**********COURSE ERA CYBER SECURITY NOTES**********

https://www.geeksforgeeks.org/difference-between-virus-worm-and-trojan-horse/

Ingres Filtering:

Ingress filtering is a method used by enterprises and internet service providers (ISPs) to prevent suspicious traffic from entering a network. When configured on an edge device such as a router or firewall,
ingress filtering examines all inbound packets and then permits or denies entry to the network based on information in the packet header.
It is a form of packet filtering.
Ingress traffic filtering is one of the first lines of defense in a network security strategy.
It is intended to prevent cyberattacks,
particularly denial of service (DoS) attacks that use IP address spoofing

Egres Filtering:

Egress filtering controls the traffic that is attempting to leave the network. Before an outbound connection is allowed, it has to pass the filter's rules (i.e. policies).
These rules are set by the administrator.
Egres filtering is used to disrupt malware, block unwanted services, stop contributing to attacks

WhiteList: the list of authorized

In access management we should see groups, physical location,timeframe,transaction type

In Incident Management: Events, incident, response team, investigation team

IN Incident Response: E-Discovery,Automated systems,BCP(business continuity point) & disaster recovery, Post-incident

Incident Response Process: Prepare, Respond, Follow up

Stateless Firewalls: Also called packet filter, filters based on layer 3 and 4 information(IP and port),lack of
state makes it less secure

Stateful Firewalls: Have state tables which allow firewall to compare current packets with previous packets

could be slower than a packet filter but more secure. application firewalls make decisions based on layer 7 information.

COURSE ERA CYBER SECURITY COURSE -02

# COURSE NAME: Cybersecurity Roles, Processes & Operating System Security

SOC-security operation center
BPM-Business operation management
ITIL - IT infrastructure library
SLA- service level agreement
ISP-Information Security Policy

Kernel mode, everything that runs in Kernel mode contains a shared single virtual address. So that kernel mode drivers are not Isolated from other drivers and from the operating system itself. So if a Kernel mode driver accidentally writes to the wrong virtual address, or to something else within the operating system, that data within the operating system could be compromised. So if a kernel mode driver crashes, the entire operating system will crash.

The /sbin, it contains executable binaries as well, but they're more related to system maintenance tasks, like iptables, like the reboot command, the fdisk or the ifconfig, for example. The /etc, it's where most of the time you'll find configuration files for all the programs installed. If we have a Linux server and we install Apache on that server, for the configuration of that specific service, you'll go to /etc/apache and you will find all the configuration files on that directory for its specific applications. The /var, it's in the specific partition designed to hold files that grow or change constantly, it's referred to as variable files.

COURSE-03 COMPLIANCE FRAMEWORKS AND SYSTEM ADMINISTRATION

A security event is a system or network detected by a security device or an application. So this can be any normal activity from entering a password. That's a security event. It can be a firewall rule check. That's a security event. It's not the same as an attack. Attack, of course, is the subset of the events. That's when you actually have some entity, or tool, or person attempting to do something malicious or untoward with your system. It can be trying to collect data, corrupt your system, create a denial-of-service, destroy your system, anything like that. Any attempt to do that is an attack. An incident then is when IBM and the world at large would consider it something worthy of deeper investigation. So we think that possibly something bad will actually happen. So we had the attack, which was the attempt, and we had the incident which means, we think maybe something actually had happened, and we need to go and figure out what happened, and what we're going to do about it.

ISO-International Organization for standards

27001 is the most common one. It is an information security management standard. It focuses on requirements for establishing and implementing, maintaining and improving your security management system. It's risk-based. So it's looking at the risk and the maturity level of your organization.

We'll look at 270018, which is focused on privacy, and 270017, which is focused on Cloud security,

SOC-System organization and control

So many organizations who know compliance actually prefer SOC 2 over ISO. ISO is a point in time testing whereas SOC 2 is continuously monitored testing over a period of time. Again, some organizations, or some clients, or some industries will accept SOC 2 in lieu of the right to audit.

SOC 2 is focused on fiscal, logical security and in specific, you know, do what you say you'll do, whereas ISO 1 is a little bit more focused on risk. ISO is internationally recognized.

SOC1 is generally used for systems working/storing financial data.It is also used to test the design effectiveness of the controls and is generally used for testing on new products.

