Task3-1017-Vuppala Likitha

**1.Write about 35 protocols and the port numbers in detail.**

**1.**File Transfer Protocol (FTP)

**Port number is 20,21**

It is a protocol that carries data guarantees that data will be delivered properly.

**2.**Secure Shell (SSH)

Port number is **22**

It is a cryptographic network protocol used to secure data communication.

**3.**Telnet

Port number is **23**

It is the used for remote management protocol for managing network devices.

**4.**Simple Mail Transfer Protocol (SMTP)

Port number is **25**

It is a communication protocol which is used to transmit email messages over the internet to the destination server.

**5.**Domian Name System (DNS)

Port number is **53**

It is used in the performance of one simple task of converting IP address

To domain names that everyone can easily understand.

**6.**Trivial File Transfer Protocol (TFTP)

Port number is **69**

TFTP is typically used by devices to upgrade software and firmware and that include cisco.

**7.**Hyper Text Transfer Protocol (HTTP)

Port number is **80**

It is a kind of protocol used to define how data is transmitted and formatted and also used by www as a channel for communication.

**8.**Dynamic Host Configuration Protocol (DHCP)

Port number is **67 & 68**

It is a kind of service used in the client and server model.

**9.**Post Office Protocol 3 (POP3)

Port number is **110**

It is a protocol used by e-mail client to retrieve e-mail from the servers.

**10.**Network News Transport Protocol (NNTP)

Port number is **119**

nntp is an application protocol used for transporting USENET news articles between news servers and the end user client.

**11.**Network Time Protocol (NTP)

Port number is **123**

It is the synchronization of time between network devices in the network.

**12.**NetBIOS

Port number is **135 & 139**

NetBIOS itself is not a protocol but is typically used in combination with IP with the NetBIOS over TCP/IP protocol.

**13.**Simple Network Management Protocol (SNMP)

Port number is **161 & 162**

It has the ability to monitor, configure and control network devices.

**14.**Lightweight Directory Access Protocol

Port number is **389**

LDAP provides a mechanism of accessing and maintaining distributed directory information.

**15.**Transport Layer Security (TLS)

Port number is **443**

It is a protocol of a secured socket layer that uses asymmetric keys to transfer data over a network.

**16.**Real-Time Transport Protocol. (RTP)

Port number is **1023 TO 65535**

It is used for delivering audio and video data over an IP network.

**17.**Hyper Text Transfer Protocol Secure. (HTTPS)

Port number is **443**

It renders authentication and encryption that provides secure communication with the use of secure socket layer.

**18.**Internet Message Access Protocol. (IMAP4)

Port number is **143**

It is an application layer protocol and an internet standards for e-mail retrieval.

**19.**Address Resolution Protocol (ARP)

Port number is **3389**

It is used to resolve the network layer address into the link address.

**20.**Border Gateway Protocol (BGP)

Port number is **179**

It is used to maintain very large routing tables and traffic processing.

**21.**Internet Relay Chat (IRC)

Port number is **194**

It is an application layer protocol that facilitate communication in the form of text

**22.**Session Initiation Protocol. (SLP)

It is used to establish, modify, and terminate multimedia communication session such as VoIP.

**23.**Session Description Protocol.(SDP) It describes the content of multimedia communication.

**24.**Remote Desktop Protocol. (RDP)

Port number is **3389**

It provides a user with a graphical interface to connect to another computer over a network connection.

**25.**Server Message Block (SMB).

It is an application layer protocol that helps in accessing network resources, such as shared files and printers.

**26.**Secure File Transfer Protocol (SFTP)

Port number is **22**

It uses the SSH protocol to access and transfer file over the network.

**27.**Internet Group Management Protocol (IGMP)

Port number is **2**

It is a communication protocol used by hosts and adjacent routers on IPv4 network to establish multicast group membership.

**28.**Route Access Protocol (RAP)

Port number is **38**

**29**.Resource Location Protocol (RLP)

Port number is **39**

It is used for determining the location of higher level service from host on a network.

