Good evening and welcome. I am Dr Michael Mann and I'll be your instructor for this series on preparing for the Security Plus exam. This 12-session series is intended to help you review key material that will be covered on the CompTIA Security+ Exam through the use of practice questions developed by the Virginia Cyber Range. In this session we are going to focus on network security.

Let's get started so good evening everyone and and welcome we're going to be going over some review questions to help you prepare for the Security+ Exam Plus exam and tonight's topic … is network security so we're going to just go ahead and jp in and get started here. What you're looking at is the Virginia Cyber Range CTF interface and it's a Jeopardy style CTF so we'll start with our first question and this is on ARP poisoning.

The question is: In a corporate ethernet LAN which of the following could be used to prevent Lan ARP poisoning (and you need to choose two): static ARP entries; patching antivirus software; physical security; and firewalls?

Let's just open it up and see what you're thinking.

So we're talking about corporate ethernet local area Networks and ARP poisoning. ARP as you may recall is address resolution protocol and we're looking for ways to mitigate ARP poisoning. Does anybody have an initial thought from the five options listed?

Firewalls; ARP entries; static ARP entries. Anyone else? I was saying and the antivirus software you gotta guess so let's start with the first correct answer and that is going to be static ARP entries and you may uh recall that arp is a means for creating relations between IP and Mac addresses and the the whole process is dynamic normally, so uh static type of ARP entry really cannot be changed once it is manually entered and so that is going to be known by the person who does the entering of this static entry and the other thing that's important about this is that it doesn't age out and it can't be overwritten by a dynamic ARP entry and that makes it resistant to tampering so there's one other suggestion here that's correct it is not firewalls and it is not antivirus software so that leaves patching or physical security. What do you think?

I'm just taking a guess but would it be patching? No.
It's not patching; actually it's physical security and the reason for this
is that ARP poisoning would occur over a local area network and this is going to require close proximity to access the local area network and so good physical security is important to mitigating ARP poisoning attacks
 that's a might be a little unexpected at first but when you think about where these attacks take place and how they're implemented it starts to make more sense any questions or comments on this one
 let's go ahead and move on to the second question, so this question involves identical Networks, the scenario is you decide to go to your local library to work on some homework while trying to connect to the internet there you notice two identical local library Wi-Fi networks were not there previously which are the following best describes what you

should do in this situation your choices are choose either Network because the library is large and
probably just needs two routers to cover the whole building choose neither Network because one is probably a rogue access point choose both networks and see which one yields the fastest internet speed or choose neither because one is probably bluejacked agendas. What do you think?

I'm gonna say nber two - choose neither Network because one is probably a rogue access point.

Very good and that is correct the giveaway here is that the SSID that's appearing is identical in both CAses there are two that's a local library Wi-Fi and that's almost always going to be a sure sign that somebody is trying to get you to do the wrong thing basically just because the library is large yeah it doesn't necessarily mean or not mean that you don't need two routers but you know you're not going to have totally identical ssids it doesn't work that way the one choosing one to see if it has a faster internet speed than the other is kind of not the right answer in fact it's not the right answer it's not kind of it's not the right answer and then bluejacking is also incorrect so what we are basically looking at here is what we would call an evil twin attack and basically it's where a hacker operates a false access point so in the attempt to get you to associate with it all right doing good.

I have a question yes please bluejack can you explain that what a what is a bluejack

I'm sorry can you speak up a little bit please

yes can you explain what what is a bluejack
Buejack so that basically occurs when an attacker sends unsolicited unsolicited text messages to a Bluetooth device and so since you're on this you know Wi-Fi network and Bluetooth is more of a personal area network we would not be using
any type of Bluetooth technology to connect to the library's Network.

Let's move on to the next one
and the next topic Network intrusion detection: Why would your network administrator configure a signature based Network intrusion detection system?
Your choices are to authenticate users attempting to connect to
the network; to authorize what users are permitted to do on the network; to
automatically update for known malicious attack patterns or; to make sure that all zero day attacks are detected.