CIS- Center for internet security

In CIS controls there are 3 types of implementation groups.
Group 1 - For an organization with limited number of resources and cybersecurity expertise to implement sub controls
Group 2- For an organization with moderate resources and cybersecurity expertise to implement sub controls

Group 3 - For a mature organization with significant resources and cybersecurity experience to allocate to sub controls

Compliance process - Establish scope, readiness assessment, gap remediation, testing/auditing, management reporting

Active directory or AD, is really a system that stores information about things on the network and makes that information easy for administrators and users to find. So it will control things like your network folders, network printers, anything that a user may need to be able to get to to do their job can be controlled by AD. AD stores the information about those resources as well permissions, and controls the permissions as to what you can get to.

For Active Directory, there really are two types of administrative responsibility: Service Administrators and then Data Administrators. So Services Administrators are managing things in the environment such as what I have access to, what I can do on my device or with the resources on the network, and then there are what we call Data Administrators who are actually managing access to the data in the environment. So things like customer records or employee records or any sensitive information that the average end user doesn't need access to.

There are two types of groups with an Active Directory by which we manage those. So there's distribution groups, those are used to create email distribution lists, and then security groups, those are used to assign permissions to shared resources.

There are three scopes that are defined by Active Directory: Universal, Global, and Domain Local.

Kerberos authentication is an authentication protocol that it's used to verify the identity of a user or a host and Windows uses it mostly around AD. So when someone logs into a system that is connected via AD most AD systems will leverage Kerberos as the authentication protocol.

Samba is an open source or free software suite that provides seamless file and print services. It uses TCP/IP protocol that is installed on the host server. If you configure this software correctly, it allows you to interact with the Microsoft Windows client or server as if it is a Windows file on a print server. So it allows for establishing communication between Linux and your server.

COURSE-04 NETWORK SECURITY AND DATABASE VULNERABILITIES

Stateless means that each packet is inspected one at a time with no knowledge of previous packets. No session table is maintained, so each packet is inspected independently of all other packets.

Stateless inspection doesn't know anything about session.There is no database with details of the packets that have already been inspected.

Stateless inspections are faster than stateful inspections. A stateless inspection gives us a degree of control over what's going on and what is going to be allowed within our network. Stateless inspections are great for troubleshooting purposes when we want to classify packets. Also, they are helpful when we have a router that supports virtualization. We can tell if we have a flow of traffic coming from a specific source trying to go to a specific destination. Then we can send it to a specific virtual instance within our router. Also, we can perform some QRS or quality of service switches which will prioritize traffic.

The IPS is going to be directly in-line in the middle of the stream of network traffic. The IPS will be tapping our communication, while the IDS is outside the direct line of communication.

Network Address Translation or NAT

The preamble is the first eight bytes of an ethernet frame. The first seven bytes are just a series of alternating ones and zeros. This is used as a buffer to separate adjacent ethernet frames, and it helps the network regulate the speed at which the data is sent. The last byte of the preamble is called the Start Frame Delimiter or SFD. The SFD lets the receiving computer know that the preamble is over and what follows is the actual frame contents.

A more advanced type of network device is a bridge. A bridge is similar to a hub, but a bridge does not send the signal to all connected ports, but only to the port the destination computer is attached to. By maintaining a MAC table, the bridge knows which machine is attached to each port. A MAC table is not the same thing as an ARP table. The bridge looks at the layer to the destination MAC address of the incoming frame and matches that to the connected port as assigned in the back table. So a bridge is a device that can be said to add some intelligence to a local area network.

computers attached to a bridge can either receive or transmit at one time but not both.

switches use full-duplex communication so they can transmit and receive data at the same time on each port. Each port is dedicated to a single device, so bandwidth is no longer shared.

Class A goes from 0.0.0.0 to 127.255.255.255. This is for special use and unicast. The default subnet mask is 255.0.0.0, which we will explore more later on. Class B, class C,

class D, and class E use these address ranges. Class D is reserved for multicast groups. So you will see protocols like that bios using addresses and this range to communicate. Finally class E, which is reserved for research development and future uses. So this is classful addressing. In class A networks, the first octet is used for the network portion and the last three octets are used for the host portion. In class B networks, the first two octets were dedicated to the network and the last two to the host. Class C networks have the first three octets dedicated to the network, and only the last octet is dedicated to the host.