**30.**Host Name Server Protocol (HNSP)

Port number is **42**

**31**.Internet Control Messages Protocol (ICMP)

It is used by a ping utility to check the reachability the device in a network.

**32**.Remote Directory Access Protocol (RDAS)

It is used retrieves information about domain names from a central registry.

**33**.Lightweight Presentation Protocol (LPP)

It is describe an approach for providing stream lined support of  OSI application services on top of TCP/IP –based network for some constrained environment

**34.**Remote Procedure Call Protocol (RPC)

It is a protocol for requesting a service from a program location in a remote computer through a network.

**35.**Network Address Translation (NAT)

Port number is **3022**

It is the method by which IP addresses are mapped from one group to another, transparent to end users.

**36.**Microsoft Active Directory Protocol (MADP)

Port number is **445**

it is used by Microsoft server operating systems for client/server access and file and printer sharing.

**37**.Calender Access Protocol (CAP)

Port number is **1026**

It is used by Novell GroupWise for its calendar access protocol and also used by windows task scheduler.

**38.** Layer Two Tunneling Protocol.(L2TP)

Port number is **1701**

It is used to connect two private business network together over an internet connection to create a virtual network.

**39**.Point To Point Tunneling Protocol (PPTP)

Port number is **1732**

A tunneling and encryption standard is used to connect two private business network together over an internet connection to create a virtual network.

**40**.Remote Procedure Call (RPC)

Port number is **135**

It holds information regarding which ports and IP addresses the services are currently running

**2.write briefly about:**

**a.NIC card**

**b.Router**

**c.Switch**

**d.Hub**

**e.Modern**

**f.Access Point**

**g.Firewall**

**a.NIC Card:-**

A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so it can connect to a network. Modern NICs provide functionality to computers, such as support for [I/O](https://www.techtarget.com/whatis/definition/input-output-I-O) interrupt, direct memory access ([DMA](https://www.techtarget.com/whatis/definition/Direct-Memory-Access-DMA)) interfaces, data transmission, network traffic engineering and partitioning.

A NIC provides a computer with a dedicated, full-time connection to a network. It implements the [physical layer](https://www.techtarget.com/searchnetworking/definition/physical-layer) circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network.

The NIC uses the [OSI model](https://www.techtarget.com/searchnetworking/definition/OSI) to send signals at the physical layer, transmit data packets at the network layer and operate as an interface at the [TCP/IP](https://www.techtarget.com/searchnetworking/definition/TCP-IP) layer.

**Types of network interface cards**

While the standard NIC is a plastic circuit board that slides into a computer to connect with the motherboard, there are multiple ways this connection can occur:

* **Wireless.** These are NICs that use an antenna to provide wireless reception through [radio frequency](https://www.techtarget.com/searchnetworking/definition/radio-frequency) waves. Wireless NICs are designed for Wi-Fi connections.
* **Wired.** These are NICs that have input jacks made for cables. The most popular wired LAN technology is Ethernet.
* **USB.** These are NICs that provide network connections through a device plugged into the USB port.
* **Fiber optics.** These are expensive and more complex NICs that are used as a high-speed support system for network traffic handling on server computers. This support could also be accomplished by combining multiple NICs.

**Components of network interface cards**

Network interface card components include the following:

* **Speed.** All NICs have a speed rating in terms of Mbps that suggests the general performance of the card when implemented in a computer network with ample [bandwidth](https://www.techtarget.com/searchnetworking/definition/bandwidth). If the bandwidth is lower than the NIC or multiple computers are connected with the same controller, the labeled speed will be slowed down. The average Ethernet NICs come in 10 Mbps, 100 Mbps, 1000 Mbps and 1 Gbps varieties.
* **Driver.** This is the required software that passes data between the computer's operating system ([OS](https://www.techtarget.com/whatis/definition/operating-system-OS)) and the NIC. When a NIC is installed on a computer, the corresponding driver software is also downloaded. Drivers must stay updated and uncorrupted to ensure optimal performance from the NIC.
* **MAC address.** Unique, unchangeable [MAC addresses](https://www.techtarget.com/searchnetworking/definition/MAC-address), also known as physical network addresses, are assigned to NICs. These are used to deliver Ethernet packets to the computer.
* **Connectivity LED.** Most NICs have an LED indicator integrated into the connector to notify the user of when the network is connected and data is being transmitted.
* **Router.** A router is also sometimes needed to enable communication between a computer and other devices. In this case, the NIC connects to the router which is connected to the internet.

