MCA 205B – CYBER SECURITY

UNIT I

History of Cyber Security-Introduction to Cyber Security-Definition-Key terms-cyber Attacks and Security tools-Security Threats-Vulnerability assessments-roles in Security-Cyber Security-today- Critical Thinking in Cyber Security

UNIT II

Cyber Threat Actors and their Motives-Security Attacks, Actors and their Motive-A brief overview of types of actors and their motives-Hacking organizations-Major different types of cyber-attack-Security Attack Definition-Security services-Security Mechanisms-Network Security Model-Organizational Threats-Attacks-Security Architecture Attacks-Security Architecture -Attack models-Malware and Ransomware-Threat Examples-Threat Protection Defined-Internet Security Threats – Mapping-Internet Security Threats - Packet Sniffing-Security Threat - IP Spoofing-Security Threats - Denial of service-Security Attacks - Host insertions-What is Social Engineering, Phishing and Vishing- Cyber warfare

UNIT III

Overview of Cyber Security Concepts-CIA Triad – Confidentiality-CIA Triad – Integrity-CIA Triad – Availability-Non - Repudiation - How does it apply to CIA?-Access Management-Incidence Response-Key Concepts - Incident Response-Incident Response Process-Introduction to Frameworks and Best Practices-IT Governance Process-Cybersecurity Compliance and Audit Overview-Pentest Process and Mile 2 CPTE Training-OWASP framework

UNIT IV

Introduction to Key Security Tools -Introduction to Firewall-Firewalls - Packet Filtering-Firewalls - Application Gateway-Firewalls - XML Gateway-Firewalls -

Stateless and Stateful- Firewall Administration – Firewall Selection-Firewall Administration – Firewall Configuration-IDPS Administration-VPN Administration-Antivirus/Antimalware-Penetration Testing Introduction-Penetration test Methodologies-Vulnerability Tests

UNIT V

Cyber Security –Organizational implications-cost of cybercrimes and IPR issues Web threats for organizations: the evils and Perils-Social media marketing Security and privacy Implications- Digital Forensic- Protecting people privacy in the organizations Forensic best practices for organizations. Case Studies.

Text Books

1. Nina Godbole & Sunit Belapure "Cyber Security", Wiley India, 2012.
2. Cyber Security by Paul Augustine, Crescent Publication
3. Information Security Policies, Procedures, and Standards: Guidelines for Effective

Information Security Management, Thomas Peltier, Auerbach Publication

References:

1. Harish Chander, "cyber laws & IT protection", PHI learning pvt.ltd, 2012.

2 MS.M.K. Geetha & Ms. Swapna Raman" Cyber Crimes and Fraud Management, "MACMILLAN,2012.

3.Pankaj Agarwal : Information Security& Cyber Laws (Acme Learning), Excel, 2013.

Lecture Notes

Unit-1

Introduction to cyber Security

Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber attackers. It is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.

It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification, or unauthorized access. Therefore, it may also be referred to as **information technology security**.

Cyber-attack is now an international concern. It has given many concerns that could endanger the global economy. As the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to take steps to protect their sensitive business and personal information.

Prerequisites

It is a basic tutorial where we can quickly understand the topics discussed if we have a basic understanding of how a firm or organization handles computer security. It is also helpful for us to have some prior experience with computer updates, firewalls, antiviruses, and other security measures.

- **Definition of cyber security**

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cyber security. We can divide cyber security into two parts one is cyber, and the other is security.

Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.

Some other definitions of cyber security are:

"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

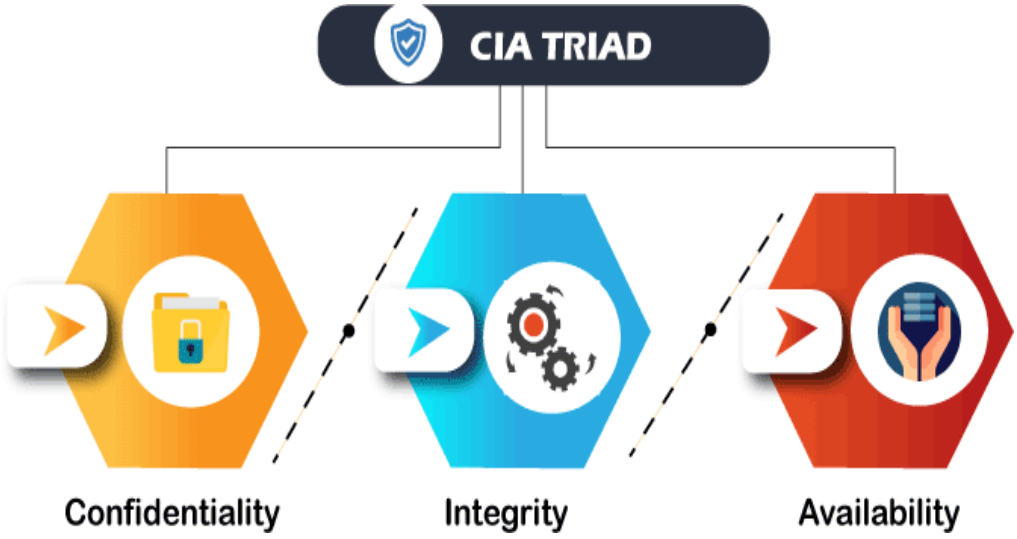
- **Key terms**

Today we live in a digital era where all aspects of our lives depend on the network, computer and other electronic devices, and software applications. All critical infrastructure such as the banking

system, healthcare, financial institutions, governments, and manufacturing industries use **devices connected to the Internet** as a core part of their operations. Some of their information, such as intellectual property, financial data, and personal data, can be sensitive for unauthorized access or exposure that could have **negative consequences**. This information gives intruders and threat actors to infiltrate them for financial gain, extortion, political or social motives, or just vack is now an international concern that hacks the system, and other security attacks could endanger the global economy. Therefore, it is essential to have an excellent cybersecurity strategy to protect sensitive information from high-profile security breaches. Furthermore, as the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to use strong cybersecurity measures and processes to protect their sensitive business and personal information.

Cyber Security's main **objective is to ensure data protection**. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the **CIA triad**. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

We can break the **CIA model into three parts**: Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security. Let us discuss each part in detail.



Confidentiality

Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. **Data encryption** is an excellent example of ensuring confidentiality.

Integrity

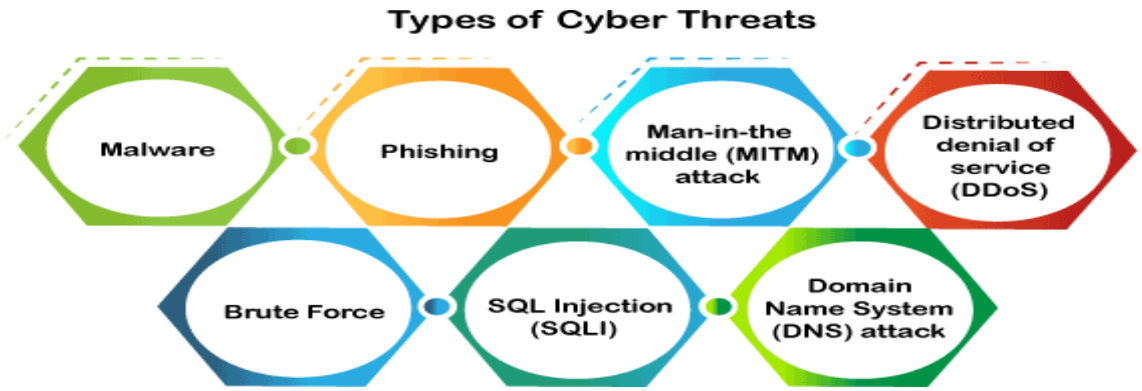
This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.

Availability

This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

➢ Security Threats

A threat in cybersecurity is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupts digital life in general. The cyber community defines the following threats available today:



Malware

Malware means malicious software, which is the most common cyber attacking tool. It is used by the cybercriminal or hacker to disrupt or damage a legitimate user's system. The following are the important types of malware created by the hacker:

- **Virus**: It is a malicious piece of code that spreads from one device to another. It can clean files and spreads throughout a computer system, infecting files, stoles information, or damage device.
- **Spyware**: It is a software that secretly records information about user activities on their system. **For example**, spyware could capture credit card details that can be used by the cybercriminals for unauthorized shopping, money withdrawing, etc.
- **Trojans**: It is a type of malware or code that appears as legitimate software or file to fool us into downloading and running. Its primary purpose is to corrupt or steal data from our device or do other harmful activities on our network.
- **Ransomware**: It's a piece of software that encrypts a user's files and data on a device, rendering them unusable or erasing. Then, a monetary ransom is demanded by malicious actors for decryption.
- **Worms**: It is a piece of software that spreads copies of itself from device to device without human interaction. It does not require them to attach themselves to any program to steal or damage the data.
- **Adware**: It is an advertising software used to spread malware and displays advertisements on our device. It is an unwanted program that is installed without the user's permission. The main objective of this program is to generate revenue for its developer by showing the ads on their browser.
- **Botnets**: It is a collection of internet-connected malware-infected devices that allow

cybercriminals to control them. It enables cybercriminals to get credentials leaks,

- unauthorized access, and data theft without the user's permission.

Phishing

Phishing is a type of cybercrime in which **a sender seems to come from a genuine organization** like PayPal, eBay, financial institutions, or friends and co-workers. They contact a target or targets via email, phone, or text message with a link to persuade them to click on that links. This link will redirect them to fraudulent websites to provide sensitive data such as personal information, banking and credit card information, social security numbers, usernames, and passwords. Clicking on the link will **also install malware** on the target devices that allow hackers to control devices remotely.

Man-in-the-middle (MITM) attack

A man-in-the-middle attack is a type of cyber threat (a form of eavesdropping attack) in which a cybercriminal **intercepts a conversation or data transfer between two individuals**. Once the cybercriminal places themselves in the middle of a two-party communication, they seem like genuine participants and can get sensitive information and return different responses. The main objective of this type of attack is to gain access to our business or customer data. **For example**, a cybercriminal could intercept data passing between the target device and the network on an unprotected Wi-Fi network.

Distributed denial of service (DDoS)

It is a type of cyber threat or malicious attempt where cybercriminals disrupt targeted servers, services, or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic. Here the requests come from several IP addresses that can make the system unusable, overload their servers, slowing down significantly or temporarily taking them offline, or preventing an organization from carrying out its vital functions.

Brute Force

A brute force attack is a **cryptographic hack that uses a trial-and-error method** to guess all possible combinations until the correct information is discovered. Cybercriminals usually use this attack to obtain personal information about targeted passwords, login info, encryption keys, and Personal Identification Numbers (PINS).

SQL Injection (SQLI)

SQL injection is a common attack that occurs when cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information. Once the attack is successful, the malicious actor can view, change, or delete sensitive company data, user lists, or private customer details stored in the SQL database.

Domain Name System (DNS) attack

A DNS attack is a type of cyberattack in which cyber criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers. It is a severe cybersecurity risk because the DNS system is an essential element of the internet infrastructure.

Latest cyber threats

The following are the latest cyber threats reported by the U.K., U.S., and Australian governments:

Romance Scams

The U.S. government found this cyber threat in **February 2020**. Cybercriminals used this threat through dating sites, chat rooms, and apps. They attack people who are seeking a new partner and duping them into giving away personal data.

Dridex Malware

It is a type of financial Trojan malware identifies by the U.S. in **December 2019** that affects the public, government, infrastructure, and business worldwide. It infects computers through phishing emails or existing malware to steal sensitive information such as passwords, banking details, and personal data for fraudulent transactions. The National Cyber Security Centre of the United Kingdom encourages people to make sure their devices are patched, anti-virus is turned on and up to date, and files are backed up to protect sensitive data against this attack.

Emotet Malware

Emotet is a type of cyber-attack that steals sensitive data and also installs other malware on our device. The Australian Cyber Security Centre warned national organizations about this global cyber threat in 2019.

The following are the system that can be affected by security breaches and attacks:

- **Communication**: Cyber attackers can use phone calls, emails, text messages, and messaging apps for cyberattacks.
- **Finance**: This system deals with the risk of financial information like bank and credit card detail. This information is naturally a primary target for cyber attackers.
- **Governments**: The cybercriminal generally targets the government institutions to get confidential public data or private citizen information.
- **Transportation**: In this system, cybercriminals generally target connected cars, traffic control systems, and smart road infrastructure.
- **Healthcare**: A cybercriminal targets the healthcare system to get the information stored at a local clinic to critical care systems at a national hospital.
- **Education**: A cybercriminals target educational institutions to get their confidential research data and information of students and employees**.**

Benefits of cybersecurity

The following are the benefits of implementing and maintaining cybersecurity:

- Cyberattacks and data breach protection for businesses.
- Data and network security are both protected.
- Unauthorized user access is avoided.
- After a breach, there is a faster recovery time.
- End-user and endpoint device protection.
- Regulatory adherence.
- Continuity of operations.
- Developers, partners, consumers, stakeholders, and workers have more faith in the company's reputation and trust.

➢ Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:

Classification of Cyber attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

8. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

9. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

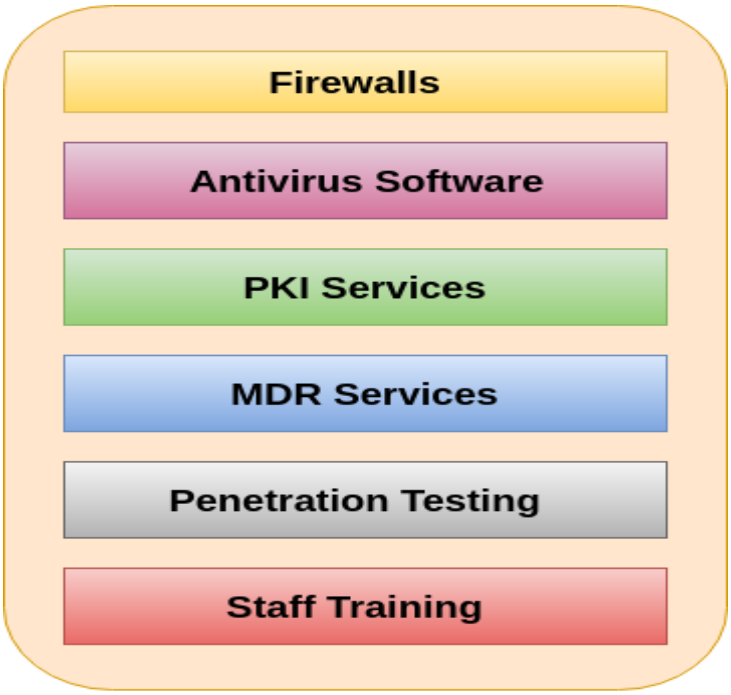
It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

➢ Security Tools

Protecting our IT environment is very critical. Every organization needs to take cybersecurity very seriously. There are numbers of hacking attacks which affecting businesses of all sizes. Hackers, malware, viruses are some of the real security threats in the virtual world. It is essential that every company is aware of the dangerous security attacks and it is necessary to keep themselves secure. There are many different aspects of the cyber defence may need to be considered. Here are six essential tools and services that every organization needs to consider to ensure their cybersecurity is



Cyber Security Tools

1. Firewalls

As we know, the firewall is the core of security tools, and it becomes one of the most important security tools. Its job is to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. The firewalls are used to prevent unauthorized internet users from accessing private networks connected to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those messages that do not meet the specified security criteria.

The Firewall is very useful, but it has limitations also. A skilled hacker knew how to create data and programs that are believing like trusted firewalls. It means that we can pass the program through the firewall without any problems. Despite these limitations, firewalls are still very useful in the protection of less sophisticated malicious attacks on our system.

2. Antivirus Software

Antivirus software is a program which is designed to prevent, detect, and remove viruses and other malware attacks on the individual computer, networks, and IT systems. It also protects our computers and networks from the variety of threats and viruses such as Trojan horses, worms, keyloggers, browser hijackers, rootkits, spyware, botnets, adware, and ransomware. Most antivirus program comes with an auto-update feature and enabling the system to check for new viruses and threats regularly. It provides some additional services such as scanning emails to ensure that they are free from malicious attachments and web links.

3. PKI Services

PKI stands for Public Key Infrastructure. This tool supports the distribution and identification of public encryption keys. It enables users and computer systems to securely exchange data over the internet and verify the identity of the other party. We can also exchange sensitive information

without PKI, but in that case, there would be no assurance of the authentication of the other party. People associate PKI with SSL or TLS. It is the technology which encrypts the server communication and is responsible for HTTPS and padlock that we can see in our browser address bar. PKI solve many numbers of cybersecurity problems and deserves a place in the organization security suite.

PKI can also be used to:

- Enable Multi-Factor Authentication and access control
- Create compliant, Trusted Digital Signatures.
- Encrypt email communications and authenticate the sender's identity.
- Digitally sign and protect the code.
- Build identity and trust into IoT ecosystems.

4. Managed Detection and Response Service (MDR)

Today's cybercriminals and hackers used more advanced techniques and software to breach organization security So, there is a necessity for every businesses to be used more powerful forms of defences of cybersecurity. MDR is an advanced security service that provides threat hunting, threat intelligence, security monitoring, incident analysis, and incident response. It is a service that arises from the need for organizations (who has a lack of resources) to be more aware of risks and improve their ability to detect and respond to threats. MDR also uses Artificial Intelligence and machine learning to investigate, auto detect threats, and orchestrate response for faster result.

The managed detection and response has the following characteristics:

- Managed detection and response is focused on threat detection, rather than compliance.
- MDR relies heavily on security event management and advanced analytics.
- While some automation is used, MDR also involves humans to monitor our network.
- MDR service providers also perform incident validation and remote response.

5. Penetration Testing

Penetration testing, or pen test, is - an important way to evaluate our business's security systems and security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities exist in operating systems, services and application, improper configurations or risky end-user behavior. In Penetration testing, cybersecurity professionals will use the same techniques and processes utilized by criminal hackers to check for potential threats and areas of weakness.

A pen test attempts the kind of attack a business might face from criminal hackers such as password cracking, code injection, and phishing. It involves a simulated real-world attack on a network or application. This tests can be performed by using manual or automated technologies to systematically evaluate servers, web applications, network devices, endpoints, wireless networks, mobile devices and other potential points of vulnerabilities

6. Staff Training

Staff training is not a 'cybersecurity tool' but ultimately, having knowledgeable employees who understand the cybersecurity which is one of the strongest forms of defence against cyber-attacks. Today's many training tools available that can educate company's staff about the best cybersecurity practices. Every business can organize these training tools to educate their employee who can understand their role in cybersecurity.

We know that cyber-criminals continue to expand their techniques and level of sophistication to breach businesses security, it has made it essential for organizations to invest in these training

tools and services. Failing to do this, they can leave the organization in a position where hackers would be easily targeted their security system. So, the expense of the investment on these training tools might put a reward for the business organization with long-term security and protection.

➢ Vulnerability Assessment

Vulnerability Assessment is a process of evaluating security risks in software systems to reduce the probability of threats. The purpose of vulnerability testing is to reduce intruders or hackers' possibility of getting unauthorized access to systems.

The vulnerability is any mistake or weakness in the system's security procedures, design, implementation, or internal control that may violate the system's security policy.

A vulnerability assessment process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage. Using a risk-based approach, vulnerability assessments may target different technology layers, the most common being host, network, and application-layer assessments.

Vulnerability assessments provide security teams and other stakeholders with the information they need to analyze and prioritize potential remediation risks in the proper context. Vulnerability assessments are a critical component of the vulnerability management and IT risk management lifecycles, helping protect systems and data from unauthorized access and data breaches.

Organizations of any size, or even individuals who face an increased risk of cyberattacks, can benefit from some form of vulnerability assessment. Still, large enterprises and other organizations subject to ongoing attacks will benefit most from vulnerability analysis. Because security vulnerabilities can enable hackers to access IT systems and applications, enterprises need to identify and remediate weaknesses before being exploited.

A comprehensive vulnerability assessment, along with a management program, can help companies improve the security of their systems.

Types of Vulnerability Assessments

Vulnerability assessment applies various methods, tools, and scanners to determine grey areas, threats, and risks. Everything depends on how well the given systems' weakness is discovered to attend to that specific need. Below are the different types of vulnerability assessment, such as:

1. Network-based scans

It helps identify possible network security attacks. The scan helps zero-in the vulnerable systems on wired or wireless networks.

2. Host-based scans

Host-based scans are used to locate and identify vulnerabilities in servers, workstations or other network hosts. This type of scan usually examines ports and services that may also be visible to network-based scans. It also provides excellent visibility into the configuration settings and patch history of scanned systems.

3. Wireless network scans

Wireless network infrastructure is scanned to identify vulnerabilities. It helps in validating a company's network.

4. Application Scans

It is used to test websites to discover all known software vulnerabilities. It also identifies security vulnerabilities in web applications and their source code by automated scans on the front-end or static or dynamic source code analysis.

5. Database Scans

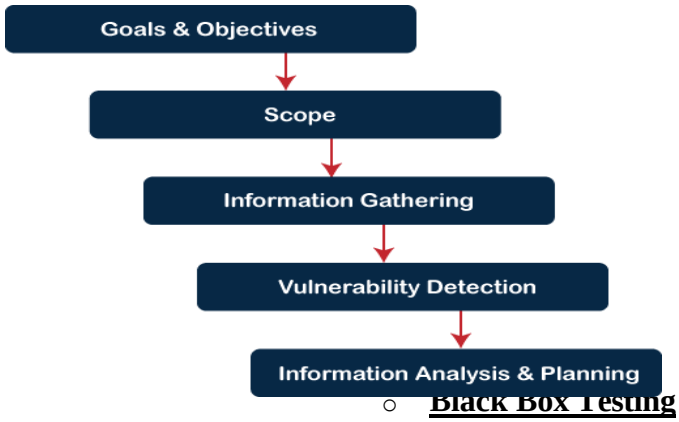
Database Scans aid in identifying grey areas in a database to prevent vicious attacks by cybercriminals. It is identifying rogue databases or insecure environments and classifying sensitive data across an organization's infrastructure.

