Chapter 3

Thursday, August 3, 2023 10:33 AM

Reviewing Basic Networking Concepts

Sniffing attack - use packet sniffer to capture data sent over a network

DoS/DDoS - single/multiple source attack to disrupt services

Poisoning attack - corrupt data stored in cache with different data

Security+ mentions **Layer 2** refer to **Open Systems Interconnection** **OSI model** **data link layer** - ensures that data is transmit to specific devices on the network

formats data into frames and adds header with MAC address for source/dest

address resolution protocol **ARP** - resolves IP addresses to MAC addresses

Layer 2 attacks - attempt to exploit [illegible] and ARP

layer 2 attacks - attacks
vulns in MAC addressing and ARP

OSI Model

Physical - physical hardware
cable types, switches, routers...

data link - ensure data is transmit
to specific devices on network

network - logical addressing into
form of IP addresses

Transport - transport data between
systems
TCP and UDP

Session - establish, maintain, terminate
sessions between systems

presentation - formatting data
needed by end-user apps

ASCII

Application - display info to user in readable format

Basic Networking Protocols

Networking protocols provide rules for pcs to comm with each other on network

Transmission control Protocol / Internet protocol (TCP/IP) protocols like TCP and IP provide basic connectivity

others like HTTP and simple mail transfer protocol SMTP support traffic types

TCP/IP is a suite of protocols

not as much emphasis on knowing ports but good to know common ones

Basic networking protocols

- Transmission control protocol TCP

traffic

- Transmission control protocol
  connection oriented traffic
  guaranteed delivery
  3-way handshake
  SYN - SYN/ACK - ACK
- User datagram Protocol UDP
  connectionless sessions without handshake
  ICMP and DoS use UDP
- IP - identify hosts in TCP/IP network and delivers traffic from one host to another
  IPv4 = 32 bit decimal
  IPv6 = 128 bit hexadecimal
- Internet control message protocol ICMP
  testing basic connectivity
  ping, pathping, tracert
  blocking ICMP prevents DoS and discovering devices on

and discover... network

ex: a scan can send ping to every IP on subnet

- Address Resolution Protocol ARP

resolves IPv4 to MAC

TCP/IP uses IP address to get packet to destination network

then uses MAC to get to destination host

Implementing Protocols for use cases

networks don't auto support all available protocols

IT pros identify need based on org goal and enable best protocol

Voice and video use case

UDP used over TCP for voice and video streaming

Real-time transport protocol RTP - delivers audio and video over IP networks

audio and video

- Voice over IP VoIP
- streaming
- video teleconferencing
- devices using web-based push to talk

Secure real-time transport protocol SRTP
encryption, message authentication, and integrity for RTP
protects against replay attacks

unicast - 1 person calling another
multicast - sent to multiple recipients

Session initiation protocol SIP - initiate, maintain, and terminate voice, video, and messaging
uses request and response messages
when establishing session
sent in text so easy to read if captured

SIP establishes connection and RTP or SRTP transports audio/video

SIP messages contain metadata about session

. . . ftware used,

SIP messages
session
info on equipment used, software used,
and private IP
can be used for logging and forensics

File transfer use case
data in transit is any traffic over
network
when sent in cleartext, can be seen
in packet analyzers
used to encrypt data in transit

File transfer protocol FTP - uploads and
downloads large files to and from
an FTP server
sends in cleartext by default

FTP active mode
TCP port 21 for control signals
TCP port 20 for data

FTP passive mode
TCP port 21 for control signals
TCP port for data

TCP port

random TCP port for data

if FTP traffic going through firewall random port usually blocked so best to disable passive mode

