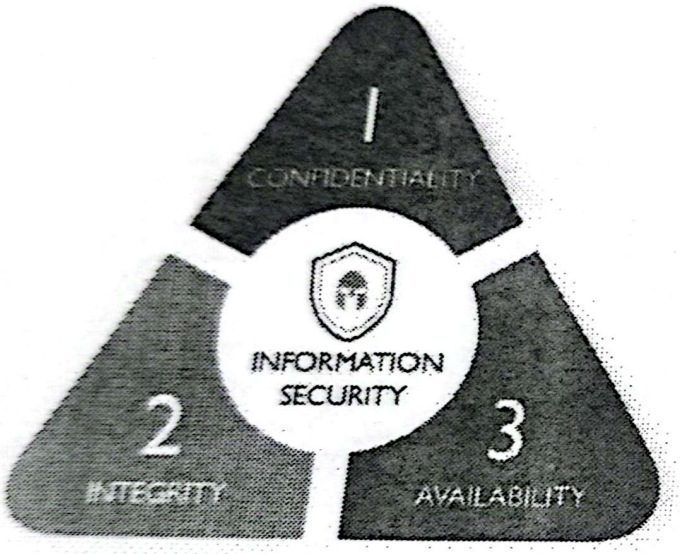


Figure 1: CIA Triad

CIA Triad

- Information security seeks to address three specific principles: **Confidentiality, integrity** and **availability**, also known as the CIA triad.
- If one of the principle is compromised, the security of the organization is threatened.
- The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.

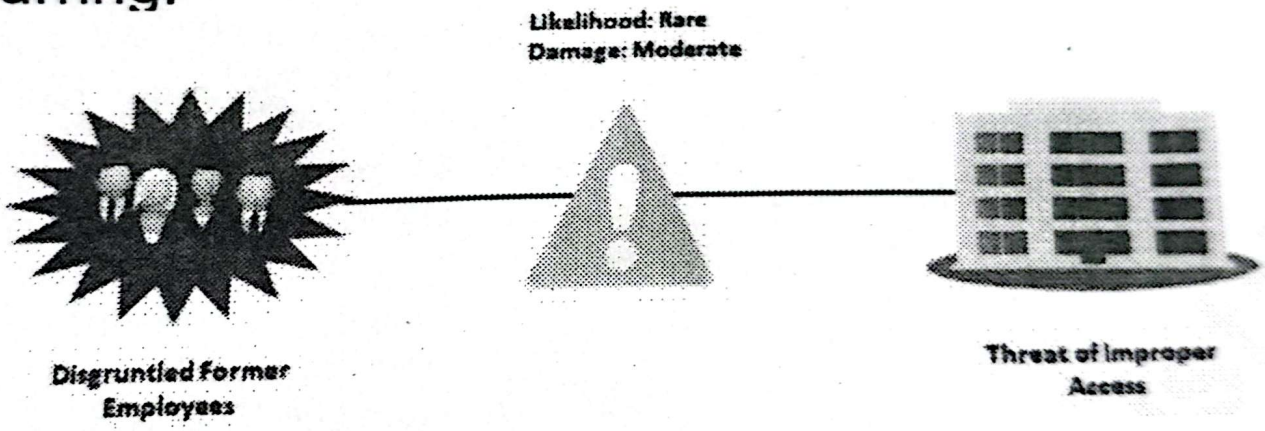
Threats

- In the realm of computer security, a threat is any event or action that could potentially cause damage to an asset or anything that could exploit a vulnerability which could break CIA triad.
- Threats are often in violation of a security requirement, policy, or procedure.
- Regardless of whether a violation is intentional or unintentional, malicious or not, it is considered a threat.
- Potential threats to computer and network security include:
  - Unintentional or unauthorized access or changes to data.
  - The interruption of services.
  - The interruption of access to assets.
  - Damage to hardware.
  - Unauthorized access or damage to facilities.

Threat means any potential danger tha
causing damage to systems, networ

Risk

- Risk is a concept that indicates exposure to the chance of damage or loss.
- It signifies the likelihood of a hazard or dangerous threat occurring.



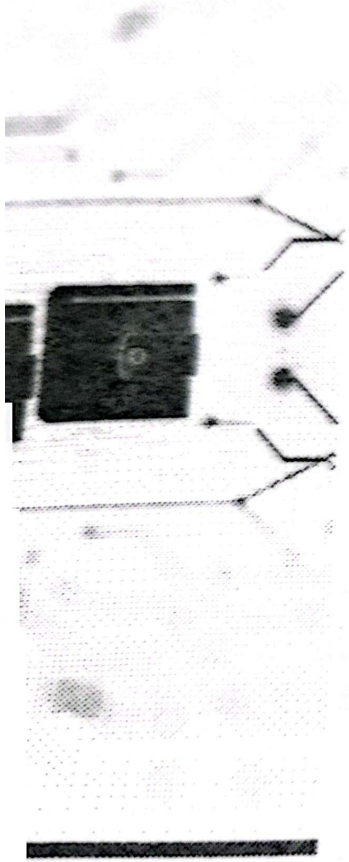
Password Policy

The password policy is an important policy to both users and administrators.

The following outlines some of the considerations that should go into the password policy:

- Minimum password length:
  - The minimum password length specifies how many characters users must have in their passwords.
  - The typical minimum length used by businesses is eight characters.
- Password history
  - The password history setting specifies how many past passwords the system should keep track of.
  - The concept here is that users are not allowed to reuse a password in the password history.
  - Companies typically set the history to 12 or 24 passwords.
- Maximum password age:
  - The maximum password age specifies how long an user is allowed to have a specific password.
  - This value is normally set anywhere from 30 to 60 days, at which time the user must change their password.

- **Operating System Updates**: Regularly update your operating system to patch vulnerabilities and protect against known exploits.
- **Software Updates**: Keep all software, including browsers, antivirus programs, and applications, up to date to ensure you have the latest security patches.
- **Automatic Updates**: Enable automatic updates to ensure you don't miss critical security fixes.



