Hey, well, good evening everyone and thank
you for joining us for this review session.

We are going to be using questions from the
Virginia Cyber Range, questions specifically
geared toward helping you review for the
Security+ certification exam.

I'm going to read the question and
see what your responses are and we'll have a
brief discussion and then proceed in that manner.

So the first question involves testing suspicious
Code. Tonight's topic is host-based security
and the first question is testing suspicious
code so: _____ is/are employed when security
engineers intentionally limit network
or system access to conduct tests and
ensure that suspicious code is not infected
with malware.
So what are we talking about?

Anybody wanna go first? We have something
in the chat: We have a vote for sandboxing.

Any other choices?
I agree.
So we've got agreement.
So sandboxing it is. Non-persistence does not really fit
in this in this situation; non-persistence is
a way of using protected information as required.
It's also a state where transmission of data is
terminated periodically or at the end of a session
so that doesn't really fit the bill for
this question. Intrusion prevention systems
are a network security tool and that can be
hardware/software that continuously monitor for
malicious activity and take action to prevent it
including reporting locking, dropping, minor curves.

And endpoint protection involves monitoring
and protecting endpoints against cyber threats
and of course endpoints are resources such as
workstations and smartphones tablets etc.

So sandboxing is really the
correct answer here.

Now let's go on to the next question.
This question is security solutions.
The network administrator has deployed a security
host-based agent that can detect incoming port
scams and block all traffic from the attack
scans. What security solution have they most

likely implemented. Let's
see what we have. What do you guys think?

There's something in the chat. NIPS, all right.
Others?
So we have one vote for Network intrusion,
and an agreement with network
intrusion and then we have PIDS.

So what is that?
Anybody?
So we're talking about
physical intrusion detection.
Any other responses?

We've got something here in agreement
with network intrusion. So this is a
security post-based agent that is… go ahead…
I don't know host based HRPS so not perimeter not Network it's host
based because you said host basic HRPS yeah
the network security The network administrator
has deployed a security host-based agent to detect
incoming port scans and block traffic so this is
not going to be wireless intrusion and as several
of you have already said; this is host-based so the
correct answer is post intrusion prevention system.

When you take this exam you definitely
need to make sure you read the questions twice
and look for clues in the question but also
information in the question that can lead you to
obviously incorrect answers. Most of the time
you'll come across questions where there will
be at least one obviously incorrect or maybe
somewhat obvious there may also be misdirectors
which look close to being the answer like
they could be but they're not all right.

Next question:

NFC - So we're talking about
acronyms. Why? Because they love acronyms.
So what is NFC? Does anybody know?
Near-field communication.
Absolutely. Which of the following is
true about Near-field communications? You are asked
to choose all that apply so your choices: NFC
provides encryption; Based on RFID technology; Has
a close physical proximity requirement; Supports
tap payments with mobile wallet apps.
Is there anything that jumps out as obviously incorrect?

We have something in the chat.
Anyone?

I'm not sure it provides encryption
but all the rest I would agree with.
Yeah and that's correct right; it is based on RFID;
close physical proximity; and supports
half payments with mobile wallet apps
NFC uses or can use encryption; it
does not provide it.

All right

Next question - Farming data project

As an IT engineer, you're asked to assist
with a rural farming data project in the
middle of a cornfield with no wired
internet telephone or electrical power.
The wireless phone signal is poor and unreliable
you plan on using a medium-sized solar panel
and battery to run your project's small
electronics and wireless data backhaul.

Which internet data connectivity technologies should you think about
using
for that data backhaul part of the setup? And
again you're asked to choose all that apply.
So here again and this is is often typical
of questions and certification exams from
many different providers. Is there
something that is obviously not correct.

I'm sorry, say again.
DSL. I forget now.
So, that’s wrong. We’re in the middle of a cornfield,
no wired internet, telephone, or electrical
Power. Is it likely we're going to be using a cable?
Probably not. So one of the things, one of the
technologies we could use is satellite network
and the other correct answer is going
to be wireless provider signal booster.

In the question the wireless
phone signal is poor and unreliable however
it's still there.
If we don't choose both of those, does that mean that we get
the whole problem, the whole question, wrong?
Do we not get any points for it?

Yeah, typically and
I can't say this with certainty because testing
protocols are kept proprietary, but it's been my
experience and not just with CompTIA but also
Cisco that credit is given for a partial answer
or is somehow figured into the final
score but that's me speaking

from personal experience; that's
not me speaking officially for CompTIA.
All right.

Here’s an oldie but goodie. This question deals with Stuxnet.

