PRATICAL THEORY

EXPT1:

What is a network topology?

A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph.

Network topologies describe the arrangement of networks and the relative location of traffic flows. Administrators can use network topology diagrams to determine the best placements for each [node](https://www.techtarget.com/searchnetworking/definition/node) and the optimal path for traffic flow. With a well-defined and planned-out network topology, an organization can more easily locate faults and fix issues, improving its data transfer efficiency.

Network geometry can be defined as the physical topology and the logical topology. Network topology diagrams are shown with devices depicted as network nodes and the connections between them as lines. The type of network topology differs depending on how the network needs to be arranged.

Packet Tracer:

Cisco Packet Tracer as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks.

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Students complete assignments using this tool, working on their own or in teams.

Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them. Also, Engineers who would like to deploy any change in the production network prefer to use Cisco Packet Tracer to first test the required changes and proceed to deploy if and only if everything is working as expected.

This makes the job easier for Engineers allowing them to add or remove simulated network devices, with a Command line interface and a drag and drop user interface.

EXPT2:

What is Wireshark?

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses of Wireshark:

Wireshark can be used in the following ways:

* It is used by network security engineers to examine security problems.
* It allows the users to watch all the traffic being passed over the network.
* It is used by network engineers to troubleshoot network issues.
* It also helps to troubleshoot latency issues and malicious activities on your network.
* It can also analyze dropped packets.
* It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

EXPT3:

1Password :

1Password is a [password manager](https://en.wikipedia.org/wiki/Password_manager) developed by AgileBits Inc. It supports multiple platforms such as [iOS](https://en.wikipedia.org/wiki/IOS), [Android](https://en.wikipedia.org/wiki/Android_(operating_system)), [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows), [Linux](https://en.wikipedia.org/wiki/Linux), and [macOS](https://en.wikipedia.org/wiki/MacOS). It provides a place for users to store various passwords, [software licenses](https://en.wikipedia.org/wiki/Software_license), and other sensitive information in a virtual vault that is locked with a [PBKDF2](https://en.wikipedia.org/wiki/PBKDF2)-guarded master password. By default, the user’s encrypted vault is hosted on AgileBits’ servers for a monthly fee. The company is based in [Toronto](https://en.wikipedia.org/wiki/Toronto).

Honeypot:

Honeypot is a network-attached system used as a trap for cyber-attackers to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

The cost of a honeypot is generally high because it requires specialized skills and resources to implement a system such that it appears to provide an organization’s resources still preventing attacks at the backend and access to any production system.

A honeynet is a combination of two or more honeypots on a network.

Types of Honeypot:

Honeypots are classified based on their deployment and the involvement of the intruder.  
Based on their deployment, honeypots are divided into:

* Research honeypots- These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.
* Production honeypots- Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

EXPT4:

What is data maintenance?

Data maintenance is the ongoing process of running regular checks to identify and correct data that does not follow company standards in your CRM database. The goal is to improve the quality and organization of your data to improve your business’s growth and profitability.

Data quality

Data quality can make or break your business, which is why it’s top of the priority list for data maintenance. Data quality is determined by whether your data fits the following six factors:

* Accuracy
* Completeness
* Reliability
* Relevance
* Timeliness
* Validity

Depending on how your data ranks for each of these factors will determine whether your data serve your organization’s needs. If the data is not meeting professional standards in one or more of these categories, data maintenance will work to improve your data quality.

Data cleaning

Data cleaning, also known as data cleansing, is a process that searches for errors (data that is incorrect, missing, mis formatted, etc.) in your data and attempts to fix these issues.

It can be easy to lump data maintenance and data cleaning into the same boat, but the two refer to different ideas. While data maintenance is a consistently run strategy that aims to improve your data, data cleaning is a process that is identifying and correcting or removing errors from your data.

Data cleaning should be performed regularly as part of your data maintenance strategy. Both are equally important and intrinsically tied together as part of regular data maintenance upkeep and improvement.

