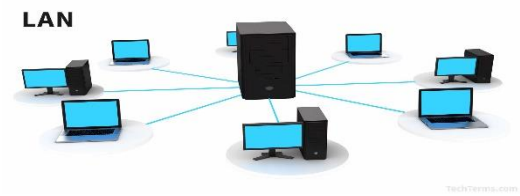
Cyber Security - SOC Analyst Notes

Abbreviation's

LAN (Local Area Network)



It is a computer network, it will connect all the devices with in a building or with in location
It is basically a network connecting all the devices, systems, servers or any data bases together in a single building that may be hospital, school, college, Organization etc all the system we connect together that is called LAN here in internet is not mandatory we can use but not required

We can keep internet also in the organization level ex in school, hospital, in that scenior it is single location

LAN is a computer network it will connect all the devices together computer means any device that device may be load balancer, router, switch, printer, work station, server, data base and so on physical single layer connection

Key word; Single Building, Single Office, Single Organization

WAN (Wide Area Network)

Compulsory Internet is Required & Router is also required Here also all the computers are connected through Geo Graphically not a single location through geo graphically or through office buildings or may be two different countries or two different cities or two different villages & so on several LANs is called WANs. In WAN you can access two different Public / Internet using LAN

It is basically complete geo graphical location wise Ex; If your office Is outside the country if you wants to connect with those geo graphical locations together via internet which means via public network here we are connecting with public network via internet here internet and router is mandatory

Key word; Geo Graphical location , Internet or Public Key word

MAN (Metro Politian Area Network)

It is computer network , it will connect all the devices geographically or across the country or cities via or through internet or public network
It is nothing but Metro Politian cities basically completes the Geo Graphical location but within the country Here Internet & Public Network is Mandatory

DC (Data Centre)

It means it is room where we can keep all of our networking related devices not only just Networking devices total end to end servers all the physical servers, Routers. All the switches like all the networking devices like load balances, fire walls, proxy servers that is called Data centre

It is expensive to maintain so that's the reason now a days people are shifting to the cloud environment

Data centre always required either rack mounted or wall mounted

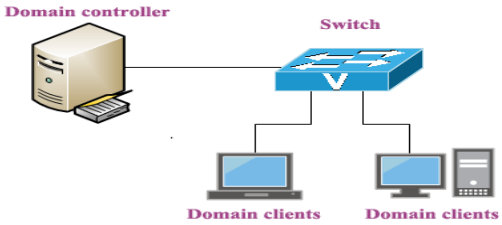
Rack Mounted

One rack will be there in that rack we have to keep our servers and also networking related devices it is a single dedicated room always cooling should require reason is all the servers & devices will disseat lot of heat because of this reason they will put on lot of Air condition in Data Centre lot of plantations will be surrounded near to Data Centre

Wall Mounted

DC (Domain Controller)

It is nothing but Centralized authentication and authorization server



Ex ; If you want to login in your laptop normally we use user name & password in the organization level company will provide the laptop to us they put some under domain once your entering the user name and password so now domain controller will validate whether your authorized user are not

AD (Active Directory)

It is a windows server basically here we maintain all the users information under the domain controller ex Any organization domain depends on the organization

even we have the Active directories groups ex devops team we are all under devops directory, HR team in one group etc., all these groups are configured in AD it provides user information, systems information, server info and so on that is called AD on top of this Domain control will be run it kind of service

EDR (End point Detection Response)

It is next generation Anti-Virus it will block malware kind of activities

AV (Anti-Virus)

Virus Is an Attack Anti-virus being a solution

AM (Anti Malware)

Malware is one type of categories of attack ex; fruit is a category Apple is one in that in a similar way malware is a attack under that we have attacks. Malware is an attack and anti-malware is an solution

HIDS (Host Intrusion Detection system)

Intrusion means dangerous, harmful, meliaceous anything this intrusion done by the attacker or hacker

Detection means Detecting it is detecting capability

Host end user security nothing but employee laptop in the employee laptop what ever harmful and meliaceous activities are happening this HIDS will detect

HIDS is only detection system only but It will not block

EX; Laptop

HIPS (Host Intrusion Prevention System)

Here whenever any Meliaceous kind of activity is happening It will detect and also it will block mostly in the we use HIPS in the organization

Malware

It is nothing but meliaceous software which is developed by the hacker if we don't have such detection meliaceous software gets compromise

NGFW (Next generation firewall)

Current generations firewalls we called had Next generation firewall . it will blocks against network layer as per OSI

WAF (Web application firewall)

It block application layer because day by day internet usage is increasing max attackers are concentrating on attacker level if we want to mitigate any attacks are coming we use WAF it will dedicatedly block application layers

NIDS (Net work Intrusion Detection system)

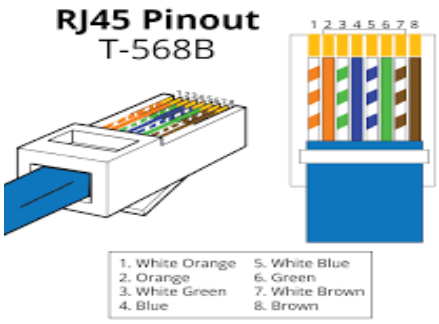
This is for network level whatever incoming traffic and outgoing traffic is coming in the organization level traffic in the sense messages basically whenever you accessing the application sending emails that is in the form of traffic

It will detect only Abnormal activity

NIPS (Network intrusion prevention system)

It will detect and block the harmful activity in the network level

RJ45 Cable or Ethernet Cable



This RJ45 cable will support up to 1G

Optical Fibre

This will support up to 1T to connect with optical fibres we need Cisco cable this is high and speed compare to RJ45 and this optical fibre only in Data centre connects with one device to the another device for interfaces

ex; Above cisco router is one of the device through this we do the interfaces whatever RJ45 & Optical fibre physically we connect here

TTP(Tactics, Techniques and procedures)

Attacker will use some Tactics, Techniques and procedures for example if I compromise one of the server or if compromise of the laptop or if I want to compromise any application so on in that scenario so here attacker will use TTP concept like what to choose , how to choose and go for the selection for the target and use some mails to compromise the system like fishing emails are any other option as well that is called TTP

SIEM (Security Information & Event Management)

This is our main tool

It is instant investigation or It is instant forensic investigation

Log collection or log analysis or log monitoring or Log processing or security alerts

In this tool only Alerts will come from different attacks as a soc we go into the SIEM tool we investigate what kind of instance we received then finally we take instant investigation whether is it really got compromise and what kind of eradication indication and also something is not compromise so how to close the instance for that we use SIEM tool

It is basically log collection or log analysis or log monitoring or security alerts

LOG ; Any computer recorded activity ex; what ever activity that employees are doing in there laptop in the back end some logs are generated are we can called as actions those logs only we send to the SIEM tool and we create certain rules and policies for such type of attacks finally whenever attacker is trying to do attack it will generate the alerts in the SIEM tool as early we do the investigation that is meant by log

SOC (Security Operations Centre)

It is room or site where security analysts will sit and monitor and take the appropriate security incident investigations for 24*7

This is our team's name it means it is a room where people will sit & monitor 24/7 and according to the alert's incidences are attacks will do instant investigation

SOC has another name also

CSIRT (Cyber security Instance Team)

CERT (Computer Emergency Response Team)

SIRT (Security Instance Response Team)

DLP (Data loss or Data leak prevention)

DLP will prevent the activities that employee doing with actions with company Asset or even external attacker

Attacker

Attacker is the person who do hacking or attacks the reason for attacking to steal the money or any kind of confidential data

For Attacker another name is Intruder or Hacker

FIM (File Integrity Monitoring)

Most of the malware kind of attacks like virus etc so attacker will do the encrypting of the files or may be delete the file are update the files so on ex in our laptop some attacker done with compromise blackmailing us for money if not delete the imp data from the laptop however deleting the file and updating the file is also FIM adding additional info is also FIM and also so on

DNS (Domain Name server)

A DNS server is a computer with a database containing the public IP addresses associated with the names of the websites an IP address brings a user to. DNS acts like a phonebook for the internet. Whenever people type domain names, like Yahoo.com, into the address bar of web browsers, the DNS finds the right IP address. The site's IP address is what directs the device to go to the correct place to access the site's data.

Once the DNS server finds the correct IP address, browsers take the address and use it to send data to content delivery network (CDN) edge servers or origin servers. Once this is done, the information on the website can be accessed by the user. The DNS server starts the process by finding the corresponding IP address for a website's uniform resource locator (URL)

It will convert domain name into IP address so it will validate ex; Google.com we do search then it will validate the back end with IP address it shows the frontend of validation

DHCP (Dynamic Host configuration protocol)

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired.

It will allow the IP address automatically here no need to do any manual every system have the IP Address it might be anything like computer, mobile, tab etc . it is use one of the process called Dora this allocation is only for the employees not for servers, databases, tools. It is dedicated to employee laptop, MacBook , work station or desktop for all the servers , databases, tools will allocate the fixed IP

IP (Internet Protocol)

numerical label or number assigned to each and every system
It is basically a Numerical Number assigned to each and every system it is only Numbers not any characters a dedicated label number which is assigned it is called IP Address. This IP address is not fix it is logical address it Is vary in organization we use PVT IP address

MAC (Media Access Control)

A Media Access Control address (MAC address) is a hardware identifier that uniquely identifies each device on a network. Primarily, the manufacturer assigns it. They are often found on a device's network interface controller (NIC) card. A MAC address can also be referred to as a burned-in address, Ethernet hardware address, hardware address, or physical address

Every Nic card Network Interface Card has a one physical address and this physical address is fixed one which will not change it is fix and unique one and every ethernet has one physical address which we called as MAC Address

ARP (Address Resolution protocol)

It converts layer 3 Network IP address to layer 2 Data Link MAC address which means it convert IP address to MAC address it is called ARP

RARP (Reverse Address Resolution Protocol)

It converts layer 2 Data link MAC address to layer 3 Network IP address which means it convert MAC address to IP Address it is called RARP

FTP (File Transfer Protocol)

It will be using for the file transferring ex; Copying the file from Laptop to the pen drive even vice versa pen drive to laptop anything transfer from laptop to some other machine, server, data base anything in this scenario we need to use FTP

SFTP (Secure File Transfer protocol)

Here we securely use but in the FTP its an plan text if we are using SFTP with the attacker point of view it is very difficult to exploit always we have to use SFTP

HTTP (Hyper Text Transfer Protocol)

It is plane text in the web browser level here we can expect more chance to get hack HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message. ex ; broken authentication access, broken authentication control, session hijacking

HTTPS (Hyper Text Transfer protocol security)

In the web browser we can identify with the lock symbol which means secure

SMTP (Simple Mail transfer protocol)

This not only used by security team it is used by all the teams ex; windows server team, Linux server team , devops team or TechOps team or machine learning team etc any team can consider it integrate with SMTP Server the reason for because the RAM utilization is very high whenever any abnormal activities are happening so they get alert notification. In the organization level IT Department level we use SMTP Server to get the email notification to send the emails and to receive the emails we use SMTP and for SMTP we have another names also like exchange server, email server , unified communication server , office 360 or outlook and so on

NFS (Network File System or Sharing)

This we will be used for the file sharing purpose which is FTP & SFTP we are using NFS is also same for sharing the file we use NFS

SSH (Secure Shell)

To login into unique operating system if you want login into unique operating system under unique operating system it is like kind of flavour or category under that particular category we have lot of operating system are there EX; RHL red hat

Linux , dockers & containers , cento etc those comes under the unique operating system how login through SSH protocol

SSL (Secure socket layer)

SSL stands for Secure Sockets Layer and it helps in creating encrypted connection between a web browser & web server, It ensure data privacy by protecting the information in online transactions which helps in maintain cyber security, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, and also preventing the criminals from reading and modifying any information transferred, including potential personal details. The two systems that create encryption link between a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).TLS (Transport Layer Security)

An SSL certificate is installed on the server side but there are cues on the browser. Which can tell users that they are protected by SSL.

Firstly, if SSL is present on the site, user will see HTTPS;// at the start of the web address. Depending on what level of validation a certificate is given to the business , a secure connection may be indicated by the presence of padlock icon or a green address bar link

TLS (Transport Layer Security)

TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet. It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established. However, it can and indeed should also be used for other applications such as e-mail, file transfers, video/audioconferencing, instant messaging and voice-over-IP, as well as Internet services such as DNS and NTP.

RDP (Remote Desktop Protocol 3389)

From your system if you want to login in another system or else if you want login into any windows server, we use RDP Remote desktop is the ability to connect with and use a faraway desktop computer from a separate computer. Remote desktop users can access their desktop, open and edit files, and use applications as if they were actually sitting at their desktop computer. Employees often use remote desktop software to access their work computers when they are traveling or working from home.

SNMP (Simple Network Management Protocol 161)

It will manage all the devices if we are enabling this SNMP in router are switch the name itself shows the management which means managing all the devices once, we

are enabling the SNMP protocol we can identify what kind of network devices are there.

Syslog (system login)

Syslog has been around for a number of decades and provides a protocol used for transporting event messages between computer systems and software applications. The Syslog protocol utilizes a layered architecture, which allows the use of any number of transport protocols for transmission of Syslog messages. It also provides a message format that allows vendor-specific extensions to be provided in a structured way.

Authentication

Providing the credentials (Username and password) and login into the system (Identify of the person or who am i) Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In doing this, authentication assures secure systems, secure processes and enterprise information security.

Authorization

To grant or permission or access to the system (Servers will validate who are you) Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features. This is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.

Most web security systems are based on a two-step process. The first step is authentication, which ensures about the user identity and the second stage is authorization, which allows the user to access the various resources based on the user's identity. Modern operating systems depend on effectively designed authorization processes to facilitate application deployment and management. Key factors contain user type, number and credentials, requiring verification and related actions and roles.

CIA Traid or AIC Traid (Confidentiality, Integrity, Availability)

The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. Mainly those are used for finding vulnerabilities and methods for creating solutions. This a model that is designed to guide policies for information security

The confidentiality, integrity, and availability of information is crucial to the operation of a business, and the CIA triad segments these three ideas into separate focal points. This differentiation is helpful because it helps guide security teams as they pinpoint the different ways in which they can address each concern. Ideally, when all three standards have been met, the security profile of the organization is stronger and better equipped to handle threat incidents.

Whatever the security can consider in the organization level that may could security , application security , end point security , network security, server security, infra structure security , data base security, so on every security evolves only these 3 things

Confidentiality; Only authorised users should access the data or content (Privacy of the data) The information should be accessible and readable only to authorised personnel. It should not be accessible by unauthorised personnel. The information should be strongly encrypted just in case someone uses hacking to access the data. So that even if the data is accessed. It is not readable or understandable

EX; Whatever on going projects that are going on, Company policies , Patents , Copy rights, Trade marks, Financial reserves, whatever back end development & PIA data and so on

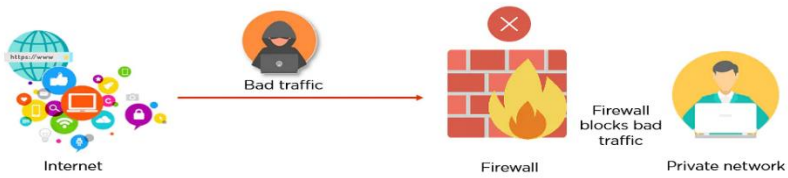
Integrity; Trustworthy of the data or secrecy of the data (Only authorised or legitimate users can add or delete or modify the data) Making sure the data has not been modified by an unauthorised entity. Integrity ensure that data is not corrupted or modified by unauthorised personal. If any authorised individual/System is trying to modify the data and the modification wasn't successful, Then the data should be reversed back and should not be corrupted

EX; Any files modification of the data unauthorised person should not change

Availability; all the applications or services or systems should be available to end user . (99.99999) The data should be available to the user whenever the user require it. Maintaing of hardware, upgrading regularly. Data backups and Recovery. Network bottle neck should be taken care of

EX; Application servers , Server should not be outage & it should not be crashed in the similar even Application server also whatever internal or external applications should be outage because Availability issues will not come

FW (Fire Wall)



It will monitor inbound traffic and outbound traffic and based on the actions defined either it will allow the traffic or deny the traffic
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. 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.

WAF(Web application firewall)

A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defence (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defence against a range of attack vectors.
It will monitor web or application (Application layer) traffic and whenever any malicious attacks will happens WAF will block or prevent

IDS (intrusion detection system)

Intrusion detection system it is a network security solution that detects the malicious traffic based on the signatures it works in Outline Mode. IDS systems compare the current network activity to a known threat data base (which is Signature Network) to detects the several kinds of behaviour like security policy violation, Malware, and port scanner, So IDS is designed to detect a potential incident, To generate an alert, Unwanted attempts at accessing and do nothing to prevent the incident from occurring.
IDS is two types

- Network Based IDS
- Host Based IDS

IDS Signature Syntax

It had 2 sections

Rule Header – It contains information like Rule action , Rule protocol , source Ip address and source port number. The direction destination Ip address and Destination port number

Rule Option – It contains the message which the alert that has to triggered SID (Signature ID), Revision that stand for what version of this rule is and if it is ever modified. And there are other various options with in the rule options that will help that will detecting the malicious activities

Type of Attacks identified by the IDS

Reconnaissance Attacks, DoS, Access Attack

IPS (Intrusion prevention system)

IPS solution that monitors a network or system activities for malicious behaviour in real time it will block it works in the Inline mode, on the other hand, it is designed to take an action to block anything that it believes to be a threat to the protected system. As malware attacks become faster and more sophisticated, this is a useful capability because it limits the potential damage than an attack can cause. An IPS is ideal for environments where any intrusion could cause significant damage, such as databases containing sensitive
Ids it will monitor abnormal or malicious or suspicious traffic and it will alert or detect and also block or prevent

Where do you place IPS?

A An IPS usually placed after the firewall. Firewall does the heavy lifting of blocking all the unwanted traffic based on TCP/IP header. And if the traffic that is allowed, IPS will do deep packet inspection. Because of this IPS needs more processing power than a firewall.

If IPS placed first, it will unnecessarily do deep packet inspection on all the traffic, while a good amount of traffic could have been blocked just by inspecting TCP/IP header with a packet filtering device like firewall

GUI (Graphical User Interface)

It is user friendly which means it is not complex to operate

CMI (Command Line Interface)

It is backend process how we to login into respective server, Data base or tools that is called Command line so command to execute something or to configure something , or to generate something

OWASP TOP 10 (The open web application security project)

It is an organization or framework will conduct some survey and they will release TOP 10 application layer attacks and mitigation steps. It is a kind of intuition they do conduct the survey's with different organizations to find out the Attacks they started from 2010,2013,2017 & 2021 and finally they make out the summary through Application layer after compilation of effective survey
EX; injection flaw attack , Cross site scripting attacks , Broken authentication.
As per 2021 Attack

Malware

As software designed to interfere with a computer's normal functioning, malware is a blanket term for viruses, trojans, and other destructive computer programs threat actors use to infect systems and networks in order to gain access to sensitive information.
Under malware have the certain category like
Virus , Worm, Ransome ware , Botnet , backdoor , Logic bomb

Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behaviour an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems. Though varied in type and capabilities, malware usually has one of the following objectives:

- Provide remote control for an attacker to use an infected machine.
- Send spam from the infected machine to unsuspecting targets.
- Investigate the infected user's local network.
- Steal sensitive data

TCP (Transmission control protocol)

It's a connection-oriented protocol it is a communications standard that enables application programs and computing devices to exchange messages over a network. It is mainly designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

It is a set of communication protocols that are used to interconnect network devices on the internet. This protocol defines the how data should be transmitted over the internet by providing end to end communication
TCP is one of the basic standards that define the rules of the internet and is included within the standards defined by the Internet Engineering Task Force (IETF). It is one of the most commonly used protocols within digital network communications and ensures end-to-end data delivery.

UDP (User Datagram protocol)

It is connection less protocol is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not formally establishing a connection before data is transferred. This allows data to be transferred very quickly, but it can also cause packets to become lost in transit

Agent

It is nothing but a peace of software This one will be provided vendor this peace of software we should install each and every end user system it will prevent respective malware kind of categories it will communicate to the sever and it will get block

Whitelisted

Which mean Allow where IP whitelisting A whitelist is a security list that provides access to only pre-approved programs, IPs, or email addresses. Whatever is on the "list" gets access to system resources, whereas the rest are denied access. Any program wanting to run on the network is matched against the "whitelist" and is allowed access only if a match is found.

Whitelists can be customized according to the unique needs of the employees and the network administrators. Best of all, they can be implemented for just about anything from emails, applications, IP addresses, and gaming servers.

Block listed

IP Address blocking is a security measure that prevents a connection between a specific or group of IP addresses and a mail, web or Internet server. This is usually done to block any undesirable sites and hosts from entering the server and causing harm to the network or individual computers.

IP blocking is usually used by companies to prevent intrusion, allow remote access as well as limit the kinds of websites that can be accessed by employees in order to keep productivity high. Schools and other academic institutions also use IP address blocking for protection against unauthorized access of confidential records and data and for enforcing censorship.

An IP address ban can effectively prevent a user from connecting to a certain web host. However, this is complicated when the user uses dynamic IP allocation since the IP cannot be pinpointed and a group or block of IP addresses has to be blocked, resulting in collateral damage as some ISPs share IP addresses for multiple users

IP Address blocking we should in Firewall
Mac Address in switch or firewall
Domain name DNS or fire wall
Website firewall or proxy
URL links firewall or proxy
In Mx Tool Website we can check whether it is malware category are not

NIC (Network Interface Card)

It will convert electrical signals into data signals whenever we are switching in the power
is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Abnormal/Malicious/suspicious

Something it will do dangerous or harmful or bad activity it is done by the attacker or hacker

Intruder or hacker or attacker

He is a criminal he compromises the system and he will gain unauthorised access or exposure of confidential data we have two reasons mainly money and data

Inbound traffic

The traffic is coming from extern or public to internal organization which means that inbound Traffic, in this context, is network traffic originating from an untrusted network towards a private host or enclave

Outbound Traffic

The traffic is going from internal to external or public

Net flow

It is combination of both Incoming + Out going that is net flow sum of the two traffics ex Inbound Traffic + Out bound Traffic net flow word has given by cisco company

Vulnerability

Vulnerability means weakness in a system or device that can be exploited to allow unauthorized access

It is the process of finding the flaws on the target, here the organization knows that their system/ network has flaws or weakness and want to find these flaws and prioritize the flaws of fixing

Which mean weakness in the system that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyberattack can run malicious code, install malware and even steal sensitive data.

Vulnerabilities can be exploited by a variety of methods including SQL injection, buffer overflows, cross-site scripting (XSS) and open-source exploit kits that look for known vulnerabilities and security weaknesses in web applications.

Many vulnerabilities impact popular software, placing the many customers using the software at a heightened risk of a data breach, or supply chain attack. Such zero-day exploits are registered by MITRE as a Common Vulnerability Exposure (CVE).

Ex: Security guard is not there Infront of the organization
AV agent is not installed in the end user machine
Firewall mis configuration rules

Reasons for Vulnerability

There are mainly 5 security reasons for Vulnerability

- Complexity
- Design Flaws
- User Data Input
- Poor System configuration
- & Unsecured connectivity

Threat

Threat is an Action that potentially compromise information security. A threat agent or threat source is someone who has the potential to cause a threat by taking advantage of a Vulnerability

So If vulnerability will be exploited by attacker, then it will come threat. threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.
Threat has three component

- Intent
- Opportunity
- Capably

Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks—

Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

Risk

Vulnerability * Threat is called Risk or likely hood * Impact likely hood we consider for 1 year base line whenever we are calculating the risk and base line is for one year Impact is nothing but consequences this consequence, we calculate in money orientated and people orientated

This risk will be calculated end point level, network level, application side , cloud side, server side, database side even physical security side as well finally will come with one figure this much of loss is existed and we will one register this register will called as risk register this one will done by IT security team
risk is the probability of exposure or loss resulting from a cyber-attack or data breach of organization.

Organizations are becoming more vulnerable to cyber threats due to the increasing reliance on computers, networks, programs, social media and data globally. Data breaches, a common cyber-attack, have massive negative business impact and often arise from insufficiently protected data.

MTTD Mean time to detection

Which Means Average time to detect the attack

MTTI (Mean time to identification)

MTTI is the length of time between a vulnerability being disclosed and attackers scanning for and identifying a vulnerable system in your network. In other words, how long it takes for an attacker to identify your vulnerable system and add it to their inventory of systems to target for exploitation

MTTR Mean time to recovery

It is the amount of time it takes an organization to neutralize an identified threat or failure within their network environment.
It measures the average time it takes to control and remediate a threat.

This is a process organizations use to identify and resolve threats to their network environment.
A threat is a malicious intrusion/infiltration into a system to steal information, negatively effect operations or damage hardware or software.

SLA (Service level Agreement)

It is always based on time It is contractual agreement between service based company and also client or customer and it Is also based on the Time and severity

it is the most effective way to ensure you conduct business in a way that satisfies the customer. For private security companies, the SLA helps provide better service and measure how successful those services are compared to other security companies.

Security Operations

OSI Layers (Open System Inter connection) 7 layers

Layer No.	Layer	Function	Devices	Protocols	PDU (Protocol Data Unit)
7	APPLICATION	• Interface between User and Computer. It provides services to the user. • Applications produce the data, which has to be transferred over the network.	-	HTTP, SMTP	Data
6	PRESENTATION	• The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. • Translation (ASCII to HEX) • Encoding/Decoding • Encryption/Decryption • Compression	-	JPEG, MPEG, TLS, SSL	Data
5	SESSION	• This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.	-	NetBIOS, NFS, RPC	Data
4	TRANSPORT	• It provides reliable message delivery from process to process • Ensures that messages are transmitted in the order in which they are sent and there is no duplication of data. • It is also responsible for error control and flow control	-	TCP/UDP	Segments
3	NETWORK	• Network layer works for the transmission of data from one host to the other located in different networks. • Takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.	Routers, Firewall, IPS	RIP, OSPF	Packets
2	DATA LINK	• The data link layer is responsible for the node to node delivery of the message. • It does Framing, error control, flow control etc. • Data Link Layer is divided into two sub layers : • Logical Link Control (LLC) • Media Access Control (MAC)	Switch	ARP	Frames
1	PHYSICAL	• It is responsible for the actual physical connection between the devices.	Hub, Bluetooth,	802.11	Bits

The Importance of OSI layers is. It is a communication channels it is provided by ISO international standard organization in 1984 which is nothing but of OSI layer concept It is a reference model for how application communicate over a network. The purpose of an OSI reference is to guide vendors and developers so the digital communication product and software programs can inter operate ex; If User A wants to communicate with User B or else if user wants to communicate with Application or if user wants to communicate with server or if user wants to communicate with website etc so

in that scenario user and application, user & server, user & website etc so on. in between what protocols has been used via nodes finally opposite peer or neighbour person, server, database or application is able to receive the data this entire process of the communication will be called as communication channel . which means set of rules & regulations and its guidelines like whenever we are accessing the Google, Facebook etc.,

If user wants to communicate to another user or server or database or application or website it will follow rules and regulations (Protocol) via node. Finally peer user or application or database or server will receive the communication. This process call it as Communication channel. This communication channel is provided ISO in 1984. This communication channel is nothing but OSI layer concepts

7 Application Layer

It provides an interface between the application and the network. It focuses on process-to-process communication and provides a communication face and

Layer Number	Layer name	Descirption or feature of the layer	PDU or data format	Attacks
7	Application layer	To provide or to get an information		owasp top 10
		Web browsing : HTTP (80) or HTTPS (443)		MITM
		Messaging : SMTP (25), SMB (445), POP3 (110), IMAP (143)		Session hijacking
		Virtual terminal: RDP (3389), SSH (22), Telnet (23)		
		File transfer : FTP (20 and 21), nfs, sftp (20 and 21)		
		DNS (53), SSL(443), TLS(443)	Data	

To provide or get an information its bi directional way This layer provides several ways for manipulating the data (information) which actually enables any type of user to access network with ease. This layer also makes a request to its bottom layer, which is presentation layer for receiving various types of information from it. The Application Layer interface directly interacts with application and provides common web application services. This layer is basically highest level of open system, which provides services directly for application process.

We have certain features like

Web browsing; HTTP (port no 80) or HTTPS (port no 443)

Messaging; SMTP (25), SMB- Sever message block. Dangerous we can get Ransome attacks (445) , POP3 – post office protocol (110), IMAP – Internet message access protocol (143) all these are messaging related protocols

Virtual Terminal; RDP – Remote Desktop protocol (3389) SSH(22),Telnet- If you want to login from one Linux server to another Linux server we use Telnet (23)

FTP – FTP (20 &21), NFS, SFTP (20 & 21)

DNS (53), SSL (443), TLS (443)

These are description & features of the protocol of Application layer

Data Format – In Application layer the Data Format is Data only

Attacks – Owasp Top 10 ,

MITM – Man in the middle ex; Attacker will on middle user & user , user & server , user & application, user & data base so on.

Session hijacking

6 Presentation Layer

6	Presentation	Converting one form of data into another form form of data		
		Ex: Encryption and Decyrption (SSL/ TLS)		
		Data acompression		
		Encoding / decoding		
		bHexa to decimal		
		decimal to binary		
		Encryption: The process of converting plain text data into encrypted dat using some of the alogorithm and also using key or password.	Data	Owasp top 10 Crptographic failures

It deals with presenting the data in a proper format and data structure instead of sending raw datagram or packets . It is converting one form of data into another form of data well Presentation Layer is the 6th layer in the Open System Interconnection (OSI) model. This layer is also known as Translation layer, as this layer serves as a data translator for the network. The data which this layer receives from the Application Layer is extracted and manipulated here as pert the required format to transmit over the network.

The main responsibility of this layer is to provide or define the data format and encryption. The presentation layer is also called as Syntax layer since it is responsible for maintaining the proper syntax of the data which it either receives or transmits to other layer(s).

We have certain features like

Ex: Encryption and Decryption (SSL/ TLS) (Interview question)

Encryption; It is a key or password in the computer terminology The process of converting plain text data into encrypted data using some of the algorithm nothing but process and also using key or password. which means what ever data that we are sending it should be encrypted. Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext.

In simpler terms, encryption takes readable data and alters it. so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on. Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext.

Decryption ; Opposite to encryption is decryption nothing but A reverse process of encryption is known as Decryption. It is a procedure of transforming Cipher Text into Plain Text. Cryptography needs the decryption technique at the receiver side to acquire the original message from non-readable message (Cipher Text).

Decryption operate by using the opposite conversion algorithm used to encode the information. The same key is needed to return the encrypted data to its initial state.

In decryption, the system extracts and transform the garbled information and change it to texts and images that are simply comprehensible not only by the reader but also by the system. Decryption can be accomplished manually or automatically. It can also be implemented with a set of keys or passwords.

Data compression; It means compressing of the data whenever the size is high, we have to compress by giving right click then it will reduce accordingly

Encoding/Decoding ; Converting one form of data into another form of data to find the solution

Decimal to binary

Portal – SSL/TLS
Data Format – In Presentation layer the Data Format is Data only
Attacks - Owasp top 10 , Cryptographic Fail

5 Session Layer ; For Managing the sessions we use session layers between two users or between two users & Application or between user & server. Controls connection between the sender & receiver. It is responsible for starting, ending and managing the session establishing. Maintaining and synchronization interaction between the sender and receiver

5	Session	Managing the sessions		Owasp Top 10
		Session management		Session hijacking
		Authentication- Identity of the user (Credentials)- Who am I?		
		Authorization- Grnating the permission or access- server- who are you?		
		SSL/TLS	Data	

The Session Layer is the 5th layer in the Open System Interconnection (OSI) model. This layer allows users on different machines to establish active communications sessions between them. It is responsible for establishing, maintaining, synchronizing, terminating sessions between end-user applications.

In Session Layer, streams of data are received and further marked, which is then resynchronized properly, so that the ends of the messages are not cut initially and further data loss is avoided. This layer basically establishes a connection between the session entities. This layer handles and manipulates data which it receives from the Session Layer as well as from the Presentation Layer.

ex; when you are making Audio call or video call one session got Audio & Video in a similar way when your sending an E-Mail may be attaching one of video or photo so here photo will take one session, Audio & Video will take one session

We have certain features like

Session Management; If you want to transfer the money through any HDFC net banking in that scenario 1st connection will be establish between user to the respective net banking whatever the transaction that you do may be home loan, Money transfer so it will form multiple session

Authentication; Authentication- Identity of the user (Credentials)- Who am I?

It mean user level it will check the identity of the user for that one we have ex; when we try to access the Gmail or Facebook, we give the authentication details that may be user name, password, mobile number etc.

authentication is nothing but credential of end user.
Authentication mainly deal identity of the person or user
Authentication which representants Who AM I (Which mean I authorized person are not to access)

Authorization; Authorization- Granting the permission or access- server- who are you?

It is not from End User level authorizations taken from the server level it will check ex; when you are typed incorrect user details in Facebook it will not reach to the server level It representants WHO ARE YOU

Portal – SSL/TLS
Data Format – In Session layer the Data Format is Data only
Attack – Owasp top 10, session hijacking

4 Transportation Layer

4	Transport	end to end communication with out any errors and data flow control	Segements and datagrams	Flooding category TCP flood, UDP flood, DOS, DDOS attacks
		Segmentation- converting larger chunk of the data into small chunk of the data		
		Error control		
		Dat flow control		
		Ex: TCP - Trnamission control procols- segments		
		UDP- User datagram protocol- Datagrams		
	iMP	TCP 3 WAY HANDSHAKE- syn, syn+ack and ack- connection estblishment		
		TCP 2 way handshake- FIN and ACK- connection closure or connection termination		
		TCP 5 way handshake- TCP 3 way + TCP 2 way- connection establish + connection closure		
		TCP and UDP differences		

Responsible for end to end communication over the network. It splits the data from the above layer and passes it to the network layer and then ensure that all the data has successfully reached at the receiver end

In general term transportation it is delivery it will do end to end communication without errors and data flow control It will form the reliable communication between two Host that may be 2 end user or end users to application or end user to the server so on it will do reliable data transfer without errors from source to destination that can be done by Transport layer

Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation and DE segmentation, and error control. Some protocols are state- and connection-oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred. Typical examples of layer 4 are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

We have certain features like

Error Control; whatever data sending from sender to receiver ex; How are you? So How 1 id, are 2 id, you 3rd the same sequence from segmentation will transfer the data without error

Data Flow; whatever data sending from sender to receiver it will be controlled flow of the data, control of the data will happen between the device's ex Laptop to mobile in laptop we have 10 gb were as in mobile we have the 5gb here laptop wants to send 4 GB data to mobile so mobile will communicate my capacity could be up to 5GB so here bidirectional control will happen between the two devices this entire process is doing by transport layer

Segmentation; It is nothing but converting of Bigger Data into smaller Data every segment will have a sequence number and port number the reason for port number we use for the communication purpose ex; How are you? How one segment, are one Segment, You One Segment for suppose if transport layer does not support error control User will get mismatch sequence like are you how in such a way (once its divided into smaller segments each and every segment has segment Id and also port number for communication purpose if you don't open the port communication will not happen this is the way how segmentation will happen

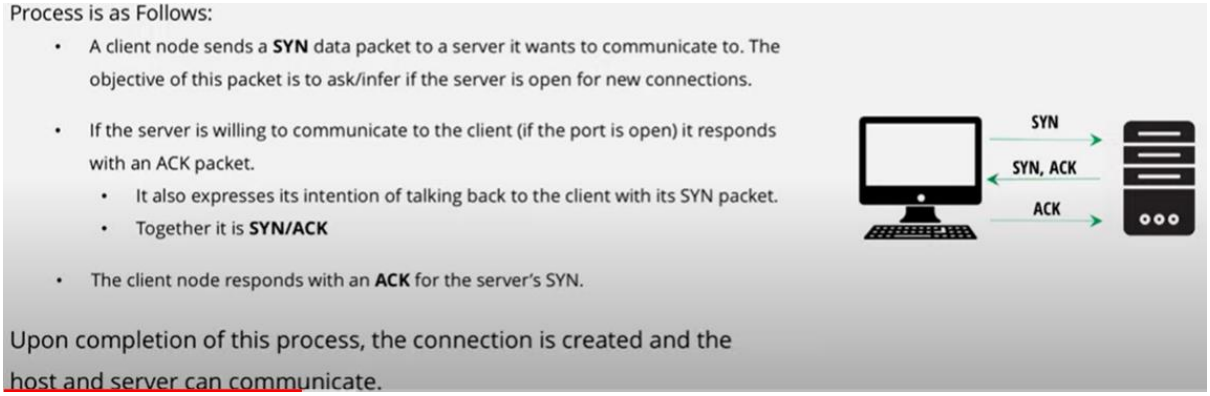
Data Format – In Transportation layer the Data Format is Data grams & segmentation
Attacks ; IP flooding (Flooding means millions of the request & billions of the request this will be done by the Attacker who will send some millions of the request to compromise the server), IP spoofing, IP sniffing, ICMP flooding, ARP spoofing

Protocols- TCP (Transmission control protocol) It is use for segments & UDP (User data diagram protocol) it uses for Data gram

TCP 3 Way hand shake – It is used for the connection establishment- syn, syn+ack and ack- connection establishment

It is a process which is used in a TCP/IP network to make a connection between the two host which means server and client. Before two system transfer the data they exchange syn/ACK packets to just confirm whether ports are open. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time. And also It allows you to transfer multiple TCP socket connections in both directions at the same time. So this entire process is happing in ways so this is called 3 way hand shake



- Syn uses to initiate and establish a connection
- ACK helps to confirm to the other side that it has received the SYN.
- SYN-ACK is a SYN message from local device and ACK of the earlier packet.
- FIN is used for terminating a connection.

Here a simple example of the three-way handshake

- Host Z begins the connection by sending the TCP SYN packet to its host destination. The packets contain a random sequence number (For example, 4521) that indicates the beginning of the sequence numbers for data that the Host Z should transmit.
- After that, the Server will receive the packet, and it responds with its sequence number. It's response also includes the acknowledgment number, that is Host Z's sequence number incremented with 1 (Here, it is 4522).
- Host Z responds to the Server by sending the acknowledgment number that is mostly server's sequence number that is incremented by 1.

After the data transmission process is over, TCP automatically terminates the connection between two separate endpoints.

TCP 2 - way hand shake This for connection Termination or connection closer The two-way handshake is a simple protocol to create a connection between two parties that want to communicate. In order to do that, this protocol uses Finish (FIN) and acknowledgment (ACK) messages. In between client & server connection or connection termination client will send finish request and server respond acknowledge that is called connection closer purpose

TCP 5- way Hand shake here we have to explain about the TCP 3 + 2 way hand shake If we are making sum then it is called TCP 5 way handshake which means connection establishment + Connect closer.

UDP – After TCP Authentication UDP works ex; like speaking on video calls whatever it is connection less protocol

Difference between TCP & UDP (Interview Question)

S.no	TCP	UDP
1	conenction oriented protocol	connection less protocol
2	Acknolwedgement or feed back will be there	There is no acknowledgement andf there is no feedback
3	It is slower	It is faster
4	TCP data format is segment	Datagrams
5	Ex: accessing any application (Youtube.com, facebook.com)	Ex: Whats audio call, skype video call

Ex;

- TCP – Web browsing, Download of file
- UDP – Zoom or blue jeans calls , DNS

3 Network layer

3	Network layer	It will provide path determination- Choosing the best or shortest route	IP Packets	IP flooding, IP spoofing, IP sniffing, ICMP flooding, ARP spoffing
		Logical andress - Ip address		
		Routing between two devices---Choosing the path or route		
		Ex: IP (internet protocol)		
		ICMP (internet control message protocol)		
		ARP- Address resolution protocol- It will convert layer 3 ip adress to Layer 2 MAC address		
		Ex: Router		
		Network layer will provide internet using router		
		VPN- virtual private network		
		If we want to connect two cities networks, two conutries networks, two state networks or two buildings, router and internet is mandatory		

Responsible for packet forwarding and providing routing paths for network communication. Here data grams are transferred from one to another. The functions of the layer are routing and logical address

Using network layer only we will get the internet ex; Router this router only will forward from source to destination between the two devices Mainly for the Routine purpose Any packet is sending from sender to receiver it will check the path determination it will check the origin of the packet and also validate the routing how the packet should go source to destination. Here data transfer between two devices using IP packets. Routers always use the shortest path that is called path determination

We have the certain features like

Logical Address – Ip address

ICMP (Internet control message protocol) –

ARP Protocol Address Resolution Protocol; It will convert one of the addresses to another address are it will convert Layer 3 IP Address to Layer 2 Mac address ex Device are router

VPN (Virtual private network) – Side to Side VPN, Remote VPN

Routing Between two devices – choosing the path or route

Example for Network layer is; Router

Every Router will form one of the table called route table or routing table every router will form one table is called rout table in the route table It contains router ID, Source IP & Destination IP 10 series is pvt ID address in the organization level

Whenever some is sending the messages in the form of IP packets the data will be in the form of IP packets it will provide source IP and destination IP it will contains the message

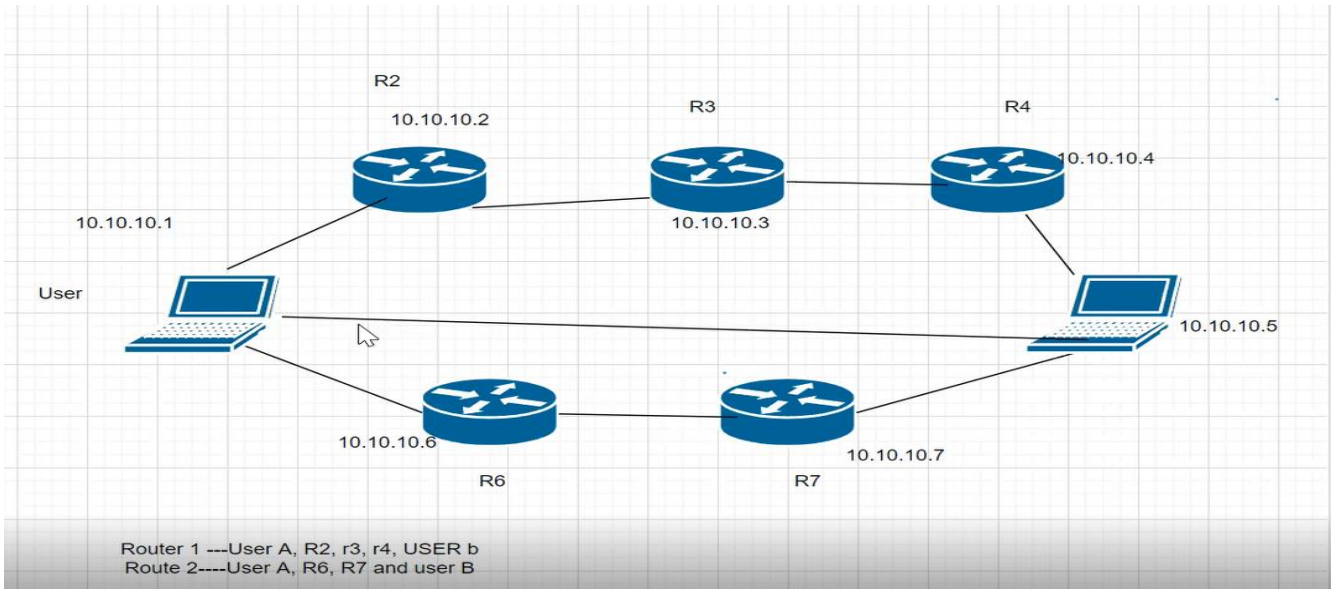
Router id is R2 which is near to user and source IP is from 10.10.10.1 from laptop that message is coming and destination ip is 10.10.10.3 it will choose always nearest router

R3 now source IP is 10.10.10.2 and destination IP is 10.10.10.4

R4 now source IP is 10.10.10.3 and destination IP is 10.10.10.5

So finally user received the messages this is called route table

Route table	Router ID	Source ip	Destination ip
	R2	10.10.10.1	10.10.10.3
	R3	10.10.10.2	10.10.10.4
	r4	10.10.10.3	10.10.10.5



If we want to connect two cities' networks, two countries networks, two state networks or two buildings, router and internet is mandatory

2 Data Link layer;

Handles the movement of data to and from the physical link. It is also responsible for encoding and decoding of data bit

It is end to end communication between 2 nodes or between 2 hosts using frames ex; sender & receiver it is completely a data format and additionally it will do error control at whatever the transport layer is doing apart this additionally it work for the one of media so that media may be Air, space, water using these medias that frames travel from one host to another Host and finally opposite person will receive the communication that is nothing but data link layer

2	Data link layer	It will provide end to end communication between two hosts using frames via media .	Frames	
		It will also provide encpulation / decapsulation		
		Media- Air , water or space		
		Frames will use TDM		
		RARP, PPP		
		RARP- Reverse address resolution protocl (It will convert Layer 2 MAC address to Layer 3 IP Address		MAC flood attack, RARP posioing attack
		Ex: Switch		
		Two sublayers 1) LLC (Logical link control)		
		1) MAC (Media access control)---		
		Switch types 1) Access switch-2500 (Lower end model it will support less speed)		
		2) Distobuited switch----4500 (It will support medium speed)		
		3) Core switch----6500 (It will support high speed)		
		Note: if you want to communicate two builingds, two citites and two contries switch will not support		
		Switch will not support internent		
		Switch will not support for VPN		

We have the certain feature like

It will also provide encapsulation / decapsulation;
So, whenever any packet is coming so it will open the packet and it will encapsulate the data and once it receives the receiver it will open the what frame Id is there it is called Encapsulation/Decapsulation ex; device is switch similar to encryption & decryption

Encapsulation ; It is nothing but additional layer we will put on top of the data for security reasons and encapsulate it we will send the data from the receiver side we will decapsulate and we exactly the data has sent it Encapsulation is the process of adding additional information when data is traveling in OSI or TCP/IP model. The additional information has been added on sender's side, starting from Application layer to Physical layer.

Decapsulation; De-encapsulation is the exact reverse process of encapsulation. The additional information added on the sender's side(during encapsulation) gets removed when it travels on the receiver's side from the Physical layer to the Application layer.

Physical Media – Air , Water , Space

Data Format – In Data link layer the Data Format is frames (Frames will use for Time division multiplexing TDM)

Protocols – RARP (Reverse Address Resolution Protocol), PPP (Point to Point Protocol)

Reverse of ARP It will convert Layer 2 Mac address to Layer 3 IP Address which will be in Data link layer

PPP- is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC

Example for data link layer is; Device is switch and switch will use the physical address called MAC Address

whenever you are trying to access any application in the organization level directly it will go to the access switch from access it will go to distributed and from distributed it will go to core

Switch types we have

- Access switch-2500 (Lower end model it will support less speed)

  The access layer is the first layer. This layer allows end users to access the network. This layer also connects user-devices such as PCs, IP phones, wireless access points, printers, and scanners to the network.

  User-devices connected to this layer use different protocols to discover each other, remove loops, and exchange data. End users access the network through this layer. Various services and security policies are also configured and enforced at this layer.

- Distributed switch----4500 (It will support medium speed)

  The distribution layer is the second layer of the Cisco three-layer hierarchical model. Switches connected in this layer are known as the distribution switches. Unlike access switches, distribution switches do not provide any service to end devices. Distribution switches connect the access switches.

- Core switch----6500 (It will support high speed)

  This is the third layer of the Cisco three-layer hierarchical model. Switches that work in this layer are known as the core switches. Core switches connect distribution switches. In a complex and large

network, core switches reduce cabling needs and switch ports while still allowing all devices to send data to all other devices in the LAN.

Usually, small or medium LAN networks do not design the core layer. Instead of designing a separate core layer, they directly connect distribution switches. This approach does not work in large networks.

Ex; in 5 floor building 4th floor one of the employee try to access the google.com the hierarchy 1st it goes to access switch, then distributed switch , and to core switch then finally to internet then to google.Com which means internet

Note: if you want to communicate two buildings, two cities and two countries
switch will not support
Switch will not support internet
Switch will not support for VPN

It will broad cast to everyone whoever is connected in the network but response will get getting back whoever is from receiver it will not take it from everyone switch is an intelligent device switch device is not supported to internet mainly it will not support to any of two cities, buildings, locations etc., when traffic comes it broadcast to everybody It is intelligent device it will broad cast with every device but it will communicate with appropriate device only nothing but destination device respond back to the respective sender device that is done by using switch

Attack ; Mac flood attack, RARP poisoning attack

We have 2 Sub layers in Data link

LLC means physically they are separate but logical they are same ex; in 3 floors building in each floor 3 hr & 3 security department used to work physically they are separate but logical they report to their respective directors that might be HR director are else Security director this logical separation by virtual Lan that is nothing Logical link control

LLC- Logical Link Control – when user is trying for Internal or external application 1st access will go the traffic switch then goes to distributed switch then it moves to the core switch from our laptop or employee laptop

MAC – Media Access Control; It is a physical address and it's a unique address We can transfer the data from one node to another node using frames node in the sense from one device to another device

1 Physical Layer

1	Physical	Using physical cables end to end communication will happen between two hosts	Raw bits (o and 1)	Physical theft
		Ex: optical, transcivers, recivers, genrators		Physical damage
		Ethernet , Optical- Protocols		
		Ex device HUB		

This is the lowest level of the OSI Model. Here data Is converted into an electrical impulse so that it can be sent through a physical medium. It is also responsible for the physical connection between the devices

Responsible for transmission of digital data from sender receiver through the communication media

Using physical cables end to end communication will happen between two hosts. Physical in the sense touchable It does End to End Data transmission between the devices from physical

We have certain features; Ex: optical, transceivers, receivers, generators

Data format ; Raw bit (0&1)

Attack; Physical theft , Physical Damage

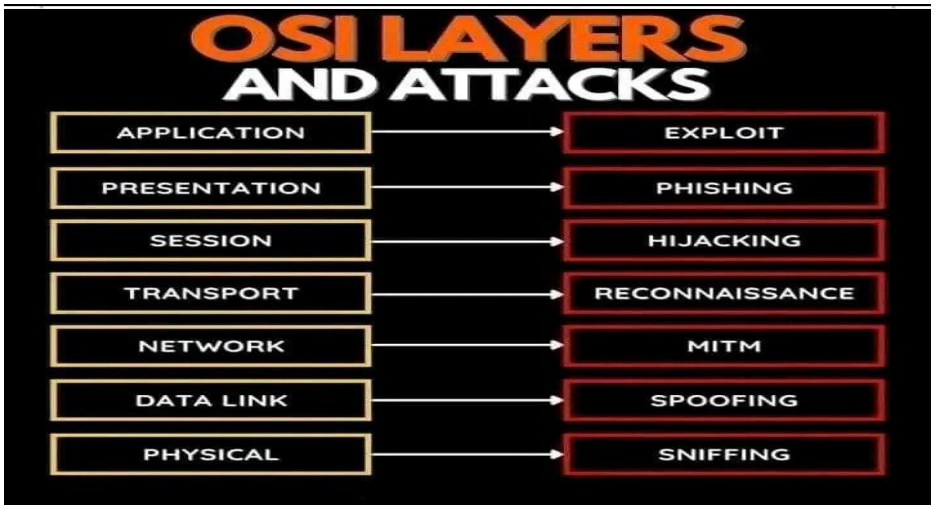
Protocol ; Ethernet , Optical fibre
Example of physical layer is Device Hub

Difference between Router & Switch (Interview question)

S.no	Router	Switch
1	Router will broadcasts the traffic	Switch will broadcasts the trafiic
2	Router intellegent device	switch also intelligent device
3	Router will use ip packets	Switch will use frames
4	Router will ip address	switch will use MAC adress
5	Router will support for internet	switch will not support for internet
6	Router will support for vpn	switch will not support for vpn
7	Router will come under network layer	switch will come under data link layer

Router is layer 3 device which is network layer – Routing happens using IP Address

Switch is layer 2 device which is physical Layer - Routing happens using MAC Address



IP Address Internet Protocol

NIC Card- Net Work Interface Card It will convert electrical signals into data signals

MAC – Media Access control Every NIC card or ethernet interface has physical address. That physical address called it as MAC address

MAC address bit size 48 (Interview question)

Ex Mac Address – It is combination of characters and address it representant 00:10:ab:cd:ef:11 so this is the way how we represent the Mac Address

How to get the mac address of the device

A We have to use CMD Command Promant (cmd:> getmac)

```
C:\Users\azams>getmac

Physical Address    Transport Name
=================== ============================================================
90-E8-68-CA-0A-6F   \Device\Tcpip_{F546E520-4DBA-43E9-8894-59B18189D49F}
00-FF-9C-2F-AE-FE   Media disconnected
N/A                 Media disconnected
```

IP Address

Numerical number or label assigned to each and every machine in the computer network ex; 10.10.10.1

Binary ---------- 2
Decimal --------- 10
Octa ------------ 8
Hexa --------- 16

Versions of the Ip address

IPv4 ---- 32 bit
IPv6 ---- 128 bit

Always IP address classification bit size will use as 2 power 8 it is nothing but 256
It will start with 0 always will end with 255 (0-255)

If 32 bit is dividing it will be 04 Octas
IPv4 billings 32 bit ---- 32 bit= 4 octa
Where we have to purchase the IP Address

IANA (Internet Assigned Authority) from this particular organization we have to purchase the IP Address.

We have to purchase always Private IP Address

Now a days almost everyone is moving from IPv4 to IPv6.
Reason is IPv4 has 8 billion address especially PVT IP addresses range may reason is like
lack of IPv4 addresses
security reasons

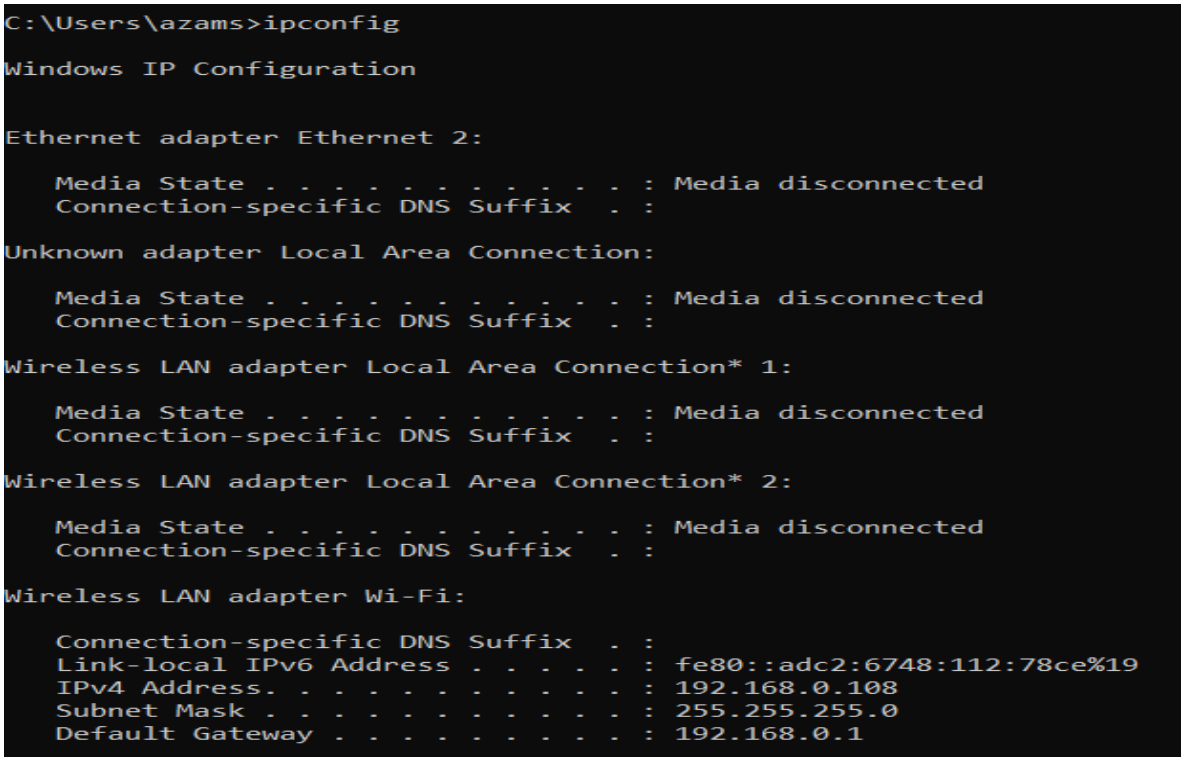
EX; IPv6 it is combination of characters & Numbers (abcd:10cd:1234:1011)
IPv4 10.10.10.1 this is simple that's why for security reasons migrating to 1Pv6

Classes of IP address (This is combination of Public + Private) {Interview Question}

Types of classes	Range	Importance
Class A	0.0.0.0-126.255.255.255	We use of Application Enterprise level or large number of devices
Class B	128.0.0.0-191.255.255.255	We use medium size organizations
Class C	192.0.0.0-223.255.255.255	LAN
Class D	224.0.0.0-239.255.255.255	We use for Multi-tasking which means more than one action
Class E	240.0.0.0-255.255.255.255	R&D
Loop back address (Local Host)	127.0.0.1	

Above Those are IPv4

Loop back; When ever if we want to install service, are if you want to listen something in your laptop are else to configure any kind of software and assigning that particular loop back address to host address. in that scenario we have to use loop back address then that loop back address we have to take to browser level address and we have to login into the respective local host then we have entered user name and password
Syntax for how to identify Ip address of the system?



Use command prompt then use the command Ipconfig (CMD:>ipconfig) then display Ip address and also apart from this it shows Mac address and entire details like default gateway

Default Gateway; Which whenever your connected with Wi-Fi & Lan. 1st you're rooting which means next routing IP Address it will act as Router a default gateway is an IP address that traffic gets sent to when it's bound for a destination outside the current network. On most home and small business networks—where you have a single router and several connected devices—the router's private IP address is the default gateway. All devices on your network send traffic to that IP address by default.

cmd>ipconfig /all

It contains every thing not only just Ip address Information It providing host name , mac address and displaying what are the ethernet interfaces are configured

Private IP Address Ranges

Pvt Ip Addresses are also called as Non – Routable Ip address

Types of class	Range
Class A	10.0.0.0-10.255.255.255
Class B	172.16.0.0-172.31.255.255
Class C	192.168.0.0-192.168.255.255

Ip Address range always 10 series number , 172.16 series ,198. 168 series only Other than this series another series comes under public only

How we can identify whether security attack or incident is internal attack or external attack ?

A By knowing the Ip address range that is i.e 10.0, 172.16, 192.168.

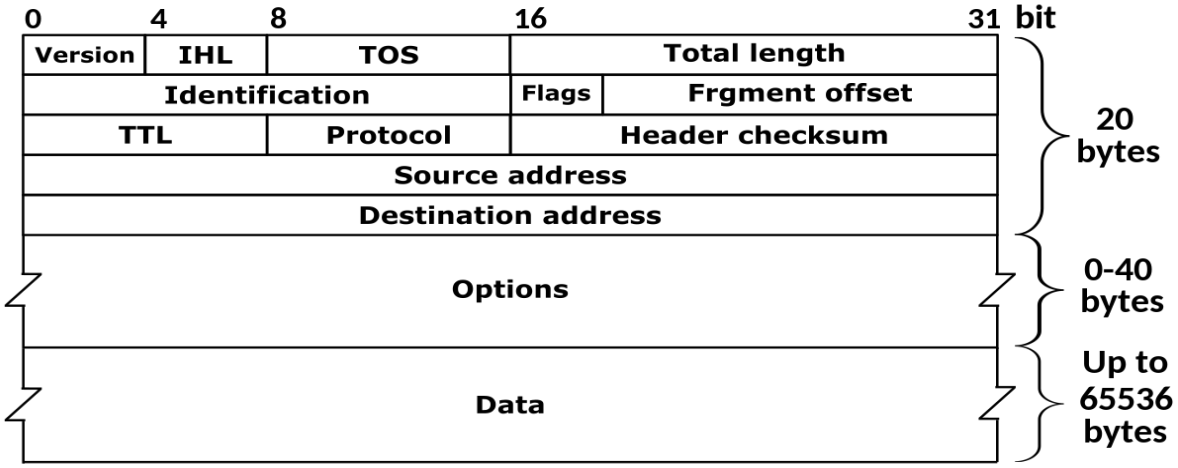
Internal attack another name is insider threat.
Examples
Brute force attack is coming from -- 192.169.0.0 – external attacker
Malware attack -- 172.15.0.0 - external attacker
Dictionary attack -- 10.0.0.255 – Internal

When ever any attack is coming in the SIEM tool 1st thing is we have to identify whether this particular attack is insider attack or external attack so if it is internal threat or insider attack

If it is Insider attack we will contact the end user that if we have the permission to contact the end user
If it is external attack in that scenario we to check the reputation of the Ip address and we have to block the particular Ip address in the fire wall level

IP Packet	IP header	Payload
IP header	Source IP and destination IP	
Pay load	Piece of written code (Message)	

IP Packets; It means Internet protocol packets this ip packets we use for routing purpose sending message from one source to another source
The format which contains Ip header & Payload



Ip packet contains the version nothing but type of the version using whether it is Ipv4 or Ipv6 and internet header length so 0 to 32 bit and 0 to 4 is the version and we can we see Time of service, total length

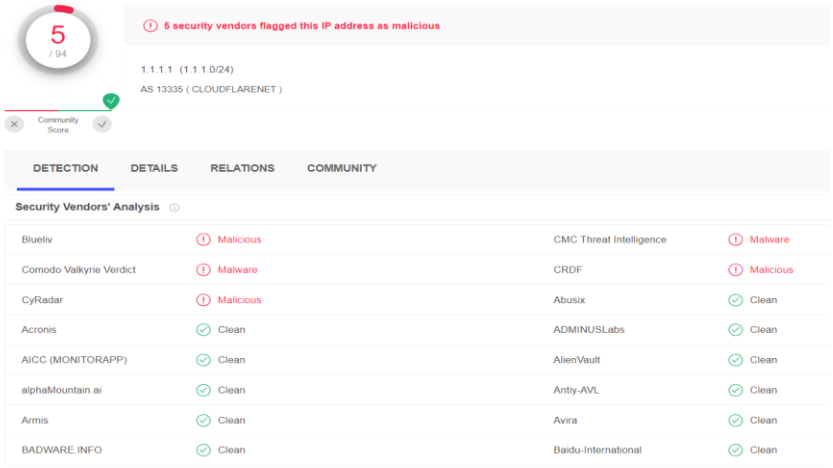
Ip header- It contains in short

contains Source Ip (A sending and email to B and whatever Ip address contains to you laptop or to mobile so that is called source Ip & Destination Ip (where the email has to reach in the scenario its me whatever Ip I'm using laptop or mobile that is nothing destination Ip

Payload – It is nothing but peace of code that is also we can say message I mean body of the content

Whenever any attacks are coming we have analyse the pay code nothing but log

Ip reputation check (virustotal.com); checking the reputation of the Ip wether what meaning whenever any incident coming to the organization level ex use any ip address like 1.1.1.1 then search it into virustotal.com website were u can see



This is how we can see 5/94 out of 94 here 5 are malware category we have to block such 5 ips address

Ports & protocols

Ports ; Software defined number associated to network protocol. It is used transmitting the data and also receiving the data for communication purpose between two devices

Port types ; we have 2 types

Open Ports

Closed Ports – Reason is If any port is open based on the permutation & combination attacker will enter into the particular port into the organization level so that's why closed ports are always better

Ports will always open in the Fire Wall

Whenever we are resining any request for tracking and auditing purpose always we have to raise the ticket in the ticketing tool that is tracking and auditing purpose as

well even for evidence also in future if any thing goes wrong we check who opened and provided the approval

Respective team will fill the respective Fire wall templet and after that so they created one of the ticketing tool later they will assign to fire wall team

And in the fire wall there will be two types of people will there

1. Approver – He will do risk assessment & risk analysis like what ever application team they raised the request and whatever product development tea, raised the request related to port like devops teams, TechOps team, Data science Team etc.,
   Approver is accountable & responsibility. The Approver will see what is the port number which team is requested will be validated by approver
   Ex; port 80 he will check what risk is involved in that senacior if risk available and he will go back to the respective team whatever risk it is open to in the organization level he might reject will ask for justification will update the status like this is risky port cannot be open and will reject the particular request. Then he will keep one more comment if you provide the business justification your Accountable & responsible now they take care who raised the request
2. Implementation – Once Approval received from Approver based on the business justification the firewall implementation guy will implement nothing but he will go to the policy or rules tab and he select the source zone & destination zone , source port , destination ports, protocol and action will define allow so finally the port will be opened

This is the above process we have to follow

which ports are better from the organization point of view ? (Interview Question)

Closed ports are better. why because if dangerous ports opened by attacker will do port scanning mechanism and he will tactics as a port scanning mechanism and he will try to enter into organization level A closed port is the opposite, ignoring and not accepting any packets that may be transmitted to it. Its inaccessibility is not the only feature that defines a closed port. A closed port is considered such not only if it is unreachable, but also if there is no software listening on that port.