Identifying Signs of a Compromised Computer

Unusual Performance Issues

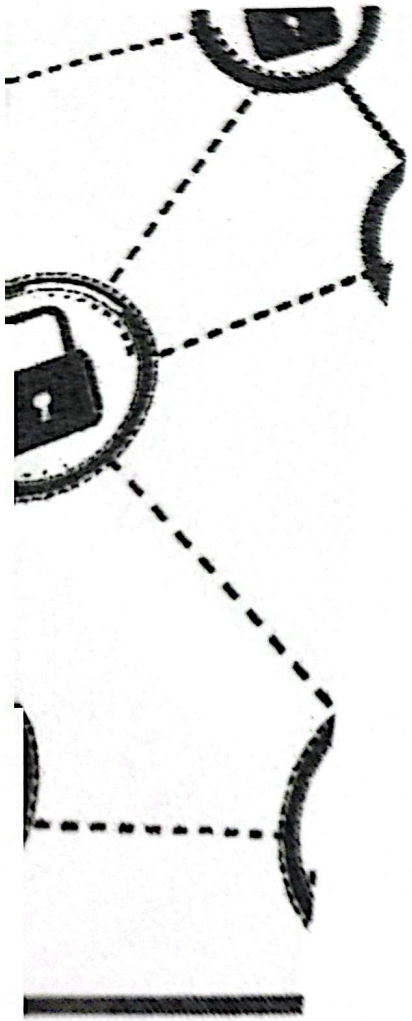
A compromised computer may exhibit slow performance, which can hinder productivity and indicate potential security threats. Sometimes programs take longer to load, or the system crashes frequently.

Unexpected Pop-Ups

Random ads or security warnings appear, especially if they urge you to take immediate action. Frequent unexpected pop-ups can be a sign of adware or malware infections that compromise computer security.

Unauthorized Access Attempts

Apps launch or close without user input. Unauthorized access attempts can signal a security breach, prompting users to take immediate action to secure their systems.



Steps to Take After a Security Breach

Immediate Disconnection

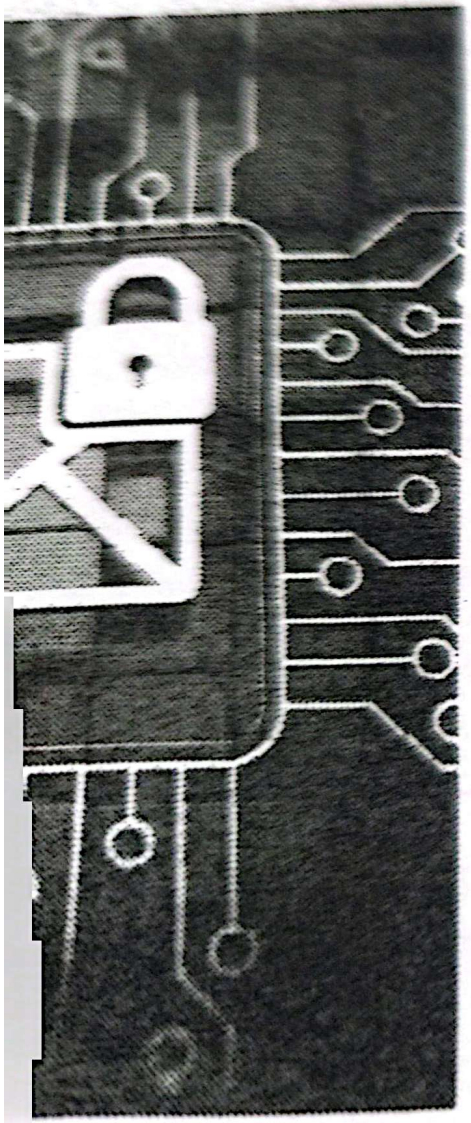
Disconnect the compromised device from the internet *immediately* to prevent further unauthorized access.

Change Passwords

Change all passwords associated with the compromised accounts to secure sensitive information from unauthorized access.

Malware Scan

Conduct a thorough scan for malware to identify and remove any malicious software that could cause further damage.



Encryption Protocols for Emails and Messages

Importance of Encryption

Encryption is vital for protecting sensitive communications from unauthorized access and ensuring confidentiality.

PGP Encryption

PGP (Pretty Good Privacy) is a widely used encryption standard that secures email communications effectively.

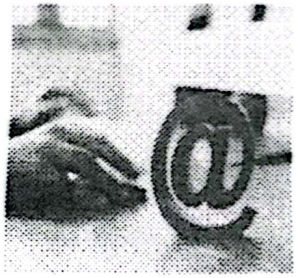
Secure Messaging Apps

Secure messaging apps utilize encryption protocols to ensure that private messages remain confidential.

Recognizing Phishing and Scam Websites

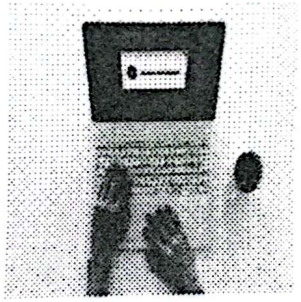
Identifying Suspicious Emails

Learn to recognize the signs of phishing emails, such as poor grammar, unexpected attachments, or generic greetings.



Verifying Sources

Always verify the source of emails and links before clicking to prevent falling victim to scams.



Common Scam Characteristics

Familiarize yourself with common characteristics of scam websites, including poor design and unusual URLs.

Key Features of Ethical Hacking

- **Permission-Based**:
  - Ethical hackers must have explicit authorization from the system owner to conduct their tests.
- **Proactive Security**: (প্রত্যাচক)
  - Focuses on identifying and mitigating vulnerabilities before they can be exploited.
- **Varied Techniques**:
  - Uses tools and methodologies similar to those used by malicious hackers, including penetration testing, social engineering, and vulnerability scanning.
- **Reporting**:
  - Ethical hackers provide detailed reports of their findings, including vulnerabilities, exploitation techniques, and recommendations for remediation.

Goals of Ethical Hacking

- **Identify Vulnerabilities:**
  - Discover security flaws in applications, networks, and systems.
- **Prevent Breaches:**
  - Protect sensitive data and maintain system integrity.
- **Improve Security Posture:**
  - Strengthen defenses through recommendations and patches.
- **Ensure Compliance:**
  - Help organizations comply with security regulations and standards like GDPR, HIPAA, or PCI-DSS.

Attack Targets and Types

- There are many things that can be targeted for an attack; however, all areas of an attack can be distilled down to three core areas.
- The first is the **network**, which is an attack on the communication structure of a network and it can target specific devices or communication protocols.
- The second is **applications**. This is the software running on devices and hosts.
- The third and last area is the **host**, which usually targets the endpoint operating system or user of the system.

The Anatomy of an Attack

- The anatomy of an attack, sometimes referred to as the **Cyber Kill Chain**, basically lays out a series of actions and events attackers commonly use to exploit a system or network.
- This model helps defenders with context and categorizing at what stage an attacker is at when detections are made.
- The cyber kill chain was adopted from the military term ***kill chain***, describing the structure of an attack.
- It was developed by Lockheed Martin as a model for identifying, detecting, and preventing intrusion activity using computers.
- It also describes the TTPs **(tactics, techniques, and procedures)** used during an attack.

