Accenture Sections	Information	Questions and Time
Cognitive Ability	• English Ability • Critical Thinking and Problem Solving • Abstract Reasoning	50 Ques in 50 mins
Technical Assessment	• Common Application and MS Office • Pseudo Code • Fundamental of Networking, Security and Cloud	40 Ques in 40 mins
Coding Round	• C • C++ • Dot Net • JAVA • Python	2 Ques in 45 mins

Technical Assessment	No. of questions
Networking Security and Cloud	10 Questions
Time limit	10 minutes
Difficulty	moderate

DEBUG WITH SHUBHAM

Accenture Technical Assessment Detailed Overview

Accenture Fundamentals of Networking Security and Cloud Questions


https://www.youtube.com/@DebugWithShubham


https://www.linkedin.com/in/debugwithshubham/


https://www.instagram.com/debugwithshubham/


https://topmate.io/debugwithshubham


https://t.me/debugwithshubham

Top Network Security Interview Questions and Answers

Q: What do you see as the objective of information security within a business or organization?

A: Network security should:

- Ensure uninterrupted network availability to all users
- Prevent unauthorized network access
- Preserve the privacy of all users
- Defend the networks from malware, hackers, and DDoS attacks
- Protect and secure all data from corruption and theft

Q: How do you define risk, vulnerability, and threat, in the context of network security?

A: A risk is defined as the result of a system being secure but not secured sufficiently, thereby increasing the likelihood of a threat. A vulnerability is a weakness or breach in your network or equipment (e.g. modems, routers, access points). A threat is the actual means of causing an incident; for instance, a virus attack is deemed a threat.

Q: What are the possible results of an attack on a computer network?

A: Possible results include:

- Loss or corruption of sensitive data that is essential for a company's survival and success
- Diminished reputation and trust among customers
- The decline in value with shareholders
- Reduced brand value
- Reduction in profits

Q: What do you use on your own personal network?

A: An interviewer will want to know what sort of security measures you use on your own home devices. After all, if you're a hotshot network security expert, clearly that must be reflected in the network that means the most to you; your personal system! An employer can tell a lot about your network savviness by analyzing what measures you use for your devices.

Q: Speaking of your home network, do you have a Wireless Access Point, and if so, how do you defend it?

A: There are many methods of protecting a WAP, but the three most popular are: employing MAC address filtering, using WPA2, and not broadcasting the SSID. This is yet another attempt by an employer to see what matters to you personally in terms of security. After all, people tend to prefer the best things for themselves!

A: Network security incidents are big news today, and there have been many high-profile news stories about data breaches and hackers in the past few years. An employer is going to want to know how well-informed you are on the latest security news and incidents. HINT: If you don't make it a practice of keeping abreast of the latest network security-related news, you better start now!
In terms of news sources, your best bets are Team Cymru, Twitter, or Reddit. Make sure to check the sources of accuracy, though.

Q: What are the best defenses against a brute force login attack?

A: There are three major measures you can take to defend against a brute force login attack. For starters, there's an account lockout. Offending accounts are locked out until such time as the administrator decides to open it again. Next comes the progressive delay defense. Here, the account stays locked for a given number of days after a few unsuccessful login attempts are made. Finally, there's the challenge-response test, which heads off automatic submissions employed on the login page.

Q: Explain the difference between symmetric and asymmetric encryption.

A: Long story short, symmetric encryption uses the same key for both encryption and decryption, whereas asymmetric encryption employs different keys for the two processes. Symmetric is faster for obvious reasons but requires sending the key through an unencrypted channel, which is a risk.

Q: Explain the difference between a white and black hat hacker.

A: Black and white hat hackers are different sides of the same coin. Both groups are skilled and talented in gaining entry into networks and accessing otherwise protected data. However, black hats are motivated by political agendas, personal greed, or malice, whereas white hats strive to foil the former. Many white hats also conduct tests and practice runs on network systems, to ascertain the effectiveness of security.

Q: Define the salting process and what it's used for.

A: Salting is the process wherein you add special characters to a password in order to make it stronger. This increases password strength in two ways: it makes it longer and it adds another set of characters that a hacker would have to guess from. It's a good measure to take for users who tend to habitually make weak passwords, but overall it's a low-level defense since many experienced hackers are already familiar with the process and take it into account.

Q: How do you deal with "Man In The Middle" attacks?

A: A Man in the Middle attack happens when there is a third party that's monitoring and controlling a conversation between two parties, with the latter completely unaware of the situation. There are two ways of dealing with this attack. First of all, stay off of open Wi-Fi networks. Second, both parties should employ end-to-end encryption.

Q: Which is the better security measure, HTTPS, or SSL?

