Okay good evening everybody and welcome to this review session on Network Security Part II. So I'm going to start with this question on network design:

There’s the questions, some answer choices, and then a diagram that I'm going to leave visible after we've gone through this and to have a little discussion and figure this one out. Okay so

Network Security Part II

Your organization needs to allow customer web clients to only access your company's front-end website while also allowing restricted access to the corporate LAN and DMZ to only authenticated employees Network admins and sys admins Respectively. What are the three technologies that need to be used for the three unlabeled network devices in the attached network diagram. All right so I'm going to roll this a little bit so we're going to be labeling based on these choices the blank areas in the diagram. Let me roll this up so we can get a good look at the diagram and I believe you can see that this is pretty simple we have the public untrusted network here. We have a device here at number three, we have a firewall, another device at number two, and something that's going to be located at this number one location. We have a DMZ with servers and the corporate land the private trusted Network and the idea here is we want to describe what technologies exist at location number one, number two, and number three. Okay

All right

okay so our choices are here and you can see there are several; in fact there are six without even or just taking a a minute to look these over.

All right so hopefully everybody can see the choices and part of the diagram and so we're looking for a technology that would be located first of all at location number one and you can see here there's kind of a direct connection from the untrusted network. So of the six choices each one of those has a choice listed and separated by commas; these would be the three choices in each of the six answer choices.

Anybody want to take a stab at what is in location
number one? Is it going to be a bastion host;
a jump host…
A VPN
VPN okay all right okay
VPN at number one, okay great, and looking at the diagram can anybody tell
me of the remaining two label devices that's
number two here and number three which of those
would be the bastion host? Number two or number
three?
Number three.
Okay, and why do you say that?
Does the bastion host not um have the direct
correlate color correlation to the internet?
Well there's a direct connection to the untrusted
network yes for the public network and it really
um does refer to um actually a military
fortification of bastion host and you know
it's specifically designed and configured to take
what gets thrown out of it let's put it that way
so number three is a representation of the bastion
host and that leaves the jump host at number two.
We did mention this in the last
session I think at least once and so
the jump host is a single point of entry between
in this case two segments the private or corporate
land as is noted there in the DMZ now between
these two different segments of the network
and basically or often privileged
resources on the network are kind of
hidden behind the jump host such that
users cannot access the resources directly

Okay from their workstations so you would need to
connect to the jump host to get at these resources
and you know sometimes this is also known as a
jump server you can see the terms interchanged
here so given this question answer Choice
D would be correct at location one is where
the VPN would be the jump host is location
two and the bastion host is location three.

All right.

Okay so there's a network design
question for you and let's see

Okay so now we go back into the CTF here
and we are going to have another question
on network design. So let's put this one up

Now this question also uses a diagram here which
pretty sure is the same one we

just looked at and it is okay
all right so it's this diagram again -
We have the public untrusted network,
we have the corporate or private
network, trusted network, and our DMZ.
In the attached enterprise network
diagram, general internet traffic comes
into the DMZ Network through the firewall while
authenticated sysadmin access to DMZ systems
is gained through device three. Let’s
bring that back here okay that's device three
The main web application running in the DMZ is a
LAMP stack mainly consisting of a headless Apache
web server, a headless Tomcat application server,
and headless MySQL DB server database server.
Given these facts what ports should you
allow through the firewall for customer use
and what admin ports will most likely be needed to
connect to DMZ systems from device three?
Okay, so…

We're going to take this just a little
bit a little piece at a time here. The answer choices do start with the
firewall
and the ports and then in the second part
of each answer choice is device three
and again we have some more port numbers.
Okay so the first thing we're being asked
is what ports should you allow through the
firewall for customer use? Let's show the picture
again okay all right and this is for customer use
So everybody take a
moment look at this diagram.

So we have front-end web servers okay
and as you would expect these are
going to be public facing servers.
So of the answer choices shown,
which of the four do you think identified ports
that we would want to allow through the firewall?
for customer use. I know these are kind of jammed
up together but Choice A is ports 22, 80 and 443
Choice B is ports 80 and 443.
Choice C is just Port 22 and Choice D is Port 80 and 443.
and we're just dealing with the
first question here about ports
that we should allow through the firewall for
customer use okay and again.
I’m confused.
Okay.

Can you ask a question or do you need
to see the diagram again would that help?
Response in the chat.

