SNP Notes

1. **What is malware?**

Malware or malicious software is a program like normal software but the difference, it is developed with a bad intension to perform some harmful operations such as corrupting computer files, stealing user information, attacking a network, encrypting sensitive date and so on. Some popular malwares are Worms, trojan horse, ransomware, rootkit, and spyware.

Despite the many variants of malware, attacks can generally be classified into two types: Targeted and Mass Campaign.

A "Targeted" attack is just that - targeted. In most cases, malware attacks that occur this way are created for a specific purpose against a specific target.

What is the famous example of a targeted attack-esque Malware that targeted Iran?
Stuxnet

A "Mass campaign" attack, the entire purpose of this type of Malware is to infect as many devices as possible and perform whatever it may - regardless of target.

What is the name of the Ransomware that used the Eternalblue exploit in a "Mass Campaign" attack?
Wannacry

2. **What is malware analysis?**

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor

Malware Analysis is important because it helps security operations teams rapidly detect and prevent malicious objects from gaining persistence and causing destruction within the organization.

there are two categories of fingerprints that malware may leave behind on a Host after an attack:

host based signature: These are generally speaking the results of execution and any persistence performed by the Malware. For example, has a file been encrypted? Has any additional software been installed? These are two of many, many host-based signatures that are useful to know to prevent and check against further infection.

Network based signature: this classification of signatures is the observation of any networking communication taking place during delivery, execution and propagation. For example, in Ransomware, where has the Malware contacted for Bitcoin payments?

What type of signature is used to classify remnants of infection on a host? **host based signature**

There are two categories used when analyzing malware, these are:

Static analysis: process of analyzing malware without executing or running it. The objective is to extract as much metadata from the malware as possible such as, analyzing the checksums.

Dynamic analysis: it is risky process, process of executing malware and analyzing it's functionality and behaviors. The objective is to understand exactly how and what the malware does during the execution. This is usually tested in a sandbox environment by malware analyzers.

MD5 "Checksums" are a prominent attribute in the malware Community. Because there can be many variants of a family of Ransomware, these MD5 "Checksums" are cryptographic "fingerprints" of the files. This allows a uniformed identification throughout the community

3. **What is Obfuscation / Packing?**
malware Authors employ obfuscation techniques such as packing, they do so with the intent to prevent people like us reversing it to understand its behaviors and ultimately with the aims of achieving infection.

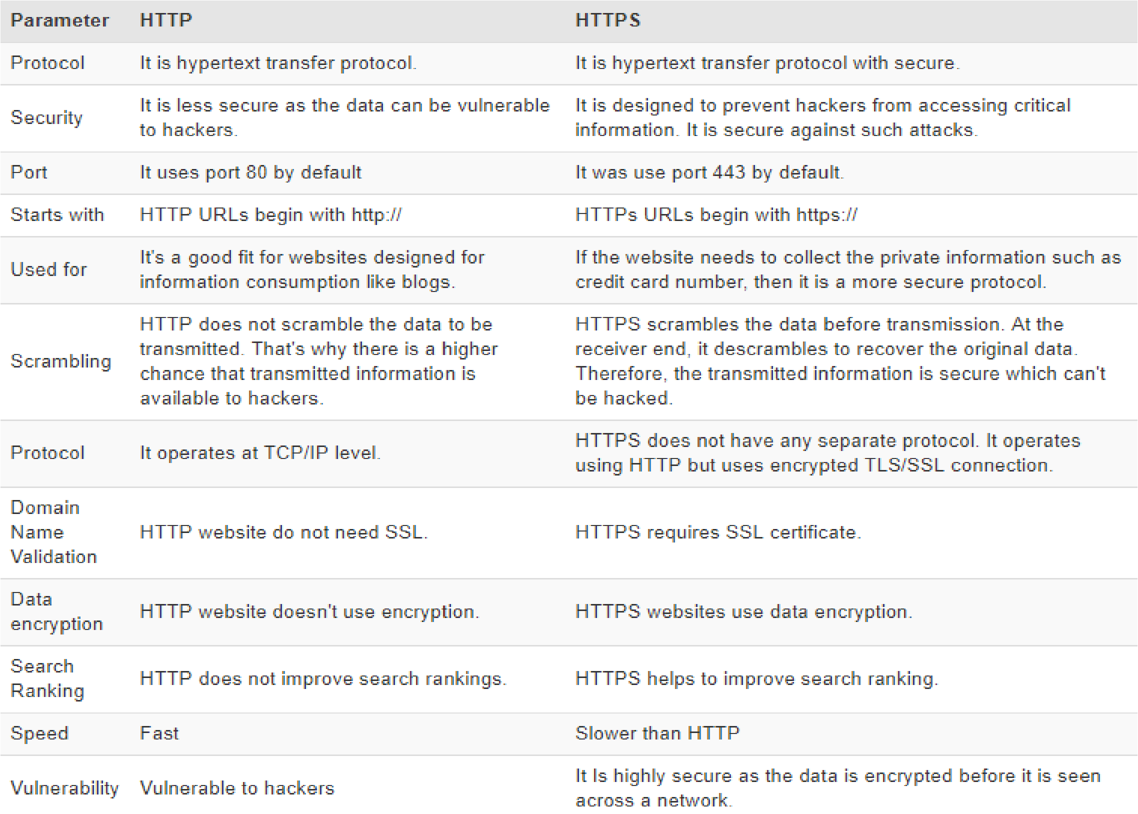
4. **What is mobSF and why it is used?**
It is a mobile security framework used for static and dynamic security analysis of mobile application

