

What is Information Security?

Information security is the practice of protecting information by mitigating information risks. It involves the protection of information systems and the information processed, stored, and transmitted by these systems from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms. Effective information security requires a comprehensive and multi-disciplinary approach, involving people, processes, and technology.

What is Information Security (InfoSec)?

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. Information can be a physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data on your mobile phone, your biometrics, etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media, etc.

During the First World War, a Multi-tier Classification System was developed keeping in mind the sensitivity of the information. With the beginning of the Second World War, formal alignment of the Classification System was done. Alan Turing was the one who successfully decrypted the Enigma Machine which was used by Germans to encrypt warfare data.

Effective information security requires a comprehensive approach that considers all aspects of the information environment, including technology, policies and procedures, and people. It also requires ongoing monitoring, assessment, and adaptation to address emerging threats and vulnerabilities.

Why We Use Information Security?

We use information security to protect valuable information assets from a wide range of threats, including theft, espionage, and cybercrime. Here are some key reasons why information security is important:

Protecting sensitive information: Information security helps protect sensitive information from being accessed, disclosed, or modified by unauthorized individuals. This includes personal information, financial data, and trade secrets, as well as confidential government and military information.

Mitigating risk: By implementing information security measures, organizations can mitigate the risks associated with cyber threats and other security incidents. This includes

minimizing the risk of data breaches, denial-of-service attacks, and other malicious activities.

Compliance with regulations: Many industries and jurisdictions have specific regulations governing the protection of sensitive information. Information security measures help ensure compliance with these regulations, reducing the risk of fines and legal liability.

Protecting reputation: Security breaches can damage an organization's reputation and lead to lost business. Effective information security can help protect an organization's reputation by minimizing the risk of security incidents.

Ensuring business continuity: Information security helps ensure that critical business functions can continue even in the event of a security incident. This includes maintaining access to key systems and data, and minimizing the impact of any disruptions.

What are the 3 Principles of Information Security?

Information security is necessary to ensure the confidentiality, integrity, and availability of information, whether it is stored digitally or in other forms such as paper documents. Information Security programs are built around 3 objectives, commonly known as CIA – **Confidentiality, Integrity, Availability.**

Confidentiality – Means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.

Integrity – Means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

Availability – Means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanding the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

CIA Triad- Information Security

Apart from this there is one more principle that governs information security programs. This is Non repudiation.

Non repudiation – Means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.

Authenticity – Means verifying that users are who they say they are and that each input arriving at destination is from a trusted source. This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission.

Accountability – This means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority.

What is an Information Security Management System (ISMS)?

An Information Security Management System (ISMS) is a structured framework designed to protect an organization's information assets. It includes policies, procedures, and controls to manage and secure sensitive data from threats like unauthorized access, data breaches, and cyberattacks. By following international standards like ISO/IEC 27001, an ISMS helps organizations identify risks, implement security measures, and continuously improve their security practices to safeguard their information.

What is the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation (GDPR) is a comprehensive privacy law established by the European Union (EU) to protect individuals' personal data. Effective since May 25, 2018, GDPR sets strict rules on how personal data is collected, used, stored, and shared. It grants individuals more control over their data, including rights to access, correct, and delete their information. GDPR also requires organizations to be transparent about their data practices and to implement strong security measures. Non-compliance can result in significant fines, emphasizing the importance of safeguarding personal data and respecting privacy rights.

Types of Information Security

Information Security (InfoSec) focuses on protecting data from threats and unauthorized access. Here are five important types:

Network Security: Protects computer networks from attacks and unauthorized access using tools like firewalls, Intrusion Detection Systems (IDS), and Virtual Private

Networks (VPNs). For example, a firewall can block malicious traffic trying to enter a company's network.

Application Security: Secures software applications by finding and fixing vulnerabilities, using methods like code reviews and security patches. An example is a web application firewall (WAF) that prevents attacks on websites by filtering and monitoring HTTP traffic.

Data Security: Ensures data safety during storage and transfer by using encryption and data masking. For instance, encrypted emails are unreadable to anyone without the decryption key, protecting sensitive information.

Endpoint Security: Secures individual devices such as computers, smartphones, and tablets through antivirus software and Endpoint Detection and Response (EDR) tools. An example is an antivirus program that scans and removes malware from a personal laptop.

Cloud Security: Protects data and applications hosted in cloud environments with measures like secure cloud configurations and Identity and Access Management (IAM). For instance, using multi-factor authentication (MFA) helps ensure that only authorized users can access cloud-based services.

Why is Information Security Important?

Advantages for implementing an information classification system in an organization's information security program:

Improved security: By identifying and classifying sensitive information, organizations can better protect their most critical assets from unauthorized access or disclosure.

Compliance: Many regulatory and industry standards, such as HIPAA and PCI-DSS, require organizations to implement information classification and data protection measures.

Improved efficiency: By clearly identifying and labeling information, employees can quickly and easily determine the appropriate handling and access requirements for different types of data.

Better risk management: By understanding the potential impact of a data breach or unauthorized disclosure, organizations can prioritize resources and develop more effective incident response plans.

Cost savings: By implementing appropriate security controls for different types of information, organizations can avoid unnecessary spending on security measures that may not be needed for less sensitive data.

Improved incident response: By having a clear understanding of the criticality of specific data, organizations can respond to security incidents in a more effective and efficient manner.

There are some potential disadvantages for implementing an information classification system in an organization's information security program:

Complexity: Developing and maintaining an information classification system can be complex and time-consuming, especially for large organizations with a diverse range of data types.

Cost: Implementing and maintaining an information classification system can be costly, especially if it requires new hardware or software.

Resistance to change: Some employees may resist the implementation of an information classification system, especially if it requires them to change their usual work habits.

Inaccurate classification: Information classification is often done by human, so it is possible that some information may be misclassified, which can lead to inadequate protection or unnecessary restrictions on access.

Lack of flexibility: Information classification systems can be rigid and inflexible, making it difficult to adapt to changing business needs or new types of data.

False sense of security: Implementing an information classification system may give organizations a false sense of security, leading them to overlook other important security controls and best practices.

Maintenance: Information classification should be reviewed and updated frequently, if not it can become outdated and ineffective.

Uses of Information Security

Information security has many uses, including:

Confidentiality: Keeping sensitive information confidential and protected from unauthorized access.

Integrity: Maintaining the accuracy and consistency of data, even in the presence of malicious attacks.

Availability: Ensuring that authorized users have access to the information they need, when they need it.

Compliance: Meeting regulatory and legal requirements, such as those related to data privacy and protection.

Risk management: Identifying and mitigating potential security threats to prevent harm to the organization.

Disaster recovery: Developing and implementing a plan to quickly recover from data loss or system failures.

Authentication: Verifying the identity of users accessing information systems.

Encryption: Protecting sensitive information from unauthorized access by encoding it into a secure format.

Network security: Protecting computer networks from unauthorized access, theft, and other types of attacks.

Physical security: Protecting information systems and the information they store from theft, damage, or destruction by securing the physical facilities that house these systems.

Issues of Information Security

Information security faces many challenges and issues, including:

Cyber threats: The increasing sophistication of cyber attacks, including malware, phishing, and ransomware, makes it difficult to protect information systems and the information they store.

Human error: People can inadvertently put information at risk through actions such as losing laptops or smartphones, clicking on malicious links, or using weak passwords.

Insider threats: Employees with access to sensitive information can pose a risk if they intentionally or unintentionally cause harm to the organization.

Legacy systems: Older information systems may not have the security features of newer systems, making them more vulnerable to attack.

Complexity: The increasing complexity of information systems and the information they store makes it difficult to secure them effectively.

Mobile and IoT devices: The growing number of mobile devices and internet of things (IoT) devices creates new security challenges as they can be easily lost or stolen, and may have weak security controls.

Integration with third-party systems: Integrating information systems with third-party systems can introduce new security risks, as the third-party systems may have security vulnerabilities.

Data privacy: Protecting personal and sensitive information from unauthorized access, use, or disclosure is becoming increasingly important as data privacy regulations become more strict.

Globalization: The increasing globalization of business makes it more difficult to secure information, as data may be stored, processed, and transmitted across multiple countries with different security requirements.

Cyber Kill Chain

The Cyber Kill Chain is a concept in cyber security. It is the process of stopping cyber attacks. In this article, we will learn about what is cyber kill chain and its types, and role of it's in cybersecurity, how the cyber kill chain works and concerns related to it. Also, it covers the weaknesses of the cyber kill chain.

What is the Cyber Kill Chain?

It is also known as a cyber attack chain. It is a framework that provides a step-by-step approach to detecting and stopping cyber attacks and protecting against hackers. Seven phases present in the cyber kill chain determine a cyber attack's activity, whether internal or external. In internal attacks, hackers target insider threats, while external attacks focus on external parties. In this attack the hacker steals the user credentials.

Role of Cyber Kill Chain in Cyber Security

The main role of the cyber kill chain is to help businesses or organizations. Organizations use various cyber security tools and techniques to stay protected from hackers.

Here are the points that protected our organization from hackers-

In each stage, the attack should be detected by using various cyber security tools and techniques.

Don't share any information related to business data with third parties or unauthorized users.

Stop giving access to unauthorized users for your system.

Use multi-factor authentication and fingerprints to protect business-related information in an organization.

How does the Cyber Kill Chain Work?

Cyber kill chain gives the overview of cyber attacks so that organizations have an understanding of each stage and recover their businesses from attack. Each phase gives the overview of a specific type of attack in the cyber kill chain model. The cyber kill chain is the step-by-step techniques that identify, detects, and stops the vulnerable activity. It starts with the phase of reconnaissance and each phase represents the activities of cyber attacks. Organizations use various security tools to identify and detect these attacks.

Here are the phases that represent the working of the cyber kill chain:

Phases of Cyber kill chain

Reconnaissance: It is the first phase in the cyber kill chain framework. It is also known as cyber intelligence gathering. It is a way of collecting data or information about vulnerabilities and potential targets. Attackers use reconnaissance as a tool that helps with their actual attack. There are two types of reconnaissance. The first one is active reconnaissance, and the second is passive reconnaissance. In active reconnaissance,

attackers connect directly with computers and steal information by using techniques like manual testing and tools like ping, netcat, etc. The process is faster but creates more noise in the system. In passive reconnaissance, hackers do not interact with the system. It collects the information that is available publicly.

Weaponization: In this phase, hackers use weaponization as a tool to attack their users. They send the malicious file in the mail, and when the user opens that file, hackers steal the information from their users. Hackers send the fake email to either businesses or vendors. The email looks real, but when the user opens that link, a hacker steals the information. Sometimes, hackers send a fake bank web page link when the user opens, and when they enter the username and password, hackers steal the information about the user's account.

Delivery: In the delivery phase, hackers wait for all the information they send to the user, like fake email attachment links, and when the user opens those links, they steal the information of the user.

Exploitation: In the exploitation phase, hackers target the users, and after targeting the system, they execute the malware code on the target system. After executing successfully, the hackers have access to the target system and gather all the information.

Installation: In the installation phase, hackers install software that connects the victim's computer. In this phase, hackers take control of the victim's account. Hackers install malware software that takes control of the user's system and gains user information. They install malware via trojan horses, backdoors, etc.

Command and control: In the command and control phase, the hackers took full control of the user system. Attackers establish command and control over the access and control of the target user network, which means hackers have full control of the user's system and can perform any task in the user's system.

Actions on the objective phase: After the command and control phase, the next step or objective is to steal data and destroy the target user's system. For example, the hacker withdraws the money from the user's account or steals the credit card information.

Critiques and Concerns Related to Cyber Kill Chain

The cyber kill chain is the framework that helps organizations to create strategic thinking and use various cyber security tools and techniques to protect themselves from cyber-attacks.

The first critique is perimeter security which provides a solutions of security that protect for any unauthorized access to our devices. It acts as the border between the organization and a hacker when a hacker tries to attack the system they detect and prevent their attack by using various approaches and security tools.

The second critique is the attack vulnerabilities. Sometimes the organization has difficulty detecting the attack by using monitoring and analysis. The organization uses more advanced monitoring and analysis to detect the attack.

Weakness of Cyber Kill Chain

One of the weaknesses in the cyber kill chain is that they have a limited number of attack detections, which means they do not detect other types of attacks.

It also does not detect the unauthorized person who steals the user credentials.

Some of the attackers do not follow the cyber kill chain step by step, which means they skip and add any of the steps, like delivery, and use the merge step of the kill chain.

