The topic coming up is Internet Encryption Part One.

And we'll go ahead and start with the first question.

This question involves blockchain.

Which of the following statements are true about blockchain technology? You are asked to choose all that apply; please take a moment read to the choices and then let's see what you're thinking.

We've got some responses coming into the chat and let's see what people are thinking.

C, let's see here; there we go B, B, D and C.

It doesn't look like anybody's saying A.
Let's talk about that. Blockchain is centralized.

If you know anything about blockchain you know it's not. We've got votes for B and C, D and B.

Blockchain is recorded in a public Ledger and that is the correct answer.

Third choice: Blockchain only deals with financial transactions like cryptocurrencies.

Is that true? Is blockchain only used for crypto?
No, that is not true.
No.
That leaves choice D, everyone has the equivalent ability to see every blockchain transaction,
which of course is a strong site.

That is one of the strengths of blockchain. Blockchain's also used for non-cryptocurrency
Applications. Can anyone name an application and something that's probably near and dear to all of our hearts. Non-crypto-based application of blockchain.

Go ahead.

Could you say that again please?

You said one that's near and dear to our hearts?
Yes, it's been in the news a bit.

How about voting?

Right.

Let's see another one could be the food sector.

You could have blockchain acting like sort of a trusted third party between brands and consumers.

It does provide traceability; let's see what we have in the chat.

NFTs, non-fungible tokens.

Traceability is an advantage.

Does it would allow us for example to understand and and follow the origin of a product and follow it through its path through processing and even the distribution.

As we've mentioned voting, corporate social responsibility. I think pretty much anything that is easily verified and not easily distorted. Not just for crypto.

The next question: FTPS

Which of the following scenarios would an FTPS solution be best suited for?

Take a moment and look at the responses

We've got votes for D and B but then a retraction on the D.

Let's say B the second one and that is the correct answer. A group wants to improve confidentiality by using SSL or TLS to encrypt data file transfers.

Choice two works

In the question because FTPS uses both SSL or TLS. Choice three a group wants to monitor
and manage firewall traffic.

Is that reasonable. No, it's not used to monitor firewall traffic.
Choice four: A group wants there to be a secure link between the client and server using SSH to transfer data files.

Now, at first glance it might look right but it's not.

If I ask what is the difference between FTPS and SFTP. What do you think?
That's a good question. I was going to ask if it was a typo.
No.
SFTP builds on secure shell protocol and adds on file transfer capabilities; FTPS builds on file transfer protocol and that's a security and encryption layer.

Let’s move on to the next question.

Key entropy: For a cryptographic system to better withstand brute force attacks, it is important that it exhibits high entropy. One element that plays a significant role in strengthening an encrypted keys entropy is by adjusting which of the following?

I think it's obvious that you need to know what entropy is.

So what is it?

What would you say it does? or is involved with?

We have a response - disorder.
Let's see we have another response - randomness
Unpredictability, uncertainty - we could say that. Insecurity. It’s a measure of the amount of uncertainty and attacker faces to determine the value of a secret and is usually stated in bits. Key entropy involves the size of a key space.

Given that, what do you think is the correct answer to this question?
Key length. Yes, key length is correct. Let’s see what our choices are.
Yep, everybody’s got A.

Key entropy is improved. Remember we're talking about uncertainty is improved with a larger key space. The larger the key space basically the better the encryption A larger key space has more possible values that would need to be calculated.

If somebody's trying to crack the key and of course you can see where brute force attacks would bring into this, the larger the space the domain if you will
the tougher it is and the more uncertainty faced by the attacker.

All right good

The next question: regex. You use the regex command on a Windows server to configure security settings to the registry.

50/50 here. This is true or false.
False. False.
Anybody think it's true
What are they doing here?
The play on words with registry and regex.
Absolutely, regex - regular expression - and reg edit - very
very close so kind of fooling around with the two words in the meaning saying
yes the answer is false not to confuse regular expressions with registry editing. They just sound alike. I kind of think this is one of those really nice questions that the kind you'd like to see.
False.

SSH- A secured link is created between the client and server using SSH over which standard TCP port?

It looks like we have some well-known port numbers here.
Oh, no, 22.
We've got a response and people coming in the chat and it is in fact 22.

All right. 443 is what?

HTTPS
Yes, HTTPS

23?
FTP
Telnet protocol

All right, lesson learned. Know your well-known port numbers.

Question - Types of hardware

Which type of hardware is needed if you decide to store digital certificates and cryptographic keys?