PASV

trivial file transfer protocol TFTP

uses UDP port 69

transfer smaller amounts of data

ex: comm with network devices

not essential protocol so usually blocked

encrypt data in transit

secure shell SSH - encrypts traffic over TCP port 22

can be used to encrypt FTP and other protocols

secure copy SCP - based on ssh and used to copy encrypted files over a network

encrypt TCP wrappers - to

a ve

can also encrypt TCP wrappers - type of ACL used on Linux to filter traffic

Secure socket layer SSL - was primary method to encrypt HTTP as HTTPS can also encrypt SMTP and lightweight Directory access protocol LDAP

has been compromised and not recommended

transport layer security TLS - replacement for SSL

many protocols that support TLS via STARTTLS - which is a command to upgrade an unencrypted connection to an encrypted connection or same port

internet protocol security IPsec - encrypt IP traffic

internet protocol

IP traffic

native to IPv6 but works on IPv4

encapsulates and encrypts IP packet payloads

uses Tunnel mode to protect VPN traffic

two main components:

- Authentication header AH
  protocol ID number 51
- Encapsulating security Payload ESP
  protocol ID number 50

uses internet key exchange IKE
UDP port 500 to create security association for the VPN

Secure File transfer Protocol SFTP
Secure implementation of FTP

Secure implementation

extension of SSH

uses TCP port 22

SSL vs. TCS

2014 Google found POODLE attack

SSL is not patched or maintained

File transfer protocol Secure FTPS

extension of FTP that uses TLS

some implementations use TCP ports

489 and 990

TLS can also encrypt traffic over ports used by FTP 20 and 21

Email and web use cases

sending and receiving email

many orgs also host web servers

provide access to web servers by external clients

STARTTLS - instead of using one

STARTTLS - instead
port to transmit data in
cleartext and another for cipher,
STARTTLS allows to use same
port for both

Simple mail transfer protocol SMTP
transfers email between clients
and SMTP servers

TCP port 25 for unencrypted
TCP port 587 for TLS encrypted
email

Can use STARTTLS

used to use SSL and port 465
but Internet Assigned numbers
authority IANA reassigned after
deprecated

Post office protocol v3 POP3 Secure
POP

transfers emails from servers
to clients

transfers email down to clients

TCP port 110 for unencrypted
TCP port 995 for encrypted

Internet message access protocol version 4
IMAP4 and secure IMAP
store email on an email server
allows users to org/manage email in folders

TCP port 143 for unencrypted
TCP port 993 for encrypted

Hypertext Transfer Protocol HTTP
transmit web traffic on internet and intranets

TCP port 80

HTTPS - HTTP over SSL/TLS
encrypts web traffic

TCP port 443

IMAPS

TCP port

Directory services and LDAPS

Network OS commonly use a directory service for management and implement secure authentication

ex: Microsoft Active directory Domain services AD DS - db of objects that provide central access point to manage users, pcs, and other objects

Kerberos also does this authentication protocol uses KDC to issue timestamped tickets on UDP port 88

lightweight directory access protocol

LDAP - specifies formats to query directories

extension of X.500

uses TCP port 389

LDAPS - LDAP secure with TLS using

LDAPS - LDAP encrypts with TLS using TCP port 636

Active directory is based on LDAP

Remote Access use case

if admin need to add user account or change group policy object GPO they rarely would go to server room access remotely

used to use telnet when remote admin systems, but this sends over cleartext

now use SSH

admins and clients use remote desktop protocol RDP - connect to other systems remotely

Microsoft uses for remote Desktop and Remote Assistance

Microsoft ...
services and Remote ...

TCP port 3389 ← more common
UDP port 3389

can also use VPN to connect remote

OpenSSH

openSSH - suite of tools that simplify use of SSH to connect to remote servers

supports SCP and SFTP

want to connect to server in network:

```
ssh gcga
```

connect using your username

connect with account on the system:

```
ssh root@gcga
```

, bif

ssh [illegible]

these will prompt for pword but OpenSSH offers passwordless login using public/private key

you keep private key, server gets copy of public key

create key pair

ssh-keygen -t rsa

id_rsa.pub
id_rsa

copy public key to server

ssh-copy-id gcga

Time Synchronization use case

often need systems on same time

Windows Time service to locate reliable internet server running Network Time protocol NTP. most [illegible] synchronization

Network Time P...

common time synchronization

1st domain controller

↑

all other domain controllers

↑

all pcs in domain

Simple NTP SNTP - can be used but not as accurate as NTP

Network Address Allocation use case

allocating IP addresses to hosts within your network

Dynamic Host Configuration Protocol

DHCP - dynamically assign IP addresses to hosts

also assigns other TCP/IP info like subnet masks, default gateways, DNS server addresses...