1. Passive Information Gathering

- Passive techniques involve collecting data without directly interacting with the target, thereby minimizing the risk of detection.

1.1 OSINT (Open Source Intelligence)

OSINT involves using publicly available information to gather intelligence abou a target.

Tools and Techniques:

- Search Engines (Google, Bing): Advanced search operators to find hidden information
- Social Media Platforms: Analyzing profiles, connections, and activities.
- Public Databases: Accessing government, business, or technical records.
- WHOIS Lookup: Retrieving domain registration details

Example:

- Identifying employee names and emails from LinkedIn.
- Checking a company's digital footprint in public forums.

2. Active Information Gathering

- *Active techniques involve direct interaction with the target, which increases the risk of detection but provides more de and accurate information.*
- **2.1 Port Scanning** → techniqve to identify which ports computer.
  - **Tools:**
    - Nmap → Network scanner
    - Masscan → TCP port scanner
  - **Purpose:**
    - Discover active services (e.g., HTTP, FTP, SSH).
    - Identify potential vulnerabilities.

Keeping Inventory ***

- When gathering information, you will need a place to keep track of it, some form of **inventory**.
- This not only keeps you from repeating steps but helps to classify what is relevant.
- Being disorganized will slow the process down and lead to less success.
- You can use any method or tool to keep track of your information.
- Spreadsheets are the most common method as they are very flexible and can be adapted to support multiple parts of the ove process.
- The sheets with tabs can cover items such as names, dates, and links, while other tabs may be adapted to support some of scanning information later, such as IP address, operating system, and login accounts.
- Starting with web searches and ending with footprinting applications, we will be looking at gathering as much informat about the target before attempting any of the other steps, including exploitation.
- It is this initial detective work that makes hackers and pen testers so effective at what they do.
- Because they have gathered and documented all the information, they are able to quickly pivot and find multiple way infiltrate and exploit the target
- In many cases, the attackers know more about an organization and how it operates than the internal personnel.

Some Useful Google Hacks *** [Command or Name]

- Google has approximately 38 advanced search functions that you can access by entering them into the Google search window, as shown in the following screenshot.

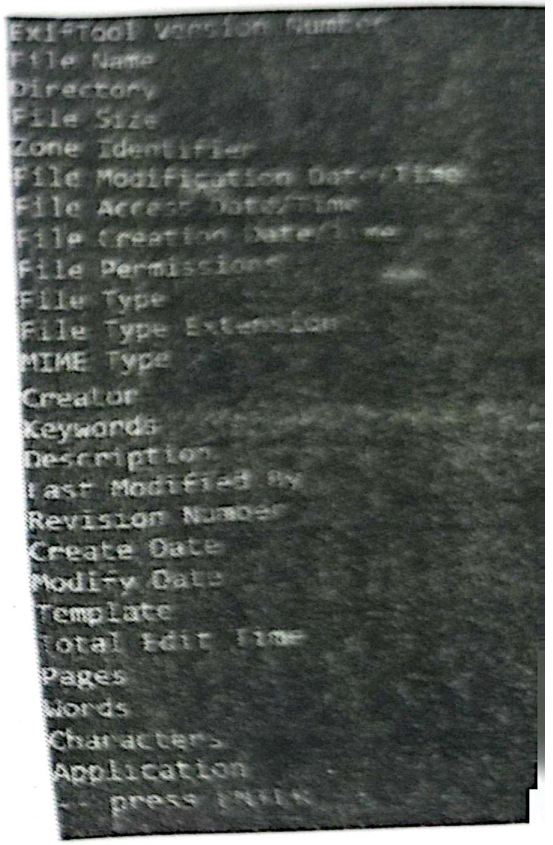
- In search vernacular, the use of quotation marks means **exact or whole phase match**, without which the search engine breaks the phrase into separate terms, and the return results may not be relevant to what you are looking for .

- **link**: This finds sites that link to the specified domain. For example, a link can be `link:starbucks.com`. It is a search operator that finds web pages that link back to the domain. This command is typically used in search engines like Bing or Yahoo (but no longer in Google, as it has removed this operator)

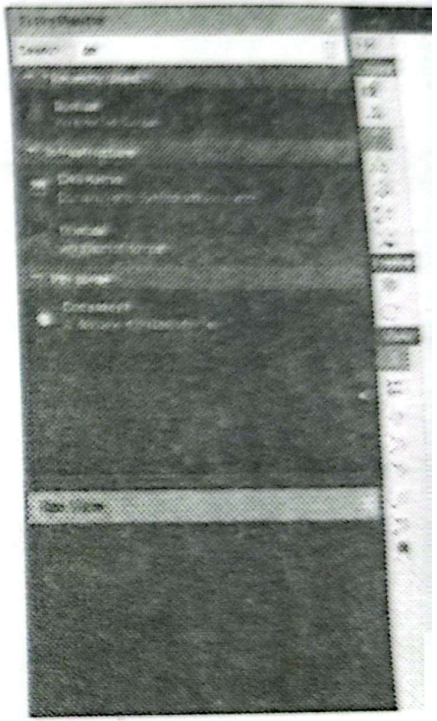
- **Numrange**: Finds a range of numbers in a query up to 5 digits. At one time, this was considered one of the most dangerous searches. It could be used to harvest phone numbers and credit cards. It still works but limitations have been placed on it.

EXIF tools

- **EXIF** stands for **Exchangeable Image File Format**.
- It is a standard that defines the storage of metadata information related to an image or other media.
- While it is commonly associated with images, it applies to documents as well.
- Using this tool, you can not only get items such as the creation and modification dates but also what application created it and who created it.
- Let's look at the output of the EXIF tool:



Maltego ***



- Maltego is a visual tool that takes data points and, by using **transforms**, tries to collect and/or connect data to draw a bigger picture.
- Visual representations of data sometimes show unexpected correlations that otherwise might not be made just by looking at the data alone.
- An example of what the data visualization looks like can be seen in the following figure:
- Once you have all the visuals you wish to have in place, you can save the file for later review or export it as an XML or CSV file that can then be incorporated into your inventory spreadsheet.

visually connect the dots by show

points using graphs → ① Trans

4. SpiderFoot Tools

SpiderFoot is an open-source reconnaissance tool designed to automate the proces intelligence about a target, whether it's an individual, organization, or network.

- It collects and correlates data from multiple open sources and APIs to provide a c view of the target's digital footprint.

Data Sources:

- SpiderFoot integrates with a wide range of sources, including:
- **DNS and WHOIS**: For domain and IP intelligence.
- **Search Engines**: Google, Bing, and other search APIs.
- **Threat Intelligence Platforms**: VirusTotal, AlienVault, and more.
- **Dark Web Sources**: Tor and related services.
- **Public Data Breaches**: Leaks and compromised credential databases.