- all in one mobile security application for android, iOS and windows pen-testing
- supports mobile app binaries (APK, IPA, and APPX) along with zipped code

5. **What is wireshark, why you have to use it and why it is important to network security engineer?**
Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet

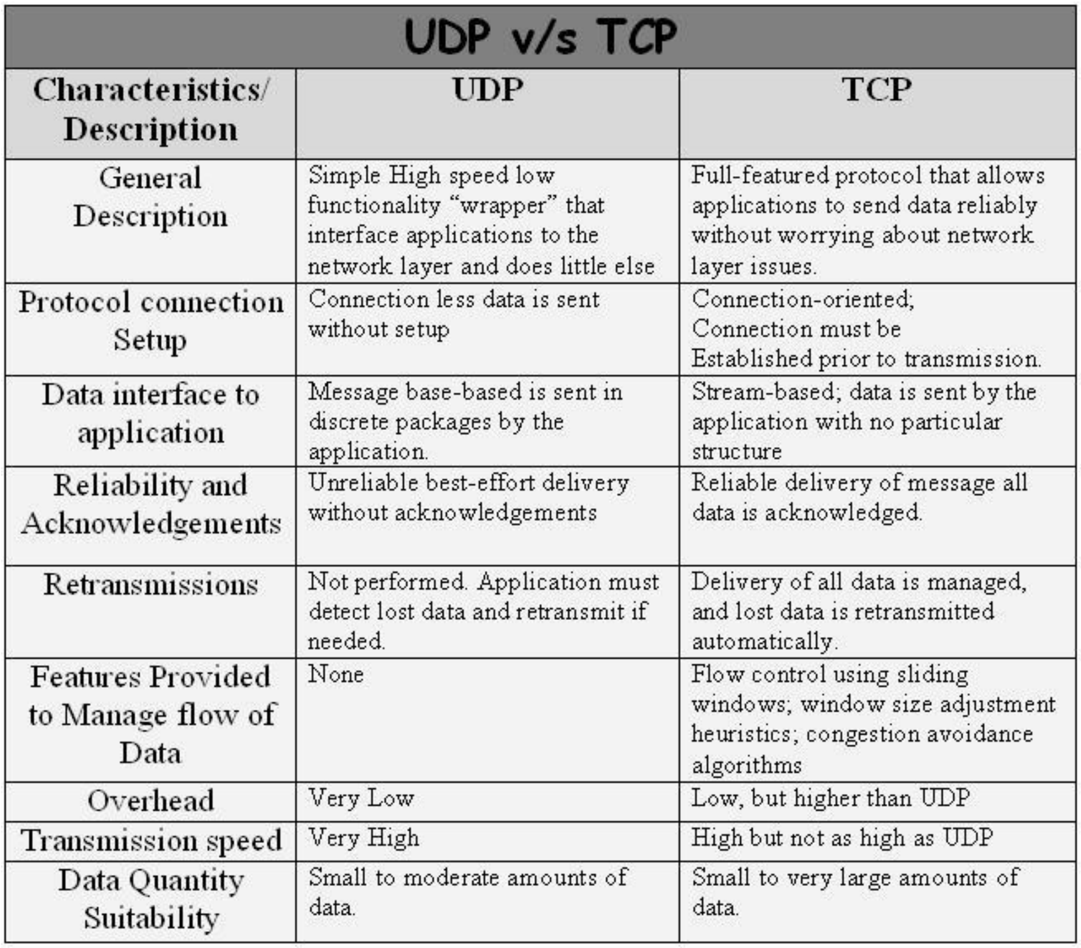
Wireshark will help you capture network packets and display them at a granular level. Once these packets are broken down, you can use them for real-time or offline analysis. This tool lets you put your network traffic under a microscope, and then filter and drill down into it, zooming in on the root cause of problems, assisting with network analysis and ultimately network security.

