scan the source code for signatures of known issues.

Human analysis of software source code is described as a manual code review. It is important that the code be reviewed by developers other than the original coders to try to identify oversights, mistaken assumptions or a lack of experience.

Dynamic code analysis - static code review will not reveal any vulnerabilities that exist in the runtime environment. dynamic analysis means that the application is tested under real world conditions using a staging environment.

Fuzzing is a means of testing that an application‘s input validation routines work well. fuzzing will deliberately generate large amounts of invalid or random data and record the responses made by the application.

Associated with fuzzing is the concept of stress testing an application to see how an application performs under extreme performance or usage scenarios.

Finally, the fuzzer needs some means of detecting an application crash and recording which input sequence generated the crash.

SECTION 12 -

EXPLAIN INCIDENT RESPONSE AND MONITORING CONCEPTS

12.1 - Incident Response Process

This is a set of policies and procedures that are used to identify, contain, and eliminate cyberattacks. The goal is to allow an organization to quickly detect and stop attacks, minimize damage and prevent future attacks of the same type.

Principal stages in incident response life cycle

- **Preparation -** Makes the system resilient to attack. this includes: hardening systems, writing policies and procedures,and creating incident response resources and procedures
- **Identification** - Determine whether an incident has taken place, assess how severe it might be and then notify the appropriate personnel.
- **Containment -** Limits the scope and magnitude of the incident. The main aim of incident response is to secure data while limiting the immediate impact on customers and business partners.
- **Eradication -** Once the incident is contained, the vulnerability/issue is removed and the affected systems are restored to a secure state.
- **Recovery -** The restored system is then reintegrated back into the business process that it supports
- **Lessons learned -** Analyze the incident and responses to identify whether procedures or systems could be improved. It is also imperative to document the incident.

12.2 Cyber Incident Response Team

Preparing for incident response means establishing the policies and procedures for dealing with security breaches and the personnel and resources to implement those policies.

First task is to define and categorize types of incidents. in order to identify and manage incidents, you should develop some method of reporting, categorizing and prioritizing them.

An incident response team can be referred to as a cyber incident response team (CIRT), computer security incident response team (CSIRT) or computer emergency response team (cert).

For Major Incidents, Expertise from Other Business Divisions might be needed

- **Legal -** The Incident Can Be Evaluated From The Perspective Of Compliance With Laws And Industry Regulations.
- **Human Resources (Hr) -** Incident Prevention And Remediation Actions May Affect Employee Contracts, Employment Law And So On.
- **Marketing -** The Team Is Likely To Require Marketing Or Public Relations Input So Any Negative Publicity From A Serious Incident Can Be Managed.

Incident response policies should establish clear lines of communication both for reporting incidents and for notifying affected parties.

Status and event details should be circulated on a need-to-know basis and only to trusted parties identified on a call list. Trusted parties might include both internal and external stakeholders.

Obligations to report the attack must be carefully considered and it may be necessary to inform affected parties during or immediately after the incident so that they can perform their own remediation e.g "change your passwords immediately"

12.3 Incident Response Plan

This lists the Procedures, Contacts and Resources Available to Responders for Various Incident Categories.

A **Playbook** Is a Data-Driven Standard Operating Procedure (SOP) to assist Junior Analysts in Detecting and Responding to Specific Cyber threat Scenarios.

One Challenge In Incident Management is to allocate Resources Efficiently and there are several factors that can affect this Process.

- **Data Integrity -** The Most important factor In Prioritizing Incidents
- **Downtime -** An Incident can Either Degrade or Interrupt the Availability Of an asset Or system.
- **Economic/Publicity -** both data integrity and downtime will have important economic effects. short-term might involve lost business opportunity while long-term may involve damage to reputation and marketing standing.
- **Scope -** Refers To the number of affected Systems In an Incident
- **Detection Time -** research has shown that more than half of data breaches are not detected for weeks or months. this demonstrates that systems used to search for intrusions must be thorough.
- **Recovery Time -** Some Incidents require Lengthy Remediation as the system Changes Required are Complex to Implement.

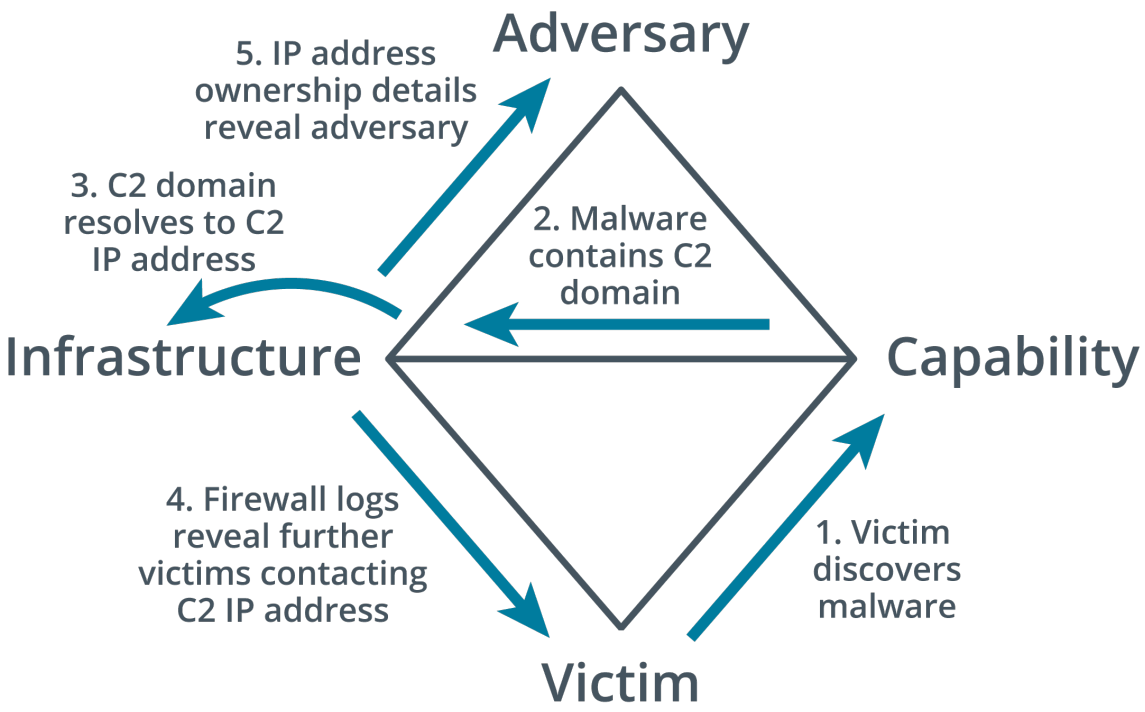
A key tool for threat research is a framework to use to describe the stages of an attack and these stages are referred to as a cyber kill chain.