So as we head into this question when you look at the responses is there anything that sticks out as obviously incorrect? Yes, I'm going to say nber one.
Nber one and and why do you think that one's obviously wrong?
I'm sorry can you say that again please.Sorry I was talking to myself

Okay, that’s a good sense, a good feeling there because I think it's your previous studies kicking in and probably what's tipping you off is the word authenticate okay so there’s one other response that's pretty uh incorrect here. What I would call an obvious misdirector; anyone would it be the last one yes it would be and why do you think that would be the misdirector because it's talking about zero day attacks and that’s it has nothing to do with the network but no one has anything to do for network well zero day attacks I mean so when you consider that a zero day exploit is basically you know uh is a leveraging of zero day vulnerabilities and zero day vulnerabilities our vulnerabilities that are unknown to the vendor in the CAse of software say a software vendor so yeah there wouldn't be a signature yet and so the correct response for this question is the third choice to automatically update for known malicious attack patterns if it's a known malicious attack then the fact that it's known means that we have a signature base for this attack and so we can use that to our advantage okay so it really doesn't have anything to do with authenticating users or authorizing users so there’s the correct answer.

Let's move to the next one. This question involves open source firewalls which are the following describes a characteristic of an open source Network firewall your choices are wired Hardware inexpensive and ineffective.

What do you think about this one?
Inexpensive
That's correct. that is the correct answer the
actually it is the best answer so if we look at the rest of these suggested answers - What’s wrong with wired? is there a possibility it it could be wired it could be but open source firewalls can also function as wireless access points so wired is definitely not the best answer what about Hardware yeah
isn't that pertaining to like physical devices yes to an appliance for example and remember when we look at these questions and oftentimes you know
the the sort of implied instruction or sometimes it's very explicit is that you need to choose the best answer and the fact is it's not necessarily going to be a hardware Appliance. It can be - so what about ineffective? Doesn’t that just kind of sound bad if it's ineffective it's not it's not working properly it's it's definitely probably the worst answer uh suggestion there because you know the popularity of Open Source
firewalls whether they're software were deployed on a hardware platform just you know they're they're very popular because they are affected and they are inexpensive and they work very very well so yeah inexpensive turns out to be the best answer uh to this question okay

Let’s take a look at the next one - So Root CAs so to be able to negotiate this
question to come to a successful conclusion you have to know what a CA is so what's a CA. Anybody? It’s the Root Certificate Authority. So the question is which of the following is true about a Root CA and we're asked to choose two:
Your choices are it resides at the highest part of the chain of trust; it resides at the lowest part of the chain of trust; IT issues certificates

to several intermediate CAs or; IT issues certificates to several single CAs. So let'stake a stab at this.

What's a good one for the first choice - so the use of the word Root may be misdirecting or misleading if you think of the root of a tree and you know when you maybe picture that you see it as the lower part of the tree but really the Root CA resides at
the highest part of the chain of trust and that's what's important about this at the chain of trust the Root certificate Authority is at the highest part it's the origin okay all right so if we believe that's true then that lets out it resides at the lowest part of the chain of trust that becomes incorrect that leaves us two more choices and we need one of those.

So what do you think?

Okay oh sorry; go ahead yes please go ahead oh is it the intermediate CAs yes it issues certificates to several intermediate CAs okay and so the Root certificates when we're talking about the Root CA first of all the thing to know is that it has a self-signed certificate okay and it uses this to digitally sign all the other certificates that it creates and the certificate used by the Root CA is known as the Root certificate and as we already said is self-signed so depending upon the size of the organization you can have one or more subordinate CAs but we typically call these intermediate CAs and these CAs the intermediate CAs have their certificates issued and digitally signed by the Root CA okay all right it doesn't really reach down to anything below the intermediate CAs so we say that it issues certificates to several intermediate CAs okay
let's move on to the next one.

I have a question yes I went to the restroom so after open source after the
question question number four open source firewalls was the fifth question Root CA yes anything yes Root CA was the fifth one and basically the question was which of the following is true and the Root CA resides at the highest part of the chain of the trust chain of trust it's the origin the point of origin and IT issues certificates to several intermediate CAs

Okay thank you.