Key Features of Shodan

1. Device Discovery:
   - Searches for internet-connected devices using specific ports, protocols, or services.
   - Common targets include: Webcams, Smart TVs, Databases (e.g., Elasticsearch, MongoDB), SCADA ,Printers
2. Real Time Monitoring:
   - Tracks newly exposed devices or changes in device configurations.
   - Can alert users to changes in their own infrastructure.
3. Data Collection:
   - Collects metadata about devices, including: Open ports, Running services, Banner information, location
4. Filters and Queries:
   Allows users to perform advanced searches using filters like: country, org, port, os
5. API Integration:
   Provides APIs for developers to integrate Shodan into their tools for automated reconnaissance
6. Exploitation Database:
   Links search results to known vulnerabilities (CVE data) for quick identification of exploitable

① Automated reconnaissance

② continuous device monitoring

Popular Social Engineering Attacks

1 IMPERSONATION:

- The most popular scenario for social engineering attacks is when the hacker impersonates another employee in the organization.
- In the following scenarios, the hacker impersonates an employee in the company who needs some help:

Hacker impersonates Administrator:

- A very popular example of a social engineering attack is when the hacker calls a user and impersonates the network administrator.
- In this scenario the hacker, posing as the administrator, tries to trick the user into compromising security by asking the user to do things such as changing their password or giving away account information.
- The hacker also may ask the user questions about the general setup of the systems.

Hacker impersonates user:

- The hacker calls the network administrator pretending to be a frustrated user. In this scenario the hacker will pretend they do not remember their password or how to get onto the system.
- An unaware administrator may help the hacker, who is acting as a frustrated user, gain access to the system by resetting a password and guiding them through the process of gaining access.

POPULAR NETWORK ATTACKS

Denial of Service

- A DoS attack involves the hacker overloading a system with requests so that the system is so busy servicing the hacker's requests that it cannot service valid requests from other clients
- (see Figure 4-2). For example, a hacker could overload a web server with numerous network requests, making the web server unable to send the web pages to customers in a timely manner.
- This typically results in the customer going to a different site to get adequate service.
- With a DoS attack, the attacker could be causing the target network to perform slowly, or the hacker could

FIGURE 4-2

A DoS attack overloads a system, causing the system to slow down or crash.

Address Resolution Protocol

ARP Poisoning

- ARP is a protocol that maps the IP address to the MAC address and then stores the IP and corresponding MAC address in memory on the system.
- This area of memory is known as the ARP cache (see Figure 4-7).
- ARP poisoning involves the hacker altering the ARP cache on a system, or group of systems, so that all systems have the wrong MAC address stored in the ARP cache for a specific IP address—maybe the address of the default gateway.
- **Typically, the hacker will poison the ARP cache so that the default gateway IP address (your router's IP address) points to the hacker's MAC address.**
- This will ensure that every time a system tries to send data to the router, it will retrieve the hacker's MAC address from the local ARP cache and then send the data to the hacker's system instead of to the router.
- This is how the hacker typically performs an MITM attack on a wired network or wireless network.
- This also allows a hacker to capture all network traffic, even in a switched environment.
- The hacker just needs to enable the routing feature on their system so that all data is then passed on to the router and out to the Internet, while in the meantime the hacker has captured every piece of data headed out to the Internet.

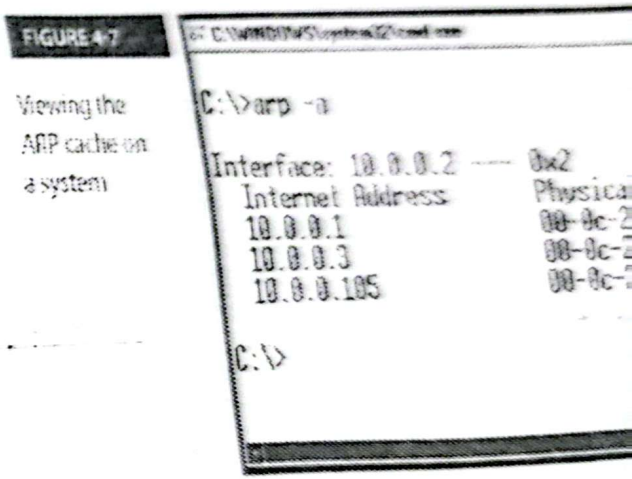


FIGURE 4-7

Viewing the ARP cache on a system

```
C:\>arp -a

Interface: 10.0.0.2 --- 0x2
  Internet Address      Physica
  10.0.0.1              00-0c-2
  10.0.0.3              00-0c-2
  10.0.0.105            00-0c-2

C:\>
```

your device .

MAC Flooding and MAC Cloning

- MAC flooding is when the attacker sends a large number of frames to the switch, causing it t the MAC address table and, as a result, remove old, valid MAC addresses but add the new fa MAC addresses.
- This will cause the switch to flood all frames from valid systems on the network.
- Flooded frames go to every port on the switch, thus allowing the attacker to capture and re them.
- MAC cloning is when the attacker copies the MAC address of another system and uses network communication.
- This could be used to bypass access control lists, where only traffic from specific MAC a allowed on the network.

The hacker alters DNS entries to re
wrong on fake websites.
① changing records on a DNS server
② Modify the DNS cache
③ Editing the local hosts file on a

DNS Poisoning

- Poisoning with computers is the concept that someone goes into an enviro incorrect settings into it in order to disrupt the environment.
- DNS poisoning is when the hacker compromises a DNS server and poiso DNS names point to incorrect IP addresses.
- Often, the hacker will modify the DNS records to point to the hacker's sy DNS name to the hacker's system.
- DNS poisoning is also the altering of the DNS cache that is located on The DNS cache stores the names of web sites already visited by empl sites.
- The cache is on your DNS server so that when another employee su already has the IP address of that site and does not need to forward
- The DNS server in your local office simply sends the IP address tha client.
- It is possible for the hacker to poison the DNS cache so that your
- Another popular technique for hackers to lead you to the wrong w

Domain Hijacking

- Domain hijacking is a type of attack that involves the hacker taking over a dom
  original registrant.
- The hacker may hijack the domain by using social engineering techniques to
  domain name and then switch ownership, or the hacker could exploit a vuln
  that host the domain name to gain unauthorized access to the domain regis

Privilege Escalation

- Privilege escalation is a popular attack that involves someone who system being able to elevate their privileges to gain administrative
- Privilege escalation normally occurs due to a vulnerability within within the operating system itself.
- It is important to keep the system and application patched in or vulnerabilities, which will help prevent privilege escalation.

