IMPORTANCE OF CYBER SECURITY

1. It helps in protecting all our data from theft and damage.
2. It helps in preventing unauthorized users from getting access to our network.
3. Protect companies against PHISHING schemes, ransom ware attacks and financial loss.
4. It helps in protecting the end users because our identities are online and it is manage by information technology.

DIFFERENT TYPES OF CYBER THREATS AND ATTACKS

1. Malware attacks: malicious software that infects or damages a device or network, such as ransom ware, Trojans, viruses, etc.
2. Social engineering attacks: manipulating or deceiving people into revealing sensitive information or performing harmful actions, such as phishing, spear phishing, whaling, etc.
3. Software supply chain attacks: compromising a software vendor or distributor to deliver malicious code to customers or users, such as the Solar Winds hack.
4. Advanced persistent threats (APT): stealthy and long-term attacks that target specific organizations or entities, such as nation-state actors or cybercriminals.
5. Distributed denial of service (DDoS) attacks: overwhelming a server or network with a large volume of traffic or requests, making it unavailable or slow for legitimate users.

THE CIA TRIAD

The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability.

The three letters “CIA” stands for Confidentiality, Integrity and Availability.

The CIA triad forms the basis for development of security systems.

They are mainly used to detect vulnerabilities and methods of creating solutions.

CONFIDENTIALITY

Simply means organizations ensuring that data and information is kept private and secured. Access to information is controlled and only authorized personnel can have access to such information. So steps have to be taken so that no unauthorized user can get access to such information or data.

INTEGRITY

It simply means making sure that your data is trustworthy and free from tampering.

For example if your company provides an information about a senior manager on your website such info must be accurate and must have integrity. If it is inaccurate, those visiting the website for information may feel your organization is not trustworthy. Someone with a vested interest in damaging the reputation of your organization may try to hack your website and alter the descriptions, photographs, or titles of the executives to hurt their reputation or that of the company as a whole.

AVAILABILITY

It simply means when data or information is needed it is readily available. It doesn’t make any sent in having confidentiality and integrity if information is needed it is not available .So systems, networks and applications must be functioning as they should.

NON REPUDIATION

It simply refers to the authenticity and integrity of a transaction or communication i.e. a sender cannot deny that he sent a message or information.  This concept refers to the ability to verify the source and authenticity of a message or action, preventing individuals from denying their involvement in a particular activity. By establishing a reliable system of non-repudiation, organizations can safeguard against fraud, disputes, and unauthorized access, ultimately bolstering trust and confidence in online interactions.

ETHICAL CONSIDERATIONS AND PROFESSIONAL ETHICS IN CYBER SECURITY

* Confidentiality: Cyber security professionals handle sensitive information and must maintain confidentiality.
* Threats and Risks: Cyber security professionals are duty-bound to respond to cyber threats.
* Balancing Security with business Interests: Cyber security professionals may encounter unethical practices within a business unit.
* Responsible Disclosure: Ethical hackers who discover vulnerabilities have an ethical obligation to disclose their findings responsibly.
* Informed Consent

INFORMATION GATHERING AND OPEN-SOURCE INTELLIGENCE (OSINT)

There are many examples of OSINT. Here are a few:

Social media: Social media platforms like Twitter, Facebook, and LinkedIn can be used to gather information about individuals and organizations 1.

Public records: Public records such as court documents, property records, and business filings can be used to gather information about individuals and organizations 1.

News articles: News articles can be used to gather information about current events, individuals, and organizations 1.

Government reports: Government reports can be used to gather information about public policy, government activities, and other topics 1.

Satellite imagery: Satellite imagery can be used to gather information about physical locations and infrastructure .

CYBER SECURITY FRAME WORKS

 It is a set of standards and practices that organizations follow to reduce cyber security risks. They help the company to identify its weak spots that might lead to data breaches and cyber-attacks.

1. Identifying the threat.
2. Protecting the organization from attacks.
3. Detecting attacks.
4. Responding to the attacks.
5. Recovering from the attack and returning the compromised devices back to work.

NIST

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

## **1. Identify**

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

## **2. Protect**

* Control who logs on to your network and uses your computers and other devices.
* Use security software to protect data.
* Encrypt sensitive data, at rest and in transit.
* Conduct regular backups of data.
* Update security software regularly, automating those updates if possible.
* Have formal policies for safely disposing of electronic files and old devices.
* Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

## **3. Detect**

Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.

