Good evening everybody and
welcome to this review session.
The topic tonight is internet encryption part two and we are going to
start with POP3S.
I'll go ahead and read the question,
give everybody a little bit of time to take a
look at the responses and then we're going to go
ahead and see what you think is the right answer.

We'll move on and proceed that way: So you have
just interviewed for a new position and you got
the job the HR manager told you to check with
your to check your email with instructions on the
next steps. So you log into your email account once
connected to your email server what does POP3S do?

Please take a moment look over these
responses and then we will see what you think.
You can go ahead and put responses in the chat
or you can use your microphone if you wish.
So we have some responses
coming in and we have a vote for A and
two votes for C. So looking at
the responses take a look at the port numbers.
Does that help you?

Yes.
Now let's see. Another vote it's definitely not
D because POP3S is not called secure post
office protocol. And another vote for C.
So POP3S uses the TCP protocol on
port number, which. We have two choices here.
I was thinking it wasn't 110 because POP3 uses 110.
So if it's S it would use a different port that is
absolutely correct it is TCP over Port 995.
So that's your first step in sort of you know
discarding at least one of the answers and then
we want to look at the other three choices which
you know the first one kind of stands out because
Port 995 is what we're looking for but you still
want to read the other choices and make sure
that there's nothing in there and of course you
want to read the first choice so POP3S enables a
client to securely access email messages stored
in a mailbox on a remote server via TCP Port
995 by default. In the second
POP3S client application securely deletes the
contents of his or her mailbox for improved
processing on the local PC before the user is
authenticated. What do you think about that choice?

I was thinking it's a little extreme
because of the question about checking

a mailbox.
Yeah so Choice B is eliminated as well as Choice C that really leaves us with A and D or the first and the last. The secure post office protocol version three receives email message from an email server to store on a cloud application.
00:04:42.120 --> 00:04:45.840
Does that do anything to change everybody's thinking?
What do you think? First choice or Last choice?
Yeah we got votes for A and that is in fact the correct answer. So once again the importance of knowing port numbers and a little bit about the protocols involved as well.
Also you should know that POP3, not secure but POP3 - does not synchronize between sender and receiver so once POP3 retrieves emails from an email server, the email server will delete the emails.

And they're probably throwing that in there to use this one as a misdirector

38
00:05:54.660 --> 00:05:55.260

39
00:05:57.960 --> 00:05:58.980
Next question.

40
00:06:03.660 --> 00:06:12.180
Remote access VM - What type of connection concentrator would you use to gain remote access to your cloud VMs from your corporate network?
So you don't need to give your Cloud VMs public IP addresses and in this one you're asked to choose all of the answers that apply. Please take take a moment and look over the responses.
Let's see what everybody's thinking here; so we've got responses in the chat.
So it looks like we have a lot of VPN responses so we can check that.
What do you think about HSM? What is HSN?
Anybody?

Is it a hardware security module?
Yes it is.

So probably doesn't really qualify it as a connection concentrator. That leaves

forward web proxy or Jump Box.
So if we don't
think it's the second choice
that leaves us with the first and
fourth. So what are you thinking?

Since it's a choose all that apply obviously you
know there's going to be more than one choice.
Sometimes in fact most of the time I think it's
important to remember that you're looking
for the best answer or best answers.

Personally I'm not familiar with a Jump Box so this…
Is Jump Box the same as like
bastion?
Not exactly no; the Jump Box
also is sometimes known as a jump server
allows access to endpoints on a remote
land from a local connection where you are.
How about the forward proxy?
Because that's going to retrieve data right
perhaps hold on to it so that really doesn't
fit the description of a connection concentrator
and that really leaves us with the two best
answers being Jump Box and VPN hardware security
module is a network device. Let's see we have
another response here Jump Box. So, the correct answers here are VPN and
Jump Box.

Let’s move on.

Server Configuration.
Oh boy, this is one of those long ones.
This is also probably a good time to remind
everybody to A - read questions very carefully
B - read them twice. It's always important
to know what you're being asked for.
You have your critical customer web servers
running Linux in your DMZ open to the internet
and the web admin group insists on being
able to log into these systems as root by
a SSH from home over the internet. Also
customer data is stored unencrypted on a disk.
As the corporate security lead you've been tasked
with ensuring that these servers are hardened.
which of the following server config
ideas could you propose to be enforced
to increase the security profile of these
web servers and mitigate against customer
data loss from many intrusions? And this we're asked to take to choose
two answers.
So what do you see that can
be eliminated fairly straight away?
Second answer

This one?