IPV4

32-bit decimal

4 decimals separated by dots

ISPs purchase/rent IP addresses to use for customers

routers on 'internet block all traffic from private IP

RFC 1918 private IP

- 10.x.y.z (map 10.255.255.255)
- 172.16.y.z – 172.31.y.z
- 192.168.y.z

the only 3 IPv4 addresses that you should allocate in a private network

IPv6

128-bit hexadecimal

8 groups of 4 hexadecimal chars separated by :

- U
separated by .

instead of private IPs, uses unique local addresses

only allocated within private networks

Start with fc00

DHCP Snooping

prevent unauth DHCP servers (rogue) from operating on network

enable on layer 2 switch ports

DHCP clients send 4 packets back and forth:

. DHCP discover - client send message asking server for lease

. DHCP offer - server answers offering lease: IP address, subnet mask, default gateway...

. DHCP request - client responds by requesting offered lease

-llocates

by requesting

- DHCP acknowledge - allocates offered IP address to client and sends back acknowledge packet

normally switch sends all broadcast traffic to all ports

DHCP snooping will change to send to only trusted ports

DHCP server connected to port 1

enable snooping

now only DHCP server messages from port 1 allowed

Domain Name Resolution use case

DNS servers host data in zones or db

Zones include records like:

record holds hostname

Zones include

- A - host record, holds hostname and IPv4 address
  most common
  DNS client queries DNS with name using a forward lookup request
  DNS responds with IPv4 address
- AAAA - hostname and IPv6
- PTR - pointer record, opposite of A
  DNS client queries w/ IP address to get name
  reverse lookup, doesn't always work
- MX - mail exchange
  identifies a mail server
  linked to A or AAAA
  when there are more than 2,
  [illegible] preference # is

when there
lowest preference # is
primary

- CNAME - canonical name or alias
  single system to have multiple names associated with single IP
- SOA - start of authority includes info about DNS zone and some settings
  lists TTL settings for DNS records (how long to cache records)

Most DNS servers run Berkeley Internet Name Domain BIND
sometimes DNS servers share info w/ each other in zone transfer
# of records but

w/ each

mostly small # of records

sometimes all

use TCP port 53 for zone transfer

UDP port 53 for name resolution queries

DNSSEC

DNS poisoning - modify DNS cache with different IP

can modify A or AAAA record for trusted site

Domain name system security extensions

DNSSEC - suite of extensions for DNS front providers validation for DNS responses

adds resource record signature RRSIG or digital signature to each record

Nslookup and dig

nslookup - name server lookup
troubleshoot problems w/ DNS
check if it can resolve hostnames
or **fully qualified domain names** **FQDN** - includes
hostname and domain name

dig - replace nslookup on linux
domain info proper

Subscription services use case

common for sub services to use
HTTPS

when sub ends, send email
using SMTP

Quality of service

quality of service **QoS** - tech
running on network that
measure and control different

measure and control
traffic types

allow admin to prio certain traffic

ex: people streaming video at work make VoIP worse

QoL can prio VoIP

Understanding Basic Network Devices

networks connect devices together to share resources

any device w/ IP is a host, client, or node

switch - connect hosts together in network

router - connect multiple networks together

routers ... together

methods IPv4 uses when addressing TCP/IP traffic

- **Unicast**
  1:1 host → host
  other hosts may see but not process
- **broadcast**
  1:all host → all hosts
  broadcast IP like 255.255...
  switches pass to all ports
  Routers do not pass

Switches

switch - can learn pcs attached to its ports

uses knowledge to create ... forward switched connections

uses [illegible]
internal switched connections
when 2 pcs comm

ex: when a switch turns on,
has no knowledge other than
that it has ports

1 device sends packet
switch doesn't know who is
who yet, so sends to
all ports

caches device MAC addr so
it knows to send addr
packets to it

the dest device will respond
and send packet w/ its
MAC addr

switch caches 2nd MAC addr

Security Benefit of a Switch

in the previous example, an
[illegible] be

in the previous example, an attacker would not be able to capture unicast packets because of switch