Port Scanning Attack

- Another popular network attack is known as port scanning or a port
- With a port scanning attack, the hacker runs software on the netwo system, which indicates to the hacker what ports are open.
- Once the hacker finds out what ports are open, they can then try t system.
- A number of different types of port scans can be used; the followir
- **TCP connect scan** With a TCP connect scan, the hacker perform port on the system. The concept is that if the hacker can do a thr port must be open.
- **SYN scan (half-open scan)** The TCP connect scan is easily de packets sent between the hacker and the system being scanne With the SYN scan, the hacker sends a SYN message but does three-way handshake after receiving an ACK/SYN from the vict detection by creating less traffic. This scan is also known as a l

PASSWORD ATTACK

Reasons of Vulnerability Assessment

- Here are a few reasons why organizations might perform or have a vulnerability assessment performed:
  - To find and identify vulnerabilities using scanners specifically designed for this type of testing
  - To discover and identify vulnerabilities that may be difficult or unique to t organization
  - To find and identify vulnerabilities resulting from a misconfiguration
  - To find and identify permissive security settings and whether least privilege place
  - If a vulnerability is discovered, to determine the viability of the attack vector
  - To assess potential business and operational impact
  - To test in-place security tools, operations, and controls to determine the the organization to detect, defend, and counterattack

Types of Vulnerability Assessment

- **Active assessment:**
  - This refers to any task that is active, including th interrogation systems and examining the respon
  - For the security team, this might mean runnin and reviewing the results.
  - For others, such as a pentester, it might inclu targeted scripts or programs.

Passive assessment:

- Here, the team gathers information from the network in **capture**.
- They then analyze what was captured to discover vulnerab
- Because applications tend to be chatty on the network, t *things* such as hostnames, applications, devices, and even
- *During* this type of assessment, no targeting of hosts *unless* specifically outlined.
- *Passive* assessment usually involves packet sniffing to *running* services, open ports, misconfigurations, and *being* passed over the network.

Third Party Risks

There are risks to working with third-party companies as well. Actions performed by third-party companies you work with may leave your company vulnerable. The following are a few examples:

- **Vendor management** How a vendor manages their products may present vulnerabilities to your environment that uses that vendor's products. For example, how does a vendor's system integrate into your network? Does it use secure protocols? Does it need an account on the network? If a product is older, it is possible that the vendor no longer supports the product. A product no longer supported does not have patches created anymore, which means you could be open to zero-day attacks.

- **Supply chain** If you are working with a supplier that does not follow security best practices, you could receive a product from the supplier that has been compromised that you then connect to your network.

- **Outsourced code development** Unsecure application code is a big cause for vulnerabilities on a system. Outsourcing the development of a component to be used by your applications could cause them to be unsecure if the outsourced company does not follow secure coding practices.

- **Data storage** You may be storing data with a third-party company—maybe as an alternate site to store data backups. Verify the third-party company is securing the system that holds your data, but also take steps of your own to ensure the data is encrypted and that only your company can decrypt the data.

Improper or Weak Patch Management

Lack of a patching strategy is one of the biggest reasons for vulnerable systems because a patch has the security fixes for known vulnerabilities.

- Be sure to apply patches to the following on a regular basis:

Firmware Apply updates to the firmware on devices such as servers, routers, switches, and any other hardware device that may exist within your company.

Operating system (OS) Patch the operating system on a regular basis and look to patch management software to automate the deployment of patches.

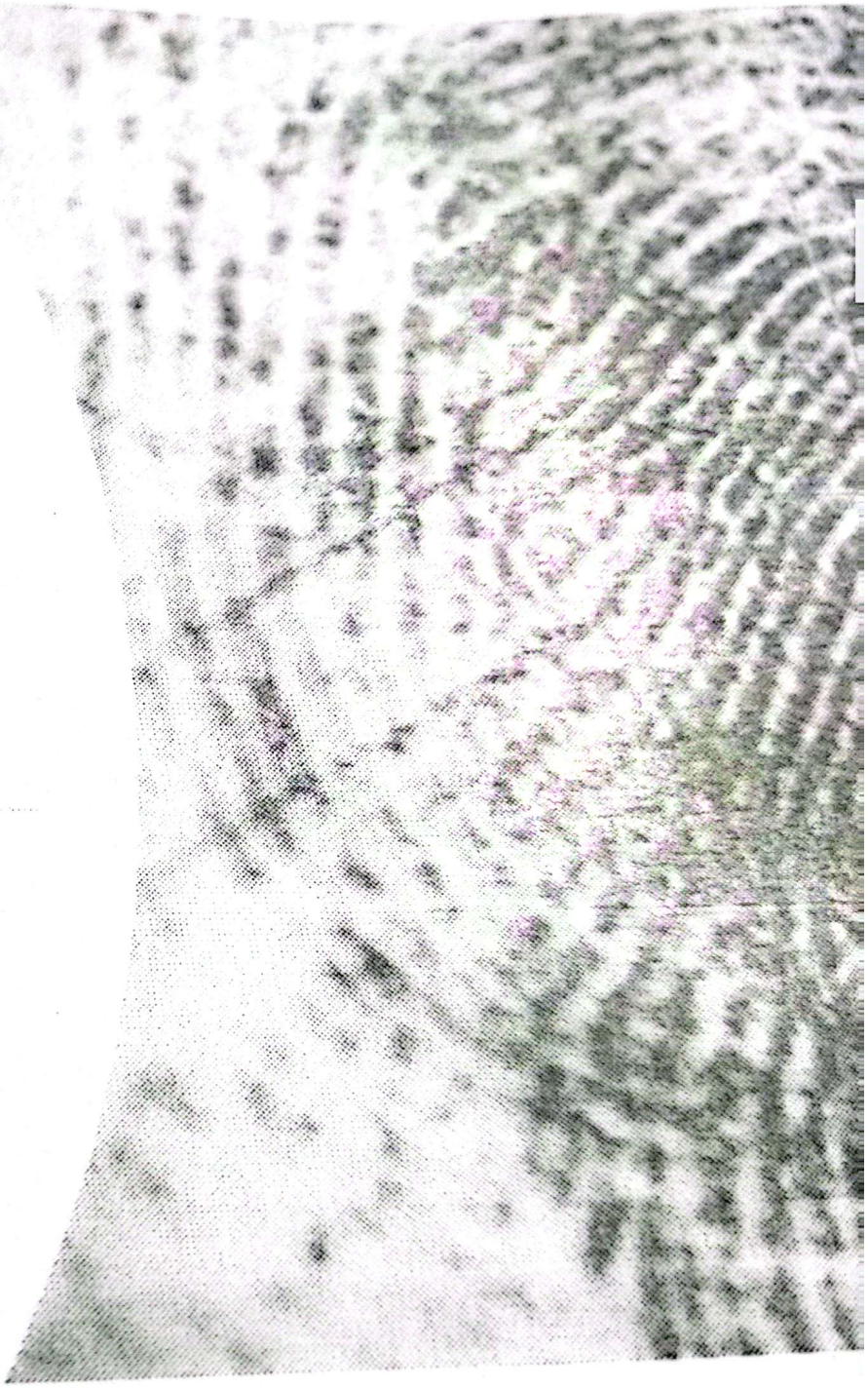
Applications Ensure that applications are patched as well. A vulnerability in an application may cause the entire system to be vulnerable to an attack.