So
if I look at these proposed answers when I see
Port map SSH Port 23 to a non-standard port
etc etc I really don't need to read
much Beyond Port 23. Why is that?
Yeah eliminate B and C
SSH is 22.
That is correct. 23
is telnet so that really isn't going to do us
any good here. You know it just so happens thatand I've seen this happen
you know it does happen where perhaps you know two out of four answers
are eliminated right off the bat and if you have
to choose more than one that leaves the other two.
So portmap SSH ports 22 to a non-standard port on
the DMZ firewall; Enforce long username pass phrases;
Force the move of customer files on
disk into a locally encrypted database.

So these all sound like techniques that meet
the requirements put forth in the question.
If you want the admins to
be able to log in as root by SSH
the question says straight up customer data is
stored unencrypted not the best of ideas probably
You've been tasked with ensuring that the
servers are hardened and you want to increase
the security profile and protect customer
data so the first choice ticks the boxes.

The last choice on the DMZ firewall, DNAT the web
admin home IPS to allow SSH only from those IPs
and that is destination net or network address
Translation. Enforce dual factor authentication for
all server logons logins and migrate the customer
files to a separate secure database server -
those suggestions tick the Box so we are left
with the first and the fourth choices here
as the best answers or the best solutions
to the scenario posed in this question.

Just gonna put this up here for a moment
and you can see it looks pretty much like
a pretty standard options UI with choices for
protocol and ports and so forth. I don't know that
we necessarily need this to answer the question
so I'm going to get rid of that.
You are
configuring a WAN/LAN firewall router
to accept and forward all incoming email traffic
for your MX server traffic from the internet
to your internal email server on 192.168.2.100
in your DMZ. What originating port protocol and

forward to port do you need to configure for

this to work? Please take a moment and look
at these choices and when you're ready pick one.

So what's the obvious one to eliminate?
Response in a chat. Port 80 not what we're looking for
so that leaves us with B, C and D
Let's see what we have in response
and that's the one to eliminate - so uh B, C and D
Do you see any others that are
obvious to eliminate or maybe not so obvious?
Well clearly this is going to take
some knowledge of port numbers
so what are we talking about with Port 25?
That's an MTP.
How about 143?
We have some responses in the chat. It's
interviewing yeah 143 yes 143 with question marks.
so IMF, yes?
One other thing to look at is the protocol; can
you eliminate another answer based on the protocol?
Well when can you eliminate B yeah it would
eliminate the UDP is not used so once we've
gone through that little mental exercise that
leaves us with choices C and D and when
email is delivered servers communicate using
TCP over port 25. So as we've already
mentioned UDP is not going to be used Port 80
and also 143 which is IMAP is not used in the
context of an email gateway. So that really
leaves us with Choice D as the correct answer.
so there's mention here in the
question of MX server traffic.
What do you think they're getting at?

So if you kind of dig into this a little
bit at least my interpretation.
is that we're talking about records MX records
as opposed to a records in DNS and so they are
useful because the MX record record differentiates
between for example web and email servers.
So further clue there.
Let's go on to the next question.
FDE
Jenny has a Windows laptop that contains a
single disk that holds the system files and data.
She would like to be to enable full
disk encryption on her computer
but her TPM has been damaged. What should
Jenny configure if she is still required
to store the cryptographic key securely so
acronyms which never ever go away. What is TPM?
trusted platform module?

Yes, very good.

However in the scenario the TPM has been
damaged so now we have to figure out
how the goal can be accomplished of
storing the cryptographic key securely.
So the first thing again and I always tend to
do this and I think most people would take the
test too you look at something that is either
obviously wrong or probably wrong. We got
responses in the chat.
So I know VPN is not it.
Yeah I know everybody in there
everybody had said C and that's correct
so apparently we have lots of Windows users.
BitLocker is is not going to work. Let's see TPM 1.2 or better is
required.
VPN not really making too much sense for what
we're trying to do which is store cryptographic
key securely and a firewall that will filter
unauthorized people from accessing the key; that's
kind of a silly answer so it really does leave us
your choice C.
Let's move on to the next one
and it seems to be hiding somewhere.

Here we go: IoT Devices: You need to allow
internet connection and management of an embedded
IoT device on your internal network, but you
don't want to expose standard ports to the
open internet. What type of router slash
firewall configuration allows for this?
Take a moment look at our
choices let's see what you think.
So once again we're
looking for something that's
that can be easily eliminated or
fairly at least easily eliminated.
We have some responses in the chat and
I see two responses for C is that what
you think can be easily eliminated or is that
what you think we need to do for this question?
C is the answer.