Cyber kill chain cannot detect insider threats, to misuse the company data or information

An insider threat is an attack that goes into the organization or company whether the attacker is any former employee, any vendors, etc.

Due to the increase in remote working, in that situation, hackers try to access the organization's data by using various techniques and sometimes it would be challenging for an organization to identify and secure it.

Introduction to Ethical Hacking

Today, computer and network security against cyber threats of increasing sophistication is more important than it has ever been. Such an endeavor cannot be accomplished without ethical hacking. Ethical hacking means that authorized individuals work at exposing a security vulnerability and ultimately eliminate it before a malefactor can exploit it.

Malicious hacking is an endeavor to exploit vulnerabilities for personal benefits, while ethical hacking involves authorized individuals exposing and eliminating the security frailties before they might be exploited by malicious hands. Thus, ethical hackers, also known as white-hat hackers, carry out controlled and systematic testing of systems, applications, and networks to identify possible vulnerabilities.

What is Ethical Hacking?

Ethical hacking involves the probing and testing of computer systems, networks, and applications purposely to identify and make amends on security vulnerabilities, an ethical hacker alias white-hat or pen tester, is mandated with similar goals to enhance security within an organization. The proactive approach of ethical hacking ensures the strength of organizational defenses against cyberattacks, protection of sensitive information, and compliance with security standards and regulations. This understanding and subsequent

simulation of techniques used by cybercriminals make ethical hackers pivotal in maintaining a good state of cybersecurity and the protection of digital assets.

Key aspects of ethical hacking include:

Reporting: Ethical hackers report back to the organization with the results of the tests.

Permission-Based: This permission becomes necessary to differentiate their job from criminal hacking jobs

Objective: The main goal is to find the holes before hostile attackers can penetrate them. This includes discovering system, application, and network vulnerabilities that an attacker could exploit.

Methodology: Today, computer and network security against cyber threats of increasing sophistication is more important than it has ever been. Such an endeavor cannot be accomplished without ethical hacking. Ethical hacking means that authorized individuals work at exposing a security vulnerability and ultimately eliminate it before a malefactor can exploit it.

Malicious hacking is an endeavor to exploit vulnerabilities for personal benefits, while ethical hacking involves authorized individuals exposing and eliminating the security frailties before they might be exploited by malicious hands. Thus, ethical hackers, also known as white-hat hackers, carry out controlled and systematic testing of systems, applications, and networks to identify possible vulnerabilities.

Importance of Ethical Hacking

Ethical hacking contributes significantly to contemporary cybersecurity, ethical hackers are able to identify and address vulnerabilities before they are exploited by simulating the strategies and tactics utilized by cybercriminals. This proactive methodology serves to:

Enhance Security: Identify and address flaws to stop data breaches and cyberattacks.

Compliance: Meet security standards set by the industry and regulatory requirements.

Management of risk: Assess and reduce potential threats to the assets of the organization

Occurrence Reaction: Enhance the company's capacity to respond to security incidents and recover from them.

Types of Ethical Hacking

Depending on the focus of the security testing, ethical hacking can be broken down into a number of different categories:

Hacking the network: involves testing the infrastructure of the network in order to find flaws in the protocols, configurations, and devices of the network

Hacking Web Applications: Centers around distinguishing shortcomings in web applications, for example, SQL injection or cross-website prearranging (XSS) weaknesses

Hacking the system: Targets working frameworks and programming to find security defects that could be taken advantage of.

Social Designing: attempts to manipulate individuals into revealing confidential information or performing actions that could compromise security, putting the human element to the test.

Hacking into wireless networks: involves identifying potential dangers in wireless communications and evaluating the security of wireless networks.

Types of Ethical Hackers

Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or network. An ethical hacker finds the weak points or loopholes in a computer, web application or network and reports them to the organization. So, let's explore more about Ethical Hacking step-by-step. These are various types of hackers:

- (1) White Hat Hackers (Cyber-Security Hacker)
- (2) Black Hat Hackers (Cracker)
- (3) Gray Hat Hackers (Both)
- (4) Blue Hat hackers
- (5) Green Hat Hackers
- (6) Red Hat Hackers.

White Hat Hackers: Here, we look for bugs and ethically report them to the organization. We are authorized as a user to test for bugs in a website or network and report it to them. White hat hackers generally get all the needed information about the application or network to test for, from the organization itself. They use their skills to test it before the website goes live or attacked by malicious hackers. To become a white hat hacker, you can earn a bachelor's degree in computer science, information technology, or

cybersecurity. In addition, certifications such as Certified Ethical Hacker (CEH) and Certified Information Systems Security Professional (CISSP) are highly recommended.

Black Hat Hackers: Here, the organization doesn't allow the user to test it. They unethically enter inside the website and steal data from the admin panel or manipulate the data. They only focus on themselves and the advantages they will get from the personal data for personal financial gain. They can cause major damage to the company by altering the functions which lead to the loss of the company at a much higher extent. This can even lead you to extreme consequences.

Grey Hat Hackers: They sometimes access to the data and violates the law. But never have the same intention as Black hat hackers, they often operate for the common good. The main difference is that they exploit vulnerability publicly whereas white hat hackers do it privately for the company. One criticism of Grey Hat hackers is that their actions can still cause harm. Even if they do not steal or damage data, their unauthorized access to computer systems can still disrupt operations and cause financial losses for companies. Additionally, there is always the risk that a Grey Hat hacker will accidentally cause damage while attempting to identify vulnerabilities.

Blue Hat hackers: They are much like the script kiddies, are beginners in the field of hacking. If anyone makes angry a script kiddie and he/she may take revenge, then they are considered as the blue hat hackers. Blue Hat hackers payback to those who have challenged them or angry them. Like the Script Kiddies, Blue hat hackers also have no desire to learn.

Green Hat hackers : They are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers. They are inspired by the hackers and ask them few questions about. While hackers are answering their question they will listen to its novelty.

Red Hat Hackers: They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate. They become ruthless while dealing with malware actions of the black hat hackers. Red hat hacker will keep on attacking the hacker aggressively that the hacker may know it as well have to replace the whole system.

Phases of Ethical Hacking

Ethical hacking typically involves the following key phases:

Preparation and planning: Characterize the extent of the test, acquire fundamental authorizations, and accumulate data about the objective framework.

Reconnaissance: Gather in-depth data about the target system, including information about its network structure, IP addresses, and potential security holes.

Scanning: Scan the target system using a variety of tools and methods to look for vulnerable services, open ports, and vulnerabilities.

Obtaining Entry: Attempt to gain access to the system by mimicking potential real-world attacks by taking advantage of identified vulnerabilities.

Keeping Access Open: Test the capacity to keep up with access inside the framework and survey ingenuity components that could be utilized by assailants.

Reporting and Analysis: Produce a comprehensive report to the organization, document findings, and offer suggestions for reducing vulnerabilities.

Benefits of Ethical Hacking.

Advantages

Ethical hacking has advantages that go beyond just enhancing security, They consist of:

Preventing Data Breach: Organizations can avoid costly data breaches by identifying vulnerabilities before attackers do.

Importance of Ethical Hacking

Ethical hacking contributes significantly to contemporary cybersecurity, ethical hackers are able to identify and address vulnerabilities before they are exploited by simulating the strategies and tactics utilized by cybercriminals. This proactive methodology serves to:

Enhance Security: Identify and address flaws to stop data breaches and cyberattacks.

Compliance: Meet security standards set by the industry and regulatory requirements.

Management of risk: Assess and reduce potential threats to the assets of the organization

Occurrence Reaction: Enhance the company's capacity to respond to security incidents and recover from them.

Types of Ethical Hacking

Depending on the focus of the security testing, ethical hacking can be broken down into a number of different categories:

Hacking the network: involves testing the infrastructure of the network in order to find flaws in the protocols, configurations, and devices of the network

Hacking Web Applications: Centers around distinguishing shortcomings in web applications, for example, SQL injection or cross-website prearranging (XSS) weaknesses

Hacking the system: Targets working frameworks and programming to find security defects that could be taken advantage of.

Social Designing: Hacking into wireless attempts to manipulate individuals into revealing confidential information or performing actions that could compromise security, putting the human element to the test.

ss networks: involves identifying potential dangers in wireless communications and evaluating the security of wireless networks.

Information Security and Cyber Laws

Last Updated : 24 Jun, 2024



Information security is a broad field that encompasses a wide range of technologies, practices, and policies to protect sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. It includes physical, network security, and application security, as well as policies and procedures for incident management and disaster recovery. Information security is important for any organization that handles sensitive information, such as personal data, financial information, or confidential business information.

What is Information Security?

Information security protects information and systems from unauthorized access, disclosure, disruption, modification, or destruction. It encompasses a range of strategies, technologies, and practices designed to safeguard sensitive data and ensure

the integrity, confidentiality, and availability of information. Information security aims to mitigate risks associated with cyber threats, such as hacking, data breaches, malware attacks, and insider threats, thereby preserving the trustworthiness of data and maintaining the operations and reputation of organizations and individuals.

Information Security Practices

There are several steps that organizations can take to improve their information security:

1. Risk assessment: Organizations should conduct regular risk assessments to identify potential vulnerabilities and threats to their sensitive information. This allows them to prioritize their security efforts and focus on the most critical risks.
2. Access control: Organizations should implement strict access controls to ensure that only authorized individuals are able to access sensitive information. This can include measures such as secure authentication, multi-factor authentication, and role-based access controls.
3. Data encryption: Organizations should encrypt sensitive information to protect it from unauthorized access and disclosure. This can include encrypting data at rest and in transit, as well as using secure protocols for communication.
4. Network security: Organizations should secure their networks to prevent unauthorized access and protect against malware and other cyber threats. This can include using firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs).
5. Incident management: Organizations should have an incident management plan in place to respond quickly and effectively to security breaches. This

- should include procedures for incident response, incident management, and incident reporting.
6. Compliance: Organizations should comply with relevant laws and regulations related to information security, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).
 7. Employee training: Organizations should provide regular training to employees on information security best practices, policies, and procedures. This can help to ensure that employees understand the importance of protecting sensitive information and know how to do so.
 8. Regularly monitoring and testing: Organizations should regularly monitor and test their security systems to ensure they are working properly and to identify potential vulnerabilities. This can include regular vulnerability scans, penetration testing, and security audits.

What is Cyber Law?

It is also known as internet laws or digital laws, are laws that govern the use of the internet and other digital technologies. These laws address a wide range of issues, including intellectual property, privacy, cybercrime, and liability for online activities. Cyber laws vary from country to country, but most countries have laws that address issues such as hacking, identity theft, and online fraud.

There are several key cyber laws that govern online activity and protect individuals and organizations from cybercrime. Some of the most important laws include:

1. The Computer Fraud and Abuse Act (CFAA): This law criminalizes unauthorized access to computer systems and networks, as well as unauthorized access to sensitive information stored on those systems.
2. The Electronic Communications Privacy Act (ECPA): This law regulates the interception and disclosure of electronic communications, including email and text messages.
3. The Health Insurance Portability and Accountability Act (HIPAA): This law regulates the use and disclosure of protected health information (PHI) in electronic form.
4. The Children's Online Privacy Protection Act (COPPA): This law regulates the collection of personal information from children under the age of 13.
5. The General Data Protection Regulation (GDPR): This EU regulation regulates the collection and processing of the personal data of EU citizens.
6. The Personal Data Protection Bill (PDPB): In India, this bill regulates the collection, storage, and processing of personal data of Indian citizens.

These are just a few examples of the many cyber laws that exist to protect individuals and organizations from cybercrime. It's important for individuals and organizations to stay informed about these laws and to comply with them in order to avoid legal repercussions.

The relationship between information security and cyber laws is close, as both fields are concerned with protecting sensitive information and preventing unauthorized access to that information. Cyber laws help to define what constitutes a security breach and the penalties for committing such a breach, while information security practices help to prevent breaches from occurring in the first place. Cyber laws also help to ensure that organizations are accountable for protecting sensitive information

and that individuals are able to take legal action if their personal information is mishandled.

What is a Virtual Organization?

A Virtual Organization is a type of organization whose members are geographically separated and usually work by computer e-mail and software system while appearing to others to be a single, combined organization with a real physical location.

Virtual Organization is defined as being closely integrated ambitious with its suppliers and downstream with its customers. In the virtual organization, each discrete firm keeps supremacy in major budgeting and pricing matters and functions as part of a greater organization coordinated by the central firm acting as a combiner of the actions done by the various partners. Interdependence among partners differentiates the virtual organization from the conventional hierarchy.