For business purpose if end user wants to open the port in system. what they have to do?

They (Devops , TechOps, dev, testing , storage, back team, db, server , and so on) have to fill the firewall templet dn they have to raise ticket in the ticketing tool and they have to assign to Firewall team for opening in the port in firewall

Ticketing Tools (Service Now, Jira etc.,)

Team Name	Source Zone	Destination IP	Source IP	Destination IP	Port number	Protocol
MS SQL	Trust	Trust	10.10.10.1	10.10.10.1	1443	TCP

After they fill this request templet, they need to raise the request in the ticketing tool after this they need assign the respective team which mean to the Firewall Team

Now the Fire wall team works

Firewall approval team will review the request whatever team is raised related port request. Also they will do risk assessment. Finally they will approve the request. he might reject will ask for justification will update the status like this is risky port cannot be open and will reject the particular request. Then he will keep one more comment if you provide the business justification from director I mean to whom they are reporting so that guy has to provide the Business justification then only its accepted in that scenario Accountable & responsible by the Application development team

Firewall implementation team will implement or create policy or rule in the firewall level. Then he can access so this is the way is process

How many zones are there in the organization level as per network Architecture diagram level? (Interview Question)

A Trust, Untrust , DMJ or DMG

In the organization level every system contains how many ports

A from 0-65535 which means 65535 In that

well known ports like from 0-1023 which mean 1024 (These ports we use regularly)

Filtered ports- In the fire wall we will whitelist & block list certain couple of ports that is called filtering in the firewall we will implement what are all the ports should be opened and closed

Protocol - set of rules & regulations for transmitting data between systems

	Protocol	Importance	Port Number
	FTP (File Transfer protocol)	Transferring of the file from one system to another system	20 & 21
	SFTP (Security File Transfer protocol)	Transferring of the file from one system to another system	20 & 21

	SSH (Secure Shell)	To log into Unix operating system (Ex: RHEL, Cent OS, Debian, ubuntu, docker, container)	22
	SCP (Secure copy)	Copying of the files with in secure manner	22
	Telnet (Telecommunication network)	Log into one Unix server to another Unix server	23
Interview Question	SMTP (Simple mail transfer protocol) or Email or UCS or Exchange	For sending the mails and receiving the mails	25
Interview Question	DNS (Domain name server)	Resolving the domain name into Ip address vice versa	53
	DHCP (Dynamic host config protocol)	Dynamically or automatically it will assign the Ip address to end user systems	67 & 68
	http(Hyper text transfer protocol)	web browsing . It is not secure protocol	80
	HTTPS(Hyper text transfer protocol secure)	web browsing . It is secure protocol. It will provide encryption, authenticity, non repudiation and integrity	443
	SSL/TLS (Secure socket layer/Transport layer security)	It is part of Https or it is subset of https. It will provide encryption, authenticity, non repudiation and integrity	443
Interview Question	NTP (Network time protocol)	It will sync up with local time of the zone. (IST, GMT, CET)	123
	Pop3 (Post office protocol)	Delivery of the messages	110
	IMAP (Internet message access protocol)	Delivery of the messages	146
	Net Bios (Network bios input and out system)	Initial config or booting or loader	137 to 139 (137,

			138 and 139)
	Ker brose (Mutual authentication)	Mutual authentication (It uses for the ticket granting system	88
Interview Question	RDP (Remote desktop Protocol)	Log into one windows system to another system	3389
Interview Question	syslog (system logging)	logging of the actions of the end user or computer recorded activity	514
	SNMP (Simple network management protocol)	It will identify the inventory and also managing of all the network devices. SNMP1, SNMP2 and SNMP3 SNMP1 and SNMP2- Clear text or plain text SNMP3- Encrypted text	161
	LDAP (Light weight discovery access protocol)	AD (Active Directory) - integration to tool	389
	LDAPS (Light weight discovery access protocol secure)	AD integration to tool with secure manner	636
	SIP (Session initiation protocol)	Session initiation between two users	5060 &5061
	SMB (Server message block) One of the dangerous	Messaging purpose in windows OS	445
	IPsec (IP Security)	Remote VPN and site to site vpn	500
	MS SQL (Microsoft Structured query language)	Data base back up	1433
	ICMP (Internet control message protocol)	no port numbers. It is service	
		ICMP protocol Ping we will use for messages or services. there are type 0 to type 255	

		messages will send or receive Type 0 – which means reply back from server	

In putty software we can check the Port numbers then just click on open button

If in case we want more way of Authentication mechanism we can use Authentication also that pvt key we can see under the SSH were we can see Auth (It is nothing but Authentication) and the time of creating the user role normally one the file will create that file is nothing but key or password

For one of the Linux server or one of the window server if you want to create the security what are the couple of things you implement (Interview Question)

A Like User Name, Password, Authentication key additionally herding bench mark and also logging & Monitoring part. Logs we have log it those logs we have to integrate it to SIEM Tool additionally we have to implement role based control. According to role of the user ex; devops , TechOps , Data science, Linux, machine learning team etc., according to their what level of access is required to enter into the Linux server that is nothing but Role based access control

Static IP & Dynamic IP

Static IP Address - it is constant or fixed Ip assigned to system It is completely Manual to assign the Static Ip address Manually

We have to go to the network & Internet option in the laptop we have click on the Adaptor options and then we can see Advance settings & click on it then we get more networks and adaptor option click on it then we can see Ethernet, LAN & WIFI from Ethernet we should choose the properties by clicking the IPv4 then we can assign IP address Statically it is always constant

Coming to Any server , Data bases are may be any security tool we have to assign static IP only expect end points all other devices we assign Static only that may be windows server, Linux server, Fire wall , SIEM tool etc., for those scenarios we have assign Ip address statically the reason is some times Ip will get change like Reboot, or any performance issue will occur so that's why for only End points related to employees that may be laptop, Mac address , work station , desktop these machine we have to assign DHCP which is dynamic

Static IP addresses are not used as commonly now, it is important to note when using a static IP address is necessary. Businesses will mostly use static IP addresses if they are hosting servers and websites.

In most cases, a static IP address will be used by businesses to ease operations with FTP, email and virtual private networks (VPNs) servers, database servers, network equipment as well as with web hosting services. In these cases, businesses that will handle a lot of data in these areas will find. having a static IP address useful for employees and customers that have to connect to the organization's servers.

Draw Back of Static Ip

Manual Allocation
Robust & Complexity
Managing the database without any errors
Ip conflict
Time consuming
For enterprise level its challenging to assign Ip address Manually

To eliminate drawbacks of static ip we will use DHCP server

Dynamic IP Address

DHCP (67&68) server will allocate IP address Dynamically or Automatically using the DORA Process for the specific period of the time that time we call as lease time.

Dynamic IP address is a temporary address for devices connected to a network that continually changes over time. An Internet Protocol (IP) address is a number used by computers to identify host and network interfaces, as well as different locations on a network. dynamic IP addresses are ideal for everyday internet users because they are easy to manage and don't require users to go through any additional setup or network configuration

Dynamic IP addresses are pulled from a pool of other IP addresses and change anywhere from within a few days to a few months. In contrast, static IP addresses assign a single, unchanging IP address to a home network. Dynamic IP addresses do not cost any extra and are simple to use. They can also be seen as more secure since they change often

DORA Process (Interview Question)

D – Discovery - once Client will connect to either LAN or Wi-Fi DISCOVERY broadcasts it will send to all the machine sin the network

O – Offer - DHCP server will respond back or OFFER stating the i am the DHCP server

R- Request - Client will REQUEST IP address to the DHCP server

A – Acknowledgement - DHCP server will validate and verify whatever empty or free slot of IP address is available in the DHCP server and it will allocate automatically for a specific time period

Employee goes to the office connect his system through LAN or Wi-fi so his laptop will broadcast the request to whatever devices are connected to LAN this discovery request is nothing but Broadcast request

Once End user or employee is connected either wi-fi or Lan in that scenario that request will go via broadcast that means that discovery request will go to the different machine now DHCP Server will respond back stating that I'm DHCP server and it will offer DHCP Server

Now DHCP Server will respond back I'm the DHCP Server now client will give request I need one of the IP addresses to my laptop so finally DHCP will acknowledge IP address of the empty free slot. Is it available so in the DHCP server that's what it will validate there will different IP address ranges will be there so what ever free slot is available it will send to the client as Acknowledge & Automatically Ip address will assign to the user that is the way how DORA process will work

It do IPAM – Ip Address Management it will do managing the IP address here no human intervention is requires only 1st time it is required with the help of network Admin

Tools –
Micro soft , Info blox

DNS Sever (Domain Name Server) 53

DNS stands for Domain Name system. It is like the internet phone book that is responsible for mapping the domain name into its corresponding IP address. It will convert or Resolve Domain Name into Ip address vice versa I mean Ip address to domain name

Ex – User enter Google.com in this scenario this DNS server will validate as per business point of view this google.com is blocklisted or whitelisted in the organization so here DNS will validate and check in its Database of the DNS Server

whether the particular domain name it is existing in the Cache are not. cache which means temporary storage, so finally in case if it is existing the cache of the DNS Server, it will respond back to the user and finally user is able to access the google.com so that's the way how this process will work

In the DNS level we will configure the filtering of DNS of the level filtering in the sense whitelisting (Allowing) & blocklisting (Blocking) of the domains these we can do in Either DNS, Firewall & Proxy any of these will support allowing & blocking of the domains

DNS will have some Authentication backend server once the user providing the Google.com is initiating the web browser and initiate any domain name or any application or any website in the browser of the respective chrome or fire fox, or may be internet explorer in that scenario request goes to our private DNS so DNS will validate whether this particular DNS whatever employee is requested it is available are not and also it will validate white list or blocklist

So then in case that is not available cache of the respective DNS server that DNS server will send back request to Authenticative server backend the request will go to www.google.com now once again this authenticative server will validate google.com is white listed or backlisted so google.com is genuine website not a fake website or it is not D phase website now autheticative server will respond back to the DNS server stating that it is genuine website that you can take the particular response. Now response will back from Authenticative server to DNS server

Now DNS server will put cache it will store here google.com so now it will respond to the user so finally user will access

Now one more user B requested another user requested same website google.com in this scenario DNS server will check the cache that google.com is existed or not so now it is available cache of the DNS server then finally it will respond back to user now backend process will not happen now so now user can access the google.com so every domain will map with IP address it will resolve domain into Ip address this is the way how this process will work

DNS Records

For converting or resolutions domain name into Ip address we will create couple of records called as DNS records

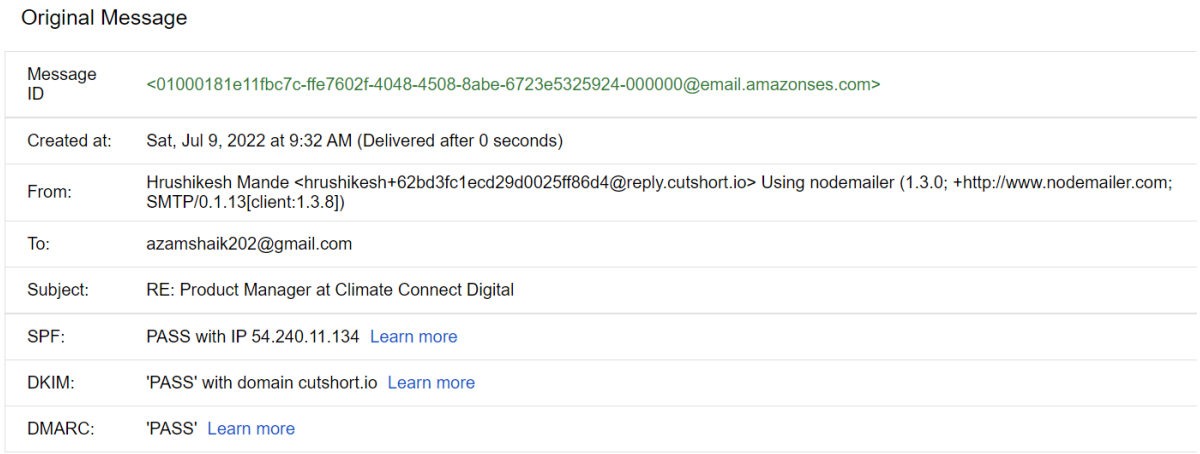
1. A Record – it is use for Authentication It will convert domain name into IPv4 Address

   Ex; Google.com 8.8.8.8

2. AAAA - It will convert domain name into IPv6 Address
3. PTR (Reverse Pointer) – Opposite to A & AAAA Records
   (It will convert Ipv4 & Ipv6 address into Domain Names)

4. MX (Mail exchange) Interview Questions (what are the email parameters) or what are the technical features contain in E-Mail
   To send and to receive an email we will use MX record
   Every email contains some of the important technical features or parameters

EX; Click on the mail on the right hand side we see the 3 dots click on it then you can check show original then we will see the interface in such a way like Message ID , Created , From, To , subject , SPF(Sender policy Framework) etc., every e-mail backend could be either java script or HTML



Original Message

Message ID	<01000181e11fbc7c-ffe7602f-4048-4508-8abe-6723e5325924-000000@email.amazonses.com>
Created at:	Sat, Jul 9, 2022 at 9:32 AM (Delivered after 0 seconds)
From:	Hrushikesh Mande <hrushikesh+62bd3fc1ecd29d0025ff86d4@reply.cutshort.io> Using nodemailer (1.3.0; +http://www.nodemailer.com; SMTP/0.1.13[client:1.3.8])
To:	azamshaik202@gmail.com
Subject:	RE: Product Manager at Climate Connect Digital
SPF:	PASS with IP 54.240.11.134 Learn more
DKIM:	'PASS' with domain cutshort.io Learn more
DMARC:	'PASS' Learn more

SPF (Sender Policy Framework) – We have to enable SPF in SMTP Server in SPF we can see PASS which mean genuine

DKIM (Domain key identification Message) - We have to enable DKIM in SMTP Server in DKIM we can see PASS which mean genuine key means in between sender & receiver it will exchange the keys that is nothing but public key and pvt key we will absorve to the particular activity so some mails we will confidential restricted and also pvt and also encrypted messages in that scenario in between sender & receiver so that keys are exchange and also encrypted mail is formed.

DMARC (Domain Message Authentication Receive Code) – It is basically digital certificate so whenever sender is sending an email in that scenario SMTP Server will authenticate whether the sender person is genuine are not it will receive one of the code and finally approve that particular code so that is called DMARC

Return Path – Return-path is a hidden email header that indicates where and how bounced emails will be processed. This header, also referred to as a bounce address or reverse path, is an SMTP address that is separate from your original sending address, and is used specifically for collecting and processing bounced messages.

DK (Domain keys) –
DNS Record -
Header Analyzer –

When ever we get any fishing E-Mails above parameters we need to investigate

5. CNAME (Canonical name) Interview Question – When ever in the web browser level if you want to enter googl.com so then it will convert it into HTTPs which means It will convert one form browser into another form of web browser

   EX; google.com / https://www.google.com

6. ISDN record (Integrated single digital network) - if we want make call to internal we will configure ISDN record
   EX ; International code 0 , country code – 91, 971 , + 1 etc., , Mobile no – xxxxxxxx

7. HINFO record (Host info record) – It means whatever DNS Record is there that hot record. Whatever DNS record & DNS Record we are configuring that info record so its related to DNS Server

Hinfo record will represent host of the DNS server Ex: RAM , CPU, SDD, Generation, core

8. NS (Name Server) Interview Question– It is configured by Domain wise & Sub domain wise and also geo graphical location as well
   EX – Google.com this is main domain under this google .com we have sub domains like

Google.com	NS (Name server)
Gmail.com	NS 1
Youtube.com	NS 2
Google chat	NS 3
Google meet	NS 4
Google drive	NS 5

The above NS1 to NS5 those are sub domains under Google.com
Geo graphical wise
EX ;

Yahoo.com	USA	Name server
Yahoo.co.in	Indian	NS 1
Yahoo.co.sg	Singapore	NS 2
Yahoo.co.uk	United Kingdom	NS 3
Yahoo.co.au	Australia	NS 4

9. SOA (Start of Authority) Interview – So basically This record will represent primary DNS, secondary DNS, DNS zones , admin email address, user name of the admin & contact details it is nothing but Start of Authority so mainly for authorization person related details whatever will be configuring respective DNS server is nothing but Start of Authority
10. TXT (Text record) - This record will be used messaging or texting purpose this will configure under DNS record

DNS Server Classification

Public DNS – Anyone can Access Ex; Google.com 8.8.8.8
Secondary or Backup DNS 8.8.4.4
Private DNS - Only Restricted can access that means within the organization
Every organization maintain 2 primary PVT DNS Servers
Primary PVT DNS server ex google.com we don't know we are not sure
Organization will have their own pvt Ip address
Secondary or Backup PVT DNS Server

DHCP & IPAM – (This functionality is done by DHCP Server)
Once you implement the DHCP Automatically it will function no human intervention is required
DNS – DNS resolution done by DNS server
If we combined DHCP, IPAM & DNS the solution is called DDI

Famous Tools or vendors in the market
Microsoft
Infoblox – even Infoblox can provide DNS server. Microsoft DNS , DHCP server will install on top of the windows server that may be 2010 R 1 & R2 , 2016 R1 & R2 , 2019 R1 & R2 etc., these are couple of Microsoft server we do have

DHCP,IMPA,DNS If we installing under the Window server it is very less expensive as compare to if we are purchase Infoblox hardware device module. Once we purchase we have to take it Data centre and we can plug the

cables in the interface. We have to configure and assign respective IP address to the server through remotely we have login into particular Ip address

Server

Server - It is a computer program or device that provides a service to another computer program and its user (Client) server will service to the multiple users

Client - Client will receive the service from server Ex; You , me & so on
Server Examples uses in the organization

Active directory (AD) , Domain controller , Data Centre (DC) , Data Base server, File server
App server, SMTP Server , web server, DHCP, DNS

Data Base Server-
DB server will store critical or non critical data of the organization
Data type – Critical & Non critical

Data Classification (Interview Question)

We need to make what type of data is it either Public or pvt
Trade marks , copy rights or patents & so on these are completely confidential data
Restricted ex financial results every organization Qutor Data
Public Data ex; Its basically advertisement its comes under public like product based on advertisement

Data classification is the process an organization follows to develop an understanding of its information assets, assign a value to those assets, and determine the effort and cost required to properly secure the most critical of those information assets.

We have to implement couple of security controls to the Data base
Under the Data base we have the different types of Data will be their

PII data (personal Identification Information) – It is nothing but GDPR compliance and it is one of the General Data protection Regulation compliance It is one of the dangerous compliance

Identification of the persons are like

Aadhar card, Pass port number, driving licence, email id , First name & Last name , Account number , credit & debit card data , mobile number
These data should not go out side

GDPR comes under the European countries

PHI Data (Personal Health Information) -

Patient Health data information should not be allowed it is restricted should not expose to the public what ever record hospital have

Examples of Data bases server

SQL (Structured query language) , MS SQL (Micro soft) , PG SQL (Post gres) , cosmos cloud (cloud) , Grid gain , Oracle , Cassandra , Mongo DB , couch base

4 File server - It is centralized server it is called RBACK Role base access control where all of the organization documents or files or reports will be saved or stored as per the team wise.

Ex; If Devops team only Devops file can access, If it is security team then only security team can only access

File Admin will take care of the file server. File Admin is authorization person to take care and verify whether the person right to access the files are not File admin will make sure that team wise access controls provided to respective team members (RBAC)

Tool for providing the access

- Cyber Ark- (IAM/IDM) - Identity access management/Identity management
- Microsoft – PAM - Privilege access Management
- Veronis - FIM – File integrity Monitoring

5 SMTP Server –

Sending the mails and receiving the mails we will SMTP server
This is also called as

- UCS (unified communication server)
- Exchange server
- E-Mail server
- Out look or office 365

Technical features or parameters

SPF – Sender policy framework
DKIM – Domain key identification message
DK – Domain key
Return path

DNs Record
Header Analyzer
DMARC – Domain message Authentication Receive code

SPF – Sender policy framework – It is an email authentication mechanism or technique. it is used to prevents spamming email (Spammer he will be spoofing of the original domain)

Ex ; x.y@gmail.com (Original Mail)

x.y@example.tcs.com (Fake account)

DMARC – Domain message Authentication Receive code

It will a sender domain to indicate that their email messages are protected by SPF and DKIM. It will tell a receiver what to do if authentication methods are passed failed which means if we don't enable SPF & DKIM obviously DMARC is fail. If enabling then its pass that is mean by DMARC policy combination of SPF & DKIM if it is fail then we have to suspect that its fishing e-mail If it is pass then it is genuine e-mail

It enables Gmail policy frame work , Enable DKIM , and enable DMARC we combine SPF & DKIM then we called as DMARC Policy

DKIM - Domain key identification message

It will be exchanging the keys, It is a protocol that allows an organization to take responsibility of transmitting messages by signing mailbox and also verify the certificate (Domain keys- Public/private) If it is signing then only encrypted channel will form between the sender & receiver and even though attacker will come in between he cannot whatever mail that we are sending & receiving, Attacker cannot read it. So if data is going in clear text or plain text more chances are to see by attacker

Return Path – Return path is equivalent to send policy frame work which means it is equal to sender email address

Header Analyzer – It contains HTML format of the mail it is entire body of the e-mail

6 Active Directory

It is directory server and it contains all the users, Ip address, domain and also all the servers and service accounts information
Active Directory

Similar group of people or team members will create a group in AD. This group called it as AD group
Who will create or manage AD ?
This will manage by Windows Admin or Sys admin guys

Microsoft is the Tool used for AD

What is difference between AD & Domain controller (Interview Question)

Domain controller

It is a service will run on top of the active directory whenever user for suppose office start from morning 9 am and ends at 6 pm usually employee get login so here DC will check that user data base is existed are not which means It is centralized authentication and authorization server.

It will validate whether employee is a part of domain or not also it will verify identify of the employee
When ever we login we get to options like Authentication success nothing but log into system

Authentication failure nothing is not able to login

For every Authentication success of Authentication failure will generate event ID in the back end

Event ID - What ever activity is happening in the windows OS system it will generate one event number is called as event id number

Event viewer - To retrieve the events information from log files in command line we can use *eventquery.vbs*. This file can be found in the directory

we can dump the events selectively based on various parameters. These parameters include event source, event id, event date, event type(*information, error , warning*), event log file name(system, application, security, IE etc).

We have to go to the event viewer in search here we can check the whatever time we have accessed, whatever time we have loged in everything it shows

What are the operating system under windows log or window server (Interview Question)

Click on windows log we get Application , security , setup , system & forwarded events

For domain control logs we have to check in security is the part of domain control log

Examples of Event IDs (Interview Question)

4624 (Authentication log on) 4798 (User Access Management)
4625 (Authentication Failure) 4672 (Special logon)

8 Application or web server

Application server will act as Intermediate or gate way between user and DB layer that is called Application or web server on top of this Application server only will host the application ex; Face book.com or you tube .com it will be host on windows server or may be Linux Server
EX server ; Apache , Tomcat, spring etc., these are for free of cost

This is basically application Architecture it contains **3 tyre Architecture**

User layer, Logical layer , Data base layer

9 Micro soft server

This is from micro soft company on top of Microsoft we configure DNS server

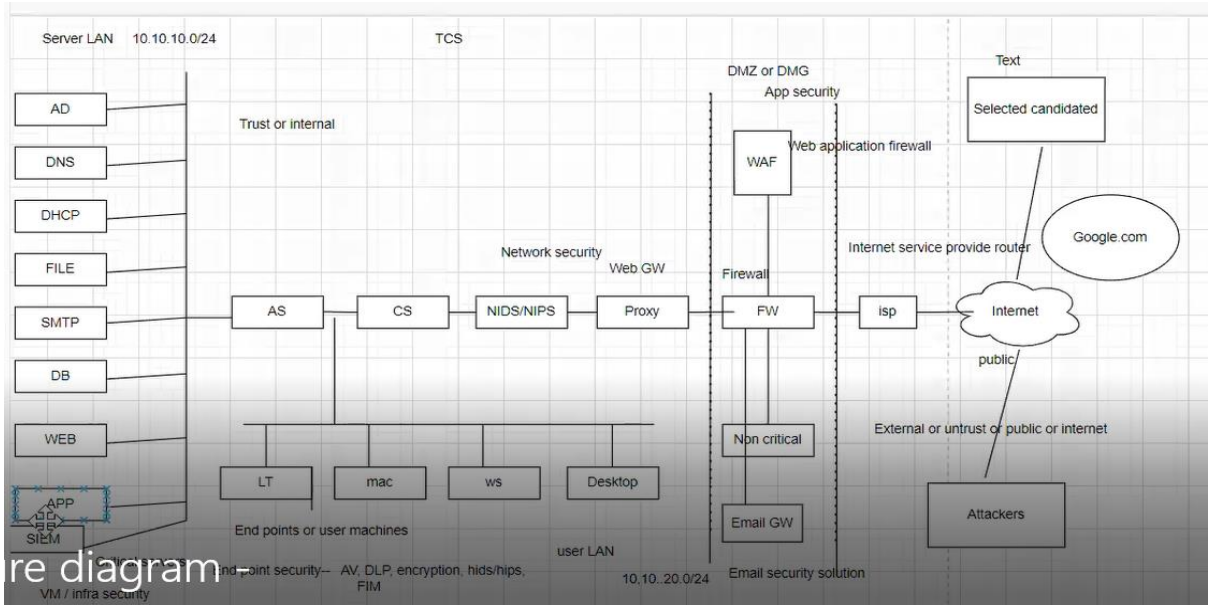
Ex ;

2008 (legacy (old server)
2012 - Windows Vista
2016 – Windows 7.0
2018 – Windows 8.1
2019 – windows 9.0
2021 – window 10.0
Latest windows 11.0

10 Unix Os

Under this we have Red hat Linux (RHEL)
Debian
Ubuntu
Container/Docker
Cent OS

Network Architecture Diagram



Whenever we want to deploy end point security, Network security & Application security , server security total end to end security in the organization level it not only applicable to on premise but also to the cloud. It describe how the networks, servers , devices , databases , applications , end point securities and so on we have to place In what place exactly that we representative in the diagrammatic way or that diagram we called as Network Architecture Diagram

1st server Lan ex 10.10.10.0/24

AD – Active Directory
DNS
DHCP
File
SMTP
DB
WEB
APP

Server Lan which mean server security part we use more into vulnerability management or Vulnerability Assessment can also called infrastructure security for scanning of the servers we called as Vulnerability management we always keep safe & secure for Attacker point of view

These above servers are critical to the organization. All these servers are internal to the organization level. We have kept always confidentially under trust worthy point of view it should not be exposed to the public & we have to provide lot of controls to

these servers. It should be kept safe & secure these servers. Reason is most of the critical data will be in these servers only. These servers will call as critical servers

Cyber Security – It is nothing but protection of all the severs , All the end points , All the systems , All the network , All the Applications, All the e-mails what we are receiving for 24/7 that is called Cyber Security we will implement under server Lan only

Access switch --- Core Switch --- NIDS/NIPS --- Proxy

Access switch, core switch in between Access & Core switch drawn one line connected to these are all end user machines
Laptop, MAC, work station, Desktop these are end points or host machine or employee machine or end user machine & so on these are nothing User Lan we will create the Ip address ex ; 10.10.20.0/24 we provide end point security to these Laptop, MAC , Work Station , Desktop these solutions are Antivirus (AV) , DLP , Encryption, HIDS /HIPS, FIM

Endpoint security or User machine

Endpoint Security – Antivirus (AV) , DLP , Encryption, HIDS /HIPS, FIM

NIDS/NIPS --- Proxy – Firewall (Network security)

Proxy will also call as Web gateway or Application gate way also it will access between user & Application it will act as Intermediate device

Above Zone we called as trust or Internal Zone (It is confidential to the organization level (Example this zone we can consider as our Home which is internal)

This below we called as DMZ or DMG (What is meant DMZ or DMG Interview Question) – DMG – Demilitarized zone this word came from military (Example this we can consider as our compound wall nothing but border kind of in between Internal zone & Public Zone)

DMZ Network is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks.
The end goal of a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure. Organizations typically store external-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, in the DMZ.

These servers and resources are isolated and given limited access to the LAN to ensure they can be accessed via the internet but the internal LAN cannot. As a result, a DMZ approach makes it more difficult for a hacker to gain direct access to an organization's data and internal servers via the internet

FW – Fire wall

(Web Application Firewall) App Security – All the layer 7 Attacks will be mitigated and prevented by web application fire wall

Non critical server – It is not that much important for the organization level

It is email gate way or E-mail security solution it is nothing but bridge in between 2 devices in between users, senders whatever sending it will access the gate way its like intermediate device

This zone we called External or Untrust or Public or Internet (This we can consider as street where we are not responsible)

ISP – Internet service provider router

Internet – It is public Network

Attacker who comes through the Internet – ISP – Firewall – Proxy – NIDS/NIPS – CS – AS and so on this is the way Attacker will target

Information Security – It is over all organization level security, its policies , Standards & Goals and objectives of the organization we define

How we can define Arch Diagram

Inbound traffic or incoming traffic ; The traffic is coming from untrust to trust zone is called call Inbound traffic

Outbound traffic ; The traffic is going from trust to untrust is called as Outbound traffic

Net flow data is the combination of Inbound & Out bound traffic it is maintained by core switch

A Ex; I'm a HR guy I want to send offer letter to X Person so it goes through the Laptop – Access Switch – SMTP – Access Switch (Because we are sending offer letter to the respective X Person via e-mail) then Core Switch – NIDS/NIPS- Proxy – firewall – ISP – internet – then finally selected candidate what ever traffic is going from inside of the organization to outside of the organization that is called out bound traffic or out going traffic

Ex ; If any employee wants to access google through any system like laptop or mac book anything – Access switch then it goes to DNS because google.com is domain name domain resolution it goes to primary PVT DNS and google.com will see whether whitelisted domain or backlisted domain if it is whitelisted it will go for Access Switch – Core Switch - NIDS/NIPS- Proxy – firewall – ISP – internet – then finally Google.com now the employee can access the google.com this is going from inside organization to outside which means trust to untrsut , Internal to Internet , Internal to public, Internal to external etc., it is nothing outbound traffic

EX; A job seeker who is applying the job for Any company he/she uses the portal career website from so & so particular company this is traffic is coming from external to inbound by using Internet – ISP – Firewall – Proxy - Access Switch – Core Switch - NIDS/NIPS- then it will go to DNS then it finally reach to Application server where ever that particular career section hosted it will reach there on top of this application candidate can apply for the job now traffic is coming form external to internal or Untrust to trust or Internet to internal or public to trust etc., this is coming inside of the organization it is called inbound traffic or incoming traffic

What are the zones in Architecture Diagram?

	CISCO Terminology Score
Trust or Internal	100 / 100
DMZ or DMG	50. 50
Untrust or Public or Internet or External	0

You're the only security guy in the organization what gone you implement (Interview Question)

Well it is nothing But green field site I have to implement everything like 1st I will implement end point level like Anti virus, DLP (Data Loss prevention) , encryption, HIDS/HIPS. & in the network level I will implement firewall , proxy NIDS/NIPS on the server level I will implement server security like hardening & vulnerability management and then application security level I will implement web application fire wall and then on physical security level I will implement like security guard or may CC TV cameras and so on and then on e-mail security side I will implement e-mail security solutions if cloud if available then I will implement cloud security solution. For monitoring entire cyber security solution I will implement SIEM Tool and it will implement everything phase by phase approach for monitoring I will implement cyber security solution as well

Network 3 tire Architecture (Interview Question)

Firewall, Proxy, NIDS/NIPS

What are END Point security control

Anti Virus , DLP, Encryption , HIDS,HIPS , FIM

What are E-Mail Security

E-mail Gate way (Its for phishing email prevention and blocking)

What is Server / Infra security

Vulnerability or vulnerability management

For cyber security what we need

SIEM Tool

Defencing & depth control (Interview Question)

It is a layer approach. If one security control is by passing second security layer it will prevent or detect, if second security layer is by passing through the third security layer it will prevent or block. This layer approach is called as Defence in depth

It is nothing But layer approach here we have to implement from Attacker point of view. which means whenever attacker is trying to do any attacks in internal in that scenario firewall is the entry point.

It means if firewall is by passing in that scenario proxy will come into the picture if proxy is also by passing the NIDS/NIPS will come into the picture. Meaning here firewall is not able to block as well proxy too here we have 3 levels of control. The reason we use for additional security because security should not compromise all these 3 level of control called as defencing depth control

Command prompt

1. Mac Address - To find the MAC address of the system every ethernet will have a one physical address that physical address is the Mac Address it's a 48 bit

```
C:\Users\azams>getmac

Physical Address    Transport Name
=================== ============================================================
90-E8-68-CA-0A-6F   \Device\Tcpip_{F546E520-4DBA-43E9-8894-59B18189D49F}
00-FF-9C-2F-AE-FE   Media disconnected
N/A                 Media disconnected
```

syntax: cmd>getmac

2. IP Address - To find the ip address of the device or system

```
C:\Users\azams>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::adc2:6748:112:78ce%19
   IPv4 Address. . . . . . . . . . . : 192.168.0.108
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

syntax: cmd>ipconfig
syntax: cmd>ipconfig/all

3. Ping – To know or to see whether the opposite system is up or down or active or in active. Here it will use ICMP (Internet Control Message Protocol) Protocol it is service base actually it doesn't have any port numbers. When it is something responding back it means it is in online or If it is not responding back it could be shut down stage nothing but off line
Below picture shows its responding

```
C:\Users\azams>ping google.com

Pinging google.com [142.250.183.142] with 32 bytes of data:
Reply from 142.250.183.142: bytes=32 time=38ms TTL=57
Reply from 142.250.183.142: bytes=32 time=41ms TTL=57
Reply from 142.250.183.142: bytes=32 time=38ms TTL=57
Reply from 142.250.183.142: bytes=32 time=41ms TTL=57

Ping statistics for 142.250.183.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 41ms, Average = 39ms
```

syntax: cmd>ping google.com

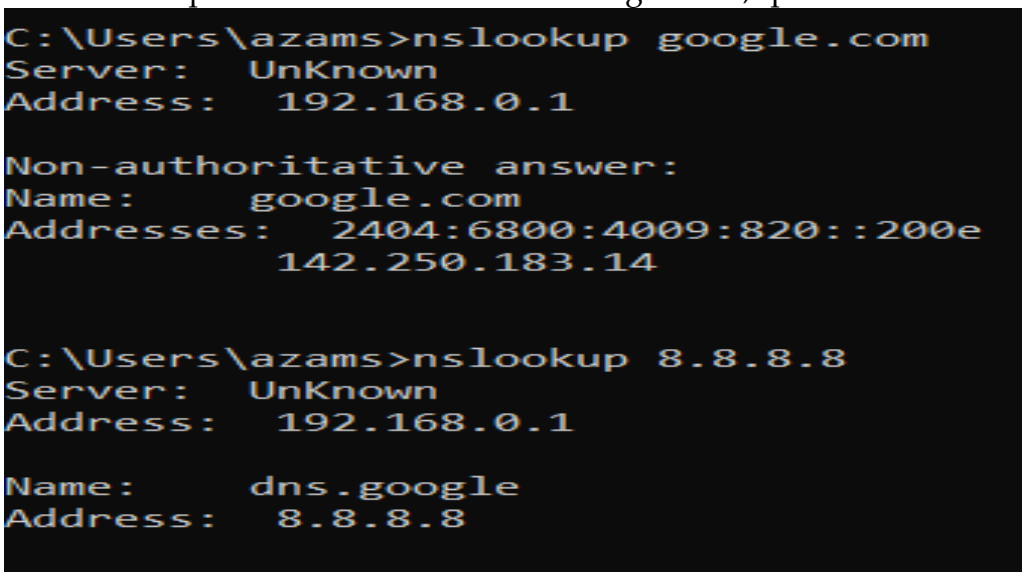
syntax: cmd>ping x.x.x.x

4. Nslookup (Name Server) - It will provide resolution ip address to hostname or host name to ip address, Whenever any security alert or security instance coming to the SIEM Tool

   Whenever any security alert will come so in that scenario if user name is there or host name is there along with Ip address is there then well and good incase if alert doesn't show any host name or any Ip address we use Nslookup along with then alert has Ip address then we type the Ip address. If have the host name then we can type Host name finally it will come

   Incase if we don't have Host Name or Ip address then we have to contact Network Admin team or Active Directory

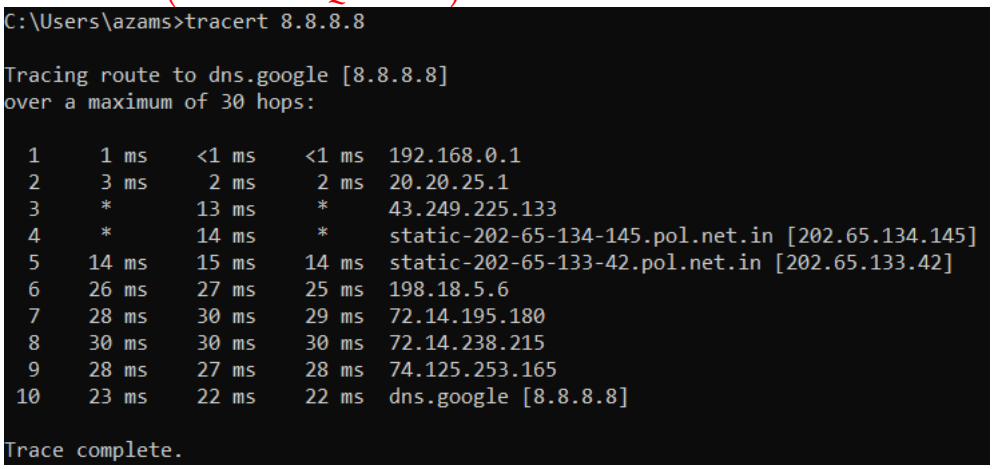
   In the below picture we can Host name Google.com , Ip address 8.8.8.8



   syntax: cmd> nslookup google.com

   syntax: cmd>nslookup x.x.x.x

5. Traceroute (Interview Question) –



   syntax: cmd> tracert google.com

   syntax: cmd>tracert x.x.x.x

It is nothing but tracing something in between source & destination or routing of something in between source and destination. It will provide the information about in between source and destination what are all the devices are available along with time. Normally this one when something got compromise want to see in between laptop or respective compromise machine how many devices are there and what Is the path , what is the route , what is the tracing that we are doing that information this will provide

Source is my laptop destination is google.com

It shows Hop devices nothing but next device which means neighbour Ip address device what are all existed. max it provide 30 Hops from my source to destination it show max 30 devices if it is more than 30 it will not show the information

When ever we made request, it will go to default gate way which is nothing but 1st HOP device then from default gate way it will go outside

For example, 8.8.8.8 or google.com (Host Name)

From default gate way like 192.168.0.1 , 20.20.25.1 , 43.249.225.133 & so on it will reach to finally it reaches to dns.google [8.8.8.8] then Trace got completed

As I said source & Destination here source is my laptop & destination is google it will show how many Hops are there in between these two devices and also how much time it is taking to reach to respective Hop that is nothing trace route