Vulnerability Assessments Benefits

Vulnerability assessments allow security teams to apply a consistent, comprehensive, and clear approach to identifying and resolving security threats and risks. This has several benefits to an organization, such as:

- Early and consistent identification of threats and weaknesses in IT security.
- Remediation actions to close any gaps and protect sensitive systems and information.
- Meet cybersecurity compliance and regulatory needs for areas like ***HIPAA*** and ***PCI DSS***.
- Protect against data breaches and other unauthorized access.
- A vulnerability assessment provides an organization with information on the security weaknesses in its environment.
- It provides direction on how to assess the risks associated with those weaknesses. This process offers the organization a better understanding of its assets, security flaws and overall risk.
- The process of locating and reporting the vulnerabilities provides a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process, Operating systems, Application Software and Network are scanned to identify vulnerabilities, including inappropriate software design, insecure authentication, etc.

Vulnerability Assessment Process



Below is the step by step vulnerability assessment process to identify the system vulnerability.

1. **Goals and Objective:** Define the goals and objectives of Vulnerability Analysis.
2. **Scope:** While performing the Assessment and Test, the assignment's Scope needs to be clearly defined. The following are the three possible scopes that exist, such as:

- **Black Box Testing**

:It is a software testing method in which software applications' functionalities are tested without knowing internal code structure, implementation details and internal paths.
Black Box Testing mainly focuses on the input and output of software applications, and it is entirely based on software requirements and specifications. It is also known as Behavioral Testing.

- **White Box Testing**

White box testing is a software testing technique in which internal structure, design and coding of software are tested to verify the flow of input-output and

also improve design, usability and security.In white-box testing, code is visible to testers, so it is also called Clear box testing, Open box testing, transparent box testing, Code-based testing and Glass box testing.

- **Grey Box Testing**
  It is a software testing technique to test a software product or application with partial knowledge of its internal structure. The purpose of grey box testing is to search and identify the defects due to improper code structure or improper applications.
  Information Gathering: Obtaining as much information about the IT environment, such as Networks, IP Address, Operating System Version, etc. It applies to all the three types of Scopes, such as Black Box Testing, White Box Testing, and Grey Box Testing.

3. **Vulnerability Detection:** In this step, vulnerability scanners scan the IT environment and identify the vulnerabilities.
4. **Information Analysis and Planning:** It will analyze the identified vulnerabilities to devise a plan for penetrating the network and systems.

How to do Vulnerability Assessment
Following is the steps to do a Vulnerability Assessment, such as:
Step 1) Setup: We need to start by determining which systems and networks will be assessed, identifying where any sensitive data resides, and which data and systems are most critical. Configure and update the tools.
Step 2) Test Execution: A packet is the data routed unit between an origin and the destination.

When any file, such as an e-mail message, HTML
file, Uniform Resource Locator (URL) request is sent from one place to another on the internet, the TCP
layer of TCP/IP
divides the file into several "chunks" for efficient routing. Each of these chunks will be uniquely numbered and will include the Internet address of the destination. These chunks are called packets.

- Run the captured data packet.
- When all the packets have arrived, they will be reassembled into the original file by the TCP layer at the receiving end while running the assessment tools.

Step 3) Vulnerability Analysis: Now define and classify network or System resources and assign priority to the resources (low, medium, high). Identify potential threats to each resource and develop a strategy to deal with the most prioritized problems. Define and implement ways to minimize the consequences if an attack occurs.
Step 4) Remediation: The vulnerability assessment results to patch key flaws or problems, whether simply via a product update or through something more involved, from installing new security tools to an enhancement of security procedures. In step 3, we prioritized the problems that ensure the most urgent flaws are handled first. It's also worth noting that some problems may have so little impact that they may not be worth the cost and downtime required for remediation.

Step 5) Repeat: Vulnerability assessments need to be conducted regularly, monthly or weekly, as any single assessment is only a report of that moment in time. These reports give a strong sense of how security posture has developed.

Vulnerability Testing Methods

Here are the following vulnerability testing methods, such as:

1. **Active Testing:** Inactive Testing, a tester introduces new test data and analyzes the results. During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test. While doing the test, the tester will actively find out the new test cases and new ideas. That's why it is called Active Testing.
2. **Passive Testing:** It is used to monitoring the result of running software under test without introducing new test cases or data
3. **Network Testing:** Network Testing is the process of measuring and recording the current state of network operation over some time. Testing is mainly done for predicting the network operating under load or find out the problems created by new services. We need to Test the following Network Characteristics, such as:
    - Utilization levels
    - Number of Users
    - Application Utilization
4. **Distributed Testing:** Distributed Tests are applied for testing distributed applications. These applications are working with multiple clients simultaneously. Testing a distributed application means testing its client and server parts separately, but by using a distributed testing method, we can test them all together. The test parts will interact with each other during the Test Run.

➢ Roles in cyber Security

Organizations are still working hard to accurately define the expectations of cyber security roles and how those roles fit into the bigger organizational picture," said Backherms.

The specific job responsibilities for any given cyber security role can also depend on the size and resources of the employer. "At a smaller or mid-size firm, you might end up being a 'jack of all trades,' while at a larger firm you're more likely to have specialists," said Champion.

Cyber security professionals can benefit from starting as generalists and then specializing in an area of interest or strength, according to Champion. These areas can include:

- Application security
- Data loss prevention
- Forensics
- Incident response
- Network security
- Security architecture
- Threat intelligence
- Vulnerability management

➢ Critical thinking in Cyber Security-Today's Manner

The growth in the number of computer systems and the increasing reliance upon them by individuals, businesses, industries, and governments means that there is an increasing number of systems at risk.

Financial systems

The computer systems of financial regulators and financial institutions like the U.S. Securities and Exchange Commission, in manipulating markets and making illicit gains. Websites and apps that accept or SWIFT, investment banks, and commercial banks are prominent hacking targets for cybercriminals interested store credit card numbers, brokerage accounts, and bank account information are also prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market. In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs.

Utilities and industrial equipment

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable.

Aviation

The aviation industry is very reliant on a series of complex systems which could be attacked.A simple power outage at one airport can cause repercussions worldwide, much of the system relies on radio transmissions which could be disrupted, and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore There is also potential for attack from within an aircraft.

Consumer devices

Desktop computers and laptops are commonly targeted to gather passwords or financial account information, or to construct a botnet to attack another target. Smartphones, tablet computers, smart watches, and other mobile devices such as quantified self devices like activity trackers have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. WiFi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach.

Large corporations

Large corporations are common targets. In many cases attacks are aimed at financial gain through identity theft and involve data breaches.

Medical records have been targeted in general identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale. Although cyber threats continue to increase, 62% of all organizations did not increase security training for their business in 2015.

Not all attacks are financially motivated, however: security firm HBGary Federal suffered a serious series of attacks in 2011 from hacktivist group Anonymous in retaliation for the firm's CEO claiming to have infiltrated their group and Sony Pictures was hacked in 2014 with the apparent dual motive of embarrassing the company through data leaks and crippling the company by wiping workstations and servers.

Automobiles

Vehicles are increasingly computerized, with engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced driver-assistance systems on many

models. Additionally, connected cars may use WiFi and Bluetooth to communicate with onboard consumer devices and the cell phone network Self-driving cars are expected to be even more complex. All of these systems carry some security risk, and such issues have gained wide attention.

Simple examples of risk include a malicious compact disc being used as an attack vector and the car's onboard microphones being used for eavesdropping..

Government

Government and military computer systems are commonly attacked by activists and foreign powers. Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records, and financial systems are also potential targets as they are now all largely computerized. Passports and government ID cards that control access to facilities which use RFID can be vulnerable to cloning.

Internet of things and physical vulnerabilities

The Internet of things (IoT) is the network of physical objects such as devices, vehicles, and buildings that are embedded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data. Concerns have been raised that this is being developed without appropriate consideration of the security challenges involved.

While the IoT creates opportunities for more direct integration of the physical world into computer-based systems, it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyberattacks are likely to become an increasingly physical (rather than simply virtual) threat. If a front door's lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices.

Medical systems

Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment and implanted devices including pacemakers and insulin pumps. There are many reports of hospitals and hospital organizations getting hacked, including ransomware attacks,Windows XP exploits, viruses, and data breaches of sensitive data stored on hospital servers.

Energy sector

In distributed generation systems, the risk of a cyber attack is real, according to Daily Energy Insider. An attack could cause a loss of power in a large area for a long period of time, and such an attack could have just as severe consequences as a natural disaster. The District of Columbia is considering creating a Distributed Energy Resources (DER) Authority within the city, with the goal being for customers to have more insight into their own energy use and giving the local electric utility, Pepco, the chance to better estimate energy demand. The D.C. proposal, however, would "allow third-party vendors to create numerous points of energy distribution, which could potentially create more opportunities for cyber attackers to threaten the electric grid.

Short Answers

1. Define cyber security ?
2. Explain CIA TRIAD ?
3. Define Security tools ?
4. Explain the role of cyber security ?

Long Answers

1.Explain about Security Threats ?
2. Explain in details about the cyber attacks ?
3. What is Vulnerability ?

UNIT-II

Cyber Threat Actors and Their Motives:

➢ Cyber Threats

A cyber threat (also known as a cyber security threat) is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

A threat can be broken down into three components -

1. A **cyber threat** is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.
2. **Cyber threat actors** are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cybersecurity awareness, and technological developments to gain unauthorised access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks.
3. The **cyber threat environment** is the online space where cyber threat actors conduct malicious cyber threat activity.
   Understand your enemy

There are different types of cyber threat actors. Understanding their motivations will help you understand which of these may see you as a target and therefore the level of risk you or your organisation could be exposed to. The most common motivation for a cyber attack is for money or acquiring something that can be traded for money such as your data, intellectual property rights (IPR), credentials, bank or credit card details.

➢ Security Attacks:

- 1. Email compromise
- 2. Phishing attacks

- 3. Supply chain attack
- 4. Vulnerability scanning
- 5. Internet of Things (IoT)

The most common cyber threats and attacks are delivered via email phishing or exploitation of already known vulnerabilities on servers or user devices such as desktops, laptops, smart devices and tablets. Many of these threats are indiscriminate but some are targeted towards businesses.

1. Email compromise

Email compromise or business email compromise is when an email account has been compromised and an attacker is impersonating you to scam others in your contact list. The attacker seeks to gain the trust of your contacts to exploit them for money or data or to get them to download malware.

2. Phishing attacks

Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to an unsafe website. The term phishing is mainly used to describe attacks that arrive by email. Phishing emails can reach millions of users directly, and hide amongst the huge number of benign emails that busy users receive.

Attackers can install malware, sabotage systems, or steal intellectual property and money. An attack can have devastating results. For individuals and business, this includes unauthorised purchases, the stealing of funds, data or identity theft. Phishing emails can hit an organisation of any size and type. You might get caught up in a mass campaign (where the attacker is just looking to collect passwords or make easy money), or it could be the first step in a targeted attack against your company. The aim could be something much more specific, like the theft of sensitive data. In a targeted campaign, the attacker may use information about your employees or company to make their messages even more persuasive and realistic - this is referred to as spear phishing.

Other types of phishing:

1. **Smishing** stands for SMS phishing. With smishing, a test message is sent to the user's phone instead of email account. The text message usually asks the user to call a phone number or go to a website to take immediate action.
2. **Vishing** (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities usually over the phone.
3. **Spear phishing** is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted
4. is a cyber attack that seeks to damage an organisation or business by targeting less secure user’s computer.

3. Supply chain attack

A supply chain attack elements in the supply network. An organisation's supply chain includes

the supplers and services that an organisation needs to deliver its business**.**

A supply chain attack can occur in any type or size of industry. become a link in one or more complex supply chains. Being a desirable, trustworthy supplier or customer now extends far beyond delivering good products or services, you must protect and secure As your organisation or business grows and starts to work with more customers, partners and suppliers, you the data of suppliers and

customers.

Supply chain vulnerability risks

- Customer/client, supplier and partner data are held increasingly on disparate, distributed databases, so one vulnerability could compromise the integrity of the entire chain.
- Every time a new organisation joins the supply chain, the greater the risk of a security breach.
- Financial safety, employee safety, intellectual property, data compliance, finances and reputation are all at stake, for all organisations in the chain.
- Data could also be shared between more links in the chain, for example via email or a single point of access online portals.

4. Vulnerability scanning

Vulnerability scanners are tools used to find weaknesses or exploitable vulnerabilities in the infrastructure or code of a website. They can be used just as effectively by the "bad guys", (known as black-hat hackers) to gain access to your devices, systems through any vulnerabilities found. A malicious security breach can have devastating results; this includes unauthorised purchases, the stealing of funds, data or identity theft.

Best practice for organisations/businesses is for penetration testers, (known as white-hat hackers), to run vulnerability scanners against your IT systems and web sites before they are ever deployed. Any vulnerabilities found are quickly corrected, maintaining security prior to launch.

5. Internet of Things (IoT)

In the broadest sense, the term Internet of Things encompasses everything connected to the internet. Usually shortened to the IoT, this collective allows smart devices such as wireless lights, thermostats, home security sensors, TV's, intelligent streetlights, smart meters, and much more to connect, talk to each other and also to us.

The Internet of Things allows us to carry out activities far easier and faster than ever before. It can help improve how we live and interact with everyday objects. As the cyber landscape develops, we must ensure that it does not present hackers with a back door into our lives. Smart devices present a great opportunity for hackers and a great vulnerability to our security. It is essential that we understand the risks and potential threats associated with their use. If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security.

A Brief overview of types of actors and their motives

Types of Threat Actors

Government-Sponsored/State- Sponsored Actors. These threat actors are funded, directed, or sponsored by nations. They've been known to steal and exfiltrate intellectual property, sensitive information, and even funds to further their nation's espionage causes. They are typically motivated by political, economic, technical, or military agendas. They are often looking for competitive information, resources, or users that can be exploited for espionage purposes.

Organized Crime/ Cybercriminals.

Crime is everywhere, and the internet is no different. Criminals who want to steal sensitive data, money, and personal information are out there. However, since they're after financial gain, the data they take does tend to show up on the black market or is sold to the highest bidder. These threat actors are also known to use ransomware to extort business owners directly. They are typically either looking for personally identifiable information (PII) of your

customers or employees, such as social security numbers, health records, credit cards, and banking information or to hijack and ransom critical digital resources.

Hacktivists. Hacktivists focus on bringing awareness.They're usually motivated by ideological activism. These attackers have a political agenda. Their goal is to either create high- profile attacks that help them distribute propaganda, or to cause damage to organizations they are opposed to. The ultimate goal is to find a way to benefit their cause or gain awareness of their issue.

Insiders. Insiders are a particularly nasty threat to any organization's cybersecurity because of the amount of access they'd have when working from within. Attackers operating inside your organization are typically disgruntled employees or ex-employees either looking for revenge or some type of financial gain. They sometimes collaborate with other threat actors, such as organized crime or government-sponsored hackers, out of a sense of loyalty, or in exchange for money or prestige.

Script Kiddies. Script Kiddies use tools developed by other attackers to penetrate a network or system. These attackers are usually amateur criminals, often referred to as script kiddies, who are driven by the desire for notoriety. Sometimes, however, they can legitimate security researchers trying to help organizations find and close security vulnerabilities, or even professional hackers (sometimes known as gray hat hackers) looking to profit from finding and exposing flaws and exploits in network systems and devices.

Internal User Errors. Even simple user errors can end in catastrophe because of their elevated permissions within an organization's systems and networks. Users making mistakes with configurations are actually the largest threat organizations face. These threat actors exist largely due to failing to design flaws out of the network, or by providing privileges to individuals who should not have them. Internal user errors have been known to bring down critical resources such as firewalls, routers, and servers, causing widespread or departmental company outages.

Common Threat Actor Motivations

Understanding threat actors and their motivations is an essential step in the cybersecurity process. It will help you map out your defenses and may help you better outmaneuver attackers successfully.

- Political, Economic, Technical, and Military Agendas
- Profits/Financial Gain
- Notoriety
- Revenge
- Overlap of Motivations

➢ Hacking—Definition, Types, Security

A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.

Hacking refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.

A traditional view of hackers is a lone rogue programmer who is highly skilled in coding and modifying computer software and hardware systems. But this narrow view does not cover the true technical nature of hacking. Hackers are increasingly growing in sophistication, using stealthy attack methods designed to go completely unnoticed by cybersecurity software and IT teams. They are also highly skilled in creating attack vectors that trick users into opening malicious attachments or links and freely giving up their sensitive personal data.

Types of Hacking/Hackers

There are typically four key drivers that lead to bad actors hacking websites or systems: (1) financial gain through the theft of credit card details or by defrauding financial services, (2) corporate espionage, (3) to gain notoriety or respect for their hacking talents, and (4) state- sponsored hacking that aims to steal business information and national intelligence. On top of that, there are politically motivated hackers—or hacktivists—who aim to raise public attention by leaking sensitive information.

A few of the most common types of hackers that carry out these activities involve: Black Hat Hackers

Black hat hackers are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign.

These individuals' actions can inflict serious damage on both computer users and the organizations they work for. They can steal sensitive personal information, compromise computer and financial systems, and alter or take down the functionality of websites and critical networks.

White Hat Hackers

White hat hackers can be seen as the "good guys" who attempt to prevent the success of black hat hackers through proactive hacking. They use their technical skills to break into systems to assess and test the level of network security, also known as ethical hacking. This helps expose vulnerabilities in systems before black hat hackers can detect and exploit them.

Grey Hat Hackers

Grey hat hackers sit somewhere between the good and the bad guys. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially. Their actions are typically carried out for the common good. For example, they may exploit a vulnerability to raise awareness that it exists, but unlike white hat hackers, they do so publicly. This alerts malicious actors to the existence of the vulnerability.

Devices Most Vulnerable To Hacking

Smart Devices

Smart devices, such as smartphones, are lucrative targets for hackers. Android devices, in particular, have a more open-source and inconsistent software development process than Apple devices, which puts them at risk of data theft or corruption. However, hackers are increasingly targeting the millions of devices connected to the Internet of Things (IoT).

Webcams

Webcams built into computers are a common hacking target, mainly because hacking them is a simple process. Hackers typically gain access to a computer using a Remote Access Trojan (RAT)

acts such in rootkit malware, which allows them to not only spy on users but also read their messages, see their browsing activity, take screenshots, and hijack their webcam.

Routers

Hacking routers enables an attacker to gain access to data sent and received across them and networks that are accessed on them. Hackers can also hijack a router to carry out wider malicious as distributed denial-of-service (DDoS) attacks, Domain Name System (DNS) spoofing, or cryptomining.

Email

Email is one of the most common targets of cyberattacks. It is used to spread malware and ransomware and as a tactic for phishing attacks, which enable attackers to target victims with malicious attachments or links.

Prevention from Getting Hacked

There are several key steps and best practices that organizations and users can follow to ensure they limit their chances of getting hacked.

Software Update

Hackers are constantly on the lookout for vulnerabilities or holes in security that have not been seen or patched. Therefore, updating software and operating systems are both crucial to preventing users and organizations from getting hacked. They must enable automatic updates and ensure the latest software version is always installed on all of their devices and programs.

Use Unique Passwords for Different Accounts

Weak passwords or account credentials and poor password practices are the most common cause of data breaches and cyberattacks. It is vital to not only use strong passwords that are difficult for hackers to crack but also to never use the same password for different accounts. Using unique passwords is crucial to limiting hackers' effectiveness.

HTTPS Encryption

Spoofed websites are another common vehicle for data theft, when hackers create a scam website that looks legitimate but will actually steal the credentials that users enter. It is important to look for the Hypertext Transfer Protocol Secure (HTTPS) prefix at the start of a web address. For.

Avoid Clicking on Ads or Strange Links

Advertisements like pop-up ads are also widely used by hackers. When clicked, they lead the user to inadvertently download malware or spyware onto their device. Links should be treated carefully.

Change the Default Username and Password on Your Router and Smart Devices

Routers and smart devices come with default usernames and passwords. However, as providers ship millions of devices, there is a risk that the credentials are not unique, which heightens the chances of hackers breaking into them. It is best practice to set a unique username and password combination for these types of devices.

➢ Security in Hacking

There are further steps that users and organizations can take to protect themselves against the threat of hacking.

Download from First-party Sources: Only download applications or software from trusted organizations and first-party sources. Downloading content from unknown sources means users do not fully know what they are accessing, and the software can be infected with malware, viruses, or Trojans.

Install Antivirus Software: Having antivirus software installed on devices is crucial to spotting potential malicious files, activity, and bad actors. A trusted antivirus tool protects users and organizations from the latest malware, spyware, and viruses and uses advanced detection engines to block and prevent new and evolving threats.

Use a VPN: Using a virtual private network (VPN) allows users to browse the internet securely. It hides their location and prevents hackers from intercepting their data or browsing activity. Do Not Login as an Admin by Default

"Admin" is one of the most commonly used usernames by IT departments, and hackers use this information to target organizations. Signing in with this name makes you a hacking target, so do not log in with it by default.

Use a Password Manager: Creating strong, unique passwords is a security best practice, but remembering them is difficult. Password managers are useful tools for helping people use strong, hard-to-crack passwords without having to worry about remembering them.

Use Two-factor Authentication: Two-factor authentication (2FA) removes people's reliance on passwords and provides more certainty that the person accessing an account is who they say they are. When a user logs in to their account, they are then prompted to provide another piece of identity evidence, such as their fingerprint or a code sent to their device.