Companies adapt to coordinating and maximizing the capabilities of suppliers which will gain more control over key elements of time from overall order-to-shipment lead time to product-specific cycle time. In addition, full-fledged alliances that tap the resources of multiple parties will effectively slash product process development time.

- A virtual organization is an energetic collection of individuals and institutions that are required to share resources to obtain specified targets.
- A virtual organization is a network of independent organizations that combine together for the production of a service or product.
- Virtual organizations are also mentioned as network organizations, organic networks, hybrid arrangements, and value-adding partnerships. This phenomenon has been driven by the effort to achieve greater effectiveness

and responsiveness in an extremely competitive environment marked by increasing globalization, technological change, and customer demands.

Virtual Organization Properties

1. **Delocalization:** Delocalization is one of the most important developments in the globalization process. It is potentially space-dependent. Therefore, enterprises become independent of space and capacity. It eliminates the need for a particular space.
2. **Temporalization:** This property deals with the inter-organizational connections and with the internal process organization, in the sense of the standard and pattern organization. Interdependence is described in the life cycle stages of a virtual organization as a circular process of creation, operation, evaluation, and dissolution.
3. **Dematerialization:** Dematerialization has virtual forms in products, communities, services, and so on along the development of virtualization. With increasing virtualization, products become potentially immaterial. It means that all object areas are immaterial. Existing correlative confidence for members, lack of physical credits, and executives can affect system performance and flexibility.
4. **Individualization:** The main reason for this property is increasing consumer demands. One of the ways to encapsulate the market is to handle mass production along with personal requirements. Mass customization is one of the ways for producers to fulfill customer demands and reach new markets.
5. **Non-Institutionalization:** Because operations are performed in a virtual environment without physical attributes, the institutionalization of inter-organizational relationships in such environments can be waived.

6. Asynchronization: This attribute causes members to asynchronously communicate and interact with each other via ICT in the context of innovations with the release of time. Some companies globally plan their working three shifts between spread locations.
7. Integrative Atomization: This property refers to integrating all atomized core competencies of the participants to satisfy the customer.

Characteristics of a Virtual Organization

- Organizations do not have a corporeal presence but subsist electronically (virtually) on the Internet.
- Virtual organization is not constrained by the legal definition of a company.
- A virtual organization is formed in an informal manner as an association of independent legal entities.
- Principle of synergy (many-to-one). Virtual organization displays a combined property because it is composed of different organizational entities that produce an effect of a single organization.
- Principle of divergence (one-to-many). A single organization can display multiplication property by engaging in many virtual organizations at the same time.
- Partners in virtual organizations share risks, costs, and rewards in search of a global market. The common characteristics of these opportunities are world-class core competence, information networks, and interdependent relationships.
- Dynamic virtual organizations have the capability to unite quickly.

Virtual Organization Life Cycle

1. Virtual Organization Creation
2. Virtual Organization Operation
3. Virtual Organization Evolution
4. Virtual Organization Dissolution

Benefits of Virtual Organization

- Virtual organizations make it possible to convince repeatedly changing customer and market needs in a competitive way.
- With the help of virtual organizations, it becomes possible to provide services exactly customized to a specific customer need.
- Virtual organizations provideth ability to participate in the total service range a company can offer to its customers.
- Participation in virtual organization enlarges the total number of end-customers a company can extend indirectly via its partners.
- By joining a virtual organization the concept-to-cash time is minimized.

Drawbacks of Virtual Organization

- Each party has its own strategy for access control and conditions of use.
- Virtual organization parties are required to build trust between them on a peer-to-peer basis.
- The assignment of resources is often dynamic since the structure of virtual organizations may change dynamically. This implies that the virtual organization beginner may not know a priority that additional resources may be required.

- Members of virtual organizations may be located in different countries under different authorities and, as a result, stick to different legal and business requirements.
- There must be mutual trust in the security system by all partners involved in a virtual organization. This leads to the challenge of coming up with a successful and pliable security system.
- Privacy and probity at a virtual organization level have to be assured. At the same time, parties have to yield access to their services and resources as mentioned in agreements.

Conclusion

Information security and cyber laws are crucial for keeping digital information safe and ensuring fair use of technology. Information security focuses on protecting data from unauthorized access or harm using various tools and methods. Cyber laws provide rules to prevent cybercrimes, protect personal information, and regulate online activities. Together, they help reduce risks from cyber threats, protect privacy, and create safer digital spaces. Following strong security practices and obeying cyber laws help organizations and people stay safe online and build trust in digital interactions.

Information security controls?

According to NIST (the National Institute of Standards and Technology), security controls are defined as “the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.”

That means that any countermeasure used to keep a computer, device, network, or safe from a data breach or another attack is a countermeasure.

That may seem extremely broad, but information security controls are often categorized, both by type and by the goals of the countermeasure. What does that mean? Below is a listing of information security controls by type:

Physical controls: Locks on doors that keep intruders from devices, the ability to remove a device from a network, and access control to physical equipment are all physical controls.

Administrative controls: incident response processes, information security awareness, and training are administrative controls.

Technical controls: Items that use technology to combat attacks, like authentication, antivirus software, and firewalls are technical controls.

Legal and regulatory or compliance controls: Privacy legislation or information security frameworks are legal or regulatory controls.

When controls are classified by a goal, however, the list looks a little different:

Preventive controls: Intended to prevent an incident from occurring, such as good cyber hygiene, network segmentation, and user authentication.

Detective controls: Tools used during an incident to respond to a breach, such as anti-malware software, a ransomware response plan, or security ratings.

Corrective controls: After the event, corrective controls limit the extent of any damage caused by the incident, such as cybersecurity insurance or new response plans.

What security controls does my organization need?

No one organization will implement every single information security control. Some may be redundant and some might not be relevant to your organization or your networks, but every organization needs some of the above.

There are several security standards and frameworks that provide a starting point for organizations when it comes to security best practices and controls.

NIST, mentioned above, offers a free, voluntary cybersecurity framework consisting of standards, guidelines, and practices to promote the protection of an organization's critical infrastructure. It lists more than 100 individual controls a company can use to mitigate risk.

Another standard, the ISO/IEC 27001, is offered by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This international standard identifies 114 controls in 14 groups, ranging from policies to incident management.

The SANS CIS Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop attacks.

COBIT5 is a proprietary control set published by ISACA which is based on five principles of security.

These are just a few examples; many regulated industries and sectors are governed by their own frameworks and control sets.

How can SecurityScorecard help?

SecurityScorecard's security ratings are technical and detective controls, meaning that they help you identify any problems with your organization's security posture before you're attacked... and that they're technical and not physical, like a lock on a door.

SecurityScorecard continuously monitors your complete infrastructure, including your extended enterprise. Our platform can track both your internal and external adherence to established policies and practices — we let you capture, report, and remediate security risks in real-time, so you're never in danger of falling out of compliance, no matter what framework or standards you adhere to.

An information security standard is a series of documented processes that define how to implement, manage, and monitor various security controls. As well as providing a blueprint for mitigating risk and reducing vulnerabilities, cybersecurity standards and cybersecurity frameworks typically detail the necessary steps for achieving regulatory compliance.

What are the 4 types of information security?

Application Security: identifying and addressing exploitable vulnerabilities in web and mobile applications so malicious actors can't use them to breach a company's network.

Network Security: implementing the policies and controls to protect the data and infrastructure within a company's network and prevent unauthorised access.

Cloud Security: strategies and solutions to secure a company's off-site cloud deployment.

Cryptography: various processes and techniques to better secure data through encryption. Cryptography prevents sensitive information from being decoded by cybercriminals in the event of a data breach.

Let's look at information security standards, why they're important, and the consequences of failing to meet them.

Why companies need to meet information security standards

There are several key reasons why it's in a company's best interest to meet information standards:

Achieve regulatory compliance

Adhering to information security standards results in companies becoming compliant with the IT security regulations required by their industry. Consequently, they can avoid the negative consequences of not being compliant, such as financial penalties and legal trouble.

- **Prevent cyberattacks**

Information security standards outline cybersecurity best practices so aligning with them is an effective way for companies to approach their information security needs.

This is because meeting IT security standards requires a company to implement the necessary measures, processes, policies, and controls that will improve its cybersecurity posture.

Now, while it's important to note that compliance doesn't necessarily translate into security, as cyberthreats evolve faster than security standards, it's an excellent starting point.

- **Increased awareness of risk**

Adhering to security standards requires a company's security teams to become more aware of cybersecurity best practices, definitions, terminology, and, most importantly, the full extent of the cyber threats they face. This reduces the chance of costly breaches due to ignorance and reduces the need to undergo trial and error to mitigate cyberattacks.

- **Enhanced reputation**

Meeting information security standards displays your company's commitment to cybersecurity and ensuring data security – especially when you receive certification for your efforts. This inspires confidence with existing and potential clients, supply chain partners, etc., and reassures them their information is secure when working with you.

Footprint & reconnaissance

A footprint is a digital trace of your activity that you leave behind on the Internet. It is like the footprint you leave behind in the sand at the beach.

These footprints can be innocuous, such as an e-mail account that you have forgotten about in Hotmail, or they can give away highly sensitive information through your browsing history on your work computer. Footprints also include information about what social networks and other websites people visit, what content they look at and for how long, who their Facebook friends are, and when they were last online; all this data is available with just one click to Google or to a range of specialized search engines.

Primary Sources:

In general, websites and search engines like Google and Bing allow you to create a footprint about yourself by disclosing your name, address, phone numbers, and other information about yourself. This information is then stored and can be found by anyone. Information about you on the web may be used to identify additional information about your social networks or connections. There are a number of software tools that can help find out more information about a person, company, or organization that has been the subject of an investigation. These include:

Footprinting is essential to identity theft hackers, who must gather as much detailed information on the identities and activities of their targets as possible in order to establish whether enough evidence exists for them to consider a fraud report to the police.

The Internet allows for a revolution in the way people collect personal information.

The tool which has been used is e-mail passwords, which are emails that have been sent by an email address.

This makes it easy for criminals to steal the password for the e-mail and thus gain access to all of their online activities and a lot of their personal information.

There are many people that do not use their passwords and do not change them often. There are also many people that choose not to use a password at all and still use the same password over and over again.

Footprinting, also known as fingerprinting, is a methodology used by penetration testers, cybersecurity professionals, and even threat actors to gather information about a target organization to identify potential vulnerabilities. Footprinting is the first step in penetration testing. It involves scanning open ports, mapping network topologies, and collecting information about hosts, their operating systems, IP addresses, and user accounts. This gathered data helps to generate a comprehensive technical blueprint of the target organization. Using footprinting, cybersecurity researchers can locate existing vulnerabilities and evaluate the security posture of the organization, while threat actors can develop exploits to target the vulnerabilities and compromise the organization's network.

Types of footprinting

The two different types of footprinting are passive and active footprinting.

Passive footprinting – This method gathers information without direct interaction with the target system using search engines and social networking sites. This approach is technically challenging as it doesn't involve active network traffic; instead, data is gathered from stored and archived sources.

Active footprinting – This method directly engages with the target system to gather information using various tools. Active footprinting requires more careful planning than passive footprinting, as it may alert the target organization and leave traces of network activity.

Methods of footprinting

Cybersecurity professionals and threat actors employ various footprinting methods based on their objectives to gather a detailed technical profile of the organization.

Footprinting through search engines – Using Google's advanced search operators, along with video, FTP, and IoT search engines to gather publicly available information about a target gives the possibility for social engineering attacks. Also, employing advanced Google hacking techniques and referring to the Google Hacking Database (GHDB) to probe for sensitive information and potential server vulnerabilities.

Footprinting through web services – Numerous online platforms could be used for footprinting, such as people search engines, financial services, business profile sites, job sites, and public source code repositories.

Footprinting through social networking sites – Valuable personal and organizational information can be gathered by publicly posted information on social profiles by employees.

Website footprinting – This technique monitors and analyzes the target website for information, including IP address, domain owner, domain name, subdirectories, parameters, site host, scripting platform, and operating system details. Tools such as web spiders, web mirrors, monitoring tools, and web data extracting tools are used for these techniques.

Email footprinting – Using email tracking tools and analyzing email headers, information such as the sender's and recipient's IP address, geolocation, routing path, proxies, links, operating system, and browser information.

WHOIS footprinting – WHOIS provides current domain and owner details, offering access to information such as domain name, owner contact information, creation date, and the public network range.

Domain Name System (DNS) footprinting – DNS records provide zone data about the selected network, such as its IP addresses, domain's mail server, CPU type, and operating systems. DNS information could be obtained through DNS interrogation and reverse DNS lookup methods.