6. **HTTP vs HTTPS**



Parameter	HTTP	HTTPS
Protocol	It is hypertext transfer protocol.	It is hypertext transfer protocol with secure.
Security	It is less secure as the data can be vulnerable to hackers.	It is designed to prevent hackers from accessing critical information. It is secure against such attacks.
Port	It uses port 80 by default	It was use port 443 by default.
Starts with	HTTP URLs begin with http://	HTTPs URLs begin with https://
Used for	It's a good fit for websites designed for information consumption like blogs.	If the website needs to collect the private information such as credit card number, then it is a more secure protocol.
Scrambling	HTTP does not scramble the data to be transmitted. That's why there is a higher chance that transmitted information is available to hackers.	HTTPS scrambles the data before transmission. At the receiver end, it descrambles to recover the original data. Therefore, the transmitted information is secure which can't be hacked.
Protocol	It operates at TCP/IP level.	HTTPS does not have any separate protocol. It operates using HTTP but uses encrypted TLS/SSL connection.
Domain Name Validation	HTTP website do not need SSL.	HTTPS requires SSL certificate.
Data encryption	HTTP website doesn't use encryption.	HTTPS websites use data encryption.
Search Ranking	HTTP does not improve search rankings.	HTTPS helps to improve search ranking.
Speed	Fast	Slower than HTTP
Vulnerability	Vulnerable to hackers	It Is highly secure as the data is encrypted before it is seen across a network.