Brush Up on Anti-phishing Techniques: Users must understand the techniques that hackers deploy to target them. This is especially the case with antiphishing and ransomware, which help users know the telltale signs of a phishing email or a ransomware attack

➢ Security Attack

Security attack definition

An attempt to gain unauthorized access to information resource or services, or to cause harm or systems. damage to information

Is any form of malicious actions taken to harm the **security** of information system components. An action is classified as malicious with respect to the enterprise **security** policy. Learn more in: Cost Estimation and Security Investment of Security Projects

Any form of malicious or actions taken to harm the **security** of information system components. An action is classified as malicious with respect to the enterprise security police **security**

Services

Cybersecurity provides Services Information and Cyber Security Strategy & Design services to give you a better security posture. Our Cybersecurity Services shield your enterprise against threats and strengthen your cyber defenses. You can depend on us to provide **comprehensive Information and cyber security services.**

- Information Security Assessments to analyze the maturity of your information security program,
- as well as identify gaps, weaknesses, and opportunities for improvement. Get our cybersecurity services and identify risk to your business.
- Virtual CISO, which provides you with wide ranging expertise needed for incident response, compliance and the latest threat intelligence to address information security flaws and execute actionable mitigation strategies. Our cybersecurity services will aligned with your business strategy.
- Data Governance, helping you handle increasingly large volumes of data and the related. Enhancing your cybersecurity posture and data management.
- Managed Security Services, Our Managed Security Services, Cyber Security Services and Managed Detection and Response (MDR) service provides advanced NexGen managed cyber security services that offer threat intelligence, threat hunting, security monitoring, and cybersecurity incident response services.
- Third Party Risk Management, Comprehensive cybersecurity services which include managed security services, Vendor/Third party cyber security assessment services. We let you know how and what your vendors are doing to secure your data from cyber threats. Do they have a cyber security program?
- Governance, Risk & Compliance, Aligning your GRC activities to business performance drivers, using frameworks such has NIST, PCI/DSS, ISO, GDPR, NYDFS, and others with our IT security service program.
- Security Awareness Education, Reveal your organization employees strength and weakness, and empower them against cyber criminals. Our cybersecurity services ensure your users are ahead of your attackers.
- Penetration Testing & Phishing, Effective security starts with a clear understanding of your vulnerabilities. Penetration testing & phishing assessment protect against cybersecurity threats

➢ Security Mechanisms

Types of Security Mechanism

Network Security is field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.

Types of Security Mechanism are :

1. **Encipherment:**
   This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.
2. **Access Control**

   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
3. **Notarization:**
   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This

4. mediator keeps record of requests made by sender to receiver for later denied.
5. **Data Integrity**

   This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
6. **Authentication exchange:**

   This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
7. **Bit stuffing**

   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
8. **Digital Signature**

   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

- **Network Security**

Network security is a broad topic with multilayered approach. It can be addressed at the data link layer, network layer and application layer. The issues concerned are: packet intrusion and encryption, IP packets and routing tables with their update version, and host-level bugs occurred at data link layer, network layer and application, respectively.

The TCP/IP protocols are being used globally irrespective of the nature of the organization whether it belongs to general category of organizations or security specific sensitive organizations. The news -:"information about hacking of some website or portal by some undesired people is very common nowadays. This shows that TCP/IP protocols are susceptible to intercept. This generated a need to ensure all round security for the network in an organization. The task of network administrator had to widen to inc1ude the overall security of the network. He has to ensure that all parts of this network are adequately protected and adequate measures of security have been implemented within a *TCP/IP* network. He should be aware of an effective security policy. He should also be able to pinpoint the main areas of risk that the network may face. Basically, these main areas of risk vary from network to network depending upon the organization functioning. There are, therefore, various security-related aspects which have direct implications for network administrator along with the means to monitor the implemented measures of security effectively arid to tackle the problem of breach ofsecurityifithappens.

Basic Requirements of Network Security

1. The main objective of the network is to share information among its users situated locally or remotely. Therefore, it is possible that undesired user can hack the network and can prove to be harmful for the health of the network or user. There are few basic points which must be followed by network administrator to provide the network an adequate security other than network-specific security as in case of e-commerce, etc. These are given below:

2. Networks are designed to share information. Therefore, the network must be clearly configured to identify the shareable information and non-shareable information.

3. The network should also clear with whom the shareable information could be shared.

4. With the increase of system security, the price for its management will also increase accordingly, therefore a compromising level between security and prices should be established as per the requirement of the network security system policy. This will largely depend upon the level of security needed to apply in the network, overall security requirements and the effective implementation of chosen level of security.

5. Division of the responsibilities concerning the network security must be clearly .defined between users and system administrator.

6. The requirements for security must be detailed within a network security policy of the organization that indicates the valuable data and their associated cost to the business. After defining the detailed network security policy and identifying the clear cut responsibilities in the organization, the system administrator should be made then responsible for ensuring that the security policy is effectively applied to the company environment, including the existing networking infrastructure,

Network Attack?

A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity. There are two main types of network attacks:

- **Passive:** Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
- **Active:** Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.

We distinguish network attacks from several other types of attacks:

- **Endpoint attacks**—gaining unauthorized access to user devices, servers or other endpoints, typically compromising them by infecting them with malware.
- **Malware attacks**—infecting IT resources with malware, allowing attackers to compromise systems, steal data and do damage. These also include ransomware attacks.
- **Vulnerabilities, exploits and attacks**—exploiting vulnerabilities in software used in the organization, to gain unauthorized access, compromise or sabotage systems.
- **Advanced persistent threats**—these are complex multilayered threats, which include network attacks but also other attack types.

1. In a network attack, attackers are focused on penetrating the corporate network perimeter and gaining access to internal systems. Very often, once inside attackers will combine other types of attacks, for example compromising an endpoint, spreading malware or exploiting a vulnerability in a system

within the network.

2. **Man in the middle attacks:** A man in the middle attack involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.

3. **Code and SQLinjection attacks:** Many websites accept user inputs and fail to validate and sanitize those inputs. Attackers can then fill out a form or make an API call, passing malicious code instead of the expected data values. The code is executed on the server and allows attackers to compromise it.

4. **Privilege escalation:** Once attackers penetrate your network, they can use privilege escalation to expand their reach. Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.

5. **Insider threats:** A network is especially vulnerable to malicious insiders, who already have privileged access to organizational systems. Insider threats can be difficult to detect and protect against, because insiders do not need to penetrate the network in order to do harm. New technologies like User and Even Behavioral Analytics (UEBA) can help identify suspicious or anomalous behavior by internal users, which can help attacks.identify insider

Network Protection Best Practices

Segregate Your Network

A basic part of avoiding network security threats is dividing a network into zones based on security requirements.This can be done using subnets within the same network, or by creating Virtual Local Area Networks (VLANs), each of which behaves like a complete separate network. Segmentation limits the potential impact of an attack to one zone, and requires attackers to take special measures to penetrate and gain access to other network zones.

to access the Internet unchecked. Pass all requests through a transparent proxy, and use it to

Regulate Access to the Internet via Proxy Server

Do not allow network users control and monitor user behavior. Ensure that outbound connections are actually performed by a human and not a bot or other automated mechanism. Whitelist domains to ensure corporate users can only access websites you have explicitly approved.

Place Security Devices Correctly

Place a firewall at every junction of network zones, not just at the network edge. If you can't deploy full-fledged firewalls everywhere, use the built-in firewall functionality of your switches and routers. Deploy anti-DDoS devices or cloud services at the network edge. Carefully consider where to place strategic devices like load balancers – if they are outside the Demilitarized Zone (DMZ), they won't be protected by your network security apparatus.

Use Network Address translation

Network Address Translation (NAT) lets you translate internal IP addresses into addresses accessible on public networks. You can use it to connect multiple computers to the Internet using a single IP address. This provides an extra layer of security, because any inbound or outgoing traffic has to go through a NAT device, and there are fewer IP addresses which makes it difficult for attackers to understand which host they are connecting to **.**

Monitor Network Traffic

Ensure you have complete visibility of incoming, outgoing and internal network traffic, with the ability to automatically detect threats, and understand their context and impact. Combine data from different security tools to get a clear picture of what is happening on the network, recognizing that many attacks span multiple IT systems, user accounts and threat vectors.

Achieving this level of visibility can be difficult with traditional security tools. Cynet 360 is an integrated security solution offering advanced network analytics, which continuously monitors network traffic, automatically detect malicious activity, and either respond to it automatically or pass context-rich information to security staff.

Use Deception Technology

No network protection measures are 100% successful, and attackers will eventually succeed in penetrating your network. Recognize this and place deception technology in place, which creates decoys across your network, tempting attackers to “attack” them, and letting you observe their plans and techniques. You can use decoys to detect threats in all stages of the attack lifecycle: data files, credentials and network connections.

Cynet 360 is an integrated security solution with built-in deception technology, which provides both off-the-shelf decoy files and the ability to create decoys to meet your specific security needs. , while taking into account your environment’s security needs.

- **Malware & Ransomware Malware**

Malware is short for "malicious software." It is a program or file designed to be disruptive, invasive and harmful to your computer. Types of malware include viruses, spyware, adware and worms. Malware frequently strikes the Ohio State campuses, causing varying degrees of trouble. It is most frequently transmitted through e-mail attachments, Instant Messages (IM), peer-to-peer downloads, phishing and misleading web sites. Virus outbreaks cause harm by destroying data on infected computers and/or by increasing network traffic by triggering e-mail messages that carry the virus to all e-mail addresses in an address book or a random combination of addresses. If viruses are not halted quickly, the flood of e-mails can swamp university servers, disrupting e- mail service for all. Virus software is identifiable by its actions and many tools are in place to combat this threat to your computer. You can also employ additional security.'

Ransomware

Ransomware is a type of malware that is designed to block access to all or part of a computer system until a sum of money is paid. Because attackers are looking to maximize their payday, the targets are typically larger entities (departments, colleges, businesses) that not only are likely to have the funds, but also experience a significant loss when they cannot access their systems. However, individuals are still a target of ransomware because they can be a doorway into an organization's systems.
When it comes to preventing or detecting ransomware, there is no silver bullet. However, you can use some of the following techniques to help prevent and detect ransomware, which may help minimize your risk of getting malware.

Limit access to network file shares:

Only allow the level of access required by the user's business function. Limiting access to network file shares will prevent a computer infected with ransomware from spreading it to other computers on the network.

Keep things updated:

Make sure all applications are up to date. Outdated applications that don't have the most recent security patches makes them vulnerable to ransomware and other malware.

Disable Microsoft macros

A macro is a set of commands that are automatically run when a file is opened. One way to infect a computer is to include a malicious macro in a file that users might download. When macros are turned on, the harmful macro may automatically run when you download the file. Turning off macros can remove this risk and help protect against ransomware and other malware. To disable macros in Microsoft Office 2016 products:

1. Open the Microsoft application/program (ex: Word, PowerPoint, etc.).
2. Go to the file tab and select "Options."
3. Go to the "Trust Center" tab and select "Trust Center Settings."
4. In the "Macros" tab there are the options for macro settings
5. Select "Disable All Macros with Notification;" this disables all macros and alerts the user if a macro is present in the file.

Use a good antivirus tool:

An antivirus is a tool that helps to detect and remove malware from your computer. You should keep an updated antivirus. If available, you should leverage a suite of antivirus tools, such as:

- **Host Intrusion Prevention System (HIPS):** HIPS monitors your computer and watches to make sure no major changes are made. If a change is made, HIPS blocks the action and raises an alert.
- **Behavior-Based Scanning:** Behavior-Based Scanning monitors for files for any irregular activity, which is based off of how the risk threshold is configured. Risk threshold rules define what actions should be monitored and raises an alert when these actions occur.

Symantec Endpoint Protection Suite(link is external) which Ohio State also offers to colleges and departments, includes a number of these tools. To get the Symantec Endpoint Protection Suite contact your IT department.

Consider using Microsoft Enhanced Mitigation Experience Toolkit:

Microsoft's Enhanced Mitigation Experience Toolkit (EMET) is a free software tool that helps to prevent vulnerabilities in select applications from being exploited. It does this by putting mitigation technologies on applications selected by the user, blocking against potential exploitation. A few examples of mitigation technologies are spam and antimalware filtering, e- mail encryption and web application filtering

Protect your department with whitelisting :

A whitelist is a list of entities that are being allow by the user. This is the opposite of blacklisting, which is a list of entities that the user doesn't allow on to its system. Whitelisting can include emails, LANs, and applications. Ohio State offers the Symantec Endpoint Protection Suite(link is external), which includes a whitelisting tool. Contact your IT department to get the Symantec Endpoint Protection Suite and the whitelisting tool.

Explore other ransomware resources:

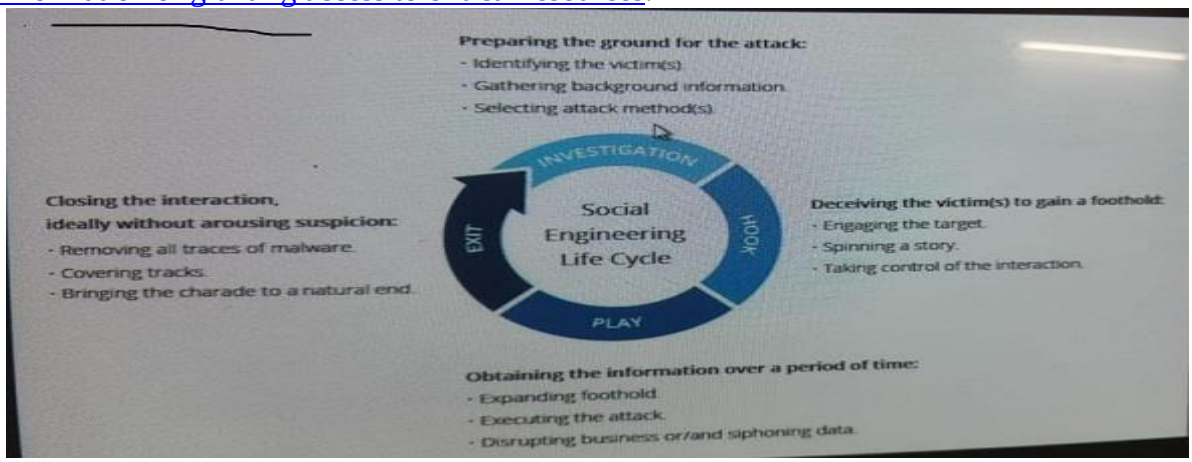
- Ohio State Ransomware Brochure
- Ohio State Ransomware

➢ Social Engineering Scenario:

What is social engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.



Social Engineering Attack Lifecycle

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Social engineering attack techniques

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

Baiting

As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.

Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation

requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.

Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.

A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials

Social engineering prevention

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm. Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

- **Don't open emails and attachments from suspicious sources** – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
- **Use multifactor authentication** – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise.
- **Be wary of tempting offers** – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- **Keep your antivirus/antimalware software updated** – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

➢ Phishing

What is a phishing attack

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then

tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.
Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.
An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Phishing attack examples

The following illustrates a common phishing scam attempt:

- A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
- The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.

Several things can occur by clicking the link. For example:

- The user is redirected to myuniversity.edurenewal.com, a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested. The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.
- The user is sent to the actual password renewal page. However, while being redirected, a malicious script activates in the background to hijack the user's session cookie. This results in a reflected XSS attack, giving the perpetrator privileged access to the university network.

Phishing techniques

Email phishing scams
Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates.
For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.
In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, as previously shown, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.
Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains. In the above example, the myuniversity.edu/renewal URL was changed to myuniversity.edurenewal.com. Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.

Spear phishing

Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.

An attack might play out as follows:

1. A perpetrator researches names of employees within an organization's marketing department and gains access to the latest project invoices.
2. Posing as the marketing director, the attacker emails a departmental project manager (PM) using a subject line that reads, Updated invoice for Q3 campaigns. The text, style, and included logo duplicate the organization's standard email template.
3. A link in the email redirects to a password-protected internal document, which is in actuality a spoofed version of a stolen invoice.
4. The PM is requested to log in to view the document. The attacker steals his credentials, gaining full access to sensitive areas within the organization's network.

By providing an attacker with valid login credentials, spear phishing is an effective method for executing the first stage of an APT.

How to prevent phishing

Phishing attack protection requires steps be taken by both users and enterprises.

For users, vigilance is key. A spoofed message often contains subtle mistakes that expose its true identity. These can include spelling mistakes or changes to domain names, as seen in the earlier URL example. Users should also stop and think about why they're even receiving such an email. For enterprises, a number of steps can be taken to mitigate both phishing and spear phishing attacks:

- Two-factor authentication (2FA) is the most effective method for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications. 2FA relies on users having two things: something they know, such as a password and user name, and something they have, such as their smartphones. Even when employees are compromised, 2FA prevents the use of their compromised credentials, since these alone are insufficient to gain entry.
- In addition to using 2FA, organizations should enforce strict password management policies. For example, employees should be required to frequently change their passwords and to not be allowed to reuse a password for multiple applications.

➢ **Vishing**

Definition Most people have heard of phishing; vishing is a different attack that falls under the general phishing umbrella and shares the same goals. Vishers use fraudulent phone numbers, voice-altering software, text messages, and social engineering to trick users into divulging sensitive information. Vishing generally uses voice to trick users. (Smishing, yet another form of phishing that uses SMS text messages to trick users, is often used in tandem with voice calls depending on the attacker's methods.)

What is the Difference Between Vishing and Phishing?

Phishing and vishing have the same goal: to obtain sensitive data from users that could be used in identity theft, monetary gain or account takeover. The main difference between phishing and vishing is the medium used to target potential victims. Whereas phishing is primarily an email-based attack, vishing uses voice, typically calls to a user's cell phone number.

Both vishers and phishers send messages to potential victims, usually in high volumes. Phishing attackers send a large number of email messages to a list of potential targets. If the attacker targets a specific organization, only a list of high-privileged user email addresses from the targeted business might be used. Phishers generally use compelling email messages to trick users into replying with sensitive information or convince the user to click a link where malware is hosted. Malicious attachments are also used in some phishing attacks.

The visher might first send a text message to potential victims in high volumes from a long list of phone numbers. The message might ask users to make a phone call to the attacker's number. Another vishing method creates an automated message and robo-dials potential victims. It uses computer-generated voice messages to remove accents and build trust. The voice message then tricks the user into connecting to a human agent who continues the scam, or the it might ask users to open an attacker-controlled website.

Although there are minor differences between vishing and phishing, the end goal is always the same: credentials, personal identifiable data and financial information. Users familiar with phishing might not be familiar with vishing, so attackers increase their chance of success.

Vishing Techniques

It's more challenging to identify a vishing attack than a phishing and smishing attack. Vishing attacks start with a text message and usually contain a phone number. The following image is an example of a vishing attack:

Scammers use scare tactics to convince users to make a phone call. In this message, the attacker pretends to be with the IRS. Most users are afraid of penalties and fees from the IRS, so any users who call this phone number will be told that they owe money. The attacker convinces the targeted user to charge their credit card or to transfer money directly from the targeted user's account. IRS scams are one of the more common attacks targeting users in the U.S.

The following image is another example of a vishing attack starting with a text message:

In the above picture, the same threats and scare tactics are used to convince users to call. If the targeted user responds with STOP, the messages will continue. By replying to the attacker, the targeted user verifies that the phone number is valid and will continue to be a target.

Notice in both images that the number listed in caller ID is a short 6-digit invalid contact number. These numbers are used by telecoms to send users messages, but it's also an indication that the message was sent from an auto-dialer API or an email account. If a message comes from one of these numbers, always be suspicious that it could be a smishing or vishing scam.

Not every message with an invalid number in caller ID is malicious. These numbers are also used in multi-factor authentication requests when the user is sent a PIN to complete the authentication process. Social engineering attackers will trick users into sending the PIN, but this involves contacting the user and tricking them into divulging the PIN. Vishing, phishing and

smishing can all be combined with social engineering for more large-scale attacks on high- privilege accounts.

Among attackers who stick to phone calls, it's become more popular to use computer programs to mask voices and geographical accents. Attackers can even use a different gendered voice to launch an attack. Often, these voices are audibly computer-generated and obvious vishing attempts. But always be aware of phone calls asking for private information over a call.

How to Prevent Vishing

The best way to avoid being a victim of vishing is to ignore the messages. Telecoms have fraud systems in place that display "Fraud Risk" (or something similar) on caller ID when a known malicious call is received. However, you can't rely on the telecoms to catch all malicious calls. Users can take their own precautions to avoid becoming a victim.

SIM swapping and social engineering leave your number vulnerable to attackers. SIM swapping involves socially engineering a telecom representative into giving an attacker access to your phone number. If you receive a strange message about a multi-factor PIN or changes to your cell phone account, always contact the telecom to ensure that you have not been the victim of SIM swapping and hijacking.

Here are a few steps to avoid becoming a victim of vishing and related attacks:

- Be aware of vishing. For organizations, educating users helps them identify vishing attacks, so they can ignore and report them. For individuals, never give out private information to someone contacting you from a text message or voice call. A legitimate institution will give the main number to call so that you can verify it's an official call.
- Identify pressure and scare tactics. Scammers will pressure targeted users into sending money immediately, either using credit cards, bank transfers, or even gift cards. For instance, a common way to get users to fall for the IRS scam is to threaten jail time if money is not sent immediately.
- Ignore calls from unknown numbers. If you do not recognize the number, let the caller go to voicemail.
- Be skeptical of any caller that wants sensitive information. Never give any caller sensitive information regardless of where the caller claims to work.

➢ Cyber warfare:

The generally accepted definition of cyberwarfare is the use of cyber attacks against a nation-state, causing it significant harm, up to and including physical warfare, disruption of vital computer systems and loss of life.

cyberwarfare generally refers to cyber attacks perpetrated by one nation-state on another, it can also describe attacks by terrorist groups or hacker groups aimed at furthering the goals of particular nations. While there are a number of examples of suspected cyberwarfare attacks in recent history, there has been no formal, agreed-upon definition for a cyber act of war, which experts generally agree would be a cyber attack that directly leads to loss of life.

What kinds of cyber weapons are used in warfare?

Examples of acts that might qualify as cyberwarfare include the following:

- viruses, phishing, computer worms and malware that can take down critical infrastructure;
- distributed denial-of-service (DDoS) attacks that prevent legitimate users from accessing targeted computer networks or devices;
- hacking and theft of critical data from institutions, governments and businesses;

- spyware or cyber espionage that results in the theft of information that compromises national security and stability;
- ransomware that holds control systems or data hostage; and
- propaganda or disinformation campaigns used to cause serious disruption or chaos.

What are the goals of cyberwarfare?

