Intro to Network Security

September 18, 2023 10:04 AM

Fundamentals of Network Security

common types of attacks:

- social engineering
  - tricking people into resetting passwords, revealing their email & password, etc.
- phishing scams
  - whale phishing - going after the big targets in a company with a lot of info
  - spear phishing - pretending to be someone that knows the target
  - phone phishing
  - email phishing
- malware attacks
  - in conjunction with phishing, to get you to download malware
- denial of service
  - overloading a network to slow or stop traffic going through
  - syn flood attack: sending the first part of a syn acknowledgement thing, then when getting a response just ignore it
- network sniffing
  - man in the middle attack - seeing the network traffic

IOT is adding a lot of complexity to things - making cybersecurity harder

Security people need to consider:

- security gateways
  - how can someone get access? are the users using admin accounts?
- SSL Inspection
  - make sure the HTTPS site has proper certificates rather than some sketchy one
- Threat prevention and detection
- Security policies
  - if you're doing things that you aren't supposed to do on company property they have a legal way to fire you
- threat intelligence platforms
  - things like FortiGuard - a company that will analyze your traffic and notify you if anything bad is going on

cybersecurity focuses on the following:

Authentication - who are you

Authorization - are you allowed in

Accounting - monitoring user activity while accessing network

Confidentiality - protecting information from being accessed by unauthorized parties

- both "at rest" - meaning stored data not being used
- and "in motion" - meaning when the data is being sent from one place to another

Integrity - making sure nothing is changed without permission/intention - can be broken through malware, data corruption, someone accidentally adding something and saving it (without having versioning on)

Availability - data staying accessible - can be broken by misconfigurations, DoS attacks

Attack Methodologies:

a successful attack typically follows these five phases:

Reconnaissance
- gathering data on the target for planning and conducting an attack
- this is usually the longest phase, can last months
- gather internet searches, social engineering info, DNS info

Scanning
- searching for vulnerabilities in the system before launching an attack
- using the info from the reconnaissance
- using port scanners, sweepers, vulnerability scanners

Gaining Access
- getting access to targeted systems to extract data
- using: phishing attacks, man in the middle, brute force, spoofing, password cracking, etc.

Maintaining Access
- this is where they may try to lay a path for future attacks
- use rootkits, trojans, port redirections

Covering Tracks
- removing logs, clearing cache, closing open ports, uninstalling attack applications

Best practices in mitigating network attacks:
- perform network auditing to find vulnerabilities
- use a threat intelligence platform
- enforce security policies
- provide user training **regularly**
- reduce/restrict attack surface by doing network and system hardening
  - dont have default configs,
  - disable default admin accounts / default services
  - restrict user permissions
- apply network security measures at different layers
  - physical network security,
  - VLAN configs,
  - ACLs,
  - Software security,
  - Intrusion **Detection** System,
  - Intrusion **Prevention** System
  - Multi-Factor Authentication
  - Web Filters

Access Control Lists

October 2, 2023 10:11 AM

In addition to security tools, such as strong passwords, mfa, physical security, Network Admins and secuirty pros must also make sure there is traffic filtering

Traffic Filtering - denying unwanted access to network and services while allowing users access to necessary services and data

Routers and **Layer 3 switches** provide basic traffic filtering capabilities with ACLs
Stateless Firewalls are operating at L3 and L4 of TCP/IP stack
- based on predefined rules (access lists) that allow or deny traffic

NGFW (new firewalls) - stateful - have more capabilities for traffic filtering than basic filtering based on packet's source and destination, and port number
- inspect data and applications, behaviour of packet, threat identification, web filtering, intrusion prevention

Access lists on routers are powerful tools for controlling behavior of packets and frames
- series of commands or filters that tell the router what type of packets to: accept or deny

Access lists are process **top-down**
- as soon as there is a match, action is taken and the rest of the statement in the ACL is ignored.
- ACLs don't have any effect until they are applied on an **inbound** or **outbound** interface.