The Internet standards committee recommends the TTL be set at 64 for most normal traffic. Note that TTL is measured in hops for the IP protocol, but some protocols like DNS, it's measured in seconds.

TFTP - trivial file transfer protocol uses port 69 and uses UDP

SMTP - port 25,  DNS - port 53
DNS uses UDP for its name queries, but it can use TCP for less common tasks.

SNMP, the Simple Network Management Protocol, uses ports 161 and 162. It is uncommon, but SNMP can also use TCP. SNMP is used to monitor and manage network devices. DHCP, the Dynamic Host Configuration Protocol, uses Port 67. DHCP automatically assigns and manages a pool of IP addresses to the systems that are subscribed to it.

VoIP, or Voice over IP, uses port 5,060. It can also be implemented using TCP

IPTV, or Internet Protocol Television, uses both UDP and TCP as well as ports 80, 5,004 and 12,000.
Port 22 is used for SSH.

DNS, the domain name service that translates domain names into IP addresses, and DHCP, the dynamic host configuration protocol that automatically configures and manages the IP addresses on endpoints from a pool of available IP addresses.

The DHCP handshake will consist of four packets that go between the requesting system and the DHCP server. They are known as discover, offer, request, and acknowledgement messages

Syslog is a standard protocol for messaging and logging.

Syslog is three layers, content, application, and transport. Content is where the actual syslog messages are contained. Application allows the syslog message to be routed, analyzed and stored, and transport handles sending the syslog message across the network

Port mirroring very simply is when a switch is configured to make a copy of all the traffic traversing one or more ports on that switch, and send the copied packets out to a single destination port.

Next Generation firewalls have functionalities like IPS,IDS, packet inspection etc

The device used to separate the network portion of an IP address from the host portion is called subnet mask.

For added security firewall is placed between database and hardened repository

So only use OS commands if absolutely necessary, if it's dictated by your business logic. Try to run your code with the least possible privilege. Do not run OS commands with shell interpreters. Try to run them directly. Use explicit paths when running applications and shared libraries. Try to use safe library functionality, there are usually multiple variants or some safer than the others. Try not to let user input reach the point where the OS command is executed unchanged. It's better to try and use generated IDs and try to sanitize all user input with whitelists.

to prevent SQL injections, including, use prepared statements, sanitize user input, do not expose native database errors to the user, limit database user permissions, use stored procedures, use ORM libraries.

XPath expressions operate on XML, on XML trees.

COURSE-05 PENETRATION TESTING, INCIDENT RESPONSE AND FORENSICS

penetration tests can occur across applications, networks, and systems like mobile devices or different operating systems. While each of these different approaches may vary, the methodology in which we use remains largely the same.

1) Planning
2) Discovery/reconnaissance
3) Attack
4) Report

IBM Security Guardium Vulnerability Assessment scans data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities and suggest remedial actions. The solution identifies exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Full reports are provided as well as suggestions to address all vulnerabilities. Guardium Vulnerability Assessment detects behavioral vulnerabilities such as account sharing, excessive administrative logins and unusual after-hours activity. It identifies threats and security gaps in databases that could be exploited by hackers.

hash injection is basically getting the password file from their server and try to decode it.

https://securitytrails.com/blog/google-hacking-techniques

Attack Phase- 1) Discovery phase
2) Gaining access
3) escalating privileges
4) system browsing
5) Install additional tools

Misconfigurations are just vulnerabilities that are introduced through security settings, particularly insecure default settings that are usually easily exploitable. The next category are kernel flaws. So the kernel code is the core of an operating system, and it enforces the overall security model for the system. So any security flaw in the kernel will put the entire system in danger. Next, we have insufficient input validation. Many applications fail to fully validate the input they receive from users. An example is a web application that embeds a value from a user in a database query. If the user enters, let's say an SQL command instead of, or in addition to the requested value, the web application doesn't filter the SQL commands. The query may be run with malicious changes that the user requested causing what is known as an SQL injection attack.