Port security

port security limits # of pcs that can connect to ports on switch

most basic level: disable unused ports

ensure RJ-45 wall jacks lead to specific ports

MAC filtering - switch remembers first 2 or 2 MAC addresses that connect to port

blocks all others

can also manually set to only accept from specific MAC

Broadcast storm and Loop Prevention

bridge loop - floods

Broadcast storm

switch loop or bridge loop - floods network w/ traffic and can disable switch

ex: user connects two ports of switch together w/ cable

creates loop where constantly sends and resends unicast transmission

Spanning tree protocol STP or Rapid STP RSTP - provide broadcast storm prevention and loop prevention

Bridge Protocol Data Unit Guard

STP sends Bridge protocol data unit BPDU messages in network to detect loops

when loops are detected, STP shuts down or blocks traffic

shuts down or blocks traffic from ports sending redundant

switches exchange BPDU using non-edge ports

edge port - switch port connected to device

these should not be sending BPDU messages

BPDU guard to detect messages on edge ports

Routers

router - connects multiple network segments into single network

routes traffic between segments

routers don't pass broadcasts so reduce load

segments separated by routers are called broadcast domains

want to make sure pcs are split evenly & broadcast

broadc

want to make sure pcs are sp

Solution also creates separate broadcast domains

most are physical but can add routing software to pcs w/ more than one NIC

ex: Windows Server products can function as routers

Routers and ACLs

Access control lists ACL - rules implemented on router and firewalls to identify which traffic allowed

router ACL provide basic packet filtering based on IP, port, some protocols

IP addresses and networks

add rule to block device based on IP

can block traffic from 1 subnet to another based on subnet ID

ports

logical

ports

block traffic based on logical ports

ex: block 443 traffic

choose to block incoming/outgoing

protocol numbers

protocols often referred to by their protocol #

ex: ICMP = 1

block traffic to only packets encrypted with IPsec or protocol 50

PPTP - point to point tunneling protocol; obsolete VPN implement

Implicit Deny

all traffic that isn't explicitly allowed is implicitly denied

Last rule in ACL

Last rule in ...

DENY ANY ANY

DENY ALL ALL

Remember

routers and stateless firewalls allow basic filtering with an ACL

implicit deny is last rule in ACL

Route Command and Route Security

route - display or modify system's routing table

Windows & Linux

route print - see all paths known by pc to other networks

if no entry for a network, uses

default gateway - IP of a router on network that provides path to internet

... to different network

route add - add path to different network

attackers can modify routing tables for systems to reroute traffic to different router and use it to capture traffic

Firewalls

filter incoming/outgoing traffic for a single host or between networks

Host-based Firewalls

host-based firewall - monitors traffic in and out of single host server/workstation

monitors traffic going in/out of NIC

Many OS have software based firewall as host based firewall

defense-in-depth: have personal firewalls and network firewalls

hardware firewalls

Firewall

Software versus hardware firewalls

Software Firewall - app running on system

Network-based firewall typically hardware system with software to monitor filter, and log traffic

would have two or more NIC and all traffic passes through firewall

most orgs include one network-based firewall at network border between intranet and internet

Linux systems include iptables, ipv6tables, arptables

known as **xtables** - configure rules in them to function as an ACL

Stateless firewalls

Stateless firewalls - use rules in ACL

Stateless firewalls - use rules to identify allow/block traffic

'implicit deny

ACL roles

- permission
  PERMIT or ALLOW
  DENY

- Protocol
  typically see TCP or UDP
  if you want to block TCP & UDP using same port use IP
  ex: ICMP