ACLs defined on a:
- per protocol (IP)
- per direction (in or out)
- per interface basis

you can have only one inbound **and** outbound ACL per interface (you can have one of each)

how ACLs work:
- a group of statements that define whether packets are accepted or rejected entering or leaving and interface
- operate in sequential order, **top-down**
- if a condition match is true, the packet is permitted or denied, then the rest of the ACL is skipped.
- if ACL statements are unmatched an implicit "deny any" is put at the end by default
- ACLs **do not** block packets that originate within the router

standard ACLs
- **1-99** or 1300-1999 number range
- can only filter on **source IP address**
- permit or deny all IP traffic (don't distinguish between TCP, UDP, HTTPS)
- permit, deny, remark (remark gives you a description)
- **wildcard mask**
- applied to port closes to destination

inbound access lists - IOS checks the packets before it is sent to the routing table

outbound access lists - ios checks the packets after it is sent to the routing table process, except destined for routers own interface

EXTENDED ACLs - used more often than standard ACL because of better control
- based on **source** AND **destination addresses, protocols,** and **port numbers**
- packets can be permitted or denied access based on where the packet originated and its destination, as well as protocol type and port addresses
- use numbers from **100-199**
- can also do named syntax
- can use **operator** and **operand** to refer to the **source** or **destination port**

inserting statements on ACL
- sequential numbers can be put before permit/deny statements to order them for the **top-down** methodology

extended access list:
- can allow / deny **TCP/UDP** and port numbers

```
ip access-list extended EDMVLAN11
 5 permit tcp 10.10.11.0 0.0.0.255 host 10.10.10.11 eq ftp
 5 permit tcp 10.10.11.0 0.0.0.255 host 10.10.10.11 eq www
 1 permit udp any eq bootpc any eq bootps
 1 permit udp any any eq domain
interface vlan 10
 ip access-group EDMVLAN11 out
```

General Rule:
- **STANDARD** ACLs do not specify destination addresses, so they should be placed as close to the destination as possible.
- Put **EXTENDED** ACLs as close as possible to the source of the traffic **denied**
- if ACLs are in the proper location, traffic can be filtered, AND it can make the whole network more efficient
- if traffic is filtered, ACL should be placed where it has the greatest impact on **increasing efficiency**

```
ip access-list extended EDMVLAN11
 5 permit tcp host 10.10.10.11 10.10.11.0 0.0.0.255 eq ftp
 5 permit tcp host 10.10.10.11 10.10.11.0 0.0.0.255 eq www
 1 permit udp any eq bootps any eq bootpc
 1 permit udp any any eq domain
interface vlan 10
 ip access-group EDMVLAN11 in
```

Reflexive Access Lists: allows reply packets **in response to an outbound connection**
- only works in extended ACLs
- the statements can be put in normal ACLs
- doesn't work in packet tracer

```
ip access-list extended <name1-out>
 permit <protocol> any any reflect <statement> [timeout <seconds>]

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

```
 ip access-list extended EDMVLAN11
 10 permit tcp 10.10.11.0 0.0.0.255 host 10.10.10.11 eq ftp
 10 permit tcp 10.10.11.0 0.0.0.255 host 10.10.10.11 eq www
 1 permit icmp any host 10.10.10.10
 2 permit udp any eq bootpc any eq bootps
 3 permit udp any host 10.10.10.10 eq domain