Network footprinting – Information about the target network's topology, operating system, and access control devices can be obtained using the network IP range and traceroute data.

Footprinting through social engineering – Sensitive data could be obtained through social engineering techniques such as eavesdropping, shoulder surfing, and impersonation.

Footprinting through Web services :

Web services such as people search services can provide sensitive information about the target. Social networking sites, people search services, alerting services, financial services, and job sites provide information about a target such as infrastructure details, physical location, and employee details. Using this information, an attacker may build a hacking strategy to break into the target organization's network and carry out other types of advanced system attacks.

This blog aims to familiarize you with finding the target company's top-level domains, sub- domains, and geographical location, performing people search on social networking sites and people search services, gathering information from job sites, financial services, third-party data repositories, performing deep and dark web footprinting, determining the operating system, VOIP and VPN footprinting through Shodan, gathering competitive intelligence, etc.

Finding a Company's Top-Level Domains (TLDs) and Sub-domains

A company's top-level domains (TLDs) and sub-domains

Collect Information through Social Engineering on Social Networking Sites

can provide a large amount of useful information to an attacker. A public website is designed to show the presence of an organization on the Internet. It is available for free public access. It is designed to attract customers and partners. It may contain information such as organizational history, services and products, and contact information. The target organization's external URL can be located with the help of search engines such as Google and Bing. The sub-domain is available to only a few people. These persons may be employ organization or members of a department. In many organizations, website administrators create sub-domains to test new technologies before deploying them on the main website. Generally, these sub-domains are in the testing stage and are insecure; hence, they are more vulnerable to various exploitations. Sub-domains provide insights into the different departments and business. units in an organization. Identifying such sub-domains may reveal critical information regarding the target, such as the source code of the website and documents on the webserver. Access restrictions can be applied based on the IP address, domain or subnet, username, and password. The sub-domain helps to access the private functions of an organization. Most organizations use common formats for sub-domains. Therefore, a hacker who knows the external URL of a company can often discover the sub-domain through trial and error, or by using a service such as Netcraft. You can also use the advanced Google search operator shown below to identify all the sub-domains of the target:

Footprinting through Social Networking Sites

2.2.3 Footprinting through Social Networking Sites

- Attackers use social engineering trick to gather sensitive information from social networking websites such as **Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+**, etc.
- Attackers create a **fake profile** on social networking sites and then use the false identity to lure the employees to give up their sensitive information.
fake id generator
- Employees may **post personal information** such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.
- Attackers collect information about employee's interests by **tracking their groups** and then trick the employee to reveal more information.

Information Available on Social Networking Sites

What Attacker Gets	What Users Do	What Organizations Do	What Attacker Gets
Contact info, location, etc.	Maintain profile	User surveys	Business strategies
Friends list, friends info, etc.	Connect to friends, chatting	Promote products	Product profile

Identify of a family members	Share photos and videos	User support	Social engineering
Interests	Play games, join groups	Recruitment	Platform/technology information
Activities	Creates events	Background check to hire employees	Type of business

2.2.4 Website Footprinting

Website Footprinting

- Website Footprinting refers to monitoring and analyzing the target organization's website for information.
- Browsing the target website may provide:
 - Software used and its version
 - Operating system used
 - Sub-directories and parameters
 - Filename, path, database field name, or query
 - Scripting platform
 - Contact details and CMS details
- Use Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug, etc. to view headers that provide:
 - Connection status and content-type
 - Accept-Ranges
 - Last-Modified information
 - X-Powered-By information
 - Web server in use and its version
- Examining HTML source provide:
 - Comments in the source code
 - Contact details of web developer or admin
 - File system structure

- Script type
- Examining cookies may provide:
 - Software in use and its behavior
 - Scripting platforms used Web spiders perform automated searches on the target websites and collect specified information such as employee names, email addresses, etc.
 - Attackers use the collected information to perform further footprinting and social engineering attacks.
- GSA Email Spider: <http://email.spider.gsa-online.de>
- Web Data Extractor: <http://webextractor.com>
 -

Website Footprinting using Web Spiders

Mirroring Entire Website

- Mirroring an entire website onto the local system enables an attacker to browse website offline; it also assists in finding directory structure and other valuable information from the mirrored copy without multiple requests to web server.
- Web mirroring tools allow you to download a website to a local directory, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer.
- wget -m
- HTTrack Web Site Copier: <http://www.httrack.com>
- SurfOffline: <http://www.surfoffline.com>

Website Mirroring Tools

Extract Website Information from <http://www.archive.org> (重要)

- Internet Archive's Wayback Machine allows you to visit archived versions of websites.

google cache:

Monitoring Web Updates Using Website-Watcher

- **Website-Watcher automatically checks web pages for updates and changes.**

Stages of footprinting

Both penetration testers and threat actors follow a four-step process in footprinting to gather important information.

1. Target identification – The first step involves recognizing the target organization and its systems for footprinting. This can be done by scanning networks for open ports or using IoT search engines such as Shodan and Censys.
2. Information gathering – Gathering vital information, including IP addresses, open ports and services, usernames, and passwords from the identified target
3. Result analysis – Extracted data is analyzed for vulnerabilities across multiple systems, or results are compared against known exploits.
4. Attack planning – The final stage is the attack phase, where the threat actor develops custom exploits or chooses a suitable attack vector based on the data collected to compromise vulnerable systems.

Tips to prevent footprinting attacks

Restrict unnecessary network traffic using a firewall – Set rules to prevent unauthorized DNS traffic and limit ICMP ping requests.

Monitor events and log files for suspicious traffic, malformed DNS queries, and use of advanced search parameters.

Use proxy servers to block fragmented or malformed packets, which are employed in footprinting attempts.

Perform TCP, UDP, and ICMP scans on the IP address space to assess network vulnerabilities and detect open ports ahead of potential threats.

Set your DNS records so that the information is private.

Ensure that only authorized users have access to essential ports and services on systems.

Engage the services of reputable penetration testers to help you identify security gaps.

Regularly monitor and update vulnerabilities to protect systems against exploits.

Email Footprinting

Tracking Email Communications

- Email tracking is used to **monitor the delivery of emails** to an intended recipient.
- Attackers track emails to gather information about a target recipient in order to perform social engineering and other attacks.
- Get recipient's system IP address
- Geolocation of the recipient
- When the email was received and read
- Whether or not the recipient visited any links sent to them
- Get recipient's browser and operating system information
- Time spent on reading the emails

Collecting Information from Email Header

Email Tracking Tools

- eMailTrackerPro: <http://www.emailtrackerpro.com>
- PoliteMail: <http://www.politemail.com>
- Email Lookup - Free Email Tracker: <http://www.ipaddresslocation.org>

Scanning Networks

After selecting a target and initial reconnaissance, as described in the **Footprinting and Reconnaissance module**, attackers search for access points into the target system, determining the system's activity status to streamline scanning efforts. Scanning, a deeper reconnaissance form, reveals information about the target's operating systems. This module provides an overview of network scanning techniques, including live system checks, port and service discovery, and strategies to circumvent IDS and firewalls.

What is Network Scanning?

Network scanning is a critical process in cybersecurity for acquiring in-depth information about a target by employing advanced reconnaissance tactics. Network scanning encompasses procedures for detecting hosts, ports, and services within a network and is also instrumental in discovering the Operating Systems (OS) on the active machines. This is a crucial step for information collection for an attacker, facilitating the construction of a comprehensive profile of the target organization. During the scanning process, an attacker collects specific IP addresses that are reachable across the network, the system architecture of the target's OS, and the services active on each system.

First, we will explore a selection of network scanning tools featured in this module. Then, leveraging these tools, we will guide you through the process of conducting a

comprehensive network scan. The following list highlights the top network scanning tools used for scanning.

- 1. Nmap:** Nmap can identify devices running on a network, discover open ports, detect security risks, and more.
- 2. Hping3:** Hping3 allows users to send custom TCP/IP packets and analyze the responses, making it useful for network testing, firewall testing, manual packet crafting, and network performance analysis.
- 3. Nessus:** Nessus is used to detect potential vulnerabilities in networked devices, such as weaknesses in firewalls, malware infections, and outdated software. It is known for its extensive plugin library that automates the detection of vulnerabilities.
- 4. Zenmap:** Zenmap is crafted to make Nmap easy to use for beginners yet it retains sophisticated features that appeal to experienced users of Nmap. It helps visualize network topologies and vulnerabilities through intuitive graphical representations.
- 5. Angry IP scanner:** Angry IP scanner is an open-source and multi-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports and has many other features.
- 6. Netcat:** Netcat is a flexible networking tool that operates over TCP/IP and is reliable for various programs and scripts. Due to its wide range of functionalities, it's often called the "Swiss army knife" of networking tools.

1. Network Scanning

Do you ever think about knowing which device is active on the network? Network scanning is the technique that lets you pinpoint all devices currently active on your network. It typically involves sending pings to all possible IP addresses within a network to identify active devices. A manual ARP scan can be used to discover local subnets. Automated scanning tools are recommended to detect devices across multiple subnets. ICMP scans, which are more complex and may include echo, timestamp, or subnet mask requests, are useful for mapping network topology. Let's see how Nmap is **used** in network scanning.

Ping: It sends an ICMP echo request to the target system and reverts the echo if the system is live.

```

(root@kali)-[/home/kali]
# ping google.com
PING google.com (142.250.207.206) 56(84) bytes of data.
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=1 ttl=128 time=13.0 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=2 ttl=128 time=12.6 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=3 ttl=128 time=13.6 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=4 ttl=128 time=14.3 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=5 ttl=128 time=12.3 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=6 ttl=128 time=17.4 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=7 ttl=128 time=13.5 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=8 ttl=128 time=12.9 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=9 ttl=128 time=13.1 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=10 ttl=128 time=13.1 ms
64 bytes from del12s10-in-f14.1e100.net (142.250.207.206): icmp_seq=11 ttl=128 time=13.0 ms
^C
— google.com ping statistics —
11 packets transmitted, 11 received, 0% packet loss, time 10020ms, the more you are able
rtt min/avg/max/mdev = 12.313/13.532/17.392/1.317 ms

```

ARP scan: ARP Scan is used to identify other active hosts on a local network.

```

(root@kali)-[/home/kali]
# arp-scan 192.168.64.0/24

Interface: eth0, type: EN10MB, MAC: 00:0c:29:44:e9:bb, IPv4: 192.168.64.142
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.64.1    00:50:56:c0:00:08    (Unknown)
192.168.64.2    00:50:56:e9:db:c2    (Unknown)
192.168.64.137  00:0c:29:92:e9:76    (Unknown)
192.168.64.138  00:0c:29:73:63:9b    (Unknown)
192.168.64.254  00:50:56:ec:5f:a3    (Unknown)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.861 seconds (137.56 hosts/sec). 5 responded

```

Ping Sweep: A Ping Sweep, also known as an ICMP Sweep or Ping Scan, enables simultaneous scanning of multiple systems on a server to gather information efficiently in a single operation.

```
(root@kali)-[/home/kali]
# nmap -sn 192.168.64.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 00:27 EDT
Nmap scan report for 192.168.64.1
Host is up (0.00016s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.64.2
Host is up (0.00044s latency).
MAC Address: 00:50:56:E9:DB:C2 (VMware)
Nmap scan report for 192.168.64.137
Host is up (0.00063s latency).
MAC Address: 00:0C:29:92:E9:76 (VMware)
Nmap scan report for 192.168.64.138
Host is up (0.00045s latency).
MAC Address: 00:0C:29:73:63:9B (VMware)
Nmap scan report for 192.168.64.254
Host is up (0.00070s latency).
MAC Address: 00:50:56:EC:5F:A3 (VMware)
Nmap scan report for 192.168.64.142
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.96 seconds
```

2. Port Scanning

Once the host's activity is confirmed, the user then proceeds to identify the operational ports and services within the network.

