Page No.
Date

Illustrate Network Security with Eg.

* Network Security
Protection of CIA of Network assets & services from associated Threats & Vulnerabilities

* Security Requirements.
① Integrity: Assurance that info has not been modified unauthorizedly
② Availability: Not able to use sys when desired
③ Confidentiality: Protection from disclosure to unauthorized person.
④ Non Repudation: Refusal of sending the message, Digital Signature.

* Network Asset.
It is something to which an organization assigns value & hence for which it requires protection.
Hardware: Server, client, STA, router, bridges.
Software: Network/Client OS, App, tools.
Data/Info: Org. data (DB, email), Network data, conf, setting, User Access.

* Threats: Can put damage/harm/loss to assets.
Threats are:
① Damage to Comm. lines.
② Deterioration of storage media
③ H/w Failure
④ Malicious S/w
⑤ Misuse of resources
⑥ Unauthorized access

Page No.
Date

Physical Threats.

(7) Theft, Fire, Flood, lighting, Earthquake, Power Fluctuation, Extreme temp., humidity.

(8) Staff Storage, Misrouting / Rerouting.

* What is Vulnerability
- Weakness associated with assets.
- Weakness may be exploited by threats causing loss/damage/harm to assets.
- Vulnerability in itself does not cause harm until exploited.

Eg.
- Insufficient Security training
- lack of security awareness
- Inadequate recruitment procedure
- Insufficient preventive maintenance
- Transfer of passwords in clear
- Unprotected public network connections.
- Poor password management.
- Well known flaw in SW
- Unsupervised work by outside staff.
- Lack of security policies.
- Unprotected communication lines.
- Poor cable joint
- Firewall is bypassed
- Gateway is bypassed
- Inadequate network mgmt.
- Lack of audit Trail (Check who is communicating)

* Security Mechanism

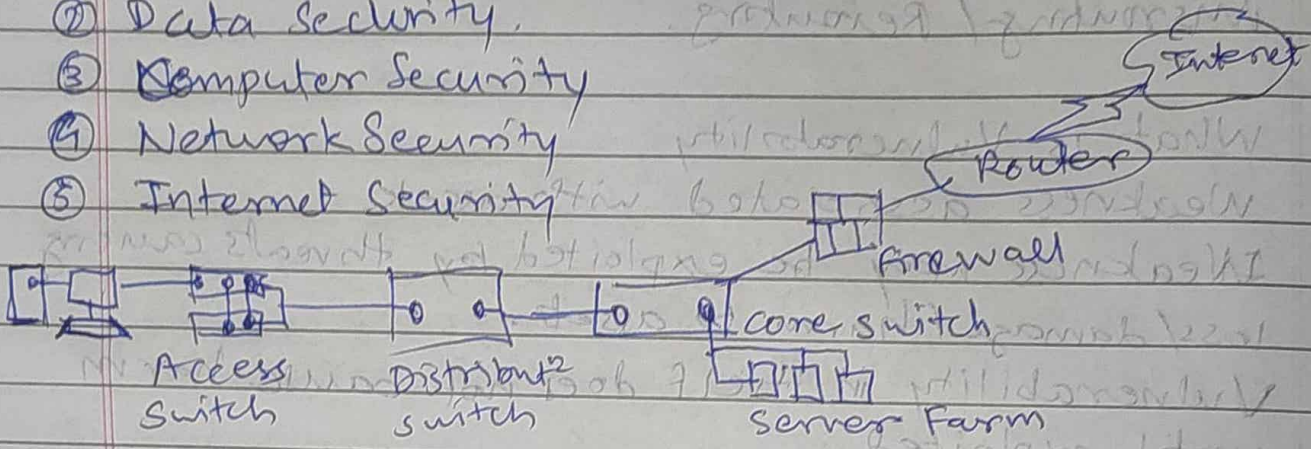
① System Security : Nothing bad happens to my Computer virus, logic bomb, etc.

② Data Security.

③ Computer Security

④ Network Security

⑤ Internet Security



Applayer	DNS	SNMP	FTP & TFTP	HTTP	SMTP
Transport	UDP	TCP			
Internet	IP	ICMP	RIP, BGP, OSPF, EGP		
	ARP	RARP			
Network Interface Layer	SLIP	PPP	Ethernet		

* Network Security Mgmt. → TCP/IP Stack (diagram)

* Categories of attack. TCP/IP attacks.

Communication → src → dest

① Interruption

② Interception

③ Modification

④ Fabrication

KDD dataset
NSL dataset

Page No.
Date

* TCP/IP with corr. categories:

①	Probe	Attack Types for them.
②	DoS	
③	R2L (Root to Local)	
④	U2R (User to root)	

Q An IP datagram has arrived with info Header in Hex as
4500 0054 0003 0000 0106 0000 7C4E 0302 B40E 0F02
- Are there any options. - NO
- is packet fragmented
- What is size of data
- Is a checksum used
- How many more routers can the pkt travel to
- What is identification no. of pkt.
- What is the type of the service
Justify ans. with reason.