A symbolic link, or symlink, is a file that points to another file. Operating systems include programs that can change the permissions granted to a file. If these programs run with privileged permissions, a user could strategically create symlinks to trick these programs into modifying or listing critical system files. Next up is file descriptor attacks. So these are, next up is file descriptor attacks. File descriptors are numbers used by the system to keep track of files in lieu of file names. Specific types of file descriptors have implied uses. So when a privileged program assigns an inappropriate file descriptor, it exposes that file to compromise. Next up is race conditions. Race conditions can occur during the time a program or process has entered into a privileged mode. A user can time an attack to take advantage of the elevated privileges while the program our process is still in that privileged mode. Buffer overflows can occur when programs do not adequately check input for appropriate length. When that occurs, arbitrary code can be introduced into the system, and executed with the privileges, often at the administrative level of the running program. The last category some vulnerabilities can fall under is the incorrect file and directory permissions. File and directory permissions control the access assigned to users and processes. Poor permissions could allow many types of attacks, including the reading or writing of password files or additions to the list of trusted remote hosts.

Ptes has broken down the summary into six major categories; background, overall posture, risk ranking, general findings, recommendations, and the roadmap for remediation.

Incident Response phases are preparation, detection and analysis, containment, eradication, and recovery, and the post-incident activity.

. An event can be something as benign and unremarkable as typing on a keyboard or receiving an email.

An incident is an event that negatively affects theIT systems, business and repudiation.

An event can lead into an incident but the reverse is not true.

Types of incident response team are central,distributed,coordination

The first thing we need to break down in detection is really the precursors and the indicators
A precursor is a sign that an incident may occur in the future.
An indicator is a sign that an event has occurred or is happening now.
In incident response all the data corresponding to the incident should be logged with the measures used for future use.also called as chain of custody(documentation)

Digital Forensics is considered to be the application of science to the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for said data.

forensics can actually be applied to many areas, some of those include operational troubleshooting, log monitoring, and data recovery.

the four steps of the forensic process into collection, examination, analysis and reporting.

Volatile data is the data only available at that particular moment

In the forensic report there are four major categories, the overview case summary, the forensic acquisition and examination preparation, the findings and report also known as your forensic analysis, and then what your conclusion is.

Most data files are smaller than the number of blocks allocated to their storage by the file system; the unused space is known as slack space.

A logical backup copies the directories and files of a logical volume.It does not capture other data that may be present on the media such as deleted files or residual data stored in slack space.

Imaging generates a bit-for-bit copy of the original media including free space and slack space.Bit stream images take more storage space and take more time than a logical backup.

One of the benefits of a logical backup is that it can be used on a live system if using the standard backup software. But imaging can't be done on a live system since the data is constantly changing.

https://www.ufsexplorer.com/articles/chances-for-data-recovery.php

In LInux The system 32 config file, this contains a system configuration directory that holds separate configuration files for each application, the var log is a directory that contains application and security logs and they're kept for about four to five week. The home user folder, this directory holds all the user data and configuration information, and last the password directory, which has the user account information in it.

The application  settings may be stored in the following three ways: configuration files, runtime options, or added to the source code.

the external authentication would have more information than the host. Proprietary authentication is most commonly seen in usernames and passwords that are application not OS-specific. Pass-through authentication is where the application uses whatever the OS authentication is.

The most common types of logs are event, audit, error, installation, and debugging logs. Event logs record actions that were performed, the date and time each action occurred, and the result of each action. Audit logs or security logs specifically track audited activities such as authentication attempts. Error logs track errors applications have with timestamps. Installation logs track when an application is installed or updated. The debugging logs are usually only meaningful to the software developer.

MAC in forensics means Modification, Access and Creation times

Scripting languages Javascript, perl, Bash, JCL(job scripting language)

Most software companies update your software by overriding the hex numbers in the files.

COURSE-06  CYBER THREAT INTELLIGENCE

https://www.securitylearningacademy.com/course/view.php?id=4527

Complete Labs in the above link

Cyber threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace.

Collect(integrate data) -> Process (Put data in the context) -> Analyze(find insight and actions) -> share(inform decisions)

Collect involves multiple sources like internal, external, technical , human,raw, packaged

Process involves normalize, correlate, confirm, enrich

Analyze involves investigate, contain, remediate, prioritize

Share involves personalize on who for what purpose,what how often, what format medium

There are 4 intelligence areas tactical, technical, operational, strategic

Tactical is focused on performing malware analysis and enrichment. Operational is focused on understanding adversarial capabilities, infrastructure and TTP's and then leveraging that understanding to conduct more targeted and prioritize security operations. Finally Strategic is focused on understanding high level trends.