Okay all right so we're dealing only with the
first part which is what ports should you allow

through the firewall for customer use bring
the diagram back our front-end servers okay.
So what is Port 22? SSL?
Yes that's correct so is that typical no
customer access to the DMZ the answer is no.
So that means as far as that first part the first
question goes we can eliminate answer Choice C
you can also eliminate answer Choice A and that
leaves ports 80 and 443 when answer choice is
B and D so 80 as hopefully everybody knows
is HTTP that's the protocol; n443, https. Okay.
So looking now at the next question what admin
ports will most likely be needed to connect to DMZ
Systems from device three and then at this point
we'd have to figure out what these ports are and
Can we eliminate either A or D no or A or C We already kind of looked
at these and said Port 22 was not an acceptable
answer so actually those have been eliminated so
that is going to get us down to answer choices
b or d and one of those two could be eliminated
okay is everybody understand why I'm saying A and C are eliminated

Yes, Okay, good. Because in the
first part the first question
we had already determined and said that
Port 22 was not appropriate for use
for customer use through DMZ so we
eliminated ANC based on that first
choice and the first question that leaves B
and D and now we're interested in admin ports
will most likely be needed to connect to the
DMZ from device three. Here's the diagram again.
So let's see what we have under…we have D in the response okay all right
so
if we look at the answer choices for B we
see that at device three we have ports 25
80, 443 and 33.89 and an answer Choice
D we have Port 22 80. 443 and 3306.
so is there anything in these two choices
that point either to b or d for any reason?
I believe RDP is 33.89.
Yeah it is.
So I would say…
that's another one of those dangerous ones and
after a while you know you start to see the number
of port 3389 and you go, oh, remote desktop protocol
though hmm yeah you probably don't want
to take advantage of that. So, yeah, by the
process of elimination we get to answer Choice d
and 3306 is the default port for the classic
my sequel okay um so knowing again something

about the port numbers and protocols associated
with them really can help you narrow down the

answer to a question and that's why I wanted to
present it to you this way because you can see
that based on the first question we were able to
eliminate answer choices A and C pretty quickly.
Now that doesn't mean it's always going to be
like this but you know the procedure can be
used even with five or possibly six answers. Let’s see other things that
you should know.
LAMP stack so LAMP is an acronym - big
surprise there huh? - what does this stand for?
Then of course there's going to be
variations on it but does anybody know?
Linux Apache My sequel and PHP, as
in the programming language.
Let's move on to the next question.
Pinging an IP address - Alice and Bob
are practicing the ping command using
both of their own PCs. Alice is able to ping
Bob's computer using his actual IP address
but Bob is not able to ping Alice's computer using
her actual IP address. What is the most logical
explanation for this scenario?
Look over the answer choices and let's see what you're thinking.
We have a couple of responses in the chat.
A, B and D.
123
So does anything come to mind in terms
of being able to eliminate pretty quickly?
If we are considering intrusion prevention
systems and based upon the question the
scenario given to us you know I would be thinking
about host intrusion prevention system.
And so you know the HIPS inserts itself
between software applications and the kernel
and it focuses on behavior.
So does this scenario sound like we are
trying to monitor some type of behavior?
I mean intrusion prevention systems are
concerned with attack behavior.

Does the scenario sound like that's what we're talking about okay. We’ve
got some more responses here?
We're talking about testing for connectivity; we’re talking about pinging
now the question
and I I think this this comes up somewhat. I
will say this I will say that in my experience
test designers have learned to become more
specific over the years and have gotten really
good about the descriptions being you know correct
and not being open to too much interpretation and
I you know kind of think this is too so in

this context pinging is not an attack and if I
look at it that way that kind of eliminates
choice and answer choices C and D for me.
I just have to read the
scenario again and think about it
and that is you know they're both
practicing the use of the ping command.
Alice can ping Bob using his actual IP but
Bob can't ping Alice using her actual IP.
okay so of the choices A and B which
do you think is the correct choice?
Okay lots of responses that's great and B yeah
Alice is going to have more than likely than
that gateway configured on her her network.
When they talk about you know her actual IP
from her point of view, it
sounds like inside local okay.
From Bob's point of view that's outsider
not his point, I mean from his point of view.
To her remote network it's an outside address
and network address translation will hide
her inside the local address which more
than likely is going to be a private IP
address and it's translated as you should
know to a public or routable IP address.
So B answer Choice B is the correct one
Here. All right let's go on to the next one.

Screened subnet:

Which of the following is not
true regarding a screened subnet:

Take a moment and look over your choices.