Data deduplication

Working with any amount of data can increase the potential for redundant data that can harm your data quality and fill up your data storage. Similarly, if your customer data is filled with redundant data, it will negatively impact your sales and marketing efforts, as well. This is where data deduplication enters the picture.

Data deduplication is a process that removes extra or excessive copies of data in your data sets. The copies are removed so that only the singular piece of data remains in the master data.

This effective technique works to improve efficiency by reducing the chances of your team using redundant data, which can hurt any and all business processes. It can increase data insight accuracy and improve your customer engagement and experience. It also allows for more data storage space and helps to improve your brand’s overall operations.

EXPT5:

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 [Internet](https://www.javatpoint.com/internet) in infected computers.

Antivirus Software:

Antivirus software is a program(s) that is created to search, detect, prevent and remove software viruses from your system that can harm your system. Other harmful software such as worms, adware, and other threats can also be detected and removed via antivirus. This software is designed to be used as a proactive approach to cyber security, preventing threats from entering your computer and causing issues. Most antivirus software operates in the background once installed, providing real-time protection against virus attacks.

While you may believe that your computer is safe as long as you don’t visit questionable websites, hackers have far more sophisticated methods of infecting your computer, which is why you need a powerful antivirus to stay to secure your data and system. The implications of a virus getting into your computer might be fatal. Viruses can cause a wide range of malicious behavior. They can crash your device, monitor your personal accounts, or spy on you through your webcam. So, always use antivirus software.

EXPT6:

GitHub:

GitHub is an increasingly popular[programming](https://www.simplilearn.com/how-to-learn-programming-article) resource used for code sharing. It's a social networking site for [programmers](https://www.simplilearn.com/how-to-become-programmer-article) that many companies and organizations use to facilitate project management and collaboration. According to [statistics collected in October 2020](https://octoverse.github.com/), it is the most prominent source code host, with over 60 million new repositories created in 2020 and boasting over 56 million total developers.

What is a Version Control System?

The Git version control system, as the name suggests, is a system that records all the modifications made to a file or set of data so that a specific version may be called up later if needed. The system makes sure that all the team members are working on the file’s latest version, and everyone can work simultaneously on the same project.

Repository

1. A GitHub repository can be used to store a development project.
2. It can contain folders and any type of files (HTML, CSS, JavaScript, Documents, Data, Images).
3. A GitHub repository should also include a licence file and a README file about the project.
4. A GitHub repository can also be used to store ideas, or any resources that you want to share.

EXPT7:

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Types Of Cryptography: In general there are three types Of cryptography:

1. Symmetric Key Cryptography: It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
2. Asymmetric Key Cryptography: Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

**Digital Signature**

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender ([authenticity](https://en.wikipedia.org/wiki/Authentication)), and that the message was not altered in transit ([integrity](https://en.wikipedia.org/wiki/Data_integrity)).

EXPT8:

\*\* From Journal \*\*

EXPT9:

HTML (Hypertext Markup Language) is a text-based approach to describing how content contained within an HTML file is structured. This markup tells a web browser how to display text, images and other forms of multimedia on a webpage.

HTML is a formal recommendation by the World Wide Web Consortium ([W3C](https://www.techtarget.com/whatis/definition/W3C-World-Wide-Web-Consortium)) and is generally adhered to by all major web browsers, including both desktop and mobile web browsers. [HTML5](https://www.techtarget.com/whatis/definition/HTML5) is the latest version of the specification.

HTML is a text file containing specific syntax, file and naming conventions that show the computer and the web server that it is in HTML and should be read as such. By applying these HTML conventions to a text file in virtually any text editor, a user can write and design a basic webpage, and then upload it to the internet.

\*\*Basic Syntax Study from Journal\*\*

EXPT10:

What is SQL injection (SQLi)?

