COMPTIA3--NETWORK

SNIFFING ATTACK. usises a protocol analyzer to capture data sent over network.
ddos/dos

service attack forom a single source to disrupt network service. ddos(multiple sources and multipe ips)

tcp ip
smtp(simple mail transfer protocol.
tcp 3 way handschake. syn, ack --synack)

ARP adress resolution protocol

voice and video use case

treal time transport delivers audio ad video over ip networks.

secure real time transport protocoal
SRTP

provides encryption message authentication and integrity for rtp(real time transport protocol)

srtp helps protect the confidentiality of data from these attacks whle ensurign data transmissions integrity... this protects against replay attacks. in a replay attack an attacker captiuures data sent from between two entities modifies it and then attempts to impersonate one of the parties by replaying the data srtp can be used for both unicast transmissions. and multicast

SIP session initioan protocal used to initiate maintaine and terminate voice video and messaing sessions. sip ESTABLISTES THE SESSION rtp ESTABLISHES THE SESSION.

FILE TRANSFER USE CASE..
DATA IN TRANSIT IS ANY TRAFFIC SENT OVER A NETWORK.
**secure shell encrypts traffic over tcp port 22 and is used to transfer encrypted files over a network transport layer security is a replacement for ssl and is used to encrypt many different types of protocals including browser based connections using https secure ftp sftp uses ssh to encrypt traffic ftp secure ftps uses tls to encrypt traffic. **

FTP file transfer proltocol. uploads and downloads large files

**tftp **trivial file transfer protol. uses udp Port 69 and is used to encrypt other protocols such as ftp. uses small amounts of data such as communicating withnetwork devices. many attacks ave used tftp, but it is not an essential protocal

SSH encrypts traffic in traypts traffic. it uses TCP port 22
nsit and can be used to encrypt other protocals such as ftp scp is based on ssh nd is used to copy encrypted files over a network. SSH can also encrypt tcp wrappers.. a thype of access control list is used on linux systems to filter traffic. when ssh encrt

TRANSPORT LAYER SECUIRTY POROTOCOL is the designated replacement for SSL and should be used instead of ssl for browsers using HTTS..
SSL secure sockets layer protocal was the primary method used oto secure http traffic as a hypertext transfer protocl secure. . ssl can encrypt other types of ttaffic, suc as smtp ldap (lightweight directory access protocol.. however has been compromised, and should not be used.)

iIPSEC

IS USED TO ENCRYPT ip TRAFFIC. IT IS NATIVE TO IPV6, BUT also works with ipv4. ipsec encapsulates and encrypts IP packet payloads and uses tunnel mode. to protect virtual private network traffic. IPSEC includes two main components. authentication header AH identfied by protocol ID number 51, ecampsualating security payload. identified by protocol. id number 50. SFTP is a secure implementatiom of FTP it is an extesion of secure sehll, using ssh to transmit the files in a n encrypted format..

**ssl versus tls

ssl has been P. not recommentd. september, a team at google discovered a serious vulnerability. with ssl they nicknamed the POODLE attack. POODLE IS short for padding oracle on downgraded legacy encryption. the SSL protocol is not maintained or patches. so this vulnerability remains..
this is one fot hte reasons that the us goverment amd many other organizations prohibit the use of SSL to protect any sensitive data.. NIST national institute. of standards and technology special publication 800 52 rev 2 guidelines for the selection configuration and use transport layer secuirty implementations specifically states that federal agencies should not usE ssl***

FTPS FILE TRANSFER PROTOCOL SECURE FTPS AN EXTENSION OF FTP USES TLS TO ENCRYPT FTP TRAFFIC..
SOME IMPLEMENTATIONS OF FTPS US TCP PORTS 989 AND 990 TLS CAN ENCRYPT THE TRAFFIC OVER PORTS USED BY FTP (20 AND 21)
TLS IS RECOMMENDED REPLACEMENT..
EMAIL AND WEB USE CASES.

SMTP SIMPLE MAIL TRANSFER PROTOCOL, TRANSFERS EMAIL BETWEEN CLIENTS AND SMTP SERVERS SMTP USES TCP PORT 25 FOR UNENCRYPTED EMAIL AND PORT 587

POP3 and SECURE pop Pos Office Protocol v3 POP transfers emails from servers down to clients. Pop3 uses tcp port 110 for unencrypted connections.
IMPA4 ND SECURE IMAP INTENET MESSAGE ACCES PROTOCOL VERSION 4 IMAP4 IS USED TO STORE EMAIL ON A EMAIL SERVER IT ALLOWS USERS TO ORGANIZE AND MANAGE EMAIL IN

FOLDERS ON THE SERVER AS AN EPMPLE GOOGLE MAIL USES IMAP4 IMAP4 USES TCP PORT 143 UNENCRYPTED CONNECTIONS AND TCP PORT 993 FOR ENCRYPTED MESSAGES.

DHcp snooping. --to prevent unauthorized DHCP servers often called (rogue dhcp serve3rs)opereating on a network. you enable it on layer 2 switch ports.

