Chettinad College of Engineering & Technology
Approved by AICTE-New Delhi and Affiliated to Anna University-Chennai

Department of Computer Science and Engineering
Academic Year 2023 - 2024
Question Bank

Year/Semester:III/ VI

Subject Code/Title : CCS340/ CyberSecurity

UNIT I
Part A

1. What is Cyber Security?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information

2. What is CyberCrime?

Cybercrime is the use of a computer to commit illegal acts, such as fraud, identity theft, or privacy violations. Cybercrime has become more important as computers have become central to commerce, entertainment, and government.

3. What is the Internet?

The internet is a global network of interconnected computers, servers, phones, and smart appliances that communicate with each other using the transmission control protocol (TCP) standard to enable a fast exchange of information and files, along with other types of services.

4. What do you mean by information security?

Information security, often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.

5. What is security risk analysis?

A security risk analysis is a process to identify and assess potential risks to an organization's assets, data, and reputation. It can help prevent data breaches and inform the need for cybersecurity programs.

6. Define Online fraud.

The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.

7.What is the need for cyber security?

Cybersecurity is important for protecting digital assets, including personal and financial information, intellectual property, and critical infrastructure. Cyberattacks can have serious consequences, such as financial loss, reputational damage, and even physical harm.

8 .Classification of cyber security?

It can be categorized into several types, including:

- Network security: Protects computer networks and the data that passes through them
- Cloud security: Secures cloud-based infrastructure, applications, and data
- Internet of Things (IoT) security: Protects the interconnected devices, sensors, and systems that make up the Internet of Things
- Critical infrastructure security: Protects infrastructures such as energy, water, transportation, and communications systems.

9. What is meant by ethical hacking ?

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization.

10.Who are hackers? Explain different types of hackers. Illustrate different hacking methodologies .

Hackers are people with exceptional computer skills who exploit vulnerabilities in computer systems to gain unauthorized access.
Hacker Types: Black Hat, White Hat, and Gray Hat Hackers.
Attackers follow a certain methodology to hack a system. They first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which they then use to exploit the target system.

11. Describe the need for computer forensics.

Computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device. Often, computer forensics is used to uncover evidence that could be used in a court of law.

12. Illustrate about CIA triad?

The CIA triad is a framework that combines three key information security principles: confidentiality, integrity, and availability.

13. Explain about the security model?

Information security models are systems that specify which people should have access to data, and the operation of the operating system, which enables management to organize access control.

PartB &C-16 marks & 8 marks

1. What is cyber security? Explain various types of Cyber threats.
2. Write a short note on (a) Deception (b) Cyber security Audit © Denial of Services
3. Explain the different cyber security safeguards.
4. What is System Administration? Explain the roles and responsibilities of System Administration ?

UNIT II

Part A

1.Define OSWAP

The Open Web Application Security Project (OWASP) is a nonprofit foundation that provides guidance on how to develop, purchase and maintain trustworthy and secure software applications.

2.What are the scope of cyber attack?

The scope of a cyber incident is the extent of the impact, damage, or exposure caused by the event. It includes the number and types of systems, networks, devices, users, data, and services affected, as well as the potential legal, regulatory, reputational, or operational consequences.

3.What do you mean by malicious attack?

Malicious Attack means intentional hacking, damaging, corrupting or misusing the Insured's Computer Systems, including Unauthorized Access or the insertion of Malicious Code by a third party or an employee.

4.How many types of malicious attack there?

Common types of malware include viruses, worms, trojans, ransomware, adware, spyware, rootkits, keyloggers, fileless malware, cryptojacking, and hybrid malware.

5.Define social engineering attack

A social engineering attack is a cybersecurity attack that relies on the psychological manipulation of human behavior to disclose sensitive data, share credentials, grant access to a personal device.

6.Is phishing a wireless attack?

Wifi Phishing is when cyber criminals create a malicious WiFi access point that appears similar or identical to a legitimate WiFi access point. This malicious WiFi access point is sometimes known as the "evil twin".

7.What is vulnerability and threat in cyber security?

A vulnerability is a weakness or flaw in an operating system, network, or application. A threat actor tries to exploit vulnerabilities to gain unauthorized access to data or systems.

8.What are the three main security tools?