**b.Router:-**

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to their intended [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between [LANs (local area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) and [WANs (wide area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

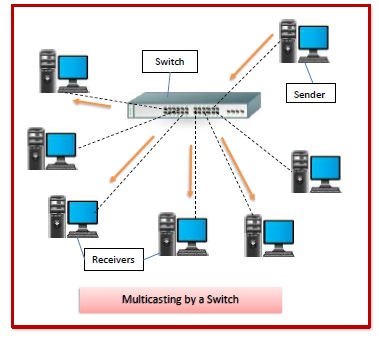
A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches\*.

\**A*[*network switch*](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/)*forwards data packets between groups of devices in the same network, whereas a router forwards data between different networks.*

**c.Switch:-**

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

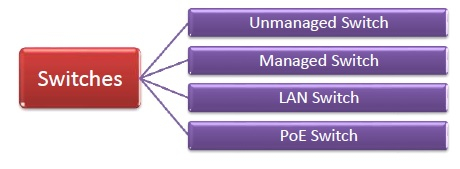


## **Features of Switches**

* A switch operates in the layer 2, i.e. data link layer of the OSI model.
* It is an intelligent network device that can be conceived as a multiport network bridge.
* It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
* It uses packet switching technique to receive and forward data packets from the source to the destination device.
* It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
* Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
* Switches are active devices, equipped with network software and network management capabilities.
* Switches can perform some error checking before forwarding data to the destined port.
* The number of ports is higher – 24/48.

## **Types of Switches**

There are variety of switches that can be broadly categorised into 4 types −

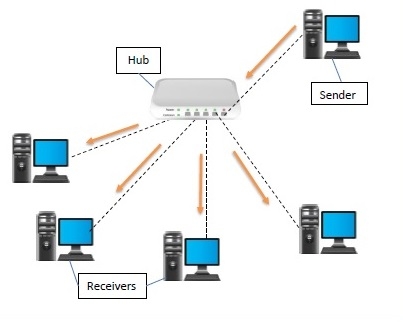


* **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
* **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
* **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
* **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

**d.Hub:-**

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.



**e.Moderm:-**

Modem stands for Modulator and Demodulator. It is a device that modulates signals to encode digital information for transmission and demodulates signals to decode the transmitted information.

A modem transmits data in bits per second (bps).

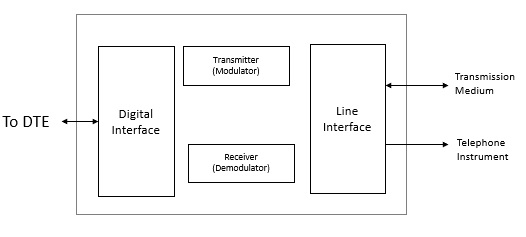
It is necessary for communication between digital devices and Analog devices.

Modem is necessary because it acts as a translator between the devices and rapidly transmits the information.

It converts the digital signal to Analog and vice versa to communicate between devices.

It encodes the signal and decodes at the other end and vice versa between the devices.

Building blocks of modem are shown in the diagram below −



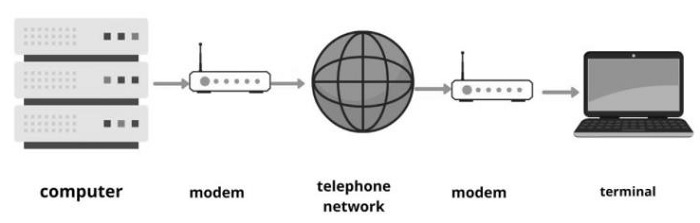
## **Types of Modems**

The different types of modems used to access the internet at home are as follows −

### Telephone modem

A computer is connected through telephone lines to access the network of other computers. It is cheaper when compared to other modems because it does not have any installation cost and also the monthly fee of a telephone modem is low. It can be used in any house if a telephone network is provided.