DHCP DDISCOVER BROADASTING MESSAGE ASKING A DHCP SERVER FOR A LEASE.
DHCP OFER A SERVER ANSWERS OFFERING A LEASE.. THIS INCLUDES AN IP ADRESS A SUBNET MASK A DEFAULKT GATEWAY AND MORE DEPENDING.
DHCP REQUEST.. CLIENT RESPONTS BY REQUESTING OFFERED LEASE
DHCP ACKNOWLEDGE ALLOCATES THE OFFERED IP TO THE DHCP CLIENT SENDS AN ACKNOWLEDE PACKET.

DNS domain name resolution resolves hostnames to IP ADRESSES.. sYSTEMS ARE CONSTANTLY QUERYING dns THOUGH IT IS USUALLY TRANSPARENT TO USERS.. DSN CLIENT..
A. ALSO CALLED A HOST RECORD.. HOLDS THE HOSTNAME AND IPV4 ADRESS AND IS THE MOST COMMONLY . THE FOLLOWING

AAAA this record holds the hostname and ipv6 adre3ss, its similar to an a record exvept that it is for ipv6
PTR ALSO CALLED A POINTER RECORD it is the opposite of an A record instad of a DNS clientqueryng dns with the name. the DNS client queries the dns with the IP ADRESS. MX also called mail exchange or mail exchanger. an mx record identifies a mail server used for email. the mx record is linked to the A record in AAAA record of a mail server. when there is one mail server the one with the lowest performance number in the mxx record is the primary mail server.

CNAME. A canonical name or alias allows a sigle system to have multiple names associated with a single ip address for example a servwer named Awecwe

SOA THE START OF AUTHORITY RECORD INCLUDES INFO ABOUT THE DNS ZONE AND SOME OF ITS SETTING.. ttl time to live settings for dns records. DNS clients use the ttlsetting to determine how ling to cache DNS results TTL times are in seconds and lower times cause clients to renew the records mre often. Most DNS servers on the internet run berkely internet Name Domain. BIND>

Directory services such as Microsoft active directory domainservices ad ds provide authentication services for a network adds users ldap encryped with Tls when querying the directory

DNSSEC dns poisoning.. successful attackers modify the dns cache with a bogus ip adress. """"sending users to malicious adresses, when intention was a good ip..

Domain name system security extensions. a sweute of extensions to dns that provides validation for dns responses.. it adds resource record signature.

NSLOOKUP command short for name server lookup to troubleshoot problems related to DNS.

the DIG command

line tool has been replaced nslppkup on linux systems.??

example of DIg

```
global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29363
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;. IN NS

;; ANSWER SECTION:
. 496068 IN NS k.root-servers.net.
. 496068 IN NS l.root-servers.net.
. 496068 IN NS m.root-servers.net.
. 496068 IN NS a.root-servers.net.
. 496068 IN NS b.root-servers.net.
. 496068 IN NS c.root-servers.net.
. 496068 IN NS d.root-servers.net.
. 496068 IN NS e.root-servers.net.
. 496068 IN NS f.root-servers.net.
. 496068 IN NS g.root-servers.net.
. 496068 IN NS h.root-servers.net.
. 496068 IN NS i.root-servers.net.
. 496068 IN NS j.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 529190 IN A 198.41.0.4
a.root-servers.net. 529212 IN AAAA 2001:503:ba3e::2:30
b.root-servers.net. 529195 IN A 199.9.14.201
b.root-servers.net. 529195 IN AAAA 2001:500:200::b
c.root-servers.net. 529191 IN A 192.33.4.12
c.root-servers.net. 529191 IN AAAA 2001:500:2::c
d.root-servers.net. 529190 IN A 199.7.91.13
d.root-servers.net. 529190 IN AAAA 2001:500:2d::d
e.root-servers.net. 544003 IN A 192.203.230.10
e.root-servers.net. 530448 IN AAAA 2001:500:a8::e
f.root-servers.net. 529190 IN A 192.5.5.241
f.root-servers.net. 529190 IN AAAA 2001:500:2f::f
g.root-servers.net. 137626 IN A 192.112.36.4
g.root-servers.net. 530448 IN AAAA 2001:500:12::d0d
```

```
h.root-servers.net. 529194 IN A 198.97.190.53
h.root-servers.net. 529194 IN AAAA 2001:500:1::53
i.root-servers.net. 529194 IN A 192.36.148.17
i.root-servers.net. 529194 IN AAAA 2001:7fe::53
j.root-servers.net. 529191 IN A 192.58.128.30
j.root-servers.net. 529191 IN AAAA 2001:503:c27::2:30
k.root-servers.net. 529192 IN A 193.0.14.129
k.root-servers.net. 529190 IN AAAA 2001:7fd::1
l.root-servers.net. 529191 IN A 199.7.83.42
l.root-servers.net. 529191 IN AAAA 2001:500:9f::42
m.root-servers.net. 529199 IN A 202.12.27.33
m.root-servers.net. 529199 IN AAAA 2001:dc3::35

;; Query time: 31 msec
;; SERVER: 75.75.75.75#53(75.75.75.75) (UDP)
;; WHEN: Sun Oct 22 18:07:15 EDT 2023
;; MSG SIZE rcvd: 8
```