Clearly this question depends on understanding
the meaning of the term screen subnet.
And let's see what people are thinking.
Okay, so C and D. Okay.
Okay so remember we are looking for which of
the following is not true and sometimes just by
putting this sort of the negative spin
you know asking what if something is not true
can make question more difficult for reasons of
what human nature I suppose um or maybe it's just
the way we're taught we're always taught to figure out what the correct answer is.
So it looks like we have a lot of votes for answer
Choice C, communication between hosts in the DMZ
and hosts on the LAN does not need to go through
a firewall and this in fact is the correct choice.
This is not true regarding a screen subnet; the
other items are true and basically a screen subnet

could also be known as a triple homed firewall. It's a network architecture that uses single
firewall with three interface. Typically the
public interface you have the connection to the
DMZ into the intranet okay so a screen subnet
offers two layers of firewall restrictions
Between the LAN and the internet yeah when users
connect to a corporate network through VPNs the

VPN appliances should be placed in a screen subnet
and a screen subnet divides the network into three
networks so these are all characteristics of
the screen sign in leaving answer. Choice C okay.
We're ready
Next question - hierarchical tracing:
The network security administrator
frequently audits certificate
infrastructure to ensure that only valid
certificates are being issued and trusted.
What method are they practicing if
they trace each CA that signs the
certificate up through the hierarchy
to the root CA? What do we call this?
Responses are in the chat. Okay. Very good, so that one
was pretty easy. Certificate chaining is the
correct answer.
What is credential harvesting?
In just a word or two what would you call that?
Anyone?
So it sounds like we're - yeah attack - sure
sometimes it's called password harvesting.
Stateful inspection does
not really fit this situation
and the certificate authority is
the trusted organization that issues
digital certificates so yeah certificate
chaining is the correct answer here.
Okay next question. What does
the MD5sum operation provide?
So clearly this depends on your
knowledge of MD5. What is it?
What stands out as obviously incorrect
or answers that can be easily eliminated?

A and B, yes, A and B. So that leaves us
with C and D so encoding or unidirectional hashing.
Well pretty sure by now it and
everybody knows that MD5 is a very
you know old hashing algorithm and
is quite easily broken there are apps
all over the place that can you know break
an md5 hash pretty quickly. So the correct
answer here is D unidirectional hashing
and that's pretty much what it is okay

Let's go on to the next question

Port mapping SSH traffic. You need to
add a rule to your corporate Network firewall
to portmap SSH traffic Port 22 from specific
admin home IPs what part of the firewall will
you be modifying. Okay take a few seconds and
let's get your responses and see what you think
I think this is uh fairly easy one and judging
by the responses coming in I think you do too
okay yeah so the answer is D here
Access Control lists.
Well it's nice to get an
easy question now and again
especially when there are lots of them.
Let's go on to the next.

Stateless firewall - Which of the following
describes a stateless type of firewall?
A few moments look over your answer choices.
So what can be fairly quickly eliminated
and it's got a vote for D as the answer let's
go back to answers that are easily eliminated.

What do you think?

I would eliminate A and B yep sure
this is stateless operation there.
is no tracking of individual sessions
no monitoring leaving us with C and D
C - a firewall that filters and can
restrict what users on the network May access
or D a firewall that tracks individual packets
without preserving previous Network sessions.
and so the best answer the one that fits the best is D
is the firewall that tracks individual packets
without preserving previous Network sessions okay
Let's go on to the next one.
TCP Port 636 - Which statement
below is true regarding TCP port
636? Okay, take second flip this over. I think
you can eliminate some answers pretty quickly.
Which of the answers
do you think is the correct choice?
Okay so we've got two choices tworesponses
and looks like d so far another one: D
I think it's pretty obvious here that
we can eliminate Choice a FTP, FTPS.
Should also be in your repertoire port numbers.

Just curious does anybody know which port
number is associated typically with that TPS?
Okay so it's 990.

All right so that leaves us with LDAP and LDAP-S. So again you know we're going to be sort of left with the the game of how well DNA report numbers
lightweight directory access protocol LDAP.
typically TCP over port 389 and secure is TCP
Port 636 so answer Choice D is the correct answer.
Next one.
Wi-Fi security your IT manager has
asked you to verify the security profile of the
Wi-Fi access points in your office so you plan to
look at several aspects of your wireless networks.
What are some of the top common vulnerabilities
you should first look for as to choose two.
I would expect by now that this is
a pretty simple one for most of us.