Given below is the diagram of telephone modem −



### Digital subscriber Line

It provides high speed internet connection through telephone lines. It is expensive when compared to a telephone modem. The DSL is also connected with phone lines similar to telephone modem, but the difference is in DSL voice communication and internet service is used simultaneously whereas in telephone modem it is not provided.

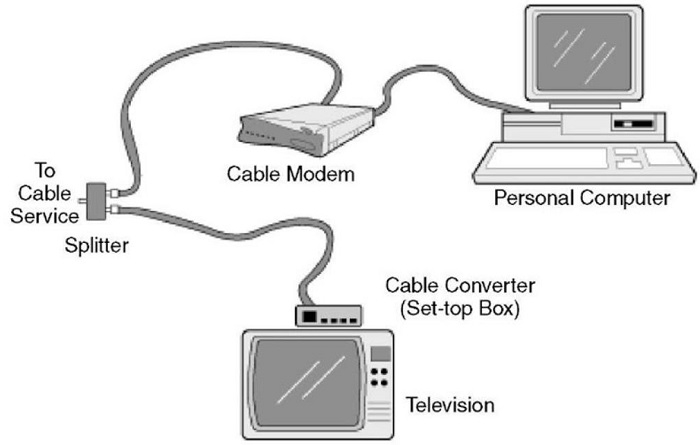
Given below is the diagram of digital subscriber line (DSL) −



### Cable modem

Cable Modem is a device that allows high-speed data access via a cable TV (CATV) network. Most cable modems are currently external devices that connect to the PC through a standard 10 BASE-T Ethernet card and twisted-pair wiring.

Given below is the diagram of cable modem −



### Satellite modem

It is a device that provides internet connection through satellite dishes. It transfers the input bits to output radio signals and then executes vice versa. It is costlier when compared to all other modems but provides better reliability to the internet network.



**f.Access Point:-**

**Definition(s):**

  A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization’s enterprise wired network.  
**g.Firewall:-**

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Firewalls have existed since the late 1980’s and started out as packet filters, which were networks set up to examine packets, or bytes, transferred between computers. Though packet filtering firewalls are still in use today, firewalls have come a long way as technology has developed throughout the decades.

* **Gen 1 Virus**
  + Generation 1, Late 1980’s, virus attacks on stand-alone PC’s affected all businesses and drove anti-virus products.
* **Gen 2 Networks**
  + Generation 2, Mid 1990’s, attacks from the internet affected all business and drove creation of the firewall.
* **Gen 3 Applications**
  + Generation 3, Early 2000’s, exploiting vulnerabilities in applications which affected most businesses and drove Intrusion Prevention Systems Products (IPS).
* **Gen 4 Payload**
  + Generation 4, Approx. 2010, rise of targeted, unknown, evasive, polymorphic attacks which affected most businesses and drove anti-bot and sandboxing products.
* **Gen 5 Mega**
  + Generation 5, Approx. 2017, large scale, multi-vector, mega attacks using advance attack tools and is driving advance threat prevention solutions.

Back in 1993, Check Point CEO Gil Shwed introduced the first stateful inspection firewall, FireWall-1. Fast forward twenty-seven years, and a firewall is still an organization’s first line of defense against cyber attacks. Today’s firewalls, including [Next Generation Firewalls and Network Firewalls](https://www.checkpoint.com/definitions/what-is-next-generation-firewall-ngfw/) support a wide variety of functions and capabilities with built-in features, including:

* [Network Threat Prevention](https://www.checkpoint.com/products/advanced-network-threat-prevention/)
* [Application and Identity-Based Control](https://www.checkpoint.com/products/application-control/)
* [Hybrid Cloud Support](https://www.checkpoint.com/products/iaas-public-cloud-security/)
* [Scalable Performance](https://www.checkpoint.com/products/maestro-hyperscale-network-security/)

## **Types of Firewalls**

### ****Packet filtering****

A small amount of data is analyzed and distributed according to the filter’s standards.