According to the Cybersecurity and Infrastructure Security Agency, the goal of cyberwarfare is to "weaken, disrupt or destroy" another nation. To achieve their goals, cyberwarfare programs target a wide spectrum of objectives that might harm national interests. These threats range from propaganda to espionage and serious disruption with extensive infrastructure disruption and loss of life to the citizens of the nation under attack.

Cyberwarfare is similar to cyber espionage, and the two terms are sometimes confused. The biggest difference is that the primary goal of a cyberwarfare attack is to disrupt the activities of a nation-state, while the primary goal of a cyber espionage attack is for the attacker to remain hidden for as long as possible in order to gather intelligence. The two activities are often used together. For example, cyber espionage can be used to build intelligence that helps a nation-state prepare for declaring a physical or cyber war.

What are the types of cyberwarfare attacks?

The threat of cyberwarfare attacks grows as a nation's critical systems are increasingly connected to the internet. Even if these systems can be properly secured, they can still be hacked by perpetrators recruited by nation-states to find weaknesses and exploit them. Major types of cyberwarfare attacks include the following.

Destabilization

In recent years, cybercriminals have been attacking governments through critical infrastructure, including such entities as transportation systems, banking systems, power grids, water supplies, dams and hospitals. The adoption of the internet of things makes the manufacturing industry increasingly susceptible to outside threats.

From a national security perspective, destabilizing critical digital infrastructure inflicts damage on vital modern services or processes. For example, an attack on the energy grid could have massive consequences for the industrial, commercial and private sectors.

Sabotage

Cyber attacks that sabotage government computer systems can be used to support conventional warfare efforts. Such attacks can block official government communications, contaminate digital systems, enable the theft of vital intelligence and threaten national security. State-sponsored or military-sponsored attacks, for example, may target military databases to get information on troop locations, weapons and equipment being used.

Data theft

Cybercriminals hack computer systems to steal data that can be used for intelligence, held for ransom, sold, used to incite scandals and chaos, or even destroyed.

The Center for Strategic and International Studies (CSIS) maintains a timeline record of cyber attacks on government agencies and defense and high-tech companies, as well as economic crimes with losses of more than $1 million. In CSIS timelines dating back to 2006, many of the recorded cyber incidents involve hacking and data theft from nation-states.

Historical examples of cyberwarfare attacks

Bronze Soldier -- 2007

In 2007, the Estonian government moved a Bronze Soldier, a painful symbol of Soviet oppression, from the center of Tallinn, the capital of Estonia, to a military cemetery on the outskirts of the city. In the following months, Estonia was hit by several major cyber attacks. This resulted in many Estonian banks, media outlets and government sites being taken offline due to unprecedented levels of traffic.

The Stuxnet worm -- 2010

The Stuxnet worm was used to attack Iran's nuclear program in what is considered one of the most sophisticated malware attacks in history. The malware targeted Iranian supervisory control and data acquisition systems and was spread with infected Universal Serial Bus devices.

Edward Snowden -- 2013

Edward Snowden, a former Central Intelligence Agency consultant, leaked details of the U.S. National Security Agency's cyber surveillance system. He attributed this act to ethical concerns about the programs he was involved with, which he says were ignored. The incident raised corporate and public awareness about how the advance of technology infringes on personal privacy and coined the term the *Snowden effect*.

DDoS attack in Ukraine -- 2014

The Russian government allegedly perpetrated a DDoS attack that disrupted the internet in Ukraine, enabling pro-Russian rebels to take control of Crimea.

Sony Pictures -- 2014

Hackers associated with the government of North Korea were blamed for a cyber attack on Sony Pictures after Sony released the film *The Interview*, which portrayed the North Korean leader Kim Jong Un in a negative light.

The Federal Bureau of Investigation found that the malware used in the attack included lines of code, encryption algorithms, data deletion methods and compromised networks that were similar to malware previously used by North Korean hackers.

***The* U.S. Office of Personnel Management -- 2015**

Cybercriminals backed by the Chinese state were accused of breaching the website of the U.S. Office of Personnel Management and stealing the data of approximately 22 million current and former government employees.

The U.S. presidential election -- 2016

The "Report on the Investigation into Russian Interference in the 2016 Presidential Election," by Special Counsel Robert Mueller, determined that Russia engaged in informational warfare to interfere with the U.S. presidential election.

The Mueller report found that Russia used social media accounts and interest groups to disrupt the political climate in the U.S. using what it called "information warfare." The operation began with discrediting the electoral system in 2014 to more explicit activities designed to benefit candidate Donald Trump in the 2016 election, according to the report.

China's Ministry of State Security -- 2018

In 2018, the U.S. Department of Justice charged two Chinese hackers associated with the Chinese government's Ministry of State Security with targeting intellectual property and confidential business information.

Short Answers

1.List out the Cyber Threats ?

2.Define Hacking ?

3.Define Security Attack ?

4.What are types of Security mechanisms ?

Long Answers

1.Explain about the Network Security ?

2.What is the difference between Vishing and Phishing ?

3.Explain about the Cyber Warfare ?

4.Define about Malware and Ransomeware ?

UNIT-III

- **Overview of Cyber security Concepts:**
- CIA Triad:

In the information security (InfoSec) community, "CIA" has nothing to do with a certain well-recognized US intelligence agency. These three letters stand for confidentiality, integrity, and availability, otherwise known as the CIA triad.

Together, these three principles form the cornerstone of any organization's security infrastructure; in fact, they (should) function as goals and objectives for every security program. The CIA triad is so foundational to information security that anytime data is leaked, a system is attacked, a user takes phishing bait, an account is hijacked, a website is maliciously taken down, or any number of other security incidents occur, you can be certain that one or more of these principles has been violated.

Security professionals evaluate threats and vulnerabilities based on the potential impact they have on the confidentiality, integrity, and availability of an organization's assets—namely, its data, applications, and critical systems. Based on that evaluation, the security team implements a set of security controls to reduce risk within their environment.

Confidentiality: Only authorized users and processes should be able to access or modify data
Integrity: Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously
Availability: Authorized users should be able to access data whenever they need to do so

These three principles are obviously top of mind for any infosec professional. But considering them as a triad forces security pros to do the tough work of thinking about how they overlap and can sometimes be in opposition to one another, which can help in establishing priorities in the implementation of security policies. We'll discuss each of these principles in more detail in a moment, but first let's talk about the origins and importance of the triad.

Confidentiality

Confidentiality refers to an organization's efforts to keep their data private or secret. In practice, it's about controlling access to data to prevent unauthorized disclosure. Typically, this involves ensuring that only those who are authorized have access to specific assets and

that those who are unauthorized are actively prevented from obtaining access. As an example, only authorized Payroll employees should have access to the employee payroll database. Furthermore, within a group of authorized users, there may be additional, more stringent limitations on precisely which information those authorized users are allowed to access. Another example: it's reasonable for ecommerce customers to expect that the personal information they provide to an organization (such as credit card, contact, shipping, or other personal information) will be protected in a way that prevents unauthorized access orConfidentiality can be violated in many ways, for example, through direct attacks designed to gain unauthorized access to systems, applications, and databases in order to steal or tamper with data. Network reconnaissance and other types of scans, electronic eavesdropping (via a man-in-the- middle attack), and escalation of system privileges by an attacker are just a few examples. But confidentiality can also be violated unintentionally through human error, carelessness, or inadequate security controls. Examples include failure (by users or IT security) to adequately protect passwords; sharing of user accounts; physical eavesdropping (also known as shoulder surfing); failure to encrypt data (in process, in transit, and when stored); poor, weak, or nonexistent authentication systems; and theft of physical equipment and storage devices.

Countermeasures to protect confidentiality include data classification and labeling; strong access controls and authentication mechanisms; encryption of data in process, in transit, and in storage; steganography; remote wipe capabilities; and adequate education and training for all individuals with access to data.

CIA triad confidentiality examples

Much of what laypeople think of as "cybersecurity" — essentially, anything that restricts access to data — falls under the rubric of confidentiality. This includes infosec's two big As: Authentication, which encompasses processes that allows systems to determine if a user is who they say they are. These include passwords and the panoply of techniques available for establishing identity: biometrics, security tokens, cryptographic keys, and the like.

Authorization, which determines who has the right to access which data: Just because a system knows who you are, it doesn't necessarily open all its data for your perusal! One of the most important ways to enforce confidentiality is establishing need-to-know mechanisms for data access; that way, users whose accounts have been hacked or who have gone rogue can't compromise sensitive data. Most operating systems enforce confidentiality in this sense by having many files only accessible by their creators or an admin, for instance.

Confidentiality can also be enforced by non-technical means. For instance, keeping hardcopy data behind lock and key can keep it confidential; so can air-gapping computers and fighting against social engineering attempts.

Integrity

In everyday usage, integrity refers to the quality of something being whole or complete. In InfoSec, integrity is about ensuring that data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable. Ecommerce customers, for example, expect product and pricing information to be accurate, and that quantity, pricing, availability, and other information will not be altered after they place an order. Banking customers need to be able to trust that their banking information and account balances have not been tampered with. Ensuring integrity involves protecting data in use, in transit (such as when sending an email or uploading or downloading a file), and when it is stored, whether on a laptop, a portable storage device, in the

data center, or in the cloud.

Countermeasures that protect data integrity include encryption, hashing, digital signatures, digital certificates Trusted certificate authorities (CAs) issue digital certificates to organizations to verify their identity to website users, similar to the way a passport or driver's license can be used to verify an individual's identity. , intrusion detection systems, auditing, version control, and strong authentication mechanisms and access controls.

CIA triad integrity examples

The techniques for maintaining data integrity can span what many would consider disparate disciplines. For instance, many of the methods for protecting confidentiality also enforce data integrity: you can't maliciously alter data that you can't access, after all. We also mentioned the data access rules enforced by most operating systems: in some cases, files can be read by certain users but not edited, which can help maintain data integrity along with availability.

But there are other ways data integrity can be lost that go beyond malicious attackers attempting to delete or alter it. For instance, corruption seeps into data in ordinary RAM as a result of interactions with cosmic rays much more regularly than you'd think. That's at the exotic end of the spectrum, but any techniques designed to protect the physical integrity of storage media can also protect the virtual integrity of data.

Availability

Systems, applications, and data are of little value to an organization and its customers if they are not accessible when authorized users need them. Quite simply, availability means that networks, systems, and applications are up and running. It ensures that authorized users have timely, reliable access to resources when they are needed.

Many things can jeopardize availability, including hardware or software failure, power failure, natural disasters, and human error. Perhaps the most well-known attack that threatens availability is the denial-of-service attack, in which the performance of a system, website, web-based application, or web-based service is intentionally and maliciously degraded, or the system becomes completely unreachable.

Countermeasures to help ensure availability include redundancy (in servers, networks, applications, and services), hardware fault tolerance (for servers and storage), regular software patching and system upgrades, backups, comprehensive disaster recovery plans, and denial-of-service protection solutions.

Applying the Principles

Depending on an organization's security goals, the industry, the nature of the business, and any applicable regulatory requirements, one of these three principles might take precedence over another.

A key concept to understand about the CIA triad is that prioritizing one or more principles can mean the tradeoff of others. For example, a system that requires high confidentiality and integrity might sacrifice lightning-speed performance that other systems (such as ecommerce) might value more highly. This tradeoff is not necessarily a bad thing; it is a conscious choice. Each organization must decide how to apply these principles given their unique requirements, balanced with their desire to provide a seamless and safe user experience.

➢ Non-Repudiation

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

Digital signatures (combined with other measures) can offer non-repudiation when it comes to online transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place. In this context, non-repudiation refers to the ability to ensure that a party to a contract or a communication must accept the authenticity of their signature on a document or the sending of a message.

Non-repudiation Principles

Non-repudiation requires the creation of artifacts which may be used to dispute the claims of an entity or organization that denies being the originator of an action or communication. These artifacts consist of:

- An identity
- The authentication of that identity
- Tangible evidence connecting the identified party to a particular communication or action

Non-repudiation Techniques

For email transmission, non-repudiation typically involves using methods designed to ensure that a sender can't deny having sent a particular message, or that a message recipient can't deny having received it. Techniques would include email tracking.

Cryptographic hash functions may be used to establish the integrity of transmitted documents. No encryption keys are involved, and strong hash functions are designed to be irreversible. Moreover, they're designed to avoid collision, which occurs in the rare cases where two separate documents give rise to the same hash value.

Why is the CIA triad important?

It's instructive to think about the CIA triad as a way to make sense of the bewildering array of security software, services, and techniques that are in the marketplace. Rather than just throwing money and consultants at the vague "problem" of "cybersecurity," we can ask focused questions as we plan and spend money: Does this tool make our information more secure? Does this service help ensure the integrity of our data? Will beefing up our infrastructure make our data more readily available to those who need it?

In addition, arranging these three concepts in a triad makes it clear that they exist, in many cases, in tension with one another. We'll dig deeper into some examples in a moment, but some contrasts are obvious: Requiring elaborate authentication for data access may help ensure its confidentiality, but it can also mean that some people who have the right to see that data may find it difficult to do so, thus reducing availability. Keeping the CIA triad in mind as you establish information security policies forces a team to make productive decisions about which of the three elements is most important for specific sets of data and for the organization as a whole.

CIA triad examples

Consider the example of a bank ATM, which can offer users access to bank balances and other information. An ATM has tools that cover all three principles of the triad:

It provides confidentiality by requiring two-factor authentication (both a physical card and a PIN

- code) before allowing access to data
- The ATM and bank software enforce data integrity by ensuring that any transfers or withdrawals made via the machine are reflected in the accounting for the user's bank account
- The machine provides availability because it's in a public place and is accessible even when the bank branch is closed.

➢ Incidence Response

When a security incident occurs, every second matters. Malware infections rapidly spread, ransomware can cause catastrophic damage, and compromised accounts can be used for privilege escalation, leading attackers to more sensitive assets.

Whatever the size of your organization, you should have a trained incident response team tasked with taking immediate action when incidents happen. Read on to learn a six-step process that can help your incident responders take action faster and more effectively when the alarm goes off.

➢ Key Concepts

Steps: 6 Steps for Responding to Security Incidents

What is incident response?

Incident response (IR) is a structured methodology for handling security incidents, breaches, and cyber threats. A well-defined incident response plan (IRP) allows you to effectively identify, minimize the damage, and reduce the cost of a cyber attack, while finding and fixing the cause to prevent future attacks.

During a cybersecurity incident, security teams face many unknowns and a frenzy of activity. In such a hectic environment, they may fail to follow proper incident response procedures to effectively limit the damage. This is important because a security incident can be a high-pressure situation, and your IR team must immediately focus on the critical tasks at hand. Clear thinking and swiftly taking pre-planned incident response steps during a security incident can prevent many unnecessary business impacts and reputational damage.

Why should you immediately report a cybersecurity incident?

When a cybersecurity incident is confirmed by security analysts, it is important to inform relevant parties as soon as possible. Privacy laws such as GDPR and California's CCPA require public notification, and in some cases personal notification to data subjects, in the event of a data breach.

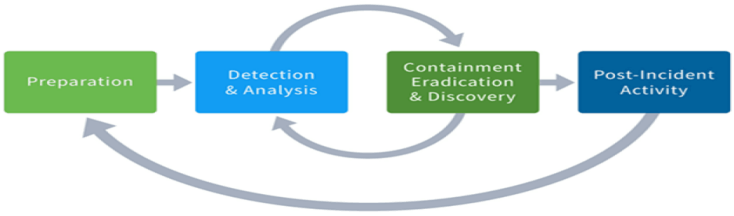
Depending on the severity of the breach, legal, press and executive management should be involved. In many cases, other departments such as customer service, finance or IT need to take immediate action. Your incident response plan should clearly state, depending on the type and severity of the breach, who should be informed. The plan should include full contact details and how to communicate with each relevant party, to save time in the aftermath of an attack.

What are the 6 steps of incident response?

The first priority when implementing incident response cyber security is to prepare in advance by putting a concrete IR plan in place. Your incident response methodology should be battle-tested before a significant attack or data breach occurs. It should address the following response phases as defined by NIST Computer Security Incident Handling Guide (SP 800-61).

- **Preparation** – Planning in advance how to handle and prevent security incidents
- **Detection and Analysis** – Encompasses everything from monitoring potential attack vectors, to looking for signs of an incident, to prioritization

- **Containment, Eradication, and Recovery** – Developing a containment strategy, identifying and mitigating the hosts and systems under attack, and having a plan for recovery
- **Post-Incident Activity** – Reviewing lessons learned and having a plan for evidence retention



Figu ybersecurity incident

re specific incident response steps

t l:

1. **Assemble your team:**

   It's critical to have the right people with the right skills, along with associated tribal knowledge. Appoint a team leader who will have overall responsibility for responding to the incident. This person should have a direct line of communication with management so that important decisions—such as taking key systems offline if necessary—can be made quickly.

In smaller organizations, or where a threat isn't severe, your SOC team or managed security consultants may be sufficient to handle an incident. But for the more serious incidents, you should include other relevant areas of the company such as corporate communications and human resources.

If you have built a Security Incident Response Team (CSIRT), now is the time to activate your team, bringing in the entire range of pre-designated technical and non-technical specialists.

If a breach could result in litigation, or requires public notification and remediation, you should notify your legal department immediately.

2. **Detect and ascertain the source.**

The IR team you've assembled should first work to identify the cause of the breach, and then ensure that it's contained.

Security teams will become aware that an incident is occurring or has occurred from a very wide variety of indicators, including:

- Users, system administrators, network administrators, security staff, and others from within your organization reporting signs of a security incident
- SIEMs or other security products generating alerts based on analysis of log data
- File integrity checking software, using hashing algorithms to detect when important files have been altered

- Anti-malware programs
- Logs (including audit-related data), which should be systematically reviewed to look at anomalous and suspicious activity with:
    - Users
    - External storage
    - Real-time memory
    - Network devices
    - Operating systems
    - Cloud services
    - Applications

3. Contain and recover:

A security incident is analogous to a forest fire. Once you've detected an incident and its source, you need to contain the damage. This may involve disabling network access for computers known to be infected by viruses or other malware (so they can be quarantined) and installing security patches to resolve malware issues or network vulnerabilities. You may also need to reset passwords for users with accounts that were breached, or block accounts of insiders that may have caused the incident. Additionally, your team should back up all affected systems to preserve their current state for later forensics.

Next, move to any needed service restoration, which includes two critical steps:

1. Perform system/network validation and testing to certify all systems as operational.
2. Recertify any component that was compromised as both operational and secure.

Ensure your long-term containment strategy includes not only returning all systems to production to allow for standard business operation, but also locking down or purging user accounts and backdoors that enabled the intrusion.

4. Assess the damage and severity

Until the smoke clears it can be difficult to grasp the severity of an incident and the extent of damage it has caused. For example, did it result from an external attack on servers that could shut down critical business components such as an e-commerce or reservation systems? Or, for example, did a web application layer intrusion perform a SQL Injection attack to execute malicious SQL statements on a web application's database or potentially use a web server as a pathway to steal data from or control critical backend systems? If critical systems are involved, escalate the incident and activate your CSIRT or response team immediately.

5.Begin the notification process

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized person.

6. Privacy laws such as GDPR and California's CCPA require public notification in the event of such a data breach. Notify affected parties so they can protect themselves from identity theft or other fallout from the disclosure of confidential personal or financial data.

7. Start now to prevent the same type of incident in the future

Once a security incident has been stabilized, examine lessons learned to prevent recurrences of similar incidents. This might include patching server vulnerabilities, training employees on how to avoid phishing scams, or rolling out technologies to better monitor insider threats. Fixing security flaws or vulnerabilities found during your post-incident activities is a given.

Also, review lessons learned from the incident and implement appropriate changes to your security policies with training for staff and employees. For example, if the attack resulted from an unwitting employee opening an Excel file as an email attachment, implement a company-wide policy and training on how to recognize and respond to a phishing email.

Every organization will have different incident response steps based on their unique IT environment and business needs. Study industry guides such as those published by NIST to ensure your IR planning includes all the necessary incident response steps to protect your organization when a cybersecurity incident occurs.

Conclusion

An incident response methodology enables organizations to define response countermeasures in advance. There is a wide range of approaches to IR. The majority of security professionals agree with the six incident response steps recommended by NIST, including preparation, detection and analysis, containment, eradication, recovery, and post-incident audits.

When it comes to preparation, many organizations leverage a combination of assessment checklists, detailed incident response plans, summarized and actionable incident response playbooks, as well as policies that can automate some of the processes. While well-planned, an incident response methodology should remain flexible, allowing for continuous improvement.

➢ Introduction to frame work and Best Practices

Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk

across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

1 Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.
- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector

- guidance most frequently referenced during the Framework development process.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of criticalservices.The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
  The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are

integrated into an organization's management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints.

Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reductionof cybersecurity risk.

Successful implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination. Still, Tier selection and designation naturally affect Framework Profiles. The Tier recommendation by Business/Process Level managers, as approved by the Senior Executive Level, will help set the overall tone for how cybersecurity risk will be managed within the organization, and should influence prioritization within a Target Profile and assessments of progress in addressing gaps. The Tier definitions are as follows:

Tier 1: Partial

- Risk Management Process – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Risk Management Program – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- External Participation – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

Tier 2: Risk Informed

- Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Risk Management Program – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- External Participation – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

Tier 3: Repeatable

- Risk Management Process – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- Integrated Risk Management Program – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
- External Participation - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

Tier 4: Adaptive

- Risk Management Process – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive

- indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
- Integrated Risk Management Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.
- External Participation - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supplychain relationships.

3 Framework Profile

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components andrecognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations. This Framework does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory can contribute to the roadmap described above. Prioritizing the mitigation of gaps is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. Furthermore, the Framework is a risk-based approach where the applicability and fulfillment of a given Subcategory is subject to the Profile's scope.

Coordination of Framework Implementation

Figure 2 describes a common flow of information and decisions at the following levels within anorganization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operationslevel for awareness of business impact.