What part of Stuxnet made it unlike any
other virus or worm that came before?
Take a moment and the choices
and let's let's take a response.
So of all the choices,
which do you think it is?
Let's check the chat here.
The last one? The first one? D?
It looks like we have two votes for the last answer choice. It
was the first digital weapon that escaped the
digital realm and that is the correct answer.
So the situation…let’s see what else we have here.
00:13:39.300 --> 00:13:47.400
So Stuxnet attacked all layers of target
infrastructure so operating system Windows,
Siemens software, and of course that software
controlled PLC's - programmable logic controllers -
and the embedded software on the PLCs themselves;
was designed to be delivered by a removable device
like a USB stick; and the facility where this
malware really was released on the Natanz
facility was known to be or thought to be air-
gapped so in other words its systems
were not connected to the internet.

And this particular worm was also designed
to spread quickly and sort of indiscriminately
and I think we all know that the
result was pretty much what was expected.

Let's go on to the next question.

So this question involves the term Rooting
and basically: Which of the following relates to
or is related to the term rooting? Again
you're asked to choose all that apply
So this is not really a performance-based question.
This is more of a knowledge-based question.

To successfully negotiate this you have
to understand what the term rooting means.
00:15:42.360 --> 00:15:44.520
So what is everybody thinking?

We have something in the chat:
Shellcode and python. Two and four.

So rooting is another term for:

Let's see we have more choices here
Shellcode. If I tell you that rooting is also
known as jailbreaking does that help?
Oh, yes.
iPhone users? Yeah.
And Android devices.
That's right.

So it's important to note that questions
like this come up and oftentimes rely on
you understanding of terms such as rooting
but also understanding the term means.
Knowing what an alternative version of the term
may be and acronyms and I can't say this enough:
They love acronyms. Now I get it. Every
profession has its language and acronyms are
important but it's just a good idea to
be well prepared for this and there are
many ways that you can do it: flash cards
in any form can be particularly effective.
One of the more fun ways to deal with this
if you're so motivated would be to download
Jeopardy template, the game Jeopardy template for
PowerPoint, off the internet and they’re
many places and it can be downloaded
at no charge and you can set up acronyms and make
a game out of it but you're going to have to
deal with it at some point. I often find that
being able to do something with knowledge-based
questions or acronym-based questions \
helps me to remember better. I really don't
like staring at a page and trying t
memorize items I'd rather do something with it
because it enables me to learn more naturally
and just the act of setting
this thing up as a PowerPoint game
is going to sort of enable this
long-term learning for you all right here.

All right.

So this question involves internet
Connectivity.
Blake just moved into a new
house where he is going to be spending a lot of
his time working from home. He has to immediately
get back to working having no time to wait for
his internet provider to set up his home router.

The problem is that Blake needs to run a drafting
application on his desktop OS computer and can't
use a mobile device but his desktop has no Wi-Fi
just ethernet and USB. What is the most secure

and efficient way Blake can achieve internet
connectivity on his home office desktop computer?
Take a moment look at the answer
choices and let's see what you're thinking.
Oh overwhelming, great, excellent. Tethering.
Very good, very good. So, yeah, asking the
co-worker to do tests. Yeah I don't think so. No,
How about the next door neighbor? No. Could you do it? Maybe.
There’s going to be lots of security problems there and there's no Wi-fi
so hot spots are out.
]
Good, all right.

So, now we're going to talk about device
Management. A large enterprise has multiple
stationary mobile and IoT devices on its
network that are used by its employees.
Which method do you recommend they apply in order
to manage the use of apps, corporate data, and
settings for all of these devices? Would it be
the second option? the smartest choice
You mean unified endpoint management?
Yes.
Yes that is it.
I agree.
The simple network management protocol - does that stand out as sort of
one of the obviously wrong answers?
And patch management.Yeah, not what we’re looking for.
Windows management
administration - this is specifications from
Microsoft for consolidating the management of
devices and application in a network from Windows
Computing systems and we have a host of systems
here so basically we're talking about unified
endpoint management. Very good all right.

The next question - Security Solutions

How can you instantly mitigate the risk
of receiving images embedded with malicious
code for your smartphone's texting app?
Disable MMS.
So I think then it's pretty clear and it looks like
lots of people got this. Images
in short message service right I mean images
embedded with code what does that sound like
Sarah, particular technique that's malware I know
it I just can't remember it it starts with an s - Steganography.

So the SMS answers then again pressing
that you understand what SMS is.
Those are going to be the obvious and standout
incorrect answers and since we are trying to

mitigate the risk of receiving images we're not
going to be enabling MMS we're going to be
disabling it all right so multimedia disable
multimedia is the correct answer for this question
Next question.
Hi, Michael. What was the answer to that last
question? I'm sorry it seemed like it went really
Fast.
Yes I'm sorry.

