2023

MCA 205B: CYBER SECURITY

UNIT III

PREPARED BY S NOORTAJ

KMMIPS:
TIRUPATHI
09-Aug-23

Overview Of Cyber Security

- The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity.
- We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data.
- And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.

Some other definitions of cybersecurity are:

- "Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."
- "Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

CIA TRIAD

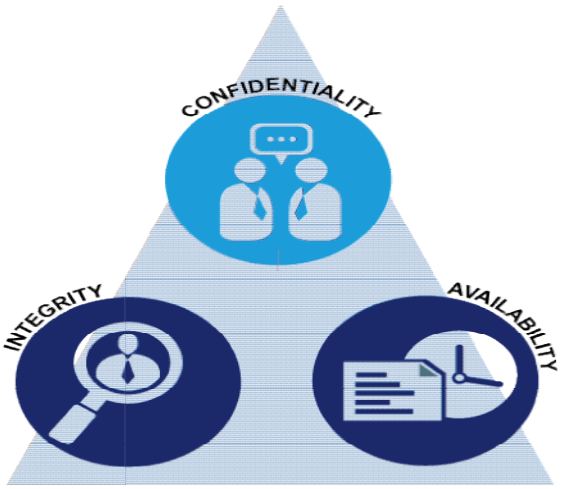
When talking about network security, the CIA triad is one of the most important model which is designed to guide policies for information security within an organization.

CIA stands for :

Confidentiality

Integrity

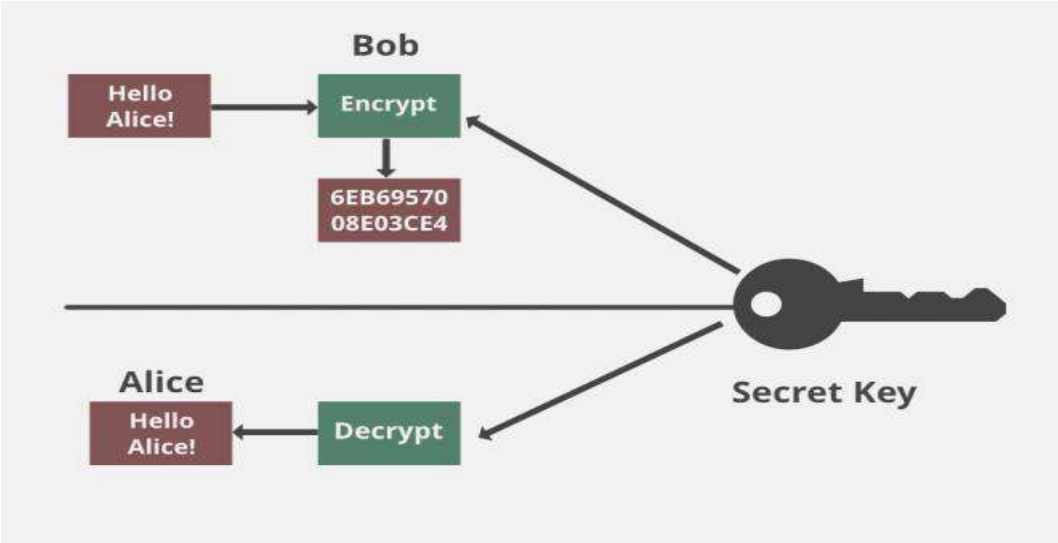
Availability



These are the objectives which should be kept in mind while securing a network.

Confidentiality :

- Confidentiality means that only the authorized individuals/systems can view sensitive or classified information.
- The data being sent over the network should not be accessed by unauthorized individuals.
- The attacker may try to capture the data using different tools available on the Internet and gain access to your information.
- A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it.
- Encryption standards include AES(Advanced Encryption Standard) and DES (Data Encryption Standard).
- Another way to protect your data is through a VPN tunnel.
- VPN stands for Virtual Private Network and helps the data to move securely over the network.