7. **TCP vs UDP**

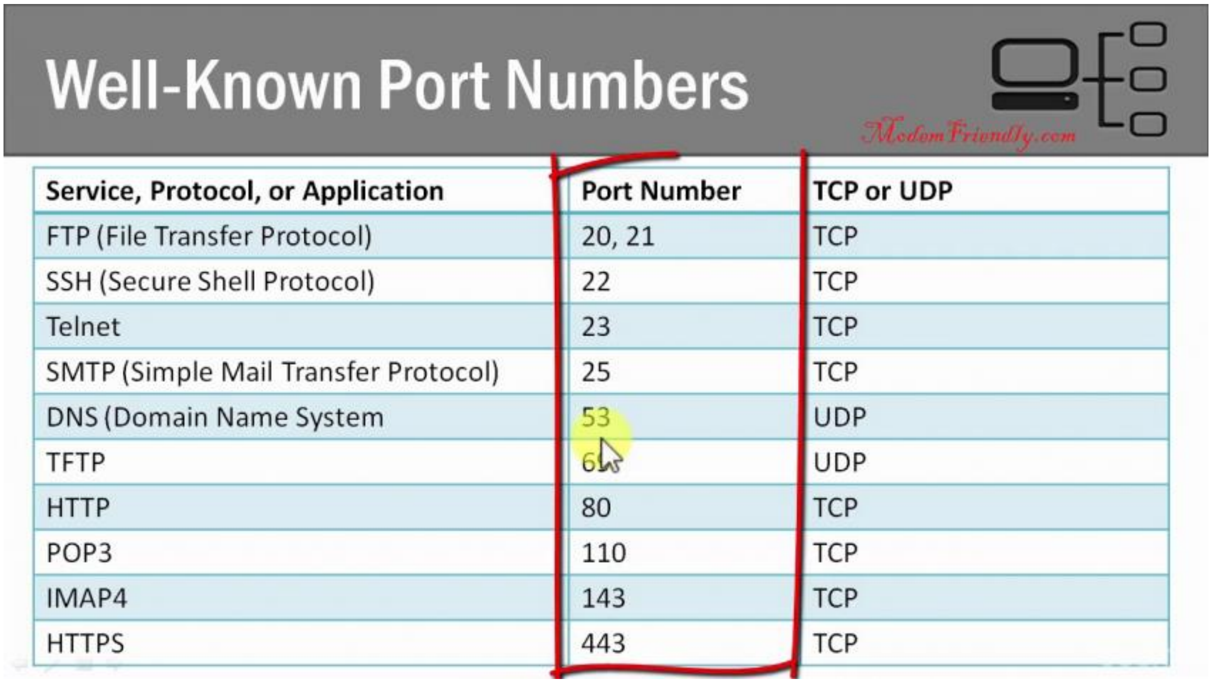


UDP v/s TCP

Characteristics/ Description	UDP	TCP
General Description	Simple High speed low functionality "wrapper" that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol connection Setup	Connection less data is sent without setup	Connection-oriented; Connection must be Established prior to transmission.
Data interface to application	Message base-based is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure
Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms
Overhead	Very Low	Low, but higher than UDP
Transmission speed	Very High	High but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data.

8. **What is port?**

Port is software defined number which is associated with a protocol that enables to send transmit and receive a particular service uniquely among networks.



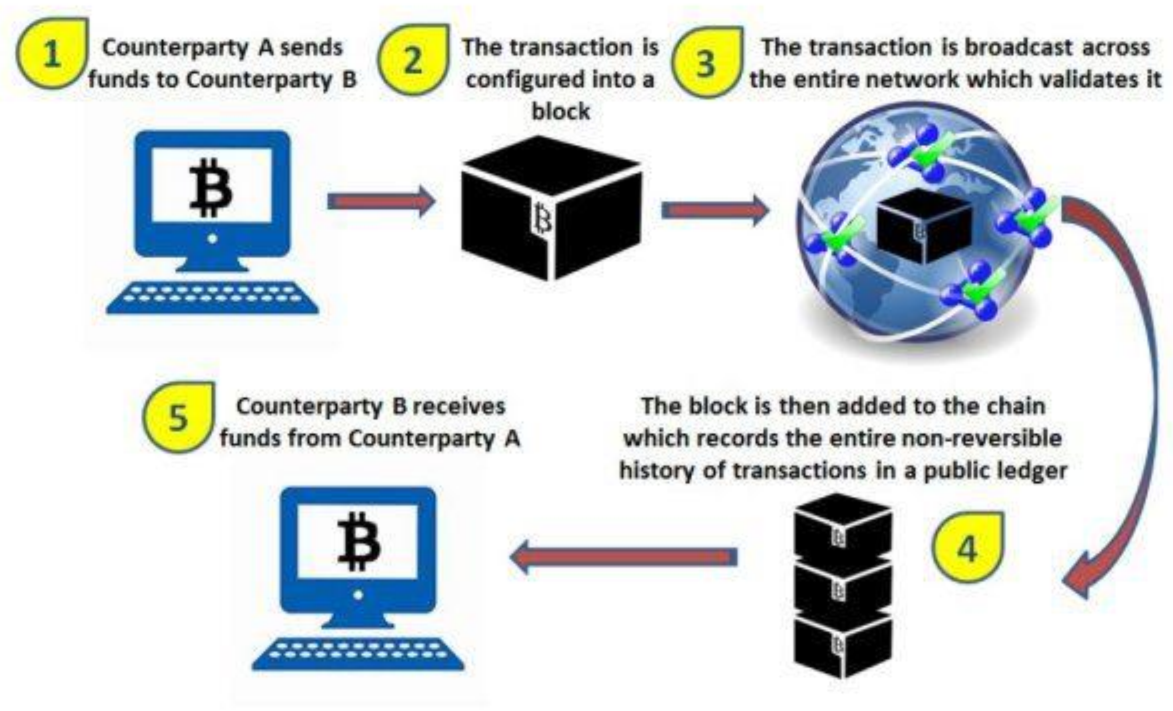
Well-Known Port Numbers

Service, Protocol, or Application	Port Number	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System	53	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
IMAP4	143	TCP
HTTPS	443	TCP

9. **What is blockchain?**

It is a type of **distributed ledger technology (DLT)**, a digital system for recording transactions and related data in multiple places at the same time. Each computer in a blockchain network maintains a copy of the ledger to prevent a single point of failure (peer to peer), and all copies are updated and validated simultaneously. Any data stored on blockchain is unable to be modified, making the technology a legitimate disruptor for industries like payments, cybersecurity and healthcare.