interface vlan 2
 ip access-group EDMVLAN11 in
```

ip access-list extended <name2-in>
 evaluate <statement>

interface <VLAN or #>
 ip access-group <name1-out> **out**
 ip access-group <name2-in> **in**

 2 permit udp any eq bootpc any eq bootps
 3 permit udp any host 10.10.10.10 eq domain

interface vlan 2
 ip access-group EDMVLAN11 in
interface vlan 3
 ip access-group EDMVLAN11 in
interface vlan 11
 ip access-group EDMVLAN11 in

Next Gen Firewalls

October 16, 2023 10:16 AM

Fundamentals:
networks must be protected at the edge from unwanted inbound and outbound traffic and threats

- edge firewalls are the devices that are placed between public and private networks
  they are also used for controlling inbound and outbound traffic for DMZs, intranet zones
- **traditional firewalls** - provide basic security for environment, including packet filtering
  traffic control relies on security policies based on source and destination **IPs**, source and destination **ports (L3/L4)**

- **NextGen firewalls (L7 firewalls)** - can analyze traffic up to and including **layer 7**
  more features than a stateful FW - application awareness / control, integrated IDS (intrusion detection) and IPS (intrusion prevention), cloud-integrated threat intelligence, deep packet inspection, URL filtering, SSL inspection, identity-based security, content filtering

when selecting a NGFW you want to look for:

- **advanced capabilities for breach prevention**
  - to quickly detect malware
  - IPS (intrusion prevention) built-in capabilities to stop hidden threats
  - URL filtering to enforce policies on hundreds of URLs
  - built-in sandbox to continuously analyze file behavior and detect/eliminate threat
  - deep learning capabilities

  - **user based policies**
  - **identity based policies**
  - decryption
  - DLP - data leak protection capabilities

  - network visibility - monitoring to see what the hosts are doing in a network
  - monitoring active applications and websites

  - flexible management and deployment options - centralized management for everything
  - evolving features to fit the landscape of the current cybersecurity trends - visibility across IoT devices

NextGen firewalls security policies

- protect network from threats and operation disruptions - blocks or allows sessions based on traffic characteristics
- all traffic through a FW is matched against a session, then the session against a security policy

Security policy components:

- **name** - label that identifies rule
- **UUID** - universally unique identifier - string that permanently identifies rules for tracking
- **source and destination zones or interfaces** - shows where traffic originates and where it terminates (through zones, group of interfaces you can apply policies to)
- **source and destination subnets/hosts**
- **user** - the user/group that the policy applies to
- **application/service** - application / service to control
- **action** - specifies an **allow** or **deny** for traffic matching criteria
- **NAT options** - specifies if NAT is applied or not to traffic
- **security profiles** - provide additional protection for threats, vulnerabilities and data leaks
- **policy objects** - subnets, hosts, FQDN addresses
- **services** - pre-defined or custom services allowed or denied through policy

Intrusion Detection and Intrusion Prevention Systems

October 23, 2023 10:14 AM

IDS and IPS are deployed to constantly inspect network traffic
- identifying possible threats, logging them, reporting them to admins, and prevent them

IPS system is an IDS system (reverse is not true)

IDS - intrusion detection system - will alert but not stop the attack
uses TAP and SPAN to not impact network performance

IPS - intrusion prevention system - detect and prevent

IPS/IDS can be: network-based or host-based
Network-Based IPS/IDS: can be complex to install as traffic needs to pass through it
Host-based IPS/IDS: protect a particular endpoint - monitor inbound and outbound network traffic

Signature-based system: compares network against **known attacks**
- compares all traffic, files, activities to a database of signatures; false positive rate very low

Anomaly-based system: builds a baseline of "normal" behavior, any deviations are classified as **anomalies**
- can catch zero-day threats, complex to setup, false positive rate pretty high

Best practices for deploying IPS systems:
- enable IPS scanning at the network edge (for all services)
- endpoint IPS scanning for threats in your network
- guard against attacks on services you make public
- **create your own profiles to suit your environment**
- if you do use default profiles - reduce IPS signatures/anomalies enabled to conserve time/memory
- if enabling anomalies, make sure to tune thresholds to your environment
- if you need protection but no audit info, disable logging

products that do IPS/IDS
SNORT - well known and popular IPS
- open source, huge library of pre-built detection rules
- supports both, signature and anomaly analysis

KISMET - wireless IDS tool
- open source, free

Security Onion - Linux IDS
- both hosts and networks

summary:
- **IDS** system is designed to detect an intrusion, **but it will not stop the attack**
- **IPS** designed to **detect and prevent** a potential cyberattack
- not one-size-fits-all solutions; need to be tailored to the environment

Virtual Private Network Technologies

October 26, 2023 2:06 PM

A VPN is a private network that is created via tunneling over a public network
benefits of VPNs:
- cost savings - can just use regular internet connection, no special tools
- security - have to authenticate both side before creating a tunnel
- scalability - can add more sites and just expand VPN access

types of VPNs:
Internet Protocol Security (IPsec) - site-to-site or client
SSL VPN (Client VPN) - remote client VPN
WireGuard (open source) - Diyaa

Site-to-Site VPN: connect sites together
- uses a tunnel to prevent someone capturing your data over the internet
- created when devices on both sides know of the VPN configuration in advance
- the VPN remains static and internal hosts (end users) have no knowledge that a VPN exists - essentially like you're in same location as other network
- extension of class WAN network
- connect remote networks to each other