Different Techniques for Port Scanning

Full scan (nmap target ip): The command `nmap target_ip` performs a scan on a specified target IP address using its default settings. This typically involves identifying open ports, detecting the target's operating system, and possibly running services.


```
(root@kali)-[/home/kali]
# nmap 192.168.64.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 02:07 EDT
Nmap scan report for 192.168.64.138
Host is up (0.0095s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
```

TCP scan

Full scan (nmap -sT target ip): The command `nmap -sT target_ip` performs a TCP connect scan on the specified target IP address. This scan type attempts to establish a full TCP connection with each targeted port. It essentially completes the traditional three-way handshake process (SYN, SYN-ACK, ACK) used by TCP to initiate a connection. If the connection is successfully established, the port is considered open.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.64.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 02:32 EDT
Nmap scan report for 192.168.64.138
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
```

Half-scan/stealth scan

nmap -sS target ip: The command `nmap -sS target_ip` performs a SYN scan on the specified target IP address. This type of TCP scan is often referred to as a “half-open” scan because it doesn’t complete the TCP connection. It sends a SYN packet (indicating the start of a TCP connection) to the target. If the target port is open, it will respond with a SYN-ACK packet, after which Nmap sends an RST packet to close the connection before it’s fully established.

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.64.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 02:33 EDT
Nmap scan report for 192.168.64.138
Host is up (0.0048s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
```

FIN Scan

nmap -sF -target ip: The `nmap -sF target_ip` command performs a FIN scan using Nmap against the specified target IP address. A FIN scan sends TCP FIN packets to the target. According to TCP protocol standards, a closed port is expected to reply with an RST packet, while an open port will ignore the FIN packet. This behavior can be used to infer which ports are open.

```

(root@kali)-[/home/kali]
# nmap -sF -p81 192.168.64.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 02:34 EDT
Nmap scan report for 192.168.64.138
Host is up (0.00036s latency).

PORT      STATE SERVICE
81/tcp    closed hosts2-ns
MAC Address: 00:0C:29:73:63:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

```

UDP scan

nmap -sU target ip: The command `nmap -sU target_ip` uses Nmap to perform a UDP scan on a specified target. This scan type is designed to identify open UDP ports on the target system, which can help discover the services running on those ports.

```

Not shown: 993 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp    open  domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp    open  rpcbind
137/udp    open  netbios-ns
138/udp    open|filtered netbios-dgm
2049/udp   open  nfs
MAC Address: 00:0C:29:73:63:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1815.33 seconds

```

X-mas scan (nmap -sX -p80 ip): This command is used to identify open ports and detect potential vulnerabilities on a target machine's IP address.

```

(root@kali)-[/home/kali]
# nmap -sX -p80 192.168.64.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 03:19 EDT
Nmap scan report for 192.168.64.138
Host is up (0.00021s latency).

PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 00:0C:29:73:63:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds

```

3. Vulnerability scanning

Vulnerability scanning is a crucial cybersecurity process aimed at identifying security weaknesses and flaws in systems and the software running on them.

Nmap target IP --script vuln: This command instructs Nmap to scan the specified target IP address and utilize scripts from its vulnerability scanning suite (--script vuln).

```

# nmap 192.168.64.138 --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 03:23 EDT
Nmap scan report for 192.168.64.138
Host is up (0.00098s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:  CVE:CVE-2011-2523  BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)

```

```

1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|   State: VULNERABLE
|   - Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|   References:
|   - https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
5432/tcp open  postgresql

```

4. Operating System Fingerprinting

Operating System (OS) Fingerprinting is a technique used in network scanning and network management to determine the operating system of a remote computer. Active OS fingerprinting involves sending packets to a target and analyzing the responses. This method can provide detailed information about the target's OS but carries a higher risk of detection by intrusion detection systems (IDS), intrusion prevention systems (IPS), or firewalls.

`nmap -O target_ip`: The command `nmap -O target_ip` is used with Nmap to conduct an operating system detection scan on the specified target IP address. This option enables Nmap's OS detection feature, which uses a combination of TCP/IP stack fingerprinting techniques to guess the operating system running on the target machine. It sends a series of TCP and UDP packets to the target and examines the responses to determine characteristics unique to specific operating systems.

```

(root@kali)-[/home/kali]
# nmap -O 192.168.64.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 06:42 EDT
Nmap scan report for 192.168.64.136
Host is up (0.00053s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown

```



```
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::s
ver_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1,
Network Distance: 1 hop
```

5. Service and Version Scanning

Service and Version Scanning is a process used in network security and administration to identify the services running on the ports of a targeted system and to determine the specific versions of those services.

nmap -sV ip_address: The command `nmap -sV ip_address` is used with Nmap to perform a service version detection scan on the specified IP address.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.64.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 06:14 EDT
Nmap scan report for 192.168.64.138
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
```

6. Packet Crafting

Packet crafting is a technique used for probing firewall rule sets and finding entry points into targeted systems or networks by manually generating packets to test network behaviors and devices rather than using existing network traffic.

hping3 -A ip_address: The `hping3 -A ip_address` command is used to send ACK packets to a specified IP address using hping3, a command-line network tool. This can be utilized to test firewalls, ports, and network behavior under certain conditions. The `-A` option specifically indicates

that ACK packets will be sent, which is a part of the TCP handshake process, often used to see how a system responds to unsolicited TCP acknowledgments, aiding in network analysis and security testing.

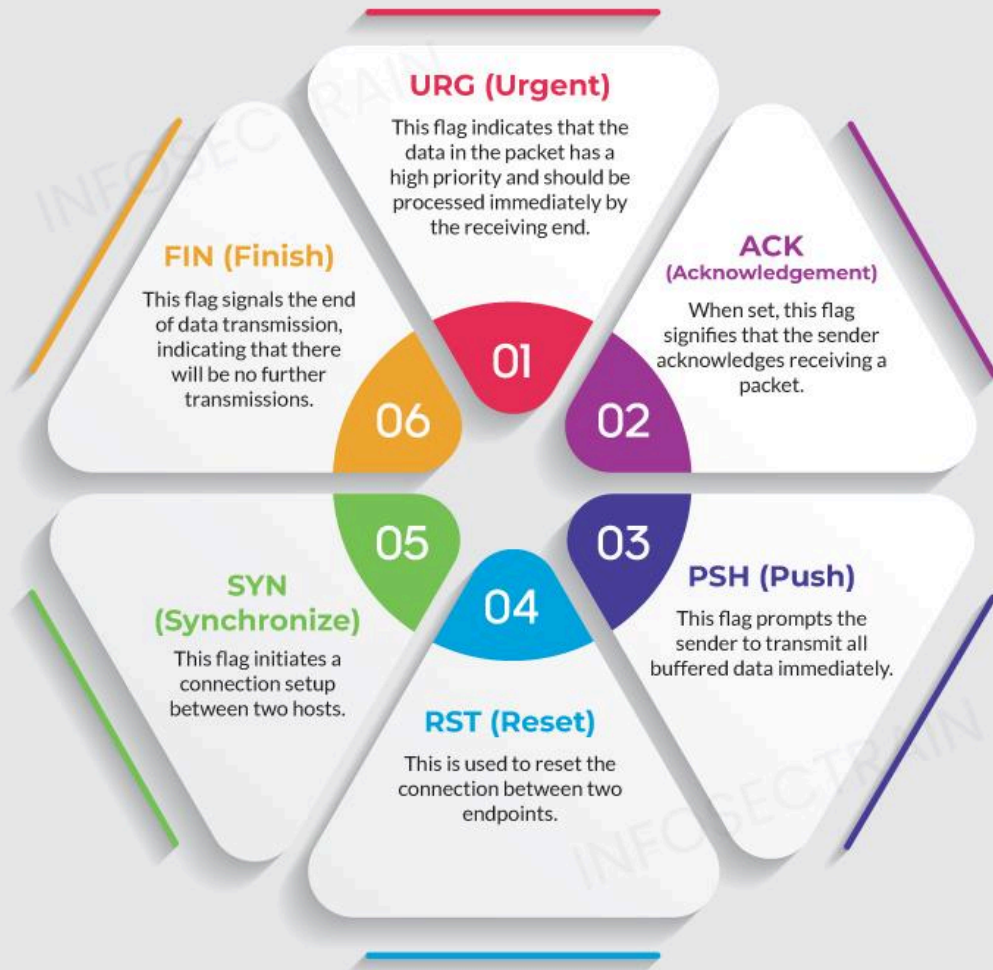
```
(root@kali)-[/home/kali]
# hping3 -A 192.168.64.138
HPING 192.168.64.138 (eth0 192.168.64.138): A set, 40 headers + 0 data bytes
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=0 win=0 rtt=14.9 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=1 win=0 rtt=14.7 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=2 win=0 rtt=14.6 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=3 win=0 rtt=15.1 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=4 win=0 rtt=15.7 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=5 win=0 rtt=15.6 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=6 win=0 rtt=15.5 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=7 win=0 rtt=16.3 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=8 win=0 rtt=14.0 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=9 win=0 rtt=14.5 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=10 win=0 rtt=15.1 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=11 win=0 rtt=15.3 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=12 win=0 rtt=16.3 ms
len=46 ip=192.168.64.138 ttl=64 DF id=0 sport=0 flags=R seq=13 win=0 rtt=15.8 ms
^C
— 192.168.64.138 hping statistic —
14 packets transmitted, 14 packets received, 0% packet loss
round-trip min/avg/max = 14.0/15.3/16.3 ms
```

Note: Advance Nmap users don't have to stick to just the standard scan options. The “--scanflags” feature with Nmap creates custom scans by choosing specific TCP flags. So what is a TCP flag?

What is a TCP Flag?

The TCP header includes flags crucial for managing data transmission over a TCP connection. Six control flags facilitate communication between hosts and provide directives to the system. The flags SYN, ACK, FIN, and RST initiate, sustain, and conclude a connection. The remaining two flags, PSH and URG, are used for specific system instructions. Each flag occupies a single bit, leading to a total of six bits for the TCP Flags section in the header. Setting a flag's value to '1' activates that particular flag.

TCP COMMUNICATION FLAG



TCP/IP Communication

Discovery, OS Discovery (Banner Grabbing/OS Fingerprinting).

Banner grabbing is a method used by attackers and security teams to obtain information about network computer systems and services running on open ports. A banner is a text displayed by a host that provides details such as the type and version of software running on the system or server. The screen displays the software version number on the network server and other system information, giving cybercriminals an advantage in cyber attacks. Banner grabbing considers collecting software banner information such as name and version. Hackers can use the OSINT tool to get the banners manually or automatically. Banner capture is one of the essential steps in both offensive and defensive penetration testing environments.

Types of Banner Grabbing:

Active Banner Grabbing: In this method, Hackers send packets to a remote server and analyze the response data. The attack involves opening a TCP or similar connection between the origin and the remote server. An Intrusion Detection System (IDS) can easily detect an active banner.

Passive Banner Capture: This method allows hackers and security analysts to get the same information while avoiding disclosing the original connection. In passive banner grabbing, the attackers deploy software and malware as a gateway to prevent direct connection when collecting data from the target. This technique uses third-party network tools and services to capture and analyze packets to identify the software and version being used. run on the server.

Usage:

Hackers can perform a banner-grabbing attack against various protocols to discover insecure and vulnerable applications and exploits. There are many services, protocols, and types of banner information that you can collect using banner grabbing. You can develop various methods and tools for the discovery process. In general, banner grab allows an attacker to discover network servers and services running along with their instances on open ports, as well as the operating system. Given the type and version of an application, a hacker, or pen tester, can quickly scan for known and exploitable vulnerabilities in that version.

Service Ports:

- Port 80 is running on Hypertext Transfer Protocol (HTTP) service.
- Port 21 is running on the File Transfer Protocol (FTP) service.
- Port 25 runs on the Simple Mail Transfer Protocol (SMTP) service.

Important Points:

- Banner Grabbing is used in Ethical Hacking to gather information about a target system before launching an attack.
- In order to gather this information, the Hacker must choose a website that displays banners from affiliate sites and navigate from the banner to the site served by the affiliate website.

- Banner Grabbing can be done through manual means or through the use of automated tools such as web crawlers, which search websites and download everything on them, including banners and files.

Banner grabbing

- Extracting information from a server's banner, such as the version of software running on it
- Can be used to gather information about a server's operating system, services, and network hosts
- Can be performed actively or passively
- Active methods involve sending packets to a server and analyzing the response
- Passive methods involve using third-party tools to capture and analyze packets

OS fingerprinting

- Determining the operating system of a remote computer on the internet
- Can be performed passively or actively
- Passive methods involve sniffing network packets traveling between hosts
- Active methods involve sending carefully crafted packets to the target machine

Tools

nmap: A network scanner that includes an OS detection module

Countermeasures:

- To avoid banner-grabbing attacks, companies can disable their banners on shady affiliate websites that are associated with known hacker forums where malicious tools are sold.
- Companies can also pay a fee to legitimate websites for their affiliate program to ensure that reputable and established sites will display the banners of the company in an attempt to target legitimate customers who would be interested in purchasing their product or service.
- Companies should always patch any software that they use, including antivirus programs and operating systems.

Enumeration is fundamentally checking. An attacker sets up a functioning associated with the objective host. The weaknesses are then tallied and evaluated. It is done mostly to look for assaults and dangers to the objective framework. Enumeration is utilized to gather usernames, hostname, IP addresses, passwords, arrangements, and so on. At the point when a functioning connection with the objective host is set up, hackers oversee the objective framework. They at that point take private data and information. Now and again, aggressors have additionally been discovered changing the

setup of the objective frameworks. How the connection is set up to the host decides the information or data the attacker will have the option to get to.

What is Enumeration?

Enumeration is the process of scanning a target system, network, or application and collecting information on it while in the process. This step is critical in the reconnaissance phase of [ethical hacking](#) or penetration testing where the aim is to find out some of the weaknesses within the target. Enumeration includes asking the system questions to get information such as usernames, machine names, shares, services, and other assets. The information that can be collected during the enumeration phase can be utilized by an attacker to understand the structure and security of the targeted system so that the attacker would understand what comes next.

Types Of Enumeration

In this section, we will be discussing the various types of Enumerations.

Aiming for a top All India Rank in [GATE CS/IT or GATE DA 2026](#)? Our courses, led by experts like **Khaleel Sir**, **Chandan Jha Sir**, and **Vijay Agarwal Sir**, offer **live classes**, **practice problems**, doubt support, quizzes, and **All India Mock Tests**—all in one place.

1. NetBIOS(Network Basic Input Output System) Enumeration

- NetBIOS name is an exceptional 16 ASCII character string used to distinguish the organization gadgets over TCP/IP, 15 characters are utilized for the gadget name and the sixteenth character is saved for the administration or name record type.
- Programmers utilize the NetBIOS enumeration to get a rundown of PCs that have a place with a specific domain, a rundown of offers on the individual hosts in the organization, and strategies and passwords.
- NetBIOS name goal isn't supported by Microsoft for Internet Protocol Version 6.
- The initial phase in specifying a Windows framework is to exploit the NetBIOS API. It was initially an Application Programming Interface([API](#)) for custom programming to get to LAN assets. Windows utilizes NetBIOS for document and printer sharing.
- A hacker who finds a Windows OS with port 139 open, can verify what assets can be gotten to or seen on the far off framework. In any case, to count the NetBIOS names, the distant framework probably empowered document and printer sharing. This sort of enumeration may empower the programmer to peruse or keep in touch with the distant PC framework, contingent upon the accessibility of offers, or dispatch a DoS.
- NetBIOS name list:

Name	NetBIOS Code	Type
<host name>	<00>	UNIQUE
<domain>	<00>	GROUP
<host name>	<03>	UNIQUE
<username>	<03>	UNIQUE
<host name>	<20>	UNIQUE

<domain>	<1D>	GROUP
<domain>	<1B>	UNIQUE

- **Nbtstat Utility:** In Windows, it shows NetBIOS over TCP/IP (NetBT) convention insights, [NetBIOS](#) name tables for both the neighborhood and distant PCs, and the NetBIOS name reserve. This utility allows a resuscitate of the NetBIOS name cache and the names selected with Windows Internet Name Service. The sentence structure for Nbtstat:

