SECR2000 - Study Guide

Module 1 slides, ICAs and labs:

Understand the 5 phases of a planned attack as per CEH

1. **Reconnaissance** - typically longest phase
   - gathering data on a target - intending to attack
   - gather internet searches, social engineering info, DNS info
2. Scanning - using info gathered in step 1 - before attack
   - **port scanners** - identify open ports on systems in network
   - **sweepers** - identify systems that are responsive in network (using ping)
   - **vulnerability scanners** - find listening applications and possible vulnerabilities
     2a. Scanning Prevention
   - **intrusion prevention and detection systems**
   - **closing unneeded ports and services**
   - **using ACLs for traffic**
   - **using host & network firewalls**
3. **Gaining Access** - being able to access targeted systems - done through:
   - **Phishing Attacks
   - **Man in the Middle attack**
   - **Brute force attacks**
   - **Spoofing attacks**
   - **Password Cracking**
4. **Maintaining Access** - making sure the attacker can get in later
   - **Rootkit** - tools that allow an attacker to gain control over a system. Various locations it can be in - hardware, firmware, OS, applications, or memory.
   - **Trojans** - type of malware that acts as a legitimate program but can allow for: remote access, corrupting data, disabling firewalls
   - **Port Redirection** - forwarding a port to allow access into a system
5. **Covering Tracks** - removing evidence of a hack by:
   - deleting/altering logs
   - clearing cache on devices
   - closing open ports
   - uninstalling apps used for the attack

Implementing secure authentication for networking devices (Lab 1)

RADIUS Configs

- Installing RADIUS (Network Policy Services)
- Adding all networking devices as clients on management VLAN
  - ip address, vendor, name, key
- Matching key on both client and RADIUS server
- `Connection Request Policy` to use RADIUS in EDM and CAL
- made read-only and read-write `Network Policies`
- users needed privilege 15 rights for administrator || privilege 7 for read-only on cisco devices

Cisco Configs

- had to setup AAA on cisco devices

  ```
  enable secret P@ssw0rd
  aaa new-model
  aaa group server radius <name>
  server <RADIUS server IP>
  ```

define Authentication, Authorization, Accounting settings

```
aaa authentication login VTY_Authen group <name> local
aaa authorization exec VTY_Author group <name> local
aaa accounting exec default start-stop group <name>
aaa session-id common
```

defining radius server client ID and key

```
radius-server host <RADIUS server IP> key <same key as RADIUS server>
```

applying configs to VTY lines

```
line vty 0 15
authorization exec VTY_Author
login authentication VTY_Authen
transport input ssh
```

applying radius to management VLAN interface (if do it in console you can lock yourself out)

```
ip radius source-interface <interface>
```

testing functionality

```
test aaa group <name> "<user>" "<pass>" new-code
```

FortiGate Configs

- Made RO admins and RW Admins in AD and on FortiGate
- made a service account (domain users perms)
- on FortiGate LDAP -> LDAP Servers - add credentials
- create user group for admins - use LDAP server for authentication

Module 2 slides and labs:

Understand how ACLs work

- tools used to accept or deny specific types of packets
- **top-down** approach to commands - as soon as the top most action has been taken all others are skipped
- ^ this is why the bottom has a "deny any" so if it didn't match the requirement it is blocked.
- ACLs only have an effect once they are applied on an **inbound** or **outbound** interface. (1 for each direction per interface)
- ACLs do **not** block packets coming from within the router
- ACL statements can have a number put before them to order them correctly in a top down method

general rules:
standard ACLs should be close as possible to the **destination**
extended ACLs should be put as close as possible to the **source**
ACLs can increase network efficiency and should therefore be placed accordingly

inbound - IOS checks packets before it reaches the routing table (think bouncer)
outbound - IOS checks packets after it is sent to routing table process (think train ticket checker)

Understand the difference between Standard and Extended ACLs

Standard ACLs

- 1-99 or 1300-1999 number range
- can only filter on **source IP address**
- permit or deny all IP traffic (no differentiation between TCP, UDP, ICMP, etc.)
- permit, deny, remark (description)
- **wildcard mask**

- applied to port closest to destination
  syntax:
  ```
  ip access-list standard <name>
  permit 10.5.10.0 0.0.0.255
  access-class <name> in
  ```

Extended ACLs

- based on **source** AND **destination addresses, protocols, port numbers**
- packets can be allowed or denied based on where the packet originated, its destination, as well as protocol type and port addresses.
- uses numbers 100-199, or names
- can specify IP traffic (UDP, TCP, ICMP, etc.)
  syntax:
  ```
  ip access-list extended <name>
  <permit/deny> <IP/TCP/UDP/ICMP> host <source-IP> host <dest-IP> eq <port#>
  access-class <name> in
  ```

Reflexive ACLs - allow reply packets in response to an outbound connection

a reflexive ACL allows a packet out and accepts anything that responds to that packet temporarily.