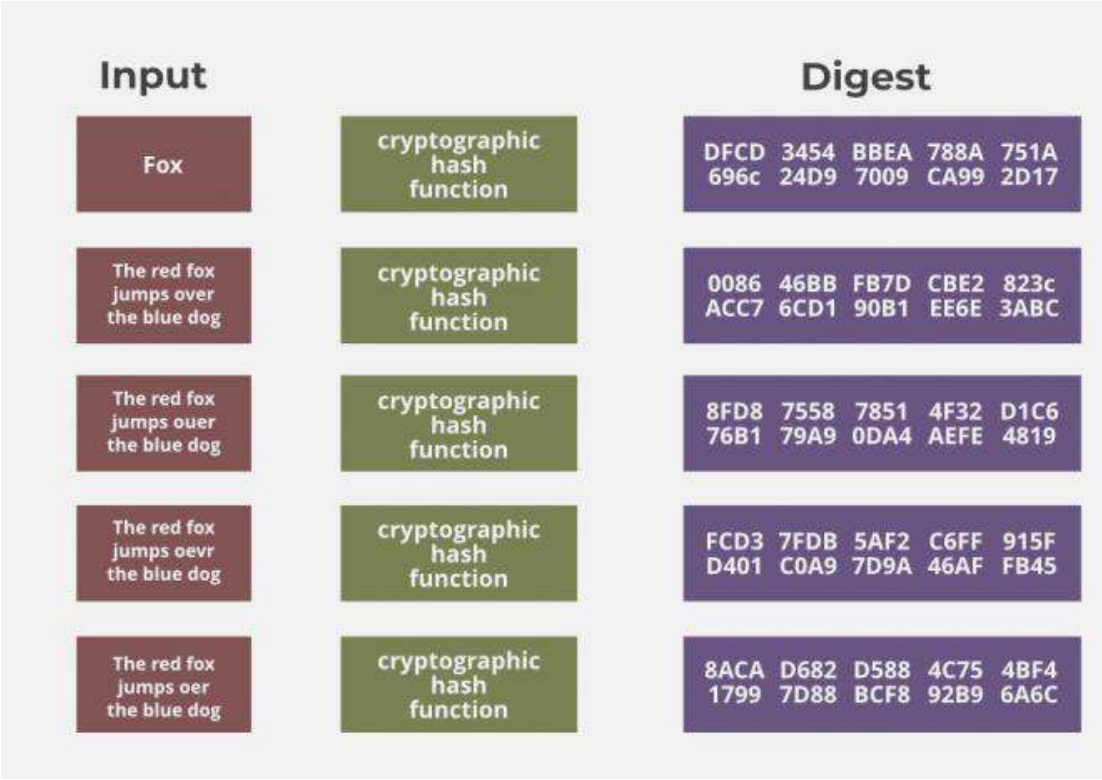
Integrity :

- The next thing to talk about is integrity.
- Well, the idea here is making sure that data has not been modified. Corruption of data is a failure to maintain data integrity.
- To check if our data has been modified or not, we make use of a hash function.

We have two common types :

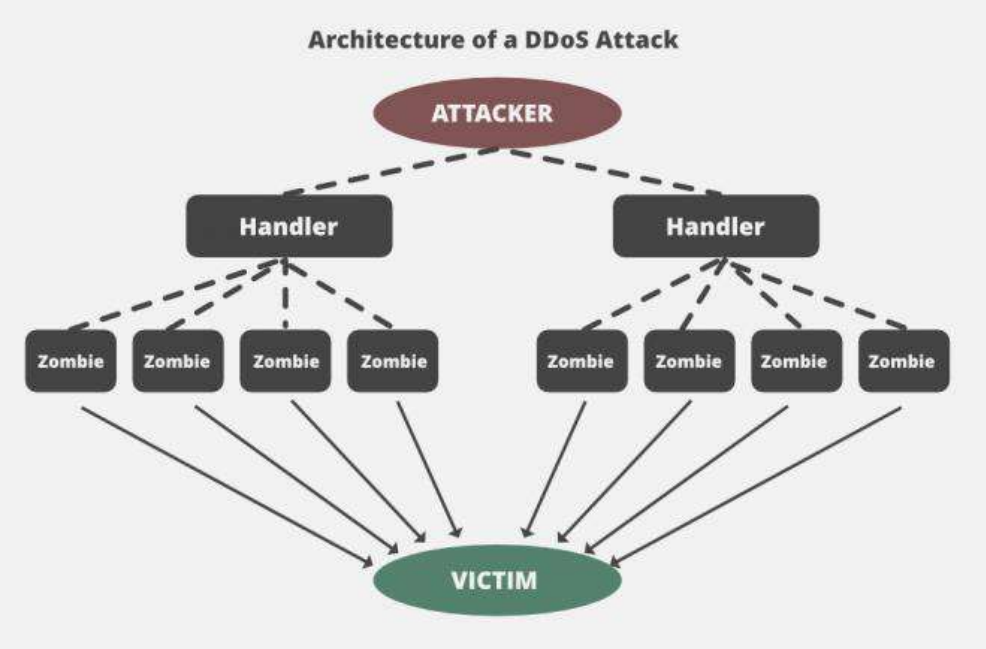
- SHA (Secure Hash Algorithm) and MD5(Message Direct 5).
- Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1.
- There are also other SHA methods that we could use like SHA-0, SHA-2, SHA-3.