A: HTTPS (Hypertext Transfer Protocol Secure) is HTTP combined with SSL, encrypting a user's browsing activity and making it safer. SSL (Secure Sockets Layer) is a protocol that protects Internet conversations between two or more parties. Though it's close, SSL wins out in terms of sheer security, though any of these are valuable things to know for the purposes of web development.

Q: Name the three means of user authentication.

A: There is biometrics (e.g. a thumbprint, iris scan), a token, or a password. There is also two-level authentication, which employs two of those methods.

Q: Which is a more secure project: open-source or proprietary?

A: This is a trick question; don't be fooled! A project's security is determined by the quality of security measures used to protect it, the number of users/developers with access, and the overall size of the project. The kind of project is irrelevant.

Q: If you work with a Linux server, what are the three significant steps you must take in order to secure it?

A: In order to secure your Linux server, you must do the following, in order:

- Audit. Scan the system using Lynis. Each category gets scanned separately, and a hardening index is generated for the next step.
- Hardening. Once auditing is done, hardening is done, based on the level of security to be employed.
- Compliance. This is an ongoing step, as the system is checked daily.

Q: You discover an active problem on your organization's network, but it's out of your sphere of influence. There's no doubt that you can fix it, though; so what do you do?

A: While the first impulse may be to immediately fix the problem, you need to go through the proper channels. Things may be as they are for a reason. Use e-mail to notify the person in charge of that department, expressing your concerns, and asking for clarification. Make sure your boss is CC'ed into the email chain, and make sure that you save a copy for yourself, in case you need to refer to it later.

Q: What's the most effective measure to take against a CSRF?

A: A Cross-Site Request Forgery (CSRF) attack causes a currently authenticated end-user to execute unauthorized commands on a web application. There are two effective defensive measures. First of all, use different names for each field of a form, as it increases user anonymity. Second, include a random token with each request.

Q: You get a phone call from a very influential executive high up on the organizational chart. He or she tells you to bend company policy to suit them and let them use their home device to do company work. What do you do?

A: This is another case of letting someone higher than you make the decision. Send the question/request up to your manager and let them sort it out. This is far outside of your realm. Let your boss deal with the higher-up.

Q: Which is worse in terms of Firewall detection, and why? A false positive or a false negative?

A: A false negative is worse by far. A false positive is simply a legitimate result that just got incorrectly flagged. While it's irksome, it's by no means fatal or difficult to correct. But a false negative means that something bad has slipped through the firewall undetected, and that means a host of problems down the road.

Q: Why are internal threats usually more effective than external threats?

A: It all comes down to a question of physical location. A disgruntled soon to be ex-employee, a hacker posing as a deliveryman, even just a careless curious user, all end up having better access to the system due to them being on-site. Being "inside" physically makes it easier to get inside virtually.

Question 1

Time: 00:00:01

Which is not an objective of network security?

- Identification 12.91%
- Authentication 8.76%
- lock **66.19%**
- Access Control 12.15%

Question 2

Time: 00:00:01

An algorithm in encryption is called _____

- Algorithm 5.48%
- Procedure 12.28%
- Cipher **72.37%**
- Module 9.87%

Question 3

Time: 00:00:00

What is ransomware?

- A nickname for the types of spyware that require a password on boot 13.02%
- Software that steals files from your computer and is used by blackmailers 23.45%
- A software that hijacks your computer and asks you to pay in order for it to be removed **39.22%**
- viruses that infect files and won't let you open them unless you know a certain pass code 24.31%

Question 4

Time: 00:00:01

Which of the following has network reliability issues?

- frequency of failures 6.10%
- recovery time after failure 8.49%
- catastrophe 7.19%
- All of the above **78.22%**

Question 5

Time: 00:00:01

A digital signature scheme consists of which of the following typical algorithms?

- ◉ Key generation, Signing and Signature Verifying Algorithm — 68.53%
- ○ Signature Verifying Algorithm — 14.85%
- ○ Key Generation Algorithm — 12.67%
- ○ Signing Algorithm — 3.95%

Question 6

Time: 00:00:01

The type of encoding in which manipulation of bit streams without regard to what the bits mean is .....

- ○ Destination encoding — 17.64%
- ◉ Entropy encoding — 36.84%
- ○ Source encoding — 27.49%
- ○ Differential encoding — 18.03%

Question 7

Time: 00:00:01

The protocol used to provide security to e-mails?

- ○ POP — 17.07%
- ◉ PGP — 14.52%
- ○ SNMP — 41.19%
- ○ HTTP — 27.22%

Question 8

Time: 00:00:01

The ..... portion of LAN management software restricts access, records user activities and audit data etc.