The next question jumps out right with port numbers so
the first thing to understand about this is the importance of knowing port numbers and protocols and you know there's really not going to be any getting around this I'm often asked you know how should I negotiate questions like this you know how do I deal with this and some of these things and this is one of them some of this information is pretty much a straight up knowledge based information it's not like a performance question it's just really something you have to know and what I usually tell people is that if there's something you can do to help you with knowledge-based information so such as protocols and port nbers if there's something that you can physically do if there's something you can create this is often very helpful to learning the material and one of the easiest things to do is to create a PowerPoint

presentation and you can also create things like Word docents maybe you're going to use them as flash cards if you really wanted to get detailed about it you can find Jeopardy style games like this CTF as a Jeopardy Style game really pretty much you can find these templates for PowerPoint download them and you know create a whole sequence or a whole series on protocols and port numbers so the question here which statement below is true regarding TCP Port 636 and your choices are it is used by FTP it is used by FTPs it is used by LDAP it is used by LDAPs so anybody have a suggestion for this one.

I want to say FTP TP; Anyone else?

Is it the fourth one?
It is. So lightweight directory access protocol secure or secure ldap uses secure sockets layer SSL over TCP Port 636 to encrypt the communication between the client and the ldap system again this is one of those things where you basically have to deal
with knowledge-based information and you know oftentimes there's a there's a great deal of it so once again my suggestion is always try to find some way to create something a study guide a self-help guide or something that works for you and but just do something because that will often help to solidify the knowledge okay and you know the thing to understand about that is that we really do want to try to avoid just cramming things into short-term memory because it really doesn't work and it's also obviously not very lasting that's why we call it short-term memory by working with the information and creating something like a study guide you can better put it into longer term memory okay all right let's go to the next question what does ldld AP stand for again lightweight directory access protocol.

Thank you you're welcome okay

The next question the topic is domain name - the question is: 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? Your choices are domain hijacking; domain poisoning; domain kiting; or domain squatting.

What do you thin?

Would it be domain squatting?

Okay, so you think it's domain squatting. Is there a reason?

Kind of just based off of the definition of squatting okay you don't necessarily own the property you're just there.

Domain squatting is basically buying a domain name and the the main reason for doing this the sole purpose for doing it is to prevent someone else from getting it or from buying it when this happens typically buyers will resell the domain name at a higher price to someone else who's you know somewhat desperate to get the name but that's not exactly what's being described here I'm going to call that one a pretty

good you know misdirector.

What about domain hijacking? Is that right or is that wrong?

Wrong yeah that's an incorrect answer okay so domain hijacking basically involves the hackers taking over a domain name from its original registrant and this can be done using social engineering techniques possibly exploiting vulnerabilities on systems that the host domain name you know to gain authorized access to the domain registration so that's not the correct answer what about domain poisoning does anybody know what this is?

I don't but I don't think that's the correct answer either it's not you may have heard this or heard of it as DNS poisoning or DNS CAs poisoning but that that's not right either and so that leaves us with domain kiting and what's Happening Here is that someone can purchase and register the domain and take advantage of grace periods and so you can use the domain for a grace period then you can cancel the registration but then go and register it again and then try to keep writing this grace period I guess for as long as you can and I think when I think about that definition and the the name domain kiting it kind of sort of resembles you know watching somebody fly a kite because the kite just doesn't go straight up and up and up and up right it goes up and comes down maybe spins around or something and you know that's really what you're trying to do here you're trying to sort of ride this wave of the grace period and then you know when the thing is heading towards the ground well then you let go of it and re-register it or you send the kite up again it's just how I think of it I'm telling you this because this is sort of the picture that comes to my mind when I think about this and you know if you have an impression based on say the name of a term being described in this CAse domain kiting that can also go a long ways to helping you remember this okay.

Let's go on to the next one.

This question involves IoT security and so of course you know what's going to matter here is that you understand again acronyms IoT. I should point out that certification exams especially.

Security+ is loaded with acronyms so here again you may be faced with needing a way a methodology to deal with acronyms and you know the first thing that comes to my mind of course is using PowerPoint presentations again you can create these neat slides that work like flash cards or any way that you know you you react best to okay some people like flash cards some people like straight up notes so what is IoT of things the internet of things and the question is IoT sensors with minimal data transmission requirements are best restrained by a blank Network design obviously our task is to fill in the blank so your choices are restricted latency client TLS certificates restricted broadCAst domain or restricted bandwidth okay all right anybody have an idea on this one?