- Let's assume Host 'A' wants to send data to Host 'B' maintaining integrity.
- A hash function will run over the data and produce an arbitrary hash value H1 which is then attached to the data.
- When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value H2.
- Now, if H1 = H2, this means that data's integrity has been maintained and the contents were not modified.



Availability :

- This means that the network should be readily available to its users.
- This applies to systems and to data.
- To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over and prevent bottleneck in a network.
- Attacks such as DoS or DDoS may render a network unavailable as the resources of the network gets exhausted.
- The impact may be significant to the companies and users who rely on the network as a business tool.
- Thus, proper measures should be taken to prevent such attacks.



NON-REPUDIATION

- Nonrepudiation is the assurance that someone cannot deny something.
- Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- To repudiate means to deny.
- For many years, authorities have sought to make repudiation impossible in some situations.
- You might send registered mail, for example, so the recipient cannot deny that a letter was delivered.
- Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.
- On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.
- Since no security technology is absolutely fool-proof, some experts warn that a digital signature alone may not always guarantee nonrepudiation.
- It is suggested that multiple approaches be used, such as capturing unique biometric information and other data about the sender or signer that collectively would be difficult to repudiate.
- Email nonrepudiation involves methods such as email tracking that are designed to ensure that the sender cannot deny having sent a

Access Management System

- An access management system can be used to manage and monitor user access permissions and access rights to files, systems, and services to help protect organizations from data loss and security breaches.
- The act of access management is all about controlling user access, which includes tracking and changing authorizations as needed. During normal business use, employees might access, change, or delete data.
- This isn't a problem if this use is accurate and appropriate, however, when not monitored properly, it's all too easy for users to make mistakes or even take malicious actions.
- Access management seeks to limit the information users can view or change to minimize the chances of improper activity.
- Limiting user access in an effective manner can be a complicated endeavor, especially since limiting access too severely can compromise business productivity.
- It can also get confusing fast. For instance, individual users may be allowed to edit File X but only view File Y. Or, a certain role-based group of users may need read-only permissions for certain types of data and no access at all for other types of data.
- Every time a user—or file—is added to the system, someone must consider—and apply—the proper access limitations, whether through manual or automatic means.
- Security access management systems are designed to automate, visualize, and streamline the process of assigning and managing the many complicated access settings outlined above.
- It's worth noting because you must manage user access consistently across your IT infrastructure, access management systems must be able to integrate with other systems, including:

Active Directory:

- A directory service for Windows® networks to both authenticate and authorize end users, ensuring security policies are followed across the network.
- Active Directory includes Group Policy, which helps define advanced permissions settings.

OneDrive:

- A Microsoft-hosted cloud storage service used to host business files. Allows for syncing and sharing files across users.

SharePoint:

- A web platform designed to function primarily as a system for collaborative business document management and storage.
- By adopting a security access management system integrated with your company's file systems or access control environments, you'll be better prepared to ensure correct security credentials are assigned across all users.
- But even with these systems in place, admins often need a mechanism with which to verify the user settings are correct and the user activity hasn't caused a data breach.

- In many cases, admins must provide reports to auditors to show their data security policies are compliant with industry regulations.
- To help you fulfill this requirement, access management systems allow you to track user activity and perform automated reporting.

OWASP Security Framework

The Open Web Application Security Project (OWASP) is a non-profit organization founded in 2001, with the goal of helping website owners and security experts protect web applications from cyber attacks.

- The OWASP Security Knowledge Framework is an open source web application that explains secure coding principles in multiple programming languages.
- The goal of OWASP-SKF is to help you learn and integrate security by design in your software development and build applications that are secure by design.
- It is a non profitable organization application.
- The main goal is to improve software security and make secure from hackers.