Exhibit 1: The Blockchain is a distributed, public ledger, most commonly known as the core underlying technology for Bitcoin


1
Counterparty A sends funds to Counterparty B
2
The transaction is configured into a block
3
The transaction is broadcast across the entire network which validates it
4
The block is then added to the chain which records the entire non-reversible history of transactions in a public ledger
5
Counterparty B receives funds from Counterparty A

Source: Goldman Sachs Global Investment Research.

10. **Key terms in blockchain technology:**

a. **Block -** Every record or data that the network produces is essentially stored inside a block and every time a record is created, there is a new block to contain it. In other words, you can also think of it as a container for holding the blockchain data.

b. **Genesis block** – It happens to be the very first block on a blockchain network and can also be considered as the pioneering record therefore, In Blockchain, it is the only block that doesn't refer to its previous block. it mainly contains the configurations and rules for the smooth running of the blockchain.

c. **Decentralization** - it means that two individuals or computers can communicate directly without depending on an intermediary (i.e., a centralized organization). Therefore, everyone has the same authority.

d. **Smart contracts** - Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible.

e. **Solidity** - This programming language is most commonly used in the blockchain industry for writing smart contracts and resembles closely with C++.

f. **Mining** - This is the core of any blockchain network, mining is a process to validate transactions by solving a difficult mathematical puzzle called proof of work, as a result this will create a new block that contains the record. Once a block is created, there is no reversal for this operation.

g. **Cryptocurrency** - This is a tradeable digital asset that runs on blockchain technology. Can be owned and used by anyone anywhere in the World, the proof of ownership can always be proved, and Can never undergo inflation by a centralized body.

h. **Nonce** - "Nonce" is a portmanteau of "number used only once." It is a four-byte number added to a hashed—or encrypted—block in a blockchain that, when rehashed, meets the difficulty level restrictions. The nonce is the number that blockchain miners are solving for. When the solution is found, the blockchain miner that solves it is given the block reward.

11. Why it is more secure?

Blockchain is distributed which means everyone obtains a copy in the case of a public blockchain. So, it is very difficult to modify the data in the blockchain because to do so every copy in every location would need to be changed (which is near to impossible) This makes blockchain both distributed and immutable along with maintaining transparency as the data in the block is not hidden in any way. All of these properties of blockchain ensure the highest levels of security which is why it is so popular in many applications that prioritize security and transparency.

12. Application of blockchain technology –

a. **Asset management** - Asset management involves the handling and exchange of different assets that an individual may own such as fixed income, real estate, equity, mutual funds, commodities, and other alternative investments. Normal trading processes in asset management can be very expensive, especially if the trading involves multiple countries and cross border payments. In such situations, Blockchain can be a big help as it removes the needs for any intermediaries such as the broker, custodians, brokers, settlement managers, etc. Instead, the blockchain ledge provides a simple and transparent process that removes the chances of error.

b. **Cryptocurrency** - One of the many advantages of cryptocurrency using blockchain as it has no geographical limitations. So crypto coins can be used for transactions all over the world. The only important thing to keep in mind is exchange rates and that people may lose some money in this process. However, this option is much better than regional payment apps such as Paytm in India that are only relevant in a particular country or geographical region and cannot be used to pay money to people in other countries.

c. **Online identity verification** - It is not possible to complete any financial transactions online without online verification and identification. And this is true for all the possible service providers any user might have in the financial and banking industry. However, blockchain can centralize the online identity verification process so that users only need to verify their identity once using blockchain and then they can share this identity with whichever service provider they want. Users also have the option to choose their identity verification methods such as user authentication, facial recognition, etc.

d. **Internet Of Things** - Any system of “things” becomes IoT once it is connected. The most common example of IoT is perhaps the Smart Home where all the home appliances such as lights, thermostat, air conditioner, smoke alarm, etc. can be connected together on a single platform. But where does Blockchain come into this? Well, Blockchain is needed for providing security for this massively distributed system. In IoT, the security of the system is only as good as the least secured device which is the weak link. Here Blockchain can ensure that the data obtained by the IoT devices are secure and only visible to trusted parties.