## **4. Respond**

### **Have a plan for:**

* Notifying customers, employees, and others whose data may be at risk.
* Keeping business operations up and running.
* Reporting the attack to law enforcement and other authorities.
* Investigating and containing an attack.
* Updating your cybersecurity policy and plan with lessons learned.
* Preparing for inadvertent events (like weather emergencies) that may put data at risk.

## **. Recover**

### **After an attack:**

Repair and restore the equipment and parts of your network that were affected.

Keep employees and customers informed of your response and recovery activities.

# ISO

ISO 27001 is the internationally recognized standard for cybersecurity and aims to assist organizations with protecting their information assets while also complying with relevant legal and regulatory requirements.

The framework defines the requirements for establishing, implementing, and managing an information security management system (ISMS). The framework enables organizations to adopt an ongoing risk management process, identify and assess information security risks and implement appropriate controls to mitigate them. ISO 27001 bolsters organizational resilience against security incidents, maintaining operations by encouraging incident response and business continuity plans for prompt recovery and minimal disruptions.

REGULATIONS, STANDARDS, AND LEGISLATIONS: GDPR, HIPAA, PCI  
DSS, FISMA

# GDPR

The General Data Protection Regulation (GDPR)

In 2016, the General Data Protection Regulation (GDPR) was implemented to enhance data security measures and practices for European Union (EU) citizens. This regulation affects all organizations situated in the EU or any enterprise that gathers and retains private information of EU citizens, encompassing U.S. businesses as well.

The framework consists of 99 provisions related to a firm's obligations to adhere to compliance, such as the rights of consumers to access their data, policies and processes for safeguarding data, mandatory data breach notifications (e.g. organizations must inform their national regulatory authority within 72 hours after detecting a breach).

# HIPAA

### Health Insurance Portability and Accountability Act (HIPAA)

HIPAA acts as a cybersecurity framework mandating healthcare institutions to establish measures for safeguarding and preserving the confidentiality of digital health data. According to HIPAA, besides proving adherence to cyber risk management best practices, like employee training, businesses in the industry also need to carry out risk evaluations to control and detect emerging threats.

# FISMA

### The Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) serves as an all-encompassing cybersecurity structure that safeguards federal government data and systems from cyber dangers. Additionally, FISMA encompasses third parties and contractors working for federal agencies.

Closely adhering to NIST standards, the FISMA structure mandates that agencies and third parties keep a record of their digital resources and recognize any connections between networks and systems. Critical data must be classified based on risk, and security measures have to adhere to minimum security criteria as outlined by FIPS and NIST 800 guidelines. Affected organizations are also required to carry out cybersecurity risk evaluations, yearly security audits, and consistently oversee their IT framework.

# PCI DSS

PAYMENT CARD INDUSTRY SECURITY STANDARD (PCI DSS)

PCI DSS stands for Payment Card Industry Data Security Standard. This compliance framework is an industry-mandated **set of standards** intended to keep consumers' card data safe when it is used with merchants and service providers. It is administered by the PCI Security Standards Council (PCI SSC), founded by leading payment card companies such as American Express, Discover, Mastercard, and Visa.

Although compliance with the standards put forth in the PCI DSS is not required of businesses by governments, the card companies that control these standards may levy fines against organizations that do not comply.

PCI DSS applies to all organizations, including merchants, banks, processors, developers, and more, that store, process, or transmit cardholder data. Actual validation of DSS compliance may not be necessary for those below a set threshold of annual transactions and may also depend on which payment cards you intend to accept at your place of business. Each PCI SSC founding member **has its own** compliance program to protect their cardholders’ data and should be contacted directly for specific requirements.

# TCP/IP BASICS

TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP)

## What Does TCP/IP Do?

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

## What is the Difference between TCP and IP?

[TCP](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/) and[IP](https://www.geeksforgeeks.org/what-is-an-ip-address/) are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.

## How Does the TCP/IP Model Work?

Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender’s end and the same packets have to be recombined at the receiver’s end to form the same data, and this thing happens to maintain the accuracy of the data. TCP/IP model divides the data into a 4-layer procedure, where the data first go into this layer in one order and again in reverse order to get organized in the same way at the receiver’s end.