Core principles:

- It provides necessary tools , materials, testing technologies, methodologies, video courses, test courses for security testing providing free.
- companies/ individuals are using these materials for learning security testing or on their own application security testing can be conduct and security the application.
- OWASP community strength is high. Because worldwide followers.
- In every organization after their client ask for security testing (OWSAP all vulnerabilities clear /not).
- OWASP-SKF does this through manageable software development projects with checklists (using OWASP-ASVS/OWASP-MASVS or custom security checklists) and labs to practice security verification (using SKF-Labs, OWASP Juice-shop, and best practice code examples from SKF and the OWASP-Cheatsheets).

The OWASP Top 10 2017 includes the following:

1. Injection.

- A code injection occurs when invalid data is sent by an attacker into a web application.
- The attacker's intent in doing so is to make the application do something it was not designed to do.

Example: SQL injection is one of the most common injection flaws found in applications. SQL injection flaws can be caused by use of untrusted data by an application when constructing a vulnerable SQL call.

Solution: Source code review is the best way to prevent injection attacks. Including SAST and DAST tools in your CI/CD pipeline helps to identify injection flaws that have just been introduced. This allows you to identify and mitigate them before production employment.

2. Broken Authentication:

- Certain applications are often improperly implemented. Specifically, functions related to authentication and session management, when implemented incorrectly, allow attackers to compromise passwords, keywords, and sessions.
- This can lead to stolen user identity and more.

Example: A web application allows the use of weak or well-known passwords (i.e. “password1”).

Solution: Multi-factor authentication can help reduce the risk of compromised accounts. Automated static analysis is highly useful in finding such flaws while manual static analysis can add strength in evaluating custom authentication schemes. Synopsys’ Coverity SAST solution includes a checker that specifically identifies broken authentication vulnerabilities.

3. Sensitive Data Exposure:

- Sensitive data exposure is when important stored or transmitted data (such as social security numbers) is compromised.

Example: Financial institutions that fail to adequately protect their sensitive data can be easy targets for credit card fraud and identity theft.

Solution: SAST tools such as Coverity and SCA tools such as Black Duck Binary Analysis include features and checkers that identify security vulnerabilities that can result in sensitive data exposure.

4. XML External Entities (XXE):

- Attackers are able to take advantage of web applications that use vulnerable component processing XML’s.
- Attackers are able to upload XML or include hostile commands or content within an XML document.

Example: An application allows untrusted sources to perform XML upload.

Solution: Static application security testing (SAST) is very helpful at detecting XXE in source code. SAST helps inspect both application configuration and dependencies.

5. Broken Access Control:

- Broken access control is when an attacker is able to get access to user accounts.
- The attacker is able to operate as the user or as an administrator in the system.

Example: An application allows a primary key to be changed. When the key is changed to another user's record, that user's account can be viewed or modified.

Solution: It is critical to use penetration testing in order to detect unintended access-controls. Changes in architecture and design may be warranted to create trust boundaries for data access [iii].

6. Security Misconfiguration:

- Security misconfigurations are when design or configuration weaknesses result from a configuration error or shortcoming.

Example: A default account and its original password are still enabled, making the system vulnerable to exploit.

Solution: Solutions like Synopsys' Coverity SAST include a checker that identifies information exposure available through an error message.

7. Cross-Site Scripting (XSS):

- XSS attacks occur when an application includes untrusted data on a webpage. Attackers inject client-side scripts into this webpage.

Example: Untrusted data in an application allow for an attacker to 'steal a user session' and gain access to the system.

Solution: SAST solutions well versed in data flow analysis can be a great tool to help find these critical defects and suggest remedies. The OWASP website also provides a cheat sheet to best practices to eliminate such defects from your code. For OWASP Top 10 categories like XSS, that also have a Common Weakness Enumerator (CWE), Black Duck will alert teams that this is the weakness that lead to the vulnerability, enabling them to better understand the vulnerability and prioritize their remediation efforts .

8. Insecure Deserialization:

- Insecure Deserialization is a vulnerability where deserialization flaws allow an attacker to remotely execute code in the system.

Example: An application is vulnerable because it deserializes hostile objects that were supplied by an attacker.

Solution: Application security tools help detect deserialization flaws and Penetration testing can be used to validate the problem.

9. Using Components With Known Vulnerabilities:

- This vulnerability's title states its nature;

- it describes when applications are built and run using components that contain known vulnerabilities.

Example: Due to the volume of components used in development, a development team may not even know or understand the components used in their application. This can result in them being out-of-date and therefore vulnerable to attack.