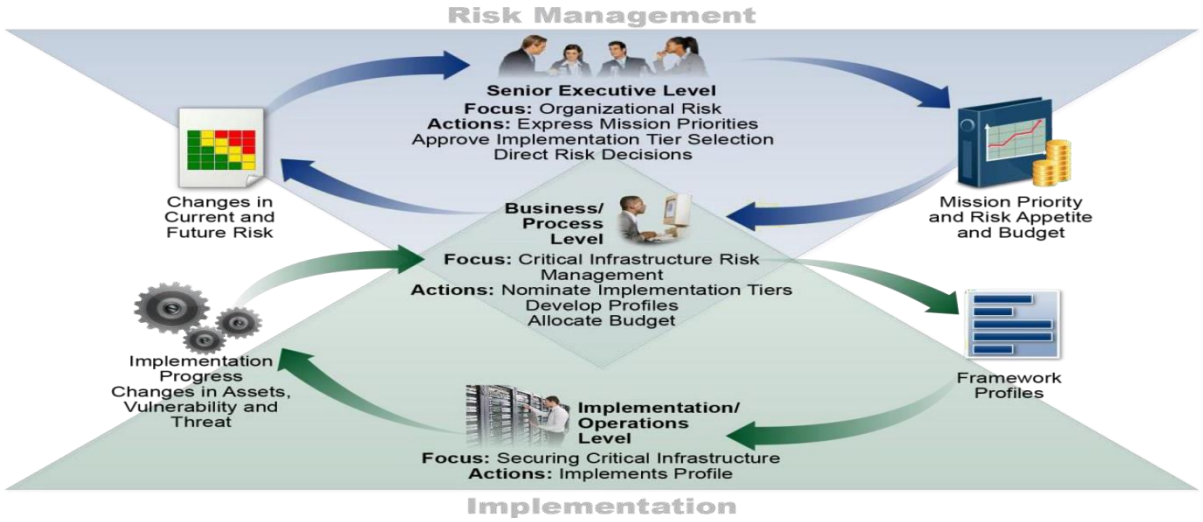


Figure 2: Notional Information and Decision Flows within an Organization

Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization's current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and

how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen theircybersecurity practices where and when deemed necessary.

Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identifythreats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent stepsby providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflectcriteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and

Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

➢ IT Goverance:

Methodology to Protect Privacy and Civil Liberties

This section describes a methodology to address individual privacy and civil liberties implications that may result from cybersecurity. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program engender privacy and civil liberties considerations. Technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and cybersecurity have a strong connection. An organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed. Some examples include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; and cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including some types of incident detection or monitoring that may inhibit freedom of expression or association.

The government and its agents have a responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or its agents that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.

To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality,integrity, and security; and accountability and auditing.

Governance of cybersecurity risk

- An organization's assessment of cybersecurity risk and potential risk responses considersthe privacy implications of its cybersecurity program.

- Individuals with cybersecurity-related privacy responsibilities report to appropriatemanagement and are appropriately trained.
- Process is in place to support compliance of cybersecurity activities with applicableprivacy laws, regulations, and Constitutional requirements.
- Process is in place to assess implementation of the above organizational measures andcontrols.

Approaches to identifying, authenticating, and authorizing individuals to accessorganizational assets and systems

- Steps are taken to identify and address the privacy implications of identity management and access control measures to the extent that they involve collection, disclosure, or useof personal information.

Awareness and training measures

- Applicable information from organizational privacy policies is included in cybersecurityworkforce training and awareness activities.
- Service providers that provide cybersecurity-related services for the organization areinformed about the organization's applicable privacy policies.

Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization's anomalous activitydetection and cybersecurity monitoring.

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities.
- Process is in place to conduct a privacy review of an organization's cybersecurity mitigation efforts

➢ Cybersecurity Compliance and Audit

No longer is a cyber attack a rare phenomenon in the world we live in. Nowadays, there is a very good chance that one will affect your company. In recent years, protecting the security of your digital perimeter has become a necessity since the consequences of failing to do so are grave. Because navigating the ever-changing sea of regulations, threats, existing defense strategies and third-party risks is a challenge, obtaining a cyber security audit is one of the best ways to reduce your risk level by protecting your business and its equipment.

The Benefits Of A Cyber Security Compliance Audit

It is often useful to solicit an objective perspective on your operations, and IT security audits are one of the best assessment tools available today. Investing in a cyber security audit can help you in four primary ways:

- Auditors have knowledge of current regulations and standards. Armed with this expertise, they can analyze your information systems, controls and practices, flag potential gaps or weaknesses and recommend solutions.
- Auditors are neutral outside entities that can evaluate vulnerabilities in your technology and assess its attractiveness to bad actors.

- Since auditors are objective, they often provide insights about your entire organizational structure that key management personnel lack because of their close proximity to the situation.
- Auditors provide credibility. This is particularly critical when it comes to your privacy policy. A third-party assessor will provide assurance that the mechanisms you have put in place are as effective as you claim them to be.

Conducting the auditing process provides your company with a report that will assess your preparedness in guarding against cyber security breaches of all kinds. With this information in hand, your team can make internal modifications, including changes to training protocols, data storage, program security and threats monitoring.

The Scope Of A Cybersecurity Audit

One of the jobs of your company's stakeholder team is to design your own cyber security audit template. This framework helps you to conduct an analysis, evaluate the effectiveness of your current solutions and plan your improved compliance strategy. A cyber security audit framework addresses how well your company identifies, detects, protects, responds and recovers from breaches and other incidents. Specifically, you are expected to document compliance in the following areas:

- Risk management, including hardware, software, assets and system interconnections. Risk level must be communicated to all stakeholders throughout the organization.
- Contractor systems, including the availability, integrity and confidentiality of all services and systems that are outsourced to third parties.
- Configuration management, including settings and baselines for all information systems as well as routine audit procedures.
- Identity, credential and access management with a related audit for these procedures.
- Implementing training in security and privacy.
- Implementing processes, protocols, assessments and procedures for continuous monitoring of information security.
- Incident response plan.
- Contingency plan.

All federal agencies must submit reports semi annually as well as FISMA audits by March 1 of each year. If your company does business with any such agency or receives government grant funding, you too must be FISMA-compliant. The more your controls, procedures and systems gel with the current FISMA gold standard, the lower is your risk. Combine that with higher client satisfaction, and your investment of time, people, resources and education/training will be more than worthwhile.

While top-of-the-line cyber security audit programs are an absolute necessity for modern businesses, it is equally important to address ongoing compliance after the audit has been completed. That means documenting your comprehensive security efforts as well as your processes for identifying vulnerabilities and closing gaps. To that end, a staff member should be given the role of remediation specialist.

This job includes having the skill set to focus on and address security incidents when they arise. Once identified, others can test all components, learn about and understand system and cost constraints, devise and practice corrective steps and eventually incorporate them into the company's information protection infrastructure.

These days, the news headlines are filled with sobering tales about the disruptive and financially destructive consequences of security and data breaches. This is an issue that shows no signs of going away anytime soon. Understanding the compliance requirements that legally pertain to

your company is the first step. Once armed with this information, you can find a respected third-party auditor who can guide you through the compliance requirements and assess your company's strengths and weaknesses pertaining to them. The time has come to get the information and support you need in the cybersecurity compliance arena.

- **pen testing (penetration testing)**

What is a pen test?

A penetration test, also called a pen test *or* ethical hacking, is a cybersecurity technique organizations use to identify, test and highlight vulnerabilities in their security posture. These penetration tests are often carried out by ethical hackers. These in-house employees or third parties mimic the strategies and actions of an attacker in order to evaluate the hackability of an organization's computer systems, network or web applications. Organizations can also use pen testing to test their adherence to compliance regulations.

Ethical hackers are information technology (IT) experts who use hacking methods to help companies identify possible entry points into their infrastructure. By using different methodologies, tools and approaches, companies can perform simulated cyber attacks to test the strengths and weaknesses of their existing security systems. *Penetration*, in this case, refers to the degree to which a hypothetical threat actor, or hacker, can penetrate an organization's cybersecurity measures and protocols.

There are three main pen testing strategies, each offering pen testers a certain level of information they need to carry out their attack. For example, white box testing provides the tester all of the details about an organization's system or target network; black box testing provides the tester no knowledge of the system; and gray box penetration testing provides the tester partial knowledge of the system.

Pen testing is considered a proactive cybersecurity measure because it involves consistent, self-initiated improvements based on the reports generated by the test. This differs from nonproactive approaches, which lack the foresight to improve upon weaknesses as they arise. A nonproactive approach to cybersecurity, for example, would involve a company updating its firewall after a data breach occurs. The goal of proactive measures, like pen testing, is to minimize the number of retroactive upgrades and maximize an organization's security.

What is the difference between pen testing and vulnerability assessment?

Pen tests are not the same as vulnerability assessments, which provide a prioritized list of security weaknesses and how to amend them, but they are often performed together. Pen testing is often conducted with a particular goal in mind. These goals typically fall under one of the following three objectives:

1. identify hackable systems
2. attempt to hack a specific system
3. carry out a data breach

Each objective focuses on specific outcomes that IT leaders are trying to avoid. For example, if the goal of a pen test is to see how easily a hacker could breach the company database, the ethical hackers would be instructed to try and carry out a data breach. The results of a pen test will not only communicate the strength of an organization's current cybersecurity protocols, but they will also present the available hacking methods that can be used to penetrate the organization's systems.

Why is pen testing important?

The rate of distributed denial-of-service, phishing and ransomware attacks is dramatically increasing, putting all internet-based companies at risk. Considering how reliant businesses are on technology, the consequences of a successful cyber attack have never been greater. A ransomware attack, for instance, could block a company from accessing the data, devices, networks and servers it relies on to conduct business. Such an attack could result in millions of dollars of lost revenue. Pen testing uses the hacker perspective to identify and mitigate cybersecurity risks before they are exploited. This helps IT leaders implement informed security upgrades that minimize the possibility of successful attacks.

Technological innovation is one of, if not the greatest, challenge facing cybersecurity. As tech continues to evolve, so do the methods cybercriminals use. In order for companies to successfully protect themselves and their assets from these attacks, they need to be able to update their security measures at the same rate. The caveat, however, is that it is often difficult to know which methods are being used and how they might be used in an attack. But, by using skilled ethical hackers, organizations can quickly and effectively identify, update and replace the parts of their system that are particularly susceptible to modern hacking techniques.

How to do penetration testing

Pen testing is unique from other cybersecurity evaluation methods, as it can be adapted to any industry or organization. Depending on an organization's infrastructure and operations, it may want to use a certain set of hacking techniques or tools. These techniques and their methodologies can also vary based on the IT personnel and their company standards. Using the following adaptable six-step process, pen testing creates a set of results that can help organizations proactively update their security protocols:

1. **Preparation.** Depending on the needs of the organization, this step can either be a simple or elaborate procedure. If the organization has not decided which vulnerabilities it wants to evaluate, a significant amount of time and resources should be devoted to combing the system for possible entry points. In-depth processes like this are usually only necessary for businesses that have not already conducted a complete audit of their systems. Once a vulnerability assessment has been conducted, however, this step becomes much easier.
2. **Construct an attack plan.** Prior to hiring ethical attackers, an IT department designs a cyber attack, or list of cyber attacks, that its team should use to perform the pen test. During this step, it is also important to define what level of system access the pen tester has.
3. **Select a team.** The success of a pen test depends on the quality of the testers. This step is often used to appoint the ethical hackers that are best suited to perform the test. Decisions like these can be made based on employee specialties. If a company wants to test its cloud security, a cloud expert may be the best person to properly evaluate its cybersecurity. Companies also often hire expert consultants and certified cybersecurity experts to carry out pen testing.
4. **Determine the stolen data type.** What is the team of ethical hackers stealing? The data type chosen in this step can have a profound impact on the tools, strategies and techniques used to acquire it.

5. **Perform the test.** This is one of the most complicated and nuanced parts of the testing process, as there are many automated software programs and techniques testers can use, including Kali Linux, Nmap, Metasploit and Wireshark.
6. **Integrate the report results.** Reporting is the most important step of the process. The results must be detailed so the organization can incorporate the findings.

➢ Mile 2 CPTE

Certified Penetration Testing Engineer (C)PTE) is an internationally recognized cyber security certification administered by the United States-based information security company Mile2. The accreditation maps to the Committee on National Security Systems' 4013 education certification. The C)PTE certification is considered one of five core cyber security certifications.

Accreditations

Obtaining the C)PTE certification requires proven proficiency and knowledge of five key information security elements, penetration testing, data collection, scanning, enumeration, exploitation and reporting.

The CPTE certification is one of several information assurance accreditations recognized by the U.S. National Security Agency. The certification has also been approved by the U.S. Department of Homeland Security's National Initiative for Cyber Security Studies and Careers (NICSS) and the U.S.-based National Security Systems Committee.

Examination

The online exam for C)PTE accreditation lasts two hours and consists of 100 multiple choice questions.

➢ OWSAP frame work

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security includes improvements in all of these areas.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security. OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Similar to many open-source software projects, OWASP produces many types of materials in a collaborative, open way.

Contact for information about communicating with OWASP Contributions for details about how to make contributions Advertising if you're interested in advertising on

the OWASP site How OWASP Works for more information about projects and governance OWASP brand usage rules for information about using the OW

About OWASP OWASP is a volunteer organization that is dedicated to developing knowledge based documentation and reference implementations and software that can be used by system architects, developers and security professionals. Our work promotes and helps consumers build more secure web applications.

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

About the OWASP Testing Project (Parts One and Two) The OWASP is currently working on a comprehensive Testing Framework. By the time you read this document Part One will be close to release and Part Two will be underway. Part One of the Testing Framework describes the Why, What, Where and When of testing the security of web applications and Part Two goes into technical details about how to look for specific issues using source code inspection and a penetration testing (for example exactly how to find SQL Injection flaws in code and through penetration testing). This check list is likely to become an Appendix to Part Two of the OWASP Testing framework along with similar check lists for source code review.

Short Answers

1.Define CIA Traid ?

2.Why is the CIA traid important ?

3.Explain the examples of CIA Traid ?

Long Answers

1.What is incident response ?

2.Explain the framework Basics ?

3.What is Pen test ?

4. Explain OWSAP frame work ?

UNIT-IV

➢ Introduction to Key Security Tools

With remotely working becoming the new normal, every organization, no matter how big or small, requires cyber security experts proficient in cyber security tools and techniques. At present, no organization can escape cyber threats and security issues without a good cyber security team. Hackers are always on the move to find loopholes in security systems to put companies in distress and benefit from it. The different aspects of cyber security, including application security, information security, network security, disaster recovery, operational security, and more are necessary to provide security from multiple cyber threats that take the form of Ransomware, Malware, Phishing, and more. Thus, cyber security tools play an important role when it comes to the protection of sensitive and private data of businesses as well as individuals.

WHAT IS NETWORK SECURITY?

Network security and security tools encompass several devices, technologies, and processes. In its simplest form, it is a set of techniques used to protect the system, accessibility, applications, confidentiality, data, and network from cyber threats. Network security is a need of the hour knowledge to escape unauthorized data access, identify theft and stay safe from cyberattacks. Information Security, App Security, Cybersecurity, Operational Security, Disaster Recovery, etc., are just a few types of network security.

WHAT ARE THE BENEFITS OF NETWORK SECURITY?

It is imperative to have an authorization and authentication system in place to protect the data and system from cyber threats, identify new users, monitor traffic, approve or block unauthorized access. In network security offers many other benefits as well like increasing productivity, managing network traffic, enhancing network performance, protecting customers' confidentiality, gaining customer trust, reducing the feasibility of websites going down, and ensuring the safe data sharing between data sources and employees.

Network security covers a wide range of functions. Some of its common capabilities include: · Firewalls

- Sandboxing
- Traffic analysis
- Malware detection
- Endpoint security
- Network Access Control
- Network mapping and visibility

Therefore, every organization and industry needs to maintain a degree of network security solutions in place to protect its vulnerabilities from ever-growing cyber threats.

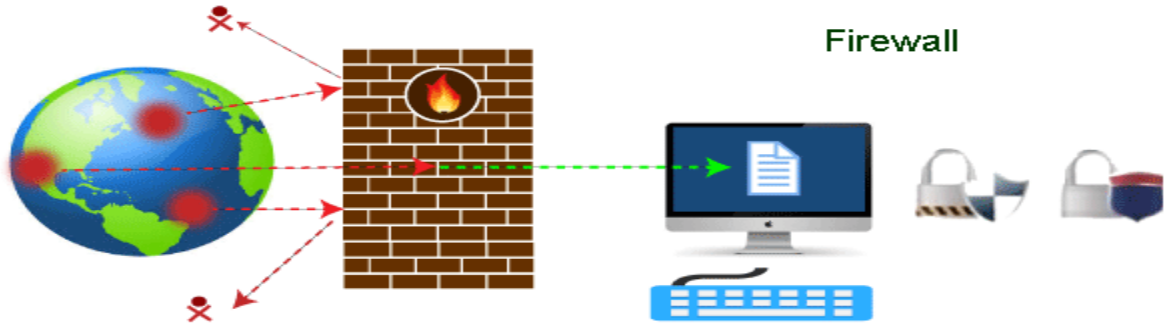
➢ Introduction to firewall

Nowadays, it is a big challenge to protect our sensitive data from unwanted and unauthorized sources. There are various tools and devices that can provide different security levels and help

keep our private data secure. One such tool is a 'firewall' that prevents unauthorized access and keeps our computers and data safe and secure. **What is a Firewall**

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious



software from accessing the Internetin infected computers.

Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security

Why Firewall

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a userspecified trusted source.

Firewalls are designed in such a way that they can react quickly to detect and counterattacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

Open Access

If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

Lost or Comprised Data

Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

Network Crashes

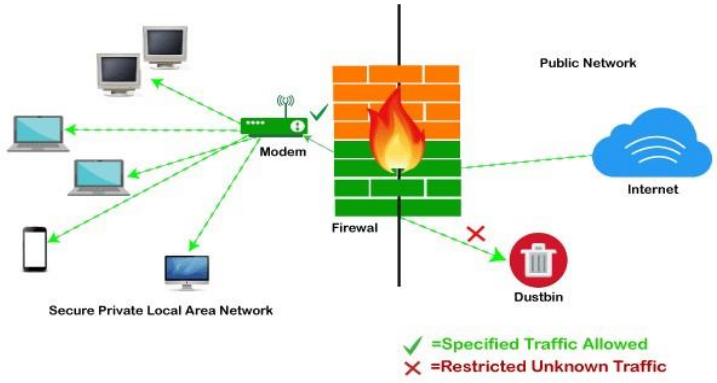
In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.

Therefore, it is essential to use firewalls and keep our network, computer, and data safe and secure from unwanted sources.

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IPaddresses, or sources.



As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

- Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control

- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

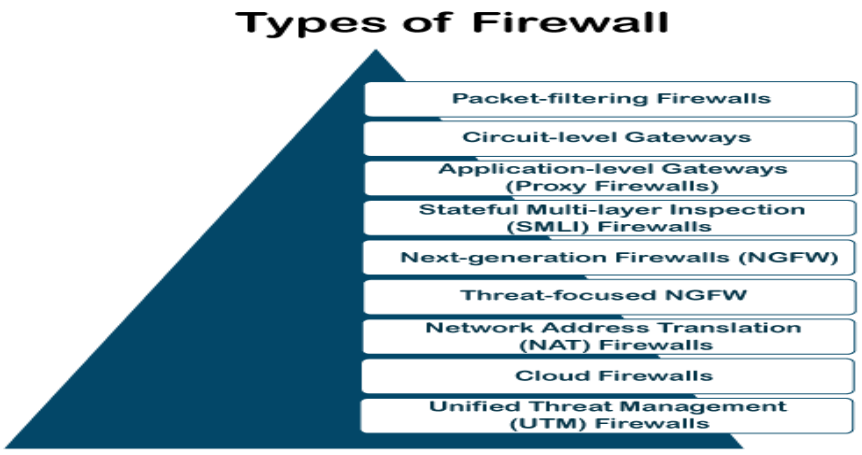
➢ Types of Firewall

There are mainly three types of firewalls, such as **software firewalls, hardware firewalls, or both**, depending on their structure. Each type of firewall has different functionality but the same purpose.

A hardware firewall is a physical device that attaches between a computer network and a gateway. For example- a broadband router. A hardware firewall is sometimes referred to as an **Appliance Firewall**. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. This type of firewall is also called a **Host Firewall**.

Besides, there are many other types of firewalls depending on their features and the level of security they provide. The following are types of firewall techniques that can be implemented as software or hardware:

- Packet-filtering Firewalls
- Circuit-level Gateways
- Application-level Gateways (Proxy Firewalls)
- Stateful Multi-layer Inspection (SMLI) Firewalls
- Next-generation Firewalls (NGFW)
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls
- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls



➢ Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.

While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations. Because these types of firewalls do not prevent web-based attacks, tare not the safest.

Circuit-level Gateways

Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying **TCP (Transmission Control Protocol)** connections and sessions. Circuit-level gateways are designed to ensure that the established sessions are protected.

Typically, circuit-level firewalls are implemented as security software or pre-existing firewalls. Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions. Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

➢ Application-level Gateways (Proxy Firewalls)

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called '**Application-level Gateways**'.

Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks. Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client.

Stateful Multi-layer Inspection (SMLI) Firewalls

Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.

In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

In most cases, SMLI firewalls are implemented as additional security levels. These types of firewalls implement more checks and are considered more secure than stateless firewalls.

Next-generation Firewalls (NGFW)

Many of the latest released firewalls are usually defined as '**next-generation firewalls**'. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include **deep-packet inspection (DPI),** surface-level packet inspection, and TCP handshake testing, etc.

NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources.

Threat-focused NGFW

Threat-focused NGFW includes all the features of a traditional NGFW. Additionally, they also provide advanced threat detection and remediation. These types of firewalls are capable of reacting against attacks quickly. With intelligent security automation, threat-focused NGFW set the security of the overall defense system.

In addition, these firewalls use retrospective security systems to monitor suspicious activities continuously. They keep analyzing the behavior of every activity even after the initial inspection. Due to this functionality, threat-focus NGFW dramatically reduces the overall time taken from threat detection to cleanup.

Network Address Translation (NAT) Firewalls

Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers.