OSI MODEL

OPEN SYSTEM INTERCONNECTION (OSI)

## What Is the OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

The seven OSI layers:

1. Physical layer: The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.
2. **Data link layer:** The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control(MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.
3. **Network Layer:** The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.
4. **Transport Layer:** The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.
5. **Session Layer:** The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.
6. **Presentation Layer:** The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.
7. **Application Layer:** The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS)

SCANNING METHODOLOGIES AND STARTEGIES

Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of the Hacker). Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks. This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms. So a pen-tester and ethical hacker list down all such vulnerabilities found in an organization's network.

Scanning is of three types:

1. Network Scanning.
2. Port Scanning
3. Vulnerability Scanning.

Objectives of Network Scanning:

1. To discover live hosts/computer, IP address, and open ports of the victim.
2. To discover services that are running on a host computer.
3. To discover the Operating System and system architecture of the target.
4. To discover and deal with vulnerabilities in Live hosts.

Scanning Methodologies:

1. Hackers and Pen-testers check for Live systems.
2. Checking for open ports.
3. Scanning beyond IDS (Intrusion Detection System)
4. Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports.
5. Scan for vulnerability
6. Prepare Proxies.

# . Port Scanning

It is a conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system. During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology. Once the Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab. Amap is a tool to perform port scanning.

Scanning techniques mainly used :

1. SYNScan: SYN scan or stealth doesn't complete the TCP three-way handshake technique.  A hacker sends an SYN packet to the victim, and if an SYN/ACK frame is received back, then the target would complete the connection, and the port is in a position to listen. If an RST is retrieved from the target, it is assumed that the port is closed or not activated. SYN stealth scan is advantageous because a few IDS systems log this as an attack or connection attempt.
2. XMASScan: XMAS scan send a packet which contains URG (urgent), FIN (finish) and PSH (push) flags. If there is an open port, there will be no response; but the target responds with an RST/ACK packet if the port is closed. (RST=reset).
3. FINScan: A FIN scan is similar to an XMAS scan except that it sends a packet with just the FIN (finish) flag and no URG or PSH flags. FIN scan receives the same response and has the same limitations as XMAS scans.
4. IDLEScan: An IDLE scan uses a spoofed/hoax IP to send the SYN packet to the target by determining the port scan response and IP header sequence number. Depending on the response of the scan, the port is determined, whether open or closed.
5. Inverse TCP Flag Scan: Here, the attacker sends TCP probe packets with a TCP flag (FIN, URG PSH) or no flags. If there is no response, it indicates that the port is open, and RST means it is closed.
6. ACK Flag Probe Scan: Here, the attacker sends TCP probe packets where an ACK flag is set to a remote device, analyzing the header information (TTL and WINDOW field). The RST packet signifies whether the port is open or closed. This scan is also used to check the target's/victim's filtering system.

# VULNERABILITY SCANNING

It is the proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited or threatened. I this case, the computer should have to be connected to the internet.

* Testing Controls.
* Identifying Weak Points.
* Determining Current Security Posture

Countermeasures Against Scanning

1. Configure firewalls and IDS to detect and block probes.
2. Use custom rules to lock down the network and block unwanted ports.
3. Run port Scanning tools to determine whether the firewall accurately detects the port scanning activities.
4. Security Experts should ensure the proper configuration of anti-scanners and anti-spoofing rules.
5. Security experts of an organization must also ensure that the IDS, routers, and firewall firmware are updated to their latest releases.

DIFFERENCIATING BETTWEEN VULNERABILITY ANALYSIS AND PENETRATION TESTING

A vulnerability assessment is the process of identifying IT security weaknesses in your network, operating systems, firewalls, and hardware, and then taking steps to fix them.

Penetration testing, also known as “pen testing,” is an intentional, simulated cyberattack against your IT systems to find vulnerabilities and test the efficacy of cybersecurity controls.

The two terms may seem interchangeable, but differences exist. So what is penetration testing, and how does it differ from vulnerability assessment?

**In three ways, primarily:**

* Breadth versus depth
* Automated versus manual
* Degree of skill needed

## Breadth Versus Depth

The main difference between vulnerability assessment and penetration testing is coverage: breadth versus depth.

