Section 11: Securing TCP/IP

78. Making TCP/IP Secure

CIA (Confidenciality, Integrity, Availablity)

Confidenciality: Encryption - Password protection

Integrity: Non-Repudiation - If someone is handing me something, I have no doubt its being handed from that person

Availablity: Is it ready to go? Is there a backup?

1. Authorization
2. Authentication

Review:

*Security can be broken into three areas: Confidenciality, integrity, and availability

*Confidentiality can be addressed through encryption

*Confidentiality and intergrity must be balanced with availablity

---

79. Symmetric Encryption

Caesar Cipher - Incrementing

Algorithm
Key
cleartext
Cyphertext

1.Start with cleartext
2.Generate a key
3.Put the cleartext into the algorithm
4.Cyphertext is the result

*cleartext is any unencrypted data

*Algorithms use keys to encrypt cleartext into ciphertext

*An algorithm that uses the same key to encrypt and decrypt is symetric encryption.

---

80. Asymmetric Encryption

Rivest-Sharmir-Adlmen: Created Asymmetric Encryption

*In Asymetric encryption you have a public key and you have a private key.

*Public keys only encrypt
*Private keys only decrypt

*A private key and its associated public key is a key pair

*public keys are distributed so others can send you encrypted data

^Key Exchange

Review:

*Asymetric Encryption uses a public and a private key

*Public keys encrypt, private keys decrypt

*For two people to communicate, they must exchange public keys

---

**81. Cryptographic Hashes

Hash - A hash algorithm creates a fixed-size hash value
Hashes are used to verify data integrity

common hashes are MD5, SHA-1, and SHA-2

Review:

*Hashes are used for varifying data, not for encryption

*Hash values are always fixed in size

*Common hashes are MD5, SHA-1, SHA-2

---

82. Identification

Identification, Authorization, Authentication

Authentication Factors (Know these for the exam*):

1.Something you know (Passwords, Pin #'s, Captcha, Security Questions)
2.Something you have (Smart Card, RSA Key)
3.Something about you (Biometrics)
4.Something you do (Authenification Program (i.e. typing rythm))
5.Somewhere you are (e.g. Creditcard)

Federated Trasitive Trust System - The systems talk and if one system trust you the other will too

Multifactor Authentification - More than one.

---

83. Access Control

*know the difference between authenification vs authorization

*Access control list - Generic term - but there will be some kind of Access Control list for Authentification and authorization

Types *memorize for Net+:

1. MAC (Mandatory Access Control) - you put labels on the resource and based on the label you know what you can do.
2. DAC (Discretionary Access Control) - Allows the resource to be defined in a number of ways
3. RBAC (Role-Based Access Control) - Can use groups and assign rights and permissions to groups (Users->Groups->Rights and Permissions)