```
nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR]
[-s] [-S] [Interval]
```

The table appeared beneath shows different Nbtstat boundaries:

Parameters
-a RemoteName

-A IPAddress

-c

-n

-r

-RR

-s

-S

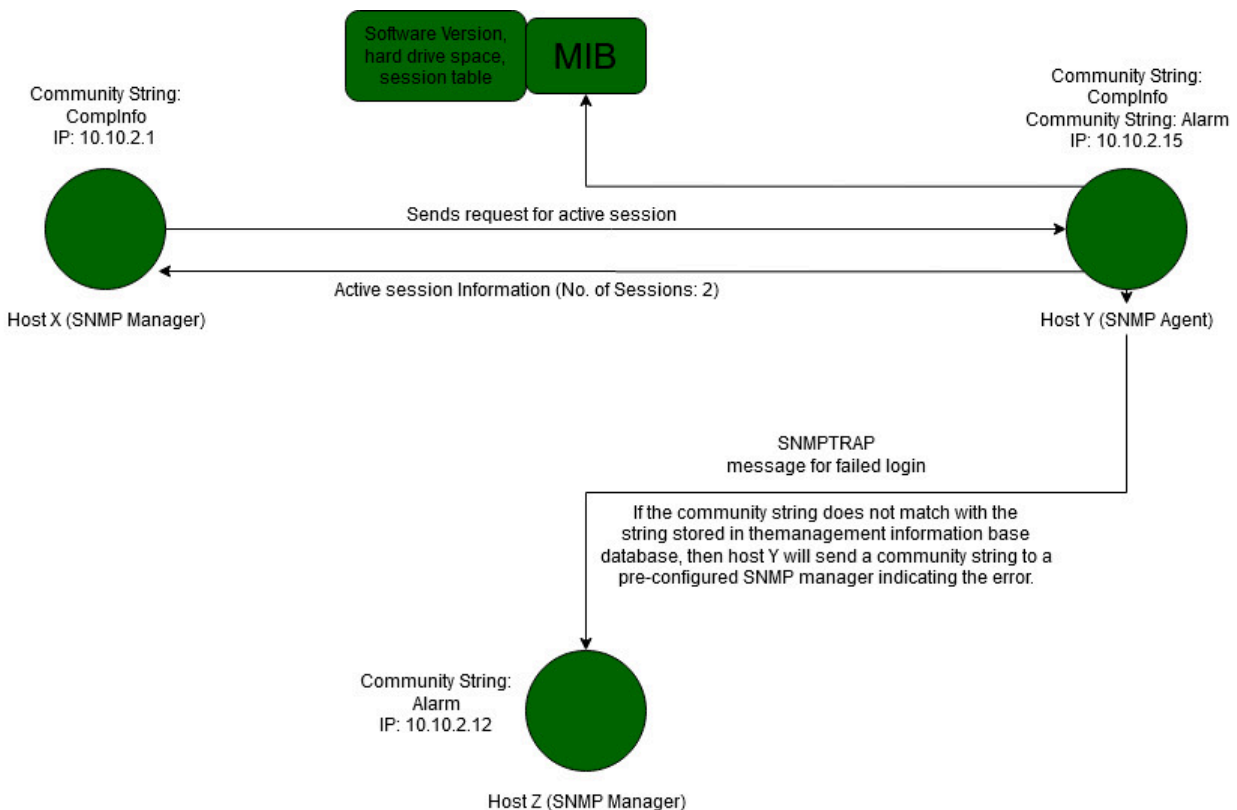
Interval

2. SNMP(Simple Network Management Protocol) Enumeration:

- SNMP enumeration is a cycle of specifying client records and gadgets on an objective framework utilizing SNMP. SNMP comprises a manager and a specialist. Specialists are inserted on each organization gadget, and the trough is introduced on a different PC.
- SNMP holds two passwords to get to and design the [SNMP](#) specialist from the administration station. Read Community String is public of course, permits review of gadget/framework setup. Read/Write people group string is private of course, permits far off altering of arrangement.
- Hackers utilize these default network strings to remove data about a gadget. Hackers list SNMP to remove data about organization assets, for example, has, switches, gadgets, shares, and so on, and network data, for example, ARP tables, directing tables, traffic, and so forth.
- SNMP utilizes dispersed engineering containing SNMP agents, managers, and a few related parts. Orders related with SNMP

include: GetRequest, GetNextRequest, GetResponse, SetRequest, Trap.

Given below is the communication between the SNMP agent and manager:



- SNMP Enumeration tools are utilized to examine a solitary IP address or a scope of IP addresses of SNMP empowered organization gadgets to screen, analyze, and investigate security dangers. Instances of this sort of instruments incorporate NetScanTolls Pro, SoftPerfect Network Scanner, SNMP Informant, and so forth

3. LDAP Enumeration:

- Lightweight Directory Access Protocol is an Internet Protocol for getting to dispersed registry administrations.
- Registry administrations may give any coordinated arrangement of records, regularly in a hierarchical and sensible structure, for example, a corporate email index.
- A customer starts an LDAP meeting by associating with a Directory System Agent on TCP port 389 and afterward sends an activity solicitation to the DSA.
- Data is sent between the customer and the worker utilizing Basic Encoding Rules.
- Programmer inquiries LDAP administration to assemble information such as substantial usernames, addresses, division subtleties, and so on that can be additionally used to perform assaults.
- There are numerous LDAP enumeration apparatuses that entrance the registry postings inside Active Directory or other catalog administrations. Utilizing these devices, assailants can identify data, for example, substantial usernames, addresses, division subtleties, and so forth from various LDAP workers.
- Examples of these kinds of tools include LDAP Admin Tool, Active Directory Explorer, LDAP Admin, etc.

4. NTP Enumeration:

- Network Time Protocol is intended to synchronize clocks of arranged PCs.
- It utilizes UDP port 123 as its essential method for correspondence.
- NTP can check time to inside 10 milliseconds (1/100 seconds) over the public web.
- It can accomplish correctness of 200 microseconds or better in a neighborhood under ideal conditions.
- Executives regularly disregard the NTP worker regarding security. Be that as it may, whenever questioned appropriately, it can give important organization data to the programmers.
- Hackers inquiries NTP workers to assemble significant data, for example, a list of hosts associated with NTP workers, Clients' IP addresses in an organization, their framework names and Oss, and Internal IPs can likewise be gotten if NTP worker is in the demilitarized zone.
- NTP enumeration tools are utilized to screen the working of SNTP and NTP workers present in the organization and furthermore help in the configuration and confirmation of availability from the time customer to the NTP workers.

5. SMTP Enumeration:

- Mail frameworks ordinarily use SMTP with POP3 and IMAP that empowers clients to spare the messages in the worker letter drop and download them once in a while from the mainframe.
- SMTP utilizes Mail Exchange (MX) workers to coordinate the mail through DNS. It runs on TCP port 25.
- SMTP provides 3 built-in commands: VRFY, EXPN, RCPT TO.
- These servers respond differently to the commands for valid and invalid users from which we can determine valid users on SMTP servers.
- Hackers can legitimately associate with SMTP through telnet brief and gather a rundown of substantial clients on the mainframe.
- Hackers can perform SMTP enumeration using command-line utilities such as telnet, netcat, etc., or by using tools such as Metasploit, [Nmap](#), NetScanTools Pro, etc.

6. DNS Enumeration using Zone Transfer:

- It is a cycle for finding the DNS worker and the records of an objective organization.
- A hacker can accumulate significant organization data, for example, DNS worker names, hostname, machine names, usernames, IPs, and so forth of the objectives.

- In DNS Zone Transfer enumeration, a hacker tries to retrieve a copy of the entire zone file for a domain from the DNS server.
- In order to execute a zone transfer, the hacker sends a zone transfer request to the DNS server pretending to be a client, the DNS then sends a portion of its database as a zone to you. This zone may contain a ton of data about the DNS zone organization.

7. IPsec Enumeration:

- IPsec utilizes ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange) to make sure about the correspondence between virtual private organization (VPN) end focuses.
- Most IPsec-based VPNs use the Internet Security Association and Key Management Protocol, a piece of IKE, to establish, arrange, alter, and erase Security Associations and cryptographic keys in a VPN climate.
- A straightforward checking for ISAKMP at the UDP port 500 can demonstrate the presence of a VPN passage.
- Hackers can research further utilizing an apparatus, for example, IKE-output to identify the delicate information including encryption and hashing calculation, authentication type, key conveyance calculation, and so forth.

8. VoIP(Voice over IP) Enumeration:

- VoIP uses the SIP (Session Initiation Protocol) protocol to enable voice and video calls over an IP network.
- SIP administration by and large uses UDP/TCP ports 2000, 2001, 5050, 5061.
- VoIP enumeration provides sensitive information such as VoIP gateway/servers, IP-PBX systems, client software, and user extensions.
- This information can be used to launch various VoIP attacks such as DoS, Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony, VoIP [phishing](#), etc.

9. RPC Enumeration:

- Remote Procedure Call permits customers and workers to impart in disseminated customer/worker programs.
- Counting RPC endpoints empower aggressors to recognize any weak administrations on these administration ports.
- In networks ensured by firewalls and other security establishments, this portmapper is regularly sifted. Along these lines, hackers filter high port reaches to recognize RPC administrations that are available to coordinate an assault.

10. Unix/Linux User Enumeration:

- One of the most vital steps for conducting an enumeration is to perform this kind of enumeration. This provides a list of users along with details like username, hostname, start date and time of each session, etc.
- We can use command-line utilities to perform Linux user enumeration like users, rwho, finger, etc.

11. SMB Enumeration:

- SMB list is significant expertise for any pen-tester. Prior to figuring out how to count SMB, we should initially realize what SMB is. SMB represents server message block.
- It's a convention for sharing assets like records, printers, by and large, any asset which should be retrievable or made accessible by the server. It fundamentally runs on port 445 or port 139 relying upon the server.
- It is quite accessible in windows, so windows clients don't have to arrange anything extra as such other than essential set up. In Linux in any case, it is somewhat extraordinary. To make it work for [Linux](#), you have to introduce a samba server since Linux locally doesn't utilize SMB convention.

- Clearly, some kind of confirmation will be set up like a username and secret word, and just certain assets made shareable. So dislike everybody can get to everything, a solid confirmation.
- The main evident defect is utilizing default certifications or effectively guessable and sometimes even no verification for access of significant assets of the server. Administrators should make a point to utilize solid passwords for clients who need to get to assets utilizing SMB. The subsequent blemish is the samba server. Samba servers are infamous for being hugely vulnerable.

Mitigation Of Different Types Of Enumeration

There are several countermeasures which can be taken into account for the mitigation of several kinds of enumeration:

1. NetBIOS Enumeration:

- Disable SMB and NetBIOS.
- Use a [network firewall](#).
- Prefer Windows firewall/ software firewalls.
- Disable sharing.

2. SNMP Enumeration:

- Eliminate the specialist or shut off the SNMP administration.

- In the event that stopping SNMP isn't a choice, at that point change the default network string names.
- Move up to SNMP3, which encodes passwords and messages.
- Actualize the Group Policy security alternative.

3. LDAP Enumeration:

- Utilize SSL technology to encrypt the traffic.
- Select a username unique in relation to your email address and empower account logout.

4. NTP Enumeration:

- Configure MD5 Layer.
- Configure NTP Authentication.
- Upgrade NTP version.

5. SMTP Enumeration:

- Ignore email messages to unknown recipients.
- Disable open relay feature.
- Breaking point the number of acknowledged associations from a source to forestall brute force exploits.
- Not to include sensitive mail server and localhost information in mail responses.

6. DNS Enumeration Using Zone Transfer:

- Incapacitate the DNS Zone moves to the untrusted hosts.
- Make sure that the private hosts and their IP addresses are not published in DNS zone files of the public DNS server.
- Use premium DNS regulation services that hide sensitive information such as host information from the public.
- Utilize standard organization administrator contacts for DNS enlistment to maintain a strategic distance from social designing assaults.
- Avoid publishing Private IP address information into the zone file.
- Disable Zone Transfer for untrusted hosts.
- Hide Sensitive information from public hosts.

7. IPsec Enumeration:

- Preshared keys utilized with both fundamental and forceful mode IKE key trade components are available to sniffing and disconnected savage power granulating assaults to bargain the shared mystery. You should utilize advanced testaments or two-factor validation components to refute these dangers.
- Pre-shared keys and forceful mode IKE uphold is a catastrophe waiting to happen. On the off chance that you should uphold forceful mode IKE, utilize advanced declarations for verification.

- Forcefully [firewall](#) and channel traffic coursing through VPN encrypted tunnel so that, in case of a trade-off, network access is restricted. This point is particularly significant while giving versatile clients network access, instead of branch workplaces.
- Where conceivable, limit inbound IPsec security relationship to explicit [IP addresses](#). This guarantees that regardless of whether an aggressor bargains a preshared key, she can only with significant effort access the VPN.

8. VoIP (Voice over IP) Enumeration:

- This hack can be smothered by actualizing SIPS (SIP over TLS) and confirming SIP queries and reactions (which can incorporate uprightness insurance).
- The utilization of SIPS and the verification of reactions can stifle many related hacks including [eavesdropping](#) and message or client pantomime.