A vulnerability assessment goes wide, attempting to uncover as many weaknesses as it can find with the goal of remediation. A pen test goes deep by simulating an attack on a particular system to examine the network environment, test defenses, and exploit flaws.

One (vulnerability assessment) is like a thief casing a neighborhood to see which houses offer the best possibility of intrusion. The other (penetration testing) is a high-end cat burglar breaking into one specific house.

## Automated Versus Manual

Another difference is the degree of automation. Vulnerability assessments typically use automated vulnerability scan tools, which allow for broader coverage. Penetration testing uses a mix of automated tools and manual techniques, which helps to dig deeper into the weakness.

## Degree of Skill Needed

Thanks to automation, vulnerability assessments don’t require as much skill as penetration testing. This means that most in-house cybersecurity teams can run the tests themselves. (Organizations also contract with third-party service providers to conduct the scans.)

Penetration testing, however, requires a greater degree of expertise because it relies on manually intensive techniques. Typically, organizations outsource the task to qualified pen testers (also known as “ethical hackers”).

In summary, a vulnerability assessment answers the question, “What are our weaknesses, and how do we fix them?” Penetration testing answers the question, “Can someone break in, and what can that attacker get access to?”

Despite the differences, the goal of both methods is to identify potential threats and keep organizations safe from cyberattack.

VULNERABILITY SCANNING TOOLS WITH NMAP, INVICTI, AND OpenVAS

Nmap

Nmap(Network Mapper) is a free and open source utility for discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest.

Nmap is ...

* **Flexible**: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many [port scanning](https://nmap.org/book/man-port-scanning-techniques.html) mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more.
* **Powerful**: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
* **Portable**: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
* **Easy**: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A *targethost*". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
* **Free**: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks.
* **Well Documented**: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book!
* **Supported**: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users.
* **Acclaimed**: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series.
* **Popular**: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc.). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

**OpenVAS**

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.  
The scanner obtains the tests for detecting vulnerabilities from a [feed](https://www.greenbone.net/en/feed-comparison/) that has a long history and daily updates.

OpenVAS has been developed and driven forward by the company Greenbone since 2006. As part of the commercial vulnerability management product family Greenbone Enterprise Appliance, the scanner forms the Greenbone Community Edition together with other open-source modules.

The main scanner OpenVAS Scanner is a full-featured scan engine that executes Vulnerability Tests(VTs) against target systems. For this, it uses the daily updated and comprehensive feeds: the full-featured, extensive, commercial [Greenbone Enterprise Feed](https://greenbone.github.io/docs/latest/glossary.html#term-Greenbone-Enterprise-Feed) or the free available Greenbone Community Feed.

INVICTI (FORMERLY KNOWN AS NETSPARKER)

1. AUTOMATION

Automate security throughout your SDLC (secure software development life cycle.

* Automate security tasks and save your team hundreds of hours each month.
* Identify the vulnerabilities that really matter — then seamlessly assign them for remediation.
* Help security and development teams get ahead of their workloads — whether you run an AppSec, DevOps, or DevSecOps program.

VISIBILTY

Seeing the complete picture of your application.

* Find all your web assets — even ones that have been lost, forgotten, or created by rogue departments.
* Scan the corners of your apps that other tools miss with our unique dynamic + interactive (DAST + IAST) scanning approach.
* Always know the status of your remediation efforts, through Invicti or native integrations with your issue tracking and ticketing software.

PROVEN ACCURACY

Finding other vulnerabilities other tools miss.

* Find more true vulnerabilities with our unique dynamic + interactive (DAST + IAST) scanning approach.
* Let no vulnerability go unnoticed with combined signature and behavior-based testing.
* Detect vulnerabilities quickly with comprehensive scanning that doesn’t sacrifice speed or accuracy.

SCALABILTY

Managing risk like a team 10X times your size.

* Reclaim the hundreds of hours your team spends chasing down false positives with features that confirm which vulnerabilities are real threats.
* Integrate security testing into your entire SDLC with powerful two-way integrations into the tools your development team already uses.
* Control permissions for unlimited users — no matter how complex your organization’s structure.

PROACTIVE SECURITY

Preventing vulnerabilities by producing more secure codes

* Build security into your culture by integrating Invicti into the tools and workflows your developers use daily.
* Give developers access to actionable feedback that helps them produce more secure code — which means less work for your security team.
* Prevent delays with continuous scanning that stops risks from being introduced in the first place.