```
C:\Users\azams>tracert 10.10.10.25

Tracing route to 10.10.10.25 over a maximum of 30 hops

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2     2 ms     1 ms     2 ms  20.20.25.1
  3    19 ms     *        *     43.249.225.133
  4    19 ms     *       21 ms  static-202-65-134-145.pol.net.in [202.65.134.145]
  5    19 ms    31 ms    20 ms  137.59.200.16
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9
```

Requested time out means the packet is dropping that means normally Net work operation centre team they will see why the packet is dropping here at 137.59.200.16 now network team will check were exactly the packet is dropping. So issue from 137.59.200.16 they will go and see whether router configuration is mismatch, whether half duplex is mismatch , whether full duplex is mismatch, whether routing is properly configured or not will be taken care by Network engineers. From this we will conclude that where ever the packets are dropping that means their exactly

issue is there. Now we have to trouble shoot, why packet is dropping there what is the issue

6 ARP (Address Resolution Protocol)

It will convert or map layer 3 ip address to layer 2 mac address

RARP (Reverse Address Resolution Protocol)
It will convert layer 2 MAC address to layer 3 ip address

Syntax ; cmd>arp
Help command some of button is like
-A , -S,-D, so on

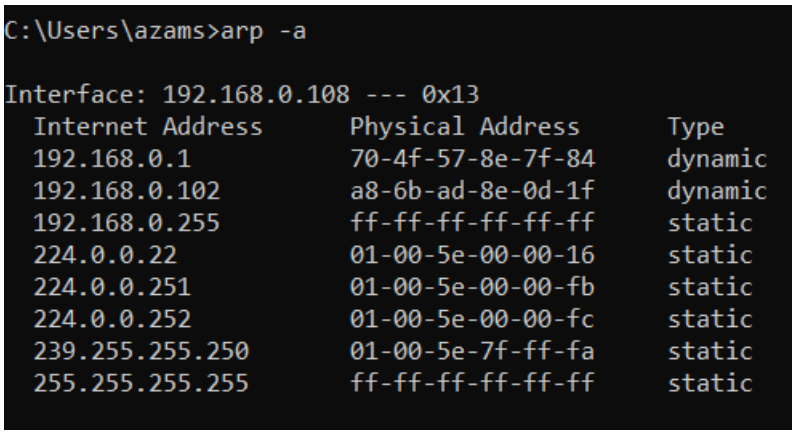
Syntax ; cmd>arp -A (Combinations can also we can type)

Syntax cmd>arp -a , cmd>arp -s , cmd>arp -d , cmd>arp -g

-a Displays current ARP entries by interrogating the current protocol data.
-g Same as -a.
-v Displays current ARP entries in verbose mode.
-d Deletes the host specified by inet_addr.
-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr.

Cmd>arp -a (It will map layer 3 address to Mac Address)

Internet is Layer Address, Physical Address is Mac Address

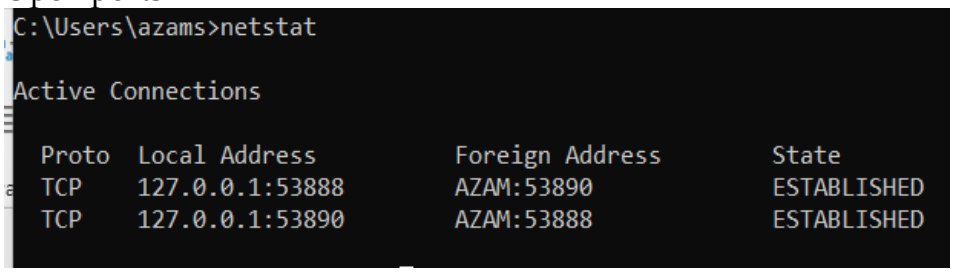


7 Netstat (Network Statistics) - it will provide the information about listening ports (what are all the ports opened in a system) These ports are used for the

communication purpose using those ports communication get established In between source & destination is called Netstat. & Netstat will provide the whatever connections are established along with what ports are open.

In any system we have the 2 ports

Closed ports
Open ports



TCP – protocol – Loopback Address – 127.0.0.1, Port (Source) number is 53388 Destination (53890)
syntax: cmd> netstat google.com

syntax: cmd>netstat x.x.x.x
syntax: cmd>netstat (For our own system

8 Path ping - This command will provide information about all the hops along with route and also time. And also it will provide the information about the between source & destination like how many hops are there along with particular IP address it is similar to the trace route. It will check whether devices are up or down

syntax: cmd>pathping 8.8.8.8

cmd>pathping google.com or hostname

Telnet 23 - It is used to log in from one unix os to another unix os

syntax: cmd>tell x.x.x.x 23

RDP (Remote Desktop 3389) - It used to log inform one windows operating system another windows operating system

When we don't have RDP access what can we do

We have to raise the request to firewall team by rising the tickets. Then firewall team will enable to access

Cyber Attacks

In Cyber Attack we have 2 frame works

Cyber kill chain process
Mitre Attack or Mitre Frame work

Cyber kill chain process (Interview Question)

Cyber kill chain is Offensive mechanism from attacker point of view. This is developed by Lockheed Martin It will step by step or we can say phase by phase approach. How the attacker will be exploiting the attacks
We have 7 phases in cyber kill chain process

Phase 1 - Reconnaissance (Recon)

In short, we call as Recon Selection of target, or research and identification of the target which means in the attacker point of view whether if I want to hack one of the Account , Application , Server , Data base & so on this is what selection of target what we are going to choose and attack that particular.

Ex How to target end user system that Ip address might 10.10.10.1, The attacker how he choose is that could be port scanning mechanism , Briber Internal employees, Phishing e-mail these are the tactics will be used by the attacker to get compromise the end user system So That is but Reconnaissance

How do you know the End user Ip address (Interview Question)

There are different way like bribe, port scanning, Many tools are available like password cracker, penetration testing tool , N map tool etc out of 100 only 70% are coming from phishing e-mails

Phase 2 – Weaponization

In Weaponization Attacker will choose the weapon how to target end user system Pair the remote a system access by choosing PDF or excel documents (Files) as weapon Attacker will inject in those files. Attacker will use as malware nothing but meliaceous software program code

EX ; Scripts or malicious malware injecting into files that may be anything

Phase 3 – Delivery

Transmission of weapon to target machine (Via email, web sites, attachments, usb drives)
EX; Email or USB drives or drive down loads

Phase 4 – Exploitation

In this stage what attacker will do is once delivered the weapon code is triggered and exploit to the vulnerable applications or systems it is nothing but attacker will identify the weakness whatever the code is sending through via e-mail , pdf or excel document it will go and it will check is there any vulnerability will existed. If it is existed that code will be exploited.

EX; Vulnerability(Weakness) and it will exploit

Persistence is not existing but in between it come from exploitation & installation persistence tactics will come so once it will identify the weakness the attacker will monitor for couple of days finally the attacker will install persistence is nothing but installation of malware of monitoring of the malware and monitoring could be anything like end user system , Application etc.,

Phase 5 – Installation

The weapon will be installed and executed will in the end user machine. Nothing but it will exploit and it will install execute that particular malware malicious software program code
EX; Malware on installed on end user machine

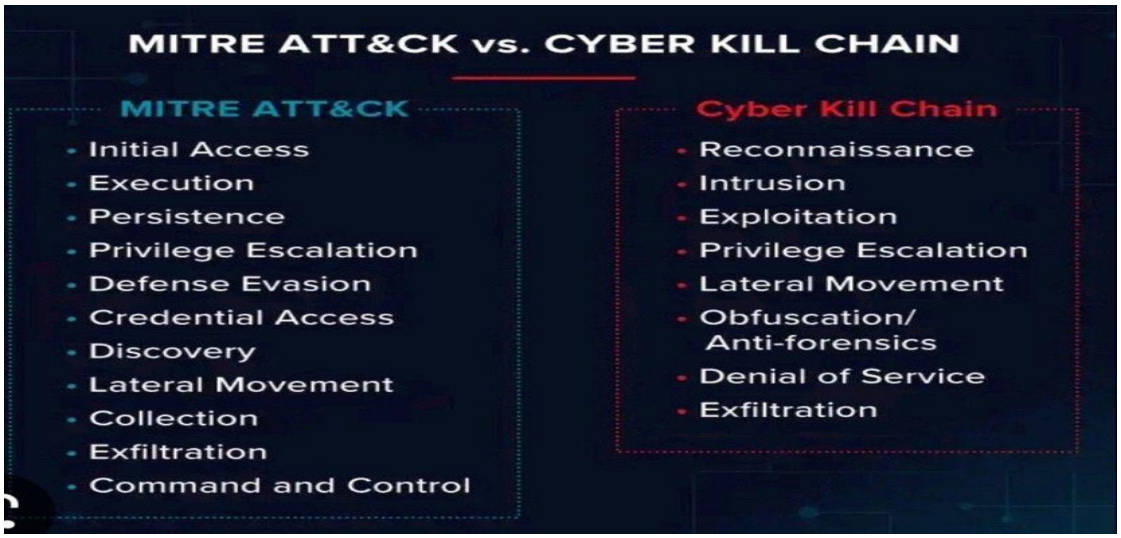
Phase 6 – Command & Control { C2C}

Now targeted machine will continuously contact the attacker machine via remote controls. Nothing but the weapon is already installed & compromised finally the attacker will under the control particular system
EX; Remote control

Phase 7 – Action on Objective
Finally the attacker will do and the attacker will achieve the object will ask for sensitive data exploitation or coping any data finally the attacker will get the unauthorize access nothing but Attacker will gain unauthorised access or sensitive data exposure to the targeted machine .

Ex ; Either need Data or Money

MITRE ATT@CK



It Is a frame work this is combination of Offensive & Defensive both it will provide attack exploitation along with preventive mechanism also. Mitre is frame work is a centralised knowledge base , it will provide tactics, techniques and also how to the attack along with preventive mechanisms. This one will be used by Offense team, red team (Hacking team), blue team (SOC team), threat hunters, reverse engineers, threat detectors , malware analyst and so on

It is three levels that are It is divided that is

Enterprise level - This for larger organization (It will provide the adversaries, Attacks and so on)

Mobile

ICS (Industrial Control System) – Like mechanical , Electrical , programmer logical array

These 3 categories providing like tactics , techniques , Mitigation & procedures knowledge based this is nothing mitre

EDR (End Point Detection Response) Tools are integrity with Mitre frame work because whenever any malware kind of attacks will come automatically will come to know exactly attacker what type of tactics is used to comprise the end user system, It could be whether attacker used like execution or script control , whether using port scanning mechanism are any installation etc

- A – Adversaries – It is nothing Attacker or hacker nothing but what hacking groups can also be called as Threat vector of Threat Actor we have that is related to Adversaries
- T – Tactics – 14 Tactics Attacker will use (Offensive)
- T – Technique – It is Dynamic in Nature but its not constant initial its 250 + but now its 500 + the attacker is using

Those 14 tactics are sub divided into 500 Techniques

- CK – Knowledge base – It is not but preventive mechanism

https://attack.mitre.org/tactics/enterprise/ (14 Tactics)

Important Questions

What is reconnaissance

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

Certain Techniques is also existed

Active Scanning , Gathering the victim Host information & Victim Identity Information , Victim Network Information, Phishing information etc

What is Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

What is meant by Privilege Escalation

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

What is later movement

The adversary is trying to move through other environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

What is Exfiltration

Which is trying to steal data

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

Network & Cyber attack classification

Malware Category (Interview Question) ; Virus, worm, trojan, backdoor, RAT, botnet, logic bomb, privilege escalation, zero day attack and Ransomware attack

Spoofing ; IP, EMAIL, DNS Spoofing and ARP

Flooding; TCP, UDP, ICMP, PING of death, Ping flood, DoS and DDoS

OWASP Top 10 (Open security Application project) ; SQL injection, CSS or XSS, CSRF, Broken authentication, MITM (Man in the middle Attack)

Phishing email category ; Spearing , whaling and smising, malware

Authentication failures ; Brute force attack, dictionary attack, password spray and VPN authentication failures

Malware (Interview Question) ; Meliaceous software program code it is developed by attacker

Ex; Virus, worm , back door, trojan , Rat (Remote Access Trojan) , root kit , logic bomb , bot net , zero day , APT (Advance persistence threat) , Privilege escalation , Ransome ware.

Malware Categories

Malware (Interview Question) ;

Meliaceous software program code it is developed by attacker

Ex; Virus, worm , back door, trojan , Rat (Remote Access Trojan) , root kit , logic bomb , bot net , zero day , APT (Advance persistence threat) , Privilege escalation , Ransome ware.

Log Sources – Firewall , NGFW, AV/EDR , Malware Analysis Tool these we integrate to the SIEM tool

Symptoms for malware entering into the organization

Automatic Restarts – It might be any like end user machine. Which is nothing but employee laptop or mac book or work station or desktop even servers or data base automatically it will restart without doing anything

CPU or RAM between utilization will be very high – That means out of 100 % utilization of the network bandwidth so related to CPU as well as RAM (Random Access Memory) and central processing unit out of 100 % it will cost more than 70%. Sometimes it reaches to 90% also in that scenario we have to suspect that is one of the malware

Performance Related Issue – System performance get very slow nothing but it will become dead slow

Cursor Movement – It completely get distract automatically cursor get move

Automatic Shutdown – It get shutdown without our knowledge

Unusual Behaviour – Once the system get infected system behaviour get change

These are the symptoms we can consider as malware injection most of the malware is causing by files

Malware Reasons – It will come through the files max it comes files related behaviour

How the malware entered into end points

Drive By downloads – Something we are downloading from the internet that files may have some malwares (Ex; Movies , Songs , or any files & so on) Drive by download cause malware , Infection that one of the possible action

Phishing E-Mail Attachments
Removable Devices - Something we are connecting to the laptop that we are removing (like Pen drive, USD, Hard disk) these are the some of Removable devices
File category names –

.PDF .ZIP
.DOC .Excel
.CSV .dll
.XML .7Zip

Malware Categories

1. Virus –

It is a part of malware category & it is a malicious software program code and it will come through user interaction by accessing the application. virus is a malicious piece of computer code designed to spread from device to device. A subset of malware, these self-copying threats are usually designed to damage a device or steal data.

It is self-replicating with in a system (Self Replication nothing but producing the copies of the files)

Examples – Heart Bleed, Anna Kournikova, I love you, Shamoon (Shamoon is one of the dangerous attack)

(These are the certain names we can see ex; like when ever if any cyclone gets different, we use in the same for virus also we do keep)

Mitigation – Antivirus / EDR (End point Detection Response) It is next generation Anti-virus Behavioural suspicious will happen through EDR & Traditional Antivirus is not sufficient for EDR. it has inbuilt features of Machine learning , Data Analytics & Artificial Intelligence

Malware Analysis Tool – Fire eye , Source Eye

NGFW (Next Generation Fire Wall) or UTM (Unified Threat Management) – Whenever any mail gets. Firewall has also had the capacity to do Analysis

2. Worm –

It is malicious software program code. if one system will get compromised through Using networking protocols other systems also will get compromised.
As compare to virus worm is very dangerous one, Because virus is within a system but worm it will spread to other devices

Worms cause damage similar to viruses, exploiting holes in security software and potentially stealing sensitive information, corrupting files and installing a back door for remote access to the system, among other issues.

Worms often utilize large amounts of memory and bandwidth, so affected servers, networks and individual systems are often overloaded and stop responding.

Self-replication with in a network which means not only one system here multiple systems get compromised

Example – Stuxnet (It is one of the worn it happen in Iran nuclear plant)

Mitigation – Antivirus /EDR , Male ware Analysis Tools, NGFW

3. Trojan

In general meaning is horse It is a malware category. And Trojan is malicious software program code It will do something beneficiary to end user but actually it will not do. (Which mean I'm trying to download something what I'm trying that I'm getting but malicious was injected into that)

It is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.

Mitigation – Antivirus /EDR , Male ware Analysis Tools, NGFW

4. Back Door –

It is malicious software program code By passing the authentication or another way of entering into organization and gaining the unauthorised access. Well backdoor itself is not sufficient so it is combination with Ransome ware, Virus , trojan, worm and so on this is how it will work

Mitigation – Antivirus /EDR , Male ware Analysis Tools, NGFW , MFA Multi Factor Authentication which means more than one factor of Authentication ex; when your opening the Gmail from new machine are new laptop it will ask security authentication to find out whether we are accessing or some other is accessing

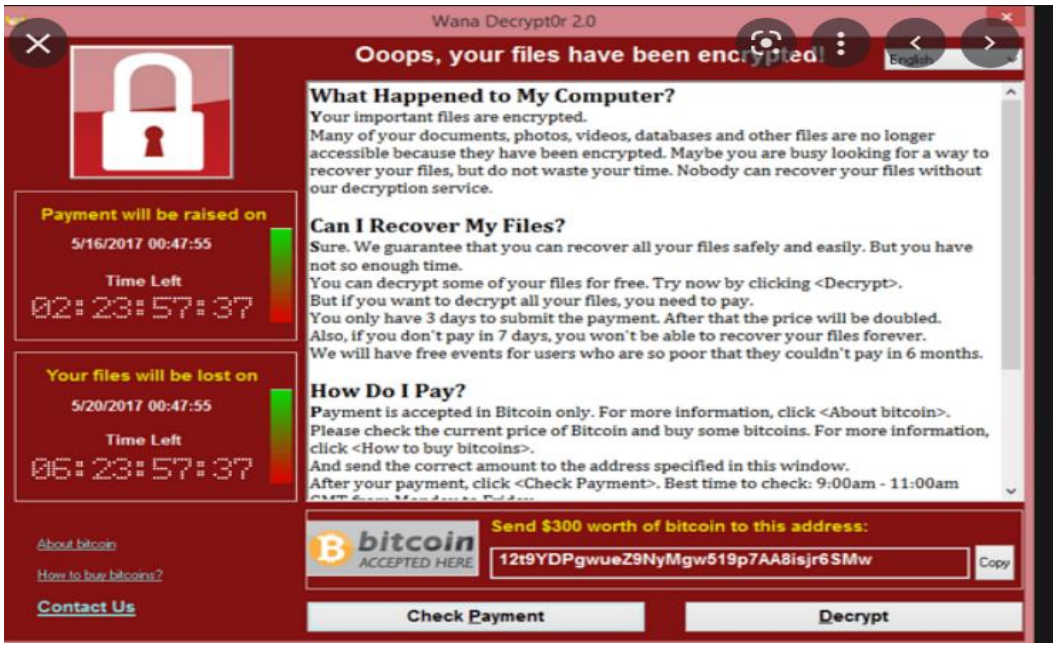
These are the mitigation steps we need to follow to care of the back door

5. Ransome wear Attack

It came into the market in 2017 ,

It a malware category, It is malicious software program code. Attacker will inject malware into targeted machine and he will encrypt single or group of lies or entire OS and finally he will ask payment as ransom (Bitcoins) is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. While some people might think "a virus locked my computer," ransomware would typically be classified as a different form of malware than a virus.

The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card, and attackers target individuals, businesses, and organizations of all kinds. Some ransomware authors sell the service to other cybercriminals, which is known as Ransomware-as-a-Service



To eliminates such type of things, we have to make sure that regular backups we have to take it is one of the preventive mechanisms

In 2017 May this happens
Series of the attacks happened in the same year

Series Name Hacking Group Names

Wanna Cry – Eternal Blue / Eternal Romance (Interview Question)
Petya - Eternal Blue
Kaseya (2021) - Regil
Maze - Cha Cha

Wanna Cry – Eternal Blue / Eternal Romance (Interview Question)
It is one of the hacking group they hack Ransome wear attack in 2017 through server message block SMB (445)

Couple of websites
Naked security
Dark reading
CSO Online
US search
India Search
Issacs
European council
In these websites we will come to know what is happening in the world wide

Wanna Cry	Petya
It is applicable to Microsoft OS applicable which means attacks only come to Microsoft OS	petya is applicable to Microsoft OS
Vulnerability using SMB (445)	Vulnerability using SMB (445) port numbers should not be open. If it is open we have to make sure the sufficient controls are existing so that is vulnerability
Exploitation group name Eternal Bule and also Eternal romance	Eternal Blue (It is a malware category comes under Ransome wear attack) so attacker will encrypt single file or group of file so finally attacker will compromise the system that is nothing but Eternal Blue
Executed via online and command and control will go to attacker Ex; Any Phishing e-mail attacks or Drive By download like something we are downloading file from the internet that file had malware that malware encrypting the file so that is called online	Petya will executes through Offline Ex; when we copying something from pen drives in that scenario this offline will happen
Propagate through network	Propagate through network , PS. Execution and windows related services

Wanna cry encrypted max 165+ countries	Petay executed max 95 Countries
Asymmetric cryptography with RSA (Rivest, Shamir, Adleman) These 3 find out Asymmetric Algorithm 2048 if attacker is using Asymmetric its challenge to decode are to decrypt.	Petya use MBR (Master Booter Record) MBR is like a memory Data encryption mechanisms like asymmetric cryptography

Mitigation – Backup Configuration is highly important whenever attack the entire system should do format, Antivirus /EDR , Male ware Analysis or scanning Tools, NGFW

6. Key Logger or Key Stroker –

It is a malicious software program code & it is a part of malware category. attacker will inject into end system and he will compromise and finally he will gain unauthorised access via keys whatever user is entering

We can say it is a type of surveillance technology used to monitor and record each keystroke on a specific computer. Keylogger software is also available for use on smartphones, such as the Apple iPhone and Android devices.

Ex; Password its one of the sensitive data , Banking related Information,

PII (Personal identifiable information) Interview Question

is information that, when used alone or with other relevant data, can identify an individual.

PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

- Personally identifiable information (PII) uses data to confirm an individual's identity.
- Sensitive personally identifiable information can include your full name, Social Security Number, driver's license, financial information, and medical records.
- Non-sensitive personally identifiable information is easily accessible from public sources and can include your zip code, race, gender, and date of birth.

Some uses of keyloggers could be considered ethical or appropriate in varying degrees. Keylogger recorders may also be used by:

- employers to observe employees' computer activities;
- parents to supervise their children's internet usage;
- device owners to track possible unauthorized activity on their devices; or
- law enforcement agencies to analyse incidents involving computer use.

Mitigation – Antivirus /EDR , Male ware Analysis Tools, NGFW

7. Spy- Ware

Spy is nothing but a secret Agent. It is malware category. Attacker will inject spyware into end user system without the knowledge of end user or without user consent. Finally he will monitor whatever end user is working on and attacker will again unauthorised access

Spyware is one of the most common threats to internet users. Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information.

Ex; Password its one of the sensitive data , Banking related Information,

Mitigation – Antivirus /EDR , Male ware Analysis Tools, NGFW

8. Adware

Adware means it is Advertisement software It is malware category. Attacker will use malicious scripts into URL's or websites and whenever user is clicked on those URL's or websites malware will be injected end user system and he will compromise the system and he again unauthorised access

Based on the human habit these adware's regularly will appear in the websites or end user systems Ex; Pop Ups

In general terms it generates revenue for its developers by automatically generating adverts on your screen, usually within a web browser. Adware is typically created for computers but can also be found on mobile devices. Some forms of adware are highly manipulative and create an open door for malicious programs.

Mitigation – Antivirus /EDR , Male ware Analysis Tools, NGFW , proxy servers we have implement why because whenever any URL has a malicious content so automatically this proxy server . when user is clicking on the websites should block that particular activity. Here proxy server play key role in Adware

9. Root kit

Root is nothing but in the Uni Operating system its high level or highest privilege

(Root access will provide entire system or server access)

In Windows terminology Root Is nothing but Admin level access same thing attacker will have the privileges to entire system

Kit is nothing but Software Tool or Bundle together which means attacker will use a malware script and the attacker will bundle together and will inject that malware into the particular end user system and finally the attacker will gain the initial level access. From their attacker will gain the root level access using some the scripts. So once the attacker the higher level access then attacker then delete, modify , update , change & so on This one the dangerous attack as well

It is a malware category. Attacker will bundle the software malware and he will inject into end user system and he will gain initial level access (User) from there using some of the scripts he will gain ROOT or ADMIN level access.

If user or attacker is getting root or admin level access he can do following things

1) He can the password of the system
2) He will remove existing user accounts or service accounts
3) Additionally attacker will modify, update, configure, add and delete the files
4) attacker can change registry keys 9nformation

Mitigation – RBAC (Role Based Access Control) We need to provide access to the particular members only , Male ware Analysis Tools, Memory dump scanning (in the Ram level or VLS chip level once opening the respective server or may be laptop need to check any malware is injected from there we can identify the issues , AV/EDR , TCP dump file and run the scans , MFA (Multifactor Authentication)

10. Privilege escalation

It Is almost equal vent to Root kit Attack only attacker will gain the initial access using some of the scripts or some of the malwares from there attacker will gain the high level access getting the higher level access from the initial access we called privilege escalation & escalation is nothing but from one layer to another layer otherwise in simple terminology lower level access to higher level access

Attacker will inject malware scripts into end user systems and he will gain initial level access like user and from there hw ill gain higher level access like root or Admin

Mitigation – RBAC (Role Based Access Control) We need to provide access to the particular members only , Male ware Analysis Tools, Memory dump scanning (in the Ram level or VLS chip level once opening the respective server or may be laptop

need to check any malware is injected from there we can identify the issues , AV/EDR , TCP dump file and run the scans , MFA (Multifactor Authentication)

11. RAT (Remote Access Trojan)

Attacker will inject malware or malicious scripts into trojan websites, once the end user is clicking on the malware or scripts as per cyber kill chain process trojan win stall in the end user machine and he will gain C2C (Remote control). Finally attacker will control end user machine and he will gain Unauthorised access.

this provide the capability to allow covert surveillance or the ability to gain unauthorized access to a victim PC. Remote Access Trojans often mimic similar behaviours of keylogger applications by allowing the automated collection of keystrokes, usernames, passwords, screenshots, browser history, emails, chat lots, etc.

Remote Access Trojans differ from keyloggers in that they provide the capability for an attacker to gain unauthorized remote access to the victim machine via specially configured communication protocols which are set up upon initial infection of the victim computer.

Mitigation – AV/EDR , Malware Analysis Tool , proxy server (It is like gate way bridge in between)

12. Logic Bomb

Logic Bomb here attacker will put some time, date & event which means when that event should happen, Automatically it will triggered and malware gets the inject so the Attacker will inject malware into end user system and also, he will define logic along with event time for deleting or executing of the malware into end user system. Finally, attacker will gain sensitive data exposure or unauthorised access

a logic bomb often remains undetected until it executes its function or launches its payload. The set of conditions able to set it off is virtually unlimited. Additionally, the degree of destruction from a logic bomb can vary greatly from deleting files and corrupting data to clearing hard drives and causing application failure.

Mitigation – AV/EDR , Malware Analysis Tool, SAST scans (static application security testing)- It is nothing but Secure code scans

13. Zero Day Attack

It is nothing but undocumented library or fix is not available from the vendor. From the vendor side we don't have the patch to fix it is nothing but upgrading of the software

If a hacker manages to exploit the vulnerability before software developers can find a fix, that exploit becomes known as a zero day attack.

Zero day vulnerabilities can take almost any form, because they can manifest as any type of broader software vulnerability. For example, they could take the form of missing data encryption, SQL injection, buffer overflows, missing authorizations, broken algorithms, URL redirects, bugs, or problems with password security.

This makes zero day vulnerabilities difficult to proactively find—which in some ways is good news, because it also means hackers will have a hard time finding them. But it also means it's difficult to guard against these vulnerabilities effectively.

Patch – Upgrading the software ex; today we have 2.0.1 tomorrow I could be 2.0.2

Mitigation – Upgrading the patch ,

We have to make sure that first of all whether we are using TPS in our organization. if we are using what are all the control are available

Ex; We can consider like Web application firewall is available , Next generation fore wall is available , whether we do have IDS/IPS & so on all those things we can make sure whether these controls are sufficient are not

Examples of zero day Attack (Interview Question)

- Apache Log 4j- whoever used from1.0 to 1.2.4 got effected (December 9th CVE- 2021-44228) which is fixed in 2.15.0 (java 8) on December 11th they released a patch - Apache log 4j 2.x got fixed
- Solar winds- August 2021 (It is node monitoring tool Application , server, Monitoring Tool it is basically supply chain attack nothing but logistic related we can consider as wall mart , amazon , filpkart etc.,
- Microsoft RCE- remote code execution- in 2022 March (In windows server this attach happened
- F5 - management console- 2022 May

TPS (Third party software) Ex; Apache , Tom Cat , Spring boot frame work, oracle java , python , perl, bash, power shell , sql , MS sql, pg sql all of them are 3rd party software's

3rd party software has 2 types

Open sources

Ex; Want to develop Google.com – In this we can use micro services application (Micro means bigger applications converted smaller application using docker , container , so on top of this docker container we will run or we will develop or will host these micro service platform related to applications

In this micro service application I want to use

- Apache Tomcat 2.0.1 (Here attacker will in this 2.0.1 Any weak ness is available
- If Any vulnerability is available in Apache tomcat 2.0.1 those application gets compromise

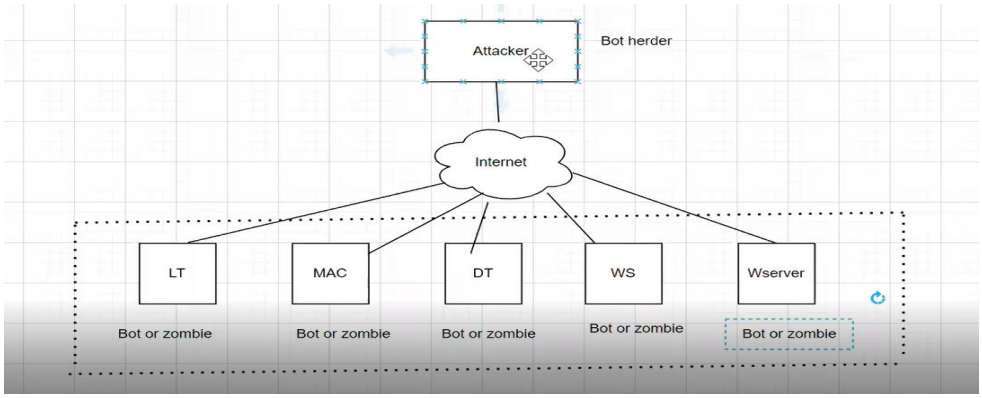
BOT NET

BOT means – Robot
NET – Either Network or Internet
If we are combing together it is Robot Network or Robot Internet

Attacker will send a phishing emails to multiple users (Spear phishing) by attaching url links or malware attachments and who ever end user is clicking on the attachment or url link those system will get compromised that too when if we don't have sufficient controls over I mean to say if the system is facing any vulnerability of weakness . Finally attacker will control all the machines through remote that is nothing CNC Control

whatever systems got compromised those systems called BOT or zombie & whatever attacker from which machine attacker is trying to do and controlling all those machines will called as BOT Header, Header is nothing but a group of the people head means the attacker will control the multiple systems so bot header means multiple systems will control by one of the owner that owner is nothing but Bot header these are connected in the LAN via Internet. So that he will gain unthorised access or sensitive data exposure

Mitigation – AV/EDR , NGFW , Malware Analysis Tool, E-Mail gate way



Well Known Attacks

Well Known means what we see regularly

1. Social Engineering Attack –

Social nothing but public which means Leaking of the confidential or sensitive data in public

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

This can also occur when someone is convinced to revel their confidential information

Three types of social engineering attacks are mainly

- Computer based – Attacker send fake email just to harm the computer. They ask people to forward such email
- Mobile based – Hacker may send SMS to others and collect imp information. If any user downloads an App, then it can be misused to access confidential information
- Human based – Hacker pretends to be a genuine user by requesting higher authority to revel confidential information

Ex: publicly announcing User name and passwords, Bank account number , credit card and debit card number etc.,

Mitigation – Security Awareness (Need to educate people to take care of confidential Data or information)

Behavioural sense – Should not revile the confidential information in public behavioural sense nothing we can say common sense

2. Shoulder surfing –

Looking into some one shoulder and taking the confidential data
Which means listing opposite information & taking the confidential data & and also we can say observing the opposite shoulder & getting the data its nothing but whatever person is speaking in public & leaking the confidential data at that moment attacker will gain the un authorised data looking some ones shoulder getting the data is nothing but shoulder surfing

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information.

Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN at an ATM or pay for something using a credit card.

EX ; publicly announcing User name and passwords, Bank account number , credit card and debit card number etc.,
Mitigation – Security Awareness (Need to educate people to take care of confidential Data or information)

Behavioural sense – Should not revile the confidential information in public behavioural sense nothing we can say common sense

3. Eaves dropping –

Secretly listening other people conversation and getting the confidential data

Mitigation – Security Awareness (Need to educate people to take care of confidential Data or information)

Behavioural sense – Should not revile the confidential information in public behavioural sense nothing we can say common sense

4. Data exfiltration –

It is Mitri Attack here we use 14 attacks
Stealing or Leaking or exposing of confidential data through network or internet

EX ; DL (Data loss) It could be like Data loss through Pen drives, USB, external devices, Sending an email from professional to personal

Mitigation – DLP (Data loss prevention) , ACL (Access Control List) , RBAC (Role Base Access Control)

5. APT (Advance persistence threat)

Persistence means continues threat
A- Advanced technologies
P- Longer time period not detected
Threat- Weakness exploitation

Attacker will use advanced hacking technologies to compromise end user system after identifying weakness and also it is not detected by any security tools longer time period

It is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time.

APT attacks are initiated to steal data rather than cause damage to the target organization's network.

Mitigation - ATP (Advanced threat prevention) solutions, AV/ EDR , NGFW , Malware Analysis Tool

Example Group – APT , Cha Cha – 2019 or 2020 , Eternal blue or etneral romance- 2017 , Regila – 2021 , Pegasus (These are ex for hacking groups)

Phishing E – Mail Attacks

Attacker will trick the end user by sending an email and he will gain unauthorised access or sensitive data exposure. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

It occurs when an attacker, act as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

Log sources are SMTP Server , Email gateway , Firewall , proxy

Symptoms of phishing E-Mails

- Lottery Mails
- Gift Cards
- Voucher cards
- Malicious URL link
- Invoice email
- Malicious domains (Fake Domain)
- Job opportunities
- Spelling Mistakes

Types of Phishing (Interview Questions)

Spear Phishing – Attacker will trick the one user or group of users or couple of users by sending a phishing email

Spear phishing is a phishing method that targets specific individuals or groups within an organization. It is a potent variant of phishing, a malicious tactic which uses emails, social media, instant messaging, and other platforms to get users to divulge personal information or perform actions

that cause network compromise, data loss, or financial loss. While phishing tactics may rely on shotgun methods that deliver mass emails to random individuals, spear phishing focuses on specific targets and involve prior research.

Whaling - Attacker will trick the end user by sending an email to board of director or senior level executives

A whaling attack, also known as whaling phishing or a whaling phishing attack, is a specific type of phishing attack that targets high-profile employees, such as the chief executive officer or chief financial officer, in order to steal sensitive information from a company. In many whaling phishing attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker.

EX; CEO , CTO, CFO,CIO, CISO

Smishing - sending a text or messages to the end users and gaining the confidential

Smishing is a form of phishing in which an attacker uses a compelling text message to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphone.

Vishing - Attacker will call the end user and gaining unauthorised access or money

Vishing is short for "voice phishing," which involves defrauding people over the phone, enticing them to divulge sensitive information. In this definition of vishing, the attacker attempts to grab the victim's data and use it for their own benefit

Malware phishing - Attacker will attach malware files in the email and send it to users and compromise the system and gain the unauthorised access

Phishing often involves e-mails containing links to websites that are infected with malware.

URL Phishing - Attacker will send malicious URL link to the end user and once end user is clicking on malicious URL links systems will get compromised and finally attacker will gain unauthorised access (Ex; www. Google.com)

Mitigation –

Email security Gate way or E-Mail security solution –
AV/EDR
NGFW
Proxy
Tools

- Proof point
- Iron port – cisco
- Mime Cast
- Outlook 365 ATP

One of the end user system got compromised by Ransome wear attack what will you do? (Interview Question)

Back up the data we have to check whether back up configuration file existed are not indirectly we have to do containment & should do formatting of the system then we have to import the backup configuration to the respective laptop

Interview Questions

- One of the end user system is got compromised by virus . how can you do investigation?
- One of the server got compromised by virus . how can you do investigation?
- One end user system got compromised ransomware attack . how can you do investigation?
- Do you have any idea on malware analysis and how can you do malware analysis?
  Here we do Manual & Automated Malware Analysis Alert tool has given notification that is nothing but Automated

- Phishing email (Ex Attacker sends once at a time 100 Phishing email what do u do?

Authentication Failure Attack

Dictionary Attack

attacker will use different dictionaries using trial and error method he compromised end user system or account. Attacker will gain unauthorised access or sensitive data exposure

A dictionary attack is a brute-force technique where attackers run through common words list file and phrases, such as those from a dictionary, to guess passwords. The fact people often use simple, easy-to-remember passwords across multiple accounts means dictionary attacks can be successful

https://www.hacksplaining.com/glossary/dictionary-attacks

Basically, it is trying every single word that is already prepared. It is done using automated tools that try all the possible words in the dictionary

Mitigation –

- Complex passwords or strong passwords
- Upper case
- Lower case
- Digit or number
- Character or symbol
- Length of the password more than 8 characters
- Password rotation should be 3 months

MFA (More than one way of authentication is called MFA) EX; when ever your login into the system it has to ask either google authenticator or Microsoft authenticator or OTP may be calling or captcha & so on reason it has ask one more security question

Account lock out policy (More than 3 to 5 Attempts if login gets fail then automatically the Account need to get lock)

We have to change the default password asap (Password should change as soon as possible)

When ever we are entering the passwords it will store in cache or buffer in the scenario if we are able to enter user name & password backend process files it will keep on trying to login. Here we no need to authenticate anything so it

will existing user name & password it will try to authenticate even we have to clear cache as well

From disabled account login failures are coming how can you mitigate (Interview question)

We should check is this from Internal IP or External IP if it is internal Ip we need to investigate what is the activity it means account status whether is active or inactive we have to identify that one and we have to identify make sure the clear cache that should be reset the password as soon as possible If the account is existing is active

If it is from External we have to check the reputation from MX tool , Virus Tool.com , or hybrid analysis.com and finally we have to block the particular Ip address from the firewall so this what we have to do

This alerts will generated through log collection & integrity all the employee logs to SIEM Tool

Brute Force Attack

Attacker will use trail and error methods to guess the password and also using different permutations and combinations where Attacker makes repeated attempts with some calculated guesswork

And then finally he will compromise the end user system and he will gain unauthorised access. Whereas Brute force Attack are automated where the software automatically works to login with credentials

Log sources Every windows events , DC – Domain controller, End user system, Active Directory

Mitigation –

- Complex passwords or strong passwords
- Upper case
- Lower case
- Digit or number
- Character or symbol
- Length of the password more than 8 characters
- Password rotation should be 3 months

MFA (More than one way of authentication is called MFA) EX; when ever your login into the system it has to ask either google authenticator or Microsoft authenticator or OTP may be calling or captcha & so on reason it has ask one more security question

Account lock out policy (More than 3 to 5 Attempts if login gets fail then automatically the Account need to get lock)

We have to change the default password asap (Password should change as soon as possible)

You're the security Analyst you have discovered number of user names & attempts in the log file what the attacker is trying to achieve (Interview Question)

Attacker is trying where it could be Dictionary Attack & Brute Force Attack

Whenever any brute force attack is coming through as alert notification as security analyst what investigation process you will do? (Interview Question)

Once the particular alert is received 1st I will classify the instant is it internal attack or external attack who is doing the attack if it is insider threat or internal attack I will identify the Ip address of the machine & I will identify the user name of the machine

If I don't know the user name of the machine then I will contact network admin team or Active directory to get the respective end user machine name

Then after that I will contact the end user whether he has done the activity by entering the wrong password so whatever response is coming back I will attach as a evidence then I will consider as the evidence is false positive then I will close the incidence that is option 01

Option 02 side once again if it is false positive or true positive if it is any attack is coming from public IP other than pvt IP & I will check reputation of the IP after checking the reputation of the IP I will block particular reputation of IP to the respective firewall without compromising alert has come

If it is from Public Ip then I will check reputation of the public IP then 1st I do the containment which means disconnecting from the network then I will change the password because the attacker will steal the data then i do additional investigation

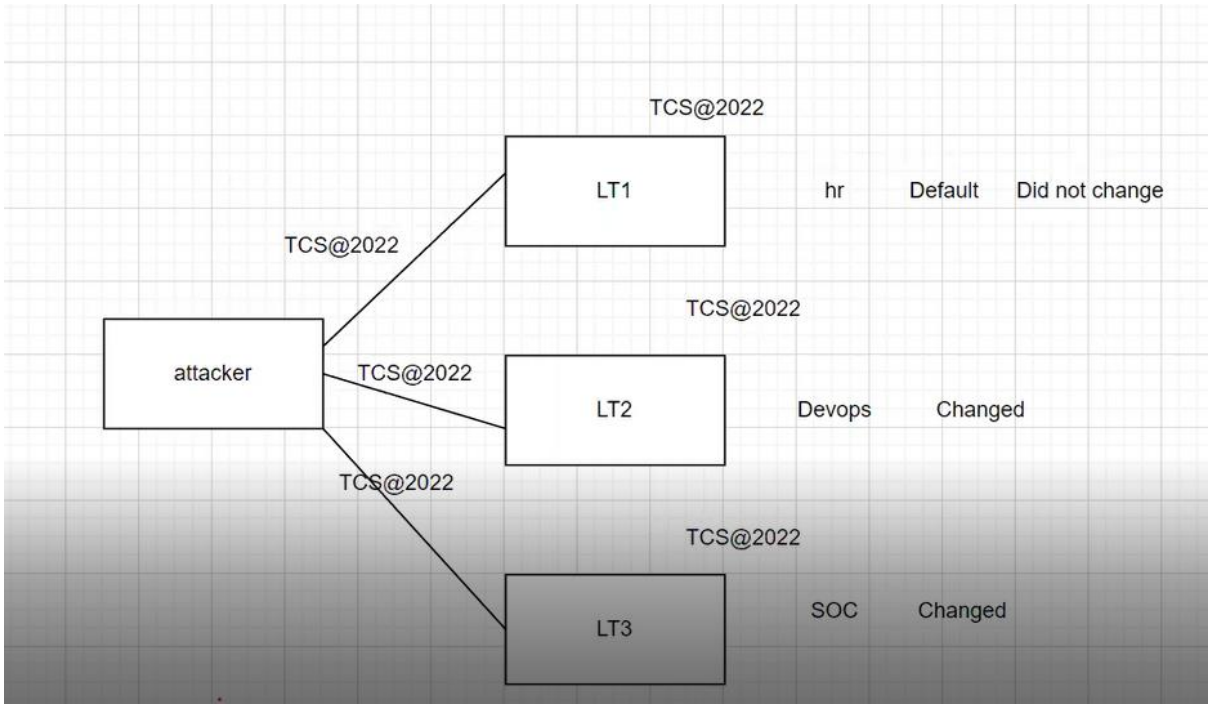
False positive tool will give the wrong results its like fake incident
True positive Real attacker will get compromise by end user system we have to take forensic analysis

Password Spray Attack –

Attacker will spray the same passwords for multiple systems at a time and he will compromise one system or more than one system and he will gai unauthorized access.

It is a type of brute force attack. In this attack, an attacker will brute force logins based on list of usernames with default passwords on the application. For example, an attacker will use one password (say, Secure@123 or TCS@2022) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

This attack can be found commonly where the application or admin sets a default password for the new users.



Mitigation –

- Complex passwords or strong passwords
- Upper case
- Lower case
- Digit or number
- Character or symbol
- Length of the password more than 8 characters
- Password rotation should be 3 months

MFA (More than one way of authentication is called MFA) EX; when ever your login into the system it has to ask either google authenticator or Microsoft authenticator or OTP may be calling or captcha & so on reason it has ask one more security question

Account lock out policy (More than 3 to 5 Attempts if login gets fail then automatically the Account need to get lock)

We have to change the default password asap (Password should change as soon as possible)

In windows what different types of log we can collect? (Interview Question)

Well Total 05 we have those are like

- Application
- Security
- Setup
- System
- Forward Events

Security is for Auditing part it shows login success or login failure

Setup is for configuration related something like we are installing some software that is nothing configuration related

Application whatever on top of the laptop or server that running application its related to Application log

System it is nothing but health utilization part I means like what is the health of the system & so on

Event ID

Always we can see in the Security Logs only

- 4624 – Authentication Success
- 4625 – Authentication Failure
- 4672 – Special Log on
- 5379 – User Account Management
- 5061 – System Integrity
- 5058 – Other system Events

VPN Authentication login Failure Attempts

For same users for same location within short span of time that means ex; working for IBM Hitech city in this situation login attempt coming from hi-tech city & 2nd login attempt coming from Madhapur 3rd login failure from Kondapur etc

Within the short span of time login failure are coming from different locations ex; 1 hour or 2 hour whatever may be 5 hours login attempt coming from hitech city, Madhapur are may be anything this activity should suspect as Abnormal or malicious activity

We should check this Authentication failure is coming from where is it from Internal Ip are from external IP

If it is from Internal Ip need to verify from End user whether really have done

Use Case –

Use case is for different types of scenarios every attack is one Use Case & every scenario is one use case. In the organization level will have the documents like SOP (Standard operating procedure document), Play Book or Run Book when ever any attack is coming from to the SIEM tool it bifurcate what L1 , L2 & L3 Team has to do

Flooding Category

Flooding means sending so many requests. Attacker will send so many requests to the targeted machine. Finally, it gets crash or it will get compromise because it cannot handle so many request & finally the server is unavailable not only server it is applicable to Application as well, as per CIA traid flooding category of the attacks are Availability issues

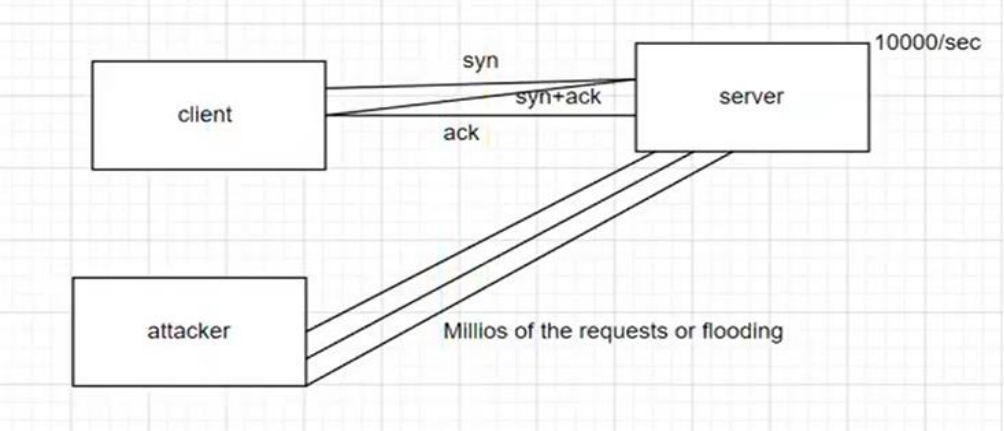
1. TCP flood/Syn Flood

Attacker will send millions of the flooding of the TCP or SYN requests to the targeted machine or server or application or DB. Because of the flooding of the request's server cannot handle these many request and finally server will become unavailable or outage or unresponsive.

A SYN flood attack is a type of denial-of-service (DoS) attack on a computer server. This exploit is also known as a *half-open attack*.

SYN floods are one of several common vulnerabilities that take advantage of TCP/IP to overwhelm target systems. SYN flood attacks use a process known as the *TCP three-way handshake*. As part of the handshake, the client and server exchange messages to establish a communication channel.

Reason why we called TCP 3-way hand shake 1st request is synchronization request so that's why syn flood is also called as TCP flood attack



Mitigation –

1) Implement Anti dos or Anti Ddos tool in parallel to isp router. Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
2)Implement NIDS/NIPS tools . Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
3) Configuring Rate limit or throttling in server which is completely assumption only (Defying per sec how many requests it should be accepted)
4) Configuring Rate limit or throttling in Firewall (Defying per sec how many requests it should be accepted)

Tool (These are contract based were look after when we don't have sufficient sources in the organization)

- Akamai
- Barracuda
- Imperva
- F5

These will generate the alert those will detect both based on the parameter those are identified based on signature detection mechanism (Signature means already known attack)

Whenever any attacker Ip address is aware of Anti Dos & Anti Ddos tools automatically it will block particular IP Address in the Anti Dos & Anti Ddos based on signature based

2. DOS (Denial of service) – Denial of service means service unavailable or service rejection

Denial is nothing but rejection

Single attacker will target the single server and he will send millions of the flooding of the requests That may be anything like (TCP, SYNC, UDP, ICMP, ARP) to the target server. Because of this reason server will damage or crash or unresponsive. And finally because of unauthorised attacker legalised or legitimate users will loose the service.

Log sources Firewall , NIDS/NIPS, Anti Dos & Anti DDOS , Backend server logs if we integrate log sources log to SIEM tool it will generate one of the alert whenever any attack will come

Mitigation –

1) Implement Anti dos or Anti Ddos tool in parallel to isp router. Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
2)Implement NIDS/NIPS tools . Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
3) Configuring Rate limit or throttling in server which is completely assumption only (Defying per sec how many requests it should be accepted)
4) Configuring Rate limit or throttling in Firewall (Defying per sec how many requests it should be accepted)

3. DDos (Distributed denial of service)

Multiple attackers or single attacker from multiple system will send the flooding of the traffic or requests (TCP, SYNC, UDP, ICMP, ARP) to the target server. Because of this reason server will become damage or unresponsive or unavailable. Finally because of illegitimate attacker legitimate users will loose the services.

Mitigation –

1) Implement Anti dos or Anti Ddos tool in parallel to isp router. Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
2)Implement NIDS/NIPS tools . Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
3) Configuring Rate limit or throttling in server which is completely assumption only (Defying per sec how many requests it should be accepted)
4) Configuring Rate limit or throttling in Firewall (Defying per sec how many requests it should be accepted)

4. ICMP (Internet control message protocol) or ping of flood

Attacker will send the flooding of the ping requests to the targeted machine and finally neighbour or peripheral device will respond back properly or unresponsive

A ping flood is a DOS attack in which the attacker attempts to exploit a targeted device with ICMP echo-request packets, causing the target to become inaccessible to normal traffic. When the attack traffic comes from multiple devices, the attack becomes a DDoS or distributed denial-of-service attack.

ICPM which is utilized in a Ping Flood attack, It is an internet layer protocol used by network devices to communicate. The network diagnostic tools traceroute and ping both operate using ICMP. Commonly, ICMP echo-request and echo-reply messages are used to ping a network device for the purpose of diagnosing the health and connectivity of the device and the connection between the sender and the device.

Mitigation –

1) Implement Anti dos or Anti Ddos tool in parallel to isp router. Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
2)Implement NIDS/NIPS tools . Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
3) Configuring Rate limit or throttling in server which is completely assumption only (Defying per sec how many requests it should be accepted)
4) Configuring Rate limit or throttling in Firewall (Defying per sec how many requests it should be accepted)

5. Ping of death

Attacker will send oversized ping packet to the targeted machine and finally server will become unresponsive.

The attack is a denial-of-service (DoS) attack, in which the attacker aims to exploit a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash. The original ping of death attack is less common today. A related attack known as an ICMP flood attack is more prevalent.

Mitigation –

1) Implement Anti dos or Anti Ddos tool in parallel to isp router. Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block

2)Implement NIDS/NIPS tools . Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
3) Configuring Rate limit or throttling in server which is completely assumption only (Defying per sec how many requests it should be accepted)
4) Configuring Rate limit or throttling in Firewall (Defying per sec how many requests it should be accepted)

6. MAC Flood Attack

Attacker will send millions of the dummy frames to the targeted machine (that is Switch) and finally switch will become exhaustive or unresponsive.

So here the Attacker is connected to a switch port floods the switch interface with very large number of Ethernet frames with different fake source MAC address.

MAC Flooding is not a method of attacking any host machine in the network, but it is the method of attacking the network switches. However, the victim of the attack is a host computer in the network.

Mitigation –

1) Implement Anti dos or Anti Ddos tool in parallel to isp router. Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
2)Implement NIDS/NIPS tools . Whenever any flooding of the requests sent by attacker based on signature-based detection and based behavioural it will detect and it will block
3) Configuring Rate limit or throttling in server which is completely assumption only (Defying per sec how many requests it should be accepted)
4) Configuring Rate limit or throttling in Firewall (Defying per sec how many requests it should be accepted)

Spoofing Attacks

Spoofing Is nothing but on behalf of original user. So, Attacker will send the request then finally attacker will gain the unauthorised access. Which means impersonating original user or on behalf of original user or employee will send the request to the End user system, server, Database, application , email and finally response will get it back.

Spoofing attacks can take many forms, from the common email spoofing attacks that are deployed in phishing campaigns to caller ID spoofing attacks. that are often used to commit fraud. Attackers may also target more technical elements of an organization's network, such as an IP address, domain name system (DNS) server, or Address Resolution Protocol (ARP) service, as part of a spoofing attack.

Types of Spoofing Attacks

- IP Spoofing
- Email Spoofing
- ARP Spoofing or Poisoning Attack
- DNS spoofing or DNS cache poisoning or DNS amplification attack

IP Spoofing

Attacker will mask original identify of Ip address of the end user and on behalf of original user or employee will send the request and finally he will gain unauthorised access.

Masking of ip is also called as TOR ip (TOR Nothing but onion router ip)

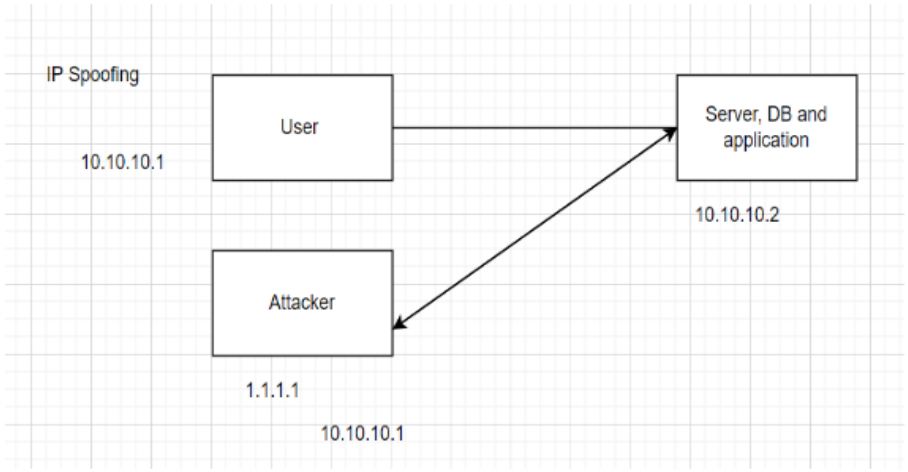
To eliminates or Mitigate we have to use

stateful inspection (Whenever any packet is entering into the organization level it will open the packet & it will check the exact status of the packet whether it is syn stage or syn, ACK stage or ACK Stage so that is the state full inspection

Deep packet Inspection – This is NGFW feature (Whenever any packet whether inbound traffic or out bound traffic is entering into the firewall level each & every packet it will open the packet will see any spoofed IP Address is available from the attacker or may be internal IP address itself & in case if any masked IP address is available that Masked IP Address will be blocked automatically based on the behaviour pattern , signature Text mechanism.

DE Packet is capable for identifying the malware scanning as well. If packet contains any malicious malware software program code it will scan particular piece of written code that is nothing message , or payload it can identify & block the particular activity

IP spoofing



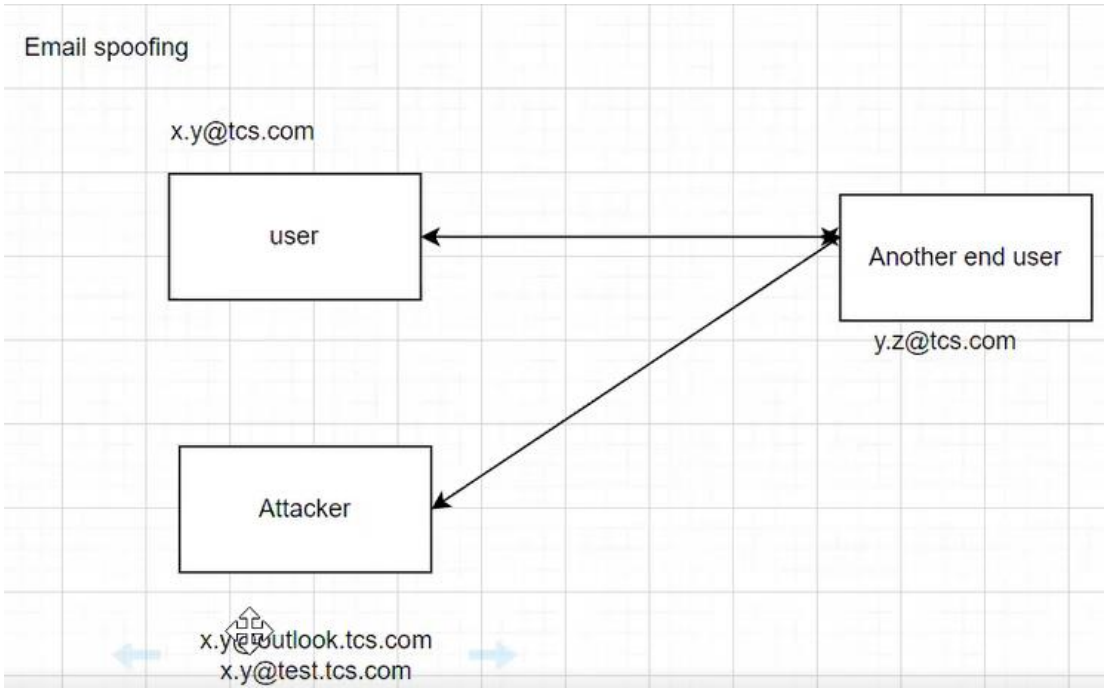
It is a type of malicious attack where the threat actor hides the true source of IP packets to make it difficult to know where they came from. The attacker creates packets, changing the source IP address to impersonate a different computer system, disguise the sender's identity or both. The spoofed packet's header field for the source IP address contains an address that is different from the actual source IP address.

IP spoofing is a technique often used by attackers to launch distributed denial of service (DDoS) attacks and man-in-the-middle attacks against targeted devices or the surrounding infrastructures. The goal of DDoS attacks is to overwhelm a target with traffic while hiding the identity of the malicious source, preventing mitigation efforts.

E-Mail Spoofing

E-Mail spoofing is subset of phishing email so. On behalf of original user attacker will mask the domain name of original end user or employee and send an email to other employee or another user and finally he will get response back from another employee or another user.

Email spoofing is a form of cyber-attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source. Email spoofing is a popular tactic used
in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a known sender. The goal of email spoofing is to trick recipients into opening or responding to the message.



Mitigation steps

Email security solution or email Gateway (Proof point, mime cast, Cisco iron port, O365 ATP)
Whitelisting or block listing of domain names in DNS or SMTP server or firewall or proxy as per our business requirement

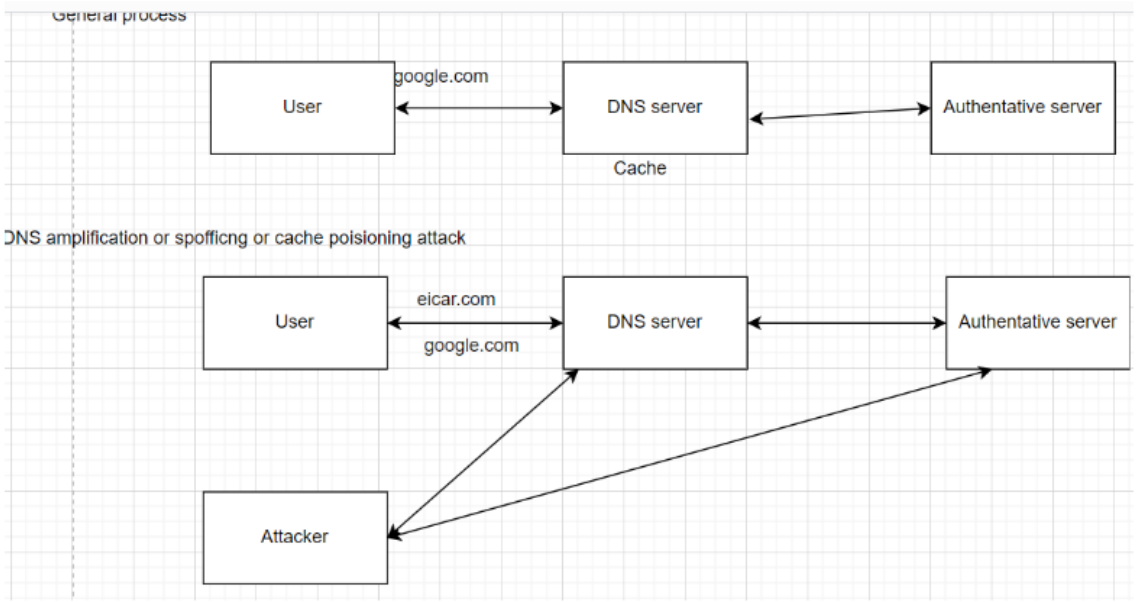
DNS spoofing or DNS cache poisoning or DNS amplification attack

Here the Attacker will do mask or spoof original end user requested domain name to the DNS server by compromising the DNS server or Authorities server. Finally, when the user is requested the domain name, & the request will go to attacker and attacker will create deface or fake or malicious websites or domain names and when the user is clicked on malicious domain names as per cyber kill chain process & the end user will system get compromised and finally attacker will gain unauthorised access

DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites. DNS cache poisoning is also known as 'DNS spoofing.' IP addresses are the 'room numbers' of the Internet, enabling web traffic to arrive in the right places. DNS resolver caches are the 'campus directory,' and when they store faulty information, traffic goes to the wrong places until the cached information is corrected. (Note that this does not actually disconnect the real websites from their real IP addresses.)

EX ; Imagine that, as a senior-year prank, high school seniors change out all the room numbers on their high school campus, so that the new students who don't know the campus layout yet will spend the next day getting lost and showing up in the wrong classrooms. Now imagine that the mismatched room numbers get recorded in a campus directory, and students keep heading to the wrong rooms until someone finally notices and corrects the directory.

DNS spoofing



Mitigation

- Implementing DNS security at DNS server level (Agent or agentless)
- Implementing malicious domains block listing in DNS server or SMTP OR NGFW and Proxy
- Should do Regularly clear the cache

ARP spoofing or ARP poisoning ARP cache attack

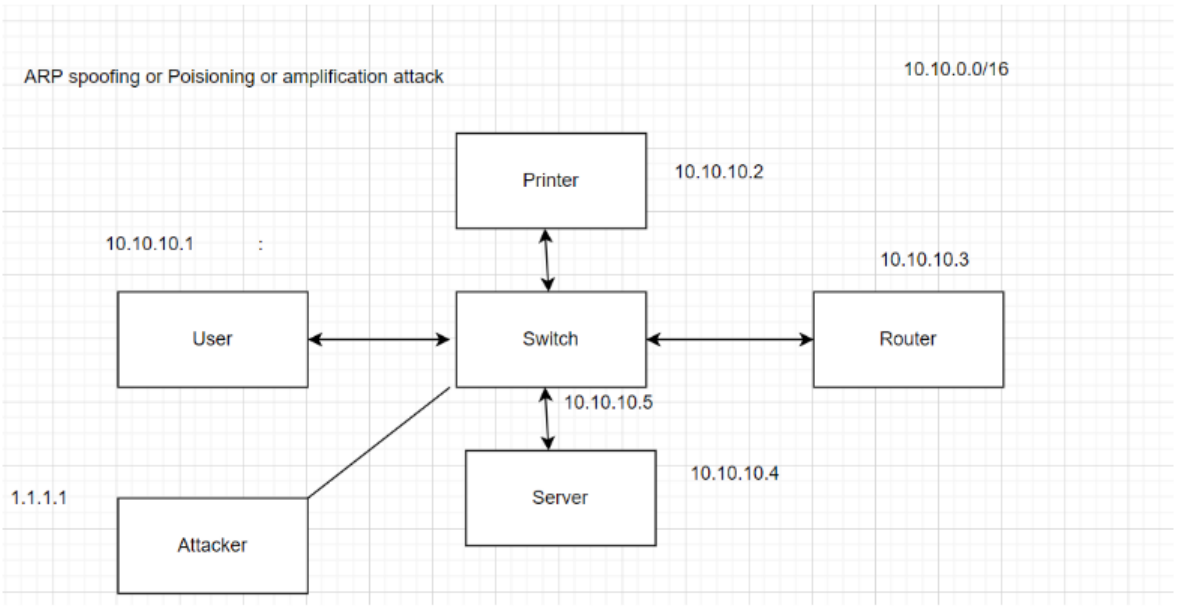
ARP poisoning (also known as ARP spoofing) is a cyber attack carried out through malicious ARP messages , An ARP attack is difficult to detect, and once it's in place, the impact is impossible to ignore.