- The utilization of digest confirmation joined with the utilization of TLS between SIP telephones and SIP intermediaries can give a station through which clients can safely validate inside their SIP domain.

- Voicemail messages can be changed over to message records and parsed by ordinary spam channels. This can just shield clients from SPIT voicemails.

9. RPC Enumeration:

- Try not to run rexd, users, or rwalld RPC administrations, since they are of negligible utilization and give aggressors both valuable data and direct admittance to your hosts.
- In high-security conditions, don't offer any RPC administrations to the public Internet. Because of the unpredictability of these administrations, almost certainly, zero-day misuse contents will be accessible to assailants before fixed data is delivered.
- To limit the danger of inner or confided in hacks against vital RPC administrations, (**for example**, NFS segments, including statd, lockd, and mountd), introduce the most recent seller security patches.
- Forcefully channel egress traffic, where conceivable, to guarantee that regardless of whether an assault against an RPC administration is effective, an associate back shell can't be brought forth to the [hacker](#).

10. Unix/Linux User Enumeration:

- Keep the kernel fixed and refreshed.

- Never run any service as root except if truly required, particularly the web, information base, and record mainframes.
- SUID digit ought not to be set to any program which lets you getaway to the shell.
- You should never set SUID cycle on any record supervisor/compiler/mediator as an aggressor can undoubtedly peruse/overwrite any documents present on the framework.
- Try not to give sudo rights to any program which lets you break to the shell.

11. SMB Enumeration:

- Impair SMB convention on Web and DNS mainframes.
- Debilitate SMB convention web confronting mainframes.
- Handicap ports TCP 139 and TCP 445 utilized by the SMB convention.
- Restrict anonymous access through the RestrictNull Access parameter from the Windows Registry.

How Enumeration Gives an Attacker Access to Sensitive Data?

Enumeration is a strong tool in the context of an adversary since the latter gets the possibility to collect as many specific data as possible in relation to

the object under attack. Once a connection with the target host is established, the attacker can extract sensitive data such as:

- **Username and Passwords:** Sometimes, through gaining knowledge of the passwords and username, an attacker can easily penetrate into several systems.
- **Network Shares and Resources:** Knowledge about shared folder, files and devices is good news to the attacker as they can take advantage of that or even gain further hold.
- **Configuration Settings:** Additional, one may discover misconfigurations in security settings that gives the attackers, potential points of entry.
- **System Architecture Details:** Getting to know the actual structure of the used system allows the attacker to better adapt in his actions.

The Enumeration Step of Security Testing

In security testing especially in penetration testing enumeration is an important phase that follows reconnaissance. In this phase, which often involves whistle blowing, testers escalate their function and seek to obtain as much information about the target system as they can. The end product is to look for the blind spots that can be exploited by a malicious user in order to compromise the system.

Key activities in the enumeration phase include:

- **Identifying User Accounts:** Finding legitimate usernames and if possible, the passwords to go with them.
- **Mapping Network Resources:** Identifying hidden resources, services and device on the network.
- **Extracting Configuration Data:** They involve collecting information on the settings of the system, established security policies as well as the security measures in place.
- **Detecting Running Services:** Gleaning service running and open ports which are potential gateway for an attack.

What is Vulnerability Assessment?

What is Vulnerability Assessment?

Last Updated : 20 Aug, 2024



Living in a world with more and more complex threats posted by cybercriminals, it is imperative that you shield your networks. A vulnerability scanning is done to understand areas that are prone to an attack by the invader before they exploit the system. The above measures not only protect data and guard against data leakage but also help meet security requirements and strengthen risk management. In this article, we'll look at what vulnerability assessment is, why it is important, and how it stands from penetration testing. We will also outline how the assessment is conducted, the provided tool, and key advantages and disadvantages.

What is a Vulnerability Assessment?

A vulnerability assessment is a procedure that is employed in an information system to determine and rate potential risks. It seeks to identify vulnerabilities that can be leveraged by an attacker to compromise the system and to employ tools and techniques that ensure that data confidentiality, integrity, and availability are achieved. This systematic review assists organizations in identifying security issues like [cross-site scripting \(XSS\)](#) and [SQL injection](#) before they can be leveraged.

Importance of Vulnerability Assessments

Vulnerability assessments are very important in the protection of information systems and data. They help by:

- **Preventing Data Breaches:** Directing single and exclusive attention to every risk in line with time and noticing the recurrent threats so as to treat them before they bring about expensive security invasions.
- **Ensuring Regulatory Compliance:** Conformity to the laws and evasion of the law.
- **Managing Risks:** Risk priority and risk control to improve the general shareholder's risk evaluation.
- **Enhancing Security Posture:** Periodic evaluations enhance security by making provisions of security to cater for emerging threats.
- **Cost-Effective Security:** This solution lowers the expensive costs associated with security incidents that occur when the vulnerabilities are not tended to as soon as they are identified.

Types of Vulnerability Assessments

- **Host Vulnerability Assessment:** Conducts analysis on the servers and host systems so as to expose and contain backend attacks.
- **Database Vulnerability Assessment:** Provides for the prevention of unauthorized access of data within the database in terms of confidentiality, integrity and availability.
- **Network Vulnerability Assessment:** Evaluates the security of networks with the aim of attainable protection against oncoming and existing network complexity.
- **Application Scan Vulnerability Assessment:** Scans application code for application level vulnerabilities in frontend and backend auto-mated tools.

Vulnerability Assessments vs Penetration Tests

Parameter	Vulnerability assessments	Penetration tests
Objective	Identification and evaluation of potential vulnerabilities	Real world attacks are simulated to exploit vulnerabilities

Methodology	Usage of manual techniques and automated systems to scan systems	Ethical hackers are involved who attempt to exploit vulnerabilities
Scope	Various aspects of the system are covered	Target specific vulnerabilities and attack vectors
Frequency	Conducted regularly as part of an ongoing strategy	Less frequent and is performed when needed
Focus	Gives a broader perspective of potential issues	Gives deeper insight into the impact of exploiting vulnerabilities
Approach	Proactive approach which helps prevent potential issues	Reactive approach which assess the effectiveness of existing security measures

How Does a Vulnerability Assessment Work?

- **Planning and Scoping:** Identify the parameters, aims and objectives and target system of the assessment.
- **Discovery:** Collect general information about the system: hosts, ports, and software, etc. Collect it with using specialized software and through manual assessment.
- **Scanning:** Make a scan to each host in order to detect open ports, mistakes or problems in configurations.
- **Analysis:** Analyze scan information to identify imperatives and determine their potential vulnerability.
- **Reporting:** Record exploits, their consequences and rank suggestions for insurance.
- **Remediation:** Apply remedies, modify settings and work on the fortification of the architecture.
- **Follow-Up:** Ensure fix and verify that fix is correct & look for new vulnerability.

How Does Vulnerability Assessment Help?

It helps any organization safeguard itself from cyber attacks by identifying the loopholes in advance. Here are some threats that we can prevent if we use vulnerability assessment.

- Injection attacks like XSS and SQL injection
- Authentication faults that lead to unidentified access to important data
- Insecure settings and weak defaults

The Process of Vulnerability Assessment

The process of Vulnerability Assessment is divided into four stages. Let us discuss them one by one.

- **Testing or Vulnerability Identification:** All the aspects of a system like networks, servers, and databases are checked for possible threats, weaknesses, and vulnerabilities. The goal of this step is to get a list of all the possible loopholes in the security of the system. The testing is done through machines as well as manually and all parameters are kept in mind while doing so.
- **Analysis:** From the first step, we get a list of vulnerabilities. Then, it is time that these are analyzed in detail. The goal of this analysis is to identify where things went wrong so that rectification can be done easily. This step aims at finding the root cause of vulnerabilities.
- **Risk Assessment:** When there are many vulnerabilities, it becomes important to classify them on the basis of risks they might cause. The main objective of this step is to prioritize vulnerabilities on the basis of data and systems they might affect. It also gauges the severity of attacks and the damage they can cause.
- **Rectification:** Once if have a clear layout of the risks, their root cause, and their severity, we can start making corrections in the system. The fourth step aims at closing the gaps in security by introducing new security tools and measures.

Tools for Vulnerability Assessment

Manually testing an application for possible vulnerabilities might be a tedious job. There are some tools that can automatically scan the system for vulnerabilities. A few such tools include:

- Simulation tools that test web applications.
- Scanners that test network services and protocols.
- Network scanners that identify malicious packets and defects in [IP addresses](#).

Advantages of Vulnerability Assessment

- Detect the weakness of your system before any data breach occurs.
- A list of all possible vulnerabilities for each device present in the system.
- Record of security for future assessments.

Disadvantages of Vulnerability Assessment

- Some advanced vulnerabilities might not be detected.
- Assessment tools might not give exact results.

How To Write a Vulnerability Assessment Report

Vulnerability assessment reports play a vital role in ensuring the security of an organization's applications, computer systems, and network infrastructure. The goal of a vulnerability assessment report is to highlight threats to an organization's security posed by vulnerabilities in its IT environment.

Creating a vulnerability assessment report involves analyzing an organization’s systems, diagnosing system vulnerabilities, and describing the severity of those vulnerabilities. These assessments are carried out by security professionals who utilize a range of automated and manual testing tools. With the help of a vulnerability assessment, companies can understand their security posture and take measures to eliminate risks (EC-Council, 2020).