- **Legacy Platforms**
- Legacy systems are something you should watch for on the network, as many legacy systems no longer have vendor support, which means they are most likely not patched anymore. Also, a legacy system may be usir older protocols that are unsecure. If you are using legacy systems on your network, look to placing them their own network segment to help reduce the chances that the systems are attacked.

Understanding the impact of vulnerabilities

- A company that does not learn how to manage the vulnerabilities that exist on a system could face disastrous results.
- The following are potential impacts to a business that does not reduce the vulnerabilities that exist in their products:
  - **Data loss** A vulnerability on the system may result in you losing access to data. For example, an attacker could exploit the vulnerability and delete the data or encrypt it with ransomware.
  - **Data breaches** A data breach occurs when an unauthorized person gets access to confidential data. A data breach is also known as a *data leak* or *data spill*. The data breach may include information such as health records, financial data, and intellectual property. The impact of a data breach could be disastrous to a company due to the cost of investigating and recovering from the data breach, but the company could also see damage to its reputation
  - **Data exfiltration** Data exfiltration occurs when someone transfers data from a computer or network without permission to do so. Examples of sensitive data that an attacker may want to transfer from a system are financial data (such as credit card numbers), personally identifiable information (PII), and usernames and passwords. To prevent data exfiltration, you can disable USB ports so that portable storage such as USB flash drives and USB external drives cannot be connected to a system, or you can use data loss prevention (DLP) features to block sensitive data from being copied or e-mailed outside the organization.

Identifying Physical Threats



Vulnerability Management Life Cycle

Overview

- Vulnerability management life cycle starts by defining the current security policies and procedures.
- If a company has already set up an information security mar important to establish any risks that may be associated with current security procedures and what may have been overloo
- Try to see what the organization looks like from an outsider's from an insider's standpoint.
- Work with management to set goals with start dates and en
- Determine which systems to begin with, set up testing s writing form, and keep management informed on the pro how you will do it, and the timing for each phase of the pro

Vulnerability Assessment Process

Overview

- A vulnerability assessment is one of the most imp
enterprise's vulnerability management lifecycle h
fix security vulnerabilities you know nothing abou
- Through the vulnerability assessment process,
are scanned and newly discovered vulnerabil

SES OF
RISK
ALYSIS

Risk Analysis Process Phase	Description
1. Asset identification	Identifying the assets that require protection and determining the value of the assets.
2. Vulnerability identification	Identifying vulnerabilities so the analyst can confirm where asset protection problems exist. Locating weaknesses exposes the critical areas that are most susceptible to vulnerabilities. Vulnerability scanning is a method used to determine weaknesses in systems. This method can, however, produce false positives, which tend to initiate reasons for concern, even when there are no actual issues or weaknesses in the system.
3. Threat assessment	Once vulnerabilities are understood, the threats that may take advantage of or exploit those vulnerabilities are determined.
4. Probability quantification	Quantifying the likelihood or probability that threats will exploit vulnerabilities.
5. Impact analysis	Once the probabilities are determined, the impact of these potential threats needs to be evaluated. This can include either the impact of recovering from the damage, or the impact of implementing possible preventive measures.
	Note: Impact analysis is covered in depth in the next topic.
6. Countermeasures determination	Determining and developing countermeasures to eliminate or reduce risks. The countermeasures must be economically sound and provide the expected level of protection. In other words, the countermeasures must not cost more than the expected loss caused by threats that exploit vulnerabilities.

Change Management

- After testing your systems with either a vulnerability scan or a penetration test, need to make changes to the configuration of the systems in order to make the
- When making changes to the system configuration, be sure to follow the chan your organization has set out.
- This process typically involves applying the change to test systems first, ba before making the change, applying the change, and then verifying the pro after the change.
- The key to change management is the documentation.
- For example, when planning for changes, you should document the desir the changes do not go as planned (this is called the rollback plan), and th change operation.

change management is the pr

t

Identify Mitigation Technique

- Once you have identified the threats and prioritized them, yo solutions to focus on, or at least how to reduce the risk of th
- This is known as *mitigating* the threat.
- Mitigating the threat typically involves spending money on implements a security control to protect the asset from thr
- You can implement fault-tolerant technologies, firewalls, control systems, to name a few.

→ reducing the chance of a th

Risk with Cloud Computing and Third Parties(Cont..)

The following are some points you should take into consideration when integrating systems and data with cloud services and third-party companies:

- **On-boarding/off-boarding business partners:** In cloud computing, **onboarding** and **offboarding** business partners refer to the processes of integrating and removing external entities—such as vendors, suppliers, or collaborators—within a cloud-based ecosystem.
- On-boarding involves setting up access, permissions, and resources for new partners to collaborate within a cloud environment. It typically includes:
  - **Identity & Access Management (IAM):** Granting appropriate permissions while ensuring security.
  - **Integration with Cloud Services:** Connecting their systems to shared cloud resources.
  - **Compliance & Security Checks:** Ensuring adherence to data protection policies.
- Off-boarding business partner: When a partnership ends, offboarding ensures secure removal of access and data. This includes:
  - **Revoking Access:** Disabling credentials and permissions.
  - **Data Migration or Deletion:** Ensuring sensitive information is handled properly.
  - **Audit & Compliance Review:** Confirming that security protocols were followed.

onboarding → Give access carefully with p
checks.

offboarding → Remove access and delete sh
data when partnership ends.

RISK MITIGATION STRATEGIES

The following are approaches you can take to dealing with threats:

- **Mitigate the risk (mitigation)** The first way to deal with the risk is by mitigating it. Mitigation implementing a security control that protects the asset from the threat. For example, to pro drive failure on the web server, you could purchase a RAID solution.
- **Accept the risk (acceptance)** Another way to handle the risk is to accept it. Accepting the you do not implement any solution to protect against the threat because you are satisfie of the threat occurring and the impact of the threat do not warrant the cost of impleme control.
- **Transfer the risk (transference)** You can also look at transferring the risk, which means somebody else's problem! For example, you may get insurance that helps you recover incident. It should be noted that for the exam, remember that an example of transfe cybersecurity insurance.