Attacker will mask original ARP request of the end user and send the request to switch or appropriate device connected in the network and finally he will get response back from appropriate device. In such way he will gain unauthorised access.

The Attacker that successfully implements either ARP spoofing or ARP poisoning so that attacker could gain control of every document on

our network. we could be subject to spying, or the traffic could grind to a halt until we give the hacker what's requested for ransom.

ARP spoofing or poisioning attack



Mitigation

- Clearing cache of the ARP table in FW, Router or switch
- Implementing NGFW
- Whitelisting only allowed traffic in router and switch level

Other Attacks

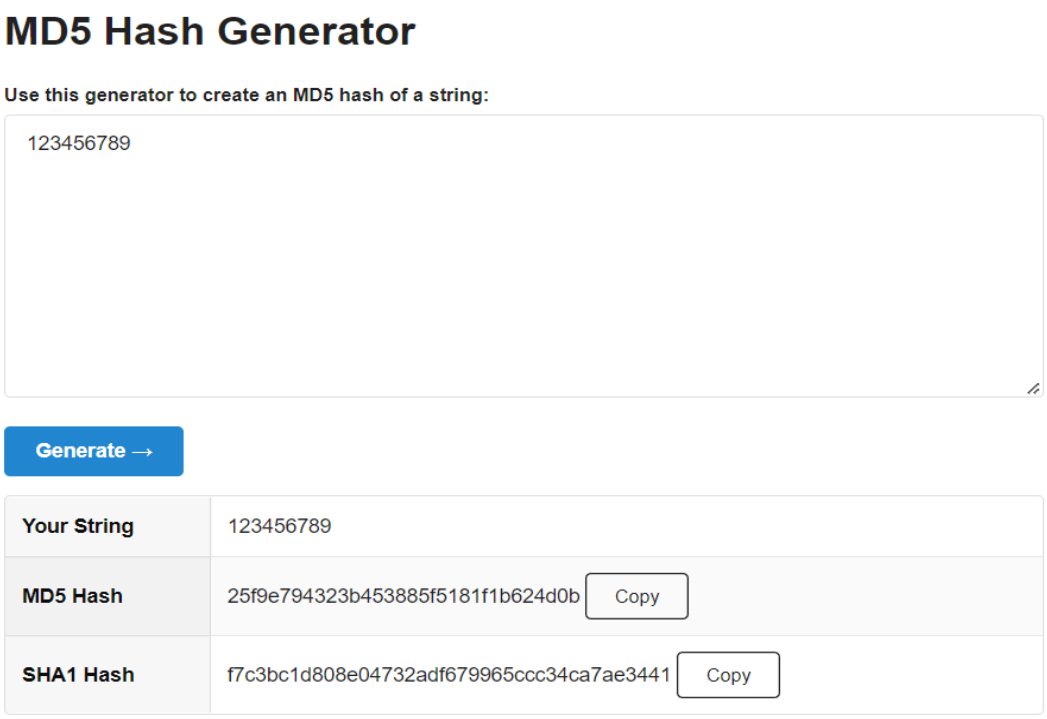
Rainbow Table Attack

It is a password cracking method that uses special table (Rainbow table) to crack the password hashes in the database

A rainbow table is a hash function used in cryptography for storing important data such as passwords in a database. Sensitive data are hashed twice (or more times) with the same or with different keys in order to avoid rainbow table attacks.

The passwords in a computer system are not stored directly as plain texts but are hashed using encryption. A hash function is a 1-way function, which means that it can't be decrypted. Whenever a user enters a password, it is converted into a hash value and is compared with the already stored hash value. If the values match, the user is authenticated

https://www.md5hashgenerator.com/ (Hash Value Generator)



Password - 5f4dcc3b5aa765d61d8327deb882cf99

123456789 - 25f9e794323b453885f5181f1b624d0b

Attacker will take the particular Hash value & will create one table in such a way attacker will try to compromise the data base passwords in a table format. Attacker will provide the list of the passwords commonly use dictionary use the hash values in the form of table finally attacker will try to get compromise by using the trail & error method so nothing but cracking the passwords basically

Mitigation

Salt Value (Interview Question) – Salt value means it is nothing but anonymous number basically in simples words randomly it will generate the numbers. This value generated cryptographically to secure the function that is added to the input hash functions .

To create the unique number that is nothing but salt value Randomly generated unique value to keep passwords safe and secure. It contains combination of characters and numbers, Infront of the hash value salt value will be added and it is stored in the DB

MFA , Complex Passwords , Salt value should be added Infront of hash value when the passwords storing or retrving from the DB

MITM (Man in the Middle Attack)

In between user and application attacker will come as a middle man and he will take the session and he gain unauthorised access

Most of the MITM is applicable to Authentication failure category or Application related ex; Session Hijacking (Taking the existing token number login to the respective application then getting the unauthorised access , VPN authentication failure , Broken Authentication ,Broken Access control it part of application OWAS Top 10

Mitigation

SSL (Secure socket Layer) /TLS (Transport layer security)- Purchased CA certificate it provides like (Confidentiality, encryption, non-repudiation, authenticity)

Google.com (Is main domain) these are for certification purchase approx. cost 120 $ to purchase any domain this cost for one year

- Sub domains
- Youtube.com
- Googlemeet.com
- Play store
- Maps

Heart Bleed

It is applicable only to the outdated Open SSL versions it is under practice here attacker will identify the vulnerabilities or weakness under the particular outdated version and finally attacker will compromise particular vulnerability

In 2014 this attack occurred

Mitigation

We have to Upgrade Open SSL version - (3.0.5 as per July 2022)

Poodle Attack (Oracle) - Padding oracle on downgraded legacy (Old) encryption

This attacker will occur when we are using outdated SSL/TLS legacy encryptions. it is an exploit used to steal information from secure connections, including cookies, passwords and any of the other type of browser data that gets encrypted as a result of the secure sockets layer (SSL) protocol.

This is applicable to oracle Data Base side initial will identify the issue that's why it a poodle attack on the oracle data base

SSL Version (Out dated)	TLS Version
1	1
1.1	1.1
1.2	1.2
	1.3

Latest version of TLS version is 1.3 (Interview Question)
1.2 & 1.3 Are updated remaining all are outdated versions

Strong mechanism like DH dhepy Helmen, RSA , ECC – Elliptical current cryptography , Kanp sack – 4096

Mitigation –
We have to use Strong ciphers with strong encryption
Should use the Latest stable TLS versions

Lateral Moment (Interview Question)

It is technique that attacker use , after compromising a system or an end point to extend that particular infection to other hosts or other systems as well
Lateral movement is a means to an end; a technique used to identify, gain access to and exfiltrate sensitive data.

after gaining initial access, it move deeper into a network in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

Ex; Credentials stealing or credentials skurfing , Phishing emails (Spear phishing)

Mitigation

- Email gateway or email security solutions
- AV/EDR
- NGFW
- Strong password policies

Mimi Katz attack (Interview Question)

Attacker will use hacking tool to extract the passwords, hashes, pin numbers and attacker will gain unauthorised access (It is applicable windows os- 32 it and 64bit)

Attackers commonly use Mimi Katz to steal credentials and escalate privileges: in most cases, endpoint protection software and anti-virus systems will detect and delete it. Conversely, pen testers use Mimi Katz to detect and exploit vulnerabilities in your networks so you can fix them.

Mitigation

- AV/EDR TCP Dump Analysis
- NGFW Memory Dump Analysis

END Point Security or END Point Protection (EPP)

EPP- Whatever security solutions or access controls we are providing end points or host machines called Epp or end point security

END Point -End point is nothing but end user machine or host machine or employee machine or systems

Example End points

- Laptop
- MacBook
- Work station
- Desktop
- Servers
- Mobiles

Whatever security solutions or preventive mechanism implementing these end points will called as End Point Protection

End Point Security solutions

- AV/EDR (Next gen AV)/AM – Anti Malware (It is must tool we have to implement in organization)
- HIDS/HIPS (It is dedicated to Host)
- Encryption (OS encryption)
- DLP (Data loss or data leak prevention)
- FIM(File integrity monitoring)
- MDM (Mobile device management)

BYOD (Bring your Own devices) – It means personal laptop entire our own
BYOL (Bring your own license) - It is applicable to cloud

Licensing

Based on total number of end points

Devices Names	Number of Devices	Cost approx. $
Laptop	2000	05
Macbook	1000	10
Work station	500	05
Desktop	500	05
Server	1000	05

Total -- 5000

License may purchase for 1 year or 3 years, or 5 years
License we have 2 types Enterprise & Normal

Enterprise – This is used for the Big organization
Normal – This is used for basic

Anti - Virus / EDR

Requirements

EX; SBI wants Anti - Virus / EDR

So SBI will release the Tender file or RFP Request for proposal couple of initial things will do by SBI like Initial screening or proof of concept
Every organization will have

Roles	TCS (Budget 100k $	Infosys (125k)	Accenture (70k)	Wipro (90k)	
Sales	Sales	Sales	Sales	Sales	Demo to SBI by all the companies
Pre sales	Pre sales	Pre sales	Pre sales	Presales	Product explanation and POC for SBI 2 weeks
Design	Design	Design	Design	Design	HLD/LLD (It defines the scope of the work)
Implementation	Implementation	Implementation	Implementation	Implementation	Deployment/implementation
Operational (L1,L2,L3)	Operational (L1,L2,L3	Operational (L1,L2,L3	Operational (L1,L2,L3	Operational (L1,L2,L3	SOC duty whenever any incident happen we have to take care

Before releasing the tender SBI will be in touch with respective companies in the above table every company will maintain these roles

As per the above companies respective sales team will coordinate with SBI do you have any requirement for End point security

If they have the requirements SBI will share the requirements to above companies

TCS will do support with Crowd Strike, Infosys Sophos EDR , Accenture Carbon Block , Wipro Micro soft defender

Whenever tenders get release will follow the EDR Granter Quadrant Report only reason they conduct the survey all over world wide. Most of the tenders will request for EDR Granter Quadrant reports only

As per Quadrant have 4 types

- Challengers
- Leaders
- Niche player
- Visionaries

Below report is as per 2021

What is short term goal & Long-term Goal (Interview Question)

My short-term goal I want to become L3 no specific time period but I try by best to get as L3 from L1 & Then I want to become the Implementation guy & then I want to become Architect then finally I want to chief security officer

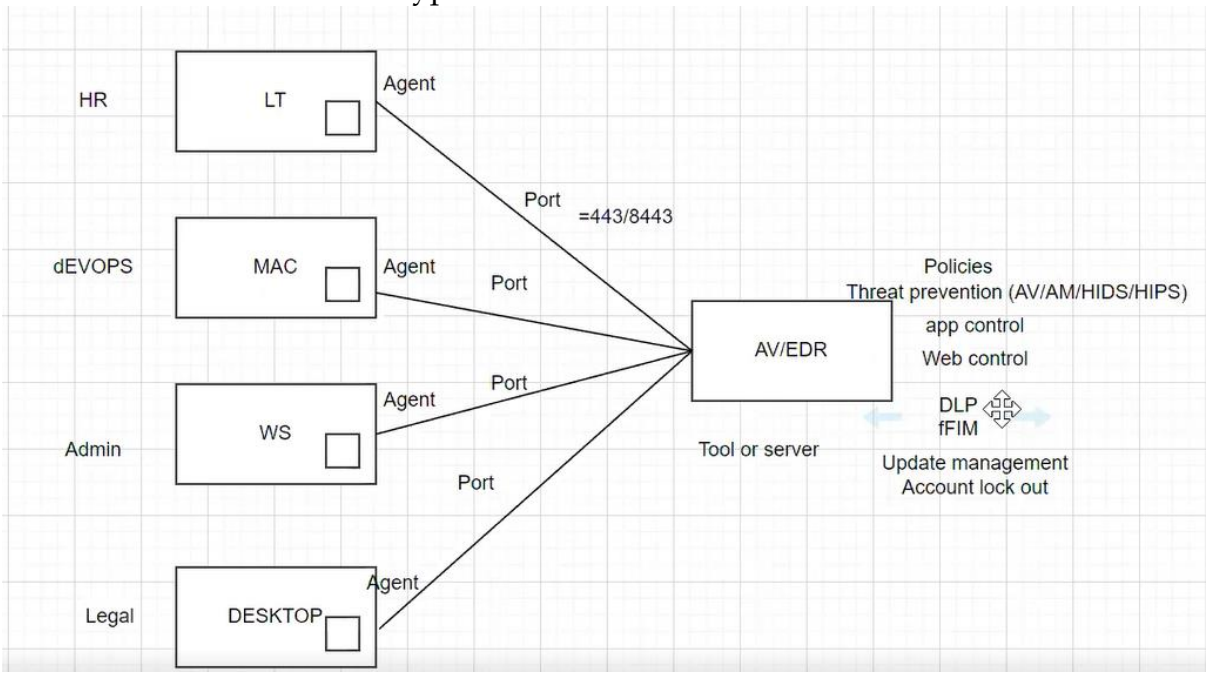
AV/EDR Design or Deployment

AV/EDR Design or Deployment

Deployment will happen here In between the client & server method. So server is nothing but AV/EDR Tool

For Every client machine we have to install AV/EDR agent which is provided by vendor so I mean, Agent is nothing a piece of file at the time of installation it will ask the port number most of the time the port number is 443 for communication purpose couple of vendors will use 8443 so through this port it will communicate & it will speak with AV/EDR this is server basically.

Because whenever any abnormal / malicious or suspicious activity will happen in the end point level. Here agent will communicate to AV/EDR server and based policies configured either it will allow, block, quarantine and clean the files. These are different type of status



AV/EDR agent status

Some times it will be

- Active – It will be completely in active status not in sleeping whenever any abnormal activity is happening in file oriented it will block automatically.
- Inactive Status – May be AV is not in functionality I mean functionality is missing
- Sleeping mode – It will be sleeping we need to do health check-up
- Unknow Status - AV Software installation issues

This is nothing but Health check up every day we have to check what is the status of the every end user machine of the AV/EDR Agent because AV/EDR Agent is a completely inactive stage , sleeping more or unknow status end user may

downloaded any malware of malicious file etc., at the time Attacker will identify the vulnerability then will compromise the end user system

Features or Policies have to configure in EDR tool

Threat prevention - because it has inbuilt feature of (AV/AM/HIDS/HIPS) including Ransome wear attack all this different malware attacks will block by EDR/AV Threat prevention policy
DLP- Data should be classified like what is critical & what is non critical data based on what parameters we have to classify which is based on sensitive & confidentiality of data these two parameters we will classify the data for that
Data classification types are like Confidential , public, Private , Restricted
we have to enable ex PIA Data Based on countries specific which is GDPR - General Data Protection Regulation, It is dedicated to European continent

FIM – If any file is adding, updating or any modification by the end user reason we will come to know who has done what it will generate the EDR tool as notification
App control – What Application should allow what App should block it is dedicated blocking & whitelisting App control
Web control – What we should allow what web should block
Account Lock out – If any trying more than 3 attempts in brute force attack for secure we have to implement account lock out policy
Update Management – It is nothing but enabling AV patch updated (automatic) regularly we get lot of signatures that may be lot of hash values , malware files , Ip addresses , or any malicious URL links it will allow lot of threat intelligence feeds

Actions of malware file status

Clean File – It will identify & scan the clean file
Quarantine - Every vendor will delete the infection file and will keep one file for future reference

Blocking file – Something malicious observe those file contain block file

Allowing of file – It is nothing but similar to clean file

Severity of the AV/EDR alerts (Interview Question)

	Sophos EDR
Critical	High
High	Medium
Medium	Low
Low	
Info	

AV/EDR agent

This software file provide vendor. That software file we have to install on every end user machine

Multiple machines if we want deploy AV/EDR (or If we want to install AV/EDR in lakhs of machines what do you do?) (Interview Question)

SCCM - server centre configuration manager
We have to Segregate the OS versions wise

It is a Windows product that enables the management, deployment and security of devices and applications across an enterprise. Amongst other potential uses, administrators will commonly use SCCM for endpoint protection, patch management and software distribution. SCCM is part of the Microsoft System Centre systems management suite.

SCCM relies on a single infrastructure, with the goal of unifying physical and virtual clients under one umbrella. SCCM also adds tools to help IT administrators with access control. SCCM discovers servers, desktops and mobile devices connected to a network through Active Directory and installs client software on each node.

It then manages application deployments and updates on a device or group basis, allowing for automated patching with Windows Server Update Services and policy enforcement with Network Access Protection. System Centre Endpoint Protection Manager is built into SCCM to secure data stored on those devices.

Detection Method

This is back-end mechanism frontend we can't see

Signature – It is not only applicable to AV/EDR it applicable almost to all the security tool signature means known Attack this will maintained by the vendor in their data base. This is applicable to IDS, IPS, web application firewall, SIEM tool, Proxy for every tool this signature is applicable

Behavioural Pattern – This is nothing but Machine learning & Artificial Intelligence (This is applicable unknown attacks) what exactly end user is accessing

Hash value method – Whenever any file is causing the malware infection that fail has to that Hash value we have to identify & After the checking the verification , validation , reputation checks we have to take the Hash value and we have to block the particular hash value in the EDR Tool

When end user system got compromised what will you do? (Interview Question)

If it is in the same location, we use the pen drive option & copy the particular file uses in the testing environment that only possible in the same location

Right click password protected file it is nothing but we are assigning on of the password to file here hash value get change

When one of your employee came with the laptop saying that system got compromised what will you do? (Interview Question)

In this scenario I use the Task manager or process monitor or process explorer these are 2 websites I check what all the processes are running on , What is the task is running on & what are all the software installed in

Virus total.com I check what is the issue

When we upload the file in Virus total.com after uploading the file we get the option called detail in that we see below information
MD5 use 128 bit
SHA – 1 use 160 bit
SHA – 2 Use 256 Bit
For example 4/65 we get the value here SHA-2 hash value should be blocked

One of the server got compromised through malware what will you do as a security analyst or what is the recent investigation you have done (Interview Question)

In a AV tool one of the end user is downloaded pdf file from the website its an internet facing end user machine & I received the particular alert I gathered the all the who is going impact victim of the IP Address & whether end user system or server where it is located , what is the file name , file size & file category from which website the end user is downloaded. Then I have taken the particular file then I went through the Virustool.com uploaded the file & then I have analysed this is false positive incident

Why your uploading the confidential file in Virus Total.com? (Interview Question)

In our organization along with virus total.com & hybrid analysis.com we have sand boxing environment also sand boxing is nothing but testing environment

Heuristic approach

It is nothing but script control or execution ex; Attacker is trying to created power shell script control related to malware infection can inject any file or excel related files then once end user is clicking on those injected files that script executed file alert generated based on Heuristic approach

Heuristic analysis is an approach to discovery, learning and problem-solving that uses rules, estimates or educated guesses to find a satisfactory solution to a specific issue. While this way of problem-solving may not be perfect, it can be highly successful when applied to computer processes where a quick answer or timely alert is required based on intuitive judgment.

Base Line Method

After installing AV/EDR Tool it will observe approx. 2 months of the traffic on an average based on the peak hours & Non peak hours will check the utilizations of the employee, what exact actions are doing & when ever the base line is crossing it will show the abnormal activity is going on the end user machine it will generate the alert then we can check what exactly is happening

Tools

- Microsoft defender
- Crow strike
- Carbon block (Its Vmwear)
- Sentinel One
- Cylance
- Sophos EDR
- Symantec
- MacAfee
- Trend Micro
- ESET
- Cisco AMP
- Palo Alto

Red colour are the popular tools in the market

Difference between AV/EDR (Interview Question)

Antivirus	EDR
It Has limited Feature	It had Advance Feature
It will do AV/AM scanning and it can detect and prevent the malware infection	It has advanced features like AV/AM, Basic DLP, HIDS/HIPS, FIM, Account lockout policies.
It will use signature, hash value and also baseline method for detection of Malwares	It will use signature, behavioural patter (ML/AI), Heuristic approach, script control, hash value method and baseline method to detect malwares

Anti-virus is not Next generation firewall	EDR will also called Next generation firewall
Anti-Virus doesn't support DLP,FIM,HIDS/HIPS, Application control & Account lock out	EDR Will support entire policies

Sandboxing environment of AV/EDR

It is on-premise / data centre testing environment where we can static analysis of malware and dynamic malware and also reverse engineering

It observe and analyse and code in a safe, isolated environment on a network that mimics end-user operating environments. Sandboxing is designed to prevent threats from getting on the network and is frequently used to inspect untested or untrusted code. Sandboxing keeps the code relegated to a test environment so it doesn't infect or cause damage to the host machine or operating system.

DLP – Data loss prevention or Data Leakage Prevention

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. So Organizations use DLP to protect and secure the data and comply with regulations.

The DLP term refers to defending organizations against both data loss and data leakage prevention. Data loss refers to an event in which important data is lost to the enterprise, such as in a ransomware attack.

Data loss prevention (DLP) -- sometimes referred to as data leak prevention, information loss prevention and extrusion prevention – basically it is a strategy to mitigate threats to critical data. DLP is commonly implemented as part of an organization's plan for overall data security.

Using a variety of software tools and data privacy practices, DLP aims to prevent unauthorized access to sensitive information. It does this by classifying the different content types within a data object and applying automated protection policies

Types of Data

- Critical
- Non critical

Data Classification (Interview Question)

Based on Sensitivity and confidentiality

Types of data classification

- Restricted – Prohibited data should not touch
- Internal – Within the limits only
- Confidential – It based on individual ex; patent right etc.,
- Private – Similar to confidential

How the data can be leaked

- Through External devices or removable devices - Ex; Pen drive, usb, memory stick or hard disk)
- E-Mail - Sending the mails professional to personal and vice versa
- Website - Social network web sites
- Through Cloud

PIIA - Personal identifiable information

(It is one of the GDPR Compliance)

It is the data that corresponds to a single person. PII might be a phone number, national ID number, email address, or any data that can be used, either on its own or with any other information, to contact, identify, or locate a person.

Personally identifiable information (PII) and **personal data** are two classifications of data that often cause confusion for organizations that collect, store and analyse such data.

On the other hand, personal data has one legal meaning, which is defined by the General Data Protection regulation (GDPR), accepted as law across the European Union (EU).

Ex; Account Numbers, Pan numbers, Passport Number, Aadhar card etc.,

PHI Data – Personal health Information

It is the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

PHI is personally identifiable information in medical records, including conversations between doctors and nurses about treatment. PHI also includes billing information and any patient-identifiable information in a health insurance company's computer system.

Protected Health Information is the definition used by HIPAA (Health Insurance Portability and Accountability Act) to define the type of patient information that falls under the jurisdiction of the law. eHealth applications that collect, store or share PHI need to follow HIPAA compliance guidelines in order to be compliant with the law.

Licensing of DLP

Based on total number of end points

Deployment/design / implementation

Agent and server based approach we follow DLP Agent we have to install in each & every end user machine that end user machine will always contact the if any abnormal/malicious activity happen then this Agent will contact the DLP Server & DLP server what ever the policies configured according to that one it will identify what exactly the end user has done it will generate the alert notification that is nothing but Agent & server based approach

Policies configure

- Removable devices
- Website
- Email
- Cloud
- PII – countries specific
- PHI

Who will provide DLP agent

- Vendor

What is Agent

It is a piece of software

Where we have to install

In Every end user machine

DLP Agent status

- Active
- Inactive
- Sleeping
- Unknown

Tools

- Symantec
- Force point
- Digital Guardian
- Micro soft

F5
Trend Micro
MacAfee Epo

3 IDS - Intrusion detection system

It will detect the abnormal activity

IPS - Intrusion prevention system

It will detect and block or prevent abnormal activity

Types of IDS/IPS

- Host Level – Host IDS. Host IPS
- Network Level – NIDS , NIPS
- Wireless level – WIDS , WIPS

Licensing

Based on number of end points

Deployment

Agent and server

Policies

- HIDS/HIPS
- Malware
- C2C Server policies
- Abnormal/Malicious/suspicious

Detection methods

- Signature based
- Behavioural pattern
- Baseline methods

HIDS/HIPS agent status

- Active
- Inactive
- Sleeping
- Unknown

Tools

- Symantec
- MacAfee
- Trend micro --- It is called Tipping point
- Cisco ---- Source Fire
- Vectra
- F5 --- F5 (It very popular)

Under IDS/IPS only we have (Interview Question)

- False positive
- False Negative
- True Positive
- True Negative

Under True Positive (This might be true Incident happened Alert Generate)

- Incident Happen – Yes
- Alert Received – Yes

Under True Negative (Very Dangerous)

- Incident Happen – Yes
- Alert Received – No

Under False Positive (This might be fake no incident but Alert Generated)

- Incident Happen – No
- Alert Received – Yes

Under False Negative (Less dangerous)

- Incident Happen – No
- Alert Received – No

Incident- No, Alert- Yes	False positve	True Positive	Incident Happens	Yes
			Alert	Yes
Incident-No	False negative	True negative	Incident Happens	Yes
Alert-No			Alert	No

4 . FIM (File Integrity Monitoring)

FIM tool will verify adding or deleting or modifying or updating the files content of who has done what.

Licensing of DLP

Based on total number of end points

Deployment
Agent and server

Agent status

- Active
- Inactive
- Sleeping
- Unknown

Tools

- Varonis
- Microsoft
- Carbon block
- Sophos EDR
- Trend Micro
- MacAfee
- Symantec
- Cyber Ark

Detection Method

- Signature
- Behavioural

5 Encryption

Encryption is nothing but Data at rest It is completely entire OS encryption that may be Disk encryption, Entering password or key to entire OS

Licensing of DLP

Based on total number of end points

Deployment

Agent and server

Where we have to install

In Every end user machine

Agent status

- Active
- Inactive
- Sleeping
- Unknown

Tools

- Symantec
- MacAfee
- Trend micro
- Bit locker
- Sophos

Sophos EDR

Sophos EDR – It is a SaaS (Software as a service) – Cloud
Model Number – Not Applicable
Sophos Version - 10.8. 13.42
Linux Agent Server – Core Agent 1.1.10.6
Windows Agent - 2.20.11

Under Sophos it is developing products for different types of customers like

End point protection, Under End Point Protection we have the

- End Point [XDR]
- Server
- Mobile
- Encryption

On the Network side we have

- Firewall
- Wireless monitoring or Wi-Fi monitoring
- Switch but they don't have Routers
- ZTNA (Zero Trust Network Access)

On cloud side we have

- Cloud Native Security
- Work Load Protection

Under Email we have

- Anti – Phishing
- Email Protection (Nothing but E-Mail Gate way)

These are the different types of products developing by Sophos company

Sophos Central

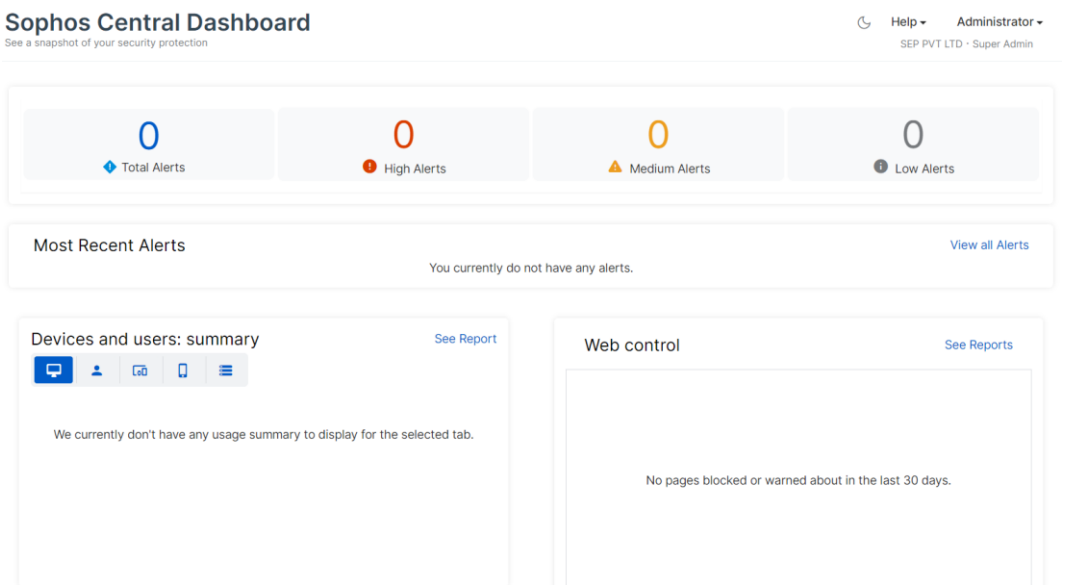
It is not a single tool or single product which means in single centralised console we can see multiple Tools that is called Sophos Central that means from single console we can monitor multiple Tools or Multiple products

Why we should not purchase all products from same vendor (Interview Question)

Mainly I belive For Support purpose because couple of times we don't know how to configure or we don't know troubleshoot something in that scenario we go & we will raise the request with the vendor. Because obviously we take the premium support from the vendor for certain period of time. The main issue will be Time zone it will be critical for the organization level we have no idea that in which time Zone that vendor will provide the assistance continuously we have chase till we catch the vendor

1. Dash Board – Dash board provide the security posture of the organisation security posture means what all the overall summary of threats available like what critical alerts we have

https://cloud.sophos.com/manage/overview/dashboard



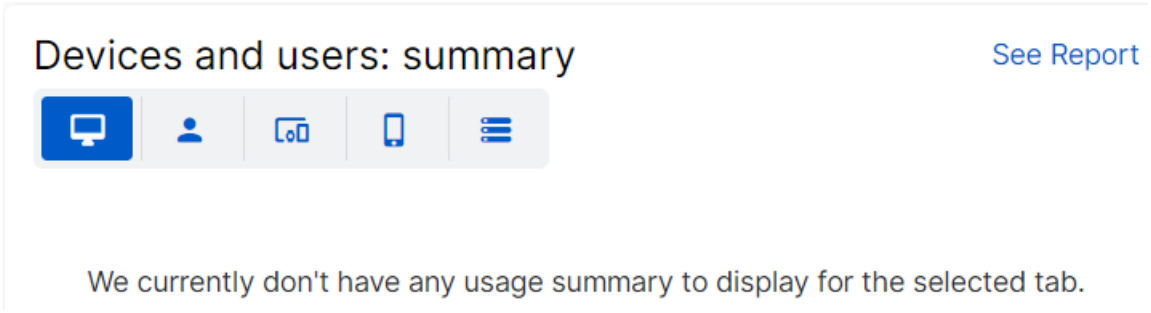
- It over provides all summary of the threats
- It will provide alerts information and most recent alerts
- It will provide summary of the threat's information via bar chart, pie chart, trending chart
- Risk information

What are all the different types of severity of the alerts we will receive in Sophos EDR?

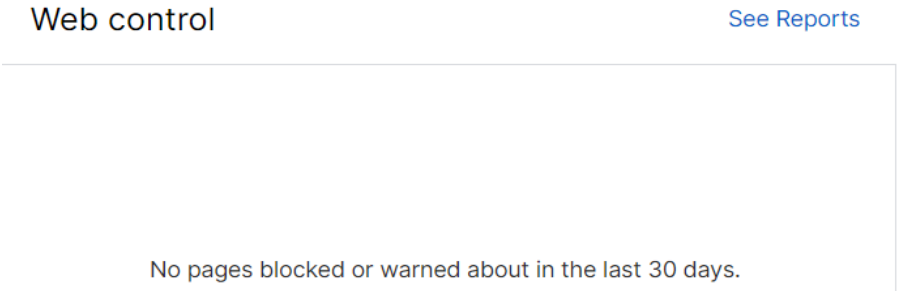
- High
- Medium
- Low

Devices and users ; Summary

It means whatever agents that we install ex we have the 5000 machines including servers, work stations , mac books, laptops etc., all the information we can see here



Web control – Whatever applications we are allowing or blocking we can we under web control



Cloud Security Posture Management – It is dedicated to cloud. If we want to monitor something in cloud environment, we use this

2. Alerts – Whatever we receive regularly

It represents what are the different types alerts received based on severity and also incidents classification and also total number of alerts information

3. Threat Analysis Centre

We have do Analysis basically here like what recent investigation that we have done here, What recent detection that we received nothing but alerts, Most recent graphs its over all graphical representation under that we have like

- Threat Graphs
- Live Discover – Here we will discover the All queries around 382
- Detection
- Investigations
- Preferences – These are basically threat Intelligence like whenever any attack is coming which tool we have to choose it states this

4. Logs & Report

Whatever logs have been generating ex; Audit log who is accessing the tool successful login & failure login called Audit login

This logs we have to integrate with SIEM Tool

5. People

Which means whoever have the access to Sophos EDR Tool we add them here nothing but Role based access control

How to get tool access – We have to raise the ticket in the ticketing tool (Either manager or process experts or L3 team or SME) On behalf of us these people will raise the ticket

Then Manager has to approve the ticket
If we are working for client then client has to approve
Finally, whoever has the access to the tool they will provide access based on role
Role based access control which means RBAC

What is the different types of Role based access control are available in Sophos EDR Tool (Interview Question)

- User – View & Read
- Super Admin - He can do everything and he more privileges access as compared admin
- Admin – We can do anything
- Help Desk
- Read Only

Devices - It will be use for to see how many devices are online and offline based on respective OS wise

Ex; Computers , Mobiles , Server , Unmanaged Devices

6. Global Settings –

This for Admin purpose main purpose is for integration Here only we have to integrate with SIEM Tool through using the API Token Management option click on Add token write the SIEM Tool Integration we have the certain features here in Global settings like

Under Administration

- Directory Service
- Role Management – What are different types of roles we have
- API Credential Management
- Sophos sign-in settings
- Verify domains
- Federated identity providers
- Registered firewall Appliance
- API Token Management (for SIEM Tool Integration) backend mechanism is Pull method

API Access link will be generated, Header & API Access URL Header is generated those links we have to copy then we have to SIEM tool should select the Sophos EDR Tool
Then we enter API Access link & API Access URL Header. Once we are entering between Sophos & respective SIEM tool connection will be established by using TCP

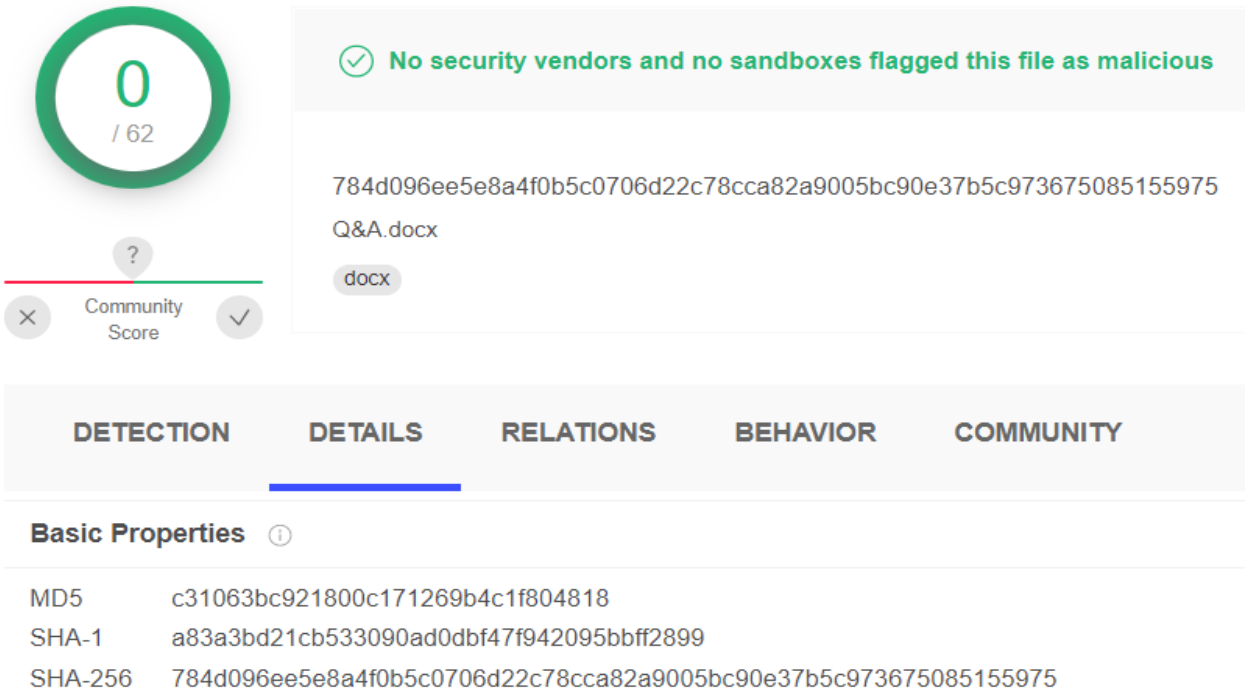
3 way hand shake finally SIEM tool will pull the logs from the Sophos EDR it Is one of the integration method

Under general we have

- Synchronized Security
- Tamer protection
- Website Management
- Proxy configuration – proxy port number 8080 by default
- Global exclusion
- Application allowed
- Manage Update Caches and Message Relays – whenever we get the Anti Virus update we have use this particular option
- Band width Usage – It show much band width that we are utilizing limit we have to keep
- Configure Email Alerts –
- Admin isolated device or containment - Whatever system got compromised we have to do network isolation or disconnecting from LAN
- Forensic Snapshots –
- Malware sample submission – whenever we are not able to find out the malware by using the respective tool like virus total.com etc., then we give to take care by vendor
- Reject Network connection
- Device migration
- Encryption Recovery key search – This option is dedicated to encryption
- Blocked Items –

When we have to block the Hash value (Interview question)

Whenever any file contains malware category of the attacks not only ransomware any system got compromised from malware category of attack 1st I will identify the file name , file size , file type , were it is located & I check how the file is causing the issue and so on , then I take the file then go to the sand boxing environment or virustool.com or hybrid analysis.com then I will check whether the file is infected malware are not. In case if reputation check is showing as infected by the malware then I take the hash value then come to the EDR Tool and will block the hash value. EX – Always we have to take the SHA256 given in the below picture this is from VirusTool.com (This Analysis is happened here)



Once we have the SHA 256 link then we have to block in EDR Tool under Global Setting option under blocked items

Hash value method is under - Global settings>General settings>blocked items

Hash Value Algorithms (Interview Question)

MD5 – 128
SHA1 – 160
SHA2 - 256

We have 2 different types of attacks we have pro active (We are doing pro active threat hunting) & Re active (Its already got compromised

Regularly we can see the threats like where we have to block (Interview Question)

- Malicious Ip address we have to block in Firewall
- Malicious Hash Value we have to block in EDR Tool
- Malicious Domains we have to block in DNS or SMTP or Firewall
- Malicious URLs we have to block in proxy & in Firewall

7. Protect Device

All these are for Implementation part mainly we use for downloads, Downloading of AV/EDR agent. This we have install in every end user machine and also server

8. Account Health Check up

It shows the status of action like Active, Inactive , Sleeping & Unknown
It will represent the health of the check of the end use machines

My Products

Under My products we can see such as

End Point Protection –
Under the end points policies plays the key role if we are enabling the policies then only Anti virus server or EDR Server or tool it will detect or block or it will prevent
As we can see certain like

- Threat Protection – It is combination of HIDS/HIPS Antivirus Malware
- Peripheral Control
- Application Control
- DLP
- Web control
- Update Management
- Windows Firewall

Third party connectors

If we want to integrate with others vendors or Tools this will useful

What is 2FA (2 – Factor Authentication) {Interview Question}
what is symmetric and asymmetric cryptography {Interview Question}

Roles & Responsibilities of EDR is

Health check up of all end points and also all the agent status which means what is the status of the server or end point or laptop or mac book or work station & so on
Whether it is online or offline and also we should check what is the status of the agent active or inactive or unknown or sleeping
Whatever ever alerts we received based on the severity and risk score we have to prioritize the incident

How you prioritize the Incident (Interview Question)

- I give 1st priority to High Alerts , 2nd for Medium & 3rd for Low
- Whatever ever alerts we received based on the severity and risk score we have to prioritize the incident
- We should check what Classification of the attack that we received - Virus, worm, ransomware

- Which system or server or end user machine that alert we received it is nothing but Triage which means gathering the information we need to identify the particular IP Address, Host name , where it is located in which country & this gathering information called Triage this also called IOC & IOA (Indicator of compromise & Indicator of Attacker information)
- Then we should find out the file name (Asset Profiling) , file size (User Profiling) , file category mainly what is the path of the file , where it is downloaded all these information we have to gather
- After Triage we should containment is required are not nothing but network isolation whether the system should get disconnected are not once we are doing the containment then we take care the mitigation steps and finally we have to bring it back to the recovery
- Then I will verify is it false positive or true positive

1 One of the End users got compromise by Ransome wear (Interview Question)
2 One of the Server got compromise by Ransome wear (Interview Question)
3 One of the phishing emails coming via whaling (Interview Question)
Out of these 03 what is your priority

A 2 , 3 , 1 (2 Reason is server will access more number of users because we are not user whether it is Internal or External server if it is external it will be accessing by multiple customers of public ex; Face book it will be access by across world if we don't give the priority in outage will occur as per CIA Triade because customer satisfaction very important and also
Even if it is internal server internal employees are going to impact
3 In whaling its like for Internal employee when the system is getting compromise here lot of business gets damage having high chances to lose the data
1 Here only one person is impacting so that its 3rd priority

What is Business Impact Analysis (Interview Question)
Business Impact Analysis Means Something when it Is getting compromised like Availability issues or confidential related issues or integrity related issue because of this reason lot of impact will be their that may be financial related impact , people related impact or process impact & so on that is business Impact Analysis see it is not only in the operational level issue it will impact on Business Impact Analysis we can do on End Point level , Network level , Application level, physical security level as well ex; Natural calamities like floods, Earth quake , Tsunami etc

You have find the File having the Malware what you do (Interview Question)

Ist i clean the file if any sensitive data is exist otherwise will delete the file then will make it as reference further in future then I will run the anti-Virus scan to verify any infection is existing are not after that, Then I will change the password ,
I will block the hash value in the EDR tool I mean MD5, Sha 1 or Sha 256

When the end user got compromise & server got compromised what you do
For End user we do containment nothing but Network isolation and we can provide backup
For server side we have to do Business Impact Analysis or Risk Assessment
when we have 2 machines are there whatever backup server is there we can make it that primary server and primary server & so on ex one server is available here I will verify who is server owner or asset owner or business owner then we have to ask what is the impact, how much we are going to lose and so on we can disconnect we can do the analysis then we need to identify the what is the Business Impact Analysis or Risk Assessment , what is the financial loss & what is the availability issue & what is the outage or unavailability issues & so on in this situation I will escalate to our manager before the containment then escalation matrix will follow

Eradication/Mitigation

- Infection cleaning
- Deleting the file
- Password change,
- Hash value method,
- Re Run the Anti Virus scan

Recovery – We have to bring it back server or system to abnormal to normal operations

Lessons learned or KB (Knowledge Base) or post motern report – we do the RCA (Root Cause Analysis) nothing but documentation how it is caused , from where we have received , what is the impact, what action we have taken and so on
What is EICAR - the European Institute for Computer Antivirus Research, (Interview Question)

Previous its open sources now This is from Trend micro to check Testing sample files available in EICAR website

In Sophos Our work max will be under Alerts & Devices options only

What is IOC – Indicator of compromise (Interview question)

It will provide the Victim related details like Ip address , Host Name , Device Name, Model number whether end user server or work station or desktop et.c, so on all these are indicators

If we want to receive the alert notification what we have to integrate

SMTP Server

What are the regular alerts we see in EDR Tool (Interview Question)

- Malware related issues
- Configuration related issues
- Virus related
- Worm related & so on

Network Security

Network security –

It will provide security to perimeter or network level security
It is perimeter level security otherwise we can called as overall level security

Under network security we have 3 solutions like

- Firewall
- Proxy
- NIDS/NIPS

Firewall

Under firewall we have certain generation like

Generation firewall

1 Packet filtering –

Allowing & denying the traffic through Router & the Router have the inbuilt feature of which packet to allow & which packet to block it will validate to the User for this we use the packing filtering

Ex; User wants to send an email here Router will scan whether to allow or to block it has the inbuilt feature

Router – configure T (configuration terminal) if you want to enter we have to give this config T
Router model – 2500 ex
Now it will ask
Router – 2500 = Username

Router – 2500 = Password

If want to block 80
Router-2500=IP acl (Access control List) source IP 10.10.10.1 Destination IP facebook.com port number 80 action deny

If want to allow 443
Router-2500=IP acl (Access control List) source IP 10.10.10.1 Destination IP google.com port number 443 action allow

This type of inbuilt feature we have of allowing in Router

2 Circuit Gateway –

Here in between client and server whether tcp 3 way handshake is completing and also in between client and server whether packet retransmission happening or packet dropping or packet allowing

3 Stateful Inspection –

circuit gateway + state of the packet based on the rules configured
In between client and server it will see whether tcp 3 way handshake is completed or not and also what is status of the packet (SYN, SYN+ACK and ACK) based on the rules configured

4 Application Gate way

It also called as proxy gate way or web gate way here It will act as a gateway or bridge between users and application and based on the rules configured either it will or block based on detection methods like signature based and behavioural based

5 UTM (Unified Threat Management)

UTM is also called as Fire wall single firewall will take care the entire threat managing it has the capabilities of Anti-virus scanning , capability of URL Filtering , capability of web filtering , capability of application control , basic ID/IPS Features so on that is nothing but UTM
Firewall will monitor inbound traffic and outbound traffic based on the rules configured either it will allow the traffic or block the traffic

What is the diff between firewall & IDS/IPS (interview question)

What is the diff between firewall & proxy
What is the diff between IDS/IPS & proxy
What is the difference between WAF (Web application firewall) & NGFW
Web application firewall It only prevent 7 application layer attacks that is nothing but OWASP TOP 10 Attack WAF is subset of NGFW
NGFW is Will do the lot of features like

- AV / Malware scanning
- Web filtering (filtering means whitelisting & block listing) or URL filtering or Content filtering or web control or application control
- DNS Filtering
- IP Filtering
- WIFI monitoring
- File Monitoring
- Stateful Inspection

Additional features of NGFW
Deep Packet Inspection
Basic IDS/IPS
Proxy functionality

Firewall features

It will do

- AV / Malware scanning
- Web filtering (filtering means whitelisting & block listing) or URL filtering or Content filtering or web control or application control
- DNS Filtering
- IP Filtering
- WIFI monitoring
- File Monitoring
- Stateful Inspection

2013 till Date current generation fire wall which NGFW

- AV / Malware scanning
- Web filtering (filtering means whitelisting & block listing) or URL filtering or Content filtering or web control or application control
- DNS Filtering
- IP Filtering
- WIFI monitoring
- File Monitoring
- Stateful Inspection

Additional features of NGFW

- Deep Packet Inspection

- Basic IDS/IPS
- Proxy functionality
- WAF (Web application firewall)- OWASP TOP 10 preventive
- VPN

Licensing

- License is based on what is the band width ex 10 G
- Based on how many number of end users EX 10K Users
- how many number of max sessions or going on EX 1 laks
- How many numbers of concurrent sessions are going on (Parallel) EX 20k
- How many number of VPN connections EX 10K
- How many number of concurrent VPN sessions EX 5K

We will provide all the information to the vendor & now vendor will validate the total number will choose the suitable model

Vendors or Tools

- Palo Alto
- FortiGate (Fortinet)
- Cisco ASA
- Juniper
- SonicWall
- Check Point
- Watch Guard
- Cyberoam
- Sophos

Why Palo Alto has the more number of features (Interview Question)

In 2013 Palo Alto came into the Market

Palo Alto	Other Vendors
It is SP3 (Single pass parallel processing) technology it has unique feature	Other vendor follows the Serial processing it will take longer time
It will not block rules or policies based port and protocol but it will block based on application	It will block based on port and protocol
user id, content id and app id	does this capability

Types of Firewalls

- Perimeter firewall (Internet facing) – must device in the organization level

- Internal firewall

Firewall deployment

Layer 3 mode or route mode or NAT mode – this for Perimeter (internet traffic)
Layer 2 mode or switch mode – this for internal traffic
HA mode (high AVAILBILITY) - maintain the primary backup
Virtual wire or Transparent – it is like dummy just for monitoring
Span or Mirror method (This method Is for proof of concept it is mainly used for the testing of the device. It will do only monitoring but it will not block) This will configure by network engineers
Router & Core switch will maintain entire traffic of the organization

What is meant by NAT (interview question)

Zones in the firewall

Internal or Trust Zone --- 100 % secure
DMG or DMZ ----- 50:50:00
Untrust or external or public or internet --- 0

Firewall 02

FortiGate website link
https://fortigate.fortidemo.com/logindisclaimer
User name – demo
Password - demo
FortiGate version number – v7.2 Demo
Firewall is must device to maintain High Availability

Firewall licences

- AV
- URL Filtering or web filtering
- IDS/IPS
- Network DLP
- Malware analysis
- Wi-Fi monitoring
- Spy ware protection
- Premium support (warranty type)

Price will vary from different types vendors

Firewall Manager

It will manage all the firewalls ex; Our office is located in multiple location lets take 10 locations head quarter is Hyderabad remaining 9 locations are branch offices. For ever location we have to purchase the two firewalls so now

- FortiGate- Forti manager
- Cisco - Cisco Firewall manager
- Palo Alto – Panorama

Natting - Network address translation (Interview Question)

It will convert or map private Ip address to public Ip address

Types of NAT

- Static NAT - Single private ip address will map single public ip
- Dynamic NAT - Multiple private ip address will map to public ip
- Port NAT - Along with private Ip address will specify the port number also for the mapping

We Map only internet related phase only we map nothing but from trust to external zone we don't map from DMG to external

Security profiles –

Very Important without this security profiles are like dummy, it cant block anything

- AV
- URL Filtering
- Application control
- Web control
- DNS filtering
- File filtering
- Wifi monitoring
- IDS/IPS
- Proxy
- Waf (web application firewall)

These are default profiles After creating security profile we have to apply these security profiles in the Security policies

Management device or management host name or management ip

If you want to access the device through remotely one of the interface we have to configure as a management ip and have to give host name as well

Fire wall policies

By default every of vendor of the firewall will come up with default rule which is Implicitly deny-Whatever traffic is going on in the firewall everything should be dropped off. Always we have to put bottom of the policy

What is Firewall rule validation (interview question)

It will follow the Top to bottom or top-down approach which means whenever any packet is entering into firewall it will validate the rule numbers 1,2,3 & so on whenever the condition get matches it will stop away ex ; 100 rules we configured so out of these 100 rules whatever rule is matching to our packet there it will stop so that is called firewall rule validation

Rule id	Rule name	Source zone	Destination zone	Source IP	Destination IP	Source user	Destination user	Port	Protocol	Application	Security Profile	Action
1	Allowing of facebbok	Trust	untrust	any	any	any	any	443	https	facebook.com	all	allow
2	Blocking of youtube	trust/internal	untrust	any	any	any	any	443	https	youtube.com	NA	block
3	Enitre category of SN allowing	Trsut	untrust	any	any	any	any	443	https	all	all	allow
4	Blocking ip 1.1.1.1	untrust	trusy	1.1.1.1	any	any	any	any	any	any	na	deny/block
5	Implictly deny	any	any	any	any	any	any	any	any	any	all	deny/block

For block no need to have the security profile its not applicable N/A

Last rule al ways should be implicit deny

Scenarios may be like

Brute force attack , password spray attack , Dos , Authentication failure

Ex Brute force attack is coming from one of the external attacker

Attacker Ip - 1.1.1.1

HR IP - 10.10.10.1

Attacker is trying to compromise the HR Laptop

Once we found the particular IP address we have to block in Firewall level

URL links should block under the proxy level & firewall

Blocking of the hash value under blocked items in EDR Tool

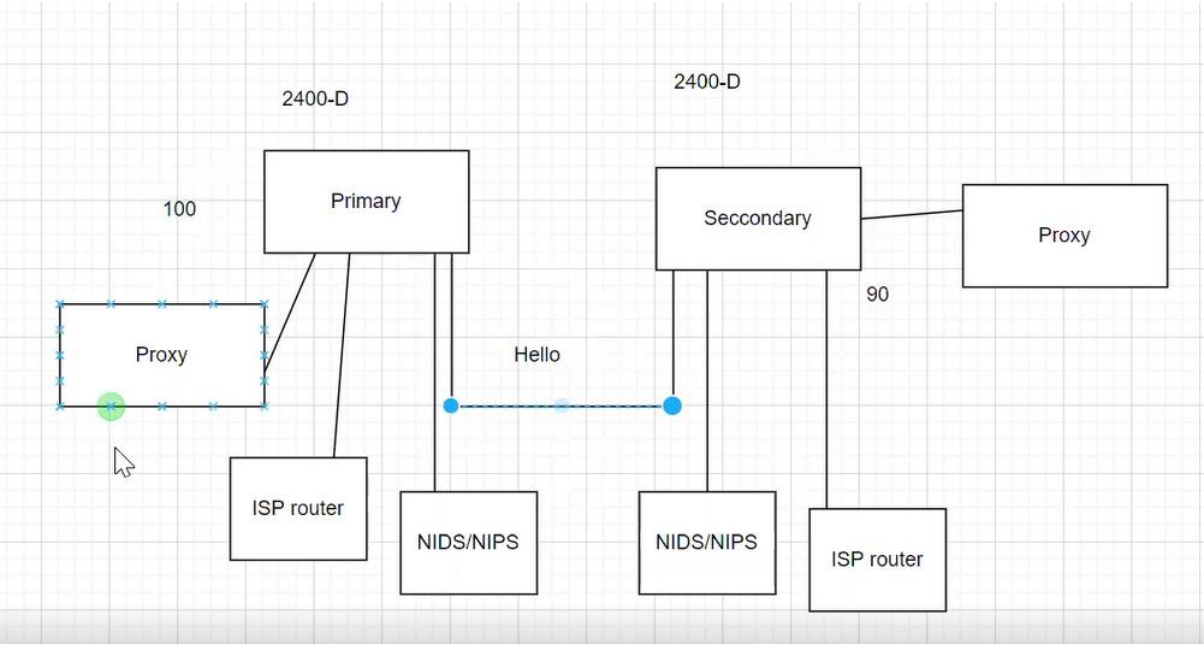
Domain name blocking under SMTP, or fire wall or DNS

Fire wall High Availability

Configuring two firewall to maintain availability issues as per CIA reason for two firewall for Availability purpose

High Availability Names

Primary – Secondary
Primary – Backup
Active – Passive
Master – Slave
Based on election settings we will configure primary and secondary election setting means primary firewall will have always higher number



Always primary firewall number will be higher than secondary
example primary firewall - 100
Secondary firewall- <100
Primary & secondary will exchange the messages, whenever primary firewall get down automatically secondary will act as primary

Conditions for maintaining high availability

1. Both the firewalls must same model number ex; primary is 2400 D & secondary should be same 2400 D only
2. Both the firewall firm aware versions must be same ex; its 7.2 & secondary should be in 7.2 only then it will synchronize

Firewall Upgrade

How can we do firewall upgrade (Interview Question)

Firewall Upgrade we have 2 types

- Primary
- Backup

If we want to upgrade the firewall we should not upgrade the 02 firewall once at a time because as per CIA Triade Availability is highly important

Firewall Upgrade process

- 1st we have to take the approval from the respective manager
- If it is from client-side approval required from respective client

For that one we have to raise the request that request is nothing but the change request. like it is ITIL process basically Infrastructure technology information library The reason for change request is something we do any modification, or upgrade or delete or implement or to configure we will use change request process

- We have to breakup the firewall it means disconnect the physical cable connection after breaking up the firewall
- We have to upgrade the secondary firewall
- And We have to monitor one or days whether all the applications are working properly and also is there any performance related issues
- Whatever secondary firewall upgraded, we should make it as primary firewall and disconnect the primary firewall
- Then Upgrade the primary firewall
- Then we have to Bring it back to High availability-based election setting

Whenever we want to upgrade its always better to contact the vendor team because to find out the what is stable release version then vendor will provide the final approval term

Change request – in This change request we have to raise the ticket
Ex ticketing tool we have service now

Change request always starts from CH00001234
Incident number starts with INC 00123456

Where we have to fill the process
In excel Firewall upgrade process
Backup plan also need to fill
After entering the details we have attach the file in ticketing tool under change request
Change request what information we have to fill

Primary contact name
Number
Email
Secondary contact Name
Number
Email
Dependency team number
Networking team
Application team

Data & Time one which date we are planning to upgrade ex; 15th Aug 2022
Change window (how much time it will take) max 8 hours

Approval

Our manager

Client approval by submitting in the CAB meeting – CAB mean change advisory board it is approved by CAB director

VPN – Virtual private network

Virtual means remotely It is a private virtual network in between user and remote office location via public network or internet

In between user and office location it will form tunnel , using that tunnel only data will be transferred

VPN provide security features like

- Encryption – forming a tunnel in between user & office location
- Non repudiation – trust worthy of data
- Authenticity – who is doing what identify of the person
- Confidentiality – privacy of the data

Vendors of VPN

- FortiGate – Forti client
- Palo alto firewall – Global protect
- Cisco firewall – Cisco client

Dedicated vendors

- Pulse secure – Juniper
- Any connect- Cisco

Zscalar - Zscalar

Citirx - Citrix

What is the VPN Backend process

3 component we have

- VPN client - VPN client have to install in the end user machine its nothing but software file provided by vendor

- VPN portal - It will provide list of gateways information and portal will choose always nearest gateway for connectivity

- VPN Gateway - It is a router provided vendor

Types of VPN

We have two types of VPN

- Remote VPN or IPsec VPN (Ip sec port no 500) - this is used for work from home option

- Site to site VPN – we have to create IPsec tunnel 1st in between one site to another site. Then we have create IKE – Internet key exchange Gate way and security negations, Should look into ciphers means key size related information & Encryption related information & also header length , Public key and also private key exchange

Two different types of phases in site-to-site vpn

Phase 1 – in 2 ways it will exchange 3 messages

Phase 2 – it will exchange key , encryption , ciphers, hellos finally follow the encrypted channel here it will reflect 6 messages

Finally it will form a tunnel between one site to another site

Pcap – packet capture

It means whatever the traffic is going on through packets that time we have to do packet capture whenever if any incident receive that we don't know where it is from whether it is from application layer issue or backend server issue or network related issue we have to take the packet capture should find out the where is the issue is existed

We mainly use trouble shooting & fixing the issue

Pcap In server level we called as TCP Dump

In firewall level or proxy or IDS/IPS we called it as Pcap

For analyzing packet capture we will use Wireshark latest release 3.6.7

Export the pcap file from firewall and import it in Wireshark & Wireshark will give TCP/IP layer approach

In TCP/IP Layers we have 4 approach (Interview Question)

Application

Transportation

Internet

Network Interface

After taking the Pcap importing the wire shark then we have to analyses the layer approach

In Application layer wise whether all the applications are working correctly or not whether DNS Record configured are not like HTTP, HTTPS traffic is going correct are not

Under Transportation layer TCP 3 way handshake in between client & sever should check packet is dropping

Under Internet layer we should verify Retransmission is happing, packet is dropping or packet is allowing

Under Network Interface we should analyze Frames, raw bits

Additionally we have to analyse the Hexadecimal

Raw codes we have to analyse even we have to analyse base 64 code

How can you filter out ip address in Wireshark? (interview question)

We have to use a command IP== ip address like10.10.10.1 ex; from client to the server packet is dropping we want to analyses whether this one application issue or network layer issue or server issue in back end in this situation we have to go and filter out client ip address were ever it is trying to connect to the server in this situation we have to use filter out . In the similar way we can filter out HTTP, HTTPS , DNS Traffic and so on

Components of the FortiGate firewall

- FortiGate is an firewall
- Fortigate is has SIEM Tool
- Fortigate has dedicated Logs collection logs that is Forti Analyzer
- Fortigate has firewall manager that is forti manager
- Fortigate has cloud service provider that is forti connector
- Fortigate has Wi-Fi that is Access point

How to integrate Firewall logs to SIEM tool? (interview question)

We have to log in to the firewall then We have to use sys log server option then we have to specify the which SIEM tool integrating we need to define the parameters like, SIEM tool name , SIEM tool IP address port number and protocol those configurations we have to do. If logs are not going to SIEM tool we have trouble shoot

Siem tool name	Siem tool ip address	Port number	Protocl	Log format	Test
IBM Q radar	10.10.10.1	514	TCP	BSD	succes ful

Trouble shooting

- Check configurations of syslog like configuration meaning here we need to check whatever configured like whether did we provide correct Ip address or not , port number correct or not , log format is in right format are not and so on and finally test is successful or not
- Take the PCAP file in between firewall and siem tool and import from firewall and export into Wireshark and analyses network, application , internet layer issues like TCP 3 way handshaking is completing, packet transmission, packet dropping,

FortiGate model number

80D ,
2400 E – Version7.2

160 D
420 D
1200 D

Pal Alto model number

PA-3050 -- version 10.2

3060, 5050, 5060, 7500

Security Devices

- Management Ip address or host name of the device
- Integrating with Primary DNS and also secondary DNS
- Integrating with AD
- Integrating with smtp server

Actions in monitoring Tab

- Allow Alert
- Block
- Rest
- Packet Dropped

Proxy

Proxy web gateway or application gateway

Proxy will act as gateway or bridge between user and applications. In proxy detection base is signature based It will hide our inter network to external attackers

Advantages

- Bandwidth savings and improved speed
- To control internet usage of employees
- Privacy benefits
- Improved security (Defence depth controls)
- Get access to blocked resources

License

- We have to know 1st what is LAN Band width or speed
- how many number of end users
- how many number of applications in organization level
- How many number of maximum sessions
- How many number of concurrent sessions

From above features we can purchase the proxy license

Deployment method

So this is Inline method or promiscuous mode we can also called as

Inline in between 2 devices deploying device that is called Inline method
Proxy will be deployed in between firewall & NIDS/NIPS

Where can we deploy the proxy (interview question)

We have two options
If the traffic is going from in bound to out bound nothing but out bound traffic I mean from trust to untrust in this secanior after network IPS we can deploy the proxy
When the traffic is coming from external to internal from untrust to trust after firewall we can deploy the proxy
In between the firewall & NIDS/NIPS

Where we will deploy firewall (Interview Question)

We have 2 options like in bound & out bound. Through Internet facing behind the ISP router under DMZ zone or after proxy we can deploy the firewall
From out going traffic its After the proxy