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

EXPT11:

\*\* From Journal \*\*

EXPT12:

\*\* From Journal \*\*

EXPT13:

\*\* From Journal \*\*

EXPT14:

\*\* From Journal \*\*

EXPT15:

\*\* From Journal \*\*

EXPT16:

Rootkit definition and meaning

A rootkit is a type of malware designed to give hackers access to and control over a target device. Although most rootkits affect the software and the operating system, some can also infect your computer’s hardware and firmware. Rootkits are adept at concealing their presence, but while they remain hidden, they are active.

Once they gain unauthorized access to computers, rootkits enable cybercriminals to steal personal data and financial information, install malware or use computers as part of a [botnet](https://www.kaspersky.com/resource-center/threats/botnet-attacks) to circulate spam and participate in [DDoS (distributed denial of service) attacks](https://www.kaspersky.com/resource-center/threats/ddos-attacks).

The name “rootkit” derives from Unix and Linux operating systems, where the most privileged account admin is called the "root". The applications which allow unauthorized root or admin-level access to the device are known as the "kit".

Types of rootkits

1. Hardware or firmware rootkit

2. Bootloader rootkit

3. Memory rootkit

4. Application rootkit

5. Kernel mode rootkits

6. Virtual rootkits

EXPT17:

Threat modeling is a procedure for optimizing application, system or business process security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent or mitigate the effects of threats to the system.

Threat modeling helps to identify the security requirements of a system or process -- anything that is mission-critical, processing sensitive or made up of valuable data. It is a systematic and structured process that aims to identify potential threats and [vulnerabilities](https://www.techtarget.com/whatis/definition/vulnerability) to reduce the risk to IT resources. It also helps IT managers understand the impact of threats, quantify their severity and implement controls.

In terms of software security, threat modeling is the [most important part of software design and development](https://www.techtarget.com/searchsecurity/tip/Why-threat-models-are-crucial-for-secure-software-development). It is impossible to build applications and systems that comply with corporate [security policies](https://www.techtarget.com/searchsecurity/definition/security-policy) and privacy and regulatory requirements without evaluating and mitigating threats.

IT-based threat modeling gained traction in the 1990s with the development of threat and attacker profiles. Microsoft introduced its STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) threat modeling methodology in 1999. There are now many other approaches. They all involve deconstructing the elements of an application or system to identify the assets to be protected and the possible threats to be mitigated. A threat modeling methodology is a way to break down a complex process into smaller tasks making it easy to spot weaknesses.

EXPT18:

* **OWASP ZAP** (short for Zed Attack Proxy) is an [open-source](https://en.wikipedia.org/wiki/Open-source_software) [web application security scanner](https://en.wikipedia.org/wiki/Web_application_security_scanner). It is intended to be used by both those new to application security as well as professional penetration testers.
* It is one of the most active Open Web Application Security Project ([OWASP](https://en.wikipedia.org/wiki/OWASP)) projects and has been given Flagship status.
* When used as a [proxy server](https://en.wikipedia.org/wiki/Proxy_server) it allows the user to manipulate all of the traffic that passes through it, including traffic using [HTTPS](https://en.wikipedia.org/wiki/HTTPS).
* It can also run in a [daemon](https://en.wikipedia.org/wiki/Daemon_(computing)) mode which is then controlled via a [REST](https://en.wikipedia.org/wiki/Representational_state_transfer) [API](https://en.wikipedia.org/wiki/Application_programming_interface).
* ZAP was added to the [Thought Works](https://en.wikipedia.org/wiki/ThoughtWorks) Technology Radar on May 30, 2015 in the Trial ring.
* ZAP was originally forked from Paros, another pentesting proxy. Simon Bennetts, the project lead, stated in 2014 that only 20% of ZAP's source code was still from Paros.