And let's see we have another response
eliminate A that's that's very interesting.
If we were going to choose something obvious
to eliminate anybody have a suggestion there
We have a response in the chat
B - oh that's really interesting
So I would have said D - Port encapsulation. When I think about
encapsulating a port I think
of things like trunking encapsulations like
802.1 Q which really doesn't do much for us.

You know stateful packet inspection
I don't think that fits the bill either.
So let's say we're left with
port forwarding and DNET
So destination, NAT - or network address
translations - translates destination IP addresses
usually of internal devices protected by
the device to public IP addresses. We want
to allow an internet connection and management of
an embedded IoT device on your internal network.
So what we're really talking about here is…..
Let's see we have something in the chat.
A - port forwarding. Support forwarding MAPs
external IP addresses and ports to internal
IP addresses and ports allowing access
to internal services from the internet.
There's a fairly popular example
of this; does anybody know what it is?

Maybe something you'd like
to do in your spare time?
Which sadly I don't have enough of but
if I did I might play a few more games.
Right and I might have to
do some port mapping there
report forwarding at least I think that's the
the popular use of this. As I said I haven't
had too much time to play lately but maybe
this summer. Let's move on to the next one.
We have a question on reconnaissance - A
threat actor is looking for ways to penetrate
an organization's network. Their first step is to
perform reconnaissance where they try to discover
which network services are open that shouldn't be.
Which tools should they use to carry out this step?

So we got some responses in the chat pretty
quickly so let's see what you're thinking.
Wow, it looks like everybody's thinking Choice
C. So, yes, that is the overwhelming choice and it is
absolutely correct. Protocol analyzer is
not going to help, right. We are looking for
ports that are open and services that are open
that should not be. These represent vulnerabilities
that can be exploited. Port scanner
is the tool you're looking for.
Protocol analyzers really just
capture transmittal traffic.
And open source intelligence - that's
not really what we're looking for here.
Vulnerability scanners - these can give us the
information we're looking for they are sometimes
a bit more intrusive and because
the question mentions reconnaissance

the implication is that the threat
actor is at this point still trying
to remain unnoticed or at least as much as
poss possible so really the best choice

the best answer for this question is Port
Scanner.
Let's move to the next question.
SNMP version three encryption algorithm - You are required to add
encryption support to your SNMP
version 3 implementation. Which of the following
encryption algorithms are you able to use?
Choose two.
So what's what's obviously
not a good choice here.
Maybe 3DES?
3DES.
I see we have some responses in the
Chat.
C and D are the answers.
I think the obvious one to eliminate is MD5.
Why is that?
Because MD5 is old compared to SHA-256.
It is and it is very very easily broken. It is as you as
you know yeah a one-way hashing algorithm
so we can eliminate that right off the bat.
We're talking about encryption so
we have advanced encryption standard
maybe as an answer that sticks out
as being correct? what do you think?
Does anybody agree with that?
Yes, so we'll choose that one. We'll
eliminate the second choice that leaves
us with SHA-256 and 3DES.
256 because it's a hashing algorithm?
Yeah, secure hash algorithm. Yeah, I've probably eliminated for
that when they specifically ask about encryption
and also triple data encryption standard
is also widely used and it's a fact that
currently SNMP version 3 supports both of these
so yeah those would be my two
choices and I believe they are the correct choices.
We can take a look at what Cyber
Range thinks - Let’s test it out here.
We have chosen wisely.
SNMPv3 encryption algorithm - Simple Network Management
Protocol version three
Very important protocol.

So let's move on to the next question

Transport layer - This is nice
when this happens by the way you get nice

222
00:33:51.420 --> 00:33:56.580
easy questions. Which of the following
is true regarding the transport layer?
I can tell you right now on the B and C are
incorrect.
Yeah, it’s not layer seven. What
is layer seven in the OSI model?
Application
And so yes that is not correct. So this choice is
not correct and the last choice that says no
options are correct. I don't buy that either.
It’s the first choice - transport
layer involves port numbers
and I guess while we're we're on this topic
here and and you can do this however you wish
for questions that involve memorization of
several related items such as the OSI model
it's nice to have a mnemonic
device to help you with this.
and you've probably heard this before but it bears
out mentioning if you're trying to remember
the layers of the OSI model. One of the
ones used is from the top down actually from
layer seven to the bottom and that is
All People Seem to Need Data Processing.
And so the first letter of each of those
happen - application presentation
session transport network data link and physical.
And then let's see there's another one
that comes to mind: Please Do Not Throw Sausage Pizza Away.
That's from the bottom up but whatever works
for you. Let’s move on to the next question.