Okay does something stand out as obviously incorrect anybody?
No it's okay take a guess constricting bandwidth okay and and you

think that is the incorrect answer oh no no no I'm so sorry I think the uh maybe it's the client TLC certificate certificate okay all right so yeah client TLS certificates yeah that kind of doesn't make too much sense I'd say the key to this particular question is that understanding that IoT sensors can exist in a wide range of items and I mean everything from refrigerators to you know fluid level sensors but the really important part of this question is minimal data transmission requirements and so if we're told up front that there are minimal data transmission requirements and we don't want to give any more quarter or any more space or room than we need to restricted latency is not going to do it for us latency doesn't make sense in this context ended bandwidth oh sorry yes yes absolutely the the answer to this question is restricted bandwidth okay and you know I mean we're talking about possibly needing a bandwidth of say two megabits per second which is very very tight very restricted okay but if the minimal if the transmission requirements are minimal which they may be coming from IoT sensors you know we we don't need a bandwidth of 50 megabits per second okay and so the idea here is that you are only giving enough quarter or room to satisfy what you need okay all right the other thing to remember is that sensor transmissions can also be tapped into to get into a network so by tightening the bandwidth you may in effect be helping to prevent attacks that are seeking to get into the network okay all right.

Let’s go on to the next question and this one involves Network design so the question is which term is most closely interchangeable to a reverse proxy? Y
our choices are forward proxy load balancer https server SNMP service okay anybody wanna take a shot at this question

Okay does anything look obviously incorrect?
Do you think SNMP service has anything to do with a reverse proxy
Do you recall what SNMP services
Does anybody remember that acronym
Okay so simple Network management protocol and this allows us to pull devices and get and set configurations so to me SNMP service and https server would be the two that stand out as the least correct okay what about a forward proxy does anybody know what that is. So forward proxy is the most common form of a proxy server generally used to pass requests from isolated private Network to the internet through a firewall. So the most closely interchangeable to reverse proxy the term would be load balancer okay now a reverse proxy facilitates a user's requests to web server or application server and the server's response a load balancer receives user requests and distributes them accordingly among a group of servers and then forwards each server response to its respective user so you can kind of tell from that that there's a bit of overlap between the functions of the two and that makes load balancer the best answer to this question okay so here the situation involves understanding the terminology what proxy servers are what they do and as well as as being able to spot incorrect answers like SNMP servers or https server

Okay, let’s move on to the next okay. This question involves PKI certificate attributes and the question is - Which of the following are included within a pki SSL: TLS
certificate and this time they want you to choose all that apply so your

choices are URL domain name in parentheses cm or common name certificate Authority reference also CA expiration date or private key okay so what are you thinking? Anything that sticks out here?

I'm sorry say again oh privacy private key. Is there a reason that you think that private Keys is are you saying that's a good answer or a bad answer oh well good answer a good answer. So it is not okay well it's okay that's okay this question
involves understanding public key infrastructure okay and so certificate attributes are components of the certificate and the private key is definitely not going to be one of them okay because it's not stored in a pki certificate certificates are files with a public key and contain information of its respective private key owner Okay so private key is not one of the correct choices what do you think about some of the others how about expiration date do certificates expire do they have a valid from date and a date and after which they expire what do you think yes yes they do okay and the certificate Authority reference what about that one is there a reference to the certificate Authority that generated the Certificate.
Do you think it's important to know where it came from yes yes okay and the URL domain name what do you think about that one it's important to know as well it is it's the sin in parentheses stands for common name and it's also known as fqdn and here we go with the acronyms again so FQDN - fully qualified domain name - so our three correct choices here are URL domain name certificate Authority reference and
expiration date all right let's push on to the next question.

SSL and TLS - The question reads: "What do SSL and TLS get you from a security compliance perspective and we're asked to choose two your choices are data encryption in transit data encryption on disk data encryption in memory and client server session encryption so clearly we're dealing with encryption here
okay so what are you thinking if we're concerned with data encryption where do you think it's most critical and Transit in transit I would agree with that and that is in fact a correct answer - oops there we go - data encryption in transit okay what
about on disk does that have anything to do with secure sockets layer or transport layer security.