MANUAL VS AUTOMATED VULNERABILITY ASSESSMENT

## What is Penetration Testing?

Penetration Testing is the process of evaluating the security of a system by finding and exploiting vulnerabilities with the help of hacker-like tactics.

It is analogous to finding the ways of breaking into a house, then assessing how many rooms were accessible from each break-in point, how easy it was to break, and how much worth of valuables could be stolen in course of the operation.

The main difference between a hack and a penetration test is that hackers break in to steal actually cause harm, and penetration testers make you aware of the exploitable flaws in your security and help you fix them.

## What is Manual Penetration Testing?

Manual penetration testing is the process where security engineers manually perform penetration testing to assess the security posture of a system. They use hacker-style techniques to find ways to break into your system, evaluate the vulnerabilities in terms of impact and exploitability, and prepare a report documenting the vulnerabilities and the way to reproduce and fix them.

### This is what a manual penetration testing process looks like

* The security experts prepare a running profile of attack methods that can be used against a target system.
* They prepare test cases and execute them in a way that detects software vulnerabilities without affecting the business functionalities that might be active on the target system.
* After that they customize attack payloads for specific applications and execute them while taking note of the environment.
* They perform an analysis of the data captured through the operation to attain vulnerability patterns, interpret the results, and prepare a plan for remediating the issues.

## What is an Automated Penetration Testing?

Automated penetration testing refers to the scanning of your systems for common vulnerabilities with the help of automated tools and processes. It is a faster, and comparatively cheap process that can give you a quick analysis of your website’s or network’s vulnerability status.

ADVANTAGES OF MANUAL VULNERABILITY TESTING

* 1. **Zero False Positives**: If you have dealt with vulnerability scanners, or if you are a security aware person in general, you would know how big a deal false positives can be. The real pain of false positives is felt by the developers wasting hours trying to fix an issue that does not exist.
  2. **Deep and Exhaustive Testing:**Automated vulnerability scanners have become really smart over the last decade with regularly expanding test cases. But let’s face the fact, they still miss vulnerabilities. You cannot have a definitive vulnerability report without a manual pentest
  3. **A Thorough Pentest Report**: Security engineers who have run a manual penetration testing of your systems can produce a detailed report with step-by-step guidelines for you to reproduce and fix vulnerabilities. Moreover, you get their assistance while trying to fix the issues.
* **4. Compliance**: Some compliance regulations like the PCI-DSS require manual penetration testing. What Are Some Key Differences Between Automated and Manual Penetration Testing?

UNDERSTANDING SOCIAL ENGINEERING TTP AND PREVENTION

What is social engineering: Social engineering is the psychology of persuasion, it targets the mind and aims to get the trust of targets so that they can lower there guard, and then encourage them into taking unsafe actions such as divulging personal information, clicking on web links or opening attachments that may be malicious.

HOW DOES SOCIAL ENGINEERING WORK :

A cybercriminal will communicate with the intended victim by saying they are from a trusted organization. In some cases, they will even impersonate a person the victim knows.

If the manipulation works (the victim believes the attacker is who they say they are), the attacker will encourage the victim to take further action. This could be giving away sensitive information such as passwords, date of birth, or bank account details. Or they might encourage the victim to visit a website where malware is installed that can cause disruptions to the victim's computer. In worse case scenarios, the malicious website strips sensitive information from the device or takes over the device entirely.

### **Why is social engineering so dangerous?**

One of the greatest dangers of social engineering is that the attacks don't have to work against everyone: A single successfully fooled victim can provide enough information to trigger an attack that can affect an entire organization.

### **How do I protect myself and my organization against social engineering?**

* Password management: Guidelines such as the number and type of characters that each password must include, how often a password must be changed, and even a simple rule that employees should not disclose passwords to anyone--regardless of their position--will help secure information assets.
* Multi-factor authentication: Authentication for high-risk network services such as modem pools and VPNs should use multi-factor authentication rather than fixed passwords.
* Email security with anti-phishing defenses: Multiple layers of email defenses can minimize the threat of phishing and other social-engineering attacks. Some email security tools have anti-phishing measures built in.