Here are three essentials that every business should put in place as a basic level of protection.
A firewall. A firewall monitors the internet traffic coming into and leaving your IT network.
A password manager for everyone in the business.
A VPN (Virtual Private Network)

9.What are the most common types of cyber security attacks?

Malware.
Phishing.
Spoofing.
Backdoor Trojan.
Ransomware.
Password attacks.
Internet of Things attack.
Cryptojacking.

10.What is the purpose of countermeasures?

Countermeasures are devices, signals, and techniques deployed to impair or eliminate the operational effectiveness of an attack by an enemy force.

11.What is the meaning of breach of security?

A security breach means unauthorized access to a device, facility, program, network, or data. It can involve the breach of security measures that protect data, network systems.

12.Is malicious software a cyber crime?

Cyber-dependent crimes fall broadly into two main categories: Illicit intrusions into computer networks, such as hacking; and. the disruption or downgrading of computer functionality and network space, such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.

13.What is a website attack called?

Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, “fishing” for access to a forbidden area by using the “bait” of a seemingly trustworthy sender.

PartB &C-16 marks & 8 marks

1. **Explain about malicious attack and it's types?**
2. **Describe about social engineering?**
3. **Explain about attack tools?**
4. **What is attack vector ? Types and how to avoid them?**

UNIT III
Part A

1.Define Reconnaissance.

Reconnaissance, sometimes known as Recon, is the first stage of the Pen Testing process. The information-gathering phase of ethical hacking is called reconnaissance, during which you gather information about the intended as

system. This information may comprise everything from network architecture to employee contact information. Reconnaissance is to locate many potential attack pathways as is practicable.

There are two types of recon strategies: active and passive.

Active recon entails engaging the target directly in order to obtain information. Because it breaks the "hiding traces" guideline in pen testing, this is not advised.

Passive recon is the process of learning about a target by utilizing the abundance of information available online. There is no fear because we aren't connecting with the target directly in it.

2. List down the various types of reconnaissance tools

1. Passive Reconnaissance Tools

• Google Search

• Shodan

• The Harvester

• Maltego

2. Active Reconnaissance Tools

• Nmap (Network Mapper)

• Hping

• Recon-ng

3. What is the purpose of the HOST command?

A network utility called the host command can be used to search up information about domain names or IP addresses using the DNS (Domain Name System). Its major function is to convert human-readable domain

found on a variety of operating systems, including Windows, Linux, and macOS, and it is frequently used in command-line environments.

4. What is Whois footprinting?

Whois Footprinting is a method of ethical hacking that gathers information on targets and their health. The operations carried out during this pre-attack phase will be covert, and every effort will be taken to keep the

target from locating you. Given that intrusion testers are aware of how hackers view this system, the footprinting is thus the first important advancement. The cybersecurity footprint process entails profiling your business and gathering information about its hosts, network, users, and business partners. The data about company's operating system, firewall, network card, IP address, domain name system details, target computer security settings, URL, virtual private network, employee ID, email address, and phone number are comprised.

5. What is the purpose of NETCRAFT?

Netcraft toolbar is a free security toolbar that can be applied to the IE and Firefox browsers (http://toolbar.netcraft.com). The toolbar issues both good and negative alerts. The toolbar notifies the user that the website they are visiting is a faked one once it has identified a phishing site. If the user chooses to disregard the warning, the toolbar shows information about the phishing site, such as the month and year it was created, its ranking, a link to submit a report about the site, the nation where the site is housed, and the hosting provider.

6. How DNS is used to resolve network address?

A web address or domain name is entered by the user into a browser. To determine which IP or network address the domain points to, the browser sends what is known as a recursive DNS query to the network.

7. What is meant by Metasploit?

Metasploit is one of the most powerful exploit tools. It's a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It comes in two versions "commercial and free edition. Matasploit can be used with command prompt or with Web UI.

With Metasploit, the following operations can be performed:

Conduct basic penetration tests on small networks

Run spot checks on the exploitability of vulnerabilities

Discover the network or import scan data

Browse exploit modules and run individual exploits on hosts

8. Brief about Burp Suite.

Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp is easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing. Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

9. Shortly explain Ping Sweep.

A ping sweep is a network scanning technique that is used to determine which IP address from a range of IP addresses map to live hosts. Ping Sweep is also known as ICMP sweep.

fping command can be used for ping sweep. This command is a ping- like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up.

fping is different from ping in which fping specify any number of hosts on the command line, or specify a file containing the lists of hosts to ping. If a host does not respond within a certain time limit and/or retry limit, it will be considered unreachable.