We've got some answers coming in the chat.

Lots of votes for TPM, trusted platform module. Key locker, not correct; Thumb drive, not a good choice. That leaves us with Hardware security modules and TPMs, trusted platform modules.

How does this relate? How do the two relate to each other?

We have a response.

Again is for software. That's interesting - HSMS are hardened tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data and creating and verifying digital signatures a TPM is a computer chip like a microcontroller that can securely store artifacts used to authenticate a platform.

The correct answer here is TPM.

CISO: The CISO of an organization has
encrypted their company's VM hard drives.

105
00:16:47.760 --> 00:16:51.780
Which of the following is the CISO protecting?

We're using encryption; we have responses.

Great, very good. Everybody - confidentiality
good? It's really important to understand the differences between confidentiality and integrity.

There are lots of different waysthe question can be asked I would be pretty confident in telling you that the most typical is to prevent the present excuse me to present a scenario like what
we have here and then ask you which of the tenants is being described. I'd say this is
a very common way to ask this question.

EAP-TLS: EAP-TLS protocol requires that both the server side and client side are configured with what?

Looks like we have me responses coming in. Let's see what we've got so far.

We have a vote for A
and some more responses, C
New factor C
Anyone else?

The correct answer here is a public key certificate.

Private keys typically belong to the owner of data.

Choice three - two-factor authentication.
What do you think about that?
I think several people said C
Extensible Authentication Protocol uses TLS security for secure authentication on wireless networks . This solution typically involves the use of
client certificates to perform Authentication. It’s not exactly having anything to do with
two-factor authentication or generic token cards.

That particular method permits the transfer of unencrypted usernames and passwords from the client to the server.

Public key certificate is the correct answer for this question.
Next question

IPSec

How did the IPSec tunnel mode and transport mode relates to each other everyone proceed?

Let's see what else we have here.

Any other responses?

And transport encrypts the data
C is what we're looking for tunnel mode
Encapsulates the original LP packets and transport mode encrypts payload data for the most part knowledge based type of questions. Let's go to the next one.

IPSec. Well we'll try this one too which of the following is true regarding IPSec

Take a moment look this over. and I'm going to take responses

We have D, a couple of choices for D

Is there anything that stands out it's obviously incorrect?

More responses too - C D and C.
All right, obviously incorrect.

YE stands for internet provider security obviously wrong how about the first one.

Is this close to correct, layer five of The OSI model? Transport there ye all right
 that leaves us with ifset cannot be implemented unless you configure specific
application supports really I don't think.

I think it's designed to encrypt all IP traffic regardless of the application that really leaves us with Choice D is the correct answer IPSec is commonly used when running a VPN.

All right.

Listening port

You are tasked with setting up a web application load balancer to handle all incoming client connections and serve web content to all clients via TLS certificate. The web app sessions are all TLS terminated at the load balancer and farmed out to the back end web app web head servers over port 8080.

What is the main listening port your load balancer needs to be listing on and we have some responses coming in.

We have a vote for 443, one for 445 any other responses
443 is the correct answer. Port 443 uses SSL and TLS

Port 80. and 81 I'd say would probably be the
most likely obvious and correct answers; 445 is used by Microsoft directory services for active
directory and for servers server message block.

Port 81 used by specialized web servers that are avoiding Port 80 for reasons like testing websites.
443 is the correct answer here.
This question involves salting. How would adding assault to a stored password frustrate an attacker who’s trying to crack your password?

Let's take a moment and look over the responses and see what you're thinking.

We have some responses.

and the response is …
the second one B
the second one and that's that's pretty much everybody's consensus and that is correct

by adding a random value to the plain text input of a hashing algorithm the attacker
cannot use pre-computed tables of hashes.The first answer, by slowing them down when you
when you put an initial key that's generated from the user password to thousands of rounds
of hasing. Yeah? No.

Three - The third choice by combining the password hash with a shared secret to strengthen the password Integrity making it impossible to Decrypt…
Hmmmm, no, and by including signs and warnings of legal penalties against password cracking and I don't think that's going to be a really big deterrent that one's obviously wrong
as well. All right very good everybody in this case it's just it's one of the ones like the other
ones where it just it's a knowledge-based question.

So pretty much you have to understand what salting is and how hashing works and then adding the salt value definitely Takes it to a new level of difficulty.

I also would note that I tend to shy away from things or saying things like impossible to decrypt mostly it's a game of resources, computing power, and time.