13. Future Cyber security use cases with blockchain –

Below are some use cases of future beneficial use of blockchain to strengthen cybersecurity:

Advanced Confidentiality and Data Integrity: Owing to its nature of public distribution, Blockchain was created without any particular access controls initially. But with time, as the technology started providing solutions to multiple industries, blockchain implementations now have scope for data confidentiality as well as access control. The complete encryption of the Blockchain ensures that data as a whole or in part is not accessible to any wrongful person or organization while in transit.

Secured private messaging: A lot of companies are looking at Blockchain to secure their personal and private information exchanged over chats, messaging apps and social media. Most social media platform users protect the services and their data with weak, unreliable passwords. Most messaging companies are warming up to blockchain for securing user data as a superior option to the end-to-end encryption which they currently use. Blockchain can be used to create a standard security protocol. For enabling cross-messenger communication capabilities, blockchain can be used to form a unified API framework.

Guard for DDoS attacks: A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or another network resource, and cause a denial of service for users of the targeted resource. This forces the system to slow down or even crash and shut down, thereby denying service to legitimate users or systems. blockchain can be used to reduce such kinds of attacks by decentralizing the DNS entries. By applying decentralized solutions, blockchain would have removed the vulnerable single points exploited by hackers.

Decentralizing medium storage: By using blockchain, sensitive data may be protected by ensuring a decentralized form of data storage. This mitigation method would make it harder and even impossible for hackers to penetrate data storage systems. Many storage service companies are assessing ways blockchain can protect data from hackers.

Protecting data transmission: Blockchain can be used in the future to prevent unauthorized access to data while in transit. By utilizing the complete encryption feature of the technology, data transmission can be secured to prevent malicious actors from accessing it, be it an individual or an organization. This approach would lead to a general increase in the confidence and integrity of data transmitted through blockchain. Hackers with malicious intent tap into data amid transit to either alter it or completely delete its existence. This leaves a huge gap in inefficient communication channels, such as emails

14. What is ISO/IEC 27001 standards?

ISO/IEC 27001 is an international standard widely adopted by different countries to secure IT assets by providing security controls based on industry best practices. 27001 is published by ISO and the International Electrotechnical Commission (IEC). This standard provides recommendations for implementing an Information Security Management System (ISMS) irrespective of the size of an organization.

15. What is the content of ISO 27001 ?

ISO/IEC 27001 standard includes 13 objectives. It provides recommendations and guidance on structure, risk assessment, and access control policy, security related to staff, and compliance.

16. What is information security management system (ISMS)?

An ISMS is a collection of following items to secure information assets from any type of attack that fails CIA principle.

>>Policies
>>Procedures
>>Guidelines
>>Associated Resources and Activities

17. What are the objectives for implementation of ISO 27001 ?

>>assurance to secure assets against threats
>>provoding framework for providing risks
>>improve controls on environment
>>provide legal and regulatory compliance

18. What is XSS ?

Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user’s browser. Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.

19. Distinguish between white hat and black hat?

A Black Hat hacker is a computer hacker who violates cybersecurity for personal gain or malicious intent. They break into secure networks with the intent of stealing or altering information. They're hacking gangs who aren't allowed to operate legally. The term "white hat" refers to a group of ethical hackers. They are computer security specialists who specialize in various computer testing techniques. They protect an organization's information system.

20. Why would you want to use SSH from a Windows PC?

SSH (TCP port 22) is a secure connection used on many different systems and dedicated appliances. Routers, Switches, SFTP servers and insecure programs being tunneled through this port all can be used to help in hardening a connection against eavesdropping. Even though most of the times when you hear about somebody ‘SSHing’ into a box it involves Linux, the SSH protocol itself is actually implemented on a wide variety of systems. Programs like PuTTY, Filezilla and others have Windows ports available, which allow Windows users the same ease-of-use connectivity to these devices as do Linux users.

21. What is salt hashes?

Salt is basically random data. When a properly protected password system receives a new password, it will create a hashed value for that password, create a new random salt value, and then store that combined value in its database. This helps you defend against dictionary attacks and known hash attacks.