In Tactical stakeholders are SOC analyst, SIEM, Firewall, endpoints,IDS/IPS

In Operational stakeholders are threat hunter, SOC analyst, vulnerability management, incident response, insider threat

In strategic stakeholders are CISO,CIO, CTO, executive board

Some of the important threat intelligence sources are Bleeping Computer, Krebs on security, DARK Reading, Trend Micro, Infosecurity Magazine, X-Force Exchange

A threat intelligence platform is defined as an emerging technology discipline that helps organizations aggregate, correlate, and analyze threat data from multiple sources in real-time to support defensive actions.

Collect, a threat intelligence platform collects and aggregates multiple data formats for multiple sources, including CSV sticks, XML, Email and various other feeds.

Full-featured threat intelligence platforms enable the flow of information collected and analyzed from feeds and disseminate and integrate the clean data to other

network tools including SIMs, internal ticketing systems, firewalls, intrusion detection systems and more.
One threat intelligence platform is from Recorded Future. Some of the features of that platform include centralizing and contextualizing all sources of threat data.Another threat intelligence platform is from FireEye. They have several subscriptions that are available to you and your organization. Choose the level and depth of intelligence, integration, and enablement your security program needs. Fusion Intelligence is a comprehensive package that includes operational, cyber crime, and cyber espionage intelligence offerings, which you can use to understand a full attack life-cycle to prepare your defense against the TTPs of the threat actors of interest.

Fusion Intelligence is a comprehensive package that includes operational, cyber crime, and cyber espionage intelligence offerings

Strategic Intelligence, learn how to align your security resources against the most likely threats and actors and manage your business and technical risks around major business decisions and security resource planning. Operational Intelligence, allows you to prioritize and add context to your alerts in order to respond more effectively and efficiently and improves defenses with high fidelity machine readable indicators of compromise with associated contextual information. Vulnerability Intelligence provides the vulnerabilities that pose the most significant threats to the organization and understands the options for patching or otherwise mitigating these vulnerabilities. Cyber Physical Intelligence, includes actionable insights into cyber threats and risks facing industrial environments and the operational technology

IBM X-Force Exchange. Is a cloud-based threat intelligence sharing platform enabling users to rapidly research the latest security threats, aggregate actionable intelligence, and collaborate with peers.

TruSTAR is an intelligent management platform that helps you operationalize data across tools and teams, helping you prioritize investigations and accelerate incident response.

The basis for some threat intelligence is heavily rooted in one of three basic models. Lockheed Martin's cyber kill chain, MITRE's ATTACK knowledge-base, and the Diamond Model of Intrusion Analysis.

One popular approach is the Diamond Model of Intrusion Analysis. This model emphasizes the relationships and characteristics of four basic components: the adversary, capabilities, infrastructure, and victims. The main axiom of this model states, “For every intrusion event, there exists an

adversary taking a step toward an intended goal by using a capability over infrastructure against a victim to produce a result." This means that an intrusion event is defined as how the attacker demonstrates and uses certain capabilities and techniques over infrastructure against a target.

the Diamond Model of Intrusion Analysis is sufficient if there are two players, the victim and the adversary

Best practices for Intelligent Detection

1) Predict and prioritize security weakness
   Gather threat intelligence information
   Manage vulnerabilities and risks
   Augment vulnerability scan data with context for optimized prioritization
   Manage device configurations(IPS/IDS/firewall,switch,router)

2) Detect deviations to identify malicious activity
   Establish baseline behaviors
   Monitor and investigate anomalies
   Monitor network flows

3) React in real time to exploits
   Correlate logs, events, network flows, identities, assets, vulnerabilities and configurations
   Use automated and cognitive stuff to make data actionable by existing staff

The goal of security intelligence is to provide actionable and comprehensive insights that reduces risk and operational effort for any organization regardless of its size

Three pillars of effective threat detection are see everything, automate intelligence, become pro active

In general organization are concerned with privileged user and credentials abuse

Endpoint alerts and network access devices are the top sources of incident information, providing alerts and investigation support respectively

In security intelligence there are 2 phases pre-exploit and post- exploit

Pre- exploit: Detect deviations from the norm that indicate early warnings of APTs,Prioritize vulnerabilities to optimize remediation processes and close critical exposures