From inbound wise behind the ISP router

Vendors

Open DNS Cisco -- Cisco Umbrella
Z Scalar
Websense
Citrix
Akamai

How to integrate Proxy logs to SIEM tool

Through Syslog server method

Log into proxy server then go to sys log option then we have specify the SIEM Tool name , SIEM Tool IP Address , Port number , protocol, log format

How to integrate Proxy logs to SIEM tool	Syslog server method				
	Siem tool name	Siem tool ip address	Port number	Protocl	Log format
	IBM Q radar or exabeam or splunk or rsa or mcafee	10.10.10.1	514	tcp	Syslog

One of the end user machine came spear phishing or whaling came via malicious URL link what all the possible log sources (Interview question)

- Proxy
- Firewall

  Proxy & firewall it defines Whether user is clicked on the URL link or not
- SMTP

- Email security solution
  Above two Who are all the users received the email

One of the phishing email attacker send a spear phish email attack to couple of users in that situation how can you do instant investigation (Interview question)

Obviously its , SMTP server it will give the information from where the Mail is received. There I will verify, sometimes when I don't have the access then I coordinate with email team , SMTP server team or out look team stating that this is the subject line , this is the sender email address could you please confirm like who are all received the emails please confirm

After confirmation from the respective team ex if approx. 10 people received the email then I will verify out of 10 how many are clicked on the URL link , How many people didn't click on URL Link.

Then I will check in proxy whether 10 user clicked or 1 user clicked & so on and also will verify whether is blocked activity or allowed activity, If it is allowed unfortunately I will check in FIM, DLP what data does the Attacker copied then I will block the attacker IP address as well That particular URL link in firewall & proxy

NIDS / NIPS

NIDS will monitor abnormal or malicious or suspicious activity and it will only detect abnormal activity. NIDS we can compare with SIEM Tool

NIPS will monitor abnormal or malicious or suspicious activity and also it will detect as well as it will block abnormal activity NIPS we can compare with Fire wall , WAF, Proxy.

NIDS Deployment - SPAN/ MIRROR method
NIPS Deployment – Inline method

NIDS	NIPS
NIDS will monitor abnormal or malicious or suspicious activity and it will only detect abnormal activity in Network level	NIPS will monitor abnormal or malicious or suspicious activity and also it will detect as well as it will lock abnormal activity in the network
Deployment method is SPAN/Mirror	Inline method

Passively connected	Actively connected
If NIDS will go down there is no impact to the organization other than alert notification	If NIPS will go down along with alert notification some impact or outage will be there

When we use more than one NIDS/NIPS?

- we will use more than one NIDS/NIPS devices based on the network traffic is going on the Network or Datacentre
- This is applicable even if it is distributed deployments

Model Numbers

Network level devices we will represent using NX Devices (NX means network level devices its more than)
For Host level HX Devices

N 3000
N 2000
N 1000
N 500
Example is F5

Licensing

- Based on number of end user
- Based LAN throughput (BW)
- Maximum number of concurrent sessions
- Maximum number of sessions

Policies

- Malware
- DoS/Ddos
- Spoofing category
- C2C server communication

Detection methods

- Signature based – Known Attacks
- Behavioural based – Unknown Attack
- Base line method – Unknown Attack

Tools/Vendor

- Tipping point – Trend Micro
- Sourcefire -- Cisco
- MacAfee NSM -- MacAfee
- Symantec
- Vectra
- F5
- snort

Forti Gate firewall

https://fortigate.fortidemo.com/logindisclaimer

- username – demo
- Password – demo

In Forti gate we can see NGFW-PRI (primary) which means NGFW have the feature of

- Anti-Virus
- Malware Scanning
- In built IDS/IPS Scanning
- WIFI Monitoring
- DLP basic , ATP Advance filtering prevention mechanism
- URL Filtering , content filtering , state full inspection , Dpact Inspection & so on

So that is called NGFW firewall

We can see HA – which Is High Availability and it is show synchronize which means in between primary & secondary both the fire walls are synchronize nothing but working fine

NGFW FortiGate model number 2000 E

Form wear version 7.2.1

On the left hand side we can see few tabs those are like

- Dashboard
- Network
- Policies & Objects & so on

Dash board – it contains the over all summary of security portion nothing but were threats that we are receiving , how many alerts that we are receiving & whatever issues we have & so on it shows the graphical presentation

Network – Network tab represents the interface tab

Policies & Object tab – Policy object means rule it will follow top to bottom approach It basically for configuration wise it very imp tab. In this we have to create security profile & those security profile we have to keep under policy it will monitor entire traffic north to south & east to west mainly we use this for Implementation purpose

Security profile – Once we are creating the security profile we have to go and we have to implement those security profiles in Policies & Object tab we use this for Implementation purpose

Policies & Object tab , Policies & Object tab are most important tabs without these two tabs firewall is dummy we use this for Implementation purpose

VPN – Its dedicated to VPN configuration that may be

- site to site VPN or
- Remote VPN

User & Authentication – It shows how users are trying to access the FortiGate demo what type of authentication it using whether Radius server integration and also show who are all users to access this particular demo by just how we can integrate eldaps server & so on we use this for Implementation purpose

WIFI switch control – Its dedicated to Wi-Fi monitoring we use this for Implementation purpose

System – It is related to system configuration it shows band width utilization , Ram Utilization all those its part of system things we use this for Implementation purpose

System fabric – It provides the logical control and also network connectors information etc.,

Log & report – It is nothing but monitoring tab

Dash Board –

Under Dash Board we have multiple component like

Mugambi - under that we Application Band width so whatever location of Mugambi and also it shows Google service , Amazon AWS , SSL, HTTPS Browser. It provide over all band width utilization

We can filter out the traffic based on the hours it could be hourly bases, 24 hours and also week if we choose anything

Under that we have IPsec which is used for VPN Connection

Forti view it is used to viewing of something it provides policies wise, Application wises, band width wise so basically its representation wise. So whatever if we want to represent we use the Forti view apart from this it will provide historical data as well real time data fortiview provide the comprehensive monitoring system

Route Monitor – It will define the Route monitoring

Under routing we have different types of protocol like RIP , Static Route, Dynamic Route

EIGRP & OSPF these two are most usable in the organization

Whatever we do in professional laptop firewall will monitor

When some one ask in the interview about the Fire wall what role did you played (Interview Question)

I have the admin fire wall access when ever any brute force attack or any phishing email attack is coming even authentication failure from the attacker ip address. After checking the reputation of the ip address will that particular IP Address in in the firewall level. I will login the firewall will go into the policies & objects tab then I will go and will create the one of the policy related to blocking of the ip address in the fire wall that is one thing I will do

2nd thing is whenever something got compromise whatever logs are coming to SIEM tool those are not giving the deeper investigation or full pledged investigation in that situation I will go firewall I will take the packet capture in the log & monitor Tab and will export the respective packet capture file and will import wire shark Tool will analyse where is the issue

3rd even in domains also couple of times couple of users will access the malicious domain then I will take the respective domain will block that particular firewall domain name

Security – Under dash board we have the security Tab which shows the Alerts & Notification

WIFI - under the WIFI we have the Forti AP Status ex Rail way station , Airport , etc., free WIFI which monitor this option

Client by Forti Ap which define who connected what in which system I mean which access point ex we have 10 A connected to 1 , B connected to 2 and so on

Signal strength which Wi-Fi give more signal strength & less signal strength this is nothing but speed wise or

Rouge Aps in WIFI terminology Rouge is nothing but hacker

Historical clients it is nothing but it show bandwidth utilization wise

Interfering SSID its to verify any over lapping

Login failure if any trying to access the WIFI connections in that situation any attempts are failing with this we will come to know internal user or external user trying to access the WIFI through IP we will identify

Muzzafe – under this we can see Forti view what ever policy that we configured it will monitor it shows what's going on network side

Tool Ips pools by Assigned Ips – whatever ips that are using under organization level like top most Ip 10.10.10.1 , 10.10.10.2 & so on

Host scan summary – If we are assigning SMTP summary protocol It will identify & it will scan how many host are available

Even FortiGate configure the DHCP server

Network – under that we have DHCP, Ip sec , Forti view sources – WAN by Bytes , Top failed Authentication by Attacker

Alreapez – Under this we can see the Application Band width if we integrate office 365 under here we can see what's going on like how many mails it is receiving overall azure office 630 matrix

Sirar – Under this we can see the system information how the firewall is deployed under this Host name we can see NGFW-PRI every hardware contain the model number nothing but serial number

We can see firmware & Mode which we have the NAT mode is nothing but Deployment

System also we can see time as well we have WAN IP

Licences option we can see under this like we have the Forti care support , Firmware & General Updates , IPS , Anti virus , Web filtering

Web filtering or App filtering or content filtering – Means URL filtering

Mumbai –

Test – It is a FortiGate cloud it get the updates

SSL VPN Monitor – What ever our site-to-site VPN as well Remote VPN or IPsec VPN whatever VPN we configured it will monitor the particular VPN

test – Under this we have the Forti Guard

Pune – under we have the WAN 1 – MPLS (Multi provision labelling switching)

Status – It provide the system information under that we can see the security fabric (it provides where ever the firewall is deployed)

It show the memory utilization & control plane (Control plane it will represents band width utilization , memory utilization system information and every thing

We have the Administrator (HTTPS , Forti explore & Administration is demo which is read only)

Under this we have License option , Forti view proxy session by Bytes , Device inventory (Whatever in inventory In the Data centre particular FortiGate firewall how many switches are there , how many devices are there all information will be under that

Forti sand box files by submitted – Analysis of malware any attack is coming by drive by download or Through Phishing email attack etc., in this situation when we don't know the where is the issue we need to connect with FortiGate company by raising the request with sand boxing team will rectify the issues

Sessions It shows the traffic of in bound & out bound traffic of the session

User & devices – It provides how many devices we are using through operating system wise like Linux , Window Forti likes OS like Asset inventory

Forti client its for VPN connection in every end user machine we can deploy

Security – Soc team will check in the security tab will verify what type of alert it has received in dash board we see

Under security tab we can see the Compromised Host verdict if any system got compromised this our main soc TAB to check the firewall alerts , regulary alerts will come here we have to pickup respective alert then we have to the investigation

Hast scan summary , Forti client Detected Vulnerability , Application wise band width (under this log are occupying more band width)

Top vulnerability End point device by detected vulnerability

Other vendor firewalls is blocking port & protocol but Pal Alto is blocking based on Application

What is the difference between firewall & IDS/IPS (Interview Question)

Firewall will monitor the Inbound & Out bound traffic based on the actions it is defined on requirements side either it will allow the traffic or will block the traffic so that is about firewall

IDS & IPS – Any Abnormal or malicious kind of activity IDS will only Detect but on the other hand IPS will detect and will block

IPS is subset of firewall now a days NGFW has a inbuilt feature of IPS capability well

Firewall user here whoever has the access of this firewall

Quarantine it is related to malware

What is content filtering (Interview Question)

Content filtering which means it is a block listing of website & white listing of websites based on business requirements content filtering can also called as web filtering & Application filtering so on

Top Threats Tab (IMP)

Under Top threats Tab we have Top threats by score it provide what threats is coming under firewall level that may be inbound traffic or out bound traffic that show under this particular Dash board

Threats score are depends under combination session it is not for single session this is for entire score

Top threats are only one category that is only blocked connection which when user of the FortiGate company trying to access respective websites it will block the particular activity it could be anything

SSL VPN Monitor

Whatever VPN it is configured in the fortigate side

Forti view Application

Whatever application attacker is trying to access to the fortigate company so all those application information it can be provided that may be HTTPS related application , Forti mail related application, out look related applications & so on

It shows which application Is causing more band width under this

Forti view Destination

From destination it consuming more band width from which IP address it dash board created dedicated destination wise

Forti View Website

We can see all the GUI as well Forti net employees list like what type of application they are trying to access

IP address Management

In short we called as IPAM it is just to monitor the IP Address

IPsec Monitor

It monitors the band width of VPN

Device Inventory Monitor

It is nothing but whatever devices that identified by Forti net firewall device inventory is based on Hardware vendor wise

If we want to identify the host network or network device which protocol we have to enable

SNMP – simple network Management protocol backend mechanism is SNMP port number 161

Forti view destination Interface

Here we can see how the traffic is going on through which interface, we have to check how much interface it is configured, how much band width its configured

Destination Interface

- WAN _Up link
- DCFW (DCFW)
- FSA – DMZ
- P22
- ISFW-HA
- Meru WLC (FWLC)

These are based on Destination interface wise

Forti view sources

It represents by Bytes what ever sources it is integrated those are identified by Forti net firewall

Fortigate monitor the DHCP also it leasing the 3 devices like

- MSFT 5.0
- Forti switch – 448 E
- Metropolis

Forti view Policies

This is dash board here we will not configure the policies here It provides which policy is consuming the more band width

For every firewall last policy is Implicit Deny

Network TAB

Under Network tab we have multiple

Interfaces – we can see the M1 & M2 so on up to 32 we have the interface. These interfaces are combination of RJ45 & Optical fibre

Here we can see the interfaces up & down along with colour which is green its up and its configured & which is in red it is down which is in hash colour it is not configured

Under this we can see the Agg which means Aggregate interface several configuration we can add into single interface aggregation means summing of all

Physical Interface , WAN interface we can see , Administrative Access (Under this we can see HTTPS, PING, SSH , FMG- Access. When ever any issues comes we can trouble shoot & debug the issues accordingly for that we have to enable Admin access

Whatever traffic is going outside only for those we have to enable PCAP (Packet capture) that to internet related only because most of the attacks from internet only

DNS – for ever device we have to integrate with DNS server like Management IP , Primary DNS & Secondary DNS

Here we can see Local domain

DNS is only one support only two protocol which is TCP/UDP

Which server support it can support both TCP as well UDP connections

DNS server protocol

- DNS (UDP)
- TLS (TCP)
- HTTPS(TCP)

Explicit proxy – Firewall will act as proxy as well proxy is subset of firewall

Proxy port is 8080

SD-WAN – This mainly for WAN interface it provides any performance issues likes band width issues most of the time it is applicable to multiple locations

Static Routes – Under static routes network admin team will give the routing

Policy Route – In policy routing we have policy base routing & static base routing (Static routing will provide over all routing)

RIP – In small companies we use because will have less under 15 networks only

OSPF – open shortest path first here we have the stub area link statement

BGP – Border gate way protocol this is can be use for external connectivity internet wise they have the different vendors

Multi cast – here we have to provide the routing

Diagnostic – This one is mainly for the whenever if we want to do trouble shoot

Packet capture we can export in log & report tab here we can download packet caputer then we have to import to wire shark

Security profiles Tab

Anti virus – under AV 3 types of security profiles are configured like

- AV – Monitor
- Default
- WIFI – default

Web filter- URL filter or Content filter one and the same

In Forti Guard category web filtering or URL filtering option what all the different actions we can see (Interview Question)

- Allow
- Monitoring
- Block
- Warning
- Authenticate

Video filter – Limited GB can be filter out here

DNS Filter – Here which domains to allow & which domains to block

Application control – Individual we can block or white list under here selection is easy

Intrusion prevention – under this 15017 forti gate is supporting by vendor

XSRF (cross site request forgery)

File filter – which files we have to enable & which files we have to block ex; zip files , Rare etc.,

VoIP (Voice over IP) – we have to integrate with firewall

Web application firewall –

Under this we have the cross site scripting attack it is one the dangerous attack in OWAS Top 19

NGFW is layer 7 fire wall or layer 4 firewall (Interview Question)

NGFW can block up to layer 7 firewall including network & transport layer as well

WAF is subset of NGFW WAF can block application layers

What is difference between WAF & NGFW (Interview Question)

SSL/SSH Inspection – It will scan the SSL certificates it can see it provides if we are using any outdated versions that we are using. Inspection is nothing but scanning of those device that provides the when it is going to get expire and so on

Application signature – It is part of application control right now how many application it is supporting

Web rating over ride – when ever end user is clicking on malicious URL link it will take to deface website nothing but will take to fake website

Web profile over ride – If we are grouping of the websites the it is called web profile

Policies & Objects

Before going to policies we have to create security profiles like VPN, AV , Filtering after security profiles we can do grouping as well in a single group

Policy firewall – Security profiles very important under firewall level for blocking the activity security profiles are not required

Block malicious by Forti EDR which means its is NGFW tool

Under this we have the DNS as well

FIT Intel NUC out bound here some of the connections are created this connection will go internal to external

Allow FSA Access FSA is one the modeul in FortiGate firewall Access from DMZ to External

How to block the IP Address in the FortiGate firewall

Block Malicious Phishing e-mail Ip address from untrust to trust zone the source would be from where this phishing email is coming from to victim IP for destination if it is spear phishing we have to block all

In Forti gate firewall where do you block the IP address (Interview Question)

Under policy & Objects

How can you block Ip address in the Firewall or do u have access to firewall (Interview Question)

Yes I do have access to firewall admin access so when ever something is blocking yes I can go and block in the firewall level

Multi cast policy – From single sources IP to multiple IP address basically it is single to any

Local in policy – if we want to create within the organization which means within the internal users which is based on application wise

IPV4 Access control list – Here we can do which Ip we have to white list & which IP we have to block list from source to destination

IPV6 Access control list – same as IPV4 above

IPV4 DoS policy – whenever any Dos & DDOS attacks are coming

IPV4 DoS policy – Almost similar to IPV 4

Proxy policy – Here it gives which website to block & which website to enable

ZTNA (Zero Trust network Access) – It is approach basically it can identify how we can secure our organization by eliminating implicit trust ever phase we have to validate every secure profiles that is called ZTNA

Authentication Rule – Whenever if we want access any website it will get the access it is based on protocol , address , parameters it can used who has to access the what base wise we configure under this one we can create scheme as well

Address –

Internet service Data base – Mainly for the what types of internet services that we are trying to access

VPN

VPN is for the we have 2 types of VPN we have

Site to site VPN & Remote VPN (IPsec VPN)

Under the VPN Tab we have

- IPsec Tunnel
- IPsec concentrator
- IPsec Tunnel Templet

Above all these Site to site VPN

We have 2 phases in Site to site VPN Akai pahse1 & Akai phase 2 Akai is nothing but internet exchange

User & Authentication

Who has the access to the particular device is called User & Authentication

User groups – Grouping similar type of group members nothing but in soc we have l1,l2,l3

Guest management – If we have to give the access to guest users here we have to create particular guest name & particular IP Address and user name of the guest user

LDAP server – Every tool we integrate with Active directory

RADIUS Server – It is remote access daily in user server we integrate with authentication purpose it is maintained by Network Admin team mainly we use for authentication & authorization , Accounting purpose

Active directory maintain – Windows Admin & Sys Admin

Single Sign – on – we use for one time we give user name & password so that we can access multiple application

Authentication settings –

Captive portal (interview question)

It will provide the Sometimes whenever user is trying to access any website it will show like website is block based on customer requirement it shows ex ; this website is disabled contact admin team

Forti Token – It is related to mobile it is additional token which is generated when we trying to access anything

Authentication Rules – Whatever Authentication schema that we configure that schema will appear under drop down list we have to select particular drop down list under the Authentication schema we can define that particular 3rd party tool as well

Wi-Fi & Switch Controller

Even Forti gate firewall can be used as Wi-Fi monitor purpose

Managed Forti Aps (Access point) – It do health check up basically whether it is active or inactive stage

Wi-Fi clients – It provides who are all connected to the respective Access point. It shows the IP address of the device as well Mac to which access point did it connected & what is the Wi-Fi name as well SSID Name who is the user and what is the device model number & so on

Wi-Fi Maps – It will provide the signal strength It will provide map wise nothing but heat map

SSID – For every access point we have to assign SSID name that is also called as wifi name 2.4GHZ we can give for guest users & 5 GHZ we can give for ourselves

Forti Ap profile - After creating all the profiles we have to create Access point profile the we have to configure 2.4GHZ & 5 GHZ signal strength

WIDS profiles (wire less Intrusion detection system) – we use detected to wireless monitoring purpose it will not support for wireless Ips , it is one of the signature based detection it will only identify the attacks It cant block it

WIDS attack names (Interview Question)

- ASLEAP Attack
- Association Frame flooding
- Authentication Frame flooding
- Broad casting de authentication

- Invalid MAC OUI
- Long duration Attack
- Wireless bridge
- Spoofed de authentication
- Spoofing category
- Rough AP

Wi-Fi settings – each and every access point configured Wi-Fi certificate

Forti link interface – Access point configuration will deploy here

Managed Forti switches – we are dedicatedly using Forti gate related switches then we can manage all the switches here

Forti switch client – each and every switch even we can configure SNMP as well

Forti switch VLN – under switch we configure VLN each and every virtual LAN we create one of the ID number assigned to the based on team wise

Forti switch port – for switch ports we can use for communication purpose

Forti switch port policies – either we have to create default policies or customized polices

NAC policies (Network Access control) – this is mainly related to end user systems for end user protection NAC can use what level of control even if particular device is sleeping it will identify what is the status of the network device for that one we have to configure SNMP community string version number 03 (Because it is encrypted user name and encrypted password)

System TAB

Administrator – based IAM or IDM it provides which user required what level of access it configured like api-admin , tmg , Forti explorer demo account

Admin profiles – her we do grouping of the devices whatever devices we have given the access

Fabric management – it provide how this Forti gate demo is deploying it can deploy logical topology, physical topology how this firewall is deploy what is the device it connected every device it say in the logical topology format

It provides what are all the devices registered and what is the upgrade version and authorization information and so on

It provides the logical topology here we no need to go to the Data centre how the devices are deployed so it can represent overall topology wise

What is the importance of NTP and its port number (Interview Question)

Network time protocol 123 port number

It Setting the time based on the time zone which time zone we located and also always our local time we have to integrated with NTP server. Why because if we don't integrate with local time when ever any incident is happen because we are not sure at what time it is happened so when we want to verify the incident investigation or forensic investigation in that situation because we should know specific time and we will go and will analyse those logs only so that's why every device not only security device even this NTP we can define to servers , devops tools , tech of tools etc., every tool we have to integrate with NTP

System Tab

GRC – Governance Risk compliance team will enable the password policy

Do you know how create the policy related to organization (Interview Question)

We have three diff types of SNAT under the settings option

- Static SNAT
- Dynamic
- Port SNAT

What is Virtual domain V Dom in FortiGate firewall (Interview Question)

V Dom means virtual domain one firewall we want to create multiple virtual firewall one physical firewall. If we want to create the multiple virtual firewall we create the V Dom we login under the Forti gate firewall and we have to go the systems tab under that we have settings option available under setting we have to go enable the virtual domain ex; purchased high end model so that may 3600 E right now the model number is 2000 E .

SNMP port number 161 (Interview question) – under SNMP we have three versions

Version1, version 2 , version 3 always better to version 3

Why we enable SNMP because to monitor the network , Discovery of the network ,

Replacements messages – it is captive portal we use here HTML & java script programming languages to show basically whenever any malicious website who is accessing by the end user

Forti Guard – It uses for regular patch updates related to AV , IPS, web control and so on each and every updates will provide regularly

When we reboot the device

Security Fabric

It represent logical Topology & Network Topology

Physical & Logical Topology is supporting by Forti gate firewall

Security Rating – It represents the what is the security poacher of the organization and what is the severity of the respective each and every issue or alert notification. We can modify based on the Business

Automation –

External connectors – Forti gate firewall is supporting to another vendors as well ex; Amazon web services , Micro soft Azure , google cloud , Ali baba and so on

Asset identifier centre –

What is trending technology in the networking side (Interview Question)

Secure SD – WAN

Fabric connectors – Forti gate related things what are all the other products we can integrate

Log & Report

It is completely monitoring purpose this Is mainly for L1 ,L2 & L3 operations purpose that may be dedicated to firewall operations or even for SOC operations as well

It represents what is inbound & out bound traffic mainly use for instant investigation purpose this particular log & report tab

Forward Traffic – Most of the cases we use Forward traffic only based on what ever policies configured we can see the traffic under here

Whenever these internal employees they are trying to access the external application that is nothing but out bound traffic in the similar way out bound they are trying to access our internal application that is nothing inbound traffic

In this situation inbound & out bound traffic whatever the packet is enter into the organization level it will reach to each and every policy not but it will validate each and every policy and when ever the policy match so it will stop particular policy. So then it will hit the particular traffic then generate traffic in the log & report tab

Based on the policies configured we can see the traffic

Policy id under forward traffic is nothing but name

Under Application name we can see who clicked and what

Whenever any blocked activity is there that one we have to suspect as a false positive

If something allowed or quarantined may be alert may be even other things we can consider as a notification we have to suspect as a true positive

NOC team will do more packet capture than soc team that too when log sources are not reflecting into SIEM Tool

Multicast traffic – From single source IP to Multiple IP Address

Local traffic – It is loop back address to whatever the traffic is going on to some other Ips as well

Sniffer traffic – some body is trying to sniffing nothing but spoofing kind of thing

ZTNA (Zero trust network Access) Traffic – it is dedicatedly to internal user or external users they don't have sufficient controls and they are trying to do activity in this situation we have to configure the ZTNA Server we can see the traffic here before that we have to create a policy based on policy ID only then it will appear here

System events – Whatever attacks are happing showing in firewall level ex; malware related , phishing email related , or domain blocking related , IP blocking and so on all those events we integrate

What type of windows related logs you will integrate to SIEM Tool (Interview Question)

- Forwarded events
- System configuration
- Application
- Security related logs

Log settings – How to integrate logs to the SIEM tool

Threat weight – It is severity wise nothing but security wise

Forti Analyzer report – It dedicated to Log report

What are different types of reports you create in Fortinet firewall (Interview Question)

- Top 10 or 20 Application Risk & control
- Band width use age wise
- Cyber bulling indicators report (From which Ips these particular attacks are coming)
- High band width application usage
- Self harm risk indicator report
- VPN Report
- Threat report
- Web usage report
- Cyber threat assessment
- 360 security report

Vulnerability Management

It is basically infrastructure security & it covers server scanning

Different types of servers

Micro soft servers	Unix	Micro soft OS End points
2008 R1 and R2 (Legacy Server)	RHEL (Red hat enterprise Linux)	Windows xp
2012 R1 and R2	Centos	Windows vista
2016 R1 and R2	Ubuntu	Windows 7
2018 R1 and R2	Debian	Windows 8.1
2019 R1 and R2	Container	Windows 9
2021 R1 and R2	Docker	windows 10
	Sues	windows 11

RHEL (Red hat enterprise Linux)

- RHEL 1.X
- RHEL 2.X
- RHEL 3.X
- RHEL 4.X
- RHEL 5.X
- RHEL 6.X
- RHEL 7.X
- RHEL 8.X

Up to 6.x all are legacy those are outdated no vendor will give support

On Docker wise latest one is 13.1

Windows or Unix							
	Micro services	Micro services	Micro services	Micro services	Micro services	Amazon.com	
	Container1	Container2			Container5		
Oracle or IBM or vmware	VM1- 100GB	VM2	VM3	VM4	VM5	Microsoft	AWS
500GB	HP 6720 L						

On top of container 1 , 2 & so one we will install the micro services applications, micro services means very bigger application can be divided into smaller ex; Amazon.com

How can you prevent windows server or Linux server from attacker (Interview Question)

- By using AV/EDR scanning agents
- We should do Regular patch updates
- Make sure that Running the vulnerability management scans
- RDP protection (windows)
- Disk encryption
- Complex user name and passwords
- MFA from attacker to protect in Linux we need to create user name & password additionally should generate private key
- DLP
- FIM
- Account lock out polices
- Security logging and auditing and have to integrate with SIEM tool
- Implement Hardening benchmark (CIS)

This is 100 % that we can stop but can reduce the risk

What is meant by vulnerability

Vulnerability means weakness in the system

- CCTV cameras are not there – Its Physical security side
- AV is not working properly – EPP (End point protection) side
- Firewall zones wrongly defined – Network security side
- Password polices not defined properly – Information security side
- Patch updates – Infra structure security side
- Input validation wrongly defined - Application or Product security side
- Our critical servers are exposing to internet (0.0.0.0) – cloud security side

Threat - If vulnerability exploited threat will occur which mean attacker will identify the vulnerability then attacker will exploit & gain the unauthorised access

Risk – Vulnerability * Threat
Likelihood * Impact

- Likelihood – One year base line How many times bad activity will happen
- Impact - What are all the consequences

What is the difference between Vulnerability , Threat & Risk (Interview Question)

To one of the person who is sleeping on bed with protection of net but that net have the small hole in that mosquito entered & bitten the person so what is vulnerability, threat & Risk hear (Interview Question)

- Hole is Vulnerability

- Mosquito is Threat
- Bitten is Risk

Vulnerability assessment

Running the vulnerability scans and identifying the vulnerabilities to the servers and patching those vulnerabilities

Vulnerability management

Managing multiple vulnerability assessment scans and identifying the vulnerabilities

Every organization contains multiple teams like

- Devops
- ML/AI
- Data analytics
- middleware
- web servers
- DB servers
- finance servers
- windows
- Linux

Vulnerability management process

- Contact the business owner or asset owner or server owner and identify the servers (Asset inventory tools, HP , CMDB, Service now and excel sheets)
- Take the approval from server owner (Date and time) like when we have to run the scan
- Log into scanning tool (Nessus, Qualys, rapid 7 and so on)
- Create a scan policy (Choose the scan template , Policy name , Hardening benchmark, Credentials)
- Create a scan rule (in tool itself we can create the scan)
- Schedule the scans (Monthly once we do the scan automatically scan get complete)
- Generate the reports (Excel and PDF)
- Analysing the reports manually (based on Risk assessment and BIA - Business impact analysis)
- Filter out based on severity (Critical, High, medium, low and info)
- Raise a ticket with respective business owner (Widows and Linux)
- Windows and Linux team will do the patch updates
- We have to re run the scans

Patching - Fixing the issue or upgrading the software versions

Scanning mechanisms

Authenticated – providing credential at the time of scanning, Credentials means (Username and password) if we are providing the credential scanning then only it can provide the full vulnerability list

If window the highest privilege is – Admin

If Linux the Highest privilege is – Root

These credential details we should take from the server owner

Unauthenticated - Without providing any credentials (Not recommended)

Scanning types (Interview question) difference between horizontal & vertical

We have two types Horizontal & Vertical scans

Horizontal - Multiple servers against single port

Vertical – we should take a single server run against multiple ports (65536) one server we have to take entire server against the ports in this we will come to know which port is open & which port is close.

Different types of scans

- OS scan (server) – entire scan its part of vulnerability management
- Port scan
- Network scan
- Application scan
- Malware scan

What is meant by port scanning (Interview Question)

Running the scan and identifying what are all the ports port opened and risk there risky port is open

CVE ID – (Interview Question)

Common vulnerability exposure It is unique id number provided to each and every vulnerability

ex: CVE -2021- 44228- Zero-day attack

CWE (Interview question)

Common weakness exploitation this for OWAS TOP 10 this is part of application layer attack

ex: A1- Broken access control

CVSS Score – (Interview Question)

Common vulnerability scoring system

This range is 0 – 10 scale range

- 9- 10 critical
- 7-9 High
- 5-7 Medium
- Below 5 Low and info

CVSS Versions

- cvss1
- cvss2
- cvss base 3

Who are all the vendors maintaining the these vulnerabilities

- NVD - National vulnerability database
- MITRE
- CVE

CVSS score is based on

- Confidentiality – that vulnerability is exposing what level of confidential privacy of the data
- Integrity – To know the trust worthy of the data to verify if any attacker can modify or delete the data
- Availability – To verify any business impact or business outage or any availability issues are there
- Scope – How scope of the work attacker will enter into the work into the server level
- Attack vector – Selection of the target by choosing the different tactics
- Attack complexity – Attacker will check the complexity whether it is easily hackable are not will check the complexity
- User interaction – When ever attacker is trying to exploit the vulnerability attacker will check the any user access is required. If user has to download anything, if user has to do something are not

According to above parameters it will validate the automatically it will validate for every vulnerability so CVSS score will generated along with CVE Id number as well

Hardening –

Hardening means doing initial set off configuration related to security nothing but After server is created doing initial security configurations and which reducing the attack surface is called hardening

EX compliance of hardening

- CIS – Centre for Internet security this from US
- DoD STIG – Department of defence this from US this dedicated to navy , defence etc.,
- ANSI -
- Singapore –

CIS benchmark levels

Level 1 - Basic configuration - Less impact and less risk

Level 2 - Difficult or advanced Compulsory (it has more impact and risk)

CIS I globally accepted bench mark

Scan template
By default every tool or every vendor is providing scan templates

- Ex; basic scan
- Network scan
- PCI DSS scan
- Malware scan
- Quarterly pci scan
- iso 27001 scan
- spectre and meltdown
- log4j

Always we use advance Network scan because it provides remaining 29 information under the Network scan

Tools or vendors

- Nessus (Tenable)
- Qualys
- Rapid 7 or nexpose
- Tripwire
- Palo alto
- IBM
- HP

Nmap (Network Mapper) which is open source tool it will identify what ports are open
Putty software Is for login into Linux server which is Unix operating system

Licensing

Based on number of servers we want scan (IP's or hostname)

Design /deployment

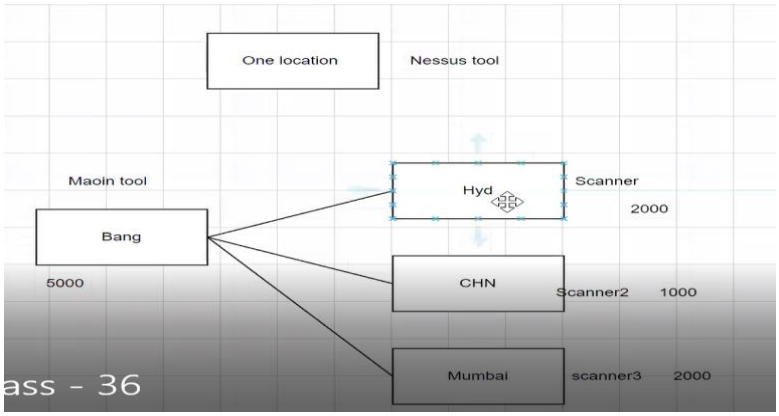
For single location - One scanning tool is sufficient

For multiple locations - More than one scanner and in main location we have to use tool

If it is one location we can deploy with Nessus Tool. Here we have to identify the servers & we have to run the scans directly because this Nessus tool as well as servers will in same LAN

If is in Multiple Location ex; If our any head quarters in Chennai location & branch offices are in Hyderabad , Delhi , pune etc this situation we have to use distribution deployment

Main Tool will be Chennai because its head quarter remaining locations we need to keep the scanners



Will you do manual Analysis whatever report that you generated or just you throw on the respective windows team & Linux team to do the patch updates (Interview Question)

I do manual Analysis. I will take to the each & every vulnerability and what exactly confidential wise, integrity wise & Availability wise & will follow the what is the vulnerability name , vulnerability description wise & so on

Roles & Responsibilities

I'm azam shaik I have 7 years exp in IT & non-IT as well in vulnerability management dedicatedly in my organization I'm working for so & so company my client is from US in my client location we have different types of servers combination of AWS , micro soft azure , even infra structure physical as well all those together we have 10,000 servers as well . those 10k servers different combinations like micro soft, centos , Debian, Unban to , Red hat Linux & so on

As a vulnerability Analyst my day start with we are running the monthly scans I create a scan policy in our organization we are using the Nessus tool for running the scans , our deployment is distributed deployment our headquarters is in US remote branch offices in new York , Chicago each and every location we install scanners in New York our main location our scanner is available, whenever if I want to run New York servers in the rule I will enable it in the same with the other locations as well . In our organization we are following the CIS bench mark

In our organization we are following the Authenticated scans so I schedule the scan policy & I will schedule a scan rule so then finally I run the scan after that I will go and I will export the report in CSV format & PDF format every vulnerability report contains the plugin id, CV number , CVSS Score , Risk or severity next vulnerability name & Vulnerability description & so on

I take each & every vulnerability I will take whatever is coming then I will go and I will do manual analysis like so what is business impact analysis & what is the risk assessment is involved will verify really that vulnerability is existing in the organization are not. So after doing all these analysis we are not following the tool based severity in our co we are following vendor severity. According to vendor severity, risk assessment will filter out severity wise like critical, High , medium , low & information

Will raise the ticket accordingly based on High, medium , low & information those tickets I will share with the respective windows team & Linux Team. After raising the ticket both the team will do the patch updates in the development environment & testing environment. After getting confirmation the both teams regarding the patch updates then will re run the scans and I will re confirm back to the respective team so after re confirming from my side then will raise the change request will implement in the prod environment

Then finally will particate with the customers , shift hand over , fine tunning , trouble shooting. Supporting other team members & so on

Nessus severity	Qualys	Unix
Critical	5	Critical
High	4	Imprtant
Medium	3	Moderate
Low	2	Low
Info	1	Low

ITIL Information technology infrastructure library

ITIL will be followed by Service based companies & Product based companies follows the NIST frame work

ITIL Provided the different types of processes

- Incident life cycle management
- Change management process
- Problem statement
- Solution statement

Incident Life cycle management – It is nothing but any incident is coming to the organization what kind of phases that we follow. which mean Step by step process of incident investigation is called as incident life cycle management

Under Incident life cycle management, we have couple of phases

Preparation - In the preparation phase whether soc room is ready, tools are implemented, resources recruited and trained , all the tools are integrated to TV's for monitoring, playbook or run book or sops or implemented

Identification - In the identification phase security analysts which we are whenever any alert is received in SIEM tool here we need to identify what types of incident alert is received. Whether it is authentication failure category, phishing email, malware, spoofing, flooding and owasp top 10

Containment - In this phase security analysts will identify network isolation is required or not and also if it is required whether it is short term or long term

Eradication/Mitigation - In the mitigation phase clean up the infection based on what type of incident received

Recovery - In the recovery phase bring the compromised incident from abnormal operations to normal operations and also do data recovery

Lessons learned - In the lessons learned phase we have to prepare a document is called RCA. (Root cause analysis).. In the RCA document we have to provide information how, when and why system is got compromised and also what are all the eradication and recovery steps taken.

Lessons learned document use full for future purpose like acknowledge base
MTTD (Mean time to Detection) , MTTI (Mean time to identification) , MTTR (Mean time to recovery)
These document we have to present with customer as well
One of the server got compromised what will you do? (Interview Question)

I will login into the SIEM Tool, will check what type of incident that received whether authentication failure category, malware category. 1st I check the classification of the incident & after that I will do log analysis then I will incident as has a false positive or true positive, then if it is false positive whatever evidences that

I gathered will attach the those evidences. Will make the summary of the notes in the respective ticketing Tool and will close the incident

If it is a True positive based on incident life cycle management process defined by ITIL then will whether the containment is required are not. In mitigation phase I go and I will see what type of infection I have to clean, in the recovery phase I will go and I will see whether any data is copied by any attacker. How to recover that particular data and also how bring from abnormal to normal. In the lesson learned document in lesson learned phase I will document everything what I have done Investigation to submit to our client as well as even it is useful for me to my future purpose

One of the system got compromise in the post-mortem report what you do? (Interview question)

We do RCA – Root cause analysis cause of the incident

2 Change Management - Some thing we are going change from existing environment we have to raise change request first and we have to take approval from our manager

That change request we have to present in the CAB meeting (Change advisory board). After approval from CAB director we have to implement the change

- Ex: Firewall upgrade
- SIEM correlation rule implementation
- Patch update in the servers
- SIEM tool upgrade
- BCP/DR- Business continuity planning and Disaster Recovery

Problem Statement - An issue should be addresses or condition to be improved

GAP analysis (Interview Question)

Current state of the issue where we to achieve to desired state . what I understand what are the security controls are available whether all the security controls are sufficient are not? Then if sufficient existing controls are not sufficient then I go & will implement additional controls if we want to implement for ex in AV in end point level only we have the AV but we don't have the DLP, FIM , Encryption & so on then will check defence in depth controls are available in the end point level are not then I suggest some more end point control in the similar network level firewall i use Gap Analysis for the improvement something were i do not have clarity in the project main reason i use were we r now and were we want to be in future basically it helps understand where starting from and were u want to go. Key important component what exactly is require.

Solution statement - It a detailed document or blue print of design of each solution that we should priories

NIST framework of Incident response

- Detect
- Identify
- Respond
- Protect
- Recover

NIST Main importance is risk assessment

Application security

- SDLC life cycle
- Cryptography controls
- Pentest and types of pentest
- Red vs blue team
- OWASP TOP 10
- WAF

SDLC life cycle

	General feature life cycle	SSDLC (Secure software development)	Tools	
Requirement	Facebook, Instagram or twitter or what's app	Requirement	No Tools	
Design	Audio call/Video call	Threat modelling	Microsoft STRIDE	10 Vulnerabilities, Critical, high, medium, low, info
Development	Application architect they will design audio call and video call	SAST- Static application security testing	SAST- Static application security testing	Secure Code scan, Checkmarks, Veracode,

				Fortify, IBM app scan
Testing	Development team will develop the audio video call feature	VAPT	DAST- Automated- Application and manual pentest VA – Automated , Nessus, Qualys - Server	Nessus, kali Linux, metapelite, burp suite, OWASP ZAF, The juice shop, post OFFCE
Release	Testing of the audio call and video call		Release to public	

STRIDE

STRIDE stands for spoofing, Tampering, Repudiation, Integrity , DOS , Elevation of privilege

Spoofing – Masking the original identity

Tampering – Modification of the existence data

Repudiation – Anything is leaking to the public

Integrity – When someone is adding , deleting or modifying who is doing what

DOS – Availability issues will come

How can you resolve the conflict of interest between two people how can you resolve (Interview Question)

Example of TPS (Third party server)

- Oracle / Java
- Python
- Power shell
- Apache
- Tomcat
- Spring boot frame work
- Hasher
- RMQ
- NGINX

- IDAP
- KIBANA
- Logstash

In TPS we have to verify

- EOL – End of life
- EOS – End of support

TPS Scan Tools

Black duck, white source , Synk

CI/CD - Continuous integration/Continues development

What is the difference between Vulnerability Assessment & Penetration Testing (Interview Question)

Vulnerability Assessment – Running the scans & identifying the vulnerabilities

Penetration Testing - Whatever vulns identified whether those vulnerabilities will be exploited or not

Three different types of pentest

	Application	Server	
White Box	Username, password, url link , admin access	IP address, host name of the server and admin	Providing entire information to pentest guy and ideting the vulnerabilities
Grey Box	Username, password, url link , admin access	Ip Address, hostname, user account, service account	Providing partial access pen tester and identifying vulnerabilities
Black Box	URL	IP ADDRESS	Providing limited information and identifying the vulns

Cryptography (Interview Topic)

Cryptography provide secure communication or securing of the information most of the cases under transit level and it will use mathematical calculation and also some computer algorithms. If we are using these mathematical calculations and also computer algorithms it can provide respective encryptions and also integrity , Authenticity, confidentiality etc. and so on

It can provide secure information and communication techniques derived from mathematical calculations and also set of rule based rule algorithms to transform messages that are hard to decipher (cipher means week encryption here decipher mean decryption nothing but it very difficult to decrypt the data whatever we are securing the communication
Ex; we have encryption & also decryption

Two types of key we have

Public key – It sharable
Private key - It is not sharable

Two types of cryptographies (Interview Question)

- Symmetric
- Asymmetric

Symmetric – The same key is used for both encryption & decryption, and It is very quick. It provides only confidentiality it provides only privacy of the data but it will not provide Authenticity, Integrity & Non repudiation

Symmetric is Also called as Private key or secret key

Formula n keys = n(n-1)/2

Drawbacks or disadvantages

- It will exchange so many keys (Out of band) if we have multiple users are there in the network that scenario it will exchange
- It will not provide authenticity, integrity and non-repudiation

Asymmetric - Two pair of keys or different keys used for both encryption and decryption, it provides Authenticity, Integrity, Confidentiality and non repudiation

For number of keys = 2N

Symmetric	Asymmetric
Same key used for both encryption and decryption	Two pair of keys used for encryption and decryption
n keys = n(n-1)/2	2n
Out of band key exchange	Less number of keys for exchanging
It provides the Confidentiality	Confidentiality, Integrity, non repudiation and authenticity
It is faster	It is slower

Example Algorithms

Symmetric	Asymmetric	
RC4 (Rivest)	DSA- Digital signature algorithm	
RC5	RSA- Rivest, shameer and Adleman	
Two fish	ECC- Elliptical curve cryptography	
Blow fish	El Gamal	
MARS	DH- Diffie Heilman	
DES- Data encryption standard	Knapsack	
AES- Advance encryption standard		
3AES- 256, 128 and 512		
IDEA		

If we want to use strong ciphers, we should use 3AES this advance one

What is the difference between DES & AES (Interview Question)

DES will use less number of BIT size

AES will use advance encryption standards it has more number of BIT size

Hybrid Cryptography

Combination of symmetric cryptography and asymmetric cryptography
Symmetric cryptography - data transfer
Asymmetric cryptography- Key exchange (Public and private)

SSL/TLS mutual authentication

another name for SSL/TLS- MTLS (Mutual Transport layer security)

Client	1. client will initiate application in the browser ex: www.Google.com	Server public key & private key
	2. server will respond back its own public key to the client	
	3. client side symmetric key will be used and it will initiate the connection	
	4. Whatever public key sent by server client will use and it will encrypt the data	
	5. Finally it will form a Encrypted channel	
	6. Server has its own private key. Server will use private key to decrypt the data and see what messages sent by client and it will respond back	

Draw back in the SSL/TLS mutual authentication

We are not sure whether legitimate server responded back public to end user or client

To eliminate drawback of second step in the hybrid cryptography or SSL/TLS mutual authentication we will use purchased CA (Certificate authority) certificate

Integrity

Integrity – Trust worthy of data secrecy of the data, Only authorised users can add, delete, update or modify the data or files,

Data gets modified

- Accidentally or unknowingly
- Intentionally or knowingly or wantedly

Integrity depending on several algorithms

- Hash
- MAC (Message Authentication Code) this is also refer as HMAC (Hash message Authentication code)
- Digital signatures

Hashing

Hashing is normally blocked in EDR or Anti virus tool hashing is only one way function reverse is not possible. it Digitally representations of the content of the file is called as Hashing

Hash Value

The contents of file are processing through a cryptography algorithm and a unique numeral value (It contains combination of both numbers and characters)

Exmaple	Password	Normal password
	5e884898da28047151d0e56f8dc62927 73603d0d6aabbdd62a11ef721d1542d8	Hashed value
	Reversing is not possible	One way function

Reversing is not possible if we entering the Hash value and we want to convert that one it will not possible will not convert as a password

What is the difference between encryption & Hashing (Interview question)

Encryption process of converting plane text data into encrypted data using some of the algorithms and also using some of the passwords are key that is encryption reversing is possible. It is mathematically two-way function which is encryption & decryption

Digitally representations of the content of the file is called as Hashing . Hashing is one way function mathematically reason is reversing is not possible here under hashing. Hashing cannot convert it into password nothing but plane text (Salt value + Hash value = Hashing)

Salt value (Interview Question) - Randomly generated numerical value (combination and characters and numbers) . It a 8 byte long or length for every user will have different salt value . When ever our password is storing in that situation Infront of the Hash value salt value will be added then only it will get store

Mainly three different hashing algorithms

MD5 or Message digest 5	Bit size - 128
SHA-1	160
SHA-2 OR SHA 256	256

- MD5 and Sha1 - Weak cryptography algorithm it use weak ciphers attacker can guess easily
- sha2 or 256 - Strong cipher

Birthday Attack

If two documents are producing same has values conflict or collusions will occur.. This type of attack called as Birthday attack. When ever we are running the vulnerability scans we will all the issues

If we are using weak ciphers couple of other attacks will occur

Sweet 32 weak ciphers –

- Hashing - md5, sha1,
- Algorithm rc4, rc5, two fish, blow fish

Birthday attack
Open SSL attack
Heart bleed
Poodle

Above frame work follow above FIPS-140-2 Framework- The federal information processing standard

MAC (Message Authentication Code) this is also refer as HMAC (Hash message Authentication code)

It can provide authenticity and also identity of the user along with body of the content. Meaning here when ever user is trying to access it will authenticate even whether the person is authorised are not? Basically identity of the person like who iam I

Digital signature

Digital signature is based on several parameters like SSL/TLS Certificate
Version of the digital signature - x.509v4