- source
  singe IP, subnet, or wildcard for all

- destination

- Port or protocol
  ex like 443

- Port or protocol
  use number like 443
  keywords like eq for =

some firewall make you include subnet mask

192.168.1.0/24 = mask 255.255.255.0

Remember

deny any any, deny any, drop all statement as last ACL rule

Stateful versus Stateless

Stateful firewall - inspects traffic and makes decisions based on traffic context or state

keeps track of established sessions, inspects traffic based on state with session

blocks traffic not in session

ex: firewall detects TCP connection [illegible] and blocks

ex: firewall detects
without handshake and blocks
it

common issue with stateless firewall
is misconfigured ACL

Web Application Firewall

firewall specifically for web apps

WAF placed between web server
and web server clients

can be standalone or software
added to another device

protects from XSS

would not replace network firewall
would be another layer

Remember

Stateless uses ACL

Stateful blocks based on state
of packet in session

Stateful
of packet in session

Next-generation Firewall

next-generation firewall NGFW

adds additional capabilities

1st gen = stateless

2nd gen = stateful

Next gen - performs deep packet inspection; app-level inspection as core feature

can identify app commands and detect potentially malicious traffic

Implementing Network Designs

segmenting and isolating good for security and performance

Intranet versus extranet

network directly to

Intranet versus

rare to connect network directly to internet

common to divide network into different zones using different topologies

intranet - internal network

extranet - can be accessed by auth entities from outside of network

network perimeter - boundary between intranet and internet

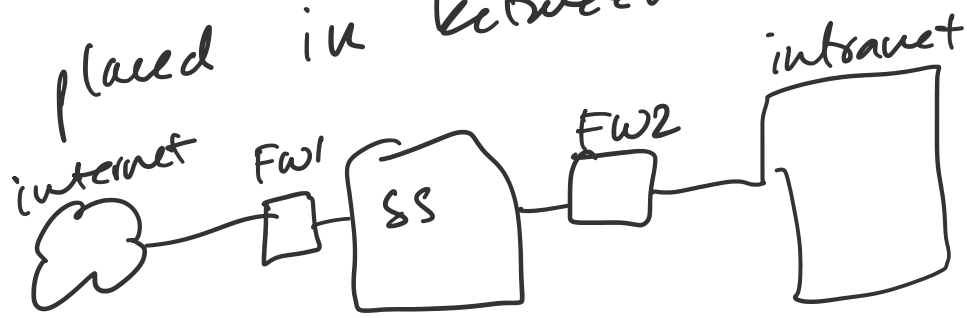
screened subnet

screened subnet - or DMZ; buffered zone between private network and internet

attackers seek out servers so any server directly on internet is at risk

screened subnet provides layer of protection for internet-facing

servers placed in between 2 firewalls



Network Address Translation Gateway

network address translation NAT - translate public IP to private IP and vice versa

NAT gateway - hosts NAT and provides internal clients w/ private IP a path to internet

also possible to enable NAT on internet facing firewall

Port address translation PAT - network address and port translation

Benefits of NAT

- public IP dont need to be bought for all clients

- public
  all circuits
- NAT hides internal pcs from internet

NAT is not compatible with IPsec

Static NAT - uses single public IP in 1:1 mapping

Dynamic NAT - multiple public IP in 1:many mapping

if lots of private IP going to 1 public, will send next requests to other public IP

Physical Isolation and Air Gaps

physical isolation - one network isnt connected to another network

Supervisory control and data acquisition

SCADA - industrial controls in infra facilities

operate in own network but must they are isolated

operate in own

to make sure they are isolated from any other network

air gap - physical isolation w/ gap of air between isolated system and other systems

ex: red (classified) and black (unclassified) networks should not be connected to each other

Logical separation and segmentation

routers and firewalls provide separation and segmentation

routers segment traffic in net w/ ACL

advice use subnetting to divide up larger IP

firewall separate traffic using packet filtering

Virtual local area network VLAN
provide local separation

Isolating traffic with a VLAN

VLAN uses switch group for diff
pcs in virtual network
group based on dep./job, etc.

isolate traffic between pcs in VLAN

manually sorts groups based on location
layer 3 switch can create
multiple VLAN to separate pcs
based on logical needs