When we look at the rest of the choices if we're concerned with encryption obviously we are trying to keep the wrong people from seeing the information or accessing it or being able to do something with it even if they have accessed it so data encryption on
disk and in memory and then client server session encryption which one of those three is not like the others and we're only talking about these three choices now here here and here if I ask it another way and I say data encryption in transit and then I
ask you to look at the remaining three choices and pick one that is like data encryption in transit which do you think it would be number four yes yes absolutely okay if we have a client server session right then we have communication between at least two endpoints and again we're sort of dealing with data in transit okay so those two are most closely related now this doesn't mean you can't do data encryption on disk okay you certainly can there are several ways to do this the most popular and

well-known are going to be full disk encryption or file level encryption and file level encryption gives you a little more granularity and control over what exactly you want to encrypt in terms of the files and data encryption on disk is just the whole thing okay all right let's move on and go to the next question

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 and we're told to choose two we're looking for common vulnerabilities the
first things you would look for your choices are MAC address filtering default admin passwords open Wi-Fi networks or AES 256 encryption
okay what do you think would it make sense to start with Wi-Fi it's open Wi-Fi networks first yes yes it would unsecured Networks a common vulnerability something that you can easily spot okay what's another one what do you think that's easily admin password.
Because what are they admin and admin admin and password right
it depends on the manufacturer now of course they do this you know too to make it easy when you take something out of the box and you're getting it set up and not to just you know put it out there with no protection but everybody knows these things now the other thing is that Mac address and MAC address filtering and you know using AES 256 encryption I mean you know they're not they are viable answers but they certainly are going to require a lot more work to see if you're using AES 128 or 256 or if you have MAC address filtering set up okay so the most obvious common as they were calling it would be default admin passwords and open Wi-Fi networks okay let's move on.

Federated identity management control - Which of the following describes a better rated identity management control? Your choices are audit specifications that are designed to ensure that cloud hosting providers meet Professional Standards a virtual item
that contains authorization data and is commonly used in multi-factor Authentication and authentication process that trusts a third-party Network authenticator to Grant access to another or different network or an authentication Service that grants Federal access so anything sticks out as obviously incorrect what do you think?

Would it be number one? Okay so audit specifications that are designed to ensure that cloud hosting providers meet Professional Standards okay why do you think that might be clearly wrong or obviously wrong because it's talking about cloud and hosting providers okay and not necessarily anything with identity management yep yeah yeah I would agree with that the other one I think that's kind of silly is the last one an authentication Service that grants Federal access I mean not even quite sure what they're getting at and you know every now and then you get lucky and you get a question and one of the answers is really kind of out there so what do you think the correct answer is here it's is it the multi-factor identification no no it's not okay no because we're we're dealing with identity management and if you are concerned with identity and identity management and we're really concerned with Authentication okay and so the correct answer an authentication process that trusts a third-party Network Authenticator to Grant access to another or different

Networks okay what's a third party what would you give an example of a third-party Network Authenticator yeah I mean it's another type of organization that maintains the information stores that can be used for single sign-on so like OCTA okay okay okay so the other thing to understand about this is Federated identity management provides single sign-on capability.

Okay. All right and let's see I think we're okay.

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? Your choices are NMAP, Mac filtering, firewall and Source IP affinity.

Okay so we're looking for methodology that allows only specific devices To access a port on the LAN. What is obviously incorrect here? Do you use MAPS?A tool yeah. It's not really a security method; it's a tool. Is there anything else in that same category that's kind of a tool and a security method? How about firewall? Does that answer make…

I do have a question with MAC filtering.

Say again.

This might sound weird but it's not MAC as…

Media Access Control is the correct answer. Okay and this is a way that it can be employed on your home network. Most modern wireless routers do have MAC
filtering built into them, small office home office and enterprise switching equipment can use and often does use MAC filtering. In fact, when a switch is set up for MAC filtering. If you connect a host to it with a different Mac address than it's
Expecting. Okay report will often go into what we might call an error disabled state; it's it's a really good method or making sure that only certain devices can access ports and if you're accessing a port on the LAN you're certainly going to be going through some type of aggregation appliance like a layer 2 switch. You can also set up ports to accept more than one MAC address but it's still filtering and that's correct and what about Source IP. Does anybody know what that is?

It's also known as simple persistence and source address affinity persistence, supports TCP and UDP protocols direct session requests to the same server based solely on the source IP address of a packet in other words it prefers that source and that's why we use the term Source IP affinity.

Just before you move on, you said uh Mac was Media Access Control.