- ○ Configuration management — 19.48%
- ◉ Security management — 66.84%
- ○ Performance management — 8.52%
- ○ None of these — 5.16%

Question 9

Time: 00:00:01

Caesar cipher with key 3, is represented as .....

○ C = (p+3)mod3	28.12%	○ C = (p+26)mod3	19.76%
○ C = (p*3)mod26	20.02%	◉ C = (p+3)mod26	**32.10%**

Question 10

Time: 00:00:01

Number of rounds in Data Encryption Standard algorithm?

○ 8 rounds	22.79%	○ 12 rounds	28.40%
◉ 16 rounds	**40.40%**	○ 24 rounds	8.40%

Question	Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN
	with frames of size 10,000 bits. Assume the signal speed in the cable to be 2,00,000 km/s.
Option 1	1 km
Option 2	2 km
Option 3	3 km
Option 4	5 km
KEY	**B**
Explanation	Data should be transmitted at the rate of 500 Mbps. Transmission Time >= 2*Propagation Time => 10000/(500*1000000) <= 2*length/200000 => lenght = 2km (max)

Question	Let G(x) be the generator polynomial used for CRC checking. What is the condition that should be satisfied by G(x) to detect odd number of bits in error?
Option 1	G(x) contains more than two terms
Option 2	G(x) does not divide 1+x^k, for any k not exceeding the frame length
Option 3	1+x is a factor of G(x)
Option 4	G(x) has an odd number of terms
KEY	**C**
Explanation	O dd number of bit errors can be detected if G(x) contains (x+1) as a factor.

Question	A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) CANNOT
Option 1	block HTTP traffic during 9:00PM and 5:00AM
Option 2	block all ICMP traffic
Option 3	stop incoming traffic from a specific IP address but allow outgoing traffic to same IP
Option 4	block TCP traffic from a specific user on a specific IP address on multi-user system during 9:00PM and 5:00AM
KEY	**A**
Explanation	HTTP is an application layer protocol. Since firewall is at layer 4, it cannot block HTTP data.

Question	A subnet has been assigned a subnet mask of 255.255.255.192. What is the maximum number of hosts that can belong to this subnet?
Option 1	15
Option 2	32
Option 3	62
Option 4	116
KEY	**C**
Explanation	he given subnet mask, 255.255.255.192, in binary is- 11111111.11111111.11111111.1100000 Number of bits for the network prefix is- 8 + 8 + 8 + 2 = 26 Number of bits available for hosts - 32 - 26 = 6 Number of addresses available = $2^6 = 64$ The first address is reserved for the subnet and the last address is reserved as the broadcast address. So, number of host addresses = 64 - 2 = 62

Question	A host is connected to a Department network which is part of a University network. The University network, in turn, is part of the Internet. The largest network in which the Ethernet address of the host is unique is:
Option 1	The subnet to which the network beongs
Option 2	The department network
Option 3	The university network
Option 4	The internet
KEY	
Explanation	Ethernet address is basically the MAC address, which is supposed to be unique to a NIC. Thus it is unique over the Internet.

Question	A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as.....
Option 1	Choke point
Option 2	Meeting point
Option 3	Firewall point
Option 4	**Secure point**
KEY	**A**
Explanation	Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines. A choke point is **a single point through which all incoming and outgoing network traffic is funnelled**. As all traffic passes through a choke point it is the natural place to focus monitoring and control efforts such as Internet firewalls.

Question	Check Sum, Error control and Length information are main features of
Option 1	SCTP
Option 2	IP
Option 3	UDP
Option 4	TCP
KEY	**C**
Explanation	The Checksum, Error control and Length information are the main features of UDP. UDP (**User Datagram Protocol**) is a communications protocol that is primarily used for establishing low-latency and loss-tolerating connections between applications on the internet. It speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.

Question	To prevent its signal from interfering with other cells, transmission power of each cell is kept
Option 1	High
Option 2	Low
Option 3	Satic
Option 4	optimized
KEY	**B**
Explanation	To prevent its signal from interfering with other cells, transmission power of each cell is kept Low.

Question	The GSM network is divided into the following three major systems :
Option 1	SS, BSS, OSS
Option 2	BSS, BSC, MSC
Option 3	CELL, BSC, OSS
Option 4	SS, CELL, MSC
KEY	**A**
Explanation	The GSM network is divided into three major systems: **the switching system (SS), the base station system (BSS), and the operation and support system (OSS)**.

Question	CaaS stands for---------- as service
Option 1	Compliance
Option 2	Computer
Option 3	Community
Option 4	Communication
KEY	**D**
Explanation	Communication as a Service (CaaS), enables the consumer to utilize Enterprise level VoIP, VPNs, PBX and Unified Communications without the costly investment of purchasing, hosting and managing the infrastructure.

THANK YOU