MITRE att&ck - an alternative to the kill chain is the MITRE corporation's adversarial tactics, techniques and common knowledge.

It provides access to a database of known TTPS and tags each technique with a unique id and places it in one or more tactic categories such as initial access , persistence or command & control.

Diamond model of Intrusion Analysis - this suggests a framework to analyze an intrusion event (e) by exploring the relationships between four core features: adversary, capability, infrastructure and victim.

Each event may also be described by meta-features such as date/time, kill chain phase etc.



12.4 Incident Response Exercises, Recovery And Retention Policy

Identi ication - This is the Process of Collating Events and Determining whether any of them should be Managed as Incidents or as Possible Precursors to an Incident.

- **Tabletop -** least costly where the facilitator presents a scenario and the responders explain what action they would take to identify, contain and eradicate the threat. flashcards are used in place of computer systems.
- **Walkthroughs -** similar to tabletop except here the responders demonstrate what actions they would take in response such as running scans and analyzing sample files.
- **Simulations -** a team based exercise where the red team attempts an intrusion, the blue team operates response and recovery controls and the white team moderates and evaluates the exercise.

Disaster recovery plan - Also called the emergency response plan. This is a document meant to minimize the effects of a disaster or disruption. meant for short term events and implemented during the event itself.

Business continuity plan - Identifies how business processes should deal with both minor and disaster-level disruption. a continuity plan ensures that business processes can still function during an incident even if at a limited scale.

Continuity of operation planning (COOP) - This terminology is used for government facilities but is functionally similar to business continuity planning. In some definitions, coop refers specifically to backup methods of performing mission functions without IT support.

Retention policy - a retention policy for historic logs and data captures sets the period of which these are retained. indicators of a breach might be discovered only months after the breach and this would not be possible without the retention policy to keep logs and other digital evidence.

Training On Specific Incident Response Scenarios Can Use Three Forms

- **Tabletop -** Least Costly where the Facilitator presents a Scenario and The Responders explain what action they Would Take to Identify, Contain and Eradicate the Threat. Flashcards are used in place of Computer Systems.
- **Walkthroughs -** Similar to Tabletop Except here The Responders Demonstrate what actions they would Take In Response Such As Running Scans and Analyzing Sample Files.
- **Simulations -** A Team Based Exercise where the Red Team Attempts an Intrusion, the Blue Team Operates Response and Recovery Controls and the White Team moderates and Evaluates The Exercise.

Disaster recovery plan - also called the emergency response plan. This is a document meant to minimize the effects of a disaster or disruption. meant for short term events and implemented during the event itself.

Business continuity plan - identifies how business processes should deal with both minor and disaster-level disruption. a continuity plan ensures that business processes can still function during an incident even if at a limited scale.

Continuity of operation planning (COOP) - this terminology is used for government facilities but is functionally similar to business continuity planning. In some definitions, coop refers specifically to backup methods of performing mission functions without IT support.

Retention policy - a retention policy for historic logs and data captures sets the period of which these are retained. indicators of a breach might be discovered only months after the breach and this would not be possible without the retention policy to keep logs and other digital evidence.

12.5 Incident Identification

Training On Specific Incident Response Scenarios Can Use Three Forms

- Using Logs, Error Messages And Ids/Firewall Alerts
- Comparing Deviations To Established Metrics To Recognize Incidents And Their Scopes
- Manual Or Physical Inspections Of Site, Premises, Networks And Hosts
- Notification By An Employee, Customer Or Supplier
- Public Reporting Of New Vulnerabilities

Correlation - This Means Interpreting The Relationship Between Individual Data Points To Diagnose Incidents Of Significance to The Security Team.

A SIEM (Security Information and Event Management System) Correlation Rule Is a Statement That Matches Certain Conditions.

These Rules Use Logical Expressions such as And And or And Operators (==, <,>, In)

A Single-User Logon Failure Might Not Raise an Alert However Multiple Failed Logins For The Same Account Over A Short Period Of Time Should Raise One.

Error.Logonfailure > 3 And Logonfailure.Alice And Duration < 10 Minutes

One of the biggest challenges in operating a SIEM is tuning the system sensitivity to reduce false positive indicators being reported as an event.

The correlation rules are likely to assign a criticality level to each match.

Trend analysis - This is the process of detecting patterns or indicators within a data set over a time series and using those patterns to make predictions about future events.

- Frequency-based trend analysis establishes a baseline for a metric such as number of errors per hour of the day. if the frequency exceeds the threshold for the baseline, then an alert is raised.
- **Volume-based trend analysis -** this can be based on logs growing much faster than usual. This analysis can also be based on network traffic and endpoint disk usage.
- Statistical deviation analysis can show when a data point should be treated as suspicious. For example, a data point that appears outside the two clusters for standard and admin users might indicate some suspicious activity by that account.

Logging platforms - Log data from network appliances and hosts can be aggregated by a siem either by installing a local agent to collect the data or by using a forwarding system to transmit logs directly to the siem server.

Syslog - Provides an open format, protocol and server software for logging event messages and it's used by a very wide range of host types.

A syslog message comprises a pri code, a header containing a timestamp and host name and a message part. usually uses UDP port 514

- Rsyslog uses the same configuration file syntax but can work over tcp and use a secure connection.
- Syslog-ng uses a different configuration file syntax but can also use tcp/secure communications and more advanced options for message filtering.

In linux, rather than writing events to syslog-format text files, logs from processes are written to a binary-format called **journald**.

Events captured by journald can be forwarded to syslog and to view events in journald directly, you can use **journalct** command to print the entire journal log.

System & security logs - The five main categories of windows event logs are:

- **Application** - Events generated by applications and services
- **Security** - Audit events such as a failed logon or denied access to a file
- **System -** Events generated by the os and its services such as storage volume health checks
- **Setup -** Events generated during the windows installation
- **Forwarded Events -** Events that are sent to the local log from other hosts.

Network logs can be generated from routers, firewalls, switches and access points.

Authentication attempts for each host are likely to be written to the security log.