Features:

* An intercepting [proxy server](https://en.wikipedia.org/wiki/Proxy_server),
* Traditional and [AJAX](https://en.wikipedia.org/wiki/Ajax_(programming)) [Web crawlers](https://en.wikipedia.org/wiki/Web_crawler)
* An automated scanner
* A passive scanner
* Forced browsing
* A [fuzzer](https://en.wikipedia.org/wiki/Fuzzing" \o "Fuzzing)
* [WebSocket](https://en.wikipedia.org/wiki/WebSocket) support
* [Scripting languages](https://en.wikipedia.org/wiki/Scripting_language)
* Plug-n-Hack support

EXPT19:

\*\* From Journal \*\*

EXPT20:

\*\* From Journal \*\*

EXPT21:

Trivy (tri pronounced like trigger, vy pronounced like envy) is a simple and comprehensive vulnerability scanner for containers and other artifacts. A software vulnerability is a glitch, flaw, or weakness present in the software or in an Operating System. Trivy detects vulnerabilities of OS packages (Alpine, RHEL, CentOS, etc.) and application dependencies (Bundler, Composer, npm, yarn, etc.). Trivy is easy to use. Just install the binary and you're ready to scan. All you need to do for scanning is to specify a target such as an image name of the container.

EXPT22:

EventLog Analyzer is a web-based, real-time, log monitoring and compliance management solution for Security Information and Event Management (SIEM) that improves network security and helps you comply with the IT audit requirements. Using an agent less architecture, EventLog Analyzer can collect, analyze, search, report on, and archive logs received from systems (Windows, Linux/UNIX), network devices (routers, switches, firewalls, and IDS/IP), applications (Oracle, SQL and Apache). It provides important insights into user activities, policy violations, network anomalies, system downtime, and internal threats. It can be used by network administrators and IT managers to perform audits for regulations such as SOX, HIPAA, PCI DSS, GLBA, etc.

You can use EventLog Analyzer to:

* Monitor activities of servers, workstations, devices, and applications spread across geographies.
* Monitor user activities like logons/logoffs and objects accessed.
* Generate reports for security events of interest.
* Generate compliance reports for PCI DSS, HIPAA, FISMA, SOX, GLBA and other regulatory mandates.
* Perform log forensics by swiftly searching the log database and save the search results as reports.
* Configure automatic e-mail or SMS alerts for indicators of compromise, such as network anomalies or compliance threshold violations.
* Execute workflows upon alert generation to respond to security threats automatically.
* Secure and tamper-proof archival of log data for forensic analysis and compliance audits.

EXPT23:

EXPT24:

What is Nmap?

Nmap is an open-source utility for network discovery. Network Mapper is a security auditing and network scanning independent tool developed by Gordon Lyon. It is used by network administrators to detect the devices currently running on the system and the port number by which the devices are connected.

Many systems and network administrators are used for managing network inventory, service upgrade schedules, monitoring hosts and service uptime.

Nmap Definition

At the top-level, [Nmap](https://www.educba.com/nmap-commands/) is defined as a tool that can detect or diagnose services that are running on an Internet-connected system by a network administrator in their networked system used to identify potential security flaws. It is used to automate redundant tasks, such as monitoring the service.

EXPT25:

\*\* From Journal \*\*

EXPT26:

\*\* From Journal \*\*

EXPT27:

Reverse engineering, sometimes called back engineering, is a process in which software, machines, aircraft, architectural structures and other products are deconstructed to extract design information from them. Often, reverse engineering involves deconstructing individual components of larger products. The reverse engineering process enables you to determine how a part was designed so that you can recreate it. Companies often use this approach when purchasing a replacement part from an original equipment manufacturer (OEM) is not an option.

The reverse engineering process is named as such because it involves working backward through the original design process. However, you often have limited knowledge about the engineering methods that went into creating the product. Therefore, the challenge is to gain a working knowledge of the original design by disassembling the product piece-by-piece or layer-by-layer.

EXPT30:

\*\* From Journal \*\*

EXPT31:

\*\* From Journal \*\*

EXPT32:

\*\* From Journal \*\*