---

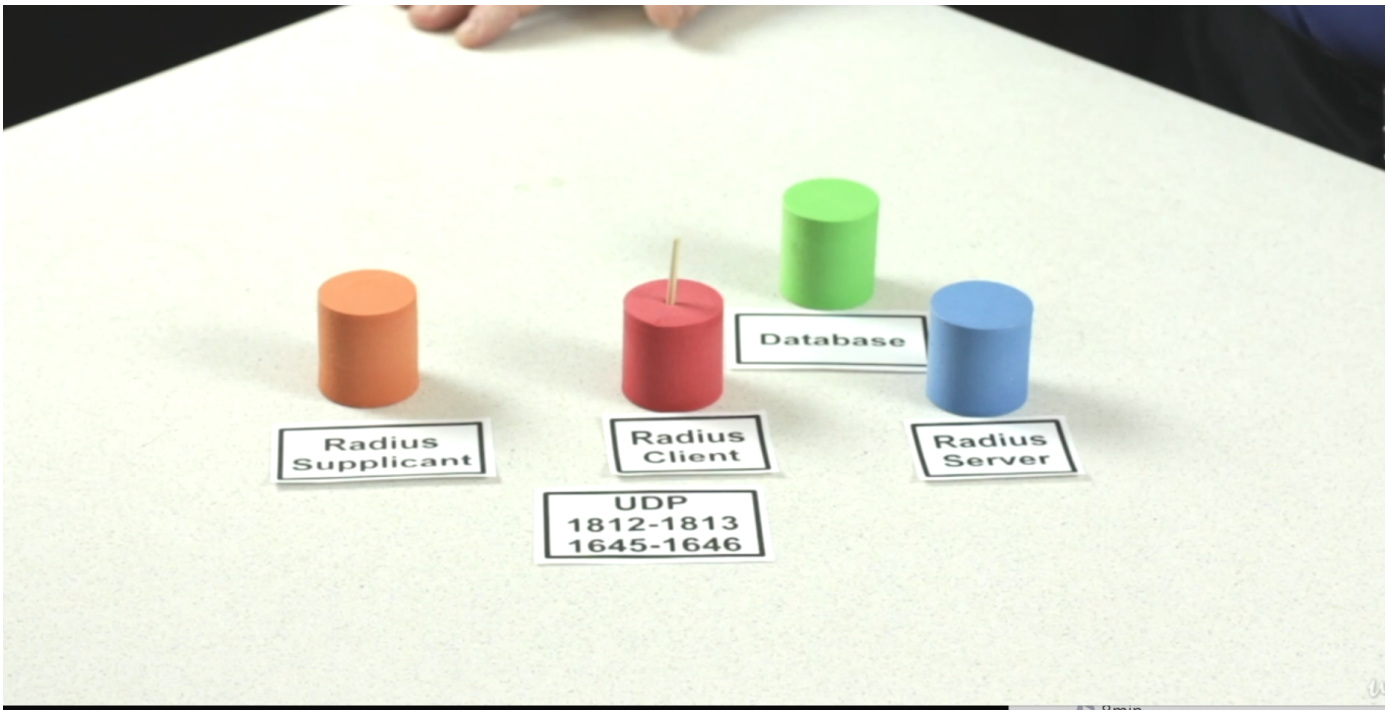
84. AAA

Radius provides AAA - Authentification, authorization, and Accounting

Radius Server - Runs some kind of radius authetification software
Radius Client - Handles authenification Requests from radius supplicant
Radius Supplicant - makes authentification requests (e.g. laptop/smartphone trying to get on)

Radius Database - Does not have to be on the radius server

Radius uses UDP ports 1812-1812 or UDP ports 1645-1646



Another Version of AAA on the Net+ - TACACS+ (a proprietary product)

*Rarely used in a wireless network

User, Client, Server
*Uses TCP Port 49

Review:

*Radius uses UDP (Ports 1812-1813 or 1645-1646)
*TACACS used TCP (Port 49)

*A radius client is an intermediary agent between a radius supplicant and a radius server

*A radius database of authenticated user and passwords may reside outside the radius server

---

85. Kerberos/EAP

Kerberos:

When you set up windows server to be a domain controller it becomes a kerberos KDC (Key Distribution Center)

A KDC is made up of two important services

1. Authetification Service (AS)
2. Ticket Granting Service (TGS)

Client sends a hash (username/Password to the KDC, and the KDC sends back a TGT <-Autenticated but not autorized, the TGT is then timestamped by the users computer and sent back to the KDC where it is timestamped again and then the KDC sends a Token to the computer.

Anytime your that computer wants to log into any computer on that network, it can use that token to do so.

Kerberos is popular, but you have to buy windows server

Downsides:
*Kerberos is a Microsoft Proprietary Technology (Cost$$$)
*Timestamped (all computers need to be on the same time)
*Made for wired Networking

Point-to-Point Protocol (PPP) is a data link layer (layer 2) communications protocol between two routers directly without any host or any other networking in between. It can provide connection authentication, transmission encryption, and compression.

EAP (Extensible Authenication Protocol)

EAP is an evelope - allows transactional based authetifications to talk to each other.

Types of EAPs:

1. EAP-PSK (Pre-Shared Key): has a common key that everyone has to login
2. PEAP (Protected Extensible Authentification Protocol) - Uses a standard username and password
3. EAP-MD5 - used as a Hash
4. EAP-TLS - Single Certificate which comes from server side passed to clients
5. EAP-TTLS - Requires the server and the clients to have a certificate

EAP is used almost exclusively to connect to wireless networks

Review:

*Kerberos handles authentication and authorization for wired networks

*Kerberos relies heavily on time stamps

*EAP enables flexible authentication

---

86. Single Sign-On

*Windows Active Directory - SSO on an LAN

Once you establish a Domain of computers you have created a trust system or "Federted Systems"

*Another type of SSO:

SAML - Security Assertion Markup Language - Designed for web apps. Allows a single person at a single place to sign on and access all web apps.

Starts with an Identity provider, you sign on to the identity provider, and then all the web apps are called service providers. So you are able to go to any web app with a token given to you by the identity provider.

*For exam think about the kind of security you need. For LAN you need Active Directory. For things that are widespread you need SAML.