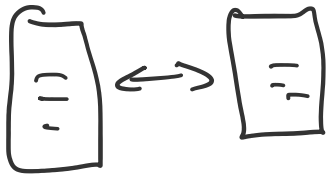
EX: VoIP takes a lot of bandwidth
could set all VoIP to its own
VLAN

East-West Traffic

east-west traffic - traffic between
a network

east-west traffic - traffic between servers in a network

horizontal traffic



vertical traffic is client to server

Zero Trust

zero trust network - default does not trust any devices

one way to implement is MFA

Network Appliances

network appliances - dedicated systems to fulfill specific need

Proxy Servers

proxy servers - forward requests for services from clients

can cache and filter content

sits on edge of network bordering internet and intranet

configure clients to use proxy for specific protocols

mostly for HTTP / HTTPS but can also be for other internet protocols like FTP

Caching Content for performance

cache results from internet so it doesnt have to fetch again

Transparent Proxy Versus Non-transparent Proxy

transparent proxy - accept and forward

transparent proxy - accept and forward requests without modifying them

non-transparent proxy - modify and filter requests

URL filters

3rd parties sell subs to URL filter lists

Reverse Proxy

reverse proxy - accepts traffic from internet

appears to clients as a web server

can be use for single web server or web farm

acts as a load balancer for web farms

Unified Threat Management

+ services

Unified Threat Management

UTM - single solution that provides multiple security controls

includes many features to reduce admin workload

Some features

- URL filtering - like a proxy server
- malware inspection
- content inspection
- DDoS Mitigator

place on network border

Jump Server

jump server - or jump box is a hardened server used to access and manage devices in another network within diff security zone

- safely access to devices

use to safely access to devices in screened subnet from internal network

ssh -j maggie@jump maggie@CT7

-j connects to jump server and TCP forwards to CT

can also use jump to connect to internal network such as SCADA isolated in VLAN

security implications of IPv6

risks of IPv6 on internal networks

ex: all devices dont support natively

might not recognize or know what to do with IPv6

on IPv4 firewalls

and Switches

on [illegible]

Summarizing Routing and Switching use cases

Switches

- prevent switch loops
- prevent BPDU attacks
- prevent unauth users from using unused ports
- increased segmentation of user pcs

Simple network management protocol version 3 SNMPv3 - monitors and manages network devices (like routers and switches

device traps - SNMPv3 agents on clients send messages to manager

encrypts credentials

encrypts credentials

UDP ports 161 and 162

Assessment Notes

1. Legacy protocol used to access browser based interfaces on switches and routers in network which to upgrade?

   TLS

2. Confidential data transferred over internal network be encrypted

   SSH

3. Need to collect network config info and net stats from devices

   SNMPv3

type=mx jcqa.com

4. nslookup -querytype=mx gcga.com

Server = Unknown

states that it is not using PTR; not a reverse lookup

address: 10.0.0.1

this is DNS address

less preference # is primary

5. DNSSEC
   - RRSIG - resource record sig
   - A
   - AAAA

6. What to use after creating SSH key-pair?

ssh-copy-id -i ~.ssh/id_rsa.pub maggie@goga

maggie&gogo

7. Network time protocol NTP

time synch

8. Disable ports = min unauth access to switches

Spanning tree protocol STP stops switch loops

Dynamic Host configuration protocol dynamically issue IP

9. Send creds for manage network devices remotely

SSH

10. Firewall

permit IP any any eq 80

any eq 443

permit IP any any
permit IP any any eq 443

forward proxy does not need ACL

11. HTTP outbound should be blocked because insecure web traffic

telnet was wrong because the wrong IP was used meaning it wouldnt matter if it was enabled

12. Air gap completely isolates systems from all other systems

two pcs in question "doesnt specify that they need to be connected to each other" so separate [illegible] not needed

to each other
isolated network not needed

13. Need to add a path to a different network

route add

14. Stateful firewall can block TCP traffic that didnt use handshake

15. DNS requests use UDP port 53
DNS zone transfers use TCP port 53

IP rule ACL will block all
or just use implicit deny

DNS zone transfer is between
other

DNS zone

each other

makes sense it is TCP

regular requests need the speed

of UDP probably