DNS event logs may be logged by a dns server while web servers are typically configured to log http traffic that encounters an error or traffic that matches some predefined rule set.

The status code of a response can reveal something about both the request and the server's behavior.

- Codes in the 400 range indicate client-based errors
- Codes in the 500 range indicate server-based errors
- "403" may indicate that the server is rejecting a client's attempts to access resources they are not authorized to.
- "502" (bad gateway) response could indicate that communications between the target server and its upstream server are being blocked or the upstream server is down.

Dump files - A system memory dump creates an image file that can be analyzed to identify the processes that are running, the contents of temporary file systems, registry data, network connections and more.

It can also be a means of accessing data that is encrypted when stored on a mass storage device.

Metadata - This the properties of data as it is created by an application stored on media or transmitted over a network. Metadata sources are useful during an investigation as they can establish timeline questions as well as containing other types of evidence.

File - File metadata is stored as attributes. The file system tracks when a file was created, accessed and modified. The acl attached to a file showing its permissions also represents another type of attribute.

Web - when a client requests a resource from a web server, the server returns the resource plus headers setting or describing its properties. headers describe the type of data returned.

Email - An email's internet header contains address information for the recipient and sender plus details of the servers handling transmission of the message between them.

Mobile - Phone metadata comprises call detail records (CDRs) of incoming, outgoing and attempted calls and sms text time, duration and the opposite party's number. meta data will also record data transfer volumes and the location history of the device can be tracked by the list of cell towers it has used to connect to the network.

Netflow/ipfix - A flow collector is a means of recording metadata and statistics about network traffic rather than recording each frame.

Flow analysis tools can provide features such as:

- Highlighting trends and patterns in traffic generated by particular applications, hosts and ports.
- Alerting based on detection of anomalies or custom triggers
- Identification of traffic patterns revealing rouge user behavior or malware in transit

12.6 Digital Forensics Documentation

Digital forensics is the practice of collecting evidence from computer systems to a standard that will be accepted in a court of law.

Prosecuting external threat sources can be difficult as the threat actor may be in a different country or have taken effective steps to disguise their location. Like dna or fingerprints, digital evidence is latent meaning that the evidence cannot be seen with the naked eye; rather it must be interpreted using a machine or process.

Due Process - term used in us and uk common law that requires that people only be convicted of crimes following the fair application of the laws of the land. The first response period following detection and notification is often critical. to gather evidence successfully, it's vital that staff do not panic or act in a way that would compromise the investigation.

Legal Hold - this refers to the fact that information that may be relevant to a court case must be preserved. This means that computer systems may be taken as evidence with all the obvious disruption to a network that entails.

Chain of Custody - this documentation reinforces the integrity and proper handling of evidence from collection, to analysis, to storage and finally to presentation. It is meant to protect an organization against accusations that evidence has been tampered with during a trial.

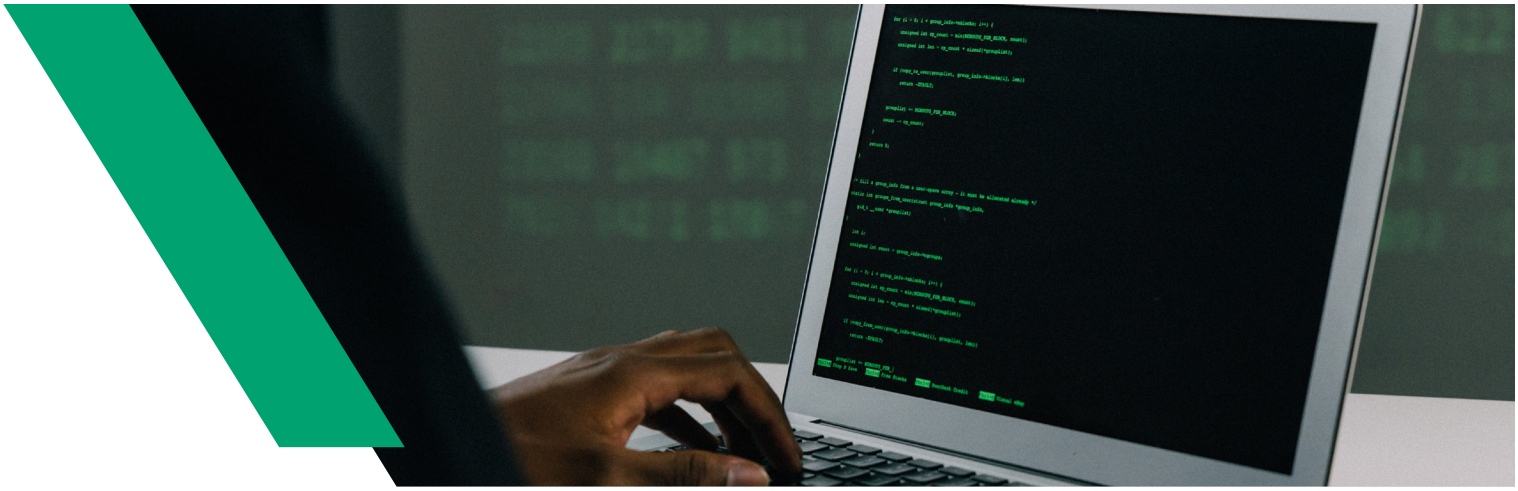
Digital Forensics Reports - a report summarizes the significant contents of the digital data and the conclusions from the investigator‘s analysis.

- Analysis must be performed without bias. conclusions and opinions should be formed only from the direct evidence under analysis.
- Analysis methods must be repeatable by third parties with access to the same evidence
- Ideally, the evidence must not be changed or manipulated.

E-Discovery - this is a means of filtering the relevant evidence produced from all the data gathered by a forensic examination and storing it in a database in a format such that it can be used as evidence in a trial.

Some Of The Functions Of E-Discovery Suites Are:

- **Identify And De -** Duplicate Files and Metadata
- **Search -** Allows Investigators to Locate Files of Interest to the Case.
- **Tags -** Apply standardized Keywords or labels to Files and Metadata to Help Organize The Evidence.
- **Security -** At all Points Evidence must be Shown to have Stored, Transmitted and analyzed without Tampering.
- **Disclosure -** An Important part of the Trial Procedure is that Evidence Is made available to Both Plaintiff And Defendant.



Video and witness interviews - The first phase of a forensics investigation is to document the scene by taking photographs and ideally audio and video.

As well as digital evidence, an investigator should interview witnesses to establish what they were doing at the scene and whether they observed any suspicious behavior or activity.

