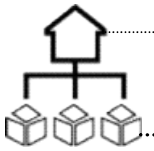

Cyber Security

Important Topics for Cyber Security M.C.Q: Virus, Malware, Sscuity System, Various types of virus and malware, Keylogger, Hacking Technique.

1. Which of the following is not a malware? *[Senior Officer (IT/ICT)-201*

a)Virus b)Worm c)Bug d)Trojan **Ans.:**c

2. Which of the following is not antivirus software? [*Senior Officer (IT/ICT)-2018*]

a) Win-pro b)AVG c) MeAfee d) Symantec **Ans:**a

3. Elaboration of VIRUS is ----------[*SBL (SO-IT/ICT)-2013*]

a) Versatile Information Research Under Seize

b) Vital Information Resource Under Seize.

c) Volume of information Resource under Seize

d) Video Information Resource Under Seize **Ans:**b

4. Which tool could be used for detecting vulnerability through sql injection?

a) nmap b)metasploit c) bit defender d) UML **Ans:**b

5. In which year the term hacking was coined?

a) 1965-67 b) 1955-60 c) 1970-80 d) 1980-82 **Ans:**b

Explanation: When hacking first started it was not thought of as that serious. The hackers were not even known as hackers but as practical jokers. The very first hack came in 1878 when the phone company, Bell Telephone, was started. A group of teenage boys, hired to run the switchboards, would disconnect or misdirect calls.

The first authentic computer hackers came in the 1960s. During those times, computers were mainframes, locked away in temperature controlled, glassed in areas. It cost a lot of money to run these machines, so programmers had limited access to them. So, the smartest ones created what they called "hacks", programming shortcuts, to complete computing tasks more quickly. In some cases the shortcuts were better than the original program. One of the hacks that was created in the 60s, 1969 to be exact, was created to act as an open set of rules to run machines on the computer frontier. It was created by two employees from the Bell Lab's think tank. The two employees were Dennis Ritchie and Ken Thompson and the "hack" was called UNIX.

6. From where the term 'hacker' first came to existence?

a) MIT b) Stanford University

c) California d) Bell's Lab **Ans:** a

7. What is the name of the first hacker's conference?

a) DEFCON b) OSCON c) DEVCON d) SECCON **Ans:** a

Explanation:DEFCON is one of the most popular and largest hacker's as well as a security consultant's conference that takes place every year in Las Vegas, Nevada, where government agents, security professionals, black and white hat hackers from all over the world attend that conference.

8. _____ is the oldest phone hacking techniques used by hackers to make free calls.

a) Phishing b) Spamming c) Phreaking d) Cracking Ans: c

Explanation:Phreaking which is abbreviated as phone-hacking is a slang term and old hacking technique where skilled professionals study, explore & experiment telephone networks in order to acquire the free calling facility.

9. Who coined the term "cyberspace"?

a) Andrew Tannenbaum

b) Scott Fahlman

c) William Gibsond) Richard Stallman Ans: c

Explanation:In the year 1821, an American – Canadian fiction pioneer cum writer, William Gibson explored the different streams of technologies and coined the term "cyberspace". The term defines interconnected technologies that help in sharing information, interact with digital devices, storage and digital entertainment, computer and network security and stuff related to information technology.

10. An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

a) Cyber-crime b) Cyber Attack c) System hijacking d) Digital crime Ans: b

Explanation:A cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cybercriminals use a variety of methods to launch a cyber attack, including malware, phishing, ransomware, denial of service, among other methods.

Cyber attack is an umbrella term used to classify different computer & network attacks or activities such as extortion, identity theft, email hacking, digital spying, stealing hardware, mobile hacking and physical security breaching.

11. Which is the legal form of hacking based on which jobs are provided in IT industries and firms?

a) Cracking b) Non ethical Hacking

c) Ethical hacking d) Hactivism Ans: c

Explanation:Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.Ethical hackers are expected to report all the vulnerabilities and weakness found during the process to the management.

12. The amateur or newbie in the field of hacking who don't have many skills about coding and in-depth working of security and hacking tools are called _____

a) Sponsored Hackers b) Hactivists

c) Script Kiddies d) Whistle Blowers **Ans:** c

Explanation:Script Kiddies are new to hacking and at the same time do not have many interests in developing coding skills or find bugs of their own in systems; rather they prefer downloading of available tools (developed by elite hackers) and use them to break any system or network. They just try to gain attention of their friend circles.

