Revision Question for TNE30012

What to know for the online exam for TNE30012

You need to achieve 40% or better to pass the course.

* Understand the main purpose of launching an attack on a network system. Is to get data off the network.
* What is the method if you have a worm that has infected your system you try to Quarantine it
* Have an understand the difference between a worm and a virus Remember a worm can spread across the network while a virus needs a host
* Have a knowledge and understanding of ping sweep. Use to block icmp echo replies.
* Have some knowledge through the Cisco IOS CLI how to initiate security audits by using Cisco AutoSecure
* What privilege are available for custom user level range from 2 to 14
* Command to block attempts remember it is login-block for x attempts number of times within certain time frame.
* Have a good understanding between what AAA stands for and what each components do.
* Know the difference between RADIUS and TACACS+ look in the Cisco academy online material.
* Setup authentication with AAA then the local database on the router? Provide fallback authentication if you forget the password and username.
* Have a good understanding of self zone on a route it looks at all traffic
* Have a good understanding of zone based policy firewall how to set it up. Basic configuration.
* What happens when you create a zone pair but not applied it get dropped.
* Know the difference between IDS and IPS and where to apply it in the network. IPS is inline and behind the router and firewall.
* What is the method used to examine network traffic that is not normal? Policy based.
* Understand what is SDEE is used and where look at Cisco academy notes
* Understand what is VLAN hopping and how to prevent remember you disable automatic trunking negotiation.
* What is the command to prevent the switch becoming the root bridge when you are running STP? Setup root guard.
* What is the purpose of using port security on a switch is to prevent overflow attacks on the CAM table. Remember CAM stands for (Content addressable memory)
* Know the difference between symmetric and asymmetric key encryption
* Symmetric key use the same key
* Asymmetric key given out public key but use your private key to decrypt it.
* What is the main purpose of Dillie-Hellman basically to setup shared keys for the public to use.
* Know the difference between block cipher and stream cipher?
* Remember block cipher is a block of 64 128 192 bit etc.
* Example of block cipher are DES, 3DES, TDRA, AES, IDEA, Blowfish, Two fish
* Stream cipher one bit at time.
* Example of stream cipher are RC4 SEAL
* Basic understanding of the CIA stands for confidentiality integrity and availability the pillar of Cybersecurity.
* Basic understanding of VPN and how to set it up and step in configure it look over the lab exercise
* they use the Diffie-Hellman to establish connection and allows to share the secret key over the insecure communication channel
* What method is used to provide data integrity? It is either MD5 or SHA better SHA then MD5 remember it is weak it can be broken.
* What looking at interesting traffic you use access list to do this.
* Have a basic understanding between ASA5505 and ASA5506-X look on the Cisco academy notes
* What is the difference between ASA ACL to Cisco IOS acl? Cisco IOS ACL configure with wildcard mask while ASA ACL uses subnet mask.
* Know what are the commands to setup default route remember or 0.0.0.0 0.0.0.0 the the next hop can be the IP address or the interface
* What is the name given you use to test your network against attacks. Using pen testing.
* Know the difference between procedures risk assessment guidelines and standards
* Have some knowledge and understanding about security policy and when creating a password policy what type of policy is this? It is a end-user policy
* What do you do if a security breach has occurred? Take photos of the offending device or devices.