Timelines - A very important part of a forensic investigation will involve tying events to specific times to establish a consistent and verifiable narrative. This visual representation of events in a chronological order is called a timeline.

Operating systems and files use a variety of methods to identify the time at which something occurred but the benchmark time is coordinated universal time (UTC).

Local time will be offset from UTC by several hours and this local time offset may also vary if a seasonal daylight saving time is in place.

NTFS uses UTC “internally“ but many OS and file systems record timestamps as the local system time and when collecting evidence, it is vital to establish how a timestamp is calculated and note the offset between the local system time and utc.

Event logs and network traffic - An investigation may also obtain the event logs for one or more network appliances and/or server hosts. network captures might provide valuable evidence.

For forensics, data records that are not supported by physical evidence (data drive) must meet many tests to be admissible in court. if the records were captured by a SIEM, it must demonstrate accuracy and integrity.

The intelligence gathered from a digital forensic activity can be used in two different ways:

- **Counterintelligence -** Identification and analysis of specific adversary tactics, techniques and procedures (TTPS) provides information on how to configure and audit systems so they are better able to capture evidence of attempted and successful intrusions.
- **Strategic Intelligence -** Data that has been analyzed to produce actionable insights. These insights are used to inform risk management and security control provisioning to build mature cybersecurity capabilities.

12.7 Digital Forensics Evidence Acquisition

Acquisition is the process of obtaining a forensically clean copy of data from a device held as evidence. if the system is not owned by the organization then the seizure could be challenged legally (BYOD)

Data acquisition is also more complicated when capturing evidence from a digital scene compared to a physical one (evidence may be lost due to system glitches or loss of power).

Data acquisition usually proceeds by using a tool to make an image from the data held on the target device. the image can be acquired from either volatile or nonvolatile storage.

Digital acquisition and order of volatility - the general principle is to capture evidence in the order of volatility from more volatile to less volatile.

According to the ISOC, the order is as follows

- Cpu registers and cache memory
- Contents of ram including routing table, arp cache, kernel statistics
- Data on persistent mass storage devices like hard drives, usbs
- Remote logging and monitoring data
- Physical configuration and network topology
- Archival media and printed documents

Digital forensics software include:

- Encase forensic is a digital forensics case management product. contains workflow templates showing the key steps in diverse types of investigation.
- The forensic toolkit (ftk) from accessdata. a commercial investigation suite designed to run on windows server.
- **The sleuth kit -** an open source collection of command line tools and programming libraries for disk imaging and file analysis. autopsy is the gui that sits on top of the kit and is accessed through a web browser.
- **Winhex -** a commercial tool for forensic recovery and analysis of binary data, with support for a range of file systems and memory dump types.
- The volatility framework which is widely used for system memory analysis.

Disk image acquisition refers to acquiring data from non-volatile storage. it could also be referred to as device acquisition meaning the ssd storage in a smartphone or media player.

There are three device states for persistent storage acquisition

Live acquisition - Means copying the data while the host is still running. this may capture more evidence or more data for analysis and reduce the impact on overall services. however the data on the actual disks will have changed so this method may not produce legally acceptable evidence.

Static acquisition by shutting down the host - runs the risk that the malware will detect the shut-down process and perform anti-forensics to try and remove traces of itself.

Static acquisition by pulling the plug - This means disconnecting the power at the wall socket. This will likely preserve the storage device in a forensically clean state but there is the risk of corrupting data.

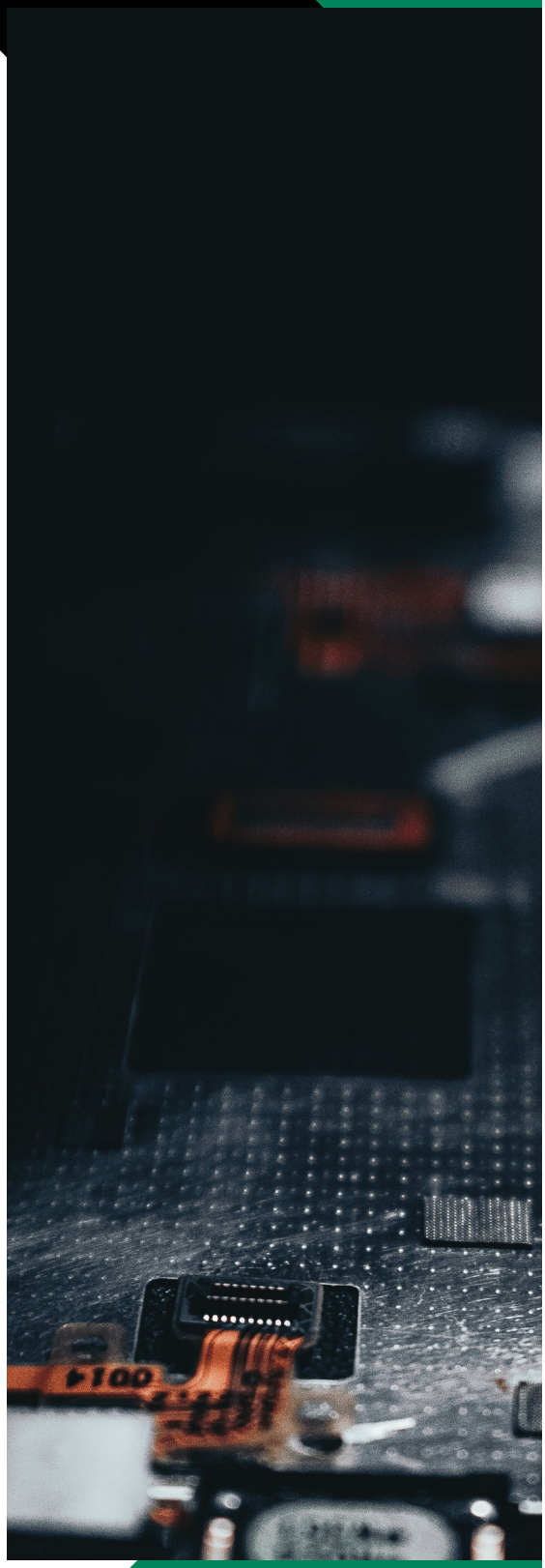
Whichever method is chosen, it is important to document the steps taken and supply a timeline of all actions.

Preservation and integrity of evidence - It is vital that the evidence collected at the crime scene conform to a valid timeline. recording the whole process establishes **provenance** of the evidence as deriving directly from the crime scene.