13. The full form of Malware is _____

a) Malfunctioned Software b) Multipurpose Software

c) Malicious Software d) Malfunctioning of Security **Ans:** c

Explanation:Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

Full description about malicious software

Introduction

Viruses, worms, Trojans, and bots are all part of a class of software called "malware." Malware is short for "malicious software," also known as malicious code or "malcode." It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks.

Malware can infect systems by being bundled with other programs or attached as macros to files. Others are installed by exploiting a known vulnerability in an operating system (OS), network device, or other software, such as a hole in a browser that only requires users to visit a website to infect their computers. The vast majority, however, are installed by some

action from a user, such as clicking an email attachment or downloading a file from the Internet.

Some of the more commonly known types of malware are viruses, worms, Trojans, bots, ransomware, backdoors, spyware, and adware. Damage from malware varies from causing minor irritation (such as browser popup ads), to stealing confidential information or money, destroying data, and compromising and/or entirely disabling systems and networks.

Classes of Malicious Software

Two of the most common types of malware are

1. viruses and
2. worms.

These types of programs are able to self-replicate and can spread copies of themselves, which might even be modified copies.

Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called *cryptoviral extortion*, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program.

Worms

On a computer, a worm is similar to a virus, in that it replicates itself. But unlike viruses, worms don’t need to be attached to other files.In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them.

Trojans

A Trojan is another type of malware named after the wooden horse that the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create backdoors to give malicious users access to the system.

Bots

"Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information, such as web crawlers, or interact automatically with Instant Messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites.

Keylogger

A **keylogger**, or **keystroke logger**, is a type of malware that records all keystrokes that a user types on their computer. A keylogger can also be a hardware device, connected somewhere between a keyboard and a computer. Keyloggers can record all sorts of personal information, such as user names, passwords, credit card numbers, and personal documents such as emails and reports. Keyloggers can be useful to obtain information that can be later used to access a user's online accounts, or for espionage.

How malware spread :

Advanced malware typically comes via the following distribution channels to a computer or network:

- Drive-by download—Unintended download of computer software from the Internet
- Unsolicited email —Unwanted attachments or embedded links in electronic mail
- Physical media—Integrated or removable media such as USB drives
- Self propagation—Ability of malware to move itself from computer to computer or network to network, thus spreading on its own

Difference between Virus, Worm and Trojan Horse:

Virus	Worm	Trojan Horse

Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.
Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility software.

14. Which of the following is an anti-virus program?

a) Norton b) K7 c) Quick Heal d) All of these **Ans:** d

15. All of the following are examples of real security and privacy threats except:

a) Hackers b) Virus c) Spam d) Worm **Ans:** c

16. Viruses are _____.

a) Man Made b) Naturally Occur

c) Machine Made d) All of these **Ans:** a

17. Firewall is a type of _____.

a) Virus b) Security Threat

c) Worm d) None of these **Ans:** d

Explanation: Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

18. _____ is a code injecting method used for attacking the database of a system website.

a) HTML injection b) SQL Injection

c) Malicious code injection d) XML Injection **Ans:** b

Explanation:SQLi (Structured Query Language Injection) is a popular attack where SQL code is targeted or injected; for breaking the web application having SQL vulnerabilities. This allows the attacker to run malicious code and take access to the database of that server.

19. XSS is abbreviated as _____

a) Extreme Secure Scripting b) Cross Site Security

c) X Site Scripting d) Cross Site Scripting **Ans:** d

Explanation:Cross Site Scripting is another popular web application attack type that can hamper the reputation of any site.

Common Hacking Techniques

1. **Phishing**

   Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

2. **Viruses and malicious code**

   Hackers can crawl almost into any website and leave in its' database malware or insert code into the website's files. There is a huge variety of viruses, and each may impact the infected site differently. But there should be no doubt that a virus, regardless of its type, will not benefit your business.

3. **UI Redress**

   This technique is similar to phishing. But in this case, a hacker would create a fake hidden user interface. Once the a user clicks the button with an intention of to proceed to a certain page, he will find himself on an unfamiliar website, usually with an inappropriate content.

4. **Cookie Theft**

   With the help of a malicious software hackers can steal your browser's cookies. And those cookies contain a lot of important information: browsing history, usernames and passwords. As you understand,that data can also contain logins and password to your website's administrator's panel.