Post-exploit: Perform forensic investigation, Gather full situational awareness through advanced security analytics
Top challenges of many organizations are data growth, new privacy regulations, operational complexity and cybersecurity skills shortage

Five epic fails in Data Security are:

1) Failure to move beyond compliance
2) Failure to recognize the need for centralized data security
3) Failure to define who owns responsibility for the data itself
4) Failure to address known vulnerabilities
5) Failure to prioritize and leverage active data monitoring

The top 12 data protection capabilities are data discovery, data classification, vulnerability assessment, data risk analysis, data and file activity monitoring, real-time alerting, blocking, masking, and quarantining, active analytics, encryption, tokenization, key management, and automated compliance reporting.

Guardium uses host-based probes by a distributed agent called the S-TAP. This provides lightweight cross platform support.

Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance or deviations from an organization's security policy.

Vulnerability scanners are made up of four main components, engine scanners, databases, report modules, and the user interface.

The engine scanner performs security checks according to its installed plugins, identifying system information and vulnerabilities. The built-in databases store all the vulnerability information, the scan results, and other data used by the scanner.

The report module provides scan result reporting, such as technical reports for system administrators, summary reports for security managers, and high level graph and trend reports for corporate executive leadership.

The common vulnerability scoring system is a way of assigning severity rankings to computer system vulnerabilities, ranging from zero, least severe, to ten, most severe.

The score itself is broken out into three main areas, a base score, a temporal score, and environmental score, which will provide the overall score of zero through ten

A base score, which gives an idea of how easy it is to exploit the vulnerability and how much damage and exploit targeting that vulnerability could inflict. The temporal score, which ranks how aware people are of the vulnerability, what remedial steps are being taken, and whether threat actors are targeting it. And an environmental score, which provides a more customized metric specific to an organization or work environment.

The five critical tenants of an effective cyber defense system as reflected in the CIS Controls are, offense in forms defense, prioritization, measurement and metrics, continuous diagnostics and mitigation, and automation.

Port 20, which is UDP, holds the File Transfer Protocol that we use for data transfer. Port 22 of a TCP holds the SSH, Secure Shell Protocol for secure logins, ftp, and port forwarding. Port 50 of a UDP is the Domain Name System, DNS, which translates names to IP addresses, and Port 80 of a TCP, which is the world wide HTTP.

Port numbers 49151 through 65536 are known as private and dynamic ports. While 0 to 1023 ports are the well known ports.

Network sniffers operate at the data link layer

In Base exploitability subscore Common Vulnerability Score (CVSS) attack complexity be reflected

In Base impact subscore the integrity of CVSS would be reflected

In temporal score CVSS impact remediation level is reflected

In environmental score impact subscore is reflected

Threat modeling is a process by which potential threats such as structural vulnerabilities or the absence of appropriate safeguards can be identified, enumerated, and mitigations can be prioritized. The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be

included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.

Typically threat modeling has been implemented using one of four approaches. Independently asset centric, attacker centric, and software centric.

Some of the popular threat modeling strategies are STRIDE, PASTA(process for attack simulation and threat analysis) , TRIKE, VAST(visual agile and simple threat modeling)

For avoiding cross site scripting there's a Java function, and StringEscapeUtils class called Escape HTML, and if, for every field, you use that, all the special characters that user may have entered will be properly replaced with HTML entities.

SIEM -Security Information and Event Management

SIEM provides organizations with next generation detection, analytics and response. SIEM combines SIM(security information management) and security event management(SEM) to provide real time analysis of security alerts generated by applications and network hardware. SIEM software matches events against rules and analytics engines and indexes them for sub-second search to detect and analyze advanced threats using globally gathered intelligence. This gives security teams both insight into and a track record of the activities within their IT environment by providing data analysis, event correlation, aggregation, reporting and log management.

SIEM also includes features like consolidation of multiple data points, custom dashboards, alert workflow management, integration with other products.

A SIEM really takes two different approaches, they can be a rules-based approach or employer's statistical correlation to establish relationships between log entries.

Flows are records of network activity between two hosts, and those hosts, although that connectivity, I should say, can last for a few seconds or days depending on the activity within the session.

SIEM deployment considerations are compliance, cost benefit and cyber security.