- only work with extended ACLs
- statements can be put in normal ACLs and still work
  syntax:
  ```
  ip access-list extended <name1 - out>
  permit <protocol> any any reflect <statement name - EXAMPLE> [timeout <seconds>]
  ```

```
ip access-list extended <name2 - in>
evaluate <statement name - EXAMPLE>
```

```
int <VLAN or int>
ip access-group <name1 - out> out
ip access-group <name2 - in> in
```

Module 3 slides and labs:

Difference between NextGen FW and Stateless FWs

Stateless FWs - operate at L3 and L4
- based on predefined rules (ACLs) that allow or deny traffic
- based on packet source and destination

NextGen FWs (stateful) - L7 firewalls
- have more capabilities for traffic filtering than just basic filtering based on packet source and destination
- can inspect data, applications, behavior of packet (threat detection), can do web filtering, intrusion prevention

Understand the features of NextGen FW:

- VDOMs - a virtual domain - allows you to segregate your firewall applications to different domains. (Take our internal and our guest VDOMs as example)
- UTM - unified threat management - provides more security than a traditional firewall, allows for things like:
    - Intrusion Detection and Prevention systems (IDS/IPS)
    - Content Filtering - through web filters (block categories of sites, specific URLS, IPs, etc.)
    - SSL Inspection - ensures that a website has a secure SSL certificate before allowing traffic to it,
    - Advanced threat protection - uses machine learning to detect suspicious activity and stop threats (FortiGates use the FortiGuard network to stop zero-day threats)
- IPS Protection - intrusion prevention system - monitors network to see if there is any suspicious activity, stops it, and reports it to admins
- Security rules - allow you to make highly customizable rules for the traffic you want to block or allow - can be based on:
    - Source IP / Ports
    - Destination IP / Ports
    - Application / Service

Module 4 slides and labs:

The purpose of and differences between IPS and IDS systems

IPS - Intrusion Prevention System
A system put into place to constantly monitor a network for any threats or suspicious activity. Upon finding bad activity, it will log them, report them, then stop them.

IDS - Intrusion Detection System
Also put into place to constantly monitor a network - doesn't stop the threat, just logs and alerts.

uses TAP and SPAN to not impact network performance.

IPS/IDS can be network-based or host-based
Network-Based - more complicated to setup, traffic needs to pass through, monitors all network.
Host-Based - easier to setup, monitors inbound and outbound of a single endpoint.

Signature Based - compares network to list of "known attacks" - less aggressive for new threats - has a much lower false positive rate
Anomaly Based - builds a baseline of "normal" behavior, any deviations are called anomalies - complex to setup, can catch zero-day threats - high false positive rate

Module 5 slides and labs:

IPsec technology

Phase 1 - **ISAKMP tunnel**
- This tunnel is created and used for management traffic only
- used as a secure way of setting up the second tunnel (phase 2 - actually carries data)