Types of SSL/TLS Certificate

These SSL/TLS certificates we use for Authentication , Security , encryption , Non repudiation , confidentiality , Integrity

- Self signed
- Purchased CA (Certificate authority)

Self signed certificate - This certificate generate from either tool or server itself, There is no cost

Purchased CA certificate from Third party - We have to buy or purchase from CA vendor

Vendors for CA

- Verisign Go daddy
- Symantec
- GTS
- Comodo
- PKI (Public key infrastructure)

If we want purchase CA certificate we have to do classification of the applications'

- Internal applications – Self signed
- Internet facing applications or public – Purchased CA

These SSL/TLS certificates will prevent MITM attacks because it has the encryption, Authenticity, Integrity , Non repudiation , Confidentiality

OWASTOP 10 (The open web application security project)

It is one of the popular for Application layer attacks

It is an institution or framework it can conduct survey on the application layer attacks and finally it can make summary of TOP 10 attacks. We have mobile also but Mobile OWASTOP 10 is difficult under mobile side that may be Android, IOS.
we have another organization like
SANS TOP 25

- 2010
- 2013
- 2017
- 2021

CWE ID Common weakness exposure or exploitation
We consider for Application layer attacks

- A01 Broken access control (It Is role based access control whatever privileges are required we have to provide that one itself)
- A02 Cryptographic failures or sensitive data exposure (Strong ciphers we have to use here)
- A03 Injection flaw Cross site scripting and XSS or CSS
- A04 Insecure design (While designing we need to consider the security it follow threat modelling)
- A05 Security Misconfiguration (Its all about ports & protocols , services , SIEM Tool Integration
- A06 Vulnerable and outdated components (Finding the vulnerabilities and if they are outdated versions we have to fix the patch)
- A07 Identification and authentication failures (It is brute force attack category)
- A08 Software and data integrity failures
- A09 Security and logging monitoring failures (When applications are not integrated with SIEM Tool by the organisations)
- A10 Server-side request forgery (It is subset of CSRF Cross site request forgery)
- A11 Click jacking or one click attack
- A12 buffer over flaw attack

Injection Flaw attack Interview Question & SQL injection Attack (Interview Question)

Injection attacks occur when the user/attacker is able to input untrusted data tricking the application /system to execute unintended commands. Attacker will he again unauthorised access or sensitive data exposure
Injection flaw attack is server side attack or client side attack & how to mitigate (Interview Question)

Server-side Attack

Mitigation – Input validation (Were development team is correctly developing are not where ever the input is required ex; in face book text box, like , comment, feedback & so on these are the feeds where user is providing the inputs. and WAF , Parametrized queries (What ever queries that we are using like LDAP, PHP,HTML & so on.

What to inject – We have to inject like

- SQL Queries
- PHP queries
- HTML queries
- Java script
- LDAP queries
- OS Queries

Normally we will and we will untrusted data here

Where to inject - Where ever input is required

- Text box
- User name
- Password
- Login
- Survey
- Like
- Feedback
- Comment URL

Why to inject - To check application is vulnerable or not because attacker will executes those queries and will try to compromise the back end server

Examples of Injection flaw attack

- SQL injection
- LDAP injection
- OS injection
- HTML
- Java script
- PHP injection

2. Cross Site Scripting (CSS or XSS)

This attack will occur when an attacker is able to inert data scripts into application or web page. The data or scripts inserted by the attacker get executed in the browser can steal user data sensitive data exposure, deface websites etc

Under Cross site scripting attack, we have different types of Attack

- Stored cross site scripting – whatever sensitive data is there of the End User those data it can be stored in the attacker command & control server so that is called stored cross site scripting attack and it is Server side Attack
- Reflected cross site scripting – Reflecting come back from the backend server and stating that of the end user browser were browser got impacted by the reflected cross site scripting attack it is from Client side Attack
- DOM Based (Document object mode) – Here request will not go to the backend server using existing sessions only reflections will be back it will not go to the back end server Client side Attack

Reflected cross site scripting (Interview Question)

In the Reflected CSS when the user is clicked on malicious data or scripts it will go to backend server and it will be executed and in the web browser of the client reflection coming as a reflected cross site scripting attack occurred

When ever Alert come its Reflected cross site scripting Attack key word Alert
<script>alert(your web browser got hacked by reflected css or xss)</script>

DOM Based - Document object mode (Interview Question)

In DOM based CSS attack attacker will use existing end user connection using either cookies or data then reflection will be as a DOM based scripting attack

<script> document. object/mozilifirefox/Laptop / agent 64bit / http 1.0 / document .csv /action download or upload </script>

Mitigation for CSS

- input validation
- Parametrized queries
- WAF
- CSP (Content security policy)

3 CSRF (Cross site request forgery) or XSRF or click jacking or one click

For already connection established between end user and also to the backend server attacker will forge by manipulating URLs or deface URL or maclious URLs by shadowing or spoofing then end user request will go to attacker and attacker will gain access and attacker can gain data as well

We have two types of attacks under CSRF

- CSRF attack (Client side) – It is Client side
- SSRF (Server side request forgery) – It is servers side

Mitigation for CSRF

- Input Validation
- WAF
- Anti CSRF Token (Most of micro services related Application for every connection establish so it has generate the token number along with cookie id number as well

4 Buffer over flow attack

Buffer overflow attack will occur when the application receives more input as compared whatever application team defined initially
Then it will occupy more yes of the memory and also storage. finally backed server will be crashed

Mitigation
We have to define proper limit (Min and max)

What is SQL injection attack (Interview Question)

In injection attack we have to identify input validation which is highly mandatory which means that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

What is Cross site scripting attack (Interview Question)

Did you participated anytime bug bounty program (Interview Question)

I participated in bug bounty program for one website but unfortunately im not rewarded

WEB Application Firewall

It will prevent layer number 7 attacks (Application layer) based on the HTTP/HTTPS request and also response using signature based detection and also Behavioural based
EX; OWASTOP 10 & SANS TOP 25

Licensing –

- Based on number of applications
- How many number of end users
- Maximum concurrent sessions
- Maximum number of sessions

Implement / Deployment – Inline method

Detection Method

- Signature
- Behavioural based (ML/AI)

Policies or I rule – OWASTOP 10

Tools

- Akamai
- Imperva
- Barracuda
- F5
- Citrix
- Aruba
- Cisco
- AWS WAF
- Azure application gate way
- GCP WAF

WAF logs integration to SIEM Tool – Syslog server

Information Security

Under Information security we have

- GRC – Governance Risk & Compliance
- Risk Management
- Implementation ISO 27001

- BCP/DR (Business continuity planning & Disaster recovery) – Every organization has to maintain BCP/DR

Governance –

It provides Business objectives and business goals should be align with information security policies

Business objective wise we use COBIT (Computer objectives for information technology) 5 Frame work we use this to identify the business objective & Business Goals even it will define what is the stake holders management & also it will define how to get the profits even it will define the customer satisfaction its all about COBIT 05 Frame work

05 Key principles

- Meet the needs of the stakeholder
- Covers enterprise end to end
- Apply single integrated framework
- Enable holistic approach
- Separate governance from management

Risk - Risk means destruction of Damage

- vulnerability * Threat
- Likelihood * Impact
- Likelihood - one year base line we have to consider
- Impact – because of impact what are consequences it is based on finance

Risk Matrix

Impact						
Critical	5	10	15	20	25	
High	4	8	12	16	20	
Medium	3	6	9	12	15	
Low	2	4	6	8	10	
Info	1	2	3	4	5	
	Info	Low	Medium	High	Critical	Likelihood

Above matrix based on Likelihood * Impact as we are calculating info * low as we can see Red – critical , Orange – High , yellow – Medium , blue – low , Green – Info

Risk Management process or frame work (RMF)

- NIST 800-53
- ISO27001
- ISC2 /ISACA (It is website they conduct certification part)

NIST

- We should prepare risk
- Risk category should take
- Risk selection
- Implementation whatever control we have identified in Risk face
- Assess Risk
- Authorization
- Monitor

ISC2 /ISACA

- Identify the risk
- Analyse the risk
- Prioritize
- Treatment plan
- Monitor the risk

Identify the risk - In this phase we have to identify the risk based on organization critical applications, servers, databases, assets

Analyse the risk – In this we have to three types of Risk Analyses
Quotatives – Based on money value
Qualitative – Experts opinion is required
Under the qualitative we have different types like

(a) Brain storming sessions
(b) Feed backs
(c) Fish bone analysis
(d) Five Yes (Here will create one templet under the templet 5 questions will be there

Hybrid Risk Analysis – Qualitative + Quantitate
Most of the organization will follows the Hybrid risk analysis only

Prioritization

Which risk we have to prioritize under this which is based on severity

Treatment plan

Risk acceptance
Risk Avoidance
Risk transfer like insurance
Risk reduction
Under the Risk reduction we have like

- Defence or detection – IDS/SIEM
- Preventative – IPS/EDR/WAF/Firewall
- Compensative - Alternative controls (defensive/offensive)

Risk register tools

- Excel sheet – Manual we do
- Logic gate
- Archer
- Zen GRC

Compliance

Compliance is nothing but Following rules and regulations
It is established guidelines, regulations or specifications or policies or the process based on legal legislation and also state and central

Ex of compliance

ISO 27001	CIS
GDPR	OWASTOP 10
HIPAA	ISO 14001
PCI DSS	ISO 9001
SOX	Fed ramp
SOC 1 & SOC 2	CCPA
NIST	Sabsa
TOGAF	GLBC

ISO 27001

Every organization has to certify with ISO 27001. It is importance of implementation security
Under this we have 18 clauses that is divided into 114 compliances
When we say compliance we have to go and we have to verify whether it is pass or fail. Every compliance we have to pass and also for every compliance we have to provide the evidence

Process Approach
Leader ship
Planning
Context of the organization
Above are definition

14 clauses

A.5 Information Security Policies - For ensuring policies are written and reviewed in line with the organization's security practices and overall direction

A.6 Organization of information security - For assigning responsibilities for specific tasks
A.7 Human resource security - For ensuring employees and contractors understand their responsibilities.
A.8 Asset management - For ensuring that organizations identify their information assets and define appropriate protection responsibilities
A.9 Access control - For ensuring employees can view only information relevant to their jobs
A.10 Cryptography - For encrypting data to ensure confidentiality and integrity.
A.11 Physical and environmental security - For preventing unauthorized physical access, damage or interference to premises or data, and controlling equipment to prevent loss, damage or theft of software, hardware and physical files
A.12 Operations security - For ensuring information processing facilities are secure
A.13 Communications Security - For protecting information networks
A.14 System acquisition, development and maintenance - For securing both internal systems and those that provide services over public networks
A.15 Supplier relationships - For properly managing contractual agreements with third parties
A.16 Information security incident management - For ensuring effective management and reporting of security incidents
A.17 Information security aspects of business continuity management - For minimizing business interruptions
A.18 Compliance - For ensuring adherence to relevant laws and regulations and mitigating the risks of noncompliance

Internal Audit – It will take min 2 day's time period here we have to coordinate with every one
Once internal audit gets complete then external Audit we have
External Audit – we have 3rd party vendors we do have like PWC, KPMG , Deloitte, EY
ISO27001 score rating is 5 at least we should 4.5 + then only we can expect the certification
Validation Is only for 1 year

Roles & Responsibilities

As a GRC I will take the risk Assessment even I participate in ISO 27001 like internal Audit member and I do collaboration of the work

GDPR (General Data Protection regulation)

This was entered into the market in 2018. This is applicable to Europe continent under the European union total 28 countries
This is mainly applicable to PIIA Data
Under GDPR we have lot of penalties & we have articles 1 to 99 it's a part of PIIA Data

Seven principles

- Transparency , lawfulness and fairness
- Purpose limitation
- Data Minimization
- Accuracy
- Storage limitation
- Confidentiality and Integrity
- Accountability

PCI (Payment card Industry) DSS Data security standards

Payment through credit card or debit, Payment card industry data security standards

This compliance is applicable when we are doing payment or financial transactions via Debit card or credit card

PCI DSS has 12 compliances under 6 categories

1) Regular patch updates for backend payment gateway servers
2) Default passwords we have to for change for payment gateway servers
3) Installing AV agent to protect malware category of the attacks
4) Protect credit card holder data
5) Use encryption mechanisms at rest and transit level
6) Assign a unique id for each user to segregate transactions
7) Logging and monitoring
8) Install and configure perimeter level firewall policies

SOX (Sarbanes Oxley act) -2002

SOX requires all financial reports or include internal controls report. It will shows company financial data and whether accurate and also safeguarding of financial data
Section 404 related to financial audits one of the compliance
ERP
SAP ORACLE
SOX operations under this

- Internal control

- Network activity
- Data base activity
- Login Activity
- User Activity
- Information Access

All these activity we have to integrate with the SIEM Tool these are controls fall under SOX Compliance

HIPAA (Health information portability accountability and act)

It is implemented in 1996
This compliance applicable to all the hospitals, healthcare product development companies and all the health insurance companies

SOC1 & SOC 2 - It is applicable to cloud deployments

Fed ramp – Under this more than 200 controls are available It is applicable to cloud deployments. Whoever is developing the product and deploying In the cloud in the North America, Those companies has to certify Fed ramp

NIST Frame work (National Institute of standard technology)

Under this we have 2 frame works

- Risk Management framework (RMF)
- Incident management or Incident response

OWASP TOP 10 - it will provide TOP 10 attacks of the application layer

ISO 9001 – QMS (Quality management system)

ISO 14001 - EMS (Environment management system)

CIS benchmark - Hardening of the servers

In DR- Disaster Recovery one of the web application firewall got comprised what will you do? (Interview Question)
Whatever WAF is there we will make it as primary WAF, & whatever primary WAF got compromised we will connect from the network that is network isolation of containment then will take the appropriate actions, will take care the incident response
Then I will check why it is got compromised , when it is got compromised , How it is got compromised then will take the incident response reacted to WAF get compromise
Will check authentication failures brute attack got compromised or may be through DOS attack WAF is got compromised or may be through Phishing e-mail WAF got compromised or may be through Malware and so on

Cyber Security Introduction

Cyber security or IT security is one and the same

What is cyber security (Interview Question)

It is a technique of protecting computers, systems, databases, servers, applications, network, end points, processes programmes from unauthorised access or attacks that are aimed for exploitation by the attacker

SOC (Security Operations Centre)

It is a site or room where security analysts will sit together will monitor 24*7*365 attacks or incidents or alerts or alarms or offenses and they will take care of incident response or incident investigation

What are all the other names for SOC

- CSIRT - Cyber Security incident response team
- CERT---Computer emergency response team
- SIRT- Security incident response team
- Sec Ops

SOC Team

L1 or Tier 01

L1 can also called Security analyst or Cyber security analyst or information security analyst
Role - Identify incident as false positive or true positive
Ex- 0 – 4 years

L2 or Tier 02

L2 can also called as Senior security analyst or Incident responder or Threat detector
Role – Identify the true positive
EX – 4 – 06 Years

L3 or Tier 03

L3 can also called as Threat Hunters, Reverse engineering and Malware analysts
Role - Escalations or Priority 1 tickets or P1 tickets and also take care of Fine tuning , Troubleshooting of log sources when ever logs are not reflecting in the siem tool, Use creation or correlation rules creation or Updating SOP's or Playbooks or run books
EX – 6 + Years

L4 or SOC Manager

L4 can also called as Escalation matrix or convincing the customer if something compromised or monitoring all the resources and SLA's

EX- 8+ Years

SIEM Security information and event management

SIEM is combination of SIM + SEM

- SIM- Security information management
- SEM- security event management
- As per Gartner report in 2005 Amrit Williams and stiffen

What SIEM Tool do

It do

- Log collection
- Log processing
- Log analysis
- Real time Log monitoring
- Notification of the alerts via SIEM dashboard

Log can also called as Data

What is Log (Interview Question)

Log is nothing but any computer recorded activity or actions it is called as Log

Event - Abnormal change of the log is called as event

Alert (Interview Question) - Notification of incident is called alert

Incident (Interview Question) - It will negatively impact CIA traid so that it will cause some business outage or impact

Notification – Action of notifying something is called notification

EPS – Event per second (Per second how many events are generating)

FPS – Flow per second

EPM – Event per minute

FPM – Flow per minute

Difference between event & flow

Abnormal activity is called event
Flow is form of packets

Log source or data source

Originator of the logs or from where the logs are generating

In your organization what types of Log sources or data sources are on boarded into SIEM Tool (Interview Question)

In my organization we have integrated log sources related logs like Firewall , proxy , NIDS/NIPS , WAF, All the servers , All the Applications , cloud , Vulnerability management & so on

Example of Log sources or Data sources;

- Network - LAN, WAN, Load balancer, Router, switches, wireless , WLC,
- Security - Firewall, proxy, IDS/IPS, WAF, AV/EDR, DLP, Encryption, FIM, Email gateways
- Infrastructure - All the servers, data bases, vulnerability management
- Application - All the applications (On-premise and cloud)
- Cloud log sources - IaaS, Paas, SaaS

Licensing option tool for SIEM tool

GB per day – All other SIEM tools – GB per day and number of end user (This is dedicated Exbeam

Licensing option tool for SIEM tool		GB/day	All other SIEM tools		
		GB/Day and Number of end users	Exbeam		
		Log Source od Data source	Total number of devvices	Eps count	Total number of EPS
	Total EPS	Firewall	10	100	1000
		Load Balncer	5	200	1000
		AD/DC	5	50	250
		Router	50	10	500
		Switch	10	5	50
					10000

Above information is provided by Business owner

Total 10k we have taken example

To know EPD (Events per day)

24hr*60sec*60sec * 10k

864000000

1-year EPD – EPD * 365 = 315360000000

1 Event or Log - 400 Kb or 500Kb

1 Year EPD/Kb/GB

1year EPD * 400 = 12614400000000 GB per day we can consider this number 126144GB

Compression ration - 1:10 or 1:15 or 1:17

- Splunk they take – 15
- IBM Q radar – 10
- MacAfee – 17

Vendor to vendor number gets change

Over all 1 year storage calculation

1year Storage before compression/10 (For Audit purpose as well as for investigation we do the storage)

IBM Q radar & MacAfee is very friendly storage calculation wise

IBM Q radar came with formal
For 90 days for 1000 EPS Counts so max storage is required 6.5 TB
For 1 years for 1000 EPS how much?
6.5*4*10 = 260 TB
For one year we have 4 quarters
This is done by Design team

Cyber security Definitions

Retention policy

How many number of days logs are storing in a device that may be online or offline it is called retention policy

Why we have to store logs

- For Auditing purpose
- For Forensic investigation

Because for analysing instant investigation
Ex ISO 27001 - 6 months offline and 6 months online

PCI DSS - 3 Months online and 3 months off line

Online Storage - storing the logs in inbuilt device

Off line - Exporting dumping into third party tools

Ex of off line storages

- SAN - storage area network
- NAS- Network area storage
- Cloud
- Tape
- IBM Q radar- Node
- MacAfee SIEM- Own Storage
- LogRhythm- Own storage

Forensic investigation

Ste by step process or Phase by phase of incident investigation is called Forensic investigation

Digital forensics

- Taking a raw image and doing forensic analysis
- Raw image – we called as Digital forensic
- Physical device- we called as Analogue

Tools

- Encase forensics
- Oxygen Forensics
- FTK-Access Dat
- Mobile forensics
- AD lab -Access Data
- Cellebrite

Aggregation –

Aggregation nothing but sum it Collection of the logs from different types of log sources or data sources and also from different locations

Ex: FW , proxy, NIDS/NIPS
Locations: Hyderabad, bang and Chennai

Normalization (Interview Question)

The processing of log into readable and structured format and also mapping them
And also we can say Rescaling of the logs is called Normalization
Ex: Raw log and Parsed log

Parsing (Interview Question)

Converting of all the log sources or data sources different types of log formats to unique log format (CEF) that should be understand by SIEM tool
Ex log formats

Syslog	Jason
BSD	XML
CSV	Jpeg

Above format is converted into CEF format

What is the difference between Normalization & Parsing (Interview Question)

CEF – Common event Format (Interview Question)

- SIEM tool will understand only CEF format
- All other SIEM tools- CEF
- If it is IBM Q radar we called as - LEEF

Parser development (Interview Question)

Parser development will be done vendors so we will provide the Raw logs to the vendor & Here vendor will develop the Parsers For unknow log format we will use parser development

Ex: Customized applications

Customized Product logs

Filtering (Interview Question)

Filtering is based log source, user , hostname, time stamp, date and time , source and so on

Querying (Interview Question)

asking for a formal way of question

Ex: SQL(DB)

Example query languages are

- AQL- Arial query language- IBM Q Radar
- PGSQL- Postgrads Structured query language- IBM Q radar
- SPL- Splunk programming language- Splunk
- SQL- structured query language- LogRhythm, MacAfee, Securonix HP ArcSight and Exbeam
- KQL- Kustof query language- Azure Sentinel

How to write example queries in SIEM too

1. In Past 24 hours of time period log in attempt failures query –
   Event id= " 4625 " {Filter time - Past 24 hours}

Boolean algebra function = AND , OR , NOT

2. Past 24 hours of log in attempt failures query along with specific user Ip or username

Event id = " 4625 " AND Username = " x "

Other example queries

- Hostname = " Appprod.com " (Application servers in production deployment)
- Hostname= " DBdev.com" (Data base environment)
- Hostname= " LT-HYD-X123 "
- IP Address = " 1010.10.10 "

*= all the logs (Pool of the logs or lake of the logs)

What is reference set in IBM Q radar (Interview Question)
In IBM Q radar this one will called as Reference set (based on references we can do the filter out option
Indexing (Interview Question)- Grouping of similar type of events or log sources

Ex: Grouping of all the firewalls
Grouping of all windows servers
Grouping of all Linux servers

Triage – Gathering information whenever any Alert come to the SIEM Tool 1st thing we will assign the ticket to ourselves. Later we create Instant ticket in the ticketing tool. There after will identify the what type of incident that we received
Triage means Gathering information related to IOC & IOA
IOC (indicator of Compromise) , IOA(Indicator of attacker)

Gathering information of IOC & IOA like any Alert is received will identify the IP address through which IP Address that Alert is received

Ip address- Source IP and Destination ip
Will identify the Location
Will identify end user system or server
Will identify whether it is Physical or virtual machines
Attacker IP Address
Will check the TTP (Tactics , Techniques and procedures)
Attacker location File name
Payload File size
Action File category
Payload Hash value

IOC – Indicators of compromise

- Victim IP or Destination IP
- Hostname or computer name or FQDN or system name
- Location
- Identification of whether it is end system or server
- File name
- File size
- File cat
- Hash Value

IOA – Indicator of Attack

- Attacker IP TTP
- Location

This above information is also called as Asset profiling or user profiling

What is IOC & IOA (Interview Question)

Threat intelligence feeds (Interview Question)

Threat intelligence feeds – This helps in proactive threat hunting it is also called as Also as called as Cyber Threat intelligence (CTI) some times we refers as GTI (Global Threat intelligence)

CTI or GTI is information gathered from a range of sources or tools about current potential attacks happening all over the world wide.
These Threat intelligences we have to take and we have to go and block in Respective tools like FW, EDR, DNS and Proxy.
Threat intelligence is subset of Proactive threat hunting
Ex: Threat intelligences for blocking we have Tools

We regularly receives these threat intelligence

We block malicious domains under DNS, Firewall , EDR
Malicious URL links or website we block under proxy, firewall
Malicious Hash values we block under EDR
Malicious IP Address we block under Firewall under policies Tab

Ex Tools

OSINT - Open source Intelligence – Open source

IBM X force	F5
Crowd strike	Source Fire
Check post	Logarithm (LR) GTI
Palo Alto	MacAfee

HP ArcSight or microfocus
From IBM X force to ArcSight is commercial

Threat Hunting - Hunting of the threats proactively . It is manual process

Proactive way of taking precautions and hunting of the threats is called proactive threat hunting
It depending on several parameters

- Threat intelligence feeds
- UEBA- UBA+ EBA (user and entity behavioural analytics) Technology which used ML/AI And Data analytics
- Vulnerability scans
- Risk assessment

- SOAR capabilities
- Crown- Jewel analysis (CJA)

UEBA

UBA- User Behavioural analytics (Based on the behaviour of the user or action of the user or habits of the user)

EBA- Entity behavioural analytics (Based on application, server, Database, system habits or action or behaviour)

UEBA concept is used for mainly unknown attacks based on Machine learning and Artificial intelligence along with Data analytics (Statistical approach)

It will notify or it will give Alert notification but it will not block

After deploying or enabling UEBA licensing SIEM tool will identify based on the behaviour of the end user or entity of the DB, application or server or end user system and finally it will generate notification of the incident using ML/AI.

Data Analytics- It is a statistical or mathematical approach for every incident is happening in the organization and it will generate risk score for every incident or alert

Risk score=anomaly factor * incident classification

Anomaly factor= Total number of abnormal events/ total number of events

Incident classification = what type of incident received . For every incident vendor provide will provide default score

- Ex: DoS =10
- DDoS =10
- Malware= 20
- SQL injection =15
- Phishing email = 10
- Authentication Failures= 15

We can do customization in number these are number given by the vendor
Ex 1/10 which is 10% so for Authentication failure is 15 = 150

Risk score = 10%*15 – 150

SOAR

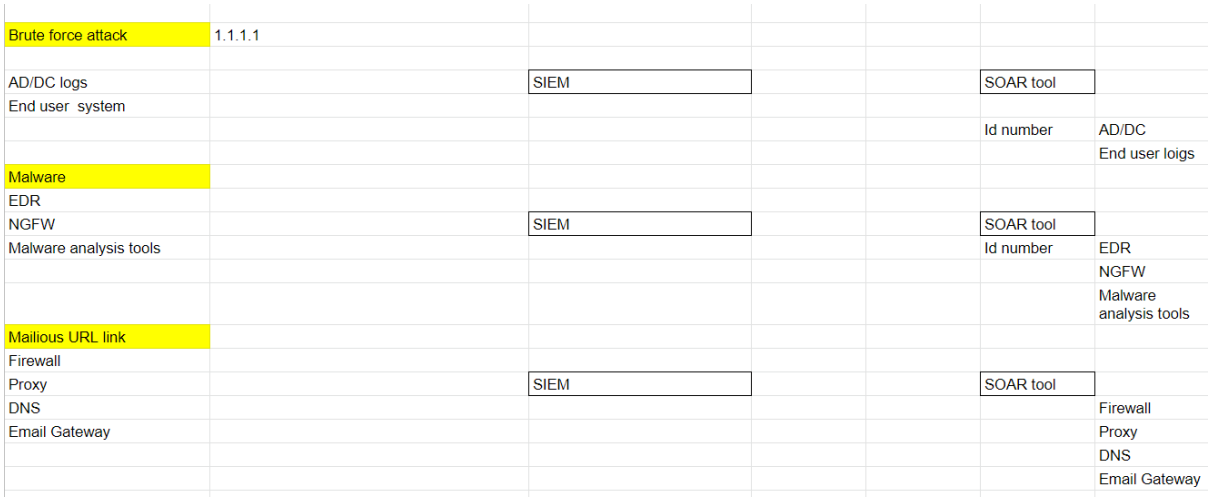
SOAR Stands for Security Orchestration and Automated response
Orchestration= Planning and designing outcome
Automation= Automatic blocking (There is no manual effort is required)
Response= Incident response will be taken in SOAR tool itself

We if combine everything may be something got compromise or may be one of the malware attack has come & so on

The main advantage is whenever any attack comes directly we can block here itself no need to go for firewall
Similar type of log sources logs will be reflected in the alert notification which means SIEM Logs whatever Logs that we are integrating to the SIEM Tool Those Logs we have to integrate to SOAR Tool
Below picture we have different types of Attacks like Brute Force Attack, Malware, malicious URL Links
For Brute force the possible log sources are

- Active Directory/ Domain controller
- End user system

AD&DC Log integration method is Collector Agent Method, even for End user same collector Agent method only
1st we have integrate these Logs to the SIEM Tool
SIEM Tool Logs then we have to Feed it into SOAR Tool
Under the SOAR Tool one ID Number will generated along with that Automatically what all possible Log sources are there Those Log sources we can get nothing but AD/DC Log sources as well as End user Log sources
After verifying this one Log Analysis , log collection , Log monitoring , Analysing everything we have found that This Brute force Attack is coming from 1.1.1.1
We will block in Fire wall but under SOAR Tool directly we can block here with out going to the Firewall
In the SOAR Tool itself Action is available we have to go the Action we have to block the IP Address that replication we can see under the Firewall so that is called Automated Response



Malware category of Attack

Possible Log sources are like

- EDR
- NGFW

Malware Analysis Tools

These Logs we integrate as it is to SIEM then we feed it into SOAR Tool

Ticket number will be generated All the log sources will be Automatically Log sources will Appear in the respective SOAR Tool

Those Replication will go to EDR Tool which ever Hash value that we blocked

Malicious URL Link

- Possible Log sources are like
- Firewall
- Proxy
- DNS
- Email security Gate way

These Logs we integrate as it is to SIEM then we feed it into SOAR Tool

Whenever these malicious URL links related automatically all these log sources, it will replicated and it will come as a attachment. Now we will do the manual verification nothing but reputation checks like whatever URL it Is coming to us then will block that particular URL Link under the proxy. That replication we can see in Proxy only

Tools we have

- Splunk- Phantom
- IBM Q radar- IBM resilient
- Exabeam- Incident Responder
- Palo Alto- XSOAR

Crown Jewel Analysis

This frame work is provided MITRE It is completely Critical Assets & It is subset of Risk Management frame work

Which means the Information assets has the greatest value and it would cause major impact to the business if it is getting compromised
Crown Jewels = Critical assets (Servers or databases or application)
First we have to identify critical Assets and have to do the risk assessment based money value

Correlation

Linking one event with another event or mapping using some logic that is called correlation

Correlation rules or Use cases

Linking event with another event or mapping using logic and also algorithms and finally alerts notification will be generated when the abnormal activity will happen in the end, network, application, cloud, databases

Did you created any time correlations or use cases (Interview Question)
It is created by implementation team, I don't have the access I didn't created any correlation rule because working as L1 but I know how create correlation rule because I do 5 to 10 correlation logics
Most recent investigation you have done (Interview Question)
Two types of correlation rules
Default (provided bu SIEM tool vendor)- it is Out of box nothing but
Customized correlation rules
Every vendor backed under event processor or Log processor or Data processor or Log manager CRE or AIE is available

Where Correlation backend process will happen (Interview Question)
Under event processer or Log processer or Log manager this is also called as Data processer as well. CRE Engine is available under the 2 component that is called Log processer or Event processer or Data processer or Log manager it is backend hardware module processing of the correlation rule will happen in the event processer

Example
Multiple authentication log in failures with 1 minutes of the time with 5 failures (It is Brute force Attack)
VPN authentication failures are coming from different geographical locations within short span of time (1 Hour)
From disabled account log in failures
From terminated account log in failures
From terminated Account Login failures how it will come what is the reason (Interview Question)
From Cache because it will store respective passwords in the Cache

Log integration or log collection methods

Basically, it is implementation level

How to collect or send logs to SIEM tool
That is nothing but Log integration & Log monitoring. We have two types

- Push
- Pull

Push –

Login to log source or data source and send the logs to SIEM tool
Ex:

- Syslog server method
- collector agent - push method
- Cloud connector

We have to login into respective log sources or data sources and there we have to do some configuration and finally we have to see the test connectivity and then we able see Logs in SIEM Tool or not which means reflecting are not that is called Push mechanism

Pull –

Log into SIEM tool pull the logs from log sources or data sources
Ex: API token method

we have to go to the SIEM Tool we have to pull Logs from the respective data sources or log sources that is the pull mechanism

Syslog server – Log into log sources or data sources

- click on syslog server
- configure syslog's

SIEM Tool Name	SIEM Host Name or IP Address	Protocol	Port Number	Log Format
Splunk	10.10.10.1	TCP/UDP	541	Bsd, syslog , xml,Jsv, cson
		Test connectivity		

Host name is nothing but management name because for every device if we want to access the device remotely we have to provide the host name for the easy remembering purpose that is called Host name

Test connectivity we have to click on in case

Once you are configuring the Logs still it is not reflecting in SIEM Tool how can you verify or Trouble shoot (Interview Question)

I will verify whether configuration done correctly or not, nothing but I cross check Host name or IP Address is correct or not , protocol & number define correct are not

1st I will validate configuration

Then I will check into the Firewall and go through the Logs & reports if it is Fortinet firewall , if it pal alto will check in Monitor tab

Then I will click on the forwarded events , forwarded traffic , then I will specify source IP as a Firewall , then Destination IP as SIEM Tool, after that we will do

packet capture. After doing Pcap then will take that particular file then will analyse in Wire shark

- We have to Verify the configuration
- Will Take the PCAP file and go to Wireshark and analyse TCP/IP layer analysis
- Then In application layer what is the issue like (DNS, hostnames or HTTP or https traffic)
- In transport layer and Network (Internet) whether TCP 3 way handshake is completing or packet retransmission happening or packet is dropping or packet is resetting the connection
- In network interface layer I will verify is there any cable issues or frames mismatch
- If it is don't work then I will raise ticket to supporting vendor

Did you on aboard any log sources or data sources to SIEM tool ? (Interview Question)

Yes, I integrated or onboarded log sources or data sources to SIEM tool

- Syslog
- Collector Agent
- Cloud connector
- API Method
- WIN Collector Agent
- MSRPC Method
- WMI Method
- APP Method
- Flow collector method

Collector Agent method

Agent will be provided vendor
for integrating server log to SIEM to we will collector agent method
Ex: Windows server, Unix, data base server, web servers, app servers
Log into server
Install agent
Specify source Ip, destination Ip, port number , protocol

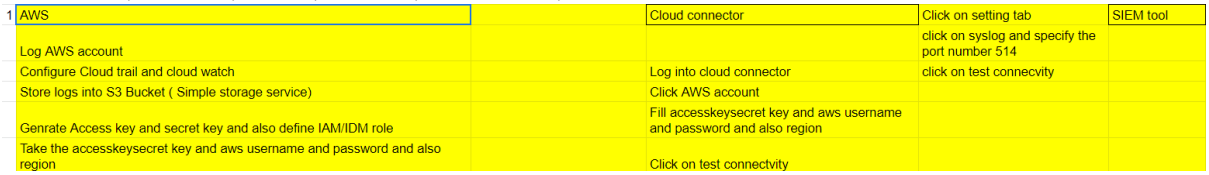
Source IP	Destination IP	Port number	Protocol
Server IP	SIEM Tool IP	Exbeam - 9093	TCP/UDP
		For other vendors 8443, 443	
		Splunk – 9997 , IBM Q Radar - 6514	

Vendor to vendor collector Agent method port number is vary

If server log or not reflecting or not able to see in the SEIM tool ? what troubleshoot will you do?
1) we have to Check the configuration
2) Then we have to Take the TCP dump file (windows or Linux) and analyse it manually
3) Network connectivity issues verify using Ping command and Traceroute from server SIEM Tool is accessible are not

Cloud connector Method

If we integrate cloud logs SIEM tool we will use Cloud connector method
Cloud connector means it will act as a Gateway or bridge or mediator
Ex: AWS, Azure, GCP, oracle, Ali baba , IBM



1	AWS		Cloud connector	Click on setting tab	SIEM tool
	Log AWS account			click on syslog and specify the port number 514	
	Configure Cloud trail and cloud watch		Log into cloud connector	click on test connecvity	
	Store logs into S3 Bucket (Simple storage service)		Click AWS account		
	Genrate Access key and secret key and also define IAM/IDM role		Fill accesskeysecret key and aws username and password and also region		
	Take the accesskeysecret key and aws username and password and also region		Click on test connectvity		

From the Above picture Cloud connector act as bridge between Cloud logs sources to the SIEM Tool or gate way we can say

Do you know how to integrate cloud log sources to SIEM Tool

AWS

Log into AWS account
Configure Cloud trail and cloud watch
Store logs into S3 Bucket (Simple storage service)
Generate Access key and secret key and also define IAM/IDM role
Take the access key secret key and AWS username and password and also region

Cloud connecter

Log into cloud connector
Click AWS account
Fill access key secret key and AWS username and password and also region
Click on test connectivity

- From cloud connector side click on Setting Tab
- click on syslog and specify the port number 514
- click on test connectivity

Above dots are common for any Log sources

We have the second method or above method
Proof point or service now or O365

We have to Ask owner of the tool create one dedicated account for admin in respective tools

- User name: Admin
- Password: xxxxxxx

Now Login to cloud connector

Click proof point ot O365 or service now
enter username and password
click on test connectivity

For deployment we have the Tools like

- Sky information
- Oracle
- IBM
- Citrix

Above these connectors we have to integrate with SIEM Tool
We install these software in SIEM Tool itself

App method

This method most of the cases applicable to Splunk
Respective vendors created customized apps to integrate or to collect log to SIEM tool

Flow collector method

This method is applicable to collect the flow data (Traffic)- Span or mirror

- Net flow
- Yes flow
- J flow data

Win collector Agent method

This method *is applicable to most of the cases IBM Q radar
Mainly this method used to windows operating system logs to SIEM tool
Log into server
Install agent
Specify source Ip, destination Ip, port number , protocol

Source IP	Destination IP	Port number	Protocol
Server IP	SIEM Tool IP	IBM Q radar 6514	TCP/UDP

WMI method

Windows messaging infrastructure
it is agent less method . it can integrate based on APPS
Draw back : 50EPS COUNT WE WILL USE WMI method

MSRPC - Microsoft Remote procedure cll

it is agent less method . it can integrate based on APPS
It will support more than 50EPS (Windows machines)
API method
Most of the cases it is applicable SaaS based applications
Log into data source
generate access key and URL and secret key
Take the access key or URL and secret key go to SIEM tool and pull the log respective data source or log source

EX – Sophos EDR , Crowd Strike
Vendors or tools

IBM Q Radar	Palo Alto
Splunk	Alien Vault (AT &T)
Exabeam	AWS Guard duty
Logrthym	Azure sentinel
RSA (Dell)	GCP SIEM
Event viewer	Cisco Manage engine
MacAfee	Forti SIEM
HP ArcSight or Microfocus	F5

In above vendor IBM Q Radar, Splunk, Exabeam, Logrthym, Azure sentinel very popular
ELK (elastic search, Kibana and log stash) – it is combination of Open source & Commercial both available

Database (What all backend Data Base SIEM Tool Use) Interview Question

- SQL
- PGSQL
- AQL
- KQL

In windows what types of Logs we see (Interview Question)
Application logs, network logs, server logs so on
In Linux what types of Logs we see (Interview Question)
Application logs, network logs, server logs so on
In Firewall what type of Logs we see (Interview Question)

In generic way Audit failure & Audit success
Application configurations

So these are other Logs
For any Log sources

SIEM components or SIEM architecture diagram

SIEM Components can also be called SIEM architecture

We have 03 components under SIEM those

- Log collector
- Log Manager or Log processor or Data Processor
- ESM-Enterprise security Manager

Log collector

Collection of the logs from different types of log sources and also different locations. After Log collector basically 3 things it will do like aggregation of the logs, normalization and parsing. Those logs it will send it to Log manger or data processor or log processor

Log Manager or Log processor or Data Processor

Log manager or log processor will do processing of the logs. It is nothing but indexing, querying and filtering and in backend we will have one more engine that is CRE – correlation Rule Engine

ESM-Enterprise security Manager

This is called User console or GUI which means we will go and we will do instant investigation here

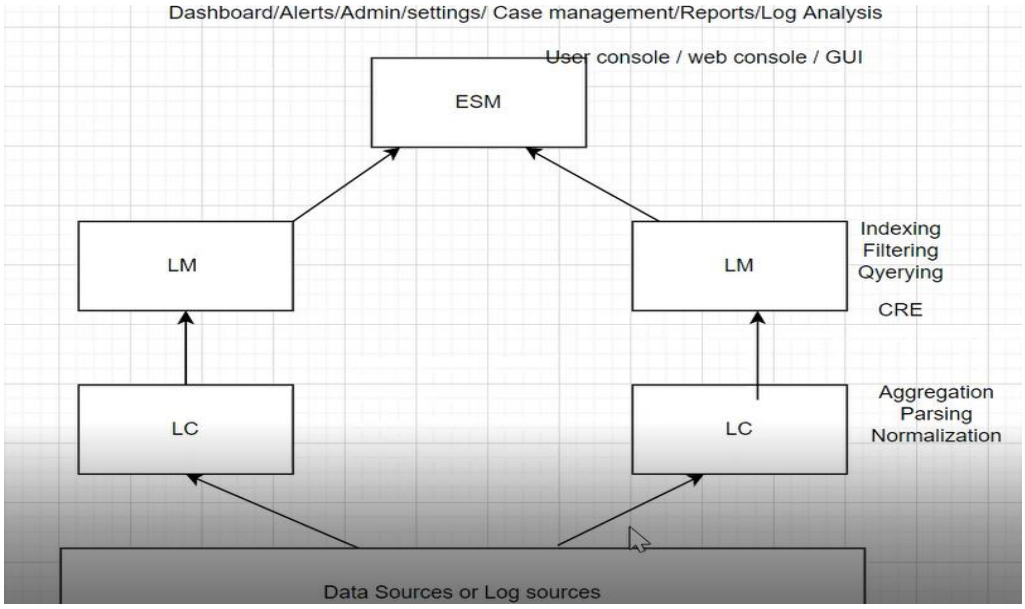
Whenever any abnormal or malicious or suspicious activity will happen in the end point, network , application, cloud, infrastructure log collector it will collect the logs and it will send to log processor . Log processor will all the log processing technologies, those processed log it will hit corelation rules or use cases and finally front end of the SIEM tool or user console or GUI incidents or alerts or alarms or offenses will be generated. As a L1, L2 and L3 teams they will do forensic or incident investigation

From the Below Architecture Diagram of SIEM Tool we can notice double of LC,LM & ESM reason is when left hand side gets down the right hand side will take action this mainly for high availability

LC (Log collectors will collect all the logs from Log sources then it will do Aggregation, Parsing & Normalization

Those Logs it will send to LM (Log Manager) and it will do indexing, querying and filtering and backend we will have one more engine that is CRE – correlation Rule Engine

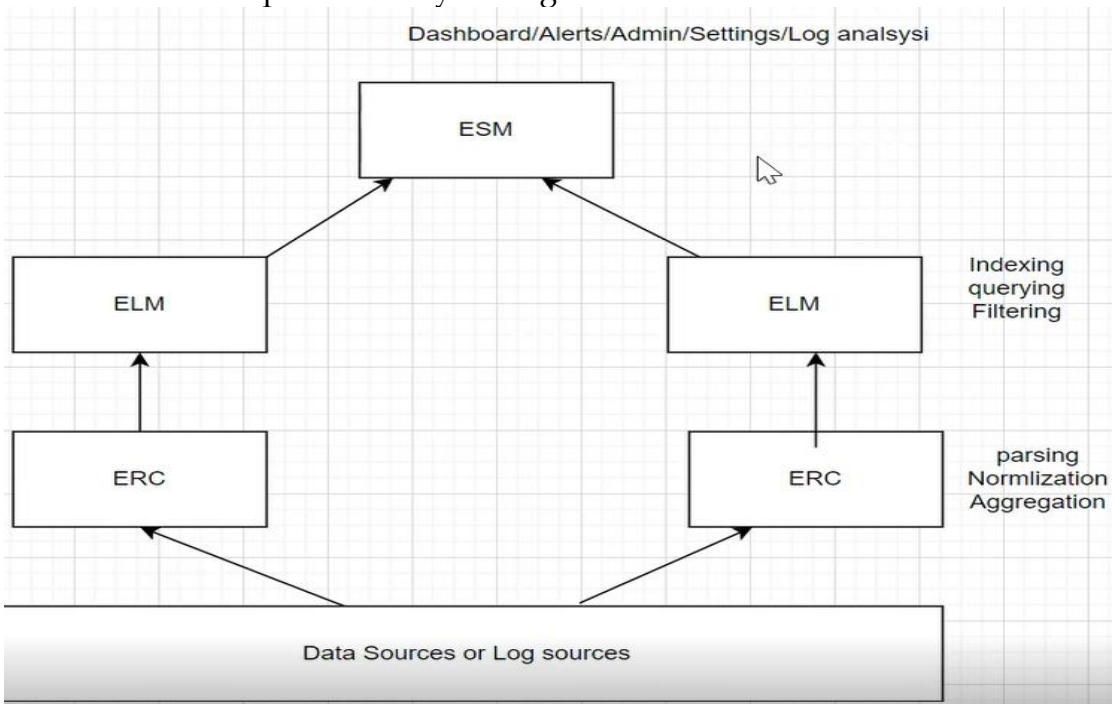
ESM is the front end tool this is called user console or web console basically SOC Main work will in ESM only



MacAfee (Risk score 0 To 100)

MacAfee has mainly three components

- ERC- Event receiver
- ELM- Event log manager
- ESM- Enterprise security manager



From the above diagram ERC will collect the Logs from Data sources using different log integration method, so after collecting of the logs it will do Aggregation, Parsing

& Normalization part. Above ESM as we can see Tabs in SIEM like Dashboard , Alerts/Admin/settings/Log Analysis
Those logs it will send to ELM & it will do processing of the Logs like indexing , filtering , querying part and back end we have correlation engine so whenever the any suspicious are any malicious or abnormal activity happening in the application or servers or Data bases so on those logs it will hit to the CRE then finally front end of the ESM nothing but SIEM tool Alerts or incidents will be generated
As a SOC team we will take care of the incident investigation otherwise forensic investigation

Case Management – we can do incident investigation there itself no need to rise the ticket in the ticketing tool like a third party

Licensing

- ADM- Application data monitor
- DEM- Database event monitor
- GTI- Global Threat intelligence
- UEBA- Third party

Storage
SOAR
Premium Support

Log Integration Methods

- Syslog
- WMI
- Collector agent (Win collector agent)

cloud connector
Flow collector

Star in the SIEM Tool it is nothing but Pool of the logs which means so many

LogRhythm (LR)

LR is popular tool according to Gartner report
LC- Log collector
DP and DI- Data processor and Data indexer
EM or PM- Event manager or Platform manager
LR contains two consoles

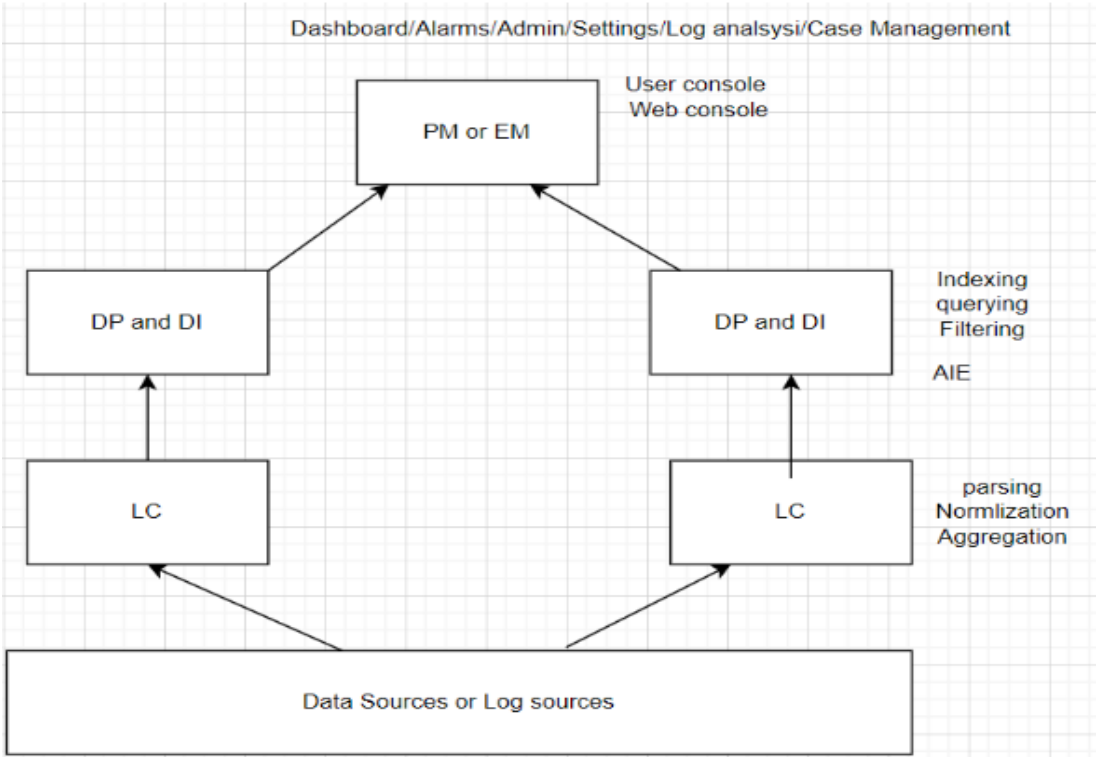
- User console - we Trouble shoot the logs, waking up the agent, we take care AIE Customized rules creation , then we have to Upgrade the software, Firm updates, then we can see the CPU utilization, RAM utilization
- Web console - Dashboard/Alarms/Admin/Settings/Log analysis/Case Management

Ex: Incidents

AIE : Privilege escalation (90) Critical

AIE : vpn authentication failure from different locations with in short span of time (100) Critical

Risk score – 0 to 100



Here we can notice Case Management which mean instant investigation we can do here in LogRhythm itself

Log collector will not collect only malicious things it will collect normal as well it is collection of both Normal & Abnormal both

Once it is collecting the logs it will send it to using different types of log integration methods like Aggregation, parsing & Normalization those logs wit will send it to data processer & Data indexer both It will do data processing of the logs as well indexing of the logs like querying , indexing , filtering part

Back end they have AIE (Advance Intelligence engine) whenever any abnormal or malicious activity get happened those logs it will hit to AIE engine and front end of the EM OR PM alarms will be generated

Licensing

UEBA Threat hunting

SOAR Premium support

LR deployments

Hardware module – 3625 All in one box deployment

Software- Windows servers

Log Integration methods

Syslog	WMI
Collector agent	Cloud Connector

Exabeam

3 components

- Log collector
- Node
- Data Lake – Mainly for search logs
- AA- Advanced analytics

Log collector will collect the log from all the log sources or Data source using different log integration method after doing log collection of the logs it will do like parsing, Aggregation & Normalization. Those logs will send it to Nodes.

Now Node will do processing of the Logs like Indexing , querying & filtering backend we have the CRE Engine

Node can be used for storing purpose ex; If Data link capacity is 1TB under Node we can store 2.5 & 2.5

Those Nodes will send it to Data lake (Data lake is nothing but Data Pool we use for search queries purpose only mainly we use for dipper investigation

Under Data link we can integrate it into AA – Advanced analytics engine (It is combination of UEBA , I has SOAR Capabilities that is incident responder in Exabeam & finally we have the threat hunting option as well . It integrate with syslog by using 514 port number

Under AA- Advanced analytics we can see

- User bevorial incidents
- Entity related incidents
- Watch guard (Dog)- Security analysts
- Senior management accounts
- Phishing emails

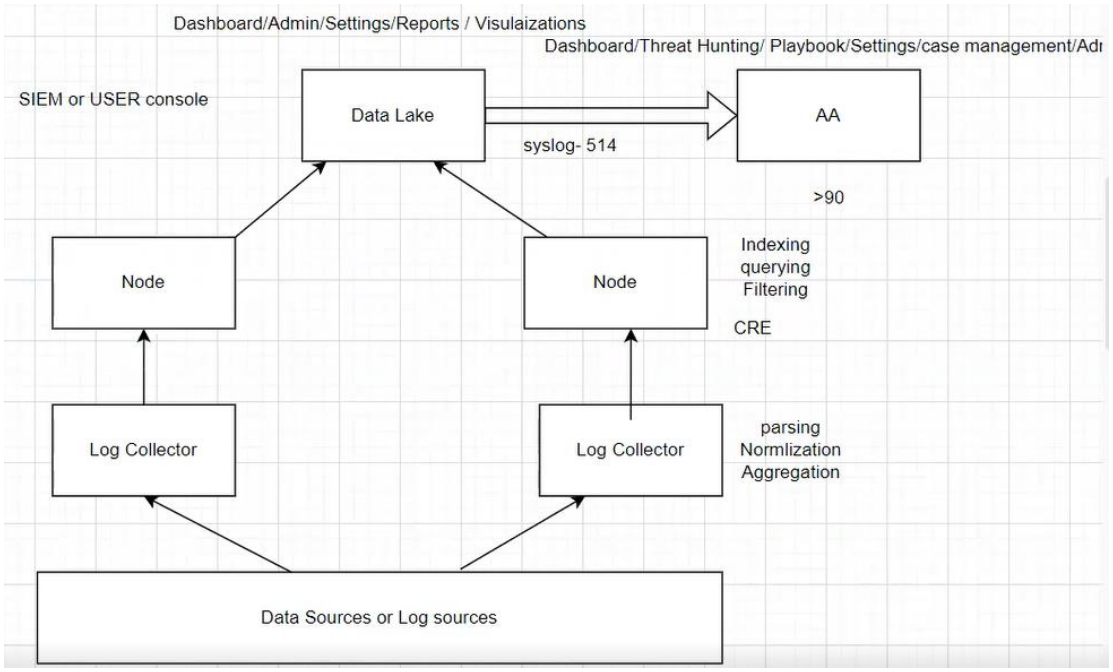
Two console we have

• Dash board	Reports
• Admin	Visualization
• Settings	

AA – It contains Dashboards, Threat hunting , Play book , Settings , Case Management

If risk score is > 90 for those incidents only we work on if it is < 90 low or less than severity

Risk score - 0 to unlimited



In LogRhythm incidents we called as Alerts or Alarms
MacAfee incidents we called as Alerts or Incidents
IBM Q Radar incidents we called as Offences
Exabeam for incidents we called incidents only

Additional licensing

UEBA ---------- Commercial
SOAR- Incident responder ---------- Commercial
Premium support ---------- Commercial
Threat hunting ---------- Free
Playbooks ---------- Free
Case management ---------- Free

Storing of the Logs - Data lake & Node

Querying of the logs - SQL
Log integration methods

- Syslog – 514
- Collector agent------9093 it support for all OS
- Cloud connector - It use sky formation

Model Number
Data Lake – 4000

Node – 2000/300
Firm wear version
Date lake-- i62
AA--i60

Deployments - Hardware module

Log source

S.no	Log soiurce nam	Owner/Team	Collection/integr	Status	Remarks/comments
1	Firewall	Network security	syslog	Onboarded	Yes
2	DC/AD	Windows admin/sys admin	collector agent	Not	some issue
3	Router	Network team	syslog	Onboarded	some issue
4	Switch	Network team	sylog	Onboarded	
5	WAF	Security team	syslog	Onboarded	
6	EDR	End point security	api	Onboarded	
7	Load balancer	Network team	syslog	not	
8	Application	Application dev team	syslog	Onboarded	
9	Web server	Server team	collector agent	not	
10	DB server	DB team	collector agent	Onboarded	

When ever we are purchasing the SIEM tool we have to identify above all these log sources and what is the status of each and every log sources

Did you on board any time log source or did you integrate any log source

Splunk

3 components

Splunk or search forwarders
Search indexers – It do processing of the Logs
Search heads (SIEM console or user console)

Splunk forwarders it will collects the logs from the different types of log sources ex; firewall , proxy , IDS/IPS & so on those logs it will do the aggregation , parsing & normalization and so on

Search indexers – It do processing of the Logs and indexing of the logs it compete with three technologies like querying , Indexing , Filtering & CRE

Search heads – Incident investigation

Splunk forwarders

- Light weight forwarder – It does collection of the logs and parsing
- Heavy weight forwarder - collection of the logs and parsing

- Universal forwarder - Collection of the logs it will do but parsing it will not do

To collect the logs we use these forwarders

Querying of the logs - SPL(Splunk programming language)

Risk score or incident score 0 – 100

Licensing

UEBA Threat Hunting
SOAR- Phantom Premium support

Log integration methods

syslog
Splunk forwarder (Collector agent)
Splunk apps

Splunk ports (Interview question)

- Splunk web port:8000
- Network port number (Syslog): 514
- Management port number : 8089
- Splunk admin: 9997

HP Arc Sight or Micro focus

3 Components

- LC (Log collector) – it do Aggregation , parsing & Normalization
- LM (Log Management) – It do processing of the logs and it does indexing , querying & filtering
- ESM or Express -

Under Log collector we have 2 components

Smart connector - collection of the logs for known format

Flex connector - If we don't know log format of the logs then we will raise ticket with vendor then they will create or develop flex connector for parsing and collection of the logs

Additional licensing

- Risk manager (Asset inventory)
- Vulnerability of scanning
- GTI (Global Threat intelligence)

Deployment - Software (Windows or Linux)

Consoles

ACC- Arc sight command centre – This is mainly used for the dash boards /Reports/CRE/Admin (Use by the Implementation team and managers)

SIEM console or user console or Arc sight console - This is mainly used for the dash boards /Reports/Alarms/Admin/Case management (Used by the security team)

Log integration methods

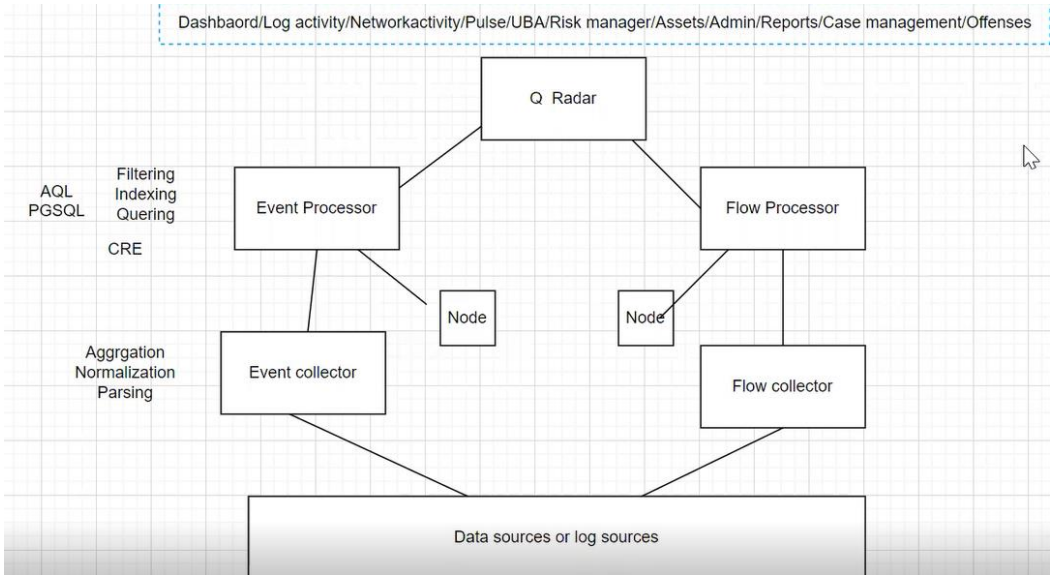
Syslog

collector agent method

Apps

WMI method

IBM Q Radar



IBM Q Radar we can deploy in the both the ways which is nothing but on premise & cloud deployment

It is user friendly as compare to Splunk , Exabeam & secure Ionics

For IBM Q Radar we have 03 components directly it has 3 components but indirectly it has 04 components

Q radar Console or SIEM console or User console or ESM (Here we do the instant investigation)

Event processor or Flow processor (sometimes it refer as a Data Processor)

Event collector and Flow collector (Data collector)

Node – For storage purpose

HP Arc Sight & MacAfee these tools will collect both net flow data as well as log Splunk , Exabeam , Azure sentinel these tools will not support both

What is the difference between the Event processor & Flow processor (Interview Question)

Event processer will collect the Events or Logs it use different types of integration method processing it will do backend It will do indexing, querying , filtering part
Flow processor will collect the flow data in the form of IP Packets it is dedicated to hard ware device like 1800 model is there , 1900 model we have & so on

Event collector and Flow collector (Data collector)

Event collector will collect the logs from the different types of log integration methods
Flow collector it will collect the flow data

Architecture

Event collector collects the logs from the different types of the log sources. In the similar way flow collector will collect the flow data from the different types of Data sources

Event collector additional it will do Aggregation , Normalization , Parsing & Flow collector will also do the same Aggregation , Normalization , Parsing

Once done those logs will send it to the event processor & event processor will do event processing of the logs

Flow processor will do the flow processing of the data then it will compete the filtering , querying , indexing.

And backend we have the core relation rule engine so whenever any abnormal or malicious activity is happening so based on the core relation rules whatever we configured or based on use case whatever we configured

Front end of the consoles offences are generated as a SOC Team member we take the incident investigation on it

Whatever processing logs are completed it will store in the Nodes it is mainly for the storing of the logs

In backend two different data bases which are supporting by IBM Q Radar

- AQL
- PGSQL

For querying purpose basically

IBM Q Radar mainly consoles are like Dash board, Log activity , network activity , plus , UBA, Risk Manager, Assets , Admin , Case management , Offense Reports these are supported by IBM Q Radar

Dash Board – we use for summary

Log Activity – we use filtering purpose it is related to events

- We can see all the Logs
- Health check up
- Log source here everything like windows , linux , firewall , proxy, IDS/IPS, AV , DLP, Cloud everything

Network Activity - It is related to flow & traffic related Activity we go to the network related Tab, If we want to Packet capture whenever any incident is coming to analyse the wire shark tool want to trouble shoot and if we want to find out root cause analysis

Root cause Analysis means when ever something got comprise we will prepare one document to the client and we have to explain why it is got comprise like what is the root what is the issue and so how it is got compromised, why it is got comprised , when it is got compromised and what all the recommendation steps that we have taken that is called Root cause Analysis

Plus – It will give over all summary of the Dash Board what's going on like health check-up & so on

Did you created anytime reports in IBM Q Radar (Interview Question)

UBA – Combination of user & entity its like a machine learning mechanism

Risk manager – It provide vulnerability scanning IBM Q Radar has inbuilt scanning of the Assets

Assets – Tools we use for asset Inventory like Service Now, HP , CMDB

Admin - what ever initial configurations we have to do kind of implementation ex; LDAP Integration , Primary DNS , Secondary server integrations then we have to define the management IP (how to login remotely) , Subnet mask , then we have to provide default way investigation , User , user Management tab , Tenant , SMTP Server Integration to receive the Alerts , Log sources

Reports – Reports will be generated based on the Log sources or process wise will be generated (process reports we have like Day report what are the incidents that in the similar way monthly reports, weekly reports & so on

- We do health check up reports
- Log sources
- Incident reports
- Firewall use cases

- Proxy use cases
- AV/EDR

Case management - Incident management or incident responder

Offenses – offenses is nothing but incidents or Alert or Alarm under this our main role here we have to monitor what is what

Under offenses we have certain classifications

My Offenses - whatever incidents that we are working on may today shift is starting at 9 AM so we login into the IBM Q Radar tool then we click on the offenses Tab then we assign the ticket to ourselves then whatever ticket I assign to myself that one is called my offense

All offenses – For entire team

Offenses by sources IP – It will come through IP Wise

Offenses by destination –

Offenses by network

Rules Tab – This is dedicated to Core relations rule tab

X Force – It is threat intelligence integration

Use Case Manager – Nothing but correlation manager by default support out of box correlation rules or use case it will manage all the use cases for different types of attacks

Do you know how to create core relation rule or Do you how to create use case creation (Interview Question)

Yes I know how to create core relation rule. I will login into the IBM Q Radar from then I go to the offenses tab then I click on the rules tab then will click on the new actions , then will click on the flow , then will click on the wizard & so on

Our main role will be under

- Log Activity
- Network Activity
- Offenses

Different types of Data source & log sources we have

Ex ; Firewall, proxy , NIDS/NIPS, All the applications , All the servers & All the cloud related applications as well

Log integration methods

- Syslog (514 & 6514)

- WMI (This is not recommended it will support only 50 events per second we above 50 we use MSRPC Method
- Win collector agent (This is dedicated to windows logs)
- MSRPC
- Apps (This is cloud connector method)
- Flow collector (SPAN or Mirror method)

Hard ware Modules

1700 , 1800 , 1900

CEF- Common format name (Interview Question) LEEF (Light extended event format)

Whatever Raw logs are generated those are not in unique format it has the different types of log format all those different types of logs sources are will be converted by SIEM Tool understandable format That is common event format
All other vendors will called as CEF But only IBM Q Radar will call as LEEF

Additional modules or licensing