## **Types of social engineering attacks**

### **Phishing**

Phishing scams are the most common type of social engineering attack. They typically take the form of an email that looks as if it is from a legitimate source. Sometimes attackers will attempt to coerce the victim into giving away credit card information or other personal data. At other times, phishing emails are sent to obtain employee login information or other details for use in an advanced attack against their company. Cybercrime attacks such as advanced persistent threats (APTs) and ransomware often start with phishing attempts.

WHALING

Whaling scams are the targeting of senior management staffs.

VISHING

Vishing scams is simply using voice channels to fool there targets.

SMISHING

Smishing scams are using text messages to fools or convince unsuspecting target.

SPAM, HOAXES, AND PREPENDING

Spam

* Unsolicited emails.
* Email address harvesting.
* Spam over internet messaging (SPIM).

Hoaxes (Antivirus)

* Delivered as spam or malware.
* Phone based scams.

Prepending

* Tagging email subject line.
* Can be used by threat actors as a consensus or urgency technique.
* Can be added by mail to warm users

### **Watering hole attacks**

Watering hole attacks are a very targeted type of social engineering. An attacker will set a trap by compromising a website that is likely to be visited by a particular group of people, rather than targeting that group directly. An example is industry websites that are frequently visited by employees of a certain sector, such as energy or a public service. The perpetrators behind a watering hole attack will compromise the website and aim to catch out an individual from that target group. They are likely to carry out further attacks once that individual's data or device has been compromised.

### **Business email compromise attacks**

Business email compromise (BEC) attacks are a form of email fraud where the attacker masquerades as a C-level executive and attempts to trick the recipient into performing their business function, for an illegitimate purpose, such as wiring them money. Sometimes they go as far as calling the individual and impersonating the executive.

### **Physical social engineering**

When talking about cybersecurity, we also need to talk about the physical aspects of protecting data and assets. Certain people in your organization--such as help desk staff, receptionists, and frequent travelers--are more at risk from physical social engineering attacks, which happen in person.

Your organization should have effective physical security controls such as visitor logs, escort requirements, and background checks. Employees in positions at higher risk for social-engineering attacks may benefit from specialized training from physical social engineering attacks.

### **USB baiting**

USB baiting sounds a bit unrealistic, but it happens more often than you might think. Essentially what happens is that cybercriminals install malware onto USB sticks and leave them in strategic places, hoping that someone will pick the USB up and plug it into a corporate environment, thereby unwittingly unleashing malicious code into their organization.

### **DNS Spoofing and Cache Poisoning Attacks**

**DNS spoofing** manipulates your browser and web servers to travel to malicious websites when you enter a legitimate URL. Once infected with this exploit, the redirect will continue unless the inaccurate routing data is cleared from the systems involved.

**DNS cache poisoning attacks** specifically infect your device with routing instructions for the legitimate URL or multiple URLs to connect to fraudulent websites.

### **Worm Attacks**

The cybercriminal will aim to attract the user’s attention to the link or infected file – and then get the user to click on it.

Examples of this type of attack include:

* **The LoveLetter worm** that overloaded many companies’ email servers in 2000. Victims received an email that invited them to open the attached love letter. When they opened the attached file, the worm copied itself to all of the contacts in the victim’s address book. This worm is still regarded as one of the most devastating, in terms of the financial damage that it inflicted.
* **The Mydoom email worm** — which appeared on the Internet in January 2004 — used texts that imitated technical messages issued by the mail server.
* **The Swen worm** passed itself off as a message that had been sent from Microsoft. It claimed that the attachment was a patch that would remove Windows vulnerabilities. It’s hardly surprising that many people took the claim seriously and tried to install the bogus security patch — even though it was really a worm.

## **How Does Social Engineering Work?**

Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data.

The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows:

1. **Prepare** by gathering background information on you or a larger group you are a part of.
2. **Infiltrate** by establishing a relationship or initiating an interaction, started by building trust.
3. **Exploit the victim** once trust and a weakness are established to advance the attack.
4. **Disengage** once the user has taken the desired action.

PREVENTION OF SOCIAL ENGINEERING ATTACKS

1. Creating awareness and educating yourself and others.

1. Be aware of the information you are releasing.
2. Keep your software up to date.
3. Screen any and every individual you share information with.

### Install and maintain anti-virus software, firewalls and email filter.