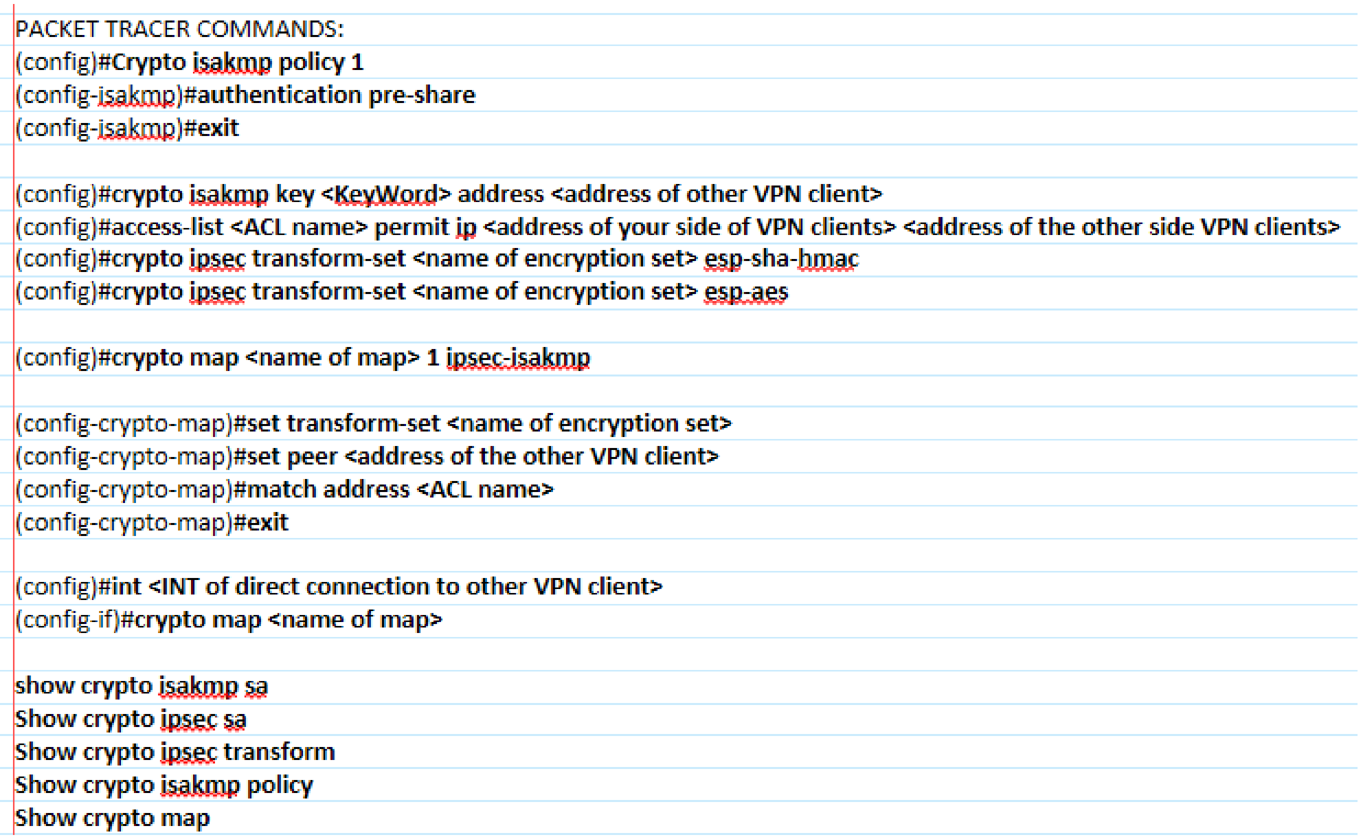
- two peers authenticate with PSK (pre-shared keys) or certificate - **used for proving identification**
- DH process happens now - each side creates a DH private key and uses that to derive a public key;
- public keys are exchanged, combines public key and their own private key to independently create the same shared DH key
    - this key is used to exchange all the info and agreements to make a symmetrical key
    - the symmetrical key is used to encrypt any information passing PHASE1 (or IKE security association)
    - **symmetric key is used for encryption, it is never shared**

Phase 2 - IPsec parameters are negotiated - **IPsec Tunnel**

- establishes an **IPsec SA** (security association) - (periodically renegotiates to ensure security)
  at this point there is a DH key on both sides, the same symmetric key, and an established tunnel
- both sides are informing each other about encryption methods and cyphers they can use - the other peer will pick the best shared method
- **they both agree on method of communication**
- now they make a new symmetrical IPsec key - designed for large scale data transfer

- this is now the key that is used for encryption and decryption of actual data across the VPN tunnel
- ^ encryption method and keys are agreed on for bulk transfer - this results in **IPsec security association.**

