Unit 4.

Q.1] How to configure the firewall.

=>.

① Network host-based firewall.

- Firewall installed on existing machine with an existing OS.
- No matter how good firewall, it depends on OS only.
- Hence the device should have hardened OS.

② Dual-homed host:

- It is firewall running on server with at least 2 n/w interfaces.
- Automatic routing fn is disabled.
- i.e. If packet from internet isn't directly routed to n/w.
- We can choose what & how to route packets.

- Systems inside & outside firewall can communicate with dual-homed host, but can't communicate directly with each other.

③ Router based firewall

- Implements firewall protection on router.
- In n/w with multiple layer of protection it is first layer
- most common type of firewall used today
- Packet filtering.

(4) Screened Host

- Combination of firewalls : bastion host & screening router.

- Screening router adds security by allowing ~~permission~~ to deny or permit certain traffic from bastion host.

22] Intrusion Detection System

- IDS inspects all inbound & outbound port activity on machine / firewall / system.
- It looks for patterns that might indicate break-in attempts.

- eg: If IDS finds series of ICMP packets were sent to each other port in sequence, this probably indicates that system is being scanned by n/w scanning s/w, such as Cerberus.

- Most common IDS categorization.

(1) Passive IDS

- Just monitors suspicious activity & logs it.
- May also notify this activity to administrator.
- It is most basic type of IDS.
- Any modern system should have, at a minimum, a passive IDS along with firewall, antivirus & other basic security measures.

② Active IDS

- Also called as IPSs (Intrusion Prevention Systems).
- Shuts down suspect comm^.

- It can be false positive (like antivirus). i.e. Might suspect something is an attack when in fact it is legitimate ~~attac~~ traffic.

- Imagine a user ~~wo~~ works bet^ 8 am to 5pm & uses small amount of bandwidth. If IDS detects user at 10 pm using 10 times the normal bandwidth, it considers as an attack & shut down offending traffic.

- But if it was user working for urgent thing, it'd be false positive.

- Hence risk analysis should be done. & decide whether passive IDS or IPS is appropriate.

- IDS elements
- Sensor // collects data & passes to analyzer
- analyzer // analyzes data.
- manager // used for management. It is s/w component
- operator // person
- Notification // alerts the operator.
- Activity // element of data source of operator.
- Event // suspicious activity, Possible attack.
- Alert // Msg from analyzer of an event occurance.
- data source.

Q3] Digital Certificates:

- The most common method to provide people with public key is via Digital certificate.
- It contains user's public key, with other info.

- It provides a means for authenticating that holder of certificate is who she claims to be.

- X.509 is international standard for format & information contained in Digital Certificate.
- Also most common type (X.509).
- It is digital document that contains public key signed by trusted third party known as certificate authority (CA).

- Basic items in X.509.

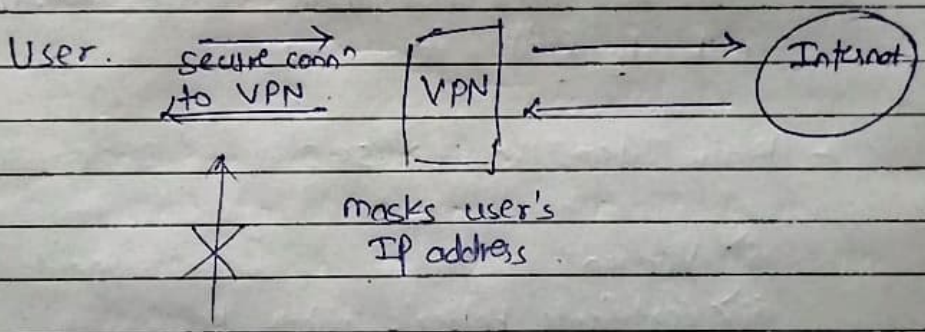
i) Version
ii) Certificate holder's public key
iii) Serial number // Unique id for this certificate.
iv) Certificate holder's unique name // domain name / email
v) Certificate's validity period // 1 yr is most common.
vi) Unique name of certificate issuer
vii) Digital sign.. of issuer
viii) Signature algorithm identifier

VPN (Virtual Private Network)

- It is a n/w service that helps to stay private online by encrypting the connection bet^n your device & internet.

- It creates virtual conn^ bet^n remote user & central location.

- This secure conn^ provides private tunnel while you use public networks.



- Three different protocols are used to create a VPN.

① PPTP (Point-to-point Tunneling Protocol).

i) Security :
- Least secure among 3 others.
- Provides encryption for data transmission.
- Uses Microsoft point-to-point encryption (MPPE).

ii) Encryption :
- MPPE uses RC4 stream cipher encryption.
- Weak compared to modern encryption algorithms.

iii) Authentication:

- Supports basic form of authentication using MS-CHAP (Challenger Handshake Auth^n Protocol) or EAP (Extensible Auth^n Protocol)
- Less secure compared to L2TP / IPsec.

(2) L2TP (Layer 2 Tunneling Protocol).

i) Security:
- L2TP relies of IPsec for encryption, auth^n & integrity protection.

ii) Encryption:
- Relies on IPsec over the VPN tunnel.
- Robust encryption algorithm like AES (Advanced Encryption Standard) are used.

iii) Authentication:
- Auth^n methods like MS-CHAP v2, EAP & certificates are supported.
- Auth^n is performed at VPN server

(3) IPsec (Internet Protocol Security).

i) Security.
- Latest, encrypts packet payload & header.

ii) Encryption:
- Algorithms: AES, 3DES.
- Encrypts before transmission, hence ensures confidentiality

iii) Authentication:
- Auth^n methods: pre-shared keys, digital cert., public key infrastructure (PKI)

Unit 6:

Q.2] OS utilities:

- They are powerful tools for forensic investigations. for gathering data.
- Conducting forensic work is to be familiar with target OS
- Since Windows is most commonly used OS utilities provided below work on Windows Command Line.
- Also these commands are most useful on live running system to catch attacks in progress.

① Net Sessions.

- Lists active sessions connected to computer on which you run it.
- Crucial for determining if an attack is ongoing & who may be accessing the system remotely.

Syntax: net session.

② Open files

- Lists any shared files that are currently open.

Syntax: openfiles

③ Fc

- (File Compare) Fc command is used to compare 2 files & display the differences.
- If a config file has been altered, you can compare it to backup.

Syntax:
fc testfile1.txt testfile2.txt

④ Netstat.
- Lists all current n/w connections..
- Not just inbound, outbound as well.

Syntax: netstat
netstat -an.

// - an is for active n/w conn^