5. **Denial of Service (DoS\DDoS)**

   A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both

instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services.

6. **DNS spoofing**

This malware is also known as DNS cache poisoning. It engages that old cache data you might have forgotten about.

Vulnerabilities in the domain name system allow hackers to redirect traffic from your website to a malicious one. Moreover, hackers can program this attack so the infected DNS server will infect another DNS and so on.

7. **SQL injection**

If your website has vulnerabilities in its SQL database or libraries, hackers can get access to your confidential information by deceiving the system.So there is no surprise that SQL injections can also be a simple tool. But this simple tool can allow a hacker to access vital information of your website.

8. **Keylogger injection**

The Keylogger that very simple and dangerous malicious code.

The malware records keystrokes , captures all of the user's actions on the keyboard, and to send all that has been recorded to the hackern ; it also installs a malicious script that produces an in-browser cryptocurrency miner.

If a hacker succeeds in obtaining data, then the result of the hacking will be stolen admin credentials that can allow hackers to easily log into your website

9. **Non-targeted website hack**

In most cases, hackers don't target a specific website. They are more interested in massive hacking.

It is easy to suffer from a non-targeted attack – you just need to overlook any CMS, plugin or template vulnerability. Any gap is a chance to get into the hacker's sight and become a victim during the next attack.

Hackers can find websites with similar weaknesses easily. They can always use Google's Hacking Database to receive a list of vulnerable websites that have the same properties. For example, hackers can find all indexed websites that have a vulnerable plugin installed. Or websites with unhidden catalogues.

10. **Brute force**

A Brute Force Attack is the simple method to gain access to a website. It tries various combinations of the passwords again and again until it gets in. This repetitive action is like an army attacking a fort.

20. This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

a) SQL injection b) HTML Injection

c) Cross Site Scripting (XSS) d) Cross Site Request Forgery (XSRF) **Ans:** c

Explanation:XSS attack can be infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage (usually a blogging page). This can hamper the reputation of a site and the attacker may place any private data or personal credentials.

21. When there is an excessive amount of data flow, which the system cannot handle, _____ attack takes place.

a) Database crash attack b) DoS (Denial of Service) attack

c) Data overflow Attack d) Buffer Overflow attack **Ans:** d

Explanation:The Buffer overflow attack takes place when an excessive amount of data occurs in the buffer, which it cannot handle and lead to data being over-flow into its adjoined storage. This attack can cause a system or application crash and can lead to malicious entry-point.

22. Which of the following is not an example of physical data leakage?

a)Phishing b)Dumpster diving

c)Shoulder surfing d) Printers and photocopiers **Ans:** a

23. Compromising a user's session for exploiting the user's data and do malicious activities or misuse user's credentials is called _____

a) Session Hijacking b) Session Fixation

c) Cookie stuffing d) Session Spying **Ans:** a

Explanation:Session hijacking is an attack where a user session is taken over by an attacker. A session starts when you log into a service, for example your banking application, and ends when you log out. The attack relies on the attacker's knowledge of your session cookie, so it is also called cookie hijacking or cookie side-jacking. Although any computer session could be hijacked, session hijacking most commonly applies to browser sessions and web applications.

24. Which of this is an example of physical hacking?

a) Remote Unauthorised access

b) Inserting malware loaded USB to a system

c) SQL Injection on SQL vulnerable site

d) DDoS (Distributed Denial of Service) attack **Ans:** b

Explanation:If a suspicious gain access to server room or into any confidential area with a malicious pen-drive loaded with malware which will get triggered automatically once inserted to USB port of any employee's PC; such attacks come under physical hacking, because that person in gaining unauthorized physical access to any room or organization first, then managed to get an employee's PC also, all done physically – hence breaching physical security.

25. Which method of hacking will record all your keystrokes?

a) Keyhijacking b) Keyjacking

c) Keylogging d) Keyboard monitoring **Ans:** c

Explanation: Keylogging is the method or procedure of recording all the key strokes/keyboard button pressed by the user of that system.

26. These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actions over a digital medium.

a) Malware b) Remote Access Trojans

c) Keyloggers d) Spyware **Ans:** d

Explanation:Spyware is professional malicious spying software that is hard to detect by anti-malware or antivirus programs because they are programmed in such a skillful way. These types of software keep on collecting personal information, surfing habits, surfing history as well as credit card details.