Vulnerability scanning includes automated network and system scans. Testers can also use [penetration testing](#) to locate vulnerabilities and determine the severity of a given risk. In this article, we’ll explain the core elements of a vulnerability assessment report.

Six Critical Elements of a Vulnerability Assessment Report

Because your client and their security team usually won’t have the time to read long explanations, it’s important to keep your report clear and concise—without omitting crucial information. Remember that you can link to quality sources to help others better understand the contents of the report while avoiding long segments of unnecessary text.

The below table outlines the six key elements of a vulnerability assessment report (EC-Council, n.d.).

Element	Description
Executive summary	<ul style="list-style-type: none">• Date range of the assessment• Purpose and scope of the assessment• General status of the assessment and summary of your findings regarding risk to the client

-
- Disclaimer

Scan results

- Explanation of the scan results, such as how you've categorized and ordered vulnerabilities
- Overview of the types of reports provided

Methodology

- Tools and tests you used for vulnerability scanning, such as penetration testing or cloud-based scans
- Specific purpose of each scan, tool, and test
- Testing environments for each tool used in the assessment

Findings

- Which systems identified by the client you successfully scanned and which you did not
- Whether any systems were not scanned and, if so, the reasons why

Risk assessment

- Index of all vulnerabilities identified, categorized as critical, high, medium, or low severity
 - Explanation of the above risk categories
 - List of all vulnerabilities with details on the plugin name, description, solution, and count information
-

Recommendations

- Full list of actions the client should take
- Recommendations of other security tools the client can use to assess the network's security posture
- Security policy and configuration recommendations

What is System Hacking? Definition, Types and Processes

In the popular imagination, the term “hacking” is synonymous with system hacking, a growing concern in cybersecurity. While malicious actors try to break into a computer system, their ethical hacker counterparts work with companies to stop these attackers in their tracks. This article will discuss everything you need to know, including the definition of system hacking, the various steps of system hacking, and the role of system hacking in [ethical hacking](#). Learn ethical hacking with a [ethical hacking course](#).

System Hacking Explained in Brief

System hacking refers to using technical skills and knowledge to gain access to a computer system or network. Hackers employ many methods to get into a system by exploiting its vulnerabilities and concealing their activities to avoid detection.

Most people imagine system hacking as the work of so-called “black hat” or “gray hat” hackers who haven’t obtained the owner’s permission to enter the system. However, system hacking is also done by [ethical hackers](#) who received authorization beforehand to test the system’s security and improve any weaknesses.

The purpose of system hacking depends on the motivations of those who perform it. Malicious actors seek to exploit their discoveries after hacking into the system, usually for financial or political gain. Ethical hackers, however, are hired by companies as security consultants to help identify and fix vulnerabilities before these same malicious actors can exploit them.

How Malicious Actors Carry Out System Hacking

Malicious actors make use of multiple system hacking tools and techniques. System hacking software such as Nmap, Metasploit, Wireshark, and Acunetix help attackers detect and capitalize on vulnerabilities in the target system. Attackers may also use dedicated tools such as a phone hacking system for mobile devices.

Perhaps the best operating system for hacking is Kali Linux, a distribution of Debian Linux. Kali Linux has a wide range of security and penetration tools and is highly customizable, making it likely the best OS for hacking. Specific use cases such as Kali Linux wifi hacking can be executed through pre-installed tools such as Aircrack-ng.

The System Hacking Steps

System hackers generally follow a well-worn set of steps to gain and maintain access to a system. Below, we'll discuss each of the four system hacking steps in detail.

1. Gaining Access

First and foremost, system hackers must be able to access a system. This can be accomplished in multiple ways:

- **Password attack:** In perhaps the most basic technique, attackers can attempt to enter a system by entering the login credentials of a legitimate user. So-called "brute force" attacks try to guess a user's password by testing all possible combinations until the correct one is discovered.
- **Stolen credentials:** System hackers may already have a user's credentials, making it easy to access the system. For example, the user may have been tricked by a phishing email into divulging their password. Attackers also use databases of usernames and passwords exposed after a data breach, assuming that users reuse the same password for multiple systems.
- **Vulnerability exploitation:** New vulnerabilities are constantly being discovered in computer systems, while old ones may still be unpatched. Technically sophisticated attackers can exploit the vulnerabilities they discover

through techniques like [SQL injection](#), [cross-site scripting](#), and [buffer overflows](#).

2. Escalating Privileges

Once inside the computer or network, a system hacker may not be able to carry out the entire plan of attack right away. Instead, the hacker needs to exploit bugs or flaws in the system to gain additional privileges beyond those authorized initially. This process is known as privilege escalation.

There are two main types of privilege escalation: horizontal and vertical.

- In **horizontal privilege escalation**, the attacker initially gains access to a standard user's account before spreading throughout the network to other user accounts. These other accounts may have files, applications, and emails that will be useful in the attack.
- In **vertical privilege escalation**, the attacker seeks to possess a higher-level user account, such as one with administrator or root access. This access makes it much easier for hackers to continue their attacks undetected and launch more diverse attacks.

3. Maintaining Access

Even after gaining access to the system, hackers must work to maintain this access so that the attack isn't interrupted—or if it's interrupted, it can continue later.

For instance, the attackers may install keyloggers or spyware on a system to record the user's activities and keystrokes. By secretly capturing user credentials, attackers can re-enter the system later, even if the password is changed.

Another technique to maintain access is installing a backdoor: a hidden "portal" that allows hackers to bypass normal security controls and directly enter the system. This can be done through malware such as Trojan horses that appear innocuous and remain hidden for a long time.

4. Clearing Logs

Finally, system hackers must cover their tracks to prevent or delay their target from discovering the attack. One common practice is to [clear the system logs](#), which can provide crucial evidence that an attacker has gained unauthorized entry. Hackers may use tools such as Meterpreter to erase the proof of their movements throughout the network.

An additional essential step involves hackers deleting the history of the commands they've executed in shell programs such as Bash (for Linux) or the Windows shell. Without deleting these commands, victims could examine their shell history to reconstruct the attacker's actions precisely.


How to Prevent Your Systems From Being Hacked

Putting a stop to system hacking by malicious actors is a never-ending process, as new vulnerabilities are discovered, and new defenses are created. The security tips and best practices below will help you prevent your systems from being hacked:

- Require users to deploy strong passwords and multi-factor authentication, making it more difficult for attackers to gain access.
- Train and educate users in recognizing common attack techniques (e.g., phishing and [social engineering](#)).
- Install IT security applications such as antivirus and antimalware software, firewalls, and SIEM (security information and event management) tools.
- Keep up-to-date with the latest security patches for your software, firmware, and operating system.
- Join forces with ethical hackers who can help you detect system flaws without exploiting them. These individuals will scan your IT environment for vulnerabilities and suggest any actions that should be taken to patch them.

What is System Hacking in Ethical Hacking?

Last Updated : 30 Jun, 2022



System hacking is the process of exploiting vulnerabilities in electronic systems for the purpose of gaining unauthorized access to those systems. Hackers use a variety of techniques and methods to access electronic systems, including phishing, social engineering, and password guessing.

Purpose of System Hacking:

Generally, the motive of the hackers behind System Hacking is gaining access to the personal data of an individual or sensitive information belonging to an organization in order to misuse the information and leak it which may cause a negative image of the organization in the minds of people, [Privilege Escalation](#), Executing malicious applications to constantly monitor the system.

How this is carried out?

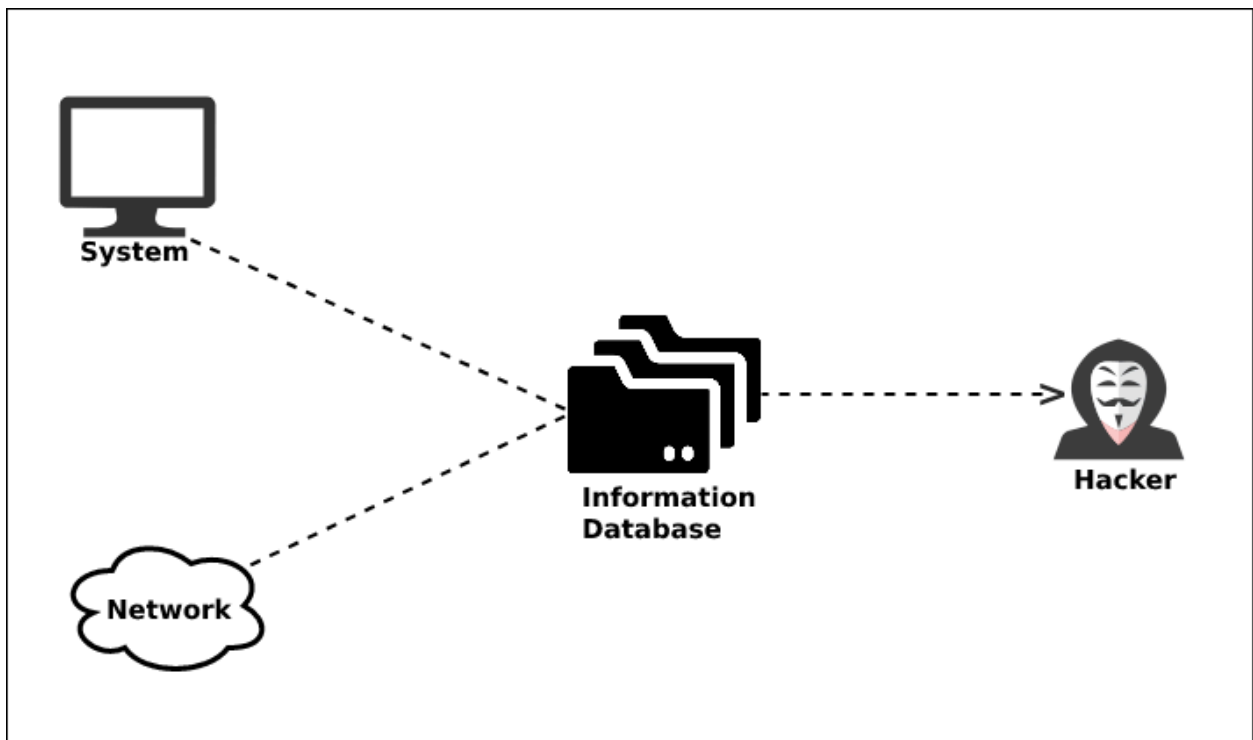
This type of hacking is generally done by a Hacker who has a lot of information regarding the System security, network, software, and how the system communicates with others in the network, often called [Footprinting](#) and [Reconnaissance](#). Then these hackers try numerous ways to carry out the attack but the common ways are:

- By deploying Viruses, Worms, Malware, Trojans
- Using phishing techniques
- Social Engineering

- Identifying and exploiting Vulnerability

Steps:

1. Reconnaissance: The first step in this type of Hacking is collecting information regarding the System's infrastructure, working, system's network. This step is very important as after this step the Hacker knows what attack to perform and how to gain access without leaving a trace.



2. Scanning: This step involves scanning the target System, which includes:

- **Vulnerability Scanning:** Checking vulnerabilities in the targeted system that can be exploited to gain access.

- **Mapping of Network:** Finding the working of the network, firewalls, routers, and systems connected to it.
- **Port Scanning:** Scanning the open ports, and services running over the System/Server.

3. Gaining Access: This is the phase in which the hacker breaks into the system and gains unauthorized access to the System/Network and then elevates his privileges to that of Administrator or SuperUser so he can play with the System files that a normal/Guest user is unable to access.

4. Maintaining the Access: After the Hacker enters the System he tries to maintain the connection with it in the background until he accomplishes the goal with which he entered it.

To know more about the phases of hacking please refer to the article [5 Phases of Hacking](#).

Prevention from Hacking:

- Using Firewall.
- Installing Anti-Virus and Anti-Spyware packages.
- Keeping the system up-to-date as security patches updates comes regularly.
- Be Aware of various phishing techniques.

Password Attacks and Countermeasures