UBA	Threat Hunting
PULSE	Premium support
Flow collector	Assets and Risk Manager
SOAR (IBM Resilient)	IBM X Force

Licensing is based on the – GB per Day in SIEM Tool

1000 EPS for 90 days and its for 6.5 TB

Deployment
On premise- IBM Q radar (Hardware)
Cloud---- Q RoC (Q Radar on Cloud)

On premise or Data centre or Deployment

- Standalone- Single
- Distributed- Multiple
- All in box- Single location (Vendor we is supporting IBM Q Radar , MacAfee , LogRhythm)
- For Cloud deployment it supports Q Rock

Q Radar Stand alone deployment (Single Location)

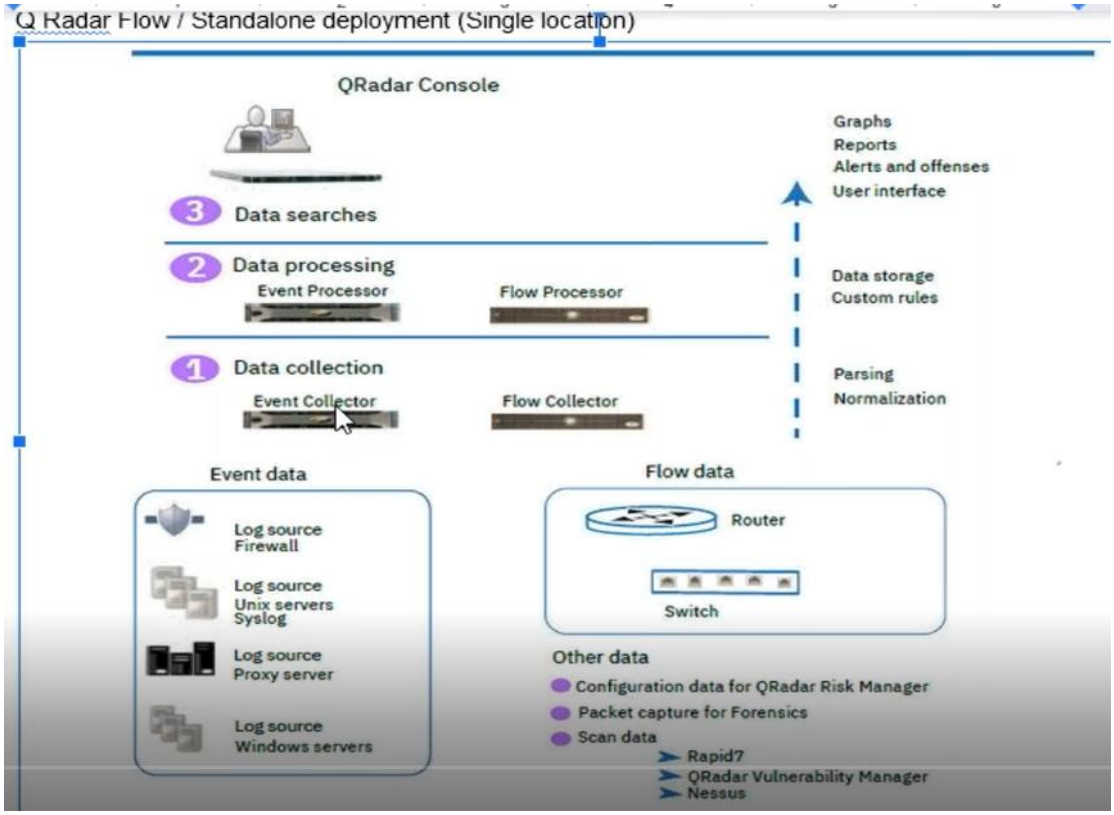
This is for single deployment we use
Event collector & Flow collector
Flow collector & Flow processor

We can see the Event data & Flow data. We collect Flow data from the Routers & Switches even load balancers , firewall , proxy, IDS/IPS & so on mainly for the network related data we use flow data

Events may be anything employee related like laptop , Domain controller , All the server related & so on

Data collection it is combination of Both Event collector & Flow collector which do parsing & Normalization

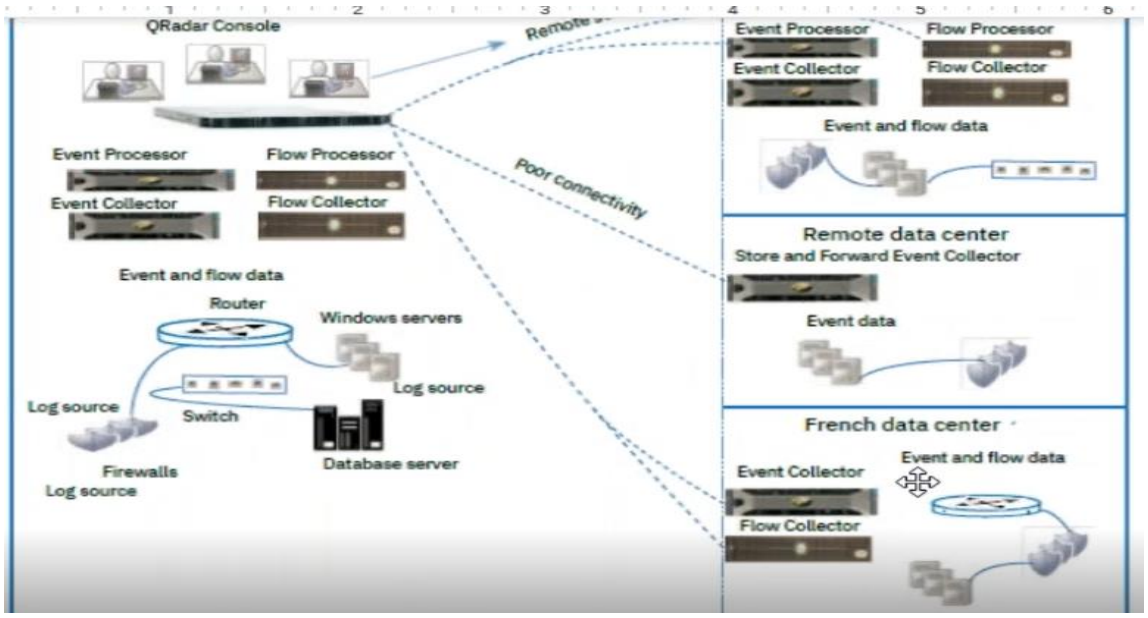
Data processing it is combination of Event process & Flow processor it do Data storage & Custom rules apart from this it do indexing , querying , Filtering also



Distributed Deployment

We use Distributed Deployment when organization is in multiple locations Ex; HDFC Bank head office is Mumbai and multiple branches Hyderabad , Delhi , Chennai etc

In the head quarters we have to keep all the modules like Event collector & Event processor & Flow collector & Flow processor main our hard wear module



Event collector will collect all the events data nothing but Logs

Flow collector will collect all the flow data then it will complete the Aggregation , parsing , normalization Those logs & flow data it will go to the event processor & flow processor

Then it will complete the Data processing , Log processing & flow processing and also it will do indexing , querying , filtering & backend they have correlation rule engine and finally those logs will go to the Q Radar console

Main module is there under the Data centre only not in any branches as we see which is in white colour those are completely remote branch offices only

One of the firewall is there how can you assume firewall events per second EPS per second how many events are generated (Interview Question)

I will go & search couple of websites like Isaca , European & so on and I will do the assumption for Fire wall it may 50 EPS count it is generating on top this additionally add some buffer then finally will choose the total number of EPS count

All in one Deployment or Q Radar All in one Box

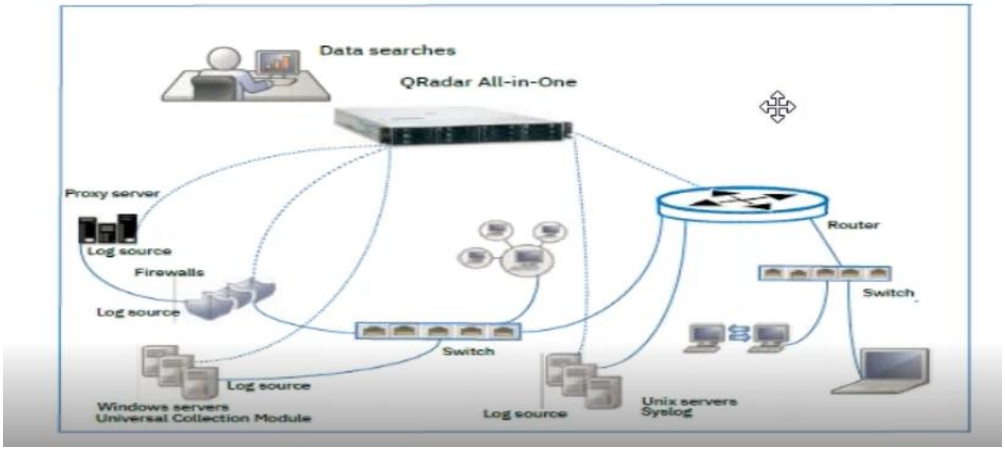
It do event collector & flow collector , Event processor & flow processor including Node will be there in a box that is called All in one Box

Vendors who are supporting

MacAfee & LogRhythm , IBM Q Radar only these three are supporting for all in one box deployment

Normally 0 to 1000 users we use this All in one deployment because it less number of users , less number of applications , Less number of EPS Count and so on

All in one deployment



For Cloud deployment it supports Q Rock

IBM Q Radar Definitions (Risk score 0 To 10)

Event collector

Collection of the logs from different type of different types of log sources or data sources using different types of log integration methods
Meaning here collection of the logs or events from the firewall or proxy or Domain controller or may be Router & switches and so on. Whatever log sources or Data sources we have 1st we have to identify so using different types of log integration methods like Syslog method , WMI Method or MSRPC Method or Q Radar flow method or Event collector method we have to use these integration methods & we have to collect the logs

Flow collector

It is used to collect flow data (Net flow or Yes flow or J flow) using SPN or Mirror method

Event Processor

Processing of the logs and also for querying, indexing and also filtering.
Additionally Event processor has CRE engine

Flow Processor

Processing of the Flow data (Ip packet) and also for querying, indexing and also filtering. Additionally, Event processor has CRE engine

Node

Storing of the logs . And also this can be used a like plug and play.

Q radar console

We use for Administration, SOC operations, Fine tuning, troubleshooting, Incident investigation, dash board creation, reports generation and also configuring email notifications and also used for custom rule creations

IBM APP Host

It can be used to managing of all the apps used by IBM Q radar and also it can be used to see what is CPU utilization, Memory, RAM utilization and also is there any extra storage required.
EX; UBA , Node , Threat hunting , IBM X Force

IBM X Force

It is a threat intelligence database managed and maintained by IBM. As a security analyst we will get regulate the updates from IBM X force and also we can verify reputation. Nothing but it is malicious are else real on are not

IBM Pulse

It is a dashboard that it can provide or communicate insights across the network and also it will provide vulnerabilities, threats and security posture of the organization

Offenses

Incident notification or alert notification or alarm notification

Building blocks (BB) (Interview Question)

Building blocks are test cases in IBM Q radar and it will not provide any alert notification. It will provide only logic using Boolean algebra functions
EX; source IP , Destination IP , Source Port , Destination port , Time frame so on

Correlation

Linking one event with another event using some logic or criteria for any abnormal activity meaning here we have couple of normal events & couple of Abnormal events correlating nothing but we have to map from Abnormal to normal event, we have to verify what is the mismatch is happening why it is Abnormal activity for that we use certain Algorithm backend & couple of logics

Correlation rule

linking one event with another event or mapping one event with another event based on the logic or criteria. Whenever any abnormal activity will happen logs or event or flows it will hit correlation rules and it will generate alert notification

What is the difference between correlation rules & building blocks (Interview Question)

Magistrate

It is IBM Radar component . it will analyse network traffic (Flow) and security events or logs against custom rules are created

Magnitude (Risk score)

A measure of the relative importance of a particular offense. It depends on the three parameters . It is a 0-10 scale range

- Credibility 0 - 10
- Relevance 0 - 10
- Severity 0 - 10

Ex: Malware category of the attach

- Severity 9
- Credibility 6
- Relevance 6

Magnitude 7 (7 is Average) 9+6+6/3 = 7

Credibility - Integrity of an event or offense we can define as 0 – 10 range we configure under the Rules (Rule Action)

Relevance - Relative impact of an event of offense on the network we can define as 0 – 10 range we configure under the Rules (Rule Action)

Severity - It is a measure of the relative threat that sources poses a destination we can define as 0 – 10 range we configure under the Rules (Rule Action)

Magnitude or risk score - Average of severity, credibility and relevance

What is magnitude in IBM Q Radar & what are the facts that are depending on (Interview Question)

DSM(Device support module) – DSM is used to integrating of the Third party log sources to IBM Q radar tool Ex;

Palo Alto	AD/DC	IBM Server
Crowed strike	Router	
Qualys tool	Switch	
Mime cast	AWS	
Blue coat	Azure	
Source fire	web Server	

What is DSM in IBM Q Radar (Interview Question)

Coalescing (Interview Question) - Removing the duplicates or bundling the events together we will coalescing

Ex; for Suresh continuously Authentication login failure attempts are coming

1	4625	Windows event authentication fialure	Suresh	LT-BNG-Suresh
2	4625	Windows event authentication fialure	Suresh	
3	4625	Windows event authentication fialure	Suresh	
4	4625	Windows event authentication fialure	Suresh	
5	4625	Windows event authentication fialure	Suresh	
6	4625	Windows event authentication fialure	Suresh	

If events per seconds increase storage calculations will increase so even GB per day get increase

Drawbacks of duplicates of events
Cost due to EPS count will be increased
Confusion or complexity
Storage required will be very high
Note - To eliminate above drawbacks we have to use coalescing

Reference set – A list of single elements that are derived from an event or flow in the network under rule responses we will configure as a reference set

Ex: IP address
Hostname or computer name or server name
User Name
Source port
Destination port
Default Domain

QID (Q Radar ID) - It is unique event id or flow id will be maintained by IBM Q radar as a signature ex; we have 6000, 7000, 3000 , 4000 series & so on

User management - Managing of all the users

Managing of all the users		
suresh	L1	Read only
mahesh	L2	Read and write
naresh	L3	Admin
nagesh	L1	Read only

This is how we can define the user management based on roles
User groups - L1 group ex; Suresh and Nagesh

Tennent Management –

- One Tennent we will configure as HQ it is location wise
- Remote branch office1
- Remote branch 2

IBM Q radar supported data bases What is the two data base are IBM Q Radar is supporting or what is backend data base is in IBM Q Radar (Interview Question)

- AQL - Ariel query data base it is default

- PGSQL - Post Grass structure query language it is third party

Regular expression – whatever logs are generated by default every logs source or data source

- AQL – Query Based
- Flow based – Net flow , J flow or yes flow
- Mathematical based – Mathematical operator

Do you know how to create parses development or regular expression (Interview Question)

With help of vendor I know how to create parsed development I will take their existence raw logs then I will go to the vendor , the will create the separate ticket or support ticket to the vendor then I will create a parses development

FPS or EPS –
EX – EPS Count is 10k buffer we added 13k (Adding 30% on 10k we got 13k)

LDAPS integration - SIEM tool has to integrate with AD

Q radar version - 7.3.4 or 7.3.3

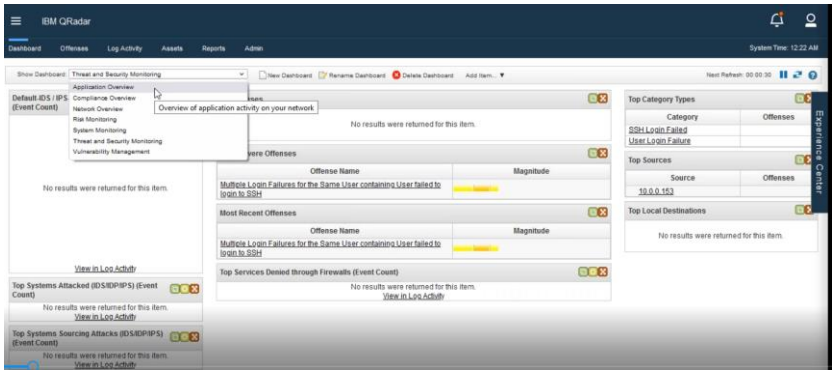
Model numbers

- 3125
- 3128
- 4125
- 4128

IBM Q Radar TOOL Cloud

Dash Board Tab

Under Dash Board we will see what all the incidents that are receiving nothing but summary of overall organization



Under the show Dash board we have the

- Application overview
- Compliance overview
- Network overview
- Risk monitoring
- System monitoring – Health check up related
- Threat and security monitoring
- Vulnerability management

We can do customize also here unlimited dash boards we can create

Under Dash Board we have certain Default like

IDS/IPS – All: Top Alarm signatures (Event Count) – This related to IDS/IPS activity whatever the Top Alarm signature meaning here whatever attacks are coming to the organization which means that IDS/IPS Logs that we are integrating ex source fire from cisco , MacAfee , Vectra , Symantec so on

Tops system Attacked (IDS,IDP,IPS) Event count – Whatever systems got attacked by IDS/IPS Logs that we are integrating to the SIEM Tool using those systems if any systems got hacked that information we can see under this one

Top systems Sourcing Attacks (IDS,IDP,IPS) – Sourcing attack means who is the attacker, from Which IP Address

My Offenses – what ever offenses that we are working on

Most severe offenses – It is based on the severity of the attack (Through Magnitude define the severity of the incident

Severity is depended on the 03 parameters

- Credibility
- Severity
- Relevance

Magnitude risk score 0 to 10

Based on the severity we will prioritize the incident

Most recent offenses – Whatever recently that we received now

Whenever if we want to go recent instant incident investigation we have to check under the My offenses Tab but our work will be under Offenses tab only

Top Category Type

It shows as per demo tool

- SSH Login failure

- User Login failure

It can be more like Brute force attack , malware , SQL Injection attacks and so on

Top sources

Which user is getting Logging attempts failure that source related user information ex; 10.0.0.153 this user is getting multiple login failure attempts

Top Local destinations

Here which user is going to get impact

Insider threat (Interview Question)

With in the organization itself whoever is trying to Enter anything knowingly & Unknowingly like entering the wrong password , DLP Related et.,

External Threat (Interview Question)

When ever attacker is trying to do some external attack who is trying into the organization by using different type of sources like Phishing email , Broken authentication failure , MITM, One of the server got compromised Etc.,

Reports that we generate from the SIEM Tool

- Top Applications (Internet facing)
- Daily user Authentication
- Top IDS/IPS Alerts
- Top WAF Related
- Geo graphic Traffic Distribution
- Data policy violation summary

Do you know how to create the Dash Board in IBM Q Radar (Interview Question)

Yes I know how to create the Dash Board. I will go to the respective Dash board of the IBM Q Radar tab then I will click on the new Dash Board if I want see the Web application firewall related to Application layer attack like OWSTOP 10 I will choose OWASTOP 10 related Attack, Then I will provide the description then will click on OK and that one I will provide under the security related incidents or threats & security related Dash Boards

Offenses Tab

95% our work will be in Offenses Tab only in IBM Q Radar

Our Target is Q Should be always empty every moment we have to click refresh option

My offenses – whatever incidents that we are working on

Under offenses tab we see the correlation rules under the rules we have the malware category this which we can see under the Group option. So under this malware category whatever that display those are virus related correlation rule

1st we have to go to the Ticketing tool then we have to create the ticket

After that we have to check & validate the incident by using

We have the certain steps which are included under the Forensic Investigation

- Identifying ---------- Malware
- Triage ---------- IOC/IOA
- Investigation ---------- Already this incident is blocked firewall/proxy/AV
- Documentation --- Incident analysis summary under ticketing tool

Like we have to write

Incident category – Malware

Description – source user xxx tried to download certain virus file from particular website

- Report submission – whatever we gathered information we have to submit below we can see

IOC (Indicator of compromise)

- Destination IP ---------- 192.165.1.1
- Destination user -------- xxxxx
- User name ---------- xxxxx
- Host name --- xyz

User profiling & Asset profiling

IOA (Indicator of Attack)

- Source IP -------- EX; Eicar website
- Source URL ----
- Source user name --- N/A
- Source country – xyz

File details

- File name – eicar.com
- File size – 500 kb
- File type – text

Above process is Triage

After that we have to incident investigation we have to do log analysis. Logs like

- Event id
- Source IP
- Destination IP
- Actions (Block / deny)
- Time (11 AM)
- Log source (Firewall / proxy/AV)

Pay load
File details eicar.txt
Source port 443
Destination port 433

The Action shows deny which firewall Is already blocked by this we can conclude by using the ITIL Process

- Preparation---------- IBM Q Radar preparation
- Identification ---------- Malware
- Containment ---------- Not required
- Eradication---------- Not required
- Recovery ---------- Not required
- Lessons learned ---------- Not required

Whatever incident comes we have to follow this process

Once done we have to incident Analysis report

Final report is mitigation – Already this incident related malware blocked by AV or firewall im considering this incidents is a false positive

If we don't have the access to the firewall or proxy if system got compromised we have to ask to respective team to escalate

Whenever we are doing any incidents always we have to keep in our mind we have to update in the Notes which we get it under the action option under the all offenses tab there we have to write ex; this is compromised scenario which im escalating to L2 Team

Basic details are incidents investigation related to malware you can see below

Like whatever we have created like IOC/IOA Etc., information

Then we have to Assign to the particular team

Before that we should assign ticket to ourselves

Whatever incidents that we are working on we should maintain that Incident tracker

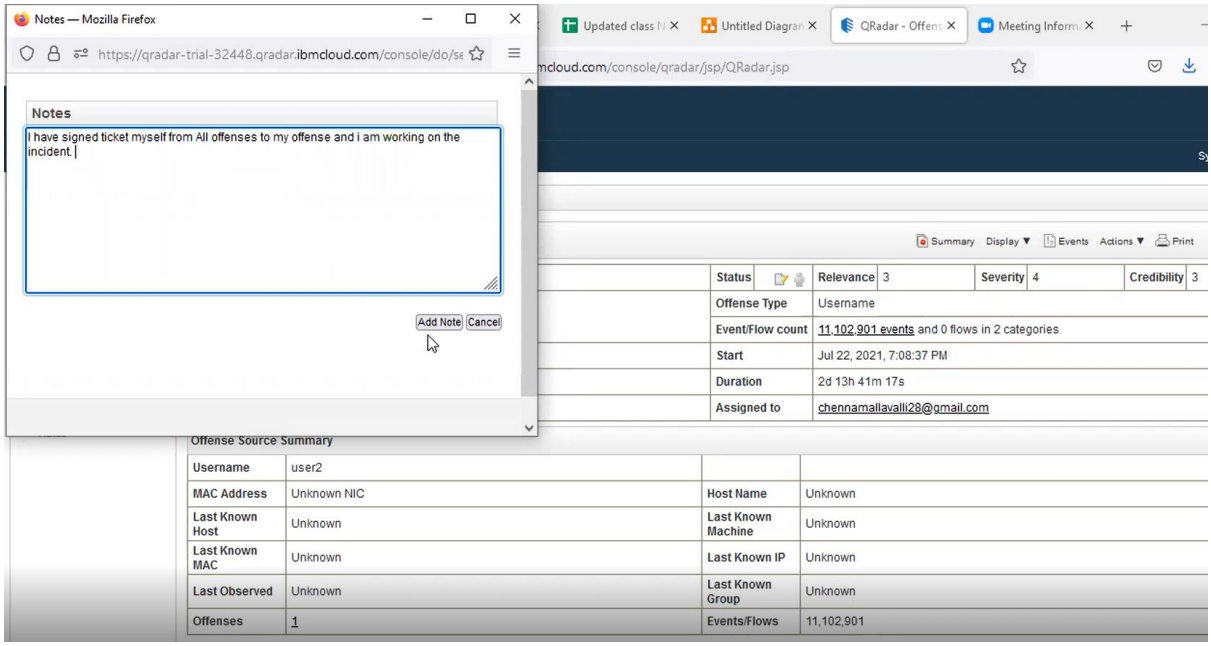
Instant Incident investigation

As we can see in the picture Under All offenses Tab

multiple login Failure for the same user containing user failed to login to SSH

1st we have to go to the Action tab then we get the drop-down option their we have to assign the ticket to ourselves.

2nd Once Assign the ticket we have to go to the Action tab where we can see Add note option then we to write the notes in it. I have assigned ticket myself from all offenses to my offenses and I'm working on particular incident



- Once we assigning then our name get appears in the search option
- Now we have to create the ticket in ticketing tool. If it is incident related ticket it will start with INC0000 or IN0000
- Some time we create the CRT Request nothing but change request. When something we want to upgrade we do change request ex; firewall update , SIEM Tool Update it start with CH0000
- Login attempt failure are 10.0.0.153
- User name ex; David (By this we can person name either person is public or private)

Incident life cycle management

Preparation – offenses

Identification – Brute force Attack

Containment – No containment (Because nothing is getting compromised)

Eradication – we have to send an email to the respective user

Two types of communication we have

Verbal communication – By calling

Written communication – By chatting , Mailing

Mitigation – End user is already confirmed has done failure log in attempts. Consider ticket as a false positive

Final Note we have to write – Based on confirm with the end user and IP Address 10.0.0.153 he forget the password and he has done multiple log in failure attempts. So based on this confirmation this incident as insider threat and it is false positive

Then we have to close the ticket under Action tab we have the option called close

Then we get the note under that based on the user confirmation this incident is consider as a false positive and i have attached the evidence and closing the ticket

Then finally ticket get closed and it will dis appear from the All offenses

Under last 5 search result

Whatever we worked on particular search results

Top 5 sources Ips

From here Attempts failures are coming , here we can see the location , if any vulnerability gathering this information we called as IOC/IOA

Top 5 Log sources

From backend Linux server logs are coming

Event processor has custom rule engine according to the custom rule engine only alert is generating

Top 5 users

Here only we can see top 5 users

Top 5 Categories

As per dome we have received the

SSH Login failure

User login failure

Last 10 events

Here we can see top 10 events under this Tab

Top 5 Annotations

It is nothing but description of the attacks, what ever rule it is hitted and what is the rule description that is called Annotation

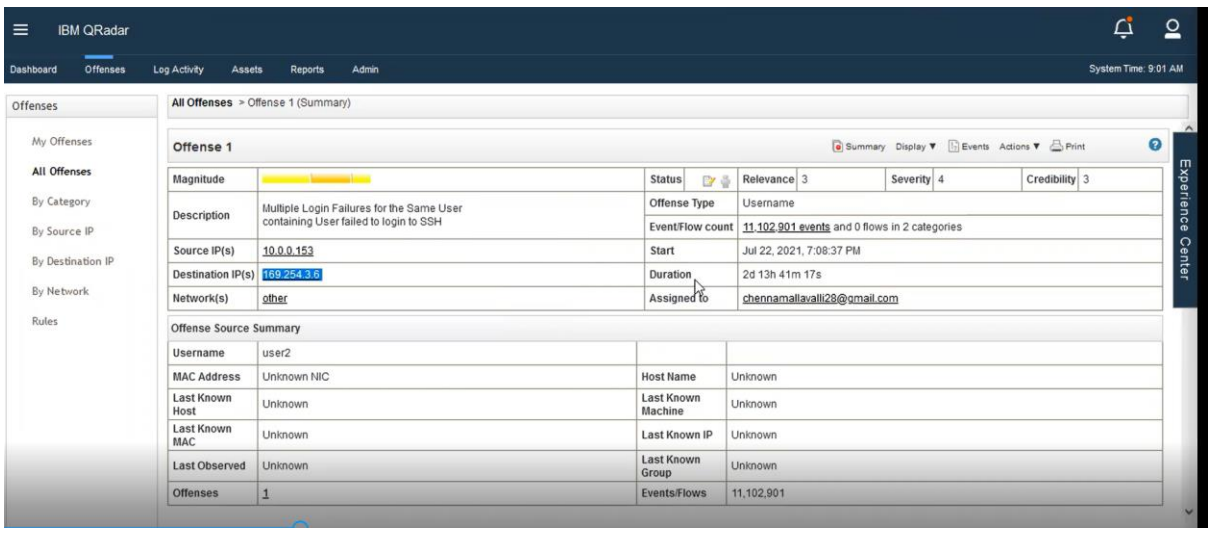
Sometimes we don't have the full information at that we moment we have to raise the ticket and we had to trouble shooting for that we have take the raw logs from the Linux server , we have to raise the separate ticket to the vendor raw log side from the Linux server all the felid as a full but when the logs are coming to the SIEM Tool those fields are showing empty

Then vendor will verify why the parsing is not happening it is nothing but fine tunning process

Incident Tracker

When ever the ticket is received in the SIEM Tool which mean incident then only SLA will start. Not when we created the ticket in ticketing tool

S.no	Incident Number	Recieved time in the siem	Ticket created time	Incident category	Status of the inci	Incident closure t	Total time taken
1	INC0001234	22/07/2021 7:08PM	22/07/2021 9:08PM	Log in attempt failure attack using SSH	resolved	2207/2021 11pm	3:52 Hours
2	INC0002345						
4	INC0003456						
5							
6							



Gathering all the information like Source IP, Destination IP , Duration etc it is called as IOC/IOA or Asset profiling or user profiling

From the source IP login attempts failures are coming

By category

Based on the whatever category of the attacks like Authentication related attacks or Malware , Dos or DDOS attack & so on

Whatever attack is coming whatever correlation rule is configured under these correlation rules

By source IP

From which source it is coming

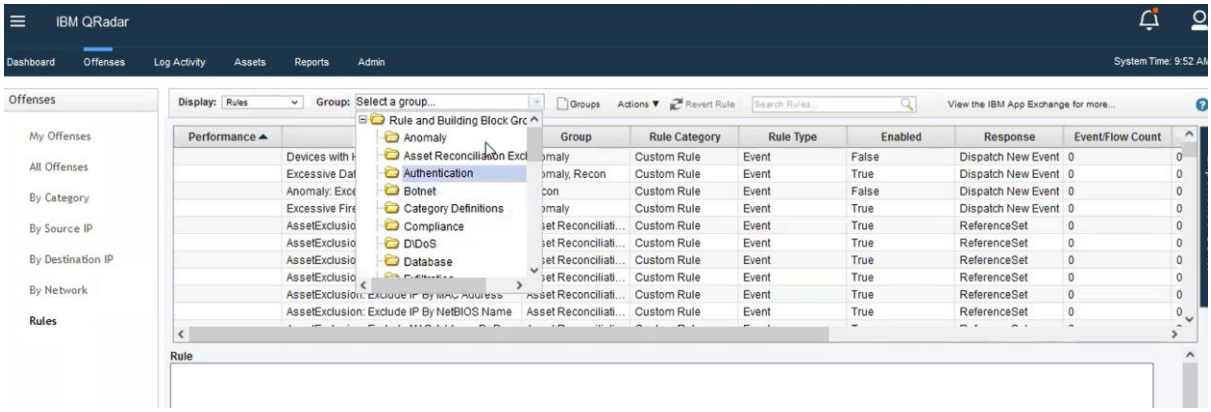
By Destination IP

To which Destination It came

By Network

If we are using multiple locations here we can see the location point of view

Rules (Interview Question)



Multiple categories wise they have created the Rules like Anomaly, Botnet etc.,

To create the correlation rule we have the option called Action button

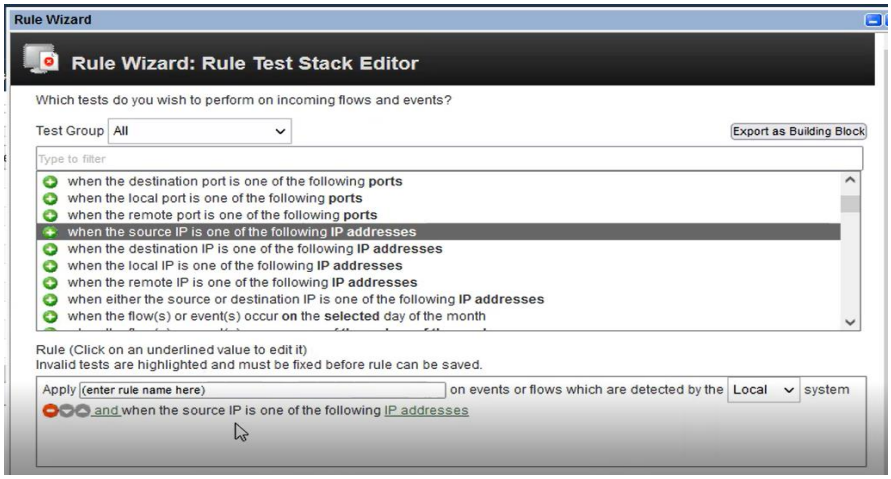
How to explain correlation creation (Interview Question)

I will login into the SIEM Tool and will go the offenses tab of the IBM Q Radar then I will click on the Rules button , then I will click on the rules actions tab , then I will click on the new offense rule , once clicking on the offense rule we will be getting three types of category

Wizard rule will come with some description

Once we click next option it provide the options which rules that we want to generate either Event , Events or flow , or offenses

For example if we have choose events or flow then the next process here we have to select building blocks



2nd box logic only they will expect in an interview(This mainly for any correlation rule logic

Invalid tests are highlighted and must be fixed before rule can be saved

Which means if some of the errors are coming when entering these logics or maybe any filed is missing it shows as a error

So before saving that particular rule we can correct it and we save that button ex; when we typed mistakenly wrong password it shows an error

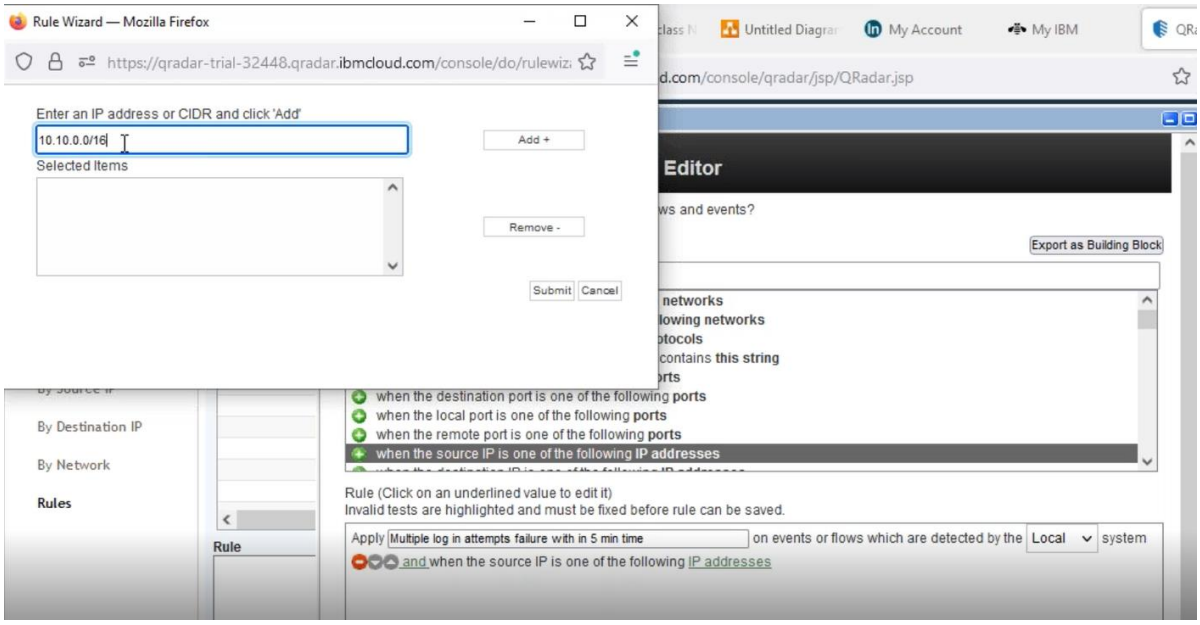
In IBM Q Radar

L2L – Local 2 Local

L2R – Local 2 Remote (Global wise)

Under the 2nd box we can the IP Address we have to click on it. We have to define particular range of the IP Address of the organization whatever we are using

Whenever any attacks are coming those particular IP Addresses will generate an Alert as we gave the example like 10.10.0.0/16



We have define the IP Address range now we have to define the Time range

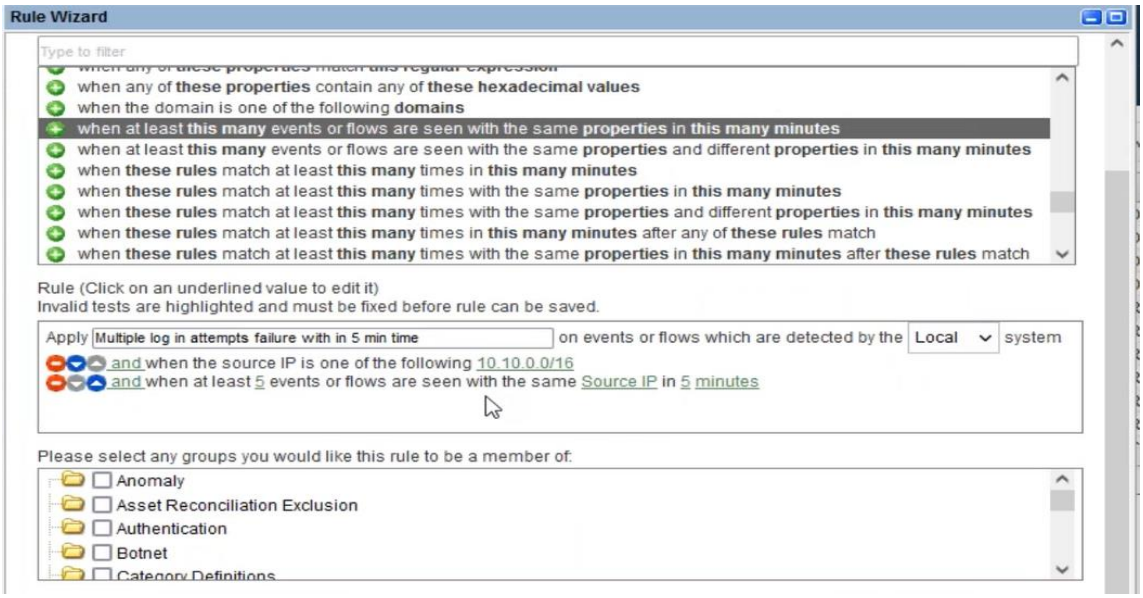
Below we have choose when at least this many events or flow are seen with the same properties in this many minutes

We have choose the

- Many – 5
- Properties – source IP
- Minutes – 5

This is the way we have to create the correlation rule

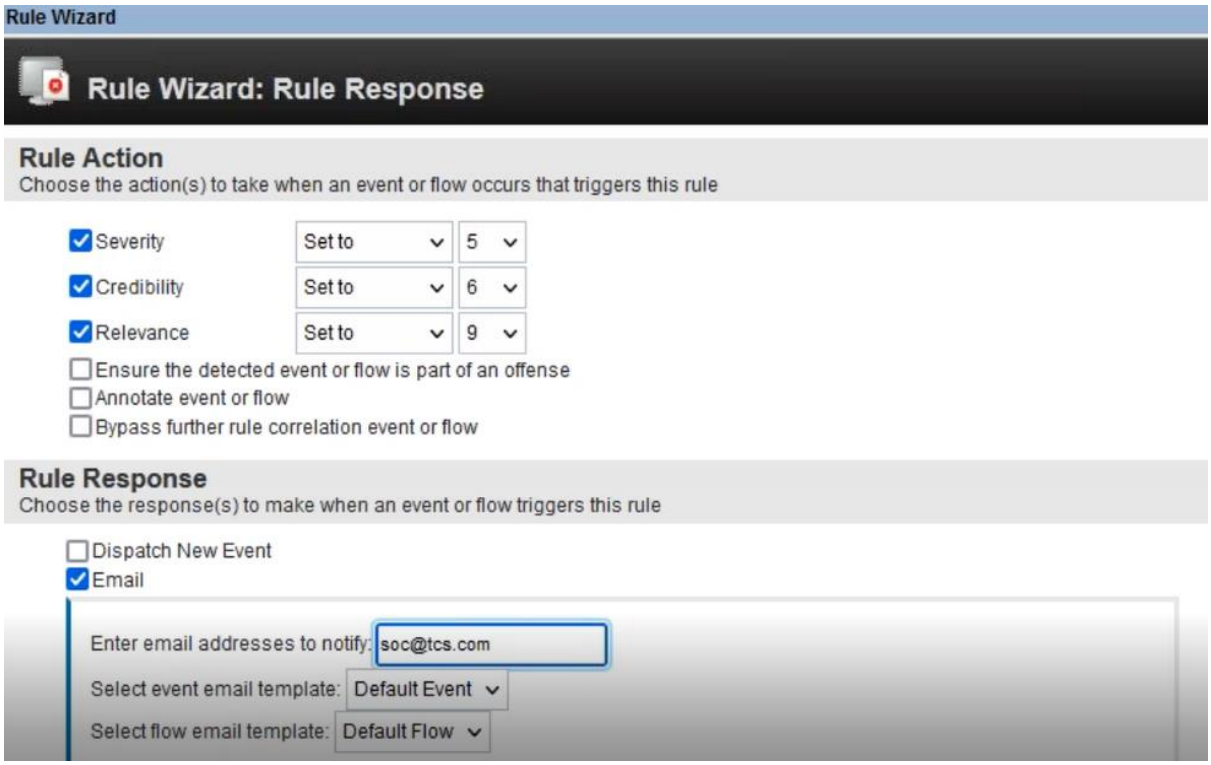
As we can see in the below picture



Once we done with the correlation rule now we need to choose the category want to create the particular attack

As we see in above picture select the Authentication once choosing we should click the next button. When we clicked something wrong error will appear here

Once done we have to choose the Severity , credibility & Relevance this is scale



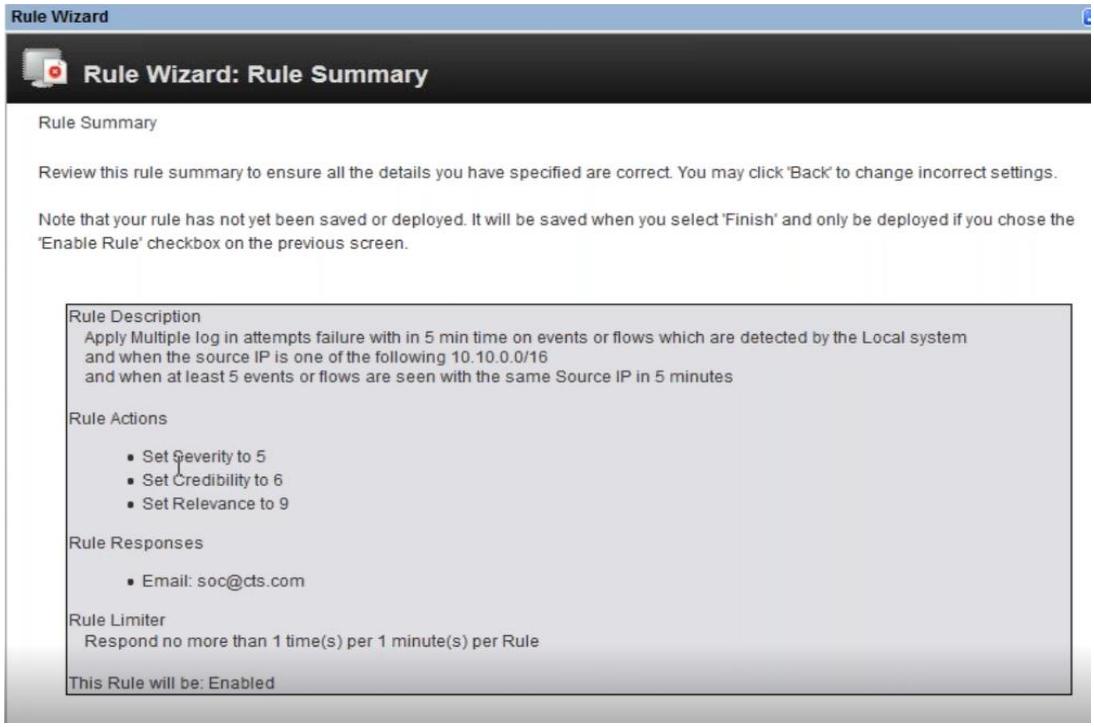
What is reference set In IBM Q Radar (Interview Question)

Reference set Whatever the incident that are receiving we will go and create rule response option whenever if we want to create the correlation rule in the IBM Q Radar and one of the option we will choose as a reference and the reference that may be source IP , Event name , Destination IP , Destination Name or Destination Address , credibility & so on based on it we will choose the reference then it will generate the Alert it is called reference set

Response Limiter

Under that we can see Respond no more than one time then we have to click next

Then Once all done it will give over all summary what we created



Have you have ever created the correlation rule (Interview Question)

Yes I have created the correlation rule which is related to login failure to disable account for that I login it into the IBM Q Radar then I go to the offenses tab under that we have the rules option, I clicked on the rules option and after that I went to the actions and I have chosen new offense rule so then I clicked on the button, when ever we want to create correlation rule always we have to create the Test cases, and then building blocks I have chosen for all the IP Addresses. And category of the building blocks Authentication to disable account

Then I have chosen when the source IP Address is one of the following IP Addresses

Then I define my total organization of the IP Address range of the Data centre apart from that additionally I have chosen one more building block category as Authentication to disabled account and after that I put that category of the Authentication related. So I have chosen and I have put those logic under the category of the correlation rule and I have clicked on the particular next button

Or

I'm working as a L1 Analyst I don't have option to create correlation rule but I know how to create

Normally we go to the offenses tab go to the rules tab then will go to the access tab will choose the New offense rule and then will choose the correlation rule for the both events & flow then we have to choose the building blocks

Then we have to choose the logic behand the particular correlation rule then we have to choose the category of the respective whatever logic that we are creating category of the incident. Then we have to go the Rule actions the we have choose the

- Severity
- Credibility
- Relevance

Out of 10 scale according to incident of the incident category the finally we have to choose Rules Responses as a email and finally I will review the correlation rule and will click on finish

After that Then I will test wontedly wether that rule is working are not by generating some logs or events and this is successfully alert is generating then we will do a change request window and we have the CAB Approval as well with SOC Manager and after that we have to implement in the production environment of the SIEM Tool

Log Activity

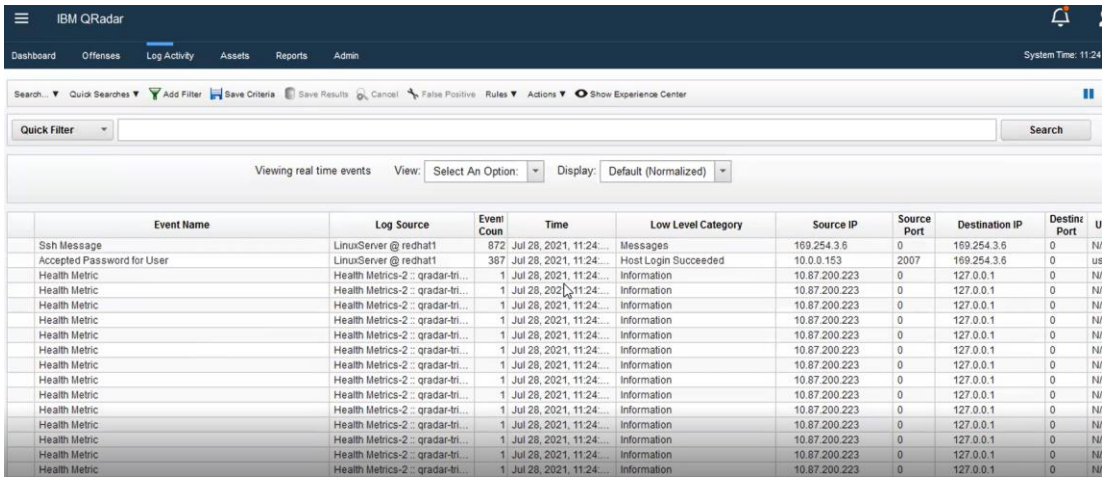
If we want any Additional Information from the particular log source. Those information which we don't get under offenses tab

When we are clicking the offenses tab here we don't get the full pledge information. If we want to attach any evidence in that situation only we have to go to log activity

To verify when the log is received , when the event is received and all how many events received from the particular source user or server, to get more details to that particular incident then we have to go for the log activity tab

In the similar we have the network activity log

In this log activity tab like a real time monitoring



As we see in the picture above picture those are real time monitoring (Real time means what ever logs that we integrated from the firewall, Proxy , IDS/IPS , clouds, Infrastructure servers & so on Those logs we directly integrated with out any delay

Directly it will come here these logs are as compare to traffic less bandwidth it will occupy

We have the filtering options like search , Quick Search , Add filter , save criteria and so on

As we see in the picture we can see the integration Linux , system information , health related these are different types of logs that we integrated so that is called Aggregation

In our Organization what ever logs we integrate so ex; Firewall, proxy servers, EDR Solution or AV , WAF, Load balancer , Routers & switches etc., which we see under the Log sources those are Aggregation logs

We aggregated through Event collector , syslog , flow collectors, collector Agent method these are all we using

Now parsing what ever the Raw Logs are generated those logs are converted to parsing

Whatever logs that we are seeing those are not Raw logs those are parsed logs or Normalized logs it will do both parsing & normalization

What ever Raw logs generated from All those different types of Logs sources it will be converted to LEEF Format in IBM Q Radar we called as LEEF

Filter options we can do based on Time , Interval which means based on the severity of the logs , or based on the severity of Alerts based on time wise also we can do filtering Ex; Last 5 mints , Last 1 Hour & so on

Indexing & Querying

Indexing will be back end process which we cannot see

Querying is nothing but asking the question

In the Data Base level of the Q Radar it will use Aerial Query language in the Backend

How can you filter out Windows login attempt failure in IBM Q Radar or if you want to see login failure attempts related to windows or Linux (Interview Question)

With 4625 we can filter out or I will go the log activity tab of the IBM Q Radar then will go the search button option or filter option so then I will move the curser name to event name and I will give the right click and I filter based on the event name user failed to login attempt if it is related to Linux are else if it is related to windows what ever may be

Past 24 hours of the windows login attempts failure I want to see what will you do in q radar or how will you identify (Interview Question)

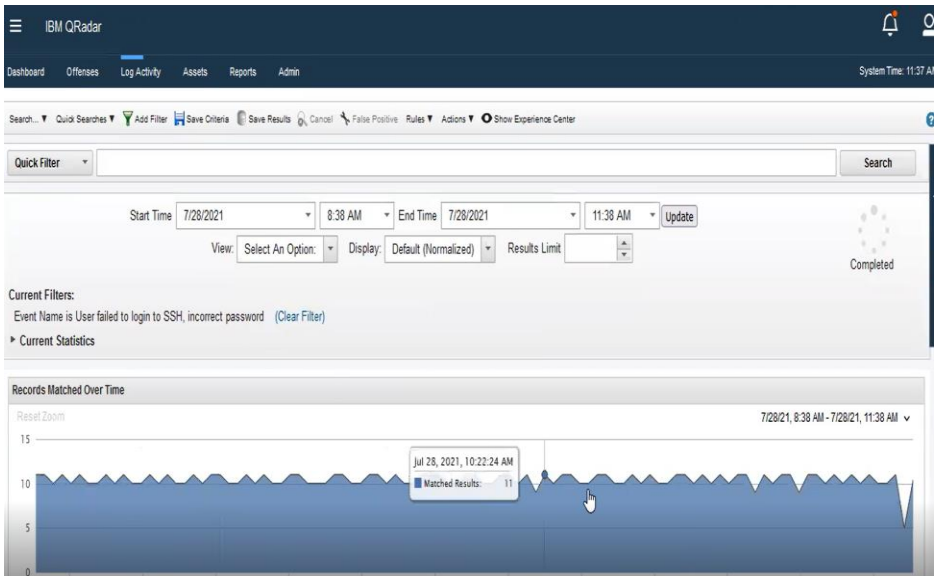
With 4625 we can filter out in the log activity tab or Under the log activity tab I will go to the Event name I will move the curser to the Event name and I will filter out window login attempts failures and also I can filter out

Here view option is there right will select that option so there also I can provide the last 24 hours time. Then I can get all those events failed attempts for windows machine

Below picture we can see we have selected for 3 hour time period

These many occurred automatically the time gets changes here as a 3 hours

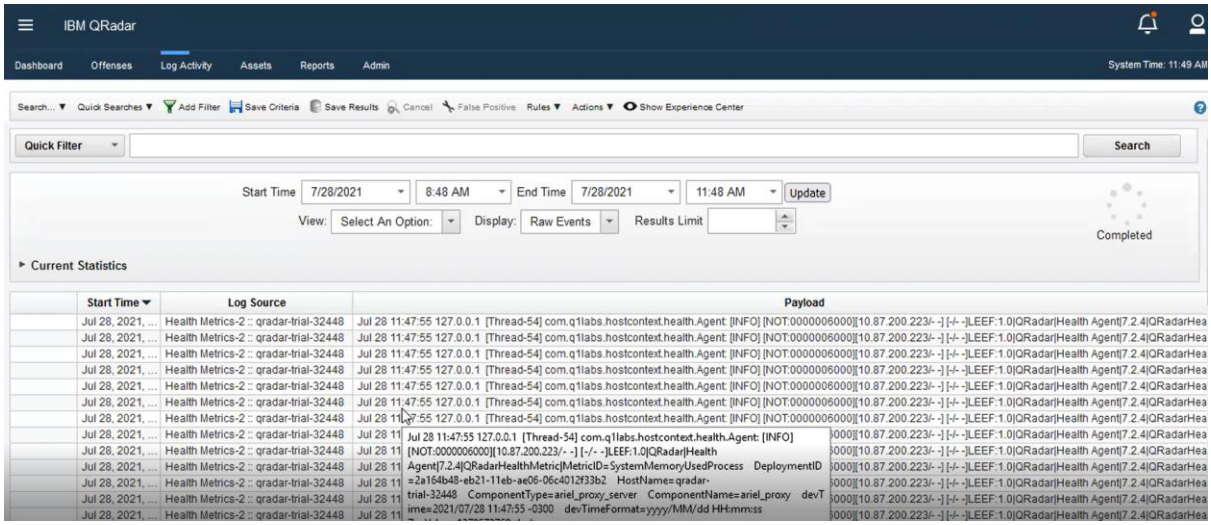
If we want to add those logs to the ticket then we have to export these logs for evidence purpose



Here we choose the multiple options under the filters which we have seen like start time , end time & so on

Under display filter we have the option drop down like Raw Data if click that get the pay load

Pay load is nothing but Data or message or Authentication success or Authentication failure and so on



If we want to get the pay load information we have to use either normalized log or Raw log

Why for everyone will not have Admin access to SIEM Tool (Interview Question)

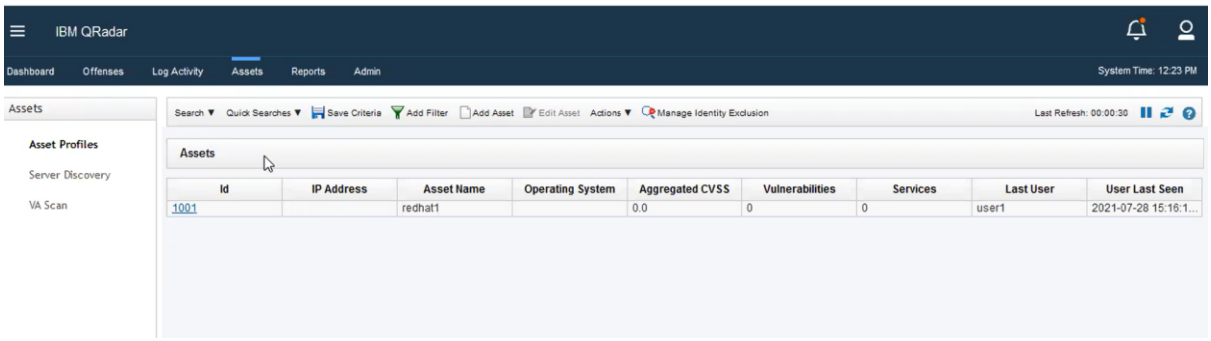
Having Huge chances to modified without knowledge by team right person only should access that

Under the Add filters we do conditions wise

Assets

Mainly for the Vulnerability scanning purpose we use the Assets Tab.

If we want to integrate with third party scanners , scanning tools like Nessus , Qualys ,Rapid 7 , trip wire and so on. If you want to run along with security operations as a Vulnerability management & Vulnerability scanning, IBM Q Radar as that functionality also No other vendor is supporting this functionality only IBM Q Radar

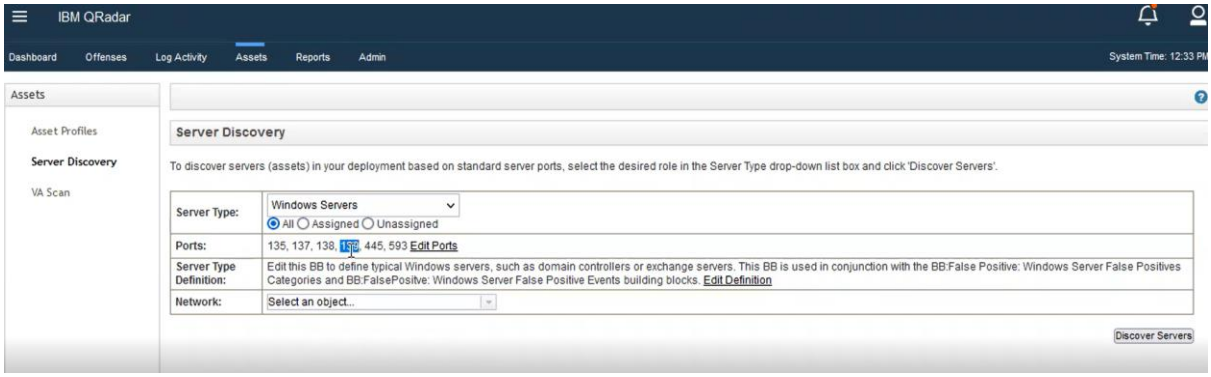


Under Asset profile To create Assets we have the option called Add Assets then it will provide the details where we have to fill like

- MAC & IP Address
- Name & Description

- Operating system
- CVSS, Weight & Compliance

Server Discovery



Port Number 135 to 139 are net baize

VA Scan (Vulnerability Assessment scanning) –

Under Admin tab we have to create the scanner , we have VA Scanner option, once we creating scanner one display gets popup we have to add into that

It will support multiple scanners like Nessus, Qualys more than 20 etc.,

If we don't the server if we are contacting to the business owners in this situation we have to implement Host discovery policy

Reports

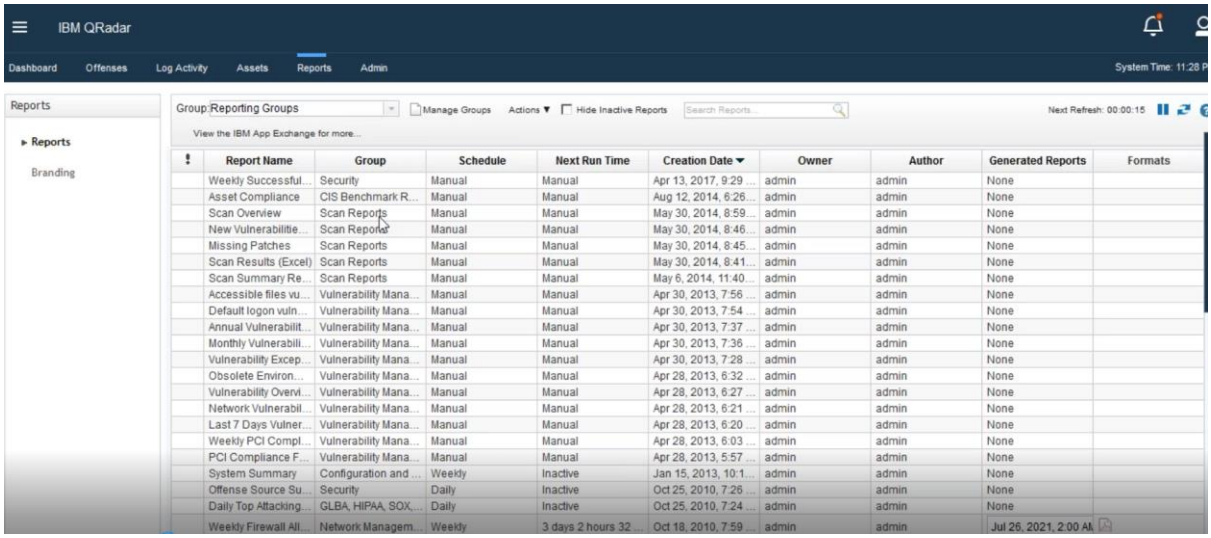
IBM Q Radar Is one the famous for Report generation

Report generation will be based on the Firewall based , proxy server based , IDS/IPS Based , then WAF Based and also server based and so on and also will do daily base generation , weekly based generation , Monthly based and so on

SOC Manager will take care this report generation

Which type of Reports you will generate (Interview Question)

Fire wall activity related malwares or proxy server related for blocking of the websites & so on or IDS/IPS related abnormal , malicious activity end user or server level activity , or server level brute force attack & so on



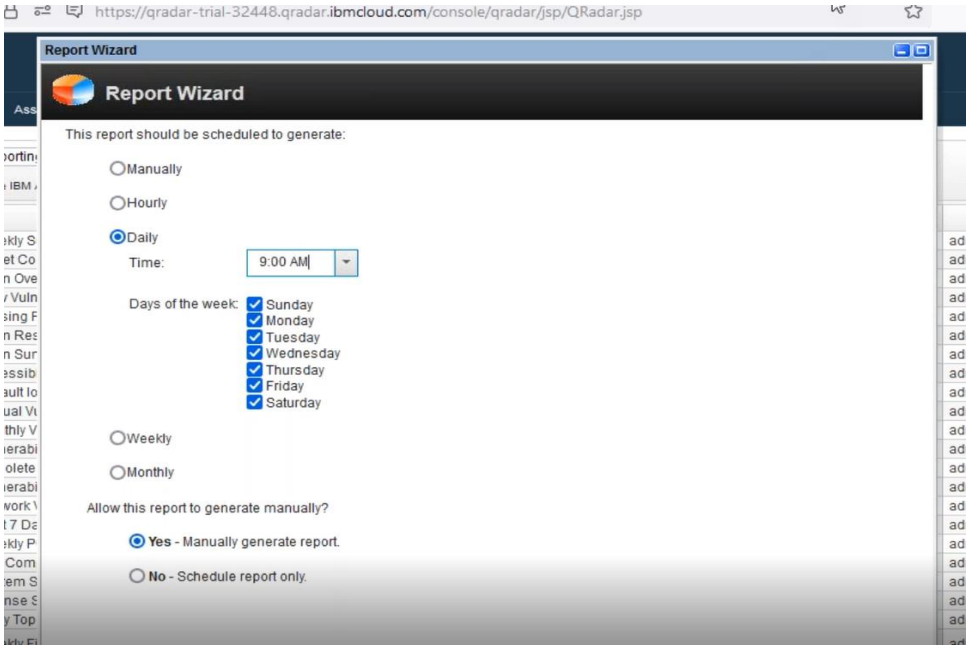
As we see in the picture Weekly successful events so who ever is trying to log into respective IBM Q Radar successful attempts

Apart from this we have different Report names like

- Asset compliance
- Scan over view
- Daily Top Attacking Host
- System summary
- PCI Compliance failure

And so on as we can see in the picture

If we want to add by default under the Action we can create and then we have to check which type of report that we should create either Bar Chart , Pie chart etc., First we have to select the particular lay out



Above which show after creation of Action we have to select the Time if we want to see manually , Hourly or Daily

Then we have to click next

Then we will get the landscape option

Then we have to choose Report Title & we can choose the logo and down we will have the another option chart Type we have selected the Asset option

Then we get the another page for selecting Container details Asset

Then page will populated for the classification then next page will be populated as you can see the report format in which format that we are make the format ex; PDF, CSV , XML & so on

Then once selecting the option we will the another page who are need to be in this particular report we can provide the access to them

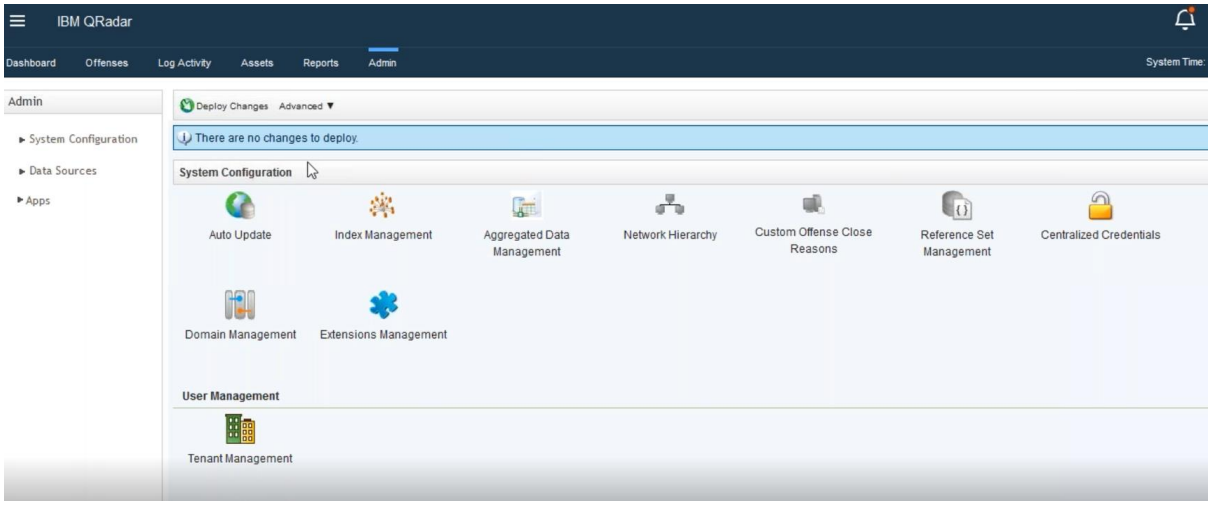
Then finally we get the finish option were we have to write the description

Based on the client requirement part we create the report ex; firewall deny activity of the daily bases report

I will goes to the reports Tab then I will go to the Actions Tab will click on the Reports button and then I will choose the Chart type and also whatever firewall that we are using in our organization

Admin

This is done by the implementation Teams



When ever we are making changes here always we have to do Deploy changes, Deploy changes is nothing but save changes configuration that we done it will save there

System configuration

Under the system configuration is system related like user creation , index management , Tennent management and so on

Under the System Configuration we have user management if click that we get the Tennent Management

Once we click the Tenent Management a page will be populated tenet means user names whoever wants to add the user tenant management we use mostly for distributed deployment

Then we have the another option Asset under the Asset we have custom Asset properties & Manage identity Exclusion

Under Custom Asset if we want to add anything Assets in the organization should add those Asset properties

What is meant by privilege (Interview Question)

It is nothing but Access based of segregation of duties we provide Access

Data sources

It is nothing but log sources Events , vulnerability where the logs are coming those information, Here only we integrate the Logs

Log Source

All the Log source information we see under this

Log source Extensions – what is the log source name want to category

Log source Parsing order – It Is nothing but converting Raw log type into parsed log using LEEF

Custom event properties – When ever we are not able to do normalization or parsing basically every log has the Raw log so nothing but event stamp when that event is generated

We use when ever that Raw log will be normalized to parsed log and some of the additional tabs & filed will be there so convert that Raw log to additional filed we use this custom event properties Ex; One of the Raw log contains event stamp, Event ID , and also source IP source port , Destination IP & Destination Port , Authentication successful or failure then pay load information

Data Obfuscation Management – Ex; we are working for SOC Operations on the front end we will see the lot of PIA Data

Vulnerability section – Mainly we have for vulnerability scanning purpose, If we want to integrate, IBM Q Radar itself as a vulnerability scanner if we want to integrate vulnerabilities also in that' situation we have to use this

What is DSM In IBM Q Radar (Interview Question)

Device Support Module If we want to integrate 3rd party log source to IBM Q Radar

Apps

If you want to use Additional 3rd party Apps under that we can see Q Roc self service which means Q Radar on cloud self service

What are the website you follow and what are the blocks you follow to get regular updates (Interview Question)

Incident Investigation

VPN Authentication failure Log source – Firewall, Z scalar

Malware Log source – AV , EDR , Firewall

Brute Force Attack – Domain controller , Active Directory (this is for windows) For Application (WAF , Firewall , Proxy, Web server or Apache Tom cat)

When explaining Incident investigation we have to remember 4 things

- Incident life cycle management process
- Business Impact Analysis (If there any outage or Availability issue or integrate related issue or Any confidential related issues etc.,)
- Risk Assessment
- Log sources

In an interview always we have to explain True positive incidents only not False positive

Brute force Attack can also be called Multiple Authentication failure

Multiple Authentication failure nothing but trail & error method here attacker will do the probability

Every incident as per Incident life cycle Management we have certain steps as follows

- Preparation
- Identification
- Containment (Network Isolation which means disconnecting from the Network)
- Eradication

- Recovery
- Lessons Learned (Is also called as Post Morten)

For False positive will be only up to preparation & Identification (We need to find out after the classification either is it Insider or External Threat)

For True Positive we do entire thing from preparation to Lessons Learned

Normally what L1 team will do?

Well Normally Alerts will to SIEM Dash Board or Email Notification, As a L1 Based on the severity or risk score we have to pickup the incidents

When ever we are picking up the Incidents we have to inform to our Team members as im working on so & so particular incident

Then we have to Assign the ticket to ourselves

After Assigning the ticket we should do the classification of the incidents

Then we have to gather IOC & IOA, Payload , Log sources Information , Asset profiling, User profiling

Classification – which type of Attack is it either Brute force , Malware and so on

IOC – We got comprised in the organization (Victim IP , User name , End user system name or computer Name or server name & so on all these details can also be called Asset profiling or user profiling)

IOA – Under IOA it is not Applicable for Internal attacks only Applicable for External only

Pay load – Every raw logs contains event stamp (event stamp means time) when that incident is happened

Ex; Brute force Attack is happened at 10 AM it provide month & date time as well and next it will appear source IP, Destination IP, Source port & Destination port , Action , Pay load and Additionally some Authentication failures or successful. All these information is available in every log

In the Logs we have to see Action This is not applicable to Authentication failure basically it is Applicable to EDR , Firewall , Proxy , WAF , IDS/IPS , For all these logs sources it is applicable

After gathering information we called as Triaging

As per the Attack we have to do the investigation ex ; Brute force attack we have finds out either Internal attack or External attacks

If it is Internal Attack we have to take that particular IP Address who is that End user, we need to check either end user system , Laptop , Mac Book , work station or Desktop and so on or server

One of the Alert is coming from 10.10.10.1 we have to identify this brute force attack is coming from the end user system or Alert

From Ns look up option as well from pay load

1st we have check Ns look up button

2nd we can check in the Logs

In case these two options are not working we can verify with system Admin or windows Admin other wise couple of Tools are also available those are like CMBD

(Configuration Management Data Base)

How can you identify it is Windows or server?

If it is windows based on OS

If it is Linux it is Cent OS, Red Hat Linux, Docker or container & so on

For Analysing the incident

Log analysis and incident investigation
Reputation checks

False positive or true positive

Option1 - False positive L1 Team

- 1st we have to make the summary of the Report
- And also we have to update & Notes Regularly event it is false positive or true positive what ever
- Then finally we have to Attach the evidence whatever we have gathered

Above will be handled by the L1 Team

If it is True Positive L1 team will provide the recommendation like

1) Please contact end user whether he/she has done the activity
2) Please go and check in EDR tool, firewall, proxy or ips or waf
Then L1 will Assign to the L2 Team

Option 2 – True Positive By L2 Team

Now L2 team will re validate

Basically L2 Team is like IR Incident Responder

Containment (Network Isolation) If it is end user system if it is one End user BIA Is not required even Risk Assessment is also not required

Containment can be done by this way like we have to disconnect the network LAN otherwise we have to speak with the end user we should tell do not connect with VPN

If it is server that only one server we have that got compromised here we have to do escalation which is escalation matrix we cant take our own decision here why because we have to talk with Asset owner & SOC Manager

If it is server then BIA (Business Impact Analysis) & Risk Assessment is required

How will come to know what is the Impact?

We have to contact to the server owners or Asset owner we have to scheduled a call them. Then we have to verify is it internet facing server or Internal facing server and also should verify any backup server is available are not, Are you taking any regular backups are not , Is there any critical applications are Hosted on the server are not, If in case doing any network isolation what is the Business Impact to the End users or to the Public

When something got compromised what level of data breach is happened what logs you will Analyse

DLP , Firewall , FIM , AD

When you have different Tools like AV , EDR , IPS and so on why your system got compromise

Because we are not using the Strong passwords and regularly we are not doing the patch update due to legacy server and AV Agent is sleeping

Do you know any scripting language for Automation?

Malware investigation (End user system or server)

Malware is malicious software program code. Attacker will develop malware program code by using different types of programming languages like HMTL , JAVA, C , C++ Etc.,

By using the programming language attacker will inject it into it the Targeted machine

We have the different category Malwares like

- Virus
- Trojan
- Worm
- Botnet
- Logic bomb
- Key logger

Zero Day
Root Kit
Spyware
Adware
Ransome ware

These are the malware categories

Symptoms of malware category manual way

- Automatic restarts
- automatic reboots
- system very slow
- CPU utilization will be very high
- cursor movement
- ram utilization will be very high

Sources of malware

- Port scanning
- Drive by downloads
- phishing email attachments
- peripheral or removable devices

What is Drive By Download (Interview Question)

Something that we are downloading from websites or Application

Malware will come though

- Files
- .dll
- .doc
- .exe
- Jpeg
- Zip

Rar
CSV
XML

These files come from E-Mail attachment, something which downloading from the internet , coping something through pen drive etc.,

As per in the interview always should say .dll file its one of the dangerous file

Mitigation steps for Malware

- AV/EDR/AM
- NGFW
- Email security
- Malware analysis
- IDS/IPS

What are the Actions under the EDR Tool

- Block
- Allow

Clean
Quarantine

Block which mean any of the employee is trying to download something from the internet in that situation EDR Architecture will be

How can you do Manual Malware Investigation & Automated Investigation or explain malware Analysis (Interview Question)

We have two process

Automated Tool wise – Using AV/EDR Alert notifications are receiving and logs are integrated to SIEM Tool using syslog server method or API Token Management method or May log collector Agent method or cloud collector Agent method and so on

Automated Tool means each and every End user Machine we will deploy EDR/AV Agent that Agent will communicated to AV/EDR Tool or server so based on the policies configured like threat prevention , DLP , HIDS/HIPS , FIM , Account lock out policy and so on

Automated malware investigation

Every EDR Tool

- Block Clean
- Allow Quarantine

Ex ; HR who is sending the Offer letter to the candidate sending through E-Mail Attachment this Attachment will go to the firewall, OS of the respective end user system. Now AV Agent will identify whether it is infected or not with or with out any Malware

This offer letter contains the malware based on the signature based action it is showing is block. This particular Block backed one log will be generated that Raw Log, Every Log contains Event time stamp nothing but when that event has happen

- Event time stamp 08/10/2022 7:00 AM
- Source IP 10.10.10.1
- Source port 443
- Destination IP 8.8.8.8
- Destination Port 443
- Action Block
- Application SMTP
- Payload Message content
- Authentication Successful
- Log source EDR
- File type .dll
- File Name test.dll

- File size 100 kb
- File path c:/usersxxx/downloads/test.dll , Virustotal.com , google.com , ibmxforce.com
- File Hash Not Applicable

Above logs only integrated to the SIEM Tool
It is False positive because already EDR Tool blocked

False Positive
Under the False positive Offer letter (Malware)

- EDR
- NGFW

Above Tools blocked
File Action – Blocked
Under SIEM It is False positive

True Positive
Under the False positive Offer letter (Malware)

- EDR
- NGFW

Above Tools didn't blocked
File Action – Allowed
Under SIEM It is True positive

End user system (Laptop, Mac, Desktop, Work station)

1st we should Triage the Incident in Triage we will do IOC & IOA

- IOC - hostname, username, IP Addresses
- IOA – Destination IP
- File name – test.dll

Containment – yes we have to do

Eradication/mitigation - Reputation malware infection file which I found

Why you are uploading file in the Virus Total.com (Interview Question)
Already we have sand boxing environment dedicatedly there I will analyse the file if the file contains and malware or not. After completing the Anlayses I found that particular file contains Malware then
If it is not useful I will delete the file
If it is useful will do re run the scan
Then changing the password

Recovery – From Abnormal to Normal operation
Then Root cause Analysis – I do identify when , where , how it got compromised

Server Got Compromised
Under Triage
In this we need to identify the

Server IP	User Name
Server Name	File Name, Path
Which Department that particular server is belongs to	File Size , Destination IP
Location	Log source
Above this is also called as Asset profiling	Server Owner

Once we are identify the server owner we have to schedule a call
Before containment we should asl couple of questions to the Server owner
Is there any backup server is available ?
Is there any critical applications are running on?
How many End users are going get impact?
Are you doing Regular patch updates are not as Vulnerability management updates?
Are you taking regular backup?
For back possible options are we have like
SAN (Storage Area Network)
NAS (Network Area storage)
Magnetic Tap & Drive
Containment – After discussing with SOC Manager & also server owner do network isolation
Eradication/Mitigation –
Before Infection cleaning we should find out that this file contains malware are not
What is the difference between the static Analysis & Dynamic Analysis of malware
Delete the file or Re run the scan
Change the passwords
Recovery stage – Bring it into normal stage
(Interview Question)
Static Analysis – It will run Against the Signature
Why the server is got compromised (Interview Question)
It is a legacy server we don't have the EOL (End of Life & EOS End of support) reason for legacy critical Applications are running on & Parallelly one more project is going on
Application computability issues & patch update issue
AV Agent is sleeping
Recommendation
Legacy Server should be migrated
Parallel we can work on Application development on top of the server

Manual Malware Investigation

Manual – Without EDR Tool
end user will give compliant service desk/help desk team/corporate IT team
When IT Team doesn't find any issue they will share with the Security Team which is SOC
Now SOC Team will verify the under the Task Manager they will check which services , Applications are running on which cause more band width utilization , Ram Utilization & More CPU Utilization
Those services or process or software or files may be causing but not sure
EX; .dll, .7z, .windows.svc may be .dll may causing more band width or .7z
These files we have take to the we should the Analysis in Virus tool.com & in sand boxing environment
Other than Task manager we can use this tool Sysmon & process monitor
Have every worked on Malware Investigation (Interview Question)

EDR alerts are not working or do not appear As a security analyst, what will you do (Interview Question) ?
1st we have to check whether email integration is done or not in the EDR Tool we should verify whether it is integrated with SMTP Server or not. If it is Automated we have to login into the EDR Tool & then go to the Administration under Administration we have setting option then we have to see whether SMTP Server integration is happened are not

Brute Force

Explain Multiple authentication failures with in short span of time (False positive) to end user laptop- 1.1.1.1- External attack

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name
- Also, I found external attacker IP address details as well
- Then I came to know that it is an external attack based on the IP address details received in the alert.

- I have done log analysis and also verified the reputation in the tools like MX tool, IP void, and IP abuse database & Later I found that this activity will happen from the malicious IP
- Then I took the IP address and blocked the IP address in the firewall
- Finally, I attached the evidence in the ticketing tool and mentioned the comments or we can say the notes then in the tool and made a summary of the report and closed the incident accordingly

Explain Multiple authentication failures with in short span of time (False positive) to end user laptop- 10.10.10.1- Internal attack

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name
- Then I found this activity is happened from an internal IP address and found one of the internal has done
- After gathering the information, I sent an email to the end-user because I have access to the contact end user and based on his confirmation, I found that it is the initial activity of the internal employee or end user.
- I got a conformation mail stating that by mistake end-user tried more than 5 attempts
- Then finally I attached mail confirmation as a piece of evidence and made a summary of the report and updated the comments and I closed the incident

Explain Multiple authentication failures with in short span of time (True positive) to end user laptop- 1.1.1.1- External attack

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident

- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name
- Then I found this activity is happened from an external attacker and I have done the log analysis of the Domain controller & also some of the victims IP connections which are keep on communicating the attacker's IP address.
- So Immediately I found that this legitimate activity is going on and it is true positive.
- As per the incident life cycle management process I have done containment after analysing BIA (Business impact analysis) and RISK assessment. Because only one user is going impact if I am doing containment
- Later I asked the windows admin team to reset the password to stop an additional data breach
- Then I have run the Av scans and also verified DLP logs if there any data breach happened. So fortunately, there is no data breach happened and data did not get copied
- Then I bring it back from abnormal to normal operations and connected back to the Network
- Also, as per the Lessons learned and post-mattern report phase I created RCA (Root cause analysis) document and reviewed it with the SOC manager and also presented this report to the client. In RCA I found that the end user did not change the default password when he onboarded initially. the same password he is using.
- And also, I updated SOP document as well
- Then finally For the future reference I provided security awareness training to employees and ask them to use complex and strong passwords.

Ransome Ware

One of the END USER SYSTEM (Laptop, MacBook, work station or desktop) got compromised by Ransomware

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.

- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name where the system is located
- I gathered additionally file names, file sizes, file categories, and file extension
- This attack was received through the .dll file when the user downloaded the file from the trojan website. As per the cyber kill chain process couple of files got infected and the system got compromised.
- I spoke with the Help desk team about whether they are taking regular backups or not. Fortunately, the help desk team/ Corporate IT team taking regular backups.
- I have done containment (As per incident life cycle mgt) from the network whatever system got compromised after analysing the BIA (business impact analysis) and also Risk assessment.
- In the eradication phase with the help of the service desk team formatted the system and re-run the AV scans.
- In the recovery, phase bring it back from abnormal to normal operations
- In the Lessons learned phase as a post mottern report, I prepared a root cause analysis document, and finally, I analysed why, how, and when it got compromised. The reason behind for compromise regularly Windows patch updates are not happening and also AV agent sleeping when the attack happened due to this reason when the user downloaded the .dll file from a trojan or illegitimate website system got compromised.
- I reviewed RCA document with SOC manager and presented to my client or customer
- Due to this reason, i got an appreciation email and was also selected for a monthly award due to my productivity and quality of the Incidents I was handling

One of the SERVER got compromised by Ransomware

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name where the system is located

- I gathered additionally file names, file sizes, file categories, and file extension
- This attack received through. dll file when the windows server admin downloaded the file from the trojan website
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- This is escalated priority 1 (P1) ticket and scheduled a call with the Asset owner and asked a couple of questions before doing the containment(Network isolation)

a) Is there any backup server is available?
b) are you taking any regular backup config?
c) are there any critical applications running on top of this server?
d) How many users are going to impact in case if we are taking network isolation

I got the below answers from the asset owner or server owner

a) Yes backup server is available and it is facing the internet and it is a critical server to the organization
b) Yes, Regular back-ups they are taking as a team
c) yes, critical legacy applications are running (Basic java based applications developed long back)
d) a large number of users are going to impact.

- Based on the server owner confirmation and details, I made a backup server as a primary and continued the business operations without impacting any users.
- whatever server got compromised I have done network isolation in the containment phase.
- In the eradication phase with the help of windows, the server team formatted the server and imported the backup config file from the backup file and bringing it back to normal operation with high availability.
- Finally, I brought it back to high availability within the SLA 4 hours defined in the recovery phase.
- In the Lessons learned phase as a post mottern report, I prepared a root cause analysis document, and finally, I analysed why, how, and when it got compromised. The reason behind for compromise regularly Windows patch updates are not happening and also AV agent sleeping when the attack happened due to this reason when the user downloaded the .dll file from a trojan or illegitimate website system got compromised.
- I reviewed RCA document with SOC manager and presented to my client or customer
- Due to this reason, i got an appreciation email and was also selected for a monthly award due to my productivity and quality of the Incidents I was handling

VPN

Multiple VPN authentication failures with in short span of time (False positive) from multiple locations (10.10.10.1-Internal attack)

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name where the system is located
- I gathered additionally file names, file sizes, file categories, and file extension
- Also, I found this alert is received as an internal IP address detail as well
- Then I came to know that it is an external attack based on the IP address details received in the alert.
- I have done log analysis and also verified the reputation in the tools like MX tool, IP void, and IP abuse database found that this activity will happen from the malicious IP
- Then I took the IP address and blocked the IP address in the firewall
- Finally i attached the evidence in the ticketing tool and mentioned the comments or notes in the tool and made summary of the report and closed the incident

Explain Multiple authentication failures with in short span of time (False positive) to end user laptop- 10.10.10.1- Internal attack

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.

- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name
- Then I found this activity is happened from an internal IP address and found one of the internal has done
- After gathering the information, I sent an email to the end-user because I have access to the contact end user and based on his confirmation, I found that it is the initial activity of the internal employee or end user.
- I got a conformation mail stating that by mistake end-user tried more than 5 attempts
- Then finally I attached mail confirmation as a piece of evidence and made a summary of the report and updated the comments and I closed the incident

Explain Multiple authentication failures with in short span of time (True positive) to end user laptop- 1.1.1.1- External attack