Registry access:

Your developers have written an application
called Finance1 that runs on a domain joined
Windows Server called Server10. When Finance1
 runs it writes to a specific registry team
you need to allow this app to access writing
to the registry how should you accomplish this??
and of course the first thing that
comes to my mind is very very carefully.
Take a look at choices and
let's see what you're thinking.
As usual looking for something
that's easily eliminated
at least one
Eliminate A
because it's an executable file.
No, I don't think I do that are. You’re referring to using regedit.exe
Yeah so now I wouldn't eliminate A
B yeah yeah it kind of doesn’t make sense for me

And maybe I've just been lucky enough to get
burned a few times by messing with the registry
not terribly bad though I always back it up of
course but the last answer D set server
tends registry to be World writable I don't even
like the way that sounds right yeah not even close.
It sounds absolutely like a disaster waiting to happen
Let's see choice C set up a scheduled
job to drop access to the registry
for only the time that Finance1 runs, I
mean that's that's impractical that's really
not a good choice so create a registry entry to
store Finance1's password yeah I don't think
so the the correct answer here is in fact a create
a service account for Finance1 and assign the
account the appropriate registry permissions
and it is done using regenerative.
it's it doesn't really necessarily have anything
to do with you know you're using a Microsoft
operating system or whatever it is you're using
but when you were going to do things that involved
changes to critical components especially
of things like operating systems
You always t to play by the
rules and typically the rules
of you know in this case Microsoft
so yeah A is the correct answer here.

Let's move on to the next question:

IPSec - How do
the IPSec tunnel mode and transport mode
relate to each other? Take a moment, look at
your choices let's see what you're thinking.
So we have some responses in the chat. Let's
see we have votes for answer C.
Tunnel mode encapsulates the original IP
packets and transport mode encrypts payload data
and this is the correct answer for this question.
if we look at the first, both utilized router
implementation and that's really not true.
Tunnel mode is commonly used between gateways
transport mode is more of an end-to-end and you
know I suppose a Gateway could be involved if it
was considered a host but that's not usual
and then let's see both ad and authentication
header after the IP header and that is incorrect.

Actually the do a little research to
remember this it's placed before the IP header
and then tunnel mode is used to secure
Communications between hosts on a private network
and transport is used for communication
between VPN gateways and it's the opposite

so that's incorrect so yeah C is the
correct answer here.

Next question - Salting - how would adding a salt to a
stored password prostrate an attacker who's trying

to crack your password. Go ahead and take a couple
of seconds or a minute here and look this over.
Let's see what you think.
Thanks.

We have more responses in the chat.
So uh looks like several folks have IPs
right out with the correct answer which is B by
adding a random value to the plain text input
of a hashing algorithm so the attacker
cannot use pre-computed tables or patches
so slowing them down when you…
go ahead yes.
I didn't mean to disrupt I was
I just gonna ask you what does salting mean/
So it is in fact the act of adding random
values to the hashing algorithm so that you
know it just makes it that much more difficult for
someone to try to crack what you're hashing
In the first choice, slowing them down when
you put an initial key that's generated from
a user password to thousands of rounds
of hashing - now that doesn't make sense.
Combining the password hash with a shared
secret to strengthen the password and integrity
no no I'm not interested in shared secrets here
including signs and warnings of legal penalty
penalties so I guess at least this shows that
the test makers have this sense of honor. The
correct answer which we've already said is B is
in fact the definition of solving
and the next question.

Types of hardware-

Which type of Hardware is needed
if you must perform centralized
public key infrastructure
management for a network of devices?
Take a moment here
and look over these choices.

Now we've got some responses in the chat
and they are so overwhelmingly A
the group has selected A and Hardware security
module is correct. it’s a special trusted network
computational device that performs cryptographic
operations like key management or key exchange.

It is not blockchain - in fact the word
centralized just completely blows that
out of the water neither sniper or password
vaults. Let’s get rid of this.
And we have one more here to go over. This one is a rerun and oldie but a goody
Oh inappropriate too. Which type of
hardware is needed if you decide to
store digital certificates and cryptographic keys.
This one should be I think pretty
easy especially after this session
lots of responses I'm betting nobody said
A or B. Let’s take a look oh there it is it's
this is why we're here so we really
really wouldn't do this on a thUMb drive the
correct answer is trusted platform module
and I wanted to bring this one back because
if you know by now I mean I think we've seen
HSM and TPM and at least uh three questions maybe
maybe some more and hopefully this is really
solidifying the differences between the two.
So clearly one HSM is
a network device and TPM is not
On that subject especially since it
may come up remember that BitLocker uses it
and if I remember correctly I believe one of
the requirements for upgrading to Windows 11 was
that you needed TPM 2.0
module if I remember correctly
Then, so, that’s it for the questions for Part II.