Solution: Software composition analysis (SCA) tools like Black Duck can be used alongside static analysis to identify and detect outdated and insecure components in your application [ii].

10. Insufficient Logging And Monitoring.

- Logging and monitoring are activities that should be performed to a website frequently, to guarantee it is secure.
- Failure to adequately log and monitor a site leaves it vulnerable to more severe compromising activities.

Example: Events that can be audited, like logins, failed logins, and other important activities, are not logged, leading to a vulnerable application.

Solution: After performing Penetration testing, developers can study the test logs to identify possible shortcomings and vulnerabilities. SAST solutions can also help identify unlogged security exceptions [ii].

What is Incident Response?

Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the “incident”). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

Organizations should, at minimum, have a clear incident response plan in place. This plan should define what constitutes an incident for the company and provide a clear, guided process to be followed when an incident occurs. Additionally, it’s advisable to specify the teams, employees, or leaders responsible for both managing the overall incident response initiative and those tasked with taking each action specified in the incident response plan.

Who Handles Incident Responses?

Typically, incident response is conducted by an organization’s computer incident response team (CIRT), also known as a cyber incident response team. CIRTs usually are comprised of security and general IT staff, along with members of the legal, human resources, and public relations departments. As Gartner describes, a CIRT is a group that “is responsible for responding to security breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks. In addition to

technical specialists capable of dealing with specific threats, it should include experts who can guide enterprise executives on appropriate communication in the wake of such incidents."

Six Steps for Effective Incident Response

The SANS Institute provides six steps for effective incident response:

1. **Preparation** - The most important phase of incident response is preparing for an inevitable security breach. Preparation helps organizations determine how well their CIRT will be able to respond to an incident and should involve policy, response plan/strategy, communication, documentation, determining the CIRT members, access control, tools, and training.

2. **Identification -** Identification is the process through which incidents are detected, ideally promptly to enable rapid response and therefore reduce costs and damages. For this step of effective incident response, IT staff gathers events from log files, monitoring tools, error messages, intrusion detection systems, and firewalls to detect and determine incidents and their scope.

3. **Containment** - Once an incident is detected or identified, containing it is a top priority. The main purpose of containment is to contain the damage and prevent further damage from occurring (as noted in step number two, the earlier incidents are detected, the sooner they can be contained to minimize damage). It's important to note that all of SANS' recommended steps within the containment phase should be taken, especially to "prevent the destruction of any evidence that may be needed later for prosecution." These steps include short-term containment, system back-up, and long-term containment.

4. **Eradication** - Eradication is the phase of effective incident response that entails removing the threat and restoring affected systems to their previous state, ideally while minimizing data loss. Ensuring that the proper steps have been taken to this point, including measures that not only remove the malicious content but also ensure that the affected systems are completely clean, are the main actions associated with eradication.

5. **Recovery** - Testing, monitoring, and validating systems while putting them back into production in order to verify that they are not re-infected or compromised are the main tasks associated with this step of incident response. This phase also includes decision making in terms of the time and date to restore operations, testing and verifying the compromised systems, monitoring for abnormal behaviors, and using tools for testing, monitoring, and validating system behavior.

6. **Lessons Learned** - Lessons learned is a critical phase of incident response because it helps to educate and improve future incident response efforts. This is the step that gives organizations the opportunity to update their incident response plans with information that may have been missed during the incident, plus complete documentation to provide information for future incidents. Lessons learned reports give a clear review of the entire incident and may be used

during recap meetings, training materials for new CIRT members, or as benchmarks for comparison.

Proper preparation and planning are the key to effective incident response. Without a clear-cut plan and course of action, it's often too late to coordinate effective response efforts and a communication plan after a breach or attack has occurred when future attacks or security events hit. Taking the time to create a comprehensive incident response plan can save your company substantial time and money by enabling you to regain control over your systems and data promptly when an inevitable breach occurs.

penetration test (pen test)

A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system. Penetration tests usually simulate a variety of attacks that could threaten a business. They can examine whether a system is robust enough to withstand attacks from authenticated and unauthenticated positions, as well as a range of system roles. With the right scope, a pen test can dive into any aspect of a system.

What are the phases of pen testing?