→ Let someone else handle the risk

→ Buy cybersecurity insurance so y

hack.

GDPR Details

- - **Strict Consent Requirements:** Organizations must obtain clear, informed, and freely given consent before processing personal data. Consent must be explicit for sensitive data and can be withdrawn at any time
- - **Right to Be Forgotten:** Also known as the right to erasure, this allows individuals to request the deletion of their personal data when it is no longer necessary, consent is withdrawn, or data has been unlawfully processed
- - **Heavy Fines for Violations:** GDPR imposes significant penalties for non-compliance. Fines can reach €20 million or 4% of global annual revenue, depending on the severity of the violation.
- Under the **California Consumer Privacy Act (CCPA)**, the **Right to Opt-Out of Data Sales** allows consumers to **prevent businesses from selling their personal information** to third parties. This means that if a company is selling your data, you have the right to request that they stop. Businesses must provide a **clear and accessible way** for consumers to opt out, often through a **"Do Not Sell My Personal Information"** link on their website.
- Additionally, the **California Privacy Rights Act (CPRA)**, which amended the CCPA, expanded this right to include **sharing personal data for targeted advertising**. Businesses must honor opt-out requests for **at least 12 months** before asking consumers for consent again.
- Under the **California Consumer Privacy Act (CCPA)**, businesses must **disclose their data collection practices** to consumers. This means they must provide clear information about:
- **What personal data** they collect.
- **Why** they collect it.
- **How** they use it.
- **Who** they share or sell it to.
- This disclosure is typically provided in a **Privacy Policy** or a **Notice at Collection**, which must be **accessible easy to understand**.

Negative side of DSA

Overly Broad Provisions: (unclean Rules)

The DSA contains **vaguely worded sections** that can be interpreted in ways that go beyond just protecting data and cybersecurity. For example:

- **Section 21**: Criminalizes "spreading negative propaganda" against the government, which can include **criticism o media**.
- **Section 25**: Punishes "hurting religious sentiments," which can be **misused to target dissenters**.
- **Section 29**: Penalizes "defamation," which can be used to **silence journalists and activists**.
- Because these terms are **not clearly defined**, authorities can **arbitrarily apply** the law against journalists, act opposition voices—**not just actual cybercriminals**.

Used to Suppress Free Speech (Limits Free Speech)

- **Journalists & Activists Arrested**: Many reporters, bloggers, and critics have been **arrested under the DSA** opinions online.
- **Self-Censorship**: Fear of prosecution has led to **reduced criticism** of the government in media and social
- **Misuse for Political Purposes**: Critics argue the law is used more to **silence opposition** than to combat

→ Fear of Speaking out: People are afraid to c government, even when its fair criticism.

Section 54

Key Provisions of Section 54

1.Criminalizes Unauthorized Access

1. It is illegal to access a **computer, network, or digital system** without pe
2. Example: Hacking into someone's email, bank account, or a company'

2.Punishes Data Theft & Tampering

1. Stealing, copying, or altering data without authorization is a crime.
2. Example: An employee leaking confidential company files.

3.Penalties

1. **Imprisonment**: Up to **7 years** (or **14 years** if done for fraudulent r
2. **Fines**: Up to **৳10 lakh (1 million BDT)**.

Challenges in Data Protection in Bangladesh

- ☑ No unified data protection law – Fragmented regulations.
- ☑ Weak enforcement – Lack of a dedicated Data Protection Authority (DPA).
- ☑ Cross-border data flows – No clear rules on international data transfers.
- ☑ Corporate compliance – Many companies lack proper data governance policies.

Recommendations for Businesses

✔ Follow best practices (e.g., encryption, consent-based data collection).

Types of Intellectual Property law

A. Copyright Original works like books, songs, f

- **Protects:** Original literary, artistic, musical, and dramatic works (e.g., books films, software).
- **Rights Granted:**
  - Reproduction (Copying)
  - Distribution (Selling / Shaning)
  - Public performance/display
  - Derivative works (adaptations)
- **Duration:**
  - **Life of the author + 70 years** (most countries)
  - **Corporate works:** 95 years from publication (e.g., Disney's Mickey Mouse
- **Examples:**
  - J.K. Rowling's *Harry Potter* books
  - The code of Microsoft Windows

ELECTRONIC TRANSACTION

- An **electronic transaction** is the process of exchanging goods services, or information through electronic means — typically the internet or digital networks.

Key Characteristics

- **Paperless**: No need for physical documents
- **Instant**: Real-time processing and confirmation
- **Automated**: Involves minimal human intervention
- **Secure**: Requires data protection, authentication, and measures

Freedom of Speech & Content Regulation

What is Freedom of Speech

Freedom of speech is the **right to express your opinions, ideas, and information fre** speech, writing, media, or the internet — **without censorship or punishment** by th government.

- It is a **fundamental human right** in many democracies (e.g., protected under Artic Indian Constitution or the First Amendment in the U.S.).
- It includes:
  - Expressing political views
  - Criticizing public authorities
  - Sharing opinions on social media
- Does not include:
  - Hate speech
  - Incitement to violence
  - Defamation (মানহানি / অপবাদ)
  - Child pornography

Jurisdiction and Cross-Border Issues

Jurisdiction refers to the **legal authority of a court or government** to hear and decide cases.

In the physical world, jurisdiction is based on **geography**:

- Where the crime occurred
- Where the parties are located

- However, in the **digital world**, jurisdiction becomes complex due t **borderless nature of the internet**.
- Jurisdiction in cyber law refers to a court's authority to hear and d cases involving online conduct.
- In cyberspace, where activities cross multiple national boundar instantly, traditional notions of **territorial jurisdiction** are chall This creates **cross-border legal conflicts** and enforcement di

more than one country.

Cross Border Enforcement Issues

- Cross-border enforcement issues refer to the legal and practical difficulties that arise when a cybercrime or digital dispute involv more than one country — making it hard to investigate, prosecu or enforce laws across national boundaries
- Why are these cross-border issues arises:
  - The **internet is global**, but **laws are national**. So when:
  - A hacker in **Country A** attacks a server in **Country B** affecting a use **Country C**,
  - **Which country has legal authority (jurisdiction)?**
  - And **how do they cooperate** to investigate or punish the attacker
  - That's where cross-border enforcement issues come in.