### ****Proxy service****

Network security system that protects while filtering messages at the application layer.

### ****Stateful inspection****

Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

### ****Next Generation Firewall (NGFW)****

Deep packet inspection Firewall with application-level inspection.

## **What Firewalls Do?**

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

## **Why Do We Need Firewalls?**

Firewalls, especially [Next Generation Firewalls](https://www.checkpoint.com/products/next-generation-firewall/), focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you’re setting up your network with specific policies to allow or block incoming and outgoing traffic.

**3.write about Cyber kill chain Methodology.**

## Introduction

Cyber threats are frequently [changing](https://www.sentinelone.com/blog/the-changing-nature-of-the-ransomware-menace-today/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE), as are defense and prevention tactics. Today, an increasing number of organizations implement a layered approach to cybersecurity that encompasses administrative, technical and physical security controls.

However, even with the most advanced technical safeguards in place, some organizations inevitably fall victim to successful cyberattacks.

Although preventing cyberattacks can feel like a challenging battle, there is a cybersecurity model that can help: **the cyber kill chain.**

This article covers the steps of the cyber kill chain, how it works, and how it helps security teams prevent and detect cyberattacks.

## What is the Cyber Kill Chain in Cybersecurity?

Derived from a military model by [Lockheed Martin](https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf) in 2011, the cyber kill chain is a step-by-step approach to understanding a cyberattack with the goal of identifying and stopping malicious activity.

Also called the cyber attack lifecycle, the cyber kill chain can help organizations gain a deeper understanding of the events leading up to a cyberattack and the points at which they can prevent, detect, or intercept attackers in the future.

Although the original cyber kill chain model contained only seven steps, cybersecurity experts expanded the kill chain to include eight phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objective, and monetization.

Most of the time, organizations use the cyber kill chain to defend against the most sophisticated cyberattacks, including [ransomware](https://www.sentinelone.com/cybersecurity-101/ransomware/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE), security breaches, and [advanced persistent threats](https://www.sentinelone.com/cybersecurity-101/advanced-persistent-threat-apt/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE) (APTs).

### How the Cyber Kill Chain Works

The term “cyber kill chain” was adapted from the military and describes the structure of an attack (either offensive or defensive) broken into a pattern of identifiable stages, including identifying a target, dispatch, decision, order, and destruction of the target.

In cybersecurity, the cyber kill chain is a model outlining the various phases of common cyberattacks. Using the cyber kill chain, organizations can trace the stages of a cyberattack to better anticipate and prevent against cyber threats in the future.

Each stage of the cyber kill chain is related to a specific type of activity in a cyberattack (regardless of whether it’s an internal or external attack).

### How Does the Cyber Kill Chain Protect Against Attacks?

The cyber kill chain is not a security system: it’s a framework that enables security teams to anticipate how attackers will act so they can stop them as quickly as possible or intercept them if the attack has already transpired.

The cyber kill chain maps out the exact path a typical attacker will take so cybersecurity teams can recognize the starting point of common cyberattacks. Cyber kill chain simulations allow security teams to gain firsthand experience in dealing with a cyber threat, and evaluating simulation responses can help organizations identify and remediate any security gaps that may exist.

It can guide strategy, training, and tool selection by revealing which parts of a security strategy may or may not need updating, such as employee training, [endpoint security software](https://www.sentinelone.com/cybersecurity-101/endpoint-security/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE), or VPNs.

## Cyber Kill Chain Steps

Computer scientists at Lockheed Martin may have been the first to take this concept and apply it to information security, but the cyber kill chain continues to evolve with the changing nature of cyber threats.At the core of the cyber kill chain is the notion that cyberattacks often occur in phases and they can be disrupted through controls established at each phase.

### Reconnaissance

During what some call the observation phase, the reconnaissance phase is when attackers begin to identify targets and make [a plan of action](https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack). This stage often includes activities such as researching potential targets, determining vulnerabilities, and exploring potential entry points. The more information an attacker can glean during this phase, the more sophisticated and successful the attack can be.