- Recently I have done multiple authentication login failures incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name
- Then I found this activity is happened from an external attacker and I have done the log analysis of the Domain controller & also some of the victims IP connections which are keep on communicating the attacker's IP address.
- So Immediately I found that this legitimate activity is going on and it is true positive.
- As per the incident life cycle management process I have done containment after analysing BIA (Business impact analysis) and RISK assessment. Because only one user is going impact if I am doing containment
- Later I asked the windows admin team to reset the password to stop an additional data breach
- Then I have run the Av scans and also verified DLP logs if there any data breach happened. So fortunately, there is no data breach happened and data did not get copied
- Then I bring it back from abnormal to normal operations and connected back to the Network

- Also, as per the Lessons learned and post-mattern report phase I created RCA (Root cause analysis) document and reviewed it with the SOC manager and also presented this report to the client. In RCA I found that the end user did not change the default password when he onboarded initially. the same password he is using.
- And also, I updated SOP document as well
- Then finally For the future reference I provided security awareness training to employees and ask them to use complex and strong passwords.

Malware Investigation

One of the END USER SYSTEM (Laptop, MacBook, work station or desktop) got compromised by Malware

- Recently I done One of the end user system got compromised Malware incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name
- I gathered additionally file name, file size,
- This attack received through. DLL file when the user downloaded the file from the trojan website
- As per the incident life cycle management process I have done containment after analysing BIA (Business impact analysis) and RISK assessment. Because only one user is going impact if I am doing containment
- I have taken the file and analysed malware analysis in the Sandboxing environment and finally, i came to know that file has malware and also I have taken SHA 256 value
- In the eradication phase, i deleted the file from the end user machine and re-run the AV scans, and also changed the password by contacting the helpdesk/service desk team.
- In the recovery, phase brings it back from abnormal to normal operations
- In the Lessons learned phase as a post motern report, i have prepared root cause analysis document and finally, i analysed why, how, and when it is got compromised. The reason behind for compromise regularly Windows patch updates are not happening and also AV agent sleep when the attack happens due to this reason when the user downloaded the .dll file from a trojan or illegitimate website system got compromised.

- I reviewed the RCA document with the SOC manager and presented to my client or customer
- Due to this reason, i got an appreciation email and was also selected for a monthly award due to my productivity and the quality of the Incidents i was handling

One of the SERVER got compromised by Malware

- Recently I done One of the Server system got compromised Malware incident investigation
- Well, An Alert is received through the IBM Q radar SEIM dashboard and also from the email notifications.
- I went to the SIEM dashboard & assigned the ticket myself and also, I acknowledged other soc team members as well about the incident
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for Tracking the incidents.
- After creating a ticket in the ticketing tool, I started triaging the information like IOC, IOA, asset profiling, and user profiling. Nothing but I have gathered victim IP-related details, IP address, username, or system name
- I gathered additionally file name, file size, File category and file extension
- This attack received through. DLL file when the user downloaded the file from the trojan website
- After that, I went and created a ticket in the ticketing tool. In my organization, we are using the Service now ticketing tool for the Tracking of incidents.
- This is escalated priority 1 (P1) ticket and scheduled a call with the Asset owner and asked a couple of questions before doing the containment(Network isolation)

  a) Is there any backup server is available?
  b) are you taking any regular backup config?
  c) are there any critical applications are running on top of this server?
  d) How many users are going to impact in case if we are taking network isolation or containment?

I got the below answers from the asset owner or server owner

a) Yes the backup server is available it is facing the internet and it is a critical server to the organization
b) Yes, the Regular back ups they are taking has been
c) yes critical legacy applications are running (Basic java based application developed long back)
d) a large number of users are going to impact.

- Based on the server owner confirmation and details, I made a back up server as a primary and continued the business operations without impacting any users.
- whatever server got compromised i have done network isolation in the containment phase.
- In the eradication, phase .dll file and verified malware analysis in the sandboxing environment and also a couple of open source tools and found that though .dll file malware got infected.
- Deleted the file through which the AV got infected. Rerun the AV scans and finally changed the passwords of the windows machine
- Finally, I brought it back to high availability with in the SLA 4 hours defined in the recover phase.
- In the Lessons learned phase as a post motern report, i have prepared root cause analysis document and finally, i analysed why, how, and when it is got compromised. The reason behind for compromise regularly Windows patch updates are not happening and also AV agent sleep when the attack happens due to this reason when the user downloaded the .dll file from a trojan or illegitimate website system got compromised.
- I reviewed the RCA document with the SOC manager and presented to my client or customer
- Due to this reason, i got an appreciation email and was also selected for a monthly award due to my productivity and the quality of the Incidents i was handling

Phishing E-Mail

Log source - Email Gateway/security, EDR(AV), Proxy and NGFW
Normally Attacker will trick the end user by sending and e-mail

Attacker will trick the end user by sending an email and he will again unauthorised access or sensitive data exposure

How can we identify?

Attacker will use either invoice copies or Attacker will use lot of spelling mistakes , Malicious Domains , Malicious URL Links, Gift card, and so on these are all the ways attacker will send an E-Mail

Types of phishing

- spear phishing - Email will send it to single user or group of users
- whaling- Board of directors or senior management or CTO, CIO, CEO, CFO, CISCO , VP, Director
- wishing- By phone call
- smishing-Through messages or SMS

- Malicious Attachment- Malicious attachment via email
- Malicious URL link

Every E-Mail Contains

- Sender email address
- Receipt email address
- Send IP
- Receipt IP
- DMARC

DK
DKIM
SPF
Return Path
Header Analyzer

Email Gateway or Email security solution

- Proof point
- Iron port
- Mime cast

O365 - ATP (Advance Threat preventation)
Trianz

When the particular e-mail is coming above tools will validate whether it is a malicious domain are not

In case if we are not using the E-Mail gate way we have the multiple options like Virus Total.com, MX Tool, IP Void, & so on EX; one email received from the Test.CTS.com this we have to validate the and we have to check the reputation

Investigation

Whenever any phishing e-mail receive, we have to do Domain validation (Whatever email that we received every e-mail contains after @ domain is existence that is domain name ex; @yahoo.com , @gmail.com & so on

Domain validation: MX Tool, ip void, cisco Talos, virustotal.com
We have two options based on the Reputation checks , Analysis , Based on the validation and after speaking with respective SMTP Server team finally if they say its malicious domain name then we have to block this one

Option 1: If it malicious domain name , we have to block in the DNS server or Proxy or NGFW
Option 2: If it is legitimate domain name , we have to do further investigation

For IP Address Validation

IP Address validation: Virustotal.com, mx tool, cisco Talos, ip void
Option 1: if it is legitimate ip address, further analysis
Option 2: If it is illegitimate ip address, we have to block firewall

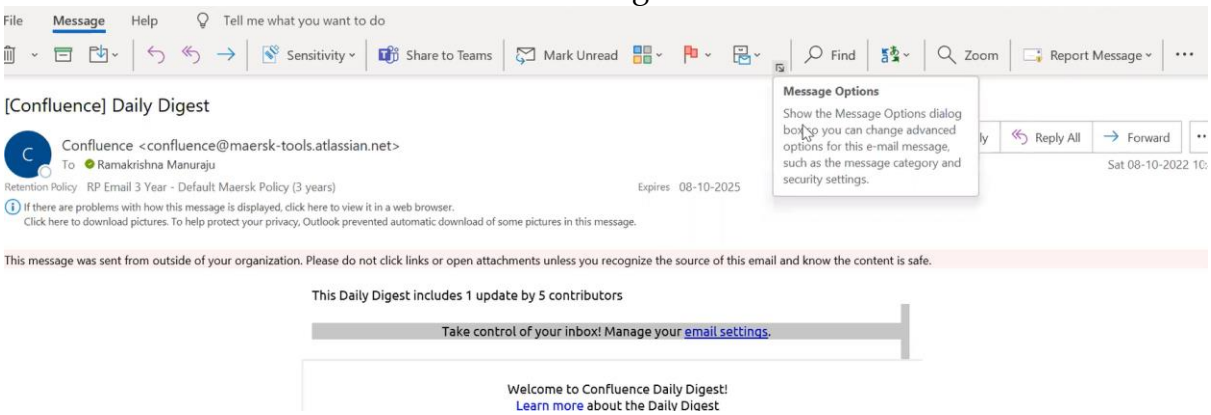
Header analyser

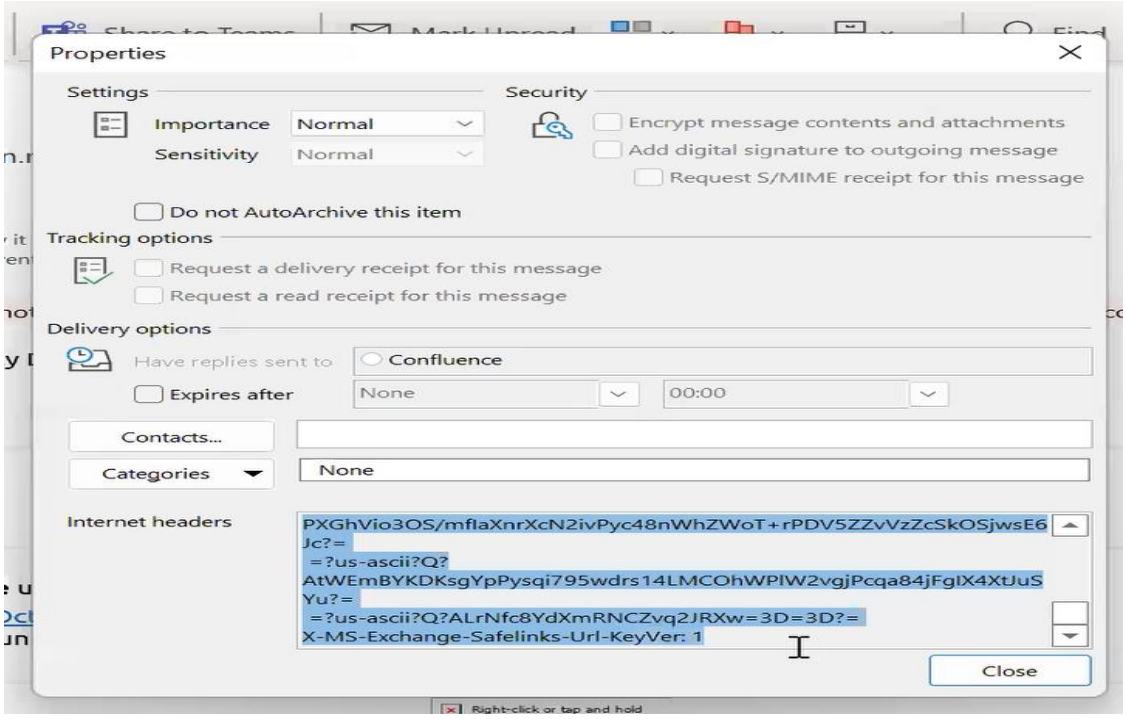
Analyse the header related DKIM, SPF, DMARC and see whether reputation is passed or failed.

Return Path

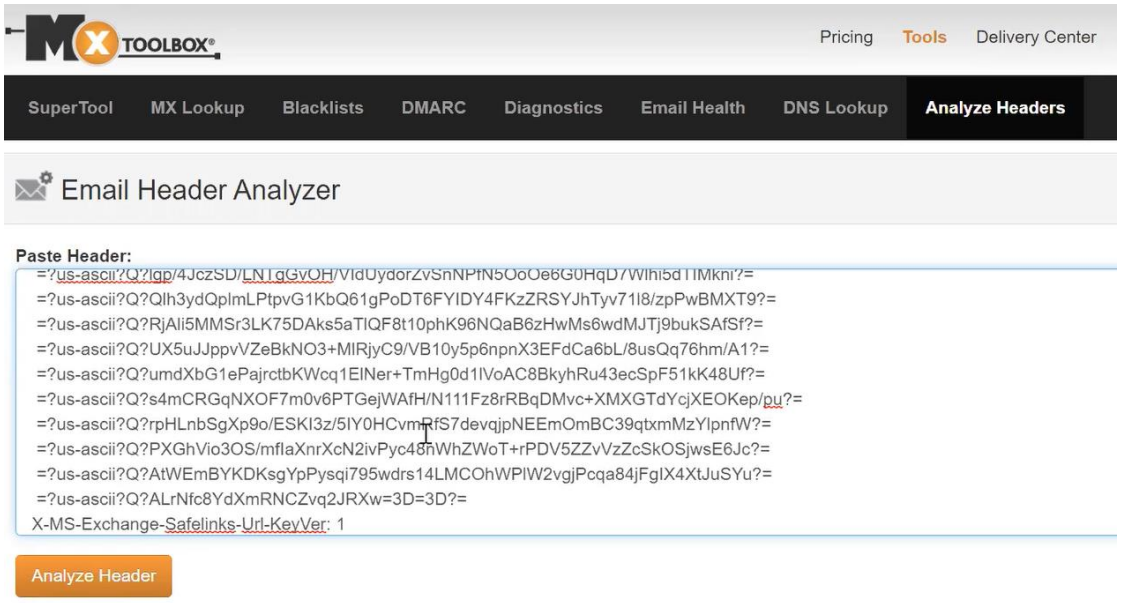
Return path is always sender or receiver email should be there this we see under the Header Analyser if we see other than sender or receiver email address we have to suspect that it is a phishing email

Under the Out look middle we will be having the Arrow Mark





As we see the Internet Header. Copy that Analyzer go to the MX Tool paste it under the Analyse Header



In header Analyser what filed you will verify (Interview Question)

Return Path

Do you know how to do Manual header Analyzer or do you use any tools to identify the Header Analyzer (Interview Question)

Yes I do Manual I check it under the MX Tool under the Analyse header

One of the spear phishing email coming as a malicious URL Link in that situation how can you do investigation? (Interview Question)

Take a URL and go to either URL scan or virustotal.com or hybrid analysis.com and verify URL reputation

Option 1: Illegitimate or malicious URL , blocking the URL either in the proxy or firewall

Option 2: Illegitimate or genuine URL, Genuine email

Additional thing we can do that if anyone clicked on that particular URL Link. We have to check how many end users are received this email whether single user are group of users

We can verify this information under email gate way, If we are not using email gate way we can verify under the SMTP server

If in case 05 clicked on it & remaining 5 didn't clicked

The log sources we can analyse in proxy , NGFW& firewall if we are using email gate way then its email gate way only

Malicious Attachments

Phishing email + Malware Analysis
How many end users are clicked on the attachment , How many end user downloaded this attachment we can identify this information with email gate way we can conclude
How many people downloaded the attachment we can see under firewall & even under proxy also
After identify how many users got received and how many of downloaded & how many people didn't touch the attachment
We have to take the file we have to go to the sand boxing environment are else we have to go to the Hybrid analysis or Virus total.com
We have to verify real this file contains malware or not
If the file is showing as malware we have to block the Hash value , delete the file & we have to re run the scan , should change the credtianls

100 phishing email attackers sending 100 phishing emails to 100 different users how can you do Phishing investigation/? It could be malicious URL or Malicious Attachment
Based on the severity we pick
We distribute within the group

1 server got compromised by malware
2 End user got compromised by Ransomware
3 CEO received phishing email

Above All these are under critical, which you take it into consideration?

1 , 3 , 2

SQL Injection Flaw Attack

Log Sources

- WAF – syslog
- Web Sever or Application server – Collector Agent method
- Application Log – syslog/API Token management method
- Data Base – syslog/Collector Agent

How SQL Injection Alert will be generated (Interview Question)

With Help of correlation rules & use cases which we created and couple of logs , log source we have integrated to the Application site, once we are integrating these logs to the SIEM Tool then OWASTOP 10 & SANS TOP 25 related Alert notification we can see in the SIEM Tool.

Blocking in the WAF those logs going into the SIEM Tool on SIEM Tool based on the correlation rule use case it is hitting and alert is generating which is false positive

But in case Alert is received in that Alert using machine learning mechanism or behavioural pattern mechanism so may user either he entered into trusted data or untrusted data or malicious script or normal scripts in that time also that particular WAF is treated as a Malicious activity in that situation

False positive

1. Under the WAF side block option will be there so these logs we already integrating it's a false positive
2. WAF Alert is generated under the False positive we collect the incident & we close the incident
   Under the True positive WAF alert Is received based on the correlation rule whatever its configured untrusted data it got entered finally it got compromise as per ITIL Process we should do

Triage

- IOC
- IOA
- Asset profiling
- User profiling

Containment

Injection flaw – Backend sever

CSS or XSS – Application Data Base , we should speak with Asset owner or application owner or server owner

Eradication and mitigation - Raise a ticket with application development to fix the input validation or parametrised queries or csp or Anti CSRF tokens

Recovery – Abnormal to Normal

Lesson learned –

- RCA we should do
- Why it is got compromised

- Is it input validation went wrong we should check

Recommendation

- Proper input validation
- Security awareness training Development team (Secure code warrior and immersive labs)
- Patch updates

HTTP Authentication code (Interview question)

We this HTTP Authentication code whenever either external or internal user trying to access the application

Code series

- 100 – (It provide the Information) It will indicate is so far ok and whatever client should continue the request or ignore if the session is finished
- 200 – (Successful Response)
- 300 – (Re directional) ex after purchase we go to payment option then it will go payment gateway
- 400 – server can not proceed
- 500 – Client

Windows Log on Type

Windows log on type we use to log in into the respective system. That system may be either server , Mac book , Desktop , work station & so on it is dedicated applicable to windows only not applicable to operating systems most of the cases its micro soft operating systems

All the Log on types we see in the Active directory once we are integrating AD or DC logs

These logs are not only applicable to successful log on but also with failure log on

Type Number	Type Name	Description
Type 2	Interactive log on	Console of a computer log on type
Type 3	Network log on	when the user access remote file shares or printer. Log on to IIS server using basic authentication

Type 4	Batch Log on	This is used scheduled tasks or also patch updates
Type 5	service log on	This is used for services and service account that log onto service restart or stop
Type 7	Unlock	This is used to unlock windows machine
Type 8	Network clear text log on	This is used when we log on over a network and passwords are sent in the clear text
Type 9	New credentials	This is used when the user is accessing the windows machine first time using default password
Type 10	Remote interactive log on	This is used for RDP based authentication to log into another windows machine or server
Type 11	Cached interactive	Using saved user name and password or credentials log into the windows machine

Windows Logs Types (Interview Question)

- System
- Audit
- Application
- Security
- Forwarded Event

Linux Log types

- * All Logs
- /var/log Normal Logs/Consif/System
- /var/log/httpd Application
- /var/log/sshd Linux Audit Logs

From disable account how login attempts failures are coming (Interview Qustion)

Using windows type 11 log on type that is called chache interactive log on type. Because our credentials got stored in the respective domain controller and that domain controller will keep on communicating to the centralized authorise server. So backend type 11 log on type it will generated using collector agent method these logs goes to the SIEM Tool and whatever correlation we have created for the disable account log in attempts failure it will those correlation rules or use cases finally it will generate the Alert notification in the SIEM Tool

Firewall Logs

- Audit
- System
- Configuration
- Malware
- Application
- IDS/IPS
- WIFI

What do you know about Linux server & windows server (Interview Question)

Linux Is more secure no need to reboot

In my roles & responsibility windows server log I will integrate

Collector Agent method to SIEM Tool from respective windows server. I have knowledge on windows server logs to SIEM Tool, Linux server logs to SIEM Tool using the collector Agent method

So normally windows log type will integrate system Audit application security and forwarded events

On the Linux side we will integrate the /var/log/httd , /var/log/sshd. These are all the path of the logs will integrate to the SIEM Tool

Additionally I do have the experience in harding side because I worked vulnerability assessment for one year I know what all the hardening bench mark will use by the windows server as well as Linux Server ex; Like network partition , Auditing related , Login and monitoring related. So total 225 compliances as a initial configuration we will configure under the windows server & Linux server so these much knowledge I have on the windows & Linux server

If need any support will raise the separate ticket to the Windows or Linux team for the support

How do you protect the security to Linux server (Interview Question)

- Regular update nothing but vulnerability patch updates
- Creating a role-based access control using a IAM based on roles & responsibility wise
- Complex credentials using strong passwords
- Using SSH
- Ips table configuration nothing we using white listing & block listing of the traffic
- We can use DLP
- Removing un using library or packages

- Integrating logging & monitoring part what are the logs are generated in the Linux server those logs we have integrated to the SIEM Tool
- We should implement hardening bench mark

What is multi factor authentication in Linux server

After entering the password if we want to provide the more secure way of communication log in to the server for that normally We should use private key

DOS & DDOS

Dos stands for Denial-of-service Dos do the rejection of the service. Server, Application, Data Base is not available for legitimate users, which is availability issue as per CIA Triade

Single Attacker will target the single Server

Log sources – NIDS/NIPS, FW , Anti DOS/ Anti DDOS , WAF logs , Server Logs

Only for server logs we use the collector Agent method from NIDS to WAF we use syslog method

DOS & DDOS is combination of both Internal & External Attack

DOS & DDOS – Internal Attack (False Positive)

1st we have to raise the ticket in the ticketing tool

We have to inform to the team

We should start Triage the incident IOC this is Internal so we have only IOC no IOA because this is not external

We have to collect under IOC Like

- IP Address
- User Name
- Computer Name
- Flooding of the request – why it is getting so many of request
- Location

After Triage we have to do Analyse IDS/IPS Logs , Firewall Logs we have to Analyse

We should also find out why the end user is sending so many request

After sending an email we will do

- Collecting of evidence
- Summary Report

- Then final close the ticket

DOS/DDOS True positive (External Attack)

With the help of IP Address we can find out

Many Ips will come in this to attack

1st we have to raise the ticket in the ticketing tool

We have to inform to the team

We should start Triage the incident IOC & IOA

We have to collect under IOC & IOA Like

- IP Address
- User Name
- Computer Name
- Flooding of the request – why it is getting so many of request
- Location

Containment is required when primary Applications are going down in the disaster recovery side whatever applications we hosted so we make that up and run the Business Operations

Eradication & Mitigation –

- Updating the signatures
- Re run the scans
- AV/EDR is agent running properly or not

Recovery – Bring it back to Normal & Ab Normal
Lesson Learned –

Why it is got compromised as DOS & DDOS
We don't have the threat intelligence commercial feed solutions & wrongly we have define the rate limit

We don't have Anti DOS & Anti DDOS

Mitigation
We have to make sure threat Intelligence feeds integration should do, Regularly we have to identify what is the malicious Ips coming all over the world wide
Those ips we have to block in the firewall or proxy or DNS

Malicious Hash values in the EDR Tool

If we are doing proactively even

How can you identify that its DDOS Attack

1st from this particular IP we have to find out one connection is coming or so many are coming, we have to do segregation with them, then we have to do reputation check finally we can block those IP Address in the SIEM Tool

Command and control server

One of the system got compromised and keep on contacting to command and control server

Main source of the C2C Communication log source is Firewall, IDS/IPS

This is maintain by the Attacker

This is not only applicable to Malware or Ransome ware category even it is applicable to Brute force Attack got compromised

It is a true positive because already got compromised it is communicating to command and control server

1st we have to assign the ticket

Then we have to find out how the attacker enter into the organization what tactics that he used

We should inform to the team members

Then I will Triage the Incident like IOC & IOA

Under IOC

- Victim IP
- user name
- server name
- host name
- location

Under IOA - Attacker ip address

TTP – Port scanning , Authentication failure , Malware , Phishing mail , OWASTOP 10, Flooding , Spoofing

In later movement What technique will attacker use (Interview Question)

Credential steeling

1st I will identify how the attack is received to the organization will find out what tactics & techniques used

What type of incidents it is breached by the hacker

Will find out which technique that attacker used

From there if it Is authentication failure will analyse domain controller logs

If it is malware then Analyse the EDR Tool & firewall

If it is phishing will use email security & SMTP Server logs

If it is OWASTOP 10 will use WAF (web application firewall)

Under flooding I will analyse the Firewall , IDS/IPS Event Anti Dos & Anti DDOS backend data server logs

I will analyse all these logs what type of Data breach

Will analyse is this end user or server

What is the victim ip

If it is end user system then I will do directly containment

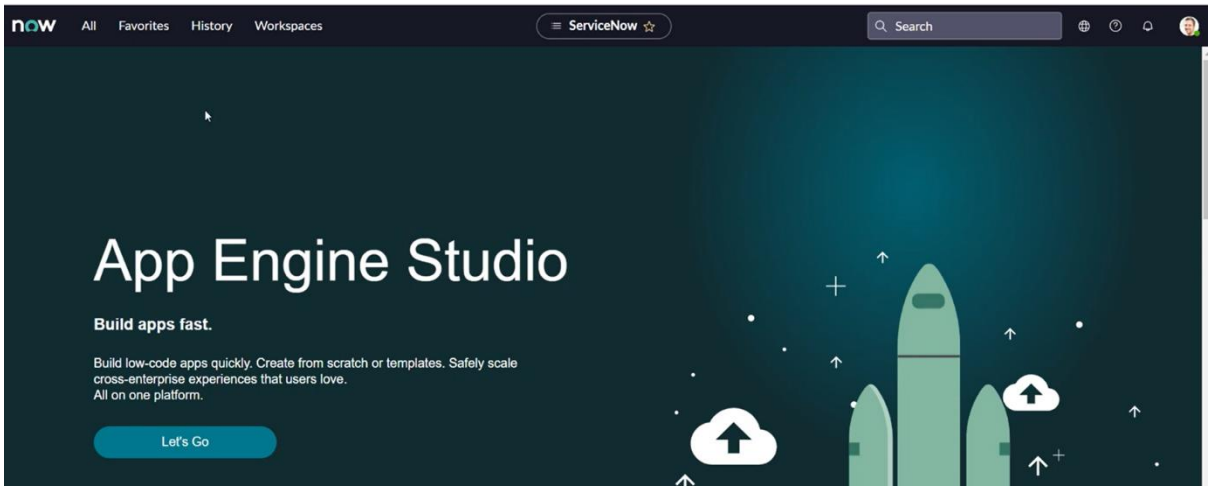
If it is sever I will contact to the business owner

Then I will take care the eradication & mitigation

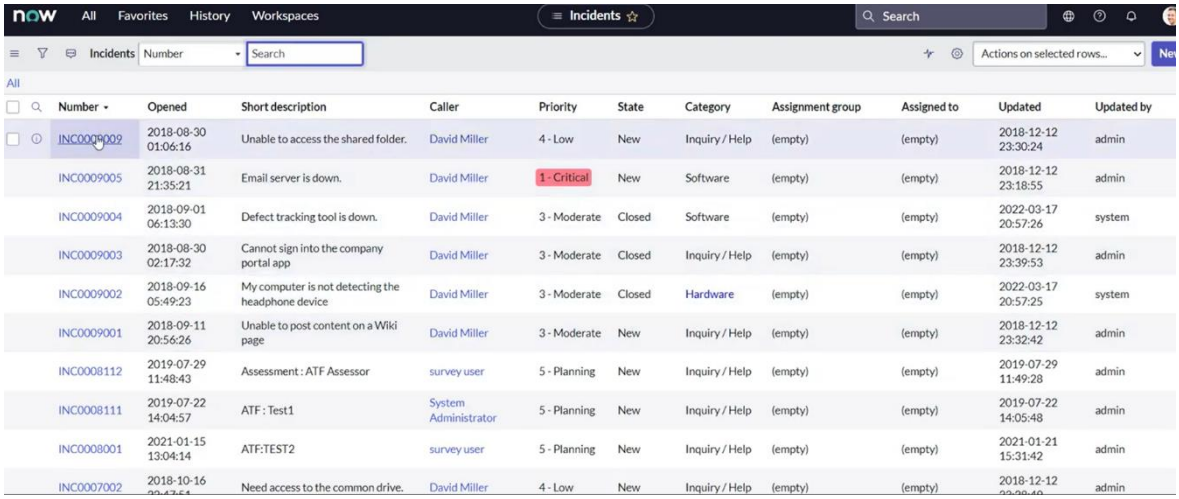
Then infection cleaning bringing back Abnormal to normal

Then preparing RCA

Service Now Ticketing Tool

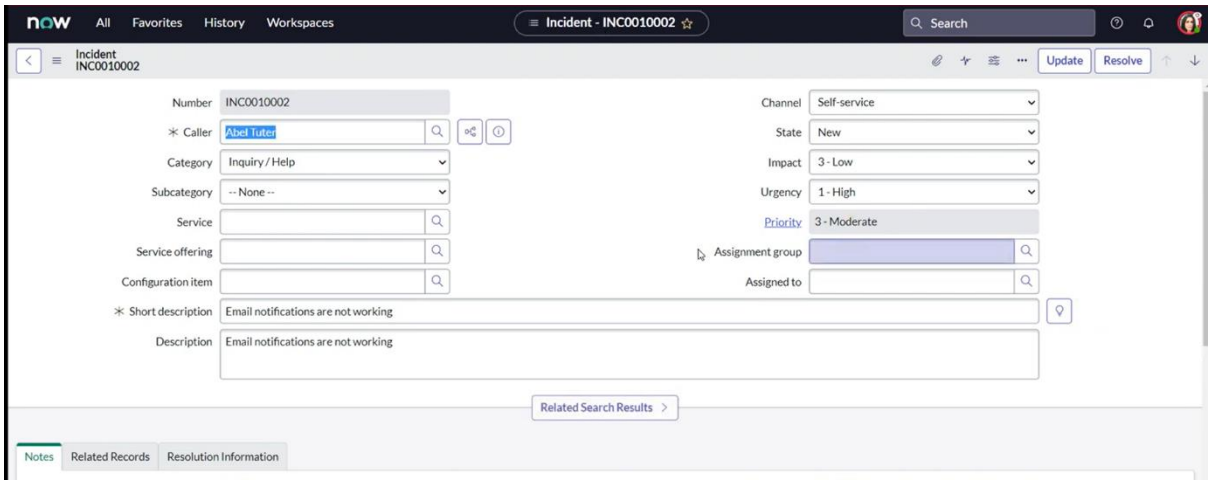


As we can see the option over there All under that we have to click incident once clicking incident we get an option called All under Resolve



After clicking the All as we see this page will be populated

Once creating a ticket automatically, the ticket number will be populated over as we see below



Under channel we no need change anything it is same as it is

Category – Under the category option what kind of incident that we seeking for like whether malware , phishing category and so on whatever the Incident that we received in the SIEM Dash board or through the Alert notification we have to choose the category of the incident

Sub category – ex malware is the category under malware category we have the received the Virus Alert we have to choose sub category as a virus

In case if we have received the Ransome ware we have to choose sub category as Ransome ware

If flooding category we received in the SIEM Tool in that situation we have to come to the service now ticketing tool and we have to create an incident once creating the

incident the above page will be populated, category we have to choose as flooding category sub category whatever incident that we received like TCP Flood, sync flood , UDP , Ping of death and so on we have to choose as a sub category

Impact – It is shows the severity of the incident whether it is critical , High , Medium , Low or informational based on the incident what we have received impact

Urgency – Similar to the Impact

Once we defining the Impact & Urgency assigned group

Assignment group – Here we should not assign to the particular person always we have to assign to group of people

Once we are assigning to the particular group it will go to their people from their they will pickup the respective ticket

Assigned to

If any dependencies is not their we have to assign ourselves ex; one of the Alert is received that alert is brute force attack

Now we are going to do ticket here under the category we have defined as Authentication failure category sub category is brute force attack

- Urgency is critical
- Impact is critical

Then this assigned to we have write our name over there

After creating ourselves we have to define the what is the description of the incident & what is the short description nothing but classification of the incident nothing but brute force attack

Description – One of the Alert is received brute force attack from the internal IP or external IP

After gathering all the information we have to define in the description page like what Is the triage of the incident IOC , IOA

Evidence we have to attach all the time its very important

IBM Q radar SIEM Correlation rules creation or use case creation

1. Multiple authentication log in failure from single user name

1. I will log into IBM q radar and will go to offences tab and will click on rules option
2. After that i will click on new corelation rule or updating existing corelation rule for events and flows
3. I will click on next button and will see the wizard window.
4. After that will click on next button and will choose the building blocks (BB)
5. Then I will go to logic button and will define the logic

Logic is when the event is matching any of the following

Logic –

- BB: Category definition: Authentication failures
- Condition AND at least 10 events are seen with the same user name in 2 Minutes

After the logic then

6. Then I will select category of the incident classification
7. Then I will click on next button and i will see rule action tab.
8. In the rule action tab I will define Relevance(0-10), Severity(0-10) and credibility(0-10)
9. In the rule response tab I will specify the email notifications (ex: SOC@TCS.COM) other than email notification couple of options are available SNMP Traps , E-Mail , Syslog , Reference set (Reference set in the sense list of single elements & it will form against those simple list format ex; Source IP or Destination IP , source port of Destination port these are the couple of options
10. After creating correlation rule then I will test wontedly from testing machine and will whether alert will be generated or not
11. If alerts will be generated then i will raise a change request and implement in the PROD environment after taking approval

2. DOS attack against single host (Flooding of the requests are coming)

1. I will log into IBM q radar and will go to offences tab and will click on rules option
2. After that i will click on new corelation rule or updating existing corelation rule for events and flows
3. I will click on next button and will see the wizard window.

4. After that will click on next button and will choose the building blocks (BB)
5. Then I will go to logic button and will define the logic, Logic is when the event is matching any of the following

Logic

- BB: Category definition : Flooding of the requests
- AND at least 50 events/sec are seen with the same hostname in 1 Minutes

After the logic then

6. Then I will select category of the incident classification
7. Then I will click on next button and i will see rule action tab.
8. In the rule action tab I will define Relevance(0-10), Severity(0-10) and credibility(0-10)
9. In the rule response tab I will specify the email notifications (ex: SOC@TCS.COM) other than email notification couple of options are available SNMP Traps , E-Mail , Syslog , Reference set (Reference set in the sense list of single elements & it will form against those simple list format ex; Source IP or Destination IP , source port of Destination port these are the couple of options
10. After creating correlation rule then I will test wontedly from testing machine and will whether alert will be generated or not
11. If alerts will be generated then i will raise a change request and implement in the PROD environment after taking approval

3. Failures from disabled account

1. I will log into IBM q radar and will go to offences tab and will click on rules option
2. After that i will click on new corelation rule or updating existing corelation rule for events and flows
3. I will click on next button and will see the wizard window.
4. After that will click on next button and will choose the building blocks (BB)
5. Then I will go to logic button and will define the logic, Logic is when the event is matching any of the following

Logic

- BB: Category definition : Authentication failures
- AND when disabled account (User account) count match 5 events in 1 minute

After the logic then

6. Then I will select category of the incident classification
7. Then I will click on next button and i will see rule action tab.

8. In the rule action tab I will define Relevance(0-10), Severity(0-10) and credibility(0-10)
9. In the rule response tab I will specify the email notifications (ex: SOC@TCS.COM) other than email notification couple of options are available SNMP Traps , E-Mail , Syslog , Reference set (Reference set in the sense list of single elements & it will form against those simple list format ex; Source IP or Destination IP , source port of Destination port these are the couple of options
10. After creating correlation rule then I will test wontedly from testing machine and will whether alert will be generated or not
11. If alerts will be generated then i will raise a change request and implement in the PROD environment after taking approval

4. Failures from terminated account

1. I will log into IBM q radar and will go to offences tab and will click on rules option
2. After that i will click on new corelation rule or updating existing corelation rule for events and flows
3. I will click on next button and will see the wizard window.
4. After that will click on next button and will choose the building blocks (BB)
5. Then I will go to logic button and will define the logic, Logic is when the event is matching any of the following

Logic
BB: Category definition : Authentication failures
AND when terminated account count match 5 times in 1 minute .

After the logic then

6. Then I will select category of the incident classification
7. Then I will click on next button and i will see rule action tab.
8. In the rule action tab I will define Relevance(0-10), Severity(0-10) and credibility (0-10)
9. In the rule response tab I will specify the email notifications (ex: SOC@TCS.COM) other than email notification couple of options are available SNMP Traps , E-Mail , Syslog , Reference set (Reference set in the sense list of single elements & it will form against those simple list format ex; Source IP or Destination IP , source port of Destination port these are the couple of options
10. After creating correlation rule then I will test wontedly from testing machine and will whether alert will be generated or not
11. If alerts will be generated then i will raise a change request and implement in the PROD environment after taking approval

Wire shark

Wire shark is useful for network traffic analyser for packet capture purpose, it is mainly for trouble shooting purpose. If we want to analyse any network traffic in this we use this particular network traffic analyser it is nothing but wire shark

Most of the cases it will used by the SOC implementation team (when ever we are integrating the logs to the SIEM Tool at that moment) & NOC Team

Wire shark will Analyse TCP IP Layers only

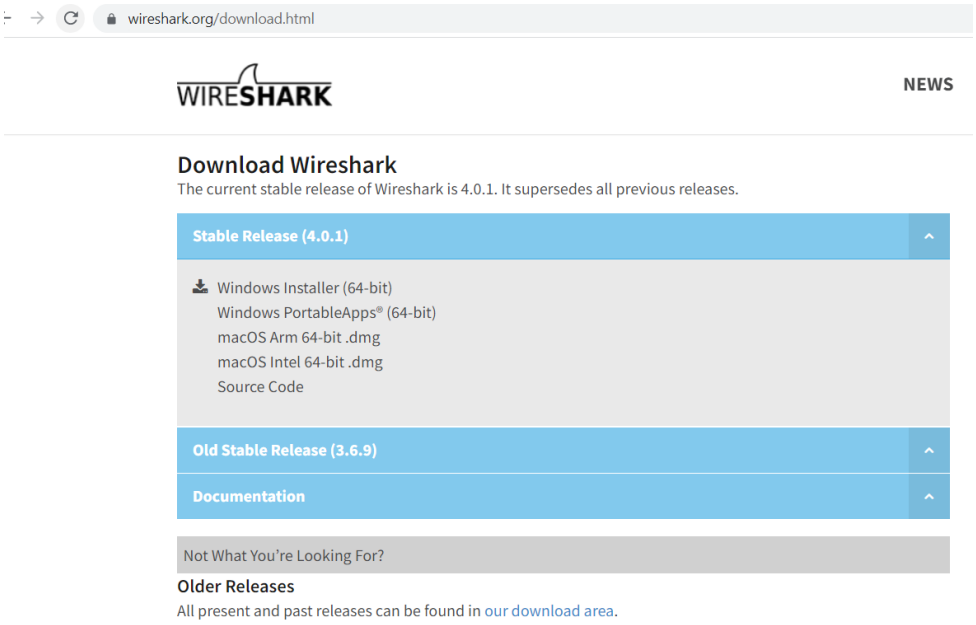
TCP Layer how we have (Interview Question)

TCP Layer we have only 04

- Application , session
- Presentation is converted it into single application layer
- Transport is Transport only
- Network is nothing but internet layer
- Data link + physical layer is nothing but network interface layer

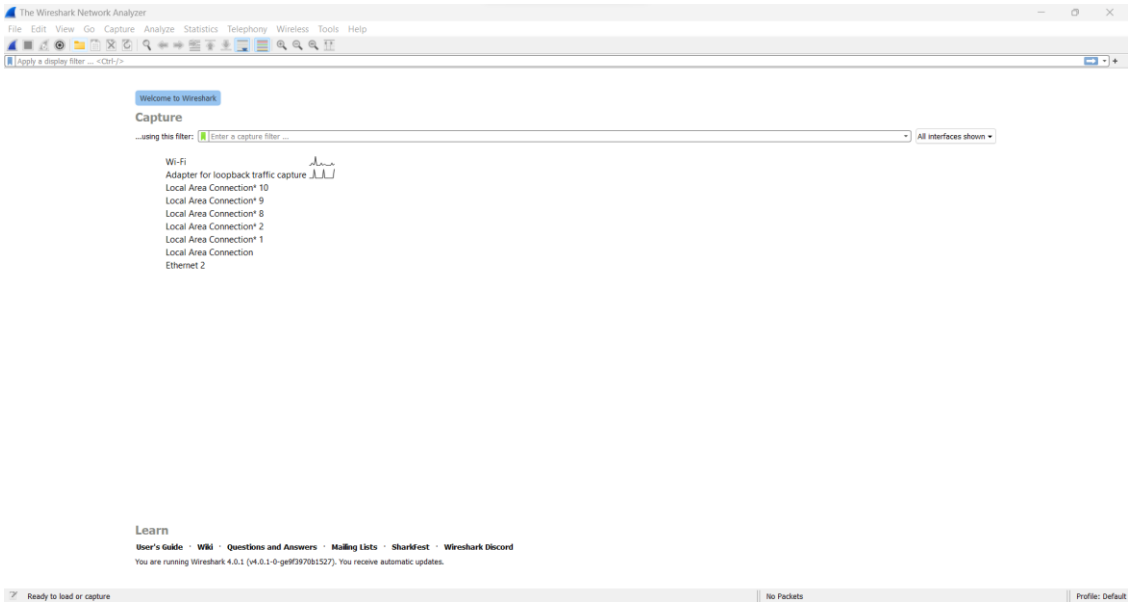
For downloading the wire shark we have to use

https://www.wireshark.org/download.html

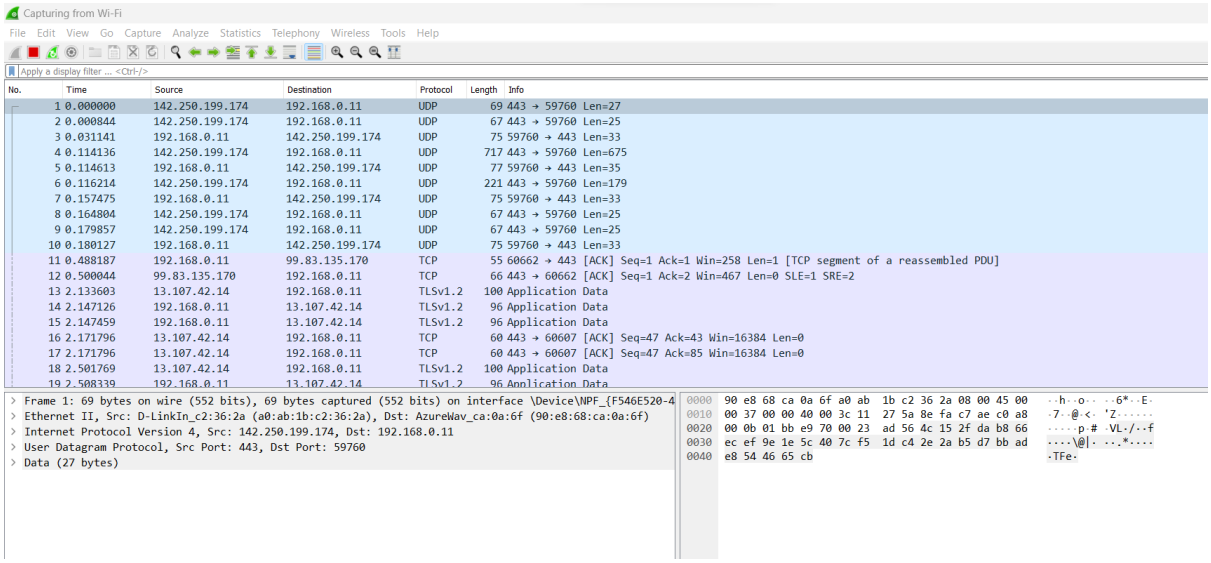


For downloading we have to click on the windows installer (64-bit) always we have to download stable release

After downloading as we can see the below picture this interface will get populated



As we can see the WIFI option as whatever WIFI traffic is going in our laptop it will monitor everything it is capturing



This is how it looks whatever traffic is going through WIFI if we want to stop we have the option red colour then it will get stop

As we the search button above it is filtering. Filtering is based on time, source, Destination, HTTP, DNS,TCP, UDP , ICMP & so on in different ways

As we see the colour over here Red nothing but some issue is going on under it

As we see only white colour which means we don't have any issues over here

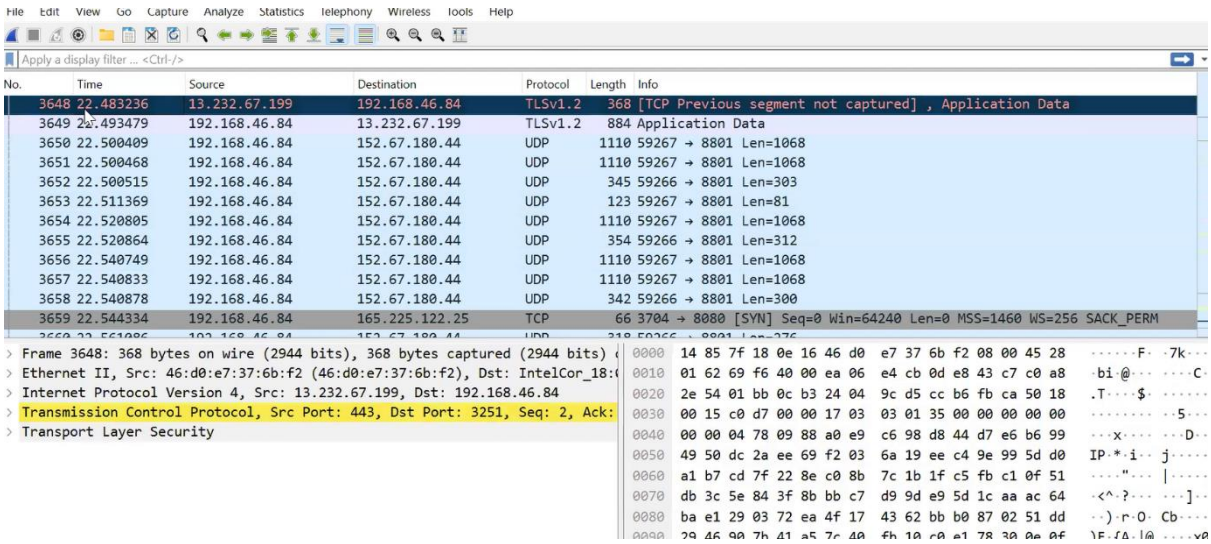
- Purple colour it will represent TCP Traffic
- Pink colour will represent UDP Traffic

Once we exporting the packet from the firewall and importing from the wire shark tool from this will come to know how to analyse the traffic

As we work only RED option only because those red colour packets are re transmission , packet is dropped , packet is not sent , communication is not establish , TCP 3 Way hand shake is not establish between these two or DNS resolution is not happened

Issues can come any layer not only in Transport layer

- Application layer
- Network layer
- Network interface layer



How can you filter out IP Address in wire shark (Interview Question)

IP.ADDR = = IP Address (Ex – 192.168.46.84 so if the respective IP Address is existing then it will comes as green colour other wise it will come as a red

What is captive portal in firewall

Captive will represent the status of the website whatever the end user is accessing whether it is allowed activity or blocked activity

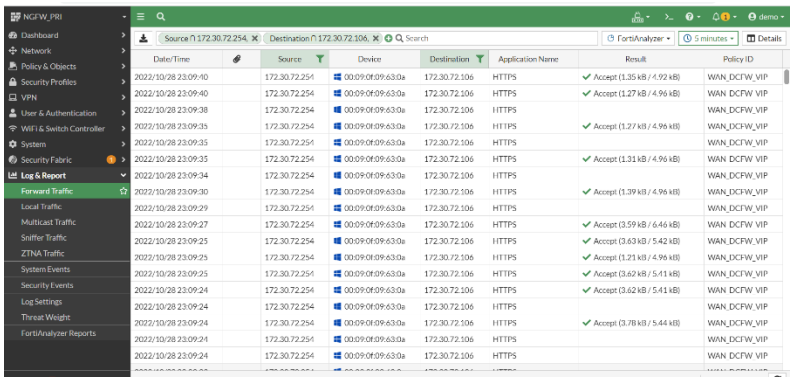
Exporting packet capture from forte Gate firewall to wire shark process

Packet capture we should take that file from forte gate firewall under the log & Report tab

Then we have to click the forward traffic option

Whatever the alert which we received in the SIEM Tool that respective Source IP & Destination IP

Once clicking on the forward option we have the + option were we can select the source IP & Destination IP as we have seen in the picture below

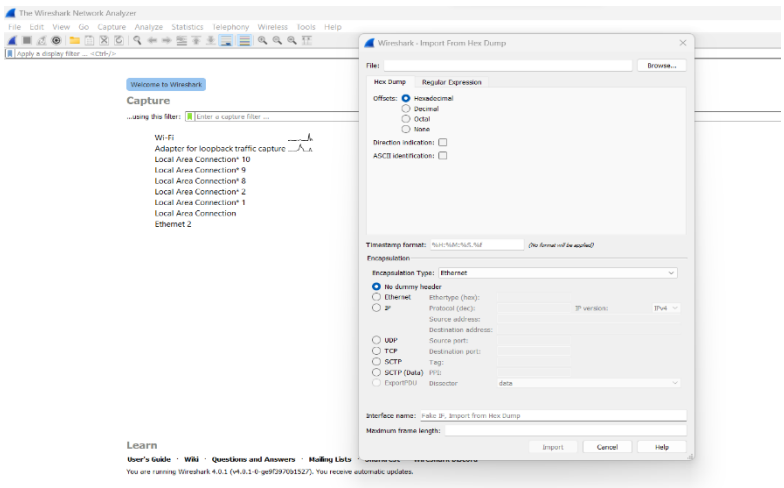


To download the file as we see in the above picture down option symbol left side as we can see

Under the wire shark we have to click on the file option then as we can see the drop down import from Hex Dump

Once clicking that we will get this interface as we can see below the picture

1st we have to export the file whatever incident is happen ex; In SIEM Tool we have received one of the Alert we are not sure what exactly the network traffic or packet capture analysis, we are not sure where is the issue EX; One of the malware kind of incident is happened or may be any dos or DDOS Kind of attack is happened so that alert will comes to the SIEM Tool. in SIEM Tool we will go and will take those Logs and whatever the incident time is happened. That time we have to go to the firewall or the that time we have to go the IDS/IPS and we have to export the packet capture file



Once downloading the file we have to browse the file as we can see the option import then we have to import

Cloud

Cloud is like virtual space this will be provided by the respective vendors ex; Amazon, Google , Oracle , IBM , Ali Baba & so on these couple famous vendors,

Cloud is cheapest solution compare to Tools that is one of the Advantage

Cloud is useful for the storing of the data and also for deployment of the servers

Advantages

- Inexpensive solutions there is no need maintain the Data centre
- Elasticity of the major in cloud
- High Availability
- No need to maintain Physical location

3 types of cloud we have

- Public cloud
- Hybrid cloud
- Private cloud

Public cloud is less expensive as compare to Hybrid , As compare to private here public is cheap

3 different types of services every cloud service is supporting

- Amazon
- Azure
- Google
- Oracle

IBM

Ali Baba

These are the biggest cloud service provider world wide

Services which they are providing is IaaS (Infrastructure as a service) , PAS (Plat form as a service) , SaaS (software as a service)

Most of the organizations are using IaaS only

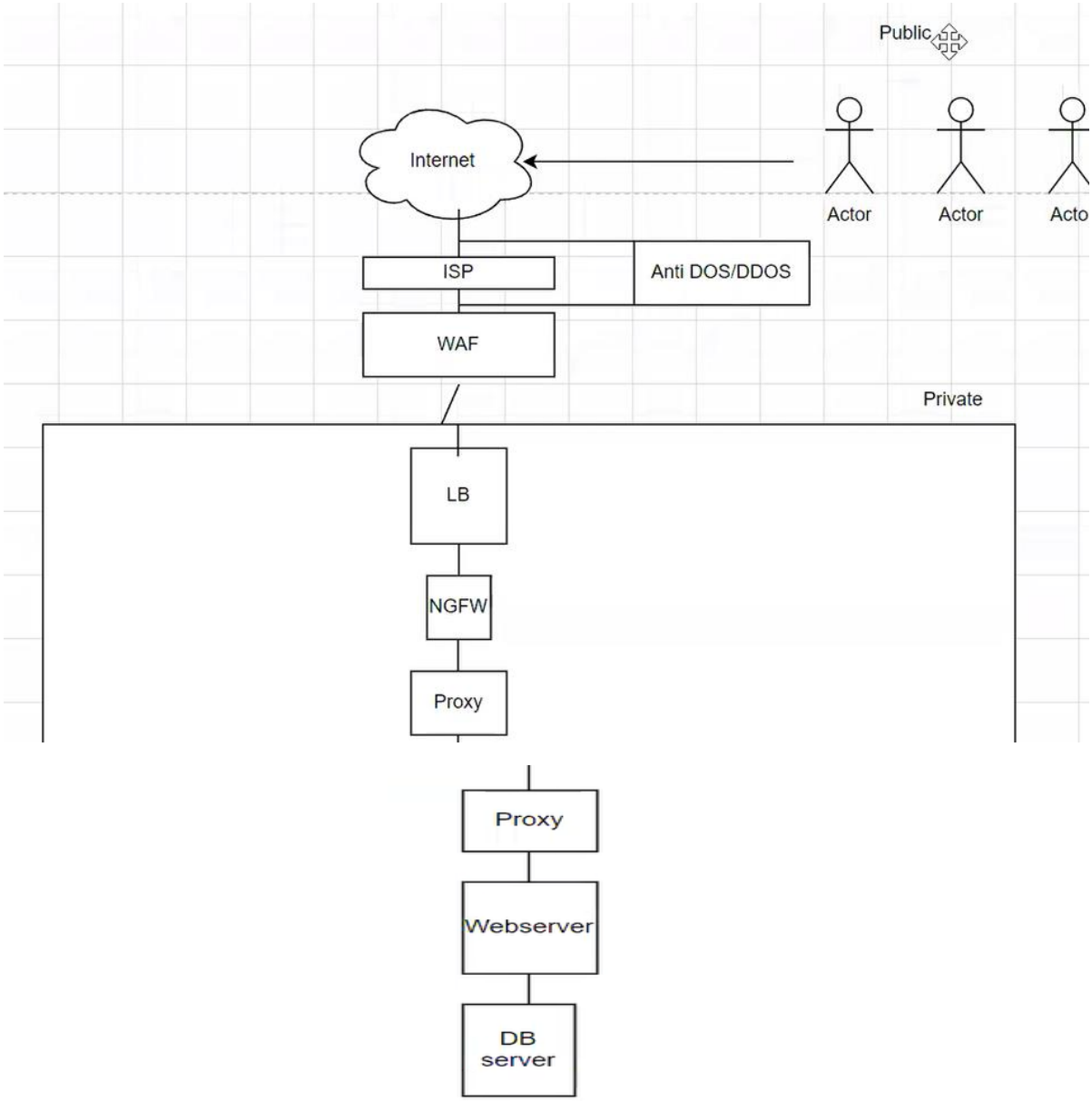
Out of these cheapest is SaaS base

2 types of services we have

Native services – whatever inbuilt cloud services are providers they are providing nothing but default

BYOL (Bring your own licences) – It is Third party vendor

Cloud Security					
	Cloud service providers		Amazon	AWS	USA
			Microsoft	Azure	USA
			Google	GCP	USA
			Oracle	OC	USA
			IBM,	IBM	USA
			Alibaba	Ali Baba	China
	Services		Native services	Default	Cloud service provider services
			BYOL	Bring your own l	Third party
	SIEM tools in cloud	Amazon	Gaurd duty	SIEM tool	
		Azure	Sentinal	SIEM tool	



As we see in the Above picture Public , when see the public it is nothing but un trust zone

If we want to access any website from traffic it will go Internet from Internet to ISP, In parallel to ISP Router that is 1st entry point, we will deploy here Anti Dos & Anti DDOS solutions where when ever any Dos & DDOS Attacks will come these Anti DOS & Anti DDOS solutions will be prevented and block

And also it will provide the Alert notification also based on the behavioural pattern mechanism

From there It will go to the traffic WAF so this WAF, if we want we can use Amazon , Azure , GCP & so on whatever we have chosen other wise if we don't want respective cloud service WAF in that situation we can go through BYOL ex; Akamai , Imperva , Barracuda these are the leading WAF in the Market

WAF we have to deploy it will prevent Against all OWASTOP 10

From there traffic will go to respective VPC – Virtual private circuit network so nothing its an Internal zone

As we see in the picture private from WAF respective traffic goes that may be inbound traffic, Out bound traffic , load balancer. In AWS , Micro soft Azure & Google cloud plat form we will do clustering part for balancing of the load or balancing of the traffic

Clustering is more than high Availability (High Availability will refer only two identical devices or two similar devices but on the other hand)

Clustering hear is similar type of devices will be there more than two or multi that is called clustering ex; More than two servers or two Data bases or more than any two devices If we are using that is called clustering mechanism

When traffic is coming from 5000 sessions per second, those 5000 sessions each and every server capacity is only may be 1000, so in that scenario those 5000 sessions will be distributed to each and every server that example nothing but 1000, That will do load balancing of the traffic

Those Load balancer will go to the NGFW so it will do on the processing of the traffic respective whatever is coming, it will AV scanning , it will do AV Malware scanning it will do, IDS/IPS scanning it will do and so on , each and every packet entering into the organization level, it will open the packet it will do the D packet inspection and also it will do Scanning of the IP Address, is there any spoofing of the IP Packet is Available or Malware scanning mechanism everything it will do

ex; NGFW it is not mandatory it use NGFW even Amazon itself is providing Amazon firewall and also Amazon itself they have net work access control list & security group

From NGFW it will go to the Proxy, so proxy will validate what is incoming traffic is coming and outbound traffic is going on, is there any malicious website user is accessing

From proxy back end web server & Data base services, so finally on top of web server & on top of the Application server we can deploy respective our Applications

So these the way how network Architecture refer from on premise Data centre net work Architecture diagram, only one thing is different that is nothing but WAF. In the data centre or on premise

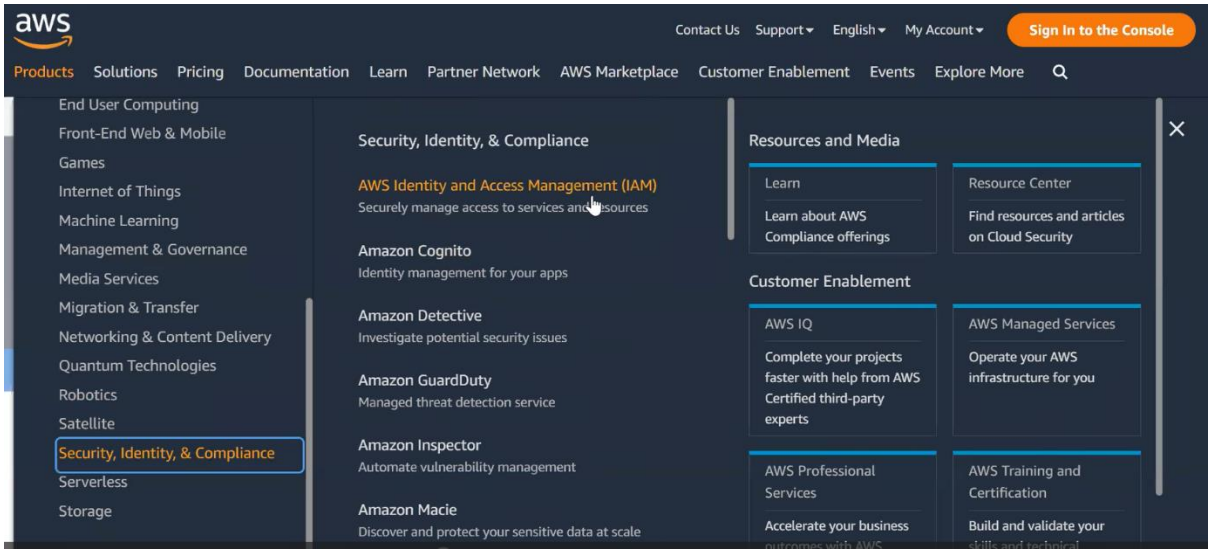
network Architecture Diagram the 1st entry point is Anti DOS , & Anti DDOS, then it will go to fire wall from fire wall it will go WAF

From other point if it cloud the 1st enter point is WAF from WAF it will go to the Firewall that is the only different but remaining everything same as it is

Under whatever is there under those LB – Load Balancer , NGFW , Proxy , Web server , DB Server. All those deploy on Top of the EC2 – Elasticity cloud computing it is like server , it is like virtual machine

Once we are clicking in Amazon web security we will be getting the website , we have to click on it https://aws.amazon.com/security/

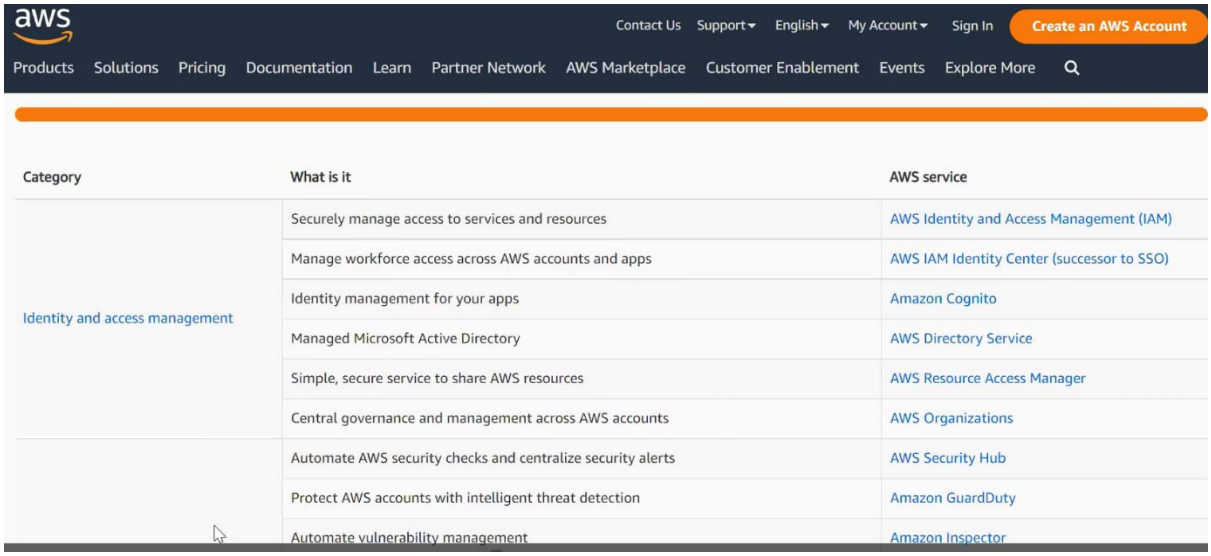
Once clicking to this website as we have to click on product as we see an option like security , identity & Compliance as we see many services which is providing by the Amazon



As we see in the picture AWS Identity and Access Management (IAM) and so on

EX ; why we use this IAM just to segregate the duties like Role based Access control, so even for accessing Amazon also different people will access our internal employees ex like devops team , techup teams , secup teams and also cloud computing team and so on, if we want to segregate all these of people, we have to implement IAM,

So we have to create a IAM access role so If the user is belongs to Devops team then we have to create as Devops role & so on this applicable to on premise as well. If we are providing IAM roles based Access control, who has done what , who logged into Amazon.com , who logged into Respective Application actually for traceability wise if any compromise is happen, so easily we can trace it so that's why it IAM Is very important so that is one of the service



Category	What is it	AWS service
Identity and access management	Securely manage access to services and resources	AWS Identity and Access Management (IAM)
	Manage workforce access across AWS accounts and apps	AWS IAM Identity Center (successor to SSO)
	Identity management for your apps	Amazon Cognito
	Managed Microsoft Active Directory	AWS Directory Service
	Simple, secure service to share AWS resources	AWS Resource Access Manager
	Central governance and management across AWS accounts	AWS Organizations
	Automate AWS security checks and centralize security alerts	AWS Security Hub
	Protect AWS accounts with intelligent threat detection	Amazon GuardDuty
	Automate vulnerability management	Amazon Inspector

These are the options will populated when we click security , identity & Compliance options

AWS IAM identity centre (Successor to SSO) – It over all centre wise and It is single sign on similar to OKTHA Single sign on ex; We are part of Wipro company, it has hosted 10 Application in cloud in the Amazon if we are enabling this AWS, IAM single sign on there is no need to go and every enter the user name and password, once time entering user name and password Automatically whatever 10 Applications is hosted all those 10 Applications we can access directly but every time we OTP Additionally security control nothing but multi factor Authentication

Amazon cognito – It means bring your own identity, so even Amazon is providing for identity purpose, Amazon is created its own Identity who has done what it is similar to IAM and But identity is depending on Third party, third party is nothing but in between Amazon and respective Applications one more person will take roles and responsibility point of view that is called Cognito it is nothing but bring your own identity so that is about Cognito

AWS Directory service – Basically its not a security service even though its related to IAM Service nothing but its like a AD, here will create couple of services, Group , AD Groups and so on

AWS Resource Access Manager – It will provide the whatever services that we are accessing,

AWS Organization – If we want to check all the Alerts centralized one from single console from there we will use the AWS Organization

AWS Security Hub – It is dedicatedly Applicable to Alerts, whatever in the cloud of the Amazon we deployed the Applications & Data Bases & Servers & storage, Back and everything, whatever Alerts are coming if we enabling the security Hub feature all those Alerts will come

Amazon Guard Duty (Interview Question) – It is equal vent to SIEM Tool and it is SIEM Tool in Amazon, Guard duty it is centralized log collection , Log processing , Log Managing , Log Alerting tool it is like a SIEM Tool. Guard Duty doesn't have as much capability as compare to Azure sentinel

Amazon Inspector – It nothing Vulnerability Management & Vulnerability Assessment Tool, if we want to run the scan whatever Virtual machines are Elastic cloud computing relating to Instance we are creating in that situation we have to enable Amazon Inspector

Ex; If we don't like Amazon Inspector as a Vulnerability Assessment tool in that we can go for third party vendor that is called BOYL

AWS Config – It is like Zincs & Auto chef these are the configuration management Tools are there third party same thing is Applicable to AWS Config

Amazon Cloud watch – Instead of using Guard duty if we want to integrate the logs to the SIEM Tool of the IBM Qradr or splunk and so on we have to use cloud connector method so in that situation 1st we have to config the cloud watch because cloud watch will monitor system configuration as well as control plane & Data plane related log

Who ever is trying to do config changes in the Amazon , system related. Then one of the person wants to install virtual machine like EC2 Instance in the Amazon its like configuration change. So that time this cloud watch it will log back end, so that is Amazon cloud watch

AWS Cloud trail – It is related to security Audit ,when ever any team have the access to Amazon.com IAM related Logs, security related Logs , Login failure as well as log in success that one will provided by cloud trail. These logs only we will store in the S3 Bucket from the S3 bucket using clod connector method we will integrated to on premise or splunk or IBM Q Radar and any other third part SIEM Tool and so on why because Guard duty doesn't have that much Capability of SIEM Related SOC

AWS IOT Device defender – It is a new service actually, when ever any tera bite Data. If we want to store in the Amazon, in that situation if those devices or data has any security related flaws, Bucks are there that time we use Device defender. It is dedicatedly applicable IOT Devices

AWS Network Firewall – When we don't have to purchase any Firewall in that situation we have to enable this firewall what Amazon is providing and also what Azure is providing

What is DDOS Protection in AWS or AWS Shield (Interview Question) -

DDOS Protection can also be called as Shield we no need to depend on the Third party tools like Anti Dos & Anti DDOS ex; Akamai, Barracuda , Imperva all these different types of tools we have and we no need to use those Tools, so directly we can enable AWS shield

Amazon Route S3 Resolver DNS Firewall – Whatever private IP We are configuring this Pvt IP should not expose to the public, in that situation this Pvt IP we have to map to the public IP that is called Network Address Translation, so that public IP only we have to expose to the Public other wise so these Attackers will try to do compromise different types of networks, OWASTOP 10 Attacks. For Routing as well as Resolving Those DNS we will use AWS DNS Resolution

AWS Web Application Firewall (WAF) – Amazon have its own WAF related to OWASTOP 10 Attacks against, if we are enabling it will block as well as it will prevent, if we don't the AWS WAF then we can choose the third party

AWS Firewall Manager – Consider our organization is distributed one our head quarters is in Hyderabad branch offices in Delhi , pune and so on each and every where Amazon deployments we will deploy the two firewalls, if we want to manage all those firewalls we will use AWS Firewall Manager

Amazon Mice – It will protect whatever sensitive data it is going like data at a rest or Data at a transit level

AWS Key management Service (AWS KMS) – whatever key are storing especially it is applicable to at data at transit level, whatever applications we are hosting at cloud deployment, if we are enabling this KMS, As we know the Mutual TLS Authentication mechanism in between client as well as respective back end server it will exchange the public key as well Pvt key, if we want store all these key as well as exchange the keys we use the AWS KMS, these keys we have to rotate as per by default AWS they are saying 365 days we can change those keys as per European council its better to change in 90 days

AWS Cloud HSM – It's a hard ware security module if we want to store passwords or secret keys then we will use HSM like a key word

AWS Security Manager – instead of going Symantec very sign or go daddy and so on third party tools, AWS Have its own to generating the certificates

AWS private certificate Authority – Instead of going for very sign these related to managing of certificate, when the certificate is going get expire, so when the

certificate we have to renew and when we have to purchase and so on but certificate Authority own but they no need to depend on third party

AWS Secrete Manager – It will maintain the All secrete and password

Amazon Detective – It will do the incident investigation process, whatever potential threats as well Alerts we are receiving if we are enabling the Amazon Detective, it will identify as well as it will throw the Alerts, Guard duty and Amazon Detective is almost similar

Guard duty will provide the entire single console it can provide the entire Alert notifications related to Logs

Amazon Detective it will provide the investigation wise what all the Alerts we have to fix , what all the security issues we have to fix and so on

AWS Elastic Disaster Recovery – whatever Amazon account we are creating ex; In India it Is in Mumbai location, if we want to maintain the disaster recovery site, for that we have to create one more account so directly we can create here itself, we have to enable disaster recovery site as well

AWS Artefact – It like compliance reports kind of ISO 20071, GDPR , HIPPA Related compliance if are enabling this Artefact then we will come to know as well as we can Generate those reports and even Hardening bench mark also it will support

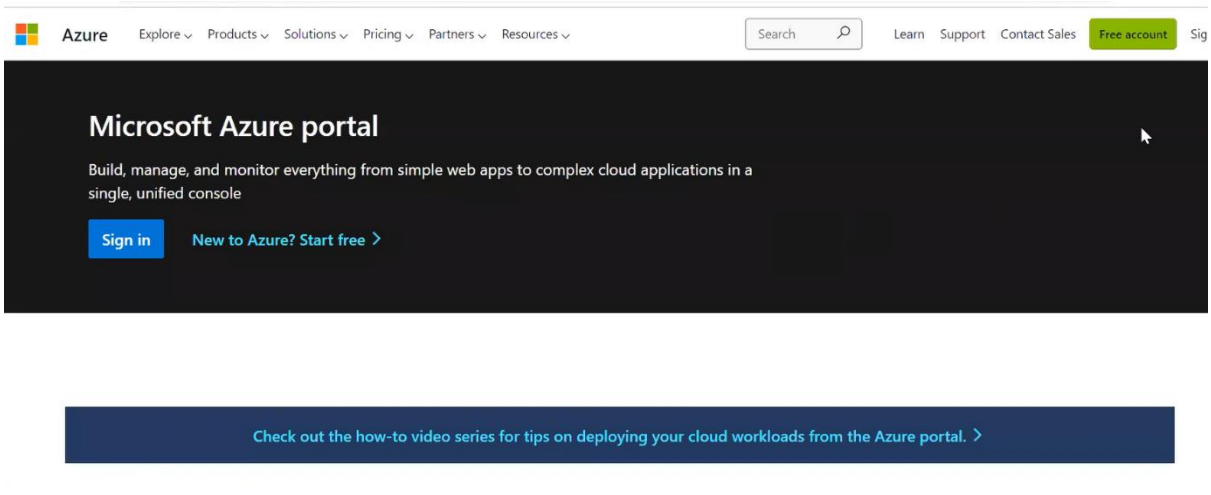
Audit Manager – It will Audit continuously what ever images we are using in the Amazon so additionally it can save the how many Audits are passed and how many are failed for suppose in case in the Linux container or Linux Docker or Linux Virtual machine, if we are using the Hardening bench mark related to centre for CS Bench mark out of 225 compliance may be 120 are passed reaming 105 are failed in that situation if we are enabling this Audit manager Automatically it will say 120 are passed remaining 105 are failed so that one also will give Audit fail. Here no need to run the Nessus tool or Quails tool and so on. If we are running this feature Automatically it will say How many Audits are failed and how many Audits are failed

What you know about cloud (Interview Question) ?

I'm working as a security Analyst, Even we are integrating the Cloud logs as well 1st in Amazon account we will go and we will create the cloud watch and we will create the cloud trail and those logs will store in the S3 Buckets using the cloud connector Method or API Token management method will integrate cloud logs related to Amazon to SIEM Tool, so that I much know. Even im aware of Guard duty as well

Similar we have the micro soft Azure Login

https://azure.microsoft.com/en-us/get-started/azure-portal



This interface we can see over here, as we have the option of free Account under this

Employee KPI , Roles & Responsibilities Under Shift Hand over

KPI – Key performance indicator

Under KPI we have 2 type

- Performance Appraisal KPI
- Operational KPI
- SOC KPI

Under operational whatever work we are doing entire project related KPIs

SOC KPI – SOC operations should be stabilize meaning here what ever SIEM Tool we are using the cyber security for 24/7 , we should check it its matured SOC or not

In general for SOC Stabilize approx. it will min 6 weeks time period from 36 days to 90 days

Once we are deploying the SIEM Tool or Any other Tool it will not stabilize with in 1 or 2 days, so it will take Approximate 6 weeks to 90 days Min that is called stabilization

Under Mature SOC we have different things

- Fine tunning (when the All the log sources logs are reflecting to SIEM Tool or not in case if logs are not reflecting how we can trouble shoot or how we can debug so that is called Fine Tunning)

- Reducing the false positive

To reduce the false positive we can use the Advance features like Automation , SOAR , UEBA , Proactive threat hunting. All these parameters

SLA (Service Level Agreements) – It is nothing but in between our service based company to respective client or we can say it is Agreement between two parties, SLA Is always Time based one of the KPI is one the SLA it is time based, so when ever any incident is coming critical or High or Medium or Low or Informational, those severity of the incidents those are receiving,

In that situation what is the time to do investigation that may be general incident investigation or that may forensic investigation so its completely time based

Cross Functional Training – If we are part of L1 Team, Always we will not do L1 Operations work may be 6 months of time period we are working on L1, in that situation we have to give training, so that training related to L2 that may be related L3 and so on, so these are cross functional training we have to do, it is not only applicable to Cyber security this might be Applicable to Machine learning, Data science and so on for every team they will do cross functional training

Tools – we have to check whether All the Tools are in the Right place or not for monitoring purpose when ever any incidents are coming all these tools are there in the place

Skill full security Analysis – we should check whether skill full people are there are not even we have to verify this which is also part of KPI

Personal Performance Management –

When ever we are expecting Hike in that moment this personal performance management will Applicable, these are the following steps are based on

- Productivity
- Quality
- Quantity
- Continuous improvement
- Training and development
- Customer satisfaction

Rating starts from 5 to 1 as we can consider Grade wise like A , B , C , D , E which is based on the employee performance

Shift Hand over –

Under in my team we are 15

In that L1 is 8 , L2 is 4 , L3 is 2 & SOC Manager

Shift hand over		15	L1		8	
			L2		4	
			L3		2	
			soc MANAGER			
				24*7		
		Shift 1	5			5 to 2
		Shift 2	5			1 to 10
		Shift 3	5			10 to 5

As we see different shifts wise like

Shift 1 5 Members 5 to 2

Shift 2 5 Members 1 to 10

Shift 3 5 Members 10 to 5

Under a shift it might L1,L2,L3 any of 5 in it as we see in the picture timings 5 to 2 and 1 to 10 and 10 to 5 those are time

And also we can notice 01 hour time gap in that we have to buffer nothing but hand over to the next team

In that 01 hour time period what ever the previous shift people who have done the work and they worked on any incidents will be handing over to the next team

Ex; May be they have received the 50 incidents out of 50 they were closed 40, in that 5 is opened didn't close and they are on hold, may be couple of things are escalated things are also there, whatever shift 01 work has done will hand over to the Shift 2 people

Now shift 02 team should take care the particular incidents that is called Shift Hand over whatever pending , WIP , Escalated one are there those things will be handled by next team

Incident Tracker

Incident tracker	S.no	Date and time	Incident number	Incident arrived	Inciodent closed	SLA time	Incident type	Status
	1	03/11/2022	inc00001234	5:00 AM	9:00 AM	4	Ransomeware a	Closed

Incident Tracker means either we use JIRA Ticketing tool or Service now ticketing Tool and so on, here we can export the reports for one year, the tickets that we are working on, these tickets incidents we are working on, it will helpful for the performance Appraisal and also it required for Auditing purpose also

When external Audit ask us what happened in the previous and also in a similar way what are the incidents that you worked on

Incident tracker its better if we use excel sheet its an manual process as we see in the above picture

At the end of the day whatever shift is going to finish we can fill the above one

Do you know Automation? What type of Automation you have done? Which programming language you know. (Interview Question)

Yes I have done something with help of service now developer because as we using service now ticketing Tool for Automation I have used python & power shell ex; whenever any incidents are coming to the SIEM Tool or may be Firewall or proxy or may be EDR Tool for filling of the one templet and to create a ticket it will take max 5 mints, if I'm doing 10 tickets per day approximately I may loose 50 mints, in such a way we have members of team is there 10 * 50 mints per day equal vent to 500 mints. That means we are loosing the time Approximate 8 hours 20 mints, that much of time we are loosing resources point of view

If I use like python or power shell any other programming language which with the help of windows development team, so what I have done from my side, using these language I prepared one of the templet and using python, when ever any incident alert is coming Automatically, that Alert integrated to the SIEM Tool and that Alert will come to service now ticketing Tool, this Automation I have done

SOAR Security orchestration Automated response – It is one the new technology in the Cyber security, so when ever any Attacks are coming using these python or power shell kind of programming languages, we have done similar type of log sources logs integrated to SOAR Tool or SOAR capability, instead of going to firewall blocking IP Address or Domain name or URL link ,

- Hash value blocking in EDR Tool
- Domain is blocking DNS server or firewall or proxy
- URL link blocking in firewall or proxy

So raising a separate ticket will take the longer time but if use some of python & power shell related to Automation, we can take the Automated response in the SOAR Tool itself that is one of the Automation I have done

Similar type of log sources logs to the SOAR Tool there itself we can block the IP Address, Domain name , URL Links , Mac Address , Hash value and so on, for this I'm one of the team member for the project implementation or Automation implementation