27. In general how many key elements constitute the entire security structure?

a) 1 b) 2 c) 3 d) 4 **Ans:** d

Explanation:The 4 key elements that constitute the security are: confidentiality, integrity, authenticity & availability. Authenticity is not considered as one of the key elements in some other security models, but the popular CIA Triad eliminates this as authenticity at times comes under confidentiality & availability.

Confidentiality

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people while making sure that authorized people can access it.

Integrity

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. It actually protects data from modification by unknown users. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by

unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls.

Integrity, in the world of information security means maintaining the accuracy, and completeness of data. It is about protecting data from being modified or misused by an unauthorized party. Integrity involves maintaining the consistency and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and precautionary steps must be taken to ensure that data cannot be altered by unauthorized people.

For example, in a breach of integrity, a hacker may seize data and modify it before sending it on to the intended recipient.

Measures to maintain the integrity of information include:

1. Encryption
2. User Access Controls
3. Version Control

Authenticity

Authenticity is verification of a message or document to ensure it wasn't forged or tampered with. Examples include digital signature and HMAC.

Availability

Availability means that information is accessible to authorized users. It is basically an assurance that your system and data are accessible by authorized users whenever it's needed. Similar to confidentiality and integrity, availability also holds a great value.

Different between Authentication and Authenticity

Athentication is the act of certifying authenticity.So if something is authentic it's real. In security it means that something is what it proports to be. For example a user really is who they claim, a program has not been tampered with, that server really does belong to your bank.

Authentication in computer security typically involves shared secrets (eg passwords, symmetric encryption keys) or asymmetric aka public key encryption where only one party knows the key but the other can mathematically authenticate that knowledge.

28. This is the model designed for guiding the policies of Information security within a company, firm or organization. What is "this" referred to here?

a) Confidentiality b) Non-repudiation

c) CIA Triad d) Authenticity **Ans:** c

Explanation:Various security models were being developed till date. This is by far the most popular and widely used model which focuses on the information's confidentiality, integrity as well as availability and how these key elements can be preserved for a better security in any organization.

29. When you use the word _____ it means you are protecting your data from getting disclosed.

a) Confidentiality b) Integrity c) Authentication d) Availability **Ans:** a

Explanation:

Confidentiality is what every individual prefer in terms of physical privacy as well as digital privacy. This term means our information needs to be protected from getting disclose to unauthorised parties, for which we use different security mechanisms like password protection, biometric security, OTPs (One Time Passwords) etc.

30. _____ means the protection of data from modification by unknown users.

a) Confidentiality b) Integrity c) Authentication d) Non-repudiation **Ans:** b

31. When integrity is lacking in a security system, _____ occurs.

a) Database hacking b) Data deletion c) Data tampering d) Data leakage **Ans:** c

Explanation: The term data tampering is used when integrity is compromised in any security model and checking its integrity later becomes costlier. Example: let suppose you sent $50 to an authorised person and in between a Man in the Middle (MiTM) attack takes place and the value has tampered to $500. This is how integrity is compromised.

32. _____ of information means, only authorised users are capable of accessing the information.

a) Confidentiality b) Integrity

c)Non-repudiation d)Availability **Ans:** d

Explanation: Information seems useful only when right people (authorised users) access it after going through proper authenticity check. The key element availability ensures that only authorised users are able to access the information.

33. Transit time and response time measure the _____ of a network

a) Performance b) Reliability c)Security d)Longevity **Ans:** a

34. Network failure is primarily a _____ issue.

a) Performance b) Reliability c)Security d)Longevity **Ans:** b

35. _____ is a network reliability issue.

a) The number of users b) The type of transmission medium

c)The frequency of failure d)Unauthorized access **Ans:** c

36. Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?

a) They help understanding hacking better

b) They are key elements to a security breach

c) They help understands security and its components better

d) They help to understand the cyber-crime better **Ans:** c

Explanation:The four elements of security viz. confidentiality, integrity, authenticity & availability helps in better understanding the pillars of security and its different components.

37. This helps in identifying the origin of information and authentic user. This referred to here as _____

a) Confidentiality b) Integrity c) Authenticity d) Availability **Ans:** c

Explanation:The key element, authenticity helps in assuring the fact that the information is from the original source.