### Weaponization

At this stage, attackers create the attack vector that will be used in the cyberattack. This could include remote access [malware](https://www.sentinelone.com/cybersecurity-101/malware-analysis/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE), ransomware, or a virus or worm that can exploit a vulnerability identified during the reconnaissance phase.

During the weaponization phase, attackers may also try to reduce the likelihood of being detected by any security solutions in place.

### Delivery

Attackers then deliver the attack vector through a medium like [phishing emails](https://www.sentinelone.com/cybersecurity-101/phishing-scams/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE) or by hacking into the target’s system or network. Regardless of the type of attack they intend to carry out, this is the stage at which the attacker officially launches an attack against a target.

### Exploitation

Next, the malicious code is executed within the target’s systems. By breaching the perimeter, attackers now have the opportunity to further exploit the target’s systems by installing tools, running scripts, or modifying security certificates. Common examples of exploitation attacks include scripting, dynamic data exchange, and local job scheduling.

### Installation

Immediately following the exploitation phase, the installation phase is when the attack vector is installed on the target’s systems. During the installation stage, attackers may also create back doors into the target’s systems or networks so they can continue to access them even if the original point of entry is identified and closed.

### Command and Control

During the command and control phase, attackers use the successfully installed attack vector to control devices or identities remotely within the target’s network. Threat actors may also [move laterally](https://www.sentinelone.com/cybersecurity-101/lateral-movement/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE) during the command and control phase in order to avoid detection and establish additional points of entry.

### Actions on Objective

In the final phase of Lockheed Martin’s cyber kill chain, attackers take the final steps to carry out their original objective, be it data theft, destruction, encryption or exfiltration.

The above steps are taken directly from Lockheed Martin’s cyber kill chain, which was originally developed in 2011. Since then, cybersecurity experts have expanded on the seven phases to include an eighth: monetization.

### Monetization

During the monetization phase, attackers focus on deriving income from the successful attack, whether through some form of ransom or selling sensitive information on the dark web.

Since its inception, the cyber kill chain has evolved to better anticipate and understand modern cyber threats. It has also been adopted by data security organizations and professionals to help define the stages of an attack.

However, because of the constantly evolving nature of cyber threats, the future of the cyber kill chain is unknown. As [extended detection and response (XDR)](https://www.sentinelone.com/singularity-xdr/?gclid=CjwKCAjw6vyiBhB_EiwAQJRoptLkQkQg7Af2947xQ9-xcQK2a6mK9NMtBquiEc8gSCgE-diE_bsfzxoC-7oQAvD_BwE) becomes increasingly important for modern cybersecurity strategy, a new XDR framework or kill chain that leverages MITRE ATT&CK framework could be more beneficial to security teams.

## Critiques of the Cyber Kill Chain

Current critiques can be bucketed into two main categories: perimeter security and attack vulnerabilities.

### Perimeter Security

One of the biggest critiques of Lockheed’s Cyber Kill Chain model is the fact that the first two phases of an attack (reconnaissance and weaponization) often occur outside the target network. This can make it difficult for organizations to understand or defend against any actions occurring during these phases.

### Attack Vulnerabilities

Some critics believe that the methodology also reinforces traditional perimeter-based and malware-prevention-based defensive strategies, which aren’t enough in today’s cybersecurity climate.

Additionally, some critics believe the traditional cyber kill chain isn’t a suitable model for simulating insider threats. This potentially puts organizations at greater risk given the likelihood of successful attacks that breach a target’s internal network perimeter.

Although many have adopted the cyber kill chain, acceptance is far from universal and there are many critics that are quick to point to what they believe are fundamental flaws. Fortunately, there are a number of other cybersecurity frameworks that may satisfy some of the cyber kill chain’s shortcomings.

**4.Hacker Classes-Types of Hackers.**

# **Types of Hackers**

Hackers can be classified into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

## **Black Hat Hacker**



Black-hat Hackers are also known as an **Unethical Hacker or a Security Cracker**. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

## **White Hat Hacker**



White hat Hackers are also known as **Ethical Hackers or a Penetration Tester**. White hat hackers are the good guys of the hacker world.\

These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

## **Gray Hat Hacker**



Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.