To obtain a clean forensic image from a non-volatile storage, you need to ensure nothing you do alters the data or metadata on the source disk or file system. A **write blocker** can ensure this by preventing any data from being changed by filtering write commands.

The host devices and media taken from the crime scene should be labeled, bagged and sealed using tamper-evident bags. bags should have anti-static shielding to reduce the possibility that data will be damaged or corrupted on the electronic media by electrostatic discharge.

The evidence should be stored in a secure facility.



Acquisition of other data types includes:

- **Network -** Packet captures and traffic flows can contain evidence. most networks will come from a SIEM.
- **Cache -** Software cache can be acquired as part of a disk image. the contents of hardware cache are generally not recoverable.
- **Artifacts and data recovery -** Artifact refers to any type of data that is not part of the mainstream data structures of an os. Data recovery refers to analyzing a disk for file fragments that might represent deleted or overwritten files. The process of recovering them is referred to as carving.
- **Snapshot -** Is a live acquisition image of a persistent disk and may be the only means of acquiring data from a virtual machine or cloud process.
- **Firmware -** Is usually implemented as flash memory. Some types like the pc firmware can potentially be extracted from the device or from the system memory using an imaging utility.

12.8 Data Sources

Incident investigation often requires analysis of several data sources in order to draw a defensible conclusion.

- Vulnerability Scans
- Log files
- SIME dashboards
- Metadata
- Packet capture

Log Analysis and Response Tools

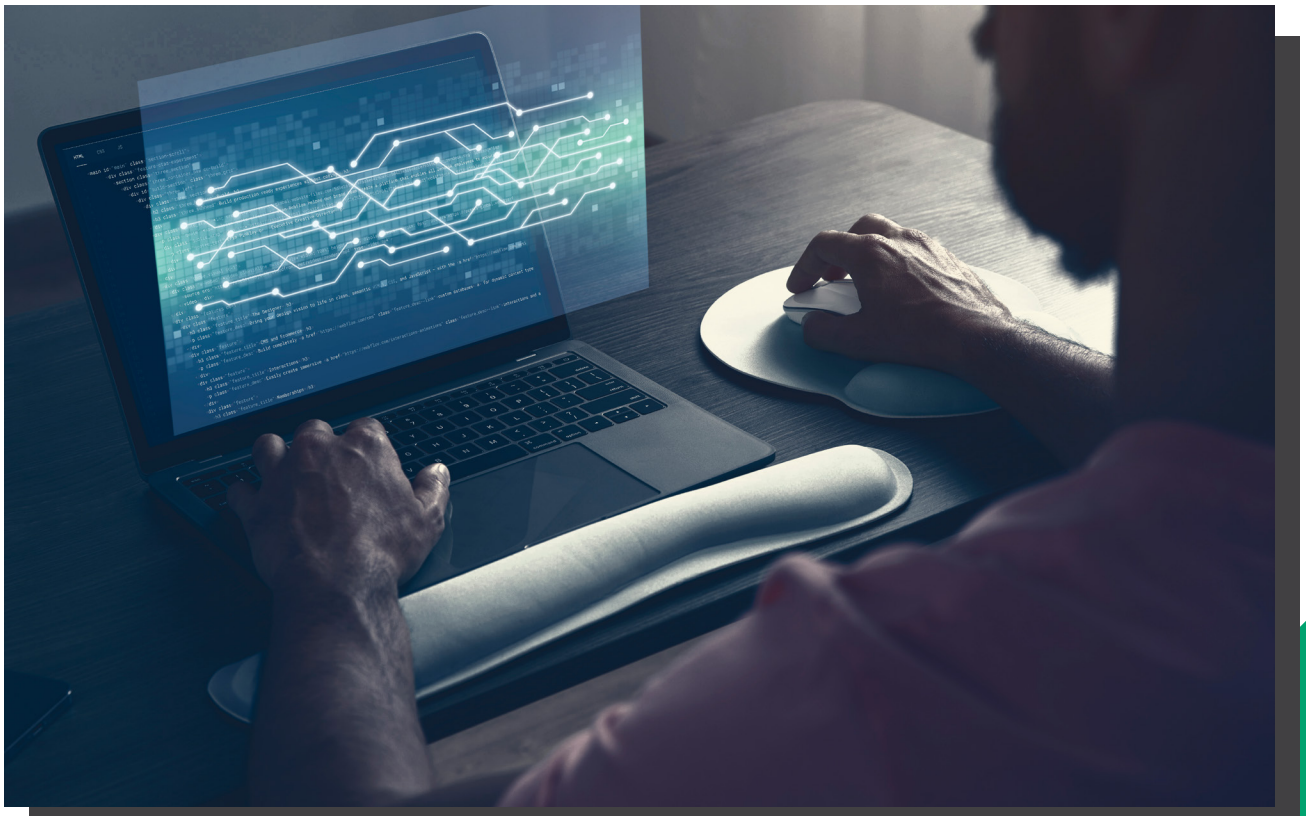
- Security Information Event Management (SIEM) is an automation tool for real-time data capture, event correlation, analysis and reporting
- Threat Intelligence Platform (TIP) is an automation tool that combines multiple threat intelligence feeds and integrates with existing SIEM solutions
- User & Entity Behavior Analytics (UEBA) - is an automation tool that models human and machine behavior to identify normal and abnormal behavior.
- Security Orchestration, Automation and Response (SOAR) is an automation tool that responds to alerts and takes remediation steps.

Packet Capture - This is the process of intercepting and logging traffic for analysis.

- A protocol analyzer (sniffer) is a tool used to capture and analyze network packets
- A port mirror captures network traffic from one or several ports of a switch and forwards a copy of the traffic to an analysis device
- A network TAP is a dedicated hardware device that is inserted between network devices and makes copies of the traffic and forwards to an analysis device.

Packet Capture Modes

- **Normal -** The network interface card (NIC) only captures frames intended for the interface (filtering by MAC address)
- **Promiscuous -** The NIC accepts any frame it captures even if it was not the intended recipient
- **Unfiltered -** Packet capture regardless of data elements
- **Filtered -** Packet capture limited to specific data elements



SECTION 13 -

ANALYZE INDICATORS OF MALICIOUS ACTIVITY

13.1 Malware Classification

Some malware classifications such as Trojan, virus and worm focus on the vector used by the malware. the vector is the method by which the malware executes on a computer and potentially spreads to other network hosts.