Why we need to use Computer Forensic

- **Crime investigation:**
  - It plays a crucial role in solving cybercrimes like hacking, identity theft, and online fraud by tracing digital footprints and recovering deleted or hidden data.
- **Legal evidence:**
  - Courts rely on digital evidence from phones, computers, and networks. Forensics ensures this evidence is collected and presented properly.
- **Corporate protection:**
  - Businesses use it to investigate data breaches, insider threats, or intellectual proper theft, helping them respond quickly and prevent future incidents.
- **Data recovery:**
  - It can retrieve lost or corrupted data, which is vital in both criminal cases and accide data loss scenarios.
- **National security:**
  - Governments use it to track cyberterrorism, espionage, and other threats that critical infrastructure.

Civil vs. Criminal Investigation

- In **digital forensics**, investigations can generally be categorized into two major types: **civil investigations** and **criminal (or digital)** investigations.
- **Civil Investigation:**
  - A **civil investigation** in digital forensics deals with disputes between individuals, organizations, or entities, usually involving private rights.
  - These cases do **not involve criminal charges**, but rather involve **lawsuits** or **civil litigation**.
- **Purpose:**
  To collect, analyze, and present digital evidence in **non-criminal legal matters**, such as:
  - Breach of contract
  - Intellectual property theft
  - Employment disputes (e.g., harassment or wrongful termination)
  - Data breaches affecting business reputation or customer rights
  - Family law cases (e.g., divorce, custody disputes involving digital evidence)
- **Example:**
  A company suspects a former employee of leaking confidential data to a competitor. A civil digital investigation be launched to recover deleted files or trace email communications.
- **Handled by:**
  Usually conducted by **private digital forensic investigators** or **corporate forensic teams**, and used in **civil**

Administrative Investigation

In the cyber world, an administrative investigation refers to a non-criminal inquiry—often internal to an organization—focused on identifying **policy violations, misconduct**, or **misuse of digital systems** by employees or affiliates.

Purpose of Administrative Investigations:

- To enforce internal policies (e.g., acceptable use of IT resources)
- To investigate suspicious behavior like data leaks, harassment, or unauthorized access
- To support HR of compliance actions such as disciplinary measures or termination

Common Cyber-Related Scenarios

- Employee data theft or unauthorized file transfers
- Viewing or sharing inappropriate content on company systems
- Bypassing security protocols or installing unauthorized software
- Misuse of email or communication tools for harassment or fraud

Why Digital Evidence is important

- **Authentication:** Proves identity or activity (e.g., who sent an email).
- **Timeline:** Establishes when something happened (timestam
- **Corroboration:** Supports or contradicts witness testimony.
- **Linking suspects:** Connects people to devices, files, or ev
- **Reconstruction:** Helps understand how a crime or event occurred.

Why to collect information from different souces

- Each source offers a different lens into user behavior, intent, and timeline. For example:
- - **A deleted file** on a **USB drive** might be recovered to prove IP theft.
- - **Chat logs** from a **gaming console** could reveal grooming or harassment.
- - **Cloud backups** might contain incriminating documents long after deletion from a local device.

Scientific Working Group on Digital Evidence

- SWGDE is a U.S.-based organization that brings together experts from **law enforcement, academia, private industry, and government** to develop **guidelines, standards, and best practices** for handling digital and multimedia evidence.
- **Core Objectives**
  - Promote consistency and quality in digital forensic practices
  - Foster communication and cooperation across forensic disciplines
  - Develop consensus-based documents to guide practitioners
  - Support the creation of national and international standards (e.g., ASTM E2763 for computer forensics)

Scenario 1: [Scenario দিয়ে Forensic Investigation দিয়ে]

you're investigating a suspect system to determine whether Dropbox was installed by an employee and possibly used for data exfiltration. The OS (Windows, macOS, Linux, etc.) influences where and how Dropbox leaves its traces (artifacts).

So, your hypothesis might be:

"Dropbox was installed and used on the suspect's device to transfer confidential files."

But that's too vague unless it's OS-aware.

So, during hypothesis formulation, you should refine your hypothesis like this:

"Dropbox was installed on a Windows 10 system and used on June 12th to sync confidential documents."

Why this matters:

- Each OS stores Dropbox artifacts in different locations with different formats.
- You'll need to frame experiments that match the OS environment and use tools suited to extract those specific traces.

🧪 **In practice:**

- If you formulate a hypothesis without considering the OS, you risk missing or misinterpreting artifacts.
- A solid forensic hypothesis should specify conditions like the operating system, expected file paths, and timeframe of activity—so your testing is targeted and scientifically valid.

Steps of Forensic Investigation Process

- **Step One:** During identification, the investigator (or investigating team) must identify what evidence is present on the device, where it is stored, and what format it is stored in.
- **Step Two:** Preservation focuses on isolating the data, securing it, and preserving it, while creating a copy, or image, that can be analyzed and investigated. This process, also known as "imaging" a device, preserves the actual evidence in its original form, so it will be admissible in court.
- **Step Three**: During analysis, the forensic investigator collects fragments of data (bits or pieces of digital evidence) and creates a holistic narrative of what happened during the crime (or other matter being investigated).
- **Step Four:** During Documentation, the investigator prepares a record of the data to be presented in court (or in whatever other venue that the investigation is being resolved).
- **Step Five:** In presentation, the investigator uses the documentation to explain the conclusions they have drawn about the event in question in a compelling manner.

6 Steps of an Incident Response Plan

Step 1: Preparation

- Preparation is the most crucial phase in the incident response plan, as it determines how well an organization will be able to respond in the event of an attack.
- It requires several key elements to have been implemented to enable the organization to handle an incident:

1. Policy: Provides a written set of principles, rules, or practices within an organization and is a crucial action that offers guidance as to whether an incident has occurred.

2. Response plan/strategy: The response plan needs to include the prioritization of incidents based on organizational impact, from minor incidents like a single workstation failing to a medium risk like a server going down, and high-risk issues like data being stolen from a department. This can help build the case for management buy-in and gain resources required to handle an incident effectively.

3. Communication: Having a communication plan is vital to ensuring the entire CSIRT knows who to contact, when, and why. Not having a plan will likely delay the response time and result in the wrong people being contacted. Thers should be escalation paths that direct issues to appropriate personnel quickly to enable swift decision-making and resolution

Step 6: Lessons Learned

- It is vital for organizations to review their incident response and adapt their approach for future attacks.
- All documentation that was not completed during the incident now needs to be compiled, along with additional information that may benefit future incidents.
- The report must provide a play-by-play review of what happened throughout the entire incident.
- This will help the CSIRT improve its performance, learn from the events that occurred, and provide reference materials for future events.
- The report can also be used as training material for new employees and to guide any drills that teams hold.