When multiple devices are used to connect to the Internet, NAT firewalls create a unique IP address and hide individual devices' IP addresses. As a result, a single IP address is used for all devices. By doing this, NAT firewalls secure independent network addresses from attackers scanning a network for accessing IP addresses. This results in enhanced protection against suspicious activities and attacks.

In general, NAT firewalls works similarly to proxy firewalls. Like proxy firewalls, NAT firewalls also work as an intermediate device between a group of computers and external traffic.

Cloud Firewalls

Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or **FaaS (firewall-as-service)**. Cloud firewalls are typically maintained and run on the Internet by third-party vendors. This type of firewall is considered similar to a proxy firewall. The reason for this is the use of cloud firewalls as proxy servers. However, they are configured based on requirements.

The most significant advantage of cloud firewalls is scalability. Because cloud firewalls have no physical resources, they are easy to scale according to the organization's demand or traffic-load. If demand increases, additional capacity can be added to the cloud server to filter out the additional traffic load. Most organizations use cloud firewalls to secure their internal networks or entire cloud infrastructure.

Unified Threat Management (UTM) Firewalls

UTM firewalls are a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support. Such firewalls are designed to provide simplicity and ease of use. These firewalls can also add many other services, such as cloud management, etc.

Which firewall architecture is best?

When it comes to selecting the best firewall architecture, there is no need to be explicit. It is always better to use a combination of different firewalls to add multiple layers of protection. For example, one can implement a hardware or cloud firewall at the perimeter of the network, and then further add individual software firewall with every network asset.

Size of the organization

If an organization is large and maintains a large internal network, it is better to implement such firewall architecture, which can monitor the entire internal network.

Availability of resources

If an organization has the resources and can afford a separate firewall for each hardware piece, this is a good option. Besides, a cloud firewall may be another consideration.

Requirement of multi-level protection

The number and type of firewalls typically depend on the security measures that an internal network requires. This means, if an organization maintains sensitive data, it is better to implement multi-level protection of firewalls. This will ensure data security from hackers.

➢ XML Gateway-Firewalls:

An XML Gateway is an externally-facing DMZ tier of a web services platform. Generally, this DMZ tier will be facing the Internet, but it may simply be between business units or facing a leased line connecting one entity to another. It can be implemented using a software solution (such as web services support in a JEE container like WAS or JBoss) or a hardware solution (using SOA Appliances).

The XML Gateway fills some or all of following functions(depending on the environment and architecture):

- Efficient XML parsing & transformations.
- Advertising a consistent web service API to external clients.
- Serves as an entry point for Web Service traffic into an organization's systems. Serves as the termination point for inbound connections for web service calls. Especially SSL connections.
- Serves as an outbound proxy for all internal web service consumers.
- Transforming between internally-facing and externally-facing security models.
- Identity Tokens
- Encryption/Digital Signature requirements.
- Etc.
- Authentication and authorization point for both incoming and outgoing Web Service calls.
- Termination point of message-level security (WS-Security, XML Encryption, XML Digital Signature).
- Schema validation of XML-based message payloads.
- Could also be validation of other types of payloads.
- Routes messages appropriately to backend systems-ie, Service Provider tiers.
- Data transformations, potentially.
- Protocol transformations, potentially.
- Service mediation, potentially.
- Support for multiple Message Exchange Patterns (MEPs)
- Synchronous Request Respond
- Asynchronous Request and Respond Fire-and-Forget (Asynchronous one-way)

➢ Stateless and Stateful :

Stateful and Stateless firewalls appear to be familiar but they are way different from each other in terms of capability, functions, principles, etc. There are different types of firewalls and the incoming and outgoing traffic follows the set of rules organizations have determined in these firewalls. The main concern of the users is to safeguard the important data and information and prevent them from falling into the wrong hands. To secure that, they have the option to choose among the firewalls that can fulfill their requirements. they are looking for. The firewall provides critical protection to the business and its information.

1.stateful firewall

This firewall monitors the full state of active network connections. A stateful firewall tracks the state of network connections when it is filtering the data packets. These firewalls can watch the traffic streams end to end. Stateful firewalls are aware of the communication path and can implement various IP security functions such as tunnels or encryptions. These firewalls are faster and perform better under heavier traffic and are better in identifying unauthorized or forged communication.

2. how stateful firewall works

Stateful Firewall inspects packets and if the packets match with the rule in the firewall then it is allowed to go through. The packets which are approved by this firewall can travel freely in the network.

3. stateful firewall example

Could be The example is the Transport Control Protocol(TCP.) It saves the record of its connection by saving its port number, source, and destination, IP address, etc.

4. stateless firewall

This firewall watches the network traffic and is based on the source and the destination or other values. They have no data on the traffic patterns and restrict the pattern based on the destination or the source. It is also termed as the Access control list (ACL). This firewall does not inspect the traffic. It just works according to the set of rules and filter

5. how stateless firewall works

Stateless firewalls monitor the incoming traffic packets. They allow or deny packets into their network based on the source and the destination address, or some other information like traffic type. They just monitor some basic information of the packets and restriction or permission depends upon that.

6. stateless firewall example

An example of a Stateless firewall is File Transfer Protocol (FTP). This is the most common way of receiving the sending files between two computers..

7. difference between the stateful and stateless firewall

Stateful firewalls are smarter and responsible to monitor and detect the end-to-end traffic stream, and to defend according to the traffic pattern and flow. It filters the packets based on the full context given to the network connection. These firewalls are faster and work excellently, under heavy traffic flow. They are also better at identifying forged or unauthorized communication. On the other hand, a stateless firewall is basically an Access Control List (ACLs) that contains the set of rules which allows or restricts the flow of traffic depending upon the source, IP address, destination, port number, network protocols, and some other related fields. This firewall doesn't interfere in the traffic flow, they just go through the basic information about them, and allowing or discard depends upon that. But there is a chance for the forged packets or attack techniques may fool these firewalls and may bypass them.

8. Advantages and disadvantages of a stateful firewall and a stateless firewall Stateful firewall advantages-

- This firewall is smarter and faster in detecting forged or unauthorized communication. This can also make future filtering decisions on the cumulative of past and present findings.
- Not many ports are required to open for effective communication in this firewall.
- The balance between the proxy security and the packet filter performance is good.
- Powerful memory.
- Extensive logging capabilities.
- Robust attack prevention.

Stateful firewall disadvantages-

- The data transfer rate is slow.
- The firewall must be updated with the latest available technologies else it may allow the hackers to compromise or take control of the firewall.
- This firewall demands a high memory and processing power as in stateful firewall tables have to maintain and to pass the access list, logic is used.
- Some of these firewalls may be tricked to allow or attract outside connections.

Stateless firewall advantages-

- These firewalls are less complex.
- Stateless firewalls are very simple to implement.
- Performance delivery is very fast.
- Perform excellent under pressure and heavy traffic.
- As compared to a stateful firewall, stateless firewalls are much cheaper. But these days, you might see significant drops in the cost of a stateful firewall too.

Stateless firewall disadvantages-

- The main disadvantage of this firewall is trust. This firewall assumes that the packet information can be trusted. It does not examine the entire packet but just check if the packets satisfy the existing set of security rules. This firewall doesn't monitor or inspect the traffic.
- To provide and maximize the desired level of protection, these firewalls require some configurations.
- The packet will pass the firewall if an attacker sends SYN/ACK as an initial packet in the network, the host will ignore it.

9. choosing between stateful firewall and stateless firewall

There are various firewalls present in the market nowadays, and the question to choose depends on your business's needs and nature. The firewall provides security for all kinds of businesses. It is up to you to decide what type of firewall suits you the most.

- What kind of traffic flow you intend to monitor.
- What operating system best suits your requirements.
- How will this firewall fit into your network?
- What suits best to your organization, an appliance, or a network solution.
- And above all, you must know the reason why you want to implement a firewall.

10. firewall for small business

Stateless firewalls are cheaper compared to the stateful firewall. A small business may not afford the cost of a stateful firewall. Small businesses can opt for a stateless firewall and keep their business running safely. The traffic volumes are lower in small businesses, so is the threat. The fast-paced performance with the ability to perform better in heavier traffics of this firewall

attracts small businesses. Few trusted people in a small office with normal and routine capabilities can easily go along with a stateless firewall.

11. firewall for large establishments

Mainly Stateful firewalls provide security to large establishments as these are powerful and sophisticated. Because of the dynamic packets filtering, these firewalls are preferred by large establishments as they offer better security features. Stateful firewalls are powerful. They, monitor, and detect threats, and eliminate them. Large corporations opt for a stateful firewall because it provides levels of security layers along with continuous monitoring of traffic.

➢ Firewall Configuration

A basic guide to configure a firewall in 5 steps: create zones, configure settings, and review firewall rules.

As the first line of defense against online attackers, your firewall is a critical part of your network security. Configuring a firewall can be an intimidating project, but breaking down the work into simpler tasks can make the work much more manageable. The following guidance will help you understand the major steps involved in firewall configuration.

There are many suitable firewall models that can be used to protect your network. You can consult a HIPAA security expert or PCI security expert to learn more about your options. The following steps are critical, regardless of the firewall model you choose. This guide assumes that you are using a business grade firewall that supports multiple internal networks (or zones) and performs stateful packet inspection.

As a heads up, due to the technical nature of firewalls, a detailed step-by-step guide is beyond the scope of this blog post. However, I will provide some direction to help illustrate the process so you can understand how to configure a firewall in 5 steps.

Step 1: Secure your firewall

If an attacker is able to gain administrative access to your firewall it is “game over” for your network security. Therefore, securing your firewall is the first and most important step of this process. Never put a firewall into production that is not properly secured by at least the following configuration actions:

Update your firewall to the latest firmware. Delete, disable, or rename any default user accounts and change all default passwords. Make sure to use only complex and secure passwords.

- If multiple administrators will manage the firewall, create additional administrator accounts with limited privileges based on responsibilities. Never use shared user accounts.
- Disable simple network management protocol (SNMP) or configure it to use a secure community string.

Step 2: Architect your firewall zones and IP addresses

In order to protect the valuable assets on your network, you should first identify what the assets (for example, payment card data or patient data) are. Then plan out your network structure so that these assets can be grouped together and placed into networks (or zones) based on similar sensitivity level and function.

For example, all of your servers that provide services over the internet (web servers, email servers, virtual private network (VPN) servers, etc.) should be placed into a dedicated zone that will allow limited inbound traffic from the internet (this zone is often called a demilitarized zone

or DMZ). Servers that should not be accessed directly from the internet, such as database servers, must be placed in internal server zones instead. Likewise, workstations, point of sale devices, and voice over Internet protocol (VOIP) systems can usually be placed in internal network zones. Generally speaking, the more zones you create, the more secure your network. But keep in mind that managing more zones requires additional time and resources, so you need to be careful when deciding how many network zones you want to use.

If you are using IP version 4, Internal IP addresses should be used for all of your internal networks. Network address translation (NAT) must be configured to allow internal devices to communicate on the Internet when necessary.

Once you have designed your network zone structure and established the corresponding IP address scheme, you are ready to create your firewall zones and assign them to your firewall interfaces or subinterfaces. As you build out your network infrastructure, switches that support virtual LANs (VLANs) should be used to maintain level-2 separation between the networks.

Step 3: Configure access control lists

Now that you have established your network zones and assigned them to interfaces, you should determine exactly which traffic needs to be able to flow into and out of each zone.

This traffic will be permitted using firewall rules called access control lists (ACLs), which are applied to each interface or subinterface on the firewall. Make your ACLs specific to the exact source and/or destination IP addresses and port numbers whenever possible. At the end of every access control list, make sure there is a "deny all" rule to filter out all unapproved traffic. Apply both inbound and outbound ACLs to each interface and subinterface on your firewall so that only approved traffic is allowed into and out of each zone.

Whenever possible, it is generally advised to disable your firewall administration interfaces (including both secure shell (SSH) and web interfaces) from public access. This will help to protect your firewall configuration from outside threats. Make sure to disable all unencrypted protocols for firewall management, including Telnet and HTTP connections.

Step 4: Configure your other firewall services and logging

If your firewall is also capable of acting as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion prevention system (IPS), etc., then go ahead and configure the services you wish to use. Disable all the extra services that you don't intend to use.

Step 5: Test your firewall configuration

Don't forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations. Testing your firewall should include both vulnerability scanning and penetration testing. Always remember to keep a backup of your firewall configuration saved in a secure place so that all of your hard work is not lost in the event of a hardware failure.

Firewall management

With your firewall in production, you have finished your firewall configuration, but firewall management has just begun. Logs must be monitored, firmware must be updated, vulnerability scans must be performed, and firewall rules must be reviewed at least every six months. Last of all, be sure to document your process and be diligent about performing these ongoing tasks to ensure t6hat your firewall continues to protect your network.

➢ Antivirus/Antimalware

Antivirus software, or **antivirus software** (abbreviated to **AV software**), also known as **anti-malware**, is a computer program used to prevent, detect, and remove malware.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other malware, antivirus software started to protect from other computer threats. In particular, modern antivirus software can protect users from malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud tools, adware, and spyware.

Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT), and botnet DDoS attacks.

Identification methods

There are several methods which antivirus engines can use to identify malware:

- **Sandbox detection**: a particular behavioural-based detection technique that, instead of detecting the behavioural fingerprint at run time, it executes the programs in a virtual environment, logging what actions the program performs. Depending on the actions logged, the antivirus engine can determine if the program is malicious or not. If not, then, the program is executed in the real environment.
- Data mining techniques: one of the latest approaches applied in malware detection. Data mining and machine learning algorithms are used to try to classify the behaviour of a file (as either malicious or benign) given a series of file features that are extracted from the file itself.

Signature-based detection

When a malware arrives in the hands of an antivirus firm, it is analysed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software. Although the signature-based approach can effectively contain malware outbreaks, malware authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and, more recently, "metamorphic" viruses, which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary.

Heuristics

Many viruses start as a single infection and through either mutation or refinements by other attackers, can grow into dozens of slightly different strains, called variants. Generic detection refers to the detection and removal of multiple threats using a single virus definition.

While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a generic signature or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie.

Rootkit detection

Anti-virus software can attempt to scan for rootkits. A rootkit is a type of malware designed to gain administrative-level control over a computer system without being detected. Rootkits can change how the operating system functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult to remove, in some cases requiring a complete re-installation of the operating system. **Real-time protection**

Real-time protection, on-access scanning, background guard, resident shield, auto protect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs. This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects. Real-time protection detects threats in opened files and scans apps in real-time as they are installed on the device. When inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed

Performance and drawbacks

Antivirus software has some drawbacks, first of which that it can impact a computer's performance..

Antivirus software itself usually runs at the highly trusted kernel level of the operating system to allow it access to all the potential malicious process and files, creating a potential avenue of attack. Anti-virus software has highly privileged and trusted access to the underlying operating system, which makes it a much more appealing target for remote attacks. Additionally anti-virus software is "years behind security-conscious client-side applications like browsers or document readers. It means that Acrobat Reader, Microsoft Word or Google Chrome are harder to exploit than 90 percent of the anti-virus products out there", researcher with Coseinc, a Singapore-based information security consultancy.

Alternative solutions

Antivirus software running on individual computers is the most common method employed of guarding against malware, but it is not the only solution. Other solutions can also be employed by users, including Unified Threat Management (UTM), hardware and network firewalls, Cloud-based antivirus and online scanners.

Hardware and network firewall

Network firewalls prevent unknown programs and processes from accessing the system. However, they are not antivirus systems and make no attempt to identify or remove anything. They may protect against infection from outside the protected computer or network, and limit the activity of any malicious software which is present by blocking incoming or outgoing requests on certain TCP/IP ports. A firewall is designed to deal with broader system threats that come from network connections into the system and is not an alternative to a virus protection system.

Cloud antivirus

Cloud antivirus is a technology that uses lightweight agent software on the protected computer, while offloading the majority of data analysis to the provider's infrastructure,cloud antivirus involves scanning suspicious files using multiple antivirus engines. This approach was proposed by an early implementation of the cloud antivirus concept called CloudAV. CloudAV was designed to send programs or documents to a network cloud where multiple antivirus and

behavioral detection programs are used simultaneously in order to improve detection rates. Parallel scanning of files using potentially incompatible antivirus scanners is achieved by spawning a virtual machine per detection engine and therefore eliminating any possible issues. CloudAV can also perform "retrospective detection," whereby the cloud detection engine rescans all files in its file access history when a new threat is identified thus improving new threat detection speed. Finally, CloudAV is a solution for effective virus scanning on devices that lack the computing power to perform the scans themselves.

Online scanning

Some antivirus vendors maintain websites with free online scanning capability of the entire computer, critical areas only, local disks, folders or files. Periodic online scanning is a good idea for those that run antivirus applications on their computers because those applications are frequently slow to catch threats. One of the first things that malicious software does in an attack is disable any existing antivirus software and sometimes the only way to know of an attack

is by turning to an online resource that is not installed on the infected computer

Specialized tools

Virus removal tools are available to help remove stubborn infections or certain types of infection. Examples include Avast Free Anti- Malware, AVG Free Malware Removal Tools, and Avira AntiVir Removal Tool. It is also worth noting that sometimes antivirus software can produce a false positive result, indicating an infection where there is none.

A rescue disk that is bootable, such as a CD or USB storage device, can be used to run antivirus software outside of the installed operating system, in order to remove infections while they are dormant. A bootable antivirus disk can be useful when, for example, the installed operating system is no longer bootable or has malware that is resisting all attempts to be removed by the installed antivirus software.

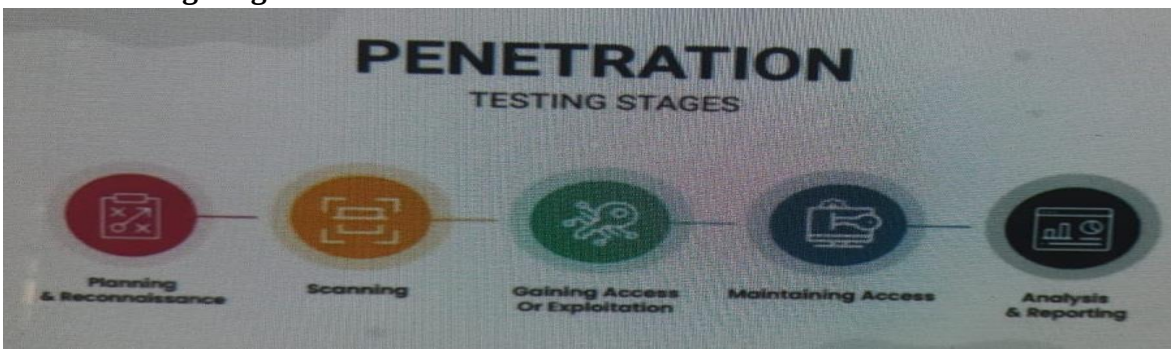
➢ Penetration test Methodologies

Penetration testing encompasses various manual and automated techniques to simulate an attack on an organization's information systems. An ethical hacker or pen tester generally conducts pen testing, who tries to break into the corporate information systems and identify and exploit known and unknown vulnerabilities before an actual attacker or a malicious actor does. The security tester primarily carries out an active analysis of the target system to identify any potential threats or vulnerabilities that could result from improper system configuration, system infrastructure flaws or operational incompetency.

Why should an organisation carry out pen testing?

To determine threats and weaknesses in the overall infrastructure, both hardware, and software, to develop a sound security control system.To uncover gaps within the organisation existing security posture and address them specifically and effectively. To ensure that the security system or controls in place are effective and mitigate the risks of an attack. To prioritise attack vectors and secure attack avenues that are more prone to an attack. To discover existing bugs in the security control system and fix them. To determine and detect the possible magnitude of the breach and to improve the overall security response time to an attack.

Penetration Testing Stages



Security test or Penetration test involves simulated breaching of any number of applications or systems such as application protocol interfaces, front-end or back-end servers, security infrastructure, and unsensitised inputs to detect vulnerabilities and threats.

The pen testing process usually includes five stages and helps the organisation to fine-tune their environment for fixing security loopholes.

The stages are as follows:

1. Planning and Reconnaissance

This stage includes defining the scope, priorities, and goals to be achieved. It also states the primary critical systems to be tested or addressed and types of test to be performed.

The reconnaissance stage includes gathering intelligence like passive and active information on network and domain names or mail servers et al. of the target system to better understand how a target works and its potential entry points.

2. Scanning

This stage involves understanding how the target system responds to various automated intrusion attempts and attacks. This is typically done using following.

Static Analysis – Inspects the application source code before a program is run by comparing it to a set of coding rules followed by debugging

Dynamic Analysis – is the testing and evaluation of the security system by executing data in realtime. The objective here is to find errors or vulnerabilities in real-time by scanning the application or systems using automated security scanning tools. Static or dynamic analysis is followed by manual verification of vulnerabilities or errors to eliminate false positives.

3. Gaining Access or Exploitation

In this stage, the vulnerabilities identified are actively exploited to gain access to the system or valuable information. The vulnerabilities can be exploited by escalating privileges, stealing data, intercepting traffic and injecting malicious code to understand or observe the magnitude of the damage caused.

4. Maintaining Access

The objective of this stage is to check if persistence access can be maintained after gaining access to the application or its underlying system. The longer the attacker maintains access to the

system, the more in-depth access he/she gains. The goal is to imitate and detect advanced persistent threats that often remain in a system without being detected.

5. Analysis and Reporting

The results of the test are then compiled into a detailed report. The report primarily contains vulnerabilities that were exploited, sensitive data that was breached and accessed, and the amount of time the security tester could remain in the system before getting detected.

Penetration Testing Methods

Many penetration testing methods are depending upon the security system and the level of motivation of the organisation. A security expert or a Cyber Security Firm should help you choose or determine a perfect match as per the organisation's requirements.

The different types of pen testing methods are as follows. Depending upon the type of information a security expert or a pen tester has, the methods can be divided into:

Black Box

A black box assessment is carried out with little information provided to the pen tester. The security consultant or the tester will have very limited knowledge about the security control system or the infrastructure. Typically, the consultant will undertake the reconnaissance methodology to gain information about the system and security infrastructure.