The Following Categories Describe Some Types Of Malware According To Vector:

- **Viruses & Worms -** spread without any authorization from the user by being concealed within the executable code of another process.
- **Trojan -** Malware Concealed within an Installer Package for Software that Appears to be Legitimate
- **Potentially Unwanted Programs/Applications (Pups/Puas) -** These are software installed alongside a package selected by the user. unlike a Trojan, their presence isn't necessarily malicious. they are sometimes referred to as grayware.
-

Other Classifications are Based on the Payload Delivered By the Malware. The Payload Is the Action Performed by the Malware

Examples Of Payload Classification Include:

- Spyware
- Rootkit
- Remote Access Trojan (Rat)
- Ransomware

13.2 Computer Viruses

This is a type of malware designed to replicate and spread from computer to computer usually by “infecting” executable applications or program code.

The Following Categories Describe Some Types Of Malware According To Vector:

- **Non-Resident/File Infector -** the virus is contained within a host executable file and runs with the host process. the virus will try to infect other process images on persistent storage and perform other payload actions.
- **Memory Resident -** when the host file is executed, the virus creates a new process for itself in memory. the malicious process remains in the memory even if the host process is terminated.
- **Boot -** the virus code is written to the disk boot sector and executes as a memory resident process when the OS starts.
- **Script And Macro Viruses -** the malware uses the programming features available in local scripting engines for the OS and/or browser such as PowerShell, javascript, Microsoft office documents or PDF documents with JavaScript enabled.

The term **multipartite** is used for viruses that use multiple vectors and **polymorphic** for viruses that can dynamically change or obfuscate their code to evade detection. Viruses must infect a host file or media. an infected file can be distributed through any normal means - on a disk, on a network, a download from a website or email attachment.

13.3 Computer Worms & Fileless Malware

Computer Worms - this is a memory resident malware that can run without user intervention and replicate over network resources. viruses need the user to perform an action but worms can execute by exploiting a vulnerability in a process and replicate themselves.

Worms can rapidly consume network bandwidth as the worm replicates and they may be able to crash an operating system or server application. worms can also carry a payload that may perform some other malicious action.

Fileless malware - as security controls got more advanced so did malware and this new sophisticated modern type of malware is often referred to as fileless.

The Following Categories Describe Some Types Of Malware According To Vector:

- Fileless malware do not write their code to disk. the malware uses memory resident techniques to run its own process within a host process or dynamic link library (DLL). the malware may change registry values to achieve persistence.
- Fileless malware uses lightweight shell code to achieve a back door mechanism on the host. the shell code is easy to recompile in an obfuscated form to evade detection by scanners. it is then able to download additional packages or payloads to achieve the actor's objectives.
- Fileless malware may use "live off the land" techniques rather than compiled executables to evade detection. this means that the malware code uses legitimate system scripting tools like power-shell to execute payload actions.

13.4 Spyware, Keyloggers, Rootkits, Backdoors, Ransomware & Logic Bombs

Spyware - This is malware that can perform adware-like tracking but also monitor local application activity, take screenshots and activate recording devices.

Adware - Grayware that performs browser reconfigurations such as allowing cookies, changing default search engines, adding bookmarks and so on.

Tracking cookies - Can be used to record pages visited, the user's ip address and various other metadata.

Keylogger - Spyware that actively attempts to steal confidential information by recording keystrokes.

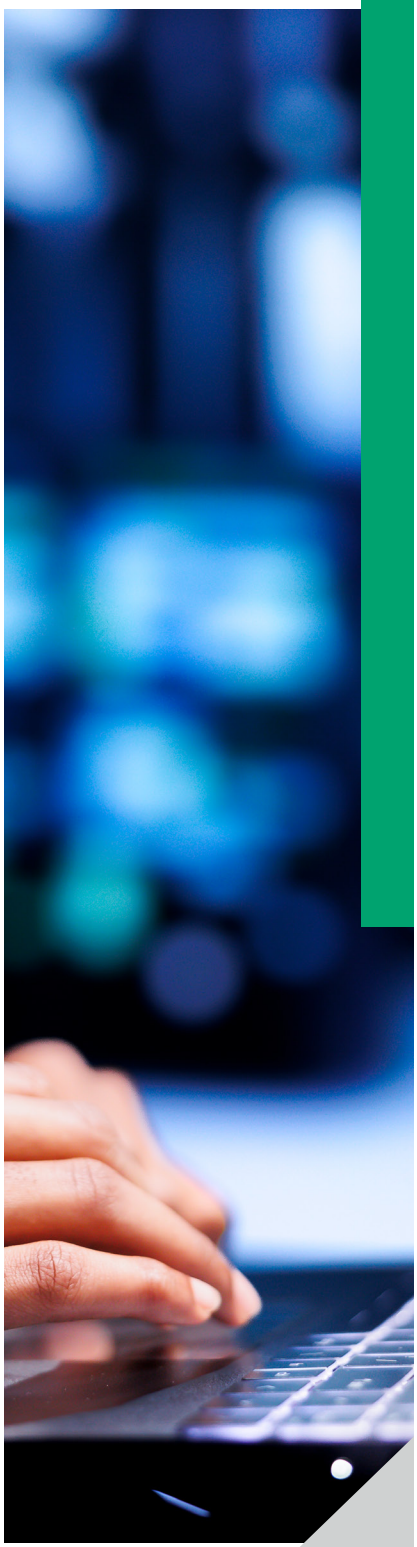
Backdoors & rats - A backdoor provides remote user admin control over a host and bypasses any authentication method. A remote access trojan is a backdoor malware that mimics the functionality of legitimate remote control programs but is designed specifically to operate covertly. a group of bots under the same control of the same malware are referred to as a botnet and can be manipulated by the herder program.

Rootkits - This malware is designed to provide continued privileged access to a computer while actively hiding its presence. it may be able to use an exploit to escalate privileges after installation.software processes can run in one of several "rings".

- Ring 0 is the most privileged and provides direct access to hardware
- Ring 3 is where user-mode processes run
- Ring 1 or 2 is where drivers and i/o processes may run.

Ransomware - This type of malware tries to extort money from the victim by encrypting the victim's files and demanding payment. ransomware uses payment methods such as wire transfer or cryptocurrency.

Logic bombs - Logic bombs are not always malware code. a typical example is a disgruntled admin who leaves a scripted trap that runs in the event his or her account is disabled or deleted. anti-malware software is unlikely to detect this kind of script and this type of trap is also referred to as a mine.