Event collector collects events from local and remote log sources and normalizes raw log source events to format them for use by QRadar. The event collector bundles or coalesces identical events to conserve system usage and sends the data to the event processor.

Event collectors can use bandwidth limiters and schedules to send events to event processors to overcome WAN limitations such as intermittent connectivity.

Event processor processes events using a custom rule engine(CRE).

Flow collector generates flow data from raw packets that are collected from monitoring ports such as SPANS, TAPS, monitor sessions etc.

Flow deduplication is the process which removes duplicate flows when multiple flow collectors provide data to flow processor appliances.

Asymmetric recombination is responsible for combining two sides of each flow when data is provided asymmetrically.This process can recognize data flows from each side and combine them into one record.However sometimes one side of the flow exists.

License  throttling monitors the number of incoming flows to the system to manage input queues and licensing

Forwarding applies routing rules for the system such as sending flow data to offsite targets, external syslog systems, JSON systems and other SIEM's.

EPS- events per second

a small deployment as one with around 300 log sources with about 1500 EPS
A medium deployment is about a thousand log sources and 7,000 EPS. And a large deployment would be about 1000 log sources and then about 15,000 EPS.

Some of the IBM QRadar components are Vulnerability Manager, User behavior analytics, network insights.

Arcsight ESM is a security information and event management solution that combines event correlation and security analytics to identify and prioritize threats in real time and remediate incidents early.

UBA -User Behaviour analytics

Dwell time is basically the duration a threat actor has undetected access in the network until it's completely removed.

When a data stream entering a SIEM exceeds the volume it is licensed to handle, what are three (3) ways the excess data is commonly handled, depending upon the terms of the license agreement? (Select 3)

The data stream is throttled to accept only the amount allowed by the license
The excess data is dropped
The excess data is stored in a queue until it can be processed

The 5 properties which are checked before the event is coalesced with other events are Username, UID, Source IP, Destination Port, Destination IP

The triad of SOC operation is people, process, technology.

Security Analytics mainly focuses on Data Correlation, Anomaly Detection and Pattern Identification.

Cyber Kill chain:  Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and control, Actions and objectives

## COURSE-07  BREACH RESPONSE CASE STUDIES

The Gh0st RAT can take full control of the remote screen on the infected bot, providing real-time as well as offline keystroke logging. Can provide live feed of webcam, microphone of an infected host. Can download remote binaries on the infected remote host and it can take control of remote shutdown, or reboot of a host. It can also disable infected computer remote pointers and keyboard input. Can enter into a shell of a remote infected host with full control. It can provide a list of all the active processes and clear all existing SSDT of all existing hooks.

Phishing, also known as brand spoofing or carding, is a term used to describe various scams that use primarily fraudulent e-mail messages sent by criminals to trick you into divulging personal information.

Spear phishing is done on a high executive official group, whaling is done on a top most executive personnel

The main objective of the Point of Sale breaches is to steal your 16-digit credit card number.

PoS malware specifically targets the RAM to steal the unencrypted information, a process called RAM scraping. These are the most common and readily available families of point of sale malware.

The Alina family malware scans the system's memory to check if the contents match regular expressions, which indicate the presence of card information that can be stolen. Vskimmer, if it does not find its server, it checks for the presence of a removable drive with the specific label.

The FYSNA malware uses the Tor network to communicate with its C&C server, and it makes detection and investigation difficult by making all the network traffic made by the malware extremely difficult to analyze. The Decebal malware checks if sandboxing or analysis tools are present on a machine before running, making detection and analysis that much more difficult. The most popular, the BlackPOS,

uses file transfer protocol to upload information to a server of the attackers choosing. This allows attackers to consolidate stolen data from multiple PoS terminals on a single server.

The only risk that still remains with P2P encryption is if someone were to install a credit card skimmer on the actual pin pad.

Supply-chain attacks also known as value-chain attacks or third party attacks, are attacks that originated from one of your third parties that has access to your system. Which includes data management companies, law firms, email providers, web hosting companies, subsidiaries, vendors, subcontractors, any external software or hardware used in your system, even the javascripts added to your website to collect analytics, and the list goes on.

The top three uses by a third party were cloud-based storage, service or hosting providers, online payment, credit card processing or point of sale systems, or JavaScript on websites, used for web analytics, visitor tracking etc.