- can branch office network to a company HQ network, or on-prem to cloud
- replaces a leased line or MPLS connection (more expensive than an internet connection)

IPsec - a "framework" of open standards developed by the IETF to create a secure tunnel at the network (IP) layer
- consists of 5 security blocks with encryption algorithms for admins to choose from and configure when implementing VPN security services
- IPsec protocol: authentication header, encryption, or both.
    - **confidentiality** - encryption on traffic
- DES (Data Encryption Standard) - 56-bits - very insecure and old
- 3DES (triple Data Encryption Standard) - 56-bits (3 times) - still insecure and still old
- AES (Advanced Encryption standard) - 256-bits - a LOT better than DES
- Software-Optimized Encryption Algorithms (SEAL) - 160-bits - the best one

    - **integrity** - a method of proving data integrity (meaning content has not been tampered with) -
    - HMAC (hashed message authentication code) can guarantee that the integrity of the message is pure using a hash value
- HMAC-Message Digest 5 (HMAC-MD5) - 128-bit - do not use if you can help it
- HMAC-Secure Hash Algorithm (HMAC-SHA)
    - SHA-160 - SHA1
    - SHA-256 - SHA2
    - SHA-384 - SHA2
    - SHA-512 - SHA2

    - **authentication (AH)** - device on other end of tunnel must be authenticated before the communication path is considered secure
- Pre-Shared Keys (PSKs) - each site independently create a has value based on PSK and other info, has values are then exchanged and verified to authenticate
- RSA signatures - based on certificates - **higher level of secure authentication**

    - **Diffie-Hellman (DH)** - public key exchange method that provides a way for two peers to establish a shared secret key that only they know
    - makes an encryption key known as a "shared secret" from the private key of one party and the public key of the other
    - symmetrical keys are derived from this DH key shared between the peers, at no point are symmetric keys exchanged

Phases of IKE negotiation:
Phase 1 - ISAKMP (encryption, authentication, hashing is negotiated between peers)
- negotiates an IKE protection suite
- exchanges keying material to protect the IKE session (DH)
- authenticates each other
- establishes the **IKE SA**

Phase 1 - ISAKMP tunnel
- used for management traffic only
- secure way to establish the second tunnel, the one that carries the data (IKE phase 2 - IPsec tunnel)
    - two peers need to authenticate using PSK or certificates, not about encryption yet; about proving identification
    - DH process - each side creates a DH private key used to derive a public key; public key can be used to encrypt data that only private key can decrypt; each side has a public and a private key
    - public keys are exchanged
    - each side uses its own private key and the shared public key - independently generates the same shared DH key (same on both side) - **does this using crazy math**
        - this is the key used to exchange all the info and agreements to make a symmetrical key
        - this is the key used to encrypt any information passing PHASE1 or the IKE security association
    - this is the core of IPsec VPN - **symmetric key used for encryption that is never shared**

Phase 2 - (IPsec parameters are negotiated) - IPsec tunnel - encrypted data
- negotiates IPsec security parameters, known as IPsec transform sets.
- establishes **IPsec SAs**
- periodically renegotiates IPsec SAs to ensure security

- keys agreed on in phase 1 are used as a starting point in phase 2 (IKE security association)

    - there is a DH key on both sides, the same symmetric key, and an established tunnel
- the peers are informing each other about encryption methods and ciphers they support, the other peer will pick the best shared one and informs the other peer. **they then agree on the method of communication**
- based on parameters negotiated above and the DH key, each peer is generating a symmetrical IPsec key, designed for large scale data transfer. it is the IPsec key that is now used for encryption and decryption of the actual data across the VPN tunnel.
- encryption method and keys are agreed on for bulk transfer of data, resulting in the **IPsec security association**

Security Associations
- negotiated parameters between two devices are known as a **security association (SA)**
- a VPN has SA entries defining the IPsec encryption parameters as well as SA entries defining the key exchange parameters
- **SAs represent a policy contract between two peers or hosts and describe how the peers use IPsec security services to protect network traffic.**
- SAs contain all the security parameters needed to securely transport packets between the peers or hosts, and practically define the security policy used in IP sec.
- Security associations are maintained within a SA database (SADB), which is established by each device

IPSEC PROCESS
Initiation: triggering of the creation of the tunnels
- for example: when you configure IPsec on a router, you can use an access-list to tell the router what data to protect.
- when the router receives something that matches the access-list, it will start the IKE process.
- also possible to manually initiate the tunnel

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

Remote Client VPNs

Remote Access VPN - allows for dynamically changing connection information, can be enabled or disabled when needed.
- Allows users in a remote location to establish a secure, encrypted connection to the corporate network.

IPSec or SSL based

SSL VPN tunnel - based on TLS protocol and allows users to establish a secure connection through web-browsers (portal-based) or client applications (tunnel based)
Advantages:
- Less administrative overhead and tech support
- More specific access control to applications
- More likely to be allowed through a firewall (use http/https)

Disadvantages:
- Greater security risk - spread of malware from client to corporate network

When using split tunneling - only corporate data goes through the tunnel, and other traffic goes through client's connection
- This can be a solution (?)

Fortigate VPN

Monday, November 6, 2023 10:13 AM

Don’t use the wizard - use custom
Use IKE version 2
Use the highest encryption available on both devices
Enable PFS - perfect forward secrecy