13.5 Malware Indicators & Process Analysis

There Are Multiple Indicators Of Malware:

- Antivirus Notifications
- Sandbox Execution
- Resource Consumption - Can Be Detected Using Task Manager Or Top Linux Utility.
- File System

Because shellcode is easy to obfuscate, it can easily evade signature-based a-v products. Threat hunting and security monitoring must use behavioral-based techniques to identify infections.

Along with observing how a process interacts with the file system, network activity is one of the most reliable ways to identify malware.

13.6 Password Attacks

Plain text/ unencrypted attacks - an attack that exploits unencrypted password storage such as those used in protocols like http, pap and telnet.

Online attacks - The threat actor interacts directly with the authentication service using either a database of known passwords or a list of passwords that have been cracked online. This attack can be prevented with the use of strong passwords and restricting the number of login attempts within a specified period of time.

Password spraying - A horizontal brute force attack where the attacker uses a common password (123456) and tries it with multiple usernames.

Offline attacks - An offline attack means the attacker has gotten access to a database of password hashes e.g %systemroot%\system32\config\sam or %systemroot%\ntds\ntds.dit (the active directory credential store)

Brute force attack - Attempts every possible combination in the output space in order to match a captured hash and guess the plaintext that generated it. the more the characters used in the plaintext password, the more difficult it would be to crack.

Rainbow table attack - A refined dictionary attack where the attacker uses a precomputed lookup table of all possible passwords and their matching hashes.

Hybrid attack - Uses a combination of brute force and dictionary attacks.

Password crackers - There are some windows tools including cain and l0phtcrack but the majority of password crackers like hashcat run primarily on linux.

Password managers can be implemented with a hardware token or as a software app:

- **Password Key** - Usb tokens for connecting to pcs and smartphones.
- **Password Vault -** Software based password manager typically using a cloud service to allow access from any device.

13.7 Tactics, Techniques & Procedures

A tactic, technique or procedure (TTP) is a generalized statement of adversary behavior. ttps categorize behaviors in terms of campaign strategy and approach (tactics), generalized attack vectors (techniques) and specific intrusion tools and methods (procedures).

An indicator of Compromise (IOC) is a residual sign that an asset or network has been successfully attacked. in other words, an ioc is evidence of a ttp.

Examples Of Iocs Include

- Unauthorized Software And Files
- Suspicious Emails
- Suspicious Registry And File System Changes
- Unknown Port And Protocol Usage
- Excessive Bandwidth Usage
- Rouge Hardware
- Service Disruption And Defacement
- Suspicious Or Unauthorized Account Usage

Strictly speaking an IOC is evidence of an attack that was successful. The term indicator of attack (IOA) is sometimes also used for evidence of an intrusion attempt in progress.

13.8 Privilege Escalation & Error Handling

Application Attack - this attacks a vulnerability in an os or application and a vulnerability refers to a design flaw that can cause the application security system to be circumvented or to crash. the purpose of this attack is to allow the attacker to run his/her own code on the system and this is referred to as arbitrary code execution.

Where the code is transmitted from one computer to another, this is referred to as remote code execution.

Privilege Escalation - a design flaw that allows a normal user or threat actor to suddenly gain extended capabilities or privileges on a system.

- **Vertical Privilege Escalation -** The User or Application Is Able to Gain Access To Functionality Or Data That Shouldn't be Available to Them.
- **Horizontal Privilege Escalation -** The User Or Application Is Able to Access Data Or Functionality Intended For Another User.

Error Handling - an application attack may cause an error message. as such applications in the event of an error should not reveal configuration or platform details that can help the attacker.

Improper Input Handling - good programming practice dictates that any input accepted by a program or software must be tested to ensure that it is valid. most application attacks work by passing invalid or maliciously constructed data to the vulnerable process.

13.9 Uniform Resource Locator Analysis & Percent Encoding

Uniform Resource Locator Analysis - besides pointing to the host or service location on the internet, a url can encode some action or data to submit to the server host. this is a common vector for malicious activity.

Http Methods - It Is Important To Understand how Http Operates.

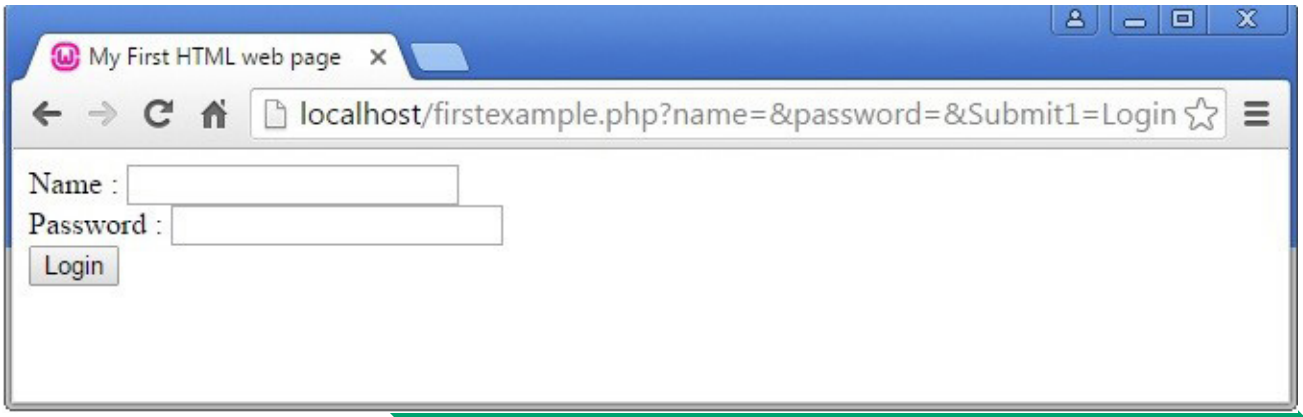
- An Http Session Starts With A Client (Web Browser) Making A Request To An HTTP Server.
- The Connection Establishes a TCP Connection
- The connection can be used for multiple requests or a client can start new TCP connections for different requests.

A request typically contains a method, resource (URL path), version number, headers and body. the principal method is get but other methods include:

- **Post -** Send Data To The Server For Processing By The Requested Resource
- **Put -** Create Or Replace The Resource. Delete Can Be Used To Remove The Resource
- **Head -** Retrieve The Headers For A Resource Only (Not The Body)

Data can be submitted to the server using a post or put method and the http headers and body or by encoding the data within the URL used to access the resource.