38. Data _____ is used to ensure confidentiality.

a) Encryption b) Locking c) Deleting d) Backup **Ans:** a

Explanation:Data encryption is the method of converting plain text to cipher-text and only authorised users can decrypt the message back to plain text. This preserves the confidentiality of data

39. Which of these is not a proper method of maintaining confidentiality?

a) Biometric verification
b) ID and password based verification
c) 2-factor authentication
d) switching off the phone **Ans:** d

Explanation:Switching off the phone in the fear of preserving the confidentiality of data is not a proper solution for data confidentiality. Fingerprint detection, face recognition, password-based authentication, two-step verifications are some of these.

40. Data integrity gets compromised when _____ and _____ are taken control off.

a) Access control, file deletion
b) Network, file permission
c) Access control, file permission
d) Network, system **Ans:** c

Explanation:The two key ingredients that need to be kept safe are: access control & file permission in order to preserve data integrity.

41. One common way to maintain data availability is _____

a) Data clustering b) Data backup
c) Data recovery d) Data Altering **Ans:** b

Explanation: For preventing data from data-loss, or damage data backup can be done and stored in a different geographical location so that it can sustain its data from natural disasters & unpredictable events.

42. _____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

a) Network Security b) Database Security

c) Information Security d) Physical Security **Ans:** c

Explanation: Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information for alteration, destruction, deletion or disclosure by unauthorised users.

43. From the options below, which of them is not a threat to information security?

a) Disaster b) Eavesdropping

c) Information leakage d) Unchanged default password **Ans:** d

Explanation: Disaster, eavesdropping and information leakage come under information security threats whereas not changing the default password of any system, hardware or any software comes under the category of vulnerabilities that the user may pose to its system.

44. From the options below, which of them is not a vulnerability to information security?

a) flood

b) without deleting data, disposal of storage media

c) unchanged default password

d) latest patches and updates not done **Ans:** a

Explanation: Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

45. Compromising confidential information comes under _____

a) Bug b) Threat c) Vulnerability d) Attack **Ans:** b

Explanation: Threats are anything that may cause damage or harm to a computer system, individual or any information. Compromising of confidential information means extracting out sensitive data from a system by illegal manner.

46. Lack of access control policy is a _____

a) Bug b) Threat c) Vulnerability d) Attack **Ans:** c

Explanation: Access control policies are incorporated to a security system for restricting of unauthorised access to any logical or physical system. Every security compliance program must need this as a fundamental component. Those systems which lack this feature is vulnerable.

47. _____ is the kind of firewall is connected between the device and the network connecting to internet.

a) Hardware Firewall b) Software Firewall

c) Stateful Inspection Firewall d) Microsoft Firewall **Ans:** a

Explanation:Hardware firewalls are those firewalls that need to be connected as additional hardware between the device through which the internet is coming to the system and the network used for connecting to the internet.

48. _____ is software that is installed using an internet connection or they come by-default with operating systems.

a) Hardware Firewall b) Software Firewall
c) Stateful Inspection Firewall d) Microsoft Firewall **Ans:** b

Explanation:Software firewalls are those kinds of firewalls that are installed in the system using internet connection as we install normal applications and update them. Some operating system vendors provide default firewalls with their operating systems.

Brief discussion about Firewall

A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (a.k.a. proxy firewalls)
- Next-gen firewalls
- Software firewalls
- Hardware firewalls
- Cloud firewalls

49. Firewall examines each _____ that are entering or leaving the internal network.

a) emails users b) updates c) connections d) data packets **Ans:** d

Explanation:Firewalls examines each data packets that are entering or leaving the internal network which ultimately prevents unauthorized access.

50. A firewall protects which of the following attacks?

a) Phishing b) Dumpster diving
c) Denial of Service (DoS) d) Shoulder surfing **Ans:** c

Explanation:Firewalls are used to protect the computer network and restricts illicit traffic. Denial of Service (DoS) attack is one such automated attack which a firewall with proper settings and the updated version can resist and stop from getting executed.

51. Packet filtering firewalls are deployed on _____

a) routers b) switches c) hubs d) repeaters **Ans:** a

Explanation:Packet filtering firewalls are deployed on routers that help in connecting internal network worldwide via the internet.

52. In the _____ layer of OSI model, packet filtering firewalls are implemented.

a) Application layer b) Session layer

c) Presentation layer d) Network layer **Ans:** d

Explanation:In the network layer, which is the third layer of the OSI (Open Systems Interconnection) model, packet filtering firewalls are implemented.