Messaging capabilities yeah thank
you you're welcome. Listen. Thank you.
We're at RFID
Which of the following is true regarding
RFID? And here we are with the acronyms
again RFID stands for router frequency ID.
That's the last one
Examples of RFID our UPC barcodes and QR codes.
No.
Let’s talk about RF what does that stand for? Radio
frequency ID.
Sure.
So we're talking about radio waves. The last choice is optical
RFID encodes information into stationary
Devices.
Does that sound right?
No.

Go ahead it's the second one.
So choice three could be considered from this
director but if you understand what an RFID is
this question is going to approach the solution
from the point of view of application of RFID.
And so you need to be prepared for that as
well it's still what I would consider knowledge
based as opposed to performance based but given
the other choices and especially that they're
for the most part obviously well received an
example of the right answer like in the real
World.
EasyPass?
Yeah, sure.
Well someone else can answer as well go ahead and I've got one too.
So I had the opportunity when I was doing my Master's to talk
to UPS drivers and we were talking about how the
trucks use RFID now this was a number of years ago
but and I don't know if they're
still doing this or not.
I don’t know if you followed it or anything but when the
trucks would pull in to the docking stations
there is RFID on them and of course when
you're in proximity to the receiver this lets
the information system know which truck has
just arrived and it starts off a whole chain

of processes about what may be on the truck, what has to be done next and so forth and so at the time that I was doing this and I'd spoken to the driver, UPS was making fair use of this technology.

Okay.

Thank you.

Healthcare Act. While a medical professional is doing an at-home check-in for their patient they use a cloud-hosting tablet to log all of their notes through the company's chosen healthcare app. This tablet has remote access to its cloud desktop and all of its applications what type of technology are they implementing? So, again you're kind of looking for anything that is wrong obviously incorrect.
Go ahead.
VPN?
Yeah so we have votes for VPN and one for BDI.

RDP is remote desktop protocol
How about DHCP?
It's another protocol
Yeah Dynamic Post Configuration. That's not what we're talking about so in the question the important information is cloud hosted tablet and then the tablet has remote access to its cloud desktop and that was thrown in on purpose and all of its applications so the technology being implemented here is virtual desktop infrastructure - VDI - not VPN.

I suppose VPN could be the misdirector of all of these answers but VDI is what we're looking for. That one was tricky. What does that stand for again?

Virtual Desktop Infrastructure.

So the next question biometric authentication. Which of the following are examples of biometric authentication and this time you're told to choose only two:
Fingerprint for one.
Gait.
It’s the way a person walks.
That's exactly right, so biometric authentication deals with what how would you describe it something that you are yeah you are yes absolutely

a pin something Smart Car Smart car is
something that you have I have something
you have fingerprints that's the easy one.
Gait. Here again, I don't know maybe
they just want to test your vocabulary skills
but a person's gait is the way they walk, the way they move and a lot of things can
affect it; certain medications that a person
may be taking can affect their gait, of course.

Some kind of physical problem can affect their
Gait. All right.
So that one was pretty easy.

Security Solutions. Which security
measure would you recommend for
administrators who want to be alerted
every time there is anomalous traffic or activity
on their network without the attacker being aware?

NIDS?
So everybody's on the network intrusion detection.
Yes. Anything else? So what's
wrong here? What's obviously wrong?
So when you see the word network right
then we're not talking about host intrusion.
So that's incorrect. What do you
guys think about the last choice?
We're not talking about storage - no
not at all - so again knowing the acronyms
those two are ruled out pretty much
right away. How about the third choice?
What is that?

So we're talking about
privileged access management
as an identity security solution that helps
protect organizations against cyber threat by
monitoring detecting and preventing unauthorized
privileged access to critical resources.
That could be considered the misdirector here
If we had to choose one but the correct answer - Network Intrusion Detection.

This one’s entitled PowerPoint: You and your co-worker are on the way to a work conference
While in the van you realize you need to share the
PowerPoint presentation with them for your speech.
if there is no Wi-fi connectivity on the van
and you only have the PowerPoint on your laptop
what is the most secure efficient and
cost-effective action you should take.
Take a moment look over your choices.
Yeah.

We have some responses in the chat: D, A, D. So it looks like people are gravitating
towards save the PowerPoint file to a thumb
drive or connect your laptops.