in short:
Initiation: triggering of the creation of the tunnels
IKE Phase 1: peers negotiate a security association to build the IKE phase 1 tunnel (ISAKMP tunnel)
IKE Phase 2: within the IKE phase 1 tunnel, the IKE phase 2 tunnel (IPsec tunnel) is built
Data transfer: the user data is protected by sending it through the IKE phase 2 tunnel
Termination: when there is no user data to protect, the IPsec tunnel will be terminated (after a while)



```
PACKET TRACER COMMANDS:
(config)#Crypto isakmp policy 1
(config-isakmp)#authentication pre-share
(config-isakmp)#exit

(config)#crypto isakmp key <KeyWord> address <address of other VPN client>
(config)#access-list <ACL name> permit ip <address of your side of VPN clients> <address of the other side VPN clients>
(config)#crypto ipsec transform-set <name of encryption set> esp-sha-hmac
(config)#crypto ipsec transform-set <name of encryption set> esp-aes

(config)#crypto map <name of map> 1 ipsec-isakmp

(config-crypto-map)#set transform-set <name of encryption set>
(config-crypto-map)#set peer <address of the other VPN client>
(config-crypto-map)#match address <ACL name>
(config-crypto-map)#exit

(config)#int <INT of direct connection to other VPN client>
(config-if)#crypto map <name of map>

show crypto isakmp sa
Show crypto ipsec sa
Show crypto ipsec transform
Show crypto isakmp policy
Show crypto map
```

^ commands

DH Algorithm in IPsec

DH (Diffie-Hellman) is the public/private key method that we use for secure encryption keys.

- each peer has a private key, and a public key that is derived from the private key in a complicated mathematical way.
- the public key is designed to be shared, the combination of a peer's public key and your own private key allow you to come to the same "shared secret" key as the other peer.

- symmetrical keys are derived from this DH key shared between the peers, at no point are symmetric keys exchanged.

SSL VPN technology

an SSL VPN tunnel is a tunnel that is based on the TLS (Transport Layer Security) protocol.

- it allows users to establish a secure connection through web-browsers (portal based), or client applications (tunnel based)
  advantages:
- less admin overhead and tech support
- more specific access control to applications
- more likely to be allowed through a firewall (using http/https)
  disadvantages:
- greater security risk - malware might spread from client to corporate network

Split tunneling can be a solution to malware

- only the corporate data goes through the tunnel, whereas the other traffic goes through the client's connection

SSL VPNs are most commonly used for remote client connections

- meaning someone remoting into work would use an SSL VPN

Steps taken to Configure SSL VPN in our lab

- created security group in AD for VPN-Users
- used for RADIUS network policy
- FortiGate was already RADIUS client
- using EAP (certificate) and AD credentials for authentication (using self signed cert)
- on FortiGate -> configure SSL-VPN - upload cert - listen on WAN1 - setup DC as DNS for tunnel network options
- in "full-access" portal - added remote clients subnet
- SSL VPN Firewall Policy - REMOTE TO LAN
  - use address object (for SSL-VPN) as source
  - also include RADIUS group as source
  - incoming interface should be the default SSL-VPN tunnel interface
  - outgoing is internal1 (LAN port)
  - destination should include your corporate network subnet
- SSL VPN Firewall Policy - REMOTE CLIENTS TO INTERNET

  - used for security of client's internet traffic
  - create a new policy that has incoming int on the SSL-VPN tunnel interface again,
  - outgoing as WAN1 interface
  - **only allow HTTP, HTTPS, ICMP** to internet.
- make sure to disable split-tunneling so the internet traffic routes correctly
- client needs to download the exported cert from the RADIUS server and install it (used for VPN)
- client uses remote gateway of firewall **WAN IP** as the target - port 10443
- authenticate with AD credentials

Research project - Syslog and SNMP monitoring

understand the purpose of SNMP monitoring and Syslog systems

SNMP - simple network monitoring protocol

- allows you to collect monitoring data about you networking devices.
  - this allows you to find if there are bottlenecks
  - get a better overview of the network and prepare for future upgrading
  - detect faults and errors within the network
  - view live statistics - allows you to see if there is a sudden influx of traffic
  - adjust settings, update configs, remotely manage devices

Syslog - collects and analyzes log messages from most devices in a network.
These can help you get a long-term view of events / security issues / potential problems within your network.

- it also keeps everything in one place
- can help you troubleshoot / diagnose issues

capabilities of SNMP monitoring and syslog systems (alerting, types of stats collected, SNMP versions and credentials/community strings)

NMS (network monitoring systems) - can pull NetFlow, sFlow, SNMP traffic

- can alert you when you are using x amount of bandwidth
- can collect stats on traffic spikes, up time, CPU usage, memory usage, time, etc.
  Syslog - can pull events and logs from various devices

- stores events and security events

SNMP version 1-3
SNMP v1 and 2 both use a generic community string authentication for Read-Only and Read-Write access to devices. (these strings were stored in plain text, womp womp)
SNMP v3 has proper encryption that it can use (AES - not just in plain text) - supports user-based security, and view-based access control (user **x** has read only | but user **y** has read write for example.)