10. List out the operations of DNSenum DNSenum script can perform the following important operations"

Get the host's addresses

Get the nameservers

Get the MX record

. Perform axfr queries on nameservers

Get extra names and subdomains via Google scraping

Brute force subdomains from file can also perform recursion on subdomain that has NS records

Calculate C class domain network ranges and perform whois queries on them.

Perform reverse lookups on netranges

11. What do you mean by Sniffing?

Sniffing is the process of monitoring and capturing all the packets P passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called wiretapping applied to the computer networks.

12. What can be sniffed?

One can sniff the following sensitive information from a network

• Email traffic

• FTP passwords

• Telnet passwords

• Router configuration

• Chat sessions

• DNS traffic

13. What is ARP Spoofing?

ARP packets can be forged to send data to the attacker's machine.

ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.

The switch is set in forwarding mode and after the ARP table is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target computer ARP cache with forged entries, which is also known as poisoning. ARP poisoning uses Man-in-the-Middle access to poison the network.

PartB &C-16 marks & 8 marks

1. Illustrate the details about information gathering with who's comamnd with suitable commands?
2. Discuss about NSlookup with its steps.
3. Discuss about the function about Netcraft.
4. Examine the functionality of the HOST command.
5. Explain three-way Handshake of TCP protocol.

UNIT IV

Part A

1. Define Intruder.

An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system.

2. List out the types of Intruders.

Masquarader

Misfeaser

Clandestine User

3. Mention the types of IDS.

Host Based Intrusion detection System (HIDS)

Network based intrusion detection System (NIDS)

Hybrid or Distributed IDS

4. How does an IDS work?

An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.

It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.

The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.

If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.

The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

5. What are the benefits of IDS?

Detects malicious activity: IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.

Improves network performance: IDS can identify any performance issues on the network, which can be addressed to improve network performance.

Compliance requirements: IDS can help in meeting compliance requirements by monitoring network activity and generating reports.

Provides insights: IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

6. Point out the types of Anomaly-based detection

Statistical based anomaly detection

Profile based anomaly detection

7. Define Statistical anomaly detection.

Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

8. Define Threshold detection.

This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

9. Define Profile based Intrusion detection.

A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

10. Define Rule-based intusion detection.

Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

11. How do honeypots work in cybersecurity?

Honeypots are network-attached systems intended to mimic likely targets of cyber attacks, such as vulnerable networks. These cyber honeypots can be used to attract, detect, and thereby deflect cybercriminals from hacking into legitimate targets. When hackers make their way into these decoy computer systems, security administrators can gather information about how cybercriminals are trying to hack into information systems and make note of their identities to block them from attacking legitimate systems.

12. Why use honeypots?

A honeypot is a cybersecurity measure with two primary uses: research

and production. Honeypots can both root out and collect information on cybercriminals before they attack legitimate targets, as well as lure them away from those real targets.

13. What are the types of honeypots?

There are different types of honeypots to gather intelligence on cyber threats: email, malware, database, and spider honeypots, along with a new type of honeypot known as a HoneyBot.

PartB &C-16 marks & 8 marks

1. Explore about the different types of Intruders and analyze why intrusion detection is important to provide security in an organization.

2. Explain in detail about Host Based Intrusion Detection.

3. Illustrate with a neat sketch about Network based Intrusion detection.

4. Elaborate with a neat sketch about Distributed or Hybrid Intrusion Detection System.

5. Investigate on how SNORT tool works as Intrusion detection.

Unit V

Part A

1. Define Firewalls.

A firewall can either be software or hardware. Software firewalls are programs installed on each computer, and they regulate network traffic through applications and port numbers. Meanwhile, hardware firewalls are the equipment established between the gateway and your network. Additionally, a firewall delivered by a cloud solution is called as a cloud firewall.

2. List down the types of Firewalls

1. Packet Filtering Firewall.

2. Proxy Service Firewall.

3. Stateful Inspection Firewall.

4. Next-Generation Firewall.

3. Mention the advantages of using Firewalls.

Firewalls play an important role in the companies for security

management. Below are some of the important advantages of using firewalls.

It provides enhanced security and privacy from vulnerable services.

It prevents unauthorized users from accessing a private network that is connected to the internet.