Pen testers simulate attacks by motivated adversaries. To do this, they typically follow a plan that includes the following steps:

- **Reconnaissance.** Gather as much information about the target as possible from public and private sources to inform the attack strategy. Sources include internet searches, domain registration information retrieval, social engineering, nonintrusive network scanning, and sometimes even dumpster diving. This information helps pen testers map out the target's attack surface and possible vulnerabilities. Reconnaissance can vary with the scope and objectives of the pen test; it can be as simple as making a phone call to walk through the functionality of a system.
- **Scanning.** Pen testers use tools to examine the target website or system for weaknesses, including open services, application security issues, and open source vulnerabilities. Pen testers use a variety of tools based on what they find during reconnaissance and during the test.
- **Gaining access.** Attacker motivations can include stealing, changing, or deleting data; moving funds; or simply damaging a company's reputation. To perform each test case, pen testers determine the best tools and techniques to gain access to the system, whether through a weakness such as SQL injection or through malware, social engineering, or something else.
- **Maintaining access.** Once pen testers gain access to the target, their simulated attack must stay connected long enough to accomplish their goals of exfiltrating data, modifying it, or abusing functionality. It's about demonstrating the potential impact.

What are the types of pen testing?

A comprehensive approach to pen testing is essential for optimal risk management. This entails testing all the areas in your environment.

- **Web apps.** Testers examine the effectiveness of security controls and look for hidden vulnerabilities, attack patterns, and any other potential security gaps that can lead to a compromise of a web app.
- **Mobile apps.** Using both automated and extended manual testing, testers look for vulnerabilities in application binaries running on the mobile device and the corresponding server-side functionality. Server-side vulnerabilities include session management, cryptographic issues, authentication and authorization issues, and other common web service vulnerabilities.
- **Networks.** This testing identifies common to critical security vulnerabilities in an external network and systems. Experts employ a checklist that includes test cases for encrypted transport protocols, SSL certificate scoping issues, use of administrative services, and more.
- **Cloud.** A cloud environment is significantly different than traditional on-premises environments. Typically, security responsibilities are shared between the organization using the environment and the cloud services provider. Because of this, cloud pen testing requires a set of specialized skills and experience to scrutinize the various aspects of the cloud, such as configurations, APIs, various databases, encryption, storage, and security controls.
- **Containers.** Containers obtained from Docker often have vulnerabilities that can be exploited at scale. Misconfiguration is also a common risk associated with containers and their environment. Both of these risks can be uncovered with expert pen testing.
- **Embedded devices (IoT).** Embedded / Internet of Things (IoT) devices such as medical devices, automobiles, in-home appliances, oil rig equipment, and watches have unique software testing requirements due to their longer life cycles, remote locations, power constraints, regulatory requirements, and more. Experts perform a thorough communication analysis along with a client/server analysis to identify defects that matter most to the relevant use case.
- **Mobile devices.** Pen testers use both automated and manual analysis to find vulnerabilities in application binaries running on the mobile device and the corresponding server-side functionality. Vulnerabilities in application binaries can include authentication and authorization issues, client-side trust issues, misconfigured security controls, and cross-platform development framework issues. Server-side vulnerabilities can include session management, cryptographic issues, authentication and authorization issues, and other common web service vulnerabilities.
- **APIs.** Both automated and manual testing techniques are used to cover the OWASP API Security Top 10 list. Some of the security risks and vulnerabilities testers look for include broken object

level authorization, user authentication, excessive data exposure, lack of resources / rate limiting, and more.

- **CI/CD pipeline.** Modern DevSecOps practices integrate automated and intelligent code scanning tools into the CI/CD pipeline. In addition to static tools that find known vulnerabilities, automated pen testing tools can be integrated into the CI/CD pipeline to mimic what a hacker can do to compromise the security of an application. Automated CI/CD pen testing can discover hidden vulnerabilities and attack patterns that go undetected with static code scanning.

What are the pros and cons of pen testing?

With the frequency and severity of security breaches increasing year after year, organizations have never had a greater need for visibility into how they can withstand attacks. Regulations such as PCI DSS and HIPAA mandate periodic pen testing to remain current with their requirements. With these pressures in mind, here are some pros and cons for this type of defect discovery technique.