White Box

In the white box assessment, the tester or the consultant is provided with information and detailed documentation regarding the infrastructure, applications, equipment's and security control system such as system architecture documents, source code and more. It is a comprehensive assessment method to identify and detect external as well internal vulnerabilities.

Grey Box

In this assessment method, the tester is provided with user-level knowledge and information needed to assess the security control system. The testers are also granted limited access and partial knowledge to the web applications and the internal network infrastructure.

Physical Penetration Tests

The organisation should be wary of hackers adopting a physical approach to gain facility access either as a standalone attack or to complement their technical attacks. The following are physical **penetration tests:**

Scoping Unsecured Areas: In this method, hackers' scope or search areas or systems that are vulnerable and are more prone to a breach or an attack. This may include smoking areas, maintenance docks, and unguarded entrances with the least resistance and visibility to gain facility access.

Piggybacking: Piggybacking, tailgating or eavesdropping are some methods wherein a hacker closely follows the employees or maintenance workers that have access to the facility area.

Social Engineering Test

These tests verify the Human Network of an organisation. This test helps determine and secure an attack from within an organization from the employee who is either initiating an attack or has his credentials or privileged access compromised. The types of attacks are:

Phishing: A deceptive method wherein personal information is gained by sending across malicious or infected codes via mail or messages.

Pretexting: Pretexting is a form of identity theft wherein the hackers present themselves as someone else who is a part of an organisation and gain access to the security infrastructure or sensitive data. most common types of pen testing / security testing:

Types of Penetration Testing Network Penetration Testing
A network penetration test is the most common and in-demand pen test method, which helps detect and exploit vulnerabilities in the network system or infrastructure. There are three types of Network pen testing, external, internal, and wireless.

External Network Penetration Testing: .
This test generally targets network areas like Firewall configuration, firewall bypass, IPS deception and DNS level attacks. Vulnerability scanning is a type of test or an automated process that utilises the shelf tools to scan and detect known vulnerabilities in your system.

A combination of automated and manual exploitation techniques is a process wherein the vulnerabilities after detection are targeted, and a variety of attacks are simulated against these weaknesses with an aim to completely take over the internet-facing systems.

Internal Network Pen Testing: This test includes identifying or detecting security network weaknesses within your internal systems or infrastructure. This test too includes vulnerability scanning and exploitation techniques to detect the vulnerabilities and then exploit them to see how the internal systems respond.

The internal network pen test fundamentally evaluates the potential of an exploit by an internal user or an unauthorised attack by an employee of the organisation, such as potential unauthorised access and leak of personal credentials or information.

Wireless Penetration Testing: Wireless systems allow hackers or attackers an opportunity to hack into or infiltrate the organisation's network security system.
Wireless pen testing allows access to the consultant into the system who then tries to detect vulnerabilities and exploit them allowing them privileged access to sensitive information,it allows the consultants to demonstrate the potential impact of the breach in the wireless network.

Web Application Penetration Testing
Web application penetration testing is a testing method wherein applications on the network are checked for any vulnerabilities or security issues caused by faulty or insecure development, weak design, or improper coding.

Mobile Application Penetration Testing
Similar to web applications, mobile applications too, is an important arena for an organisation. Mobile application penetration testing or security testing is an empowered and simulated hacking attempt against a native mobile application running on devices such as Android, Windows, and iOS.

Penetration testing tools:

There is a full suite of automated testing tools available now, which allows you to carry out penetration testing efficiently. The following are some of the well-known tools used for Pen testing:

Kali Linux

Kali Linux is a Linux-based operating system containing vast arrays of tools and can be used for end-to-end penetration testing from information gathering to reporting.

Kali has over 600 ethical hacking tools and contains special tools used for brute force password cracking. Tools include vulnerability analysis, web applications, information gathering, wireless attacks, reverse engineering, password cracking, spoofing, sniffing and other advanced exploitation tools.

Metasploit

It help in managing security assessments, detects threats and flaws, and probable weak points. This tool helps set up a watertight and robust security control system that is difficult to breach. The GUI of Metasploit is easy to use and is open-source software. **Wireshark**

Wireshark is a network analyzer tool that captures and interprets network traffic. It provides both offline analysis and network real-time capture options.

Generally used to understand data packets flow and TCP/IP issues. It provides details of packet moments and network activities.

ZED attack Proxy

This tool is similar to one of the most popular proxy and scanning tool BURP suite and is almost as effective except that it is completely free.

Aircrack

Aircrack NG is a set of tools and a software suite that helps you attack and defend wireless networks. The tools package includes a detector, packet sniffer, WEP/WPA cracker, and so on. Aircrack primarily intercepts the packets, captures them, and then reads the packet patterns to crack the wireless system. Aircrack is open-source software and mainly used to check Wi-Fi connections **John the Ripper**

Passwords are the most vulnerable and are easy to attack in an information system. JTR is a password-cracking tool that cracks encryption and provides the password.

Costing And Budgeting Of Penetration Testing

The costing and budgeting depend on several factors and is not constant. The following factors affect the cost of penetration testing service.

Objective: The pricing fairly depends on the objectives or aims you wish to accomplish. Whether it is to test the physical access of a small organisation or transmission station of a utility, the pricing differs. The size is a factor when it comes to pricing. The pricing differs when

an entire network, including external and internal networks. The information you make available to the security tester also affects the pricing. The greater and more complex the objectives in number, the higher is the pricing.

Scope: Scope helps to determine organisations objectives and amount of time a tester or a essential to check whether the Pen test has the desired effect or not. The pricing policy differs when Retesting is taken into consideration.

➢ Vulnerability Tests

Vulnerability Testing also called Vulnerability Assessment is a process of evaluating security risks in software systems to reduce the probability of threats. The purpose of vulnerability testing is reducing the possibility for intruders/hackers to get unauthorized access of systems. It depends on the mechanism named Vulnerability Assessment and Penetration Testing(VAPT) or VAPT testing.

A vulnerability is any mistake or weakness in the system's security procedures, design, implementation or any internal control that may result in the violation of the system's security policy.

Vulnerability Assessment Process

Here is the step by step **Vulnerability Assessment Process** to identify the system vulnerabilities.

Step 1) Goals & Objectives : – Define goals and objectives of Vulnerability Analysis.

Step 2) Scope : – While performing the Assessment and Test, Scope of the Assignment needs to be clearly defined.

The following are the three possible scopes that exist:

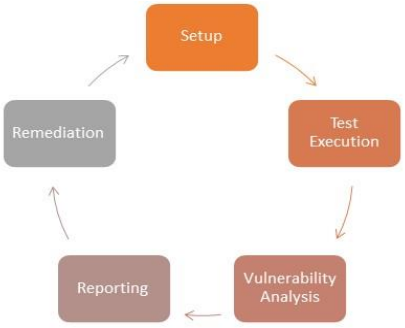
- Black Box Testing : – Testing from an external network with no prior knowledge of the internal network and systems.
- Grey Box Testing : – Testing from either external or internal networks with the knowledge of the internal network and system. It's the combination of both Black Box Testing and White Box Testing.
- White Box Testing : – Testing within the internal network with the knowledge of the internal network and system. Also known as Internal Testing.

Step 3) Information Gathering: – Obtaining as much information about IT environment such as Networks, IP Address, Operating System Version, etc. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing and White Box Testing.

Step 4) Vulnerability Detection: – In this process, vulnerability scanners are used to scan the IT environment and identify the vulnerabilities.

Step 5) Information Analysis and Planning: – It will analyze the identified vulnerabilities to devise a plan for penetrating into the network and systems.

How to do Vulnerability Assessment



Following is the step by step process on **How to do Vulnerability Assessment**:

Step 1) Se

- Begin Documentation
- Secure Permissions
- Update Tools
- Configure Tools **Step 2) Test**

Execution: Run the Tools

- Run the captured data packet (A packet is the unit of data that is routed between an origin and the destination. When any file, for example, e-mail message, HTML file, Uniform Resource Locator(URL) request, etc. is sent from one place to another on the internet, the TCP layer of TCP/IP divides the file into a number of "chunks" for efficient routing, and each of these chunks will be uniquely numbered and will include the Internet address of the destination. These chunks are called packets. When all the packets are arrived, they will be reassembled into the original file by the TCP layer at the receiving end while running the assessment tools **Step 3) Vulnerability Analysis:**
- Defining and classifying network or System resources. Assigning priority to the resources(Ex: – High, Medium, Low) Identifying potential threats to each resource.
- Developing a strategy to deal with the most prioritized problems first.
- Defining and implementing ways to minimize the consequences if an attack occurs. **Step 4) Reporting**

Step 5) Remediation:

- The process of fixing the vulnerabilities.
- Performed for every vulnerability

Types of a vulnerability scanner 1.

Host Based

- Identifies the issues in the host or the system.
- The process is carried out by using host-based scanners and diagnose the vulnerabilities.
- The host-based tools will load a mediator software onto the target system; it will trace the event and report it to the security analyst. 2. **Network-Based**
- It will detect the open port, and identify the unknown services running on these ports.

  Then it will disclose possible vulnerabilities associated with these services.
- This process is done by using Network-based Scanners.

3. **Database-Based**

It will identify the security exposure in the database systems using tools and techniques to prevent from SQL Injections. (SQL Injections: – Injecting SQL statements into the database by the malicious users, which can read the sensitive data's from a database and can update the data in the Database.)

Tools for Vulnerability Scanning

1) Acunetix

Intuitive and easy to use, Acunetix by Invicti helps small to mediumsized organizations ensure their web applications are secure from costly data breaches. It does so by detecting a wide range of web security issues and helping security and development professionals act fast to resolve them.

Features:

- Advanced scanning for 7,000+ web vulnerabilities, including OWASP Top 10 such as SQLi and XSS
- Automated web asset discovery for identifying abandoned or forgotten websites
- Advanced crawler for the most complex web applications, incl. multi-form and password-protected areas
- Combined interactive and dynamic application security testing to discover vulnerabilities other tools miss
- Proof of exploit provided for many types of vulnerabilities
- DevOps automation through integrations with popular issue tracking and CI/CD tools Compliance reporting for regulatory standards, such as PCI DSS, NIST, HIPAA, ISO 27001, and more. **2) Intruder**

Intruder is a powerful online vulnerability scanner that discovers security weaknesses across your IT environment. Offering industryleading security checks, continuous monitoring and an easy-to-use platform, Intruder keeps businesses of all sizes safe from hackers.

Features:

- Best-in-class threat coverage with over 10,000 security checks
- Checks for configuration weaknesses, missing patches, application weaknesses (such as SQL injection & cross-site scripting) and more
- Automatic analysis and prioritisation of scan results
- Intuitive interface, quick to set-up and run your first scans
- Proactive security monitoring for the latest vulnerabilities
- AWS, Azure and Google Cloud connectors
- API integration with your CI/CD pipeline

Advantages of Vulnerability Assessment

 Open Source tools are available.
Identifies almost all vulnerabilities
Automated for Scanning.

- Easy to run on a regular basis.

Disadvantages of Vulnerability Assessment

- High false positive rate
- Can easily detect by Intrusion Detection System Firewall.
- Often fail to notice the latest vulnerabilities. **Vulnerability Testing Methods**

Active Testing

- Inactive Testing, a tester introduces new test data and analyses the results.
- During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test.
- While doing the test, the tester will actively involve in the process of finding out the new test cases and new ideas. That's why it is called Active Testing.

Passive Testing

- Passive testing, monitoring the result of running software under test without introducing new test cases or data **Network Testing**
- Network Testing is the process of measuring and recording the current state of network operation over a period of time.
- Testing is mainly done for predicting the network operating under load or to find out the problems created by new services.
- We need to Test the following Network Characteristics:- □ Utilization levels □ Number of Users
- Application Utilization **Distributed Testing**
- Distributed Tests are applied for testing distributed applications, which means, the applications that are working with multiple clients simultaneously. Basically, testing a distributed application means testing its client and server parts separately, but by using a distributed testing method, we can test them all together.
- The test parts will interact with each other during the Test Run. This makes them synchronized in an appropriate manner. Synchronization is one of the most crucial points in distributed testing.

Short Answers:

1.What is Network Security ?

2.What is Firewall ?

3.Explain about the Packet filtering Firewalls?

Long answers:

1.Explain the types of Fire Walls ?

2.Explain the Stateless and State full firewall ?

3.What is Antivirus ?

4.What is penetration test methodologies ?

➢ Organizational Implications -Introduction

In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices or intense scans from criminal groups.

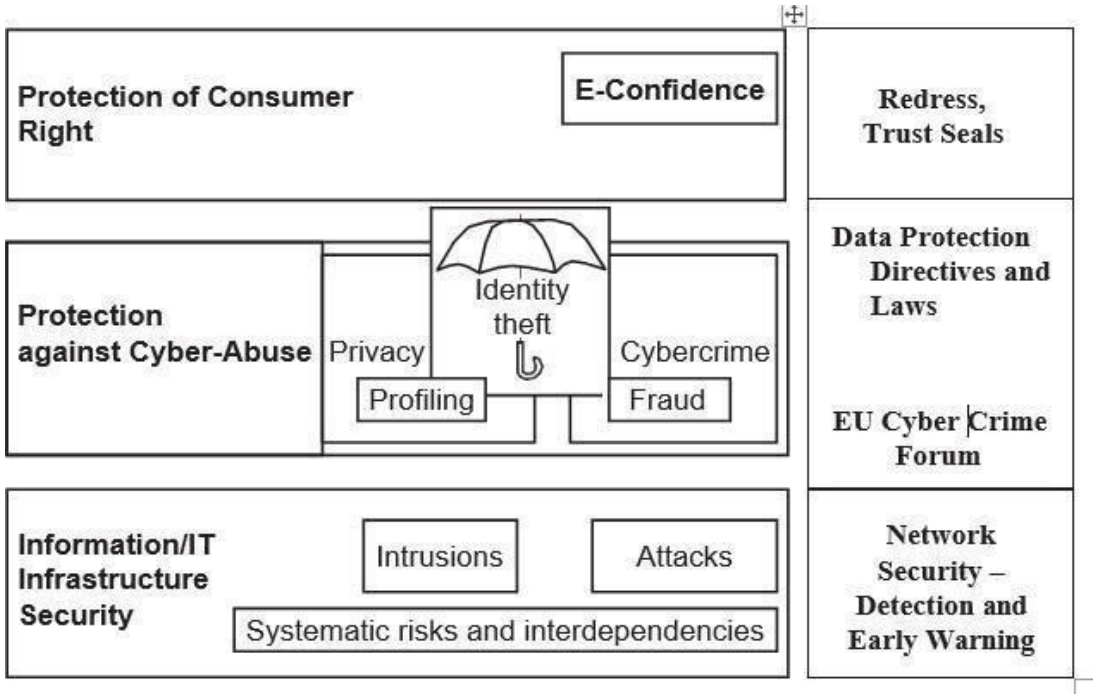


Fig: A cyber security perspective. EU is the European Union.

PI is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Most information the organization collects about an individual is likely to come under "PI" category if it can be attributed to an individual. For an example, PI is an individual's first name or first initial and last name in combination with any of the following data:

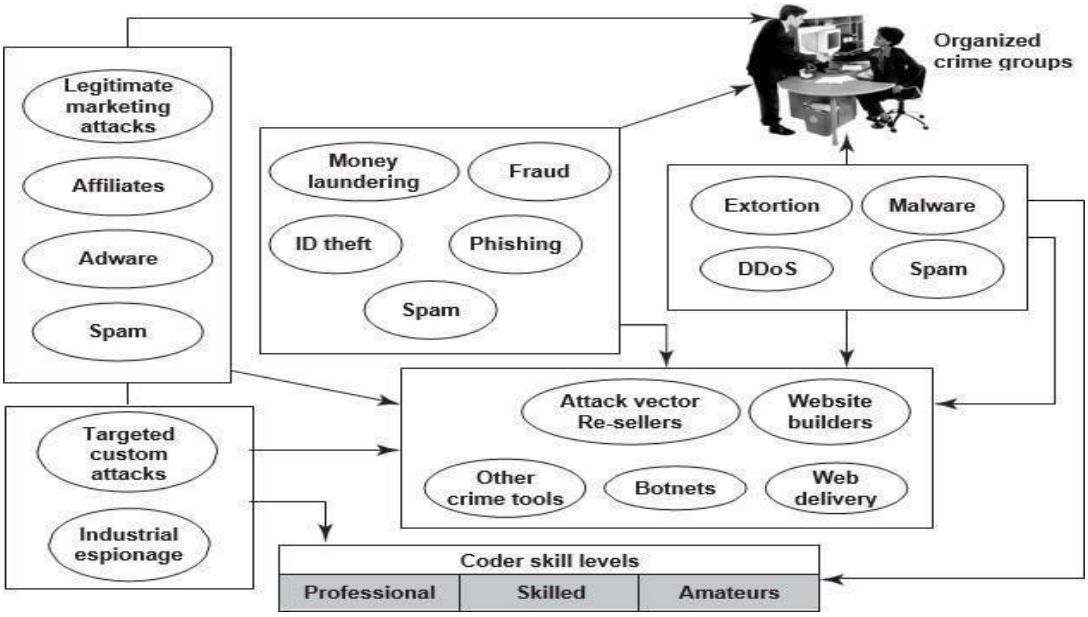
1. Social security number (SSN)/social insurance number.
2. Driver's license number or identification card number.

3. Bank account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account.
4. Home address or E-Mail address.
5. Medical or health information.

An insider threat is defined as "the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other 'trusted' individuals."

Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of "insiders" such as:

1. A malicious insider is motivated to adversely impact an organization through a



range of actions that compromise information confidentiality, integrity and/or availability.

2. A careless insider can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.

3. A tricked insider is a person who is "tricked" into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via "pretexting" (known as social engineering).

- **Insider Attack Example 1: Heartland Payment System Fraud**

A case in point is the infamous "Heartland Payment System Fraud" that was uncovered in January 2010. This incident brings out the glaring point about seriousness of "insider attacks. In this case, the concerned organization suffered a serious blow through nearly

100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is trans- mitted through a payment network.

- **Insider Attack Example 2: Blue Shield Blue Cross (BCBS)**

  Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private information of approximately 500,000 customers at risk in at least 32 states.

  The two lessons to be learnt from this are:

  1. Physical security is very important.
  2. Insider threats cannot be ignored.

  What makes matters worse is that the groups/agencies/entities connected with cybercrimes are all linked. There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc. to name a few.

Fig: Cybercrimes – the flow and connections.

A key message from this discussion is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cybersecurity practices and "privacy" which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

1. **Informational/data privacy:** It is about data protection, and the users' rights to determine how, when and to what extent information about them is communicated to other parties.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.
3. **Communication privacy:** This is as in networks, where encryption of data being transmitted is important.
4. **Territorial privacy:** It is about protecting users' property for example, the user devices from being invaded by undesired content such as SMS or E-Mail/Spam messages. The paradigm shift in computing brings many challenges for organizations; some such key challenges are described here

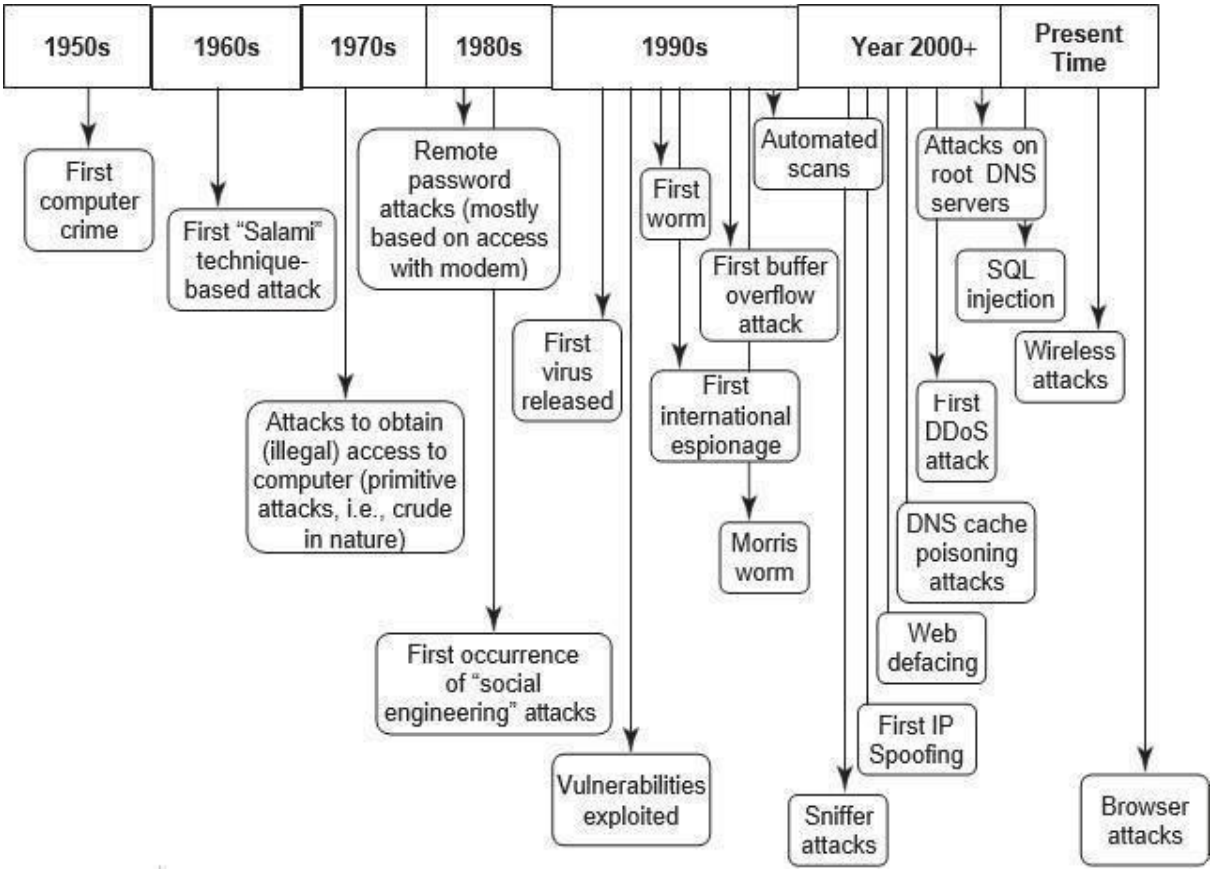


Fig: Security threats – paradigm shift.