Firewalls provide faster response time and can handle more traffic loads.

A firewall allows you to easily handle and update the security protocols from a single authorized device.

It safeguards your network from phishing attacks.

4. How to Use Firewall Protection?

To keep your network and devices safe, make sure your firewall is set up and maintained correctly. Here are some tips to help you improve your firewall security:

Constantly update your firewalls as soon as possible: Firmware patches keep your firewall updated against any newly discovered vulnerabilities.

Use antivirus protection: In addition to firewalls, you need to use antivirus software to protect your system from viruses and other infections.

Limit accessible ports and host: Limit inbound and outbound connections to a strict whitelist of trusted IP addresses.

Have an active network: To avoid downtime, have active network redundancies. Data backups for network hosts and other critical systems can help you avoid data loss and lost productivity in the case of a disaster.

5. Highlight the Importance of NAT and VPN

NAT and VPN are both basic network translation functions in firewalls.

NAT (Network Address Translation):

It hides or translates internal client or server IP addresses that are usually in a "private address range". It is defined in RFC 1918 as a public IP address.

NAT preserves the limited number of IPv4 addresses and also defends against network reconnaissance as the IP address from the Internet is hidden.

VPN (Virtual Private Network):

VPN is used to extend a private network across a public network inside a tunnel that can be often encrypted. However, the contents inside the packets are protected especially when they are traversing the Internet.

VPN enables users to safely send and receive data across shared or public networks.

6. What are Next Generation Firewalls (NGFW)?

Next-Generation Firewalls are used to inspect packets at the application level of the TCP/IP stack, enabling them to identify applications such as Skype, or Facebook and enforce security policies concerning the type of application. Next-Generation Firewalls also include sandboxing technologies, and threat prevention technologies such as intrusion prevention systems (IPS), or antivirus to detect and prevent malware and threats in the files.

7.Difference between a Firewall and Antivirus.

Firewall

A firewall is essential software or firmware in network security that is used to prevent unauthorized access to a network.

It is used to inspect the incoming and outgoing traffic with the help of a set of rules to identify and block threats by implementing it in software or hardware form.

Firewalls can be used in both personal and enterprise settings, and many devices come with one built-in, including Mac, Windows, and Linux computers.

Antivirus

Antivirus is also an essential component of network security. It is basically an application or software used to provide security from malicious software coming from the internet.

An antivirus working is based upon 3 main actions, Detection, Identification, and Removal of threats.

Antivirus can deal with external threats as well as internal threats by implementing only through software.

8. Point out the limitations of a Firewall.

Firewalls are not able to stop the users from accessing the data or information from malicious websites, making them vulnerable to internal threats or attacks.

It is not able to protect against the transfer of virus-infected files or software if security rules are misconfigured, against non-technical security risks (social engineering)

It does not prevent misuse of passwords and attackers with modems from dialing in to or out of the internal network.

Already infected systems are not secured by Firewalls.

9. How is Firewall useful in Network Security?

A firewall is a security mechanism that prevents unwanted access to private data on your network. Firewalls also protect systems from harmful malware by establishing a barrier between trusted internal networks and untrusted external networks.

10. What Is the Difference Between Firewall And Network Security?

A firewall may protect both software and hardware on a network, whereas an antivirus can protect other software as an impartial software. A firewall prevents harmful software from accessing the system, whereas antivirus software removes corrupted files and software from your computer and network.

11. How does the firewall work?

A firewall protects the network by acting as a 24/7 filter, examining data that seeks to enter the network and blocking anything that appears suspect.

12. What is the Purpose of a Firewall?

Firewalls defend computer or network from outside cyber attackers by filtering out dangerous or superfluous network traffic. Firewalls can also prevent harmful malware from gaining access to a computer or network through the internet.

13. What are the 3 types of firewalls?

Depending on their construction, firewalls can be classified as software firewalls, hardware firewalls, or both. Each sort of firewall serves a distinct purpose but has the same functionality. However, it is best practice to have both for optimal protection.

PartB &C-16 marks & 8 marks

1. List three design goals for a firewall.

2. List four characteristics used by firewalls to control access and enforce a security policy.

3. What information is used by a typical packet filtering firewall?

4. What are some weaknesses of a packet filtering firewall?

5. What is the difference between a packet filtering firewall and a state ful inspection firewall?

6. What is an application-level gateway?