Pros of pen testing

- Finds holes in upstream security assurance practices, such as automated tools, configuration and coding standards, architecture analysis, and other lighter-weight vulnerability assessment activities
- Locates both known and unknown software flaws and security vulnerabilities, including small ones that by themselves won't raise much concern but could cause material harm as part of a complex attack pattern
- Can attack any system, mimicking how most malicious hackers would behave, simulating as close as possible a real-world adversary

Cons of pen testing

- Is labor-intensive and costly
- Does not comprehensively prevent bugs and flaws from making their way into production

How does pen testing differ from automated testing?

Although pen testing is mostly a manual effort, pen testers do use automated scanning and testing tools. But they also go beyond the tools and use their knowledge of the latest attack techniques to provide more in-depth testing than a vulnerability assessment (i.e., automated testing).

Manual pen testing

Manual pen testing uncovers vulnerabilities and weaknesses not included in popular lists (e.g., OWASP Top 10) and tests business logic that automated testing can overlook (e.g., data validation, integrity checks). A manual pen test can also help identify false positives reported by automated testing. Because

pen testers are experts who think like adversaries, they can analyze data to target their attacks and test systems and websites in ways automated testing solutions following a scripted routine cannot.

Automated testing

Automated testing generates results faster and needs fewer specialized professionals than a fully manual pen testing process. Automated testing tools track results automatically and can sometimes export them to a centralized reporting platform. Also, the results of manual pen tests can vary from test to test, whereas running automated testing repeatedly on the same system will produce the same results.

What is a Cyber security Compliance Audit?

A cyber security compliance audit is a process by which a third-party agency assesses whether or not you have the proper security systems in place while also ensuring regulatory compliance. the best way to prepare for an external audit is to conduct a comprehensive internal audit in-house.

Conducting an internal cybersecurity compliance audit comes with numerous benefits. Firstly, it enables you to self-evaluate the current state of your data security efforts. Through this self-evaluation, you'll be able to discover and remediate vulnerabilities before an attacker leverages them in the form of a breach.

If you decide not to conduct a cybersecurity compliance audit, you can open your organization up to several risks:

- **Increased Breach Risk:** If you have not evaluated your system for vulnerabilities, you leave your organization open to an increased risk of attack.
- **Damaged Organizational Reputation:** In the event of a breach, your organization can face reputation damage and lost customer trust.
- **Lack of Preparedness:** If you do not take the time to conduct a self-audit, you miss the opportunity to prepare your processes, systems, and team for an external audit.

the six steps necessary to conduct your own internal audit.

1. Identify Stakeholders

Step one of your audit is to identify your stakeholders. Who is responsible for cybersecurity compliance in your organization? If your organization is a small business, you may only have one or two stakeholders. However, enterprises may have a full team of stakeholders spread across multiple departments across the business.

Once you have identified the parties who must be involved in your audit, establish each person's responsibilities in writing. Ensure you are prepared to hold teams and individuals accountable to the responsibilities assigned.

2. Evaluate Existing Policies

What policies do you currently have in place regarding your information security processes? Take this opportunity to review all active policies, searching for areas where they are insufficient or outdated.

Watch out for any policies that exist in their current form because *"that's the way we've always done things."* Use your cybersecurity compliance audit as a chance to make positive changes in your organization's processes, enacting and updating policies to reflect modern cybersecurity threats and challenges.

Once established an understanding of the current policies and developed a plan to update them where necessary, it may inventory the IT assets.

3. Inventory IT Assets

What counts as IT assets? In this step, you will want to examine hardware, software, databases, and services. Additionally, ensure you account for any third-party data storage solutions or cloud services your organization uses.

4. Conduct a Security Risk Assessment

Begin your security risk assessment by examining current cybersecurity threats. Consider trends, past cybersecurity events in your organization, and more.

Note that a security risk assessment is not a "one and done" process. You will want to conduct this type of assessment on a regular basis.

5. Remediate Identified Risks

In all likelihood, your compliance audit will reveal weak spots and vulnerabilities. Take note of these risks and use step five of your audit to remediate those risks.

Create and implement practices and policies to close gaps with your team's data access. You may also note new technologies you need to solve these challenges and help make compliance more seamless for your team.

6. Create an Incident Response Plan

Regardless of how much effort you put into preventing a cybersecurity incident from occurring, there is always the possibility that an attacker will manage to breach your defenses. In the event of a breach, you will need a robust incident response plan to minimize the impact.

Your incident response plan will include the following:

- **Response Protocol:** A guide to indicate how each employee in your organization must respond in the event of a breach.

- **Business Continuity Plan:** A plan for how your business will recover and return to business-as-usual post-breach.