The key challenges from emerging new information threats to organizations are as follows:

1. **Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names.
3. **IP-based "cloaking":** Businesses are global in nature and economies are interconnected.
4. **Cyberterrorism:** "Cyberterrorism" refers to the direct intervention of a threat source toward your organization's website.

Confidential information leakage: "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solutions

➢ Cost of Cybercrimes and IPR Issues: Lessons for Organizations

cybercrimes cost a lot to organizations.

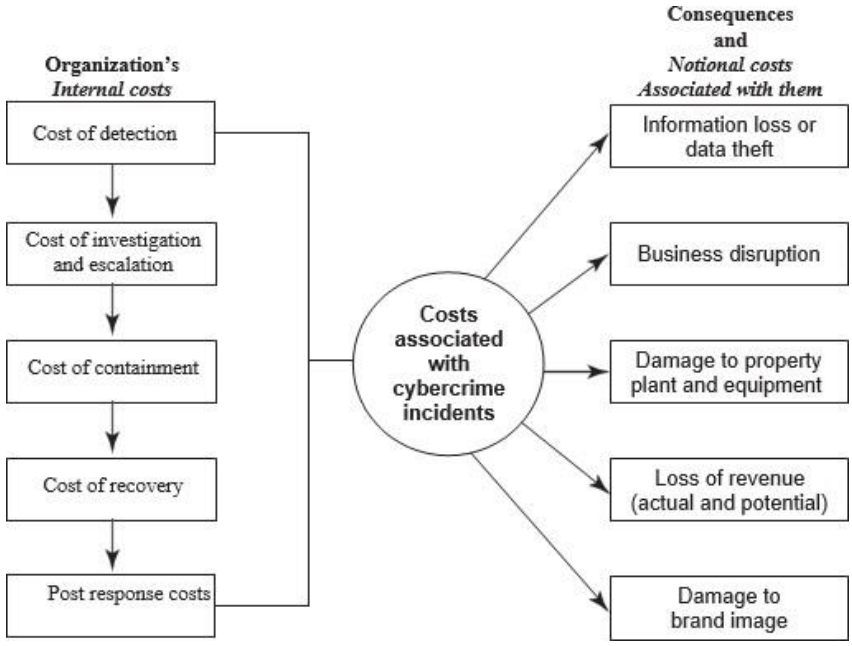


Fig: Cost of cybercrimes.

When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

Detection and recovery constitute a very large percentage of internal costs. This is supported by a benchmark study conducted by Ponemon Institute USA carried out with the sample of 45 organizations representing more than 10 sectors and each with a head count of at least 500 employees.

- **Organizations have Internal Costs Associated with Cyber security Incidents**

The internal costs typically involve people costs, overhead costs and productivity losses. The internal costs, in order from largest to the lowest and that has been supported by the benchmark study mentioned:

1. Detection costs.(25%)
2. Recovery costs.(21%)
3. Post response costs.(19%)
4. Investigation costs.(14%)
5. Costs of escalation and incident management.(12%)
6. Cost of containment.(9%)

- **The consequences of cybercrimes and their associated costs, mentioned**

1. Information loss/data theft.(42%)
2. Business disruption.(22%)
3. Damages to equipment, plant and property.(13%)

4. Loss of revenue and brand tarnishing.(13%)
5. Other costs.(10%)

- **The impact on organizations by various cyber crimes**
  1. Virus,worms and Trojans-100%
  2. Malwares-80%
  3. Botnets-73%
  4. Web based attacks-53%
  5. Phishing and Social engineering-47%
  6. Stolen devices-36%
  7. Malicious insiders-29%
  8. Malicious code-27%
- **Average days taken to resolve cyber Attacks**

  Attacks by Malicious insiders-42 days

  1. Malicious code-39 days
  2. Web based attacks-19 days
  3. Data lost due to stolen devices-10 days
  4. Phishing and social engineering attacks-9 days
  5. Virus,worms,and trojans-2.5 days
  6. Malware-2 days
  7. Botnets- 2 days
- **There are many new endpoints in today's complex networks; they include hand-held devices.**

  Again, there are lessons to learn:

  1. **Endpoint protection:** It is an often-ignored area but it is IP-based printers, although they are passive devices, are also one of the endpoints.
  2. **Secure coding:** These practices are important because they are a good mitigation control to protect organizations from "Malicious Code" inside business applications.
  3. **HR checks:** These are important prior to employment as well as after employment.
  4. **Access controls:** These are always important, for example, shared IDs and shared laptops are dangerous.
  5. **Importance of security governance:** It cannot be ignored policies, procedures and their effective implementation cannot be over-emphasized.
- **Organizational Implications of Software Piracy**

  Use of pirated software is a major risk area for organizations.

From a legal standpoint, software piracy is an IPR violation crime. Use of pirated software increases serious threats and risks of cybercrime and computer security when it comes to legal liability.

The most often quoted reasons by employees, for use of pirated software, are as follows:

1. Pirated software is cheaper and more readily available.
2. Many others use pirated software anyways.
3. Latest versions are available faster when pirated software is used.

➢ Web Threats for Organizations: The Evils and Perils

Internet and the Web is the way of working today in the interconnected digital economy. More and more business applications are web based, especially with the growing adoption of cloud computing.

- **Overview of Web Threats to Organizations**

  The Internet has engulfed us! Large number of companies as well as individuals have a connection to the Internet. Employees expect to have Internet access at work just like they do at home.

  IT managers must also find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

- **Employee Time Wasted on Internet Surfing**

  This is a very sensitive topic indeed, especially in organizations that claim to have a "liberal culture." Some managers believe that it is crucial in today's business world to have the finger on the pulse of your employees.

  People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.

- **Enforcing Policy Usage in the Organization**

  An organization has various types of policies. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization.

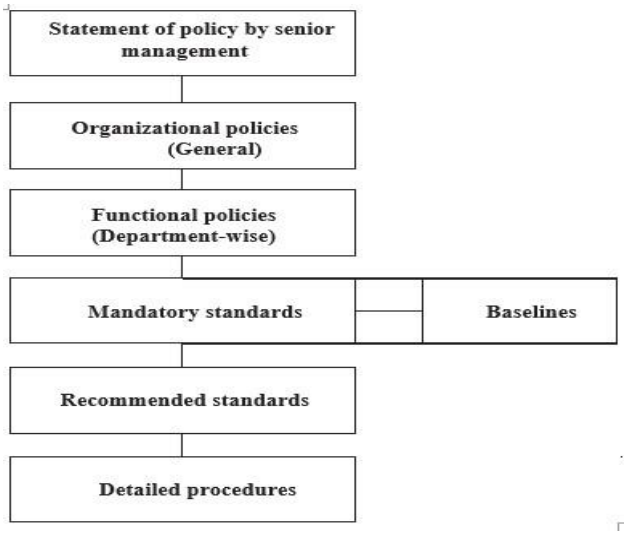


Fig: Policy hierarchy chart.

- **Monitoring and Controlling Employees' Internet Surfing**

  A powerful deterrent can be created through effective monitoring and reporting of employees' Internet surfing.

  Even organizations with restrictive policies can justify a degree of relaxation; for example, allowing employees to access personal sites only during the lunch hour or during specified hours.

- **Keeping Security Patches and Virus Signatures Up to Date**

  Updating security patches and virus signatures have now become a reality of life, a necessary activity for safety in the cyberworld! Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management.

- **Surviving in the Era of Legal Risks**

  As website galore, most organizations get worried about employees visiting inappropriate or offensive websites. We mentioned about Children's Online Privacy Protection.

Serious legal liabilities arise for businesses from employee's misuse/inappropriate use of the Internet.

- **Bandwidth Wastage Issues**

  Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images.

  There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

- **Mobile Workers Pose Security Challenges**

Use of mobile handset devices in cybercrimes. Most mobile communication devices for example, the personal digital assistants has raised security concerns with their use. Mobile workers use those devices to connect with their company networks when they move. So the organizations cannot protect the remote user system as a result workforce remains unprotected. We need tools to extend web protection and filtering to remote users, including policy enforcement

- **Challenges in Controlling Access to Web Applications**

Today, a large number of organizations' applications are web based. There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications. Employees use personal mail id to send business sensitive information (BSI) for valid or other reasons. It leads to data security breach. The organizations need to decide what type of access to provide to employees.

- **The Bane of Malware**

Many websites contain malware. Such websites are a growing security threat. Although most organizations are doing a good job of blocking sites declared dangerous, cyber attackers, too, are learning. Criminals change their techniques rapidly to avoid detection.

- **The Need for Protecting Multiple Offices and Locations**

Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today. Most large organizations have several offices at multiple locations. In such scenario Internet-based host service is best idea to protect many locations.

➢ Security and privacy implications from cloud computing

Cloud computing is one of the top 10 Cyber Threats to organizations. There are data privacy risks through cloud computing. Organizations should think about privacy scenarios in terms of "user spheres". There are three kinds of spheres and their characteristics:

1. **User sphere:** Here data is stored on users' desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to users and monitor that access to ensure misuse does not happen.
2. **Recipient sphere:** Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data. Organizations responsibility is to minimize users privacy risk by ensuring unwanted exposure of personal data of users does not happen
3. **Joint sphere:** Here data lies with web service provider's servers and databases. This is the in between sphere where it is not clear to whom does the data belong. Organization responsibility is to provide users

some control over access to themselves and to minimize users futures privacy risk.

➢ Social Media Marketing: Security Risks and Perils for Organizations

Social media marketing has become dominant in the industry. According to fall 2009 survey by marketing professionals; usage of social media sites by large business-to-business (B2B) organizations shows the following:

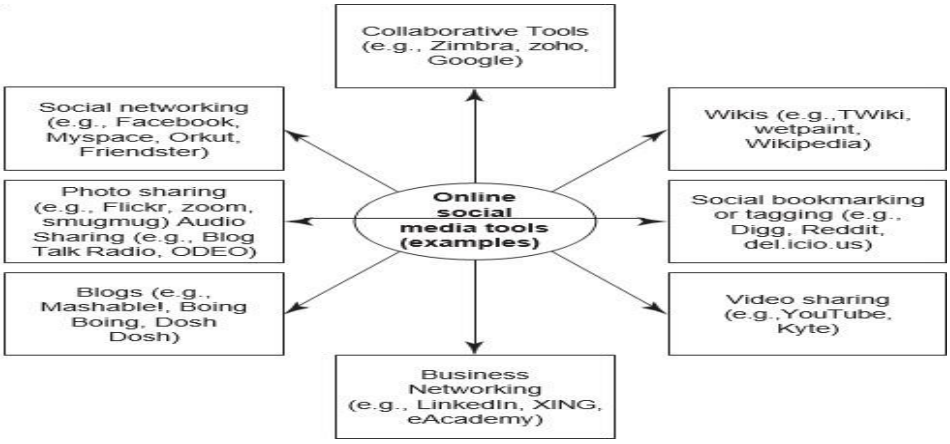


FIG: Social Media Marketing Tools

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. My Space is used by 6% of the organizations.

Although the use of social media marketing site is rampant, there is a problem related to

"social computing" or "social media marketing" – the problem of privacy threats. Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of "social media marketing."

➢ Understanding Social Media Marketing

Most professionals today use social technologies for business purposes. Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development.

Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
2. To increase traffic to their website coming from other social media websites by using Blogs and social and business-networking.

Companies believe that this, in turn, may increase their "page rank" resulting in increased traffic from leading search engines.

3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
4. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
5. To collect potential customer profiles. Social media sites have information such asuser profile data, which can be used to target a specific set of users for advertising

There are other tools too that organizations use; industry practices indicate the following:

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
2. Professional networking tool LinkedIn is used to connect with and create a communityof top executives from the Fortune 500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
4. YouTube (the video capability tool to run demonstrations of products/services, etc.) is used to increase the brand awareness and create a presence for corporate videos.
5. Wikipedia is also used for brand building and driving traffic.

There are conflits views about social media marketing some people in IT say the expensive and careless use of it.Some illustrate the advantages of it with proper control of Security risk

➢ Digital Forensic:Protecting people privacy in the organizations Forensic best practices for Organizations

Digital forensics is the application of scientific principles to the process of discovering information from a digital device. A form of digital forensics has been around nearly as early as computers were invented, but forensic capabilities have witnessed many advances in the past years as digital forensic processes have matured and needs have become more prevalent. Digital forensics can involve nearly any digital device, not just computers, although technology often evolves faster than forensic capabilities do. Some of the common areas in which digital forensics are used include computers, printers, cell phones, mobile devices, global positioning systems, and storage media.

Less common areas include automobile systems, appliances, office equipment, and other programmable devices

These days, cyber criminals seem to be everywhere. They lurk in the darkest corners of the internet, defrauding people, hacking, stealing, and hiding from authorities with virtual anonymity. According to Wired, cyber criminals are wreaking havoc by unleashing ransomware attacks, stealing data, even them to justice. And they're using digital forensics to do it.

The good news is companies and government agencies are getting better at combating cyber criminals, finding them, and bringing jobs are, and what it takes to succeed.

Digital Forensics in Cyber Security Defined

People who work with digital forensics in cyber security are on the front lines in the fight against cybercrime. They're the people who collect, process, preserve, and analyze computer-related evidence.

They help identify network vulnerabilities and then develop ways to mitigate them. They go deep inside networks, computers, and smartphones in search of evidence of criminal activity. And they run counterintelligence against hackers, criminals, and others with nefarious intensions.

Where Digital Forensics in Cyber Security is Used

These days, anyone who uses the internet benefits from digital forensics in cyber security. That's because any company that collects data from internet users employs people who fight and investigate cybercrime.

Agencies and organizations have to be hyper-vigilant with the data they collect and protect, so they are constantly testing their systems, looking for vulnerabilities and aggressively pursuing the people who hack into networks in order to commit crimes. Facebook, Twitter, Instagram, Homeland Security, the FBI, Target Corp., the military, local and state law enforcement, and nearly every bank uses digital forensics in cyber security to protect people using the internet.

What Skills are Needed for Digital Forensics in Cyber Security

As you can imagine, not just anyone with a laptop and internet access can be a digital forensics professional. It takes a lot of knowledge and plenty of skills, including:

- a deep understanding of computers, technology across a broad spectrum, and cybersecurity principles and practices,
- a working knowledge of computers, networks, and coding,
- in-depth investigative abilities,
- critical-thinking skills and analytical talent
- the ability to effectively communicate and work with a wide range of people

What makes the job so interesting is that sometimes the evidence is easily accessible, but other times it's hidden deep within the computer or network. Often, it's been deleted by the suspect. It's the job of the professionals to use their knowledge and skills to find the evidence, where ever it may be hiding.

- Case studies:

Data Theft – Confidential and Client Information Breach

We were asked to investigate a case by an international recruitment agency to conduct a forensic examination of the company laptop and mobile phone of a senior employee who had left the company. The company suspected that this employee had forwarded contact client information and confidential data to his personal e-mail address and copied a large amount

business critical files onto his memory stick shortly before his departure and used this information to set up a rival company. A forensic investigation into his laptop, mobile phone and memory stick revealed that prior to deleting his e-mails and resetting his laptop, a large number of files and sensitive client database entries has been taken away. Using the digital evidence provided by Computer Forensics Lab investigators, the employee was found in breach of his employment contract and legal proceedings were taken against him. The employers managed to successfully take him to court and sought damages.

Harassment

A senior member of the management team of a financial institution was experiencing a series of distressing occurrences of unsolicited worrying emails and text messages from, what appeared to be, someone within their own organisation. Computer Forensics Lab were commissioned to investigate the circumstances and find out the potential trail of evidence that might lead to the identification of those involved. Even though the email headers had been forged, it was quickly established that the distressing emails were not originating from within the recipient's organisation. In fact the messages were originating from a rival financial institution member of staff who used to work for the client's organisation. Our findings resulted in the prosecution of the offender involved.

Impersonation & Financial Fraud

The client was approved for a mortgage and he had hired a solicitor in order to handle the purchase of his dream house. After meeting the solicitor in her office, the client was given all the paperwork and it was agreed that he pays the house deposit to an escrow account provided by the solicitor. They agreed to exchange emails from that point onwards. After several email exchanges, the client received an email from the solicitor requesting to pay the deposit to a different account which was not the one provided in the paperwork. The email appeared to be from the solicitor with all her usual signature and contact details and there was no reason to make our client suspicious. He paid £55,000 to the new account and called her the next day to ask whether the solicitor had received the house deposit. To our client's disappointment, the answer was no and the solicitor said she had never requested a change of bank accounts by email. Forensic investigation of the client and the solicitor's email address provided evidence that the solicitor's computer had a trojan virus and a fraudster located in Abuja, Nigeria, had gained access to her email system and had in fact impersonated the solicitor.

Invasion of Privacy and Domestic Abuse

We handled the case of a wife who was subject to bullying and domestic abuse by her husband who happened to be a senior IT technician specialising in computer security and this was quite a tricky one because the husband knew everything about hiding his identity and covering his tracks using proxy chains and had managed to infect his wife's mobile, tablet and personal computer with trojans and thereby had full control on all the electronic devices she used. The family had an ultrafast internet connection and this enabled the husband to do full audio, video and computer surveillance on the wife using her mobile, tablet, personal computer and unusually, the family smart TV and used that information to bully and intimidate her. The wife was completely unaware of this for over 4 years and due to her lack of IT skills, she did not know anything about her husband's spying activities.

The husband's controlling behaviour subjected the wife to constant domestic abuse making the wife extremely scared and isolated. As a consequence, she wouldn't trust anyone with her family secrets fearing that the husband might find out and this could cause even more trouble for her. By pure coincidence, she found out that she had been spied on all these years and she was extremely upset and distressed and confronted him. This just led to more abusive behaviour. Eventually she plucked up the courage to talk about it to a close friend who persuaded her to approach a computer forensics expert. She came to us for help and we asked her to provide us with all the devices that she had including mobile phones, tablet and personal computer. This gave us the opportunity to collect all digital evidence that was required for the court. As a result of our investigations, the husband was cautioned for his actions by the police and was later convicted for the invasion of privacy his wife. Some of the digital evidence we had gathered helped her case to bring domestic abuse charges which led to serious court sanctions of the husband and a divorce with her custody of the children

Short Answers:

1.What is Cybercrime ?

2.Explain the flow of Cybercrime ?

3.What is cost of cyber crime ?

Long Answers:

1.Explain Web Threats for Organizations ?

2.Define Security and privacy implications from cloud computing ?

3.Explain about Social Media Marketing ?

S.V.U COLLEGE OF COMMERCE MANAGEMENT AND COMPUTER SCIENCE :: TIRUPATHI

DEPARTMENT OF COMPUTER SCIENCE

TIME:2 Hours **INTERNAL EXAMINATIONS-1**
Max.Marks:30

SECTION-A

Answer any Five questions

Each question carries two marks 5*2=10m

1.Define Hacking ?

2.Define Security Attack ?

3.What are types of Security mechanisms ?

5.Define cyber security ?

6. Explain CIA TRIAD ?

7. Define Security tools ?

8. Explain the role of cyber security ?

SECTION - B

Answer any one Question from each unit

2*10=20Mark

Unit-1

9.Explain in details about the cyber attacks ?

(Or)

10.Explain about the Network Security ?

Unit 2

11.What is Vulnerability ?

(or)

12.What is the difference between Vishing and Phishing ?

S.V.U COLLEGE OF COMMERCE MANAGEMENT AND COMPUTER SCIENCE:: TIRUPATHI

DEPARTMENT OF COMPUTER SCIENCE

TIME:2 Hours **INTERNAL EXAMINATIONS-1**
Max.Marks:30

SECTION-A

Answer any Five questions

Each question carries two marks 5*2=10m

1)What is password cracking

2)What is the need for computer forensic

3).What is risk.

4.Define Cipher text

5.what are the deliverables of risk assessment

6.What is an attack& threat

7.Write a note on security policy

8.What is a law and ethics

9.List our three security policies

10.What is ISO

SECTION - B

Answer any one Question from each unit 2*10=20Marks

Unit-1

11.Explain about different types of attacks on computer based systems.

(Or)

12.Explain different phases of Security Systems Development Life cycle(SSDLC)

Unit-2

13.Discuss the legal and ethical issues associated with the information security.

(Or)

14. What is intrusion detection system? Explain its categories and operation models in detail

MASTER OF COMPUTER APPLICATIONS DEGREE EXAMINATIONS,

JANUARY-2022

SECOND SEMESTER

PAPER:MCA 205B-CYBER SECURITY

(Under C.B.C.S. New regulations w.e.f.2020-2021 and 2016-2017)

(Common paper to University and all Affiliated Colleges)

Time :3 hours
Max marks:70

PART-A (Compulsory)

Answer any five of the following questions.
Each question carries 4 marks (5*4=20)

1.A) What is cybercrime ? Who are Cybercriminals? Explain.

B).Define Cipher text

c)what are the deliverables of risk assessment

d).What is an attack& threat

e)Write a note on security policy

f)What is a law and ethic?

g)Define cyber security ?

h) Explain CIA TRIAD ?

i). Define Security tools ?

j) Define Cipher text?

Part – B

Answer five questions choosing one question from each unit.

Each question carries 10 marks (5*10=50)

UNIT-1

2.Discuss about various types of cyber-attacks.

(Or)

3.Discuss how critical thinking is important in Cyber Security.

UNIT-II

4.Describe Network Security model with neat sketch.

(Or)

5.In detail discuss about Internet Security threats.

UNIT-III

6.What is CIA Triad? Explain the three components of CIA traid

(OR)

7. a) Discuss about incidence response in cyber security.

b) Briefly explain about cyber security frame works

UNIT-IV

8. a) Discuss the use of packet filtering firewalls

b) Briefly explain about penetration test Methodologies.

(Or)

9 a) Explain the importance of XML. Gateway firewall in cyber security.

b) Discuss about Vulnerability tests.

UNIT-10

10.In detail Discuss the web threats for organisations with case studies.

(Or)

11.What is meant by social media marketing? Explain different social media marketing tools.