SSOCircle provides a variety of service provider (SP) samples

---

87. Certificates and Trust

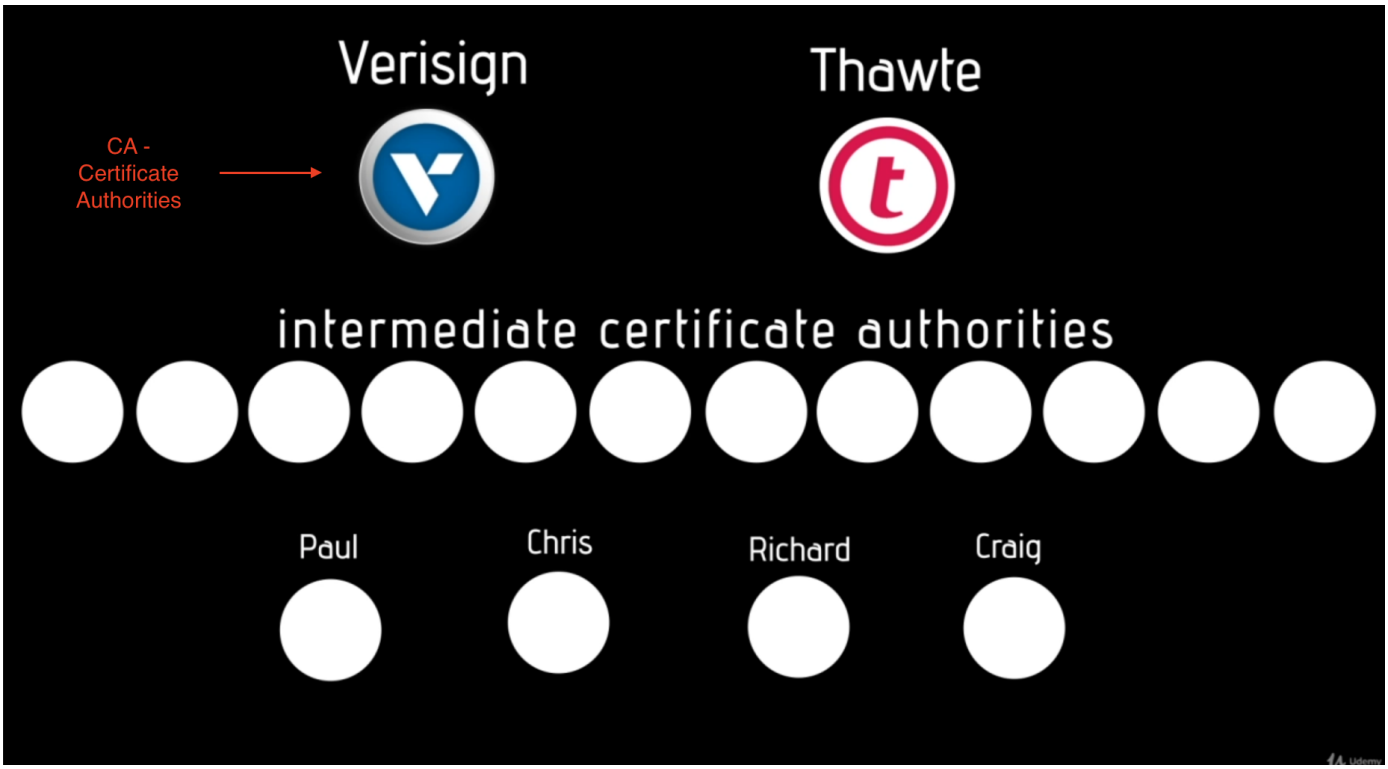
For secury access to a site with asymetric encryption heres what happens:

A Digital Signature is a hash - The site generates a private and public key. Then when the user visits the site the website encryptes the page with the private key and then sends the user a hash of the webpage and public key. The users system verifys the hash from the encrypted site with the public key.

Digital Certificate - This is a document - Inside is your Public key, your Digital Signature, and a 3rd party Digital Signature

*Three ways to do trust:

1. Unsigned Certificate: Generate your own certificate
2. Web of Trust: a web of people, requires lots of maintenance
3. PKI (Public Key Infrastructure



Review:
*Certificates include a public key and at least one digital signature
*Web of trust uses a web of mutually trusting peers
*Public key infrastructure uses hierarchical structure with root servers

88. Certificate Error Scenarios

1. Self Signed Certificate: Doesnt stop you, just gives you warnings. Throws a 443 Error because the certificate has not been issued by a certificate authority.
2. Expired Certificates: Can be viewed, then fixed either by getting a new certificate from its issuer or accepting the certificate in its current state.
3. Certificate is not valid

To Check if a certificate is valid there are two tools you can use called

1. CRL
2. OCSP

*Setting query to OSCP to confirm the current validity of certificates is a good security setting.

QUIZ

1. When securing IP Networks, developers focus on several key principles. Which of the following is NOT one of those principles?
   a. Performance
   b. Confidentiality
   c. Integrity
   d. Availability
2. In terms of network security, what is the purpose of hashing?
   a. Hash is a great side dish with eggs.
   b. Hashing encrypts data
   c. hashes are used to verify data integrity
   d. Hashing decrypts data that was encrypted by hashing
3. Which of the following is not an authentication factor?
   a. Something you are
   b. Something you can do
   c. Something you know
   d. Something you have
4. What is a digital signature?
   a. a hashed webpage
   b. an encrypted web page
   c. a hash of an encrypted data chunk that sender and receiver both have
   d. a web page that has been hashed with a private key
5. Which of the following is not a common Certificate error or warning?
   a. Certificate is on the certificate relocation list (CRL)
   b. Self-signed Certificate

c. Expired Certificate
d. Certificate not valid for the site