Data submitted via a URL is delimited by the ? character which follows the resource path and query parameters are usually formatted as one or more name=value pairs, with ampersands delimiting each pair.



Percent Encoding - a URL can contain only unreserved and reserved characters from the ASCII set. reserved ASCII characters are used as delimiters within the URL syntax.

Reserved Characters **: / ? # [ ] @ ! $ & ' ( ) * + , ; =**

There are also unsafe characters which cannot be used in a URL. Control characters such as null string termination, carriage return, line feed, end of file and tab are unsafe.

Character	Percent Encoding
null	%00
space	%20
CR (Carriage Return)	%0D
LF (Line Feed)	%0A
+	%2B
%	%25
/	%2F
\	%5C
.	%2E
?	%3F
"	%22
'	%27
<	%3C
>	%3E
&	%26
|	%7C

13.10 Api & Replay Attacks, Cross-Site Request Forgery, Clickjacking & Ssl Strip Attacks

Application Programming Interface Attacks - web applications and cloud services implement application program interfaces (APIs) to allow consumers to automate services.

If the API isn't secure, threat actors can easily take advantage of it to compromise the services and data stored on the web application. API calls over plain http are not secure and could easily be modified by a third party.

Some Other Common Attacks Against APIs Include

- Ineffective secrets management, allowing threat actors to discover an API key and perform any action authorized to that key.
- Lack of input validation allowing the threat actor to insert arbitrary parameters into api methods and queries. this is often referred to as allowing unsanitized input.
- Error Messages Revealing Clues to a Potential Adversary. (Username/Password)
- Denial of Service (DoS) by Bombarding the API with Bogus Calls.

Replay Attacks - session management enables web applications to uniquely identify a user across a number of different actions and requests.

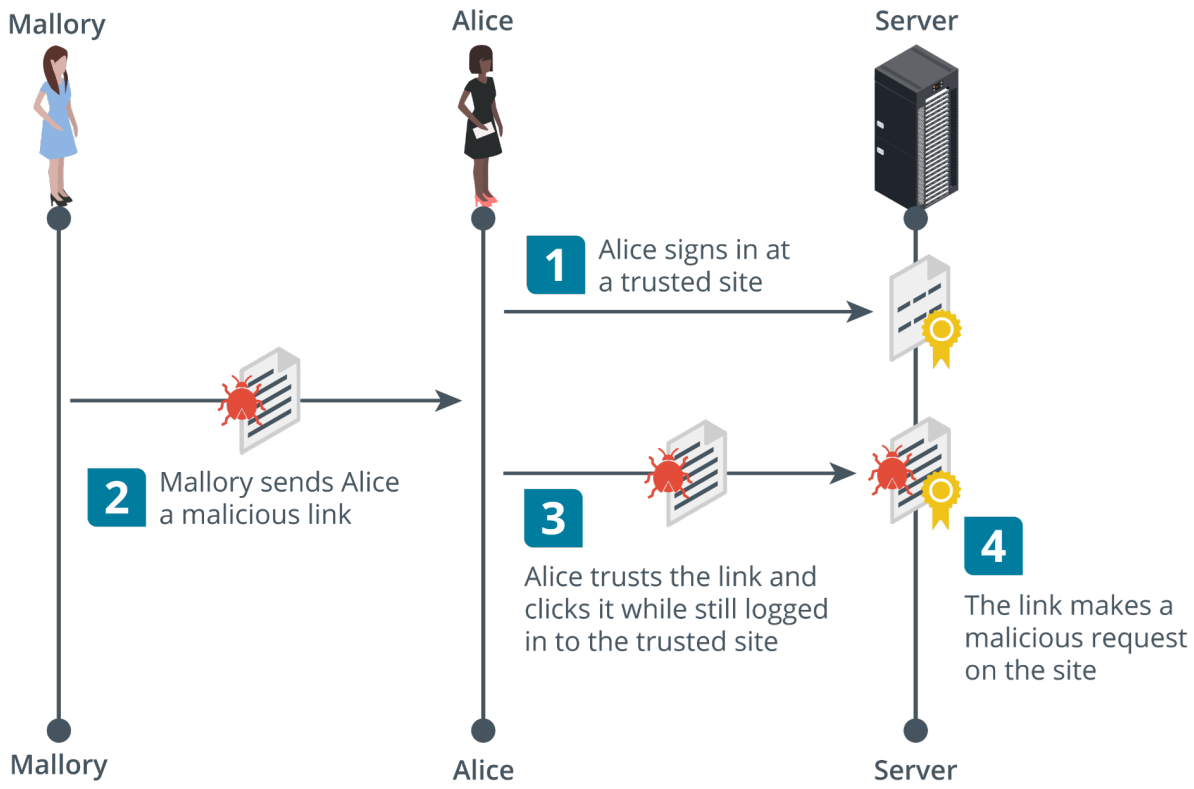
To establish a session, the server normally gives the client some type of token and a replay attack works by sniffing or guessing the token value and then submitting it to re-establish the session illegitimately.

HTTP by default is a stateless protocol meaning the server preserves no information about the client but cookies allow for the preservation of data.

A cookie has a name, value and optional security and expiry attributes. cookies can either be persistent and non-persistent.

Cross-Site Request Forgery - a client-side or cross-site request forgery (CSRF or XSRF) can exploit applications that use cookies to authenticate users and track sessions.

In order to work, the attacker must convince the victim to start a session with the target site. the attacker must then pass an http request to the victim's browser that spoofs an action on the target site such as changing a password or an email address.



if the target site assumes the browser is authenticated because there is a valid session cookie, it will accept the attacker's input as genuine. this is also referred to as a confused deputy attack.

Clickjacking - this is an attack where what the user sees and trusts as a web application with some sort of login page or form contains a malicious layer or invisible iframe that allows an attacker to intercept or redirect user input.

Clickjacking can be launched using any type of compromise that allows the adversary to run arbitrary code as a script. it can be mitigated by using http response headers that instruct the browser not to open frames from different origins.

SSL Strip - this is launched against clients on a local network as they try to make connections to websites. the threat actor first performs a MITM attack via ARP poisoning to masquerade as the default gateway. When a client requests an http site that redirects to an HTTPs site in an unsafe way, the SSL strip utility proxies the request and response, serving the client the http site with an unencrypted login form thus capturing any user credentials.