Choice one would not be considered efficient
use your personal smart phones hotspot to
email the PowerPoint. Is that a good choice?
There's no wi-fi though, but you said personal smartphone. Never mind.
So not secure and the fourth not really efficient
that leaves us with Implement Wi-Fi Direct.
Wi-Fi Direct is a connection that allows for
device to device communication linking devices
together without a nearby centralized network.
One device acts as an access point and the other
device connects to it using Wi-Fi protected setup
and Wi-Fi protective access security protocols
so Wi-Fi direct to transfer
the PowerPoint file is the choice.
I have a question.
Go ahead.
Is this also like for Apple devices like airdrop?
I believe it is. I'm not well versed
with Apple devices to be honest with you
but I think it's close .

Thank you.

Firmware elements.
You need to analyze the boot log of your PC to
ensure that there are no signs of compromise
like the presence of unsigned drivers if the PC
can only boot with trusted operating systems which
firmware elements are most likely cousin? Choose
Two. Take a moment and look your choices over.
Let's see what we have.
Two and four. TPM, UEFI.
So first of all what is firmware?
What do you think?
So let's talk about that and define
the term firmware - software that provides

Is it something like…

Say again please.
I'm gonna type it.
Let's take a look at the chat you got
there
Right programming and non-volatile
Memory…
So firmware is software that
provides basic machine instructions that
allow hardware to function and communicates

with other software running on a device.
Firmware provides low level
control for devices, hardware
sometimes known as embedded software.
So EAP is that something we would consider

What is EAP?
So EAP is Extensible Authentication Protocol.
is that a firmware element?
No, it's a protocol for wireless networks so that's out of the running.
How about HSM? Is that firmware?
What is HSM?
So HSM is not firmware. That is an
acronym for Hardware Security Module
which is a physical device that provides
extra security for sensitive data so that leaves us with UEFI, NTPM. So
unified extensible firmware interface
has the word firmware so again knowing your
acronyms is important and then TPM. What is TPM?
Trusted Platform Module. Yes, exactly and so
that is going to qualify as an acceptable answer.
What does UEFI stand for? I have
Unified Extensible Firmware Interface. Thank you
All right.
That leaves us with API.
Which of the following terms best describes
the API based process of substituting the
transmission of sensitive authentication or
authorization data with unique abstract signed
metadata in order to reference the original
information without compromising its security?
So the question is what are we describing here?
I have some responses coming into the chat
Let's see we have -
Hashing.
Encryption.
Hashing. Hmmmm.
So we are substituting the transmission of
sensitive authentication or authorization data
substituting it with unique
abstract signed metadata.
the goal is to reference the original
but without compromising its security.
So we have some more coming
into the chat. See what we have.
Ah, Token and D. Sure.
So the correct
answer here is tokenization and let's think
about this. Encryption vs. tokenization. What do you think is the
difference?
The substituting part ?
Which are you talking about?
Encryption

or tokenization.
What are we basically doing wrapping
the information so we're scrambling
sensitive data. This also implies more
than likely the use of keys to decrypt it.
Encryption equals scrambling
token equals substitute so tokenization involves
swapping sensitive data for a token that must then
be presented in order to retrieve the data without
using keys. Big difference. What
are we talking about here?

Is it when you and I could be wrong is it
when you put other data over that data like

data so you can't recognize what it is?
Yeah,
What's an application data masking?

Steganography

Something which protects sensitive data so
some common use cases the password
when you hide the password -h
When someone types a password
and a dots come up does that count?
Yeah, that enables the set the use
of a data set without exposing the real data so
if you're talking about every time
you hit a key you see a little star up here
on the screen yeah so that doesn't expose the real
data and it does present us with a type of token
other use cases could be things
like software testing or user training
Typically a way of creating a similar
version of data that can be used for purposes
such as software testing but yeah so
that's masking and what about hashing?
So if we talk about hashing we are talking
about it typically an algorithm for what we more
commonly would call a one-way function and it
takes some data as an input and then outputs
a single numeric value. Let’s see we have here
transferring the key to a string
so why would we use hashing what what
does it get us what does it do for us
password code
If I was going to talk about
one of the three basic tenants of cyber security
there we go - integrity

so the numeric value can be stored transmitted
it can be used to verify the Integrity of data
that was hashed and this is commonly

seen for example if you are downloading a
file something right perhaps an image maybe an
ISO image and oftentimes a hash is presented with
it so that you can check once you've downloaded
the data that the Integrity has been maintained

because the hash value is the same let's see
what else TCP Communications what about it

Jordan can you explain that a bit?
Utilizing hashing to verify Integrity.
Any other thoughts on this?
so again the correct answer is tokenization.