The one that stuck out and this one for me was none of the other ones used the word value and I know that it had something to do with adding values and random values. You really do have to look at the language in the both the question but also in the responses.

To see if you can see something that doesn't belong or which of these things is not like the others, all of these little tests that you can use to help you.

I think it's equally important to be able to do that because I think anybody can get rattled in an exam. I think back to some personal experiences I've had, I remember
when this was years ago but it was probably I guess the third time that I had to test to
re-up my CCNA and at this particular incident I had gone to a Pearn VUE testing center and
it's funny and and I don’t really have a good reason for it but I just never expected that
someone would be in there and perhaps not testing for an IT certification and I don't know maybe I was just focused on recertifying my CCNA and I was probably halfway through the
certification exam and another person had come into the room and they were sitting not
close to me but within a very short amount of time.

I couldn't help but hear them typing madly I would describe it on the keyboard I'm also quite loudly like I guess they were striking the keys on the

keyboard pretty aggressively. and it was nearly non-stop and I I would catch myself listening to it or maybe even getting a little annoyed by it and I think once I even looked over and from what I could tell just by a quick glance this person was typing an essay and like I said it just didn't dawn on me that you might have somebody coming in there to est out and maybe their test was to type up several pages of narrative and I really had to fight to get my focus back for for a couple of minutes and I guess I was a little surprised at how much it kind of set me off of my game and that it actually took me two to three minutes maybe two minutes probably no more than that but that's still two minutes to refocus on on what I was looking at and it was more of a performance type of question and the lesson there obviously is to try not to be distracted and to try to to stay focused when you are negotiating questions that perhaps don't require a lot of time to answer maybe it's something like the true false question we saw I think in the last session or maybe a straight-up knowledge-based question if you can answer it and say 20 seconds maybe even less if it's just like like I said like a true false that gives you perhaps another 45 seconds to put back in the time bank that when you do approach a question that maybe is performance related and could take you a minute or maybe a little more you have that extra time and I've learned and trained myself to think about it in these terms.

Just because for me no matter how much money I have into it it's still running out of my pocket and I have a little bit of a sense of pride I've never failed a certification exam. I've always passed on the first attempt but I generally tend to over prepare for them if there is such a thing but that that particular experience really kind of threw me for a minute and really made me come to the understanding that people are there for lots of different reasons and not just reading questions like we're doing and then choosing correct one or more correct answers from the list.

Now let's go to the next one.

Types of Hardware II

Which type of hardware is needed if you must perform centralized public key infrastructure management for a network of devices?

What do you think?

We've got responses coming in.

It looks like everybody's selecting A and that is the correct answer.

Hardware security modules - something obviously incorrect when the answer choice is shown.
Blockchain?
Blockchain. Yeah. Sniper is an automated scanner that can be used during the penetration test to generate and scan for vulnerabilities.

the password vaults or password manager or password locker is a program that stores usernames and passwords for multiple applications securely and in an encrypted format.
Yes, HSM.

Next question

Digital signature and decryption: Creating a digital signature and decrypting a message both utilize which of the following (and you're instructed to choose the best single answer).

We have some responses coming in

We have votes for C

Anything else?

What would you say is obviously or the most obvious incorrect answers here?

Private keys.
Which? symmetric?

Go ahead
I was thinking both
So, with symmetric keys you have two disadvantages

In using symmetric encryption and that is how do you communicate the key to the party who
needs it to decrypt the message. You must ensure that whatever you whatever way you communicate it the key is sent in a secure manner and that makes it tough. Both for C
Asymmetric encryption is used in key exchange
email security web security and other encryption systems that require key exchange over the public Network. Two keys - public and private cannot be derived to the public; the public key
can be freely distributed without confidentially being compromised.
Anybody changing their answer ?
How about asymmetric private keys?
All right, let's see what we have here.
C
Why do you think C?

Uh I I didn't quite get the public and private part The public and private part, yeah, a asymmetric private key not a public key because right the private keys held by the owner
of the data messages are encrypted with the recipient's public key the messages
encrypted by the recipient with their private key The correct answer is asymmetric
private keys.

Next question

Digital signature - What is a digital signature?

What are you thinking?

Responses coming in.

We have lots of people saying A, a plain text string that is hashed using a private key Anything obviously incorrect?

Anything stating public key
All right.

That leaves us then with a plain text string that is hashed using a private key or a hash that is in that is then encrypted using a private key

Yeah it's B.
It is the correct answer: B.
A hash that is then encrypted using a private key.