Common vulnerabilities
We've got several responses
B and C, B and C, B and C two and three.
Default admin passwords definitely
an open Wi-Fi networks okay
Now the question says what are some of the
topic common vulnerabilities you should first
Look for okay so you know it's not that MAC
address filtering couldn't be a problem
um but it's definitely going to require more
work to get in and look at MAC filtering lists.
The easiest and quickest things to see
are going to be default admin passwords
and open networks.
Let’s go on to the next question
Domain name - A startup business thinks that
they have found a way to cut some costs by
registering a domain name for a short period
and then deleting it repeatedly so that they
can avoid paying for the domain name expenses
in this example what term is being described?
So we're gonna give you the definition you give us
the term. That's the game here okay all
right what are you thinking A, B, C, or D?
Okay, D, D, D.
All right see what other choices we have
here; The C. The correct answer
is C - Domain kiting.
Hijacking type of attack, poisoning or DNS cache poisoning - you know we're
again an attack domain squatting, the practice
of buying a domain name for the sole purpose of
preventing someone else from getting it that's
domain squatting so domain kiting this is where
you're taking advantage of the grace period okay
so that is the correct answer for this question
Okay

Open source firewall - Which

of the following describes a
characteristic of an open source network firewall?
Okay all right let's say your response is in the
Chat. C, C, C, C. Okay so inexpensive sure that's the
correct answer. Ineffective that's wrong
wired open source firewalls can function as
lapse that can be deployed on hardware platforms
there's a software-based solution okay. So, yes, the

answer here is C inexpensive.
Next question: PKI Certificate Attributes.
Which of the following are included within a PKI
SSL TLS certificate? Choose all that apply.
Take a few moments look at the choices; let's see which ones you're thinking.
Okay all right so we have some responses
in the chat and two, three, four - A,B,C - all okay
All right let's take a few more and then we'll go through these
Okay all right see we got here: two
three and all okay so in the certificate
yes URL domain name or common name okay
What do you think - yes or no - certificate
authority reference is that part of a certificate?
Yeah it is okay great expiration date kind of
another important piece of information to know

Private Key….
What do you think? yes or no?
Okay maybe no private key is not stored
in the certificate, okay, so it's all but
answer Choice D here. Let's move on to the next one
Federated identity management control-

Which of the following describes a
federated identity management control?
Okay, so this depends on knowing what identity federation is or involves
as I look at these
responses and we look at the last one D an
authentication service that grants federal access
Okay so what we're seeing here
is uh somebody's sense of humor
so I'm going to eliminate this choice right
out of hand okay so of the first three choices
Which do you think we're looking
at for the correct answer?
Is federal federated identity management
concerned with audit specifications?
No, so that leaves us with B or C, a virtual item that contains
authorization data and is commonly used
in multi-factor authentication.
That's pretty suspicious
an authentication process that
trusts a third-party network authenticator to
grant access to another or different networks.

This is the answer that sounds a
lot like …What do you think?
One of the the big capabilities that Federated
identity management provides and
we like it generally speaking,
Single sign-on bravo absolutely
single sign-on capability okay

Let's go on to the next question
LAN Court Access

The network administrator for your organization
needs to configure a security method that allows
only specific devices to a port on the
LAN what method should they administer?
What method should they administer?
Some responses here: B, C and B.
More from Mac filtering okay so Mac filtering is
the correct answer NMAP and firewalls are tools
more than methods MAC filtering is a method. Source IP affinity it's also
known as simple persistence
so the best answer for this
question is MAC filtering all right.

One more:

Network Edge security solution - you've
been tasked with setting up a secure
fast multi-homed network edge security
solution that controls access to various
types of traffic into your network.
Which type of solution should you employ?
A few responses let's get a few more.
Let's see what you're thinking here.
All right so it doesn't look like anybody chose
C all right so that's good C is not correct
B is not correct it is being fact between A and D.
A bastion host provides remote access to
private networks from an external network
and I suspect that you understand what a hardware firewall is and does?
We're talking about answer A or D

it still looks like we've got a D One D in there

Okay so the correct Choice here is D, hardware
Firewall. Controls access to various types of
traffic into your network
The other thing to note about let's see
everybody a lot of people said hey bastion hosts
old remote access technology that doesn't really
work in sort of today's decentralized networks
Okay so it basically runs as a kind of a a
lockdown single purpose system if you will
so definitely not as usable or easily fitted

to the different types of situations that we would find in modern networks okay so the answer here again the hardware firewall

That does it for this session on network security part II.