• IP Datagram
TTL = 0 → Packet is dropped

4	5	00	0054	0003	0000	0106	0000	7C4E0302	B40E0F02
Ans ④		8	16	16	3	13	8	8	16
Ver	HLEN	Service Type	Total len	Identif.	Flag	Frag' off.	TTL	Protocol	Header checksum

7C4E0302	B40E0F02		
32 bit (ipv4)	128. ipv6	options	data
Src ip	Dest. ip		

↑ No options

Q1 HLEN = $(5)_{16}$ = 5 × 4 = 20 byte
→ Head length − Actual HLEN = 20 − 20 = 0
→ Option size = 0

Page No.
Date

Q2 Is pkt frag? 7th & 8th bytes = 0000
→ Not fragmented
frag. offset = 13 bits

Q3 - Data size = Total length - header len.
- Tot len = $(54)_{16}$ = HLEN $(01011010)_2 = (84)_{10}$ Hex → bin → decimal
Data size = 84 - 20 = 64 bytes.

Q4 11th & 12th by = $(0000)_{16}$
∴ checksum is not used.

Q5 How many more routers can pkt travel to.
TTL (9th byte) = $(20)_{16} = 00100000 = (32)_{10}$
∴ datagram can travel to 32 more routers.

Q6 Identification no. of pkt?
5th & 6th byte = 00 03
∴ Id. of pkt = $(0003)_{16} = (0003)_{10}$

Q7 Type of Service (TOS) provided by DS (differentiated service) field in IP datagram. which has format
→ DS is 2nd byte as $(00)_{16}$
∴ TOS = 0000 default.
∴ Default service is provided by packet.

Page No.
Date

* Application Layer
- DNS : ~~SNMP, FTP~~ - Protocol
- DOS : Attack
apache, back, land, mailbomb, neptune, pod, processtable, smurf, teardrop, udpstorm, ~~arppoison~~ arp poison, crashiis, dosnuke, mailbomb, queue

Q Generate Question (Header of DNS) similar to previous question.

- Tool : Network Miner.
capture traffic

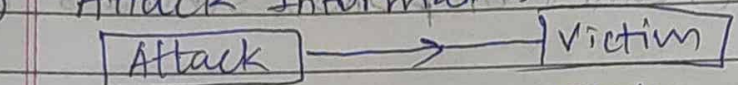
Eg (1) { if (Src_add_ip == src addr_ethr)
{ detect as "normal pkt"
Return True;
}
Else { ~~retun~~ Detect attack as "IP spoofing" }
END;
}

(2) Fragmentation Attack
capture traffic {
Filter ICMP pkt.
{ if (m tv > us cd)
For (i=0, i<=n, i++)
{ sequence shld be n:0;
IF (MF_last=1 || MF_more==1)
Frag_offset=0;
Detect attack as "IP frag. attack"
}
END)
}

Page No.
Date

* DNS Packet

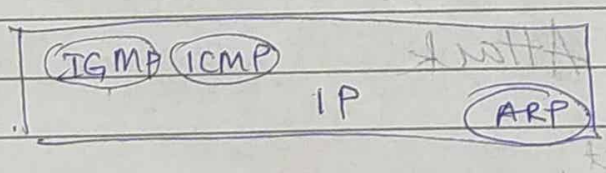
1) Prepare questions
2) Weaknesses or Vulnerabilities in Protocol
3) Vulner 1 - Attack 1
   Vulner 2 - Attack 2
   Vulner 3 - Attack 3
4) Experiment - Do attack. — OS commands / Tools — Network Miner Tool
5) Attack Information



TCP/IP
TCP/IP
(Attack Info)
log file

* ICMP

- IP protocol has no error reporting/error correcting mechanism
- What happens if router must discard a datagram because it can not find a router to final dst or TTL=0?

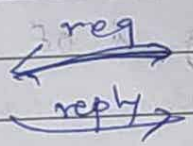


Q An ICMP msg arrived with hex header 03031020000000000
What is type of msg.? What is code.? What is purpose of msg.

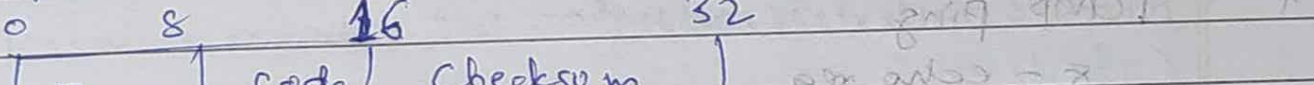
* What is ICMP?
protocol that network devices

2. what happens if final dst. host must discard all frag. datagram.

* ICMP



* Pkt Structure. (3 Fields are there)



Category	Type	Msg.
Error reporting	3	Dst unreachable
	4	source quench
	11	Time exceeded
	12	Param problem
	5	Redirection.
query msg.	8 or 0	Echo req./reply.
	13/14	Timestamp req./reply.

Ans (i) 03 03 10 20 00 00 00 00
Type of msg. given by first byte in ICMP
In our ICMP msg. the first byte is $(03)_{16}$
∴ Type = $(03)_{16}$
Which is of form or 03 means dst. unreachable.

(ii) Code is given by 2nd byte in ICMP.
In our ICMP msg. the code field = $(03)_{16}$
$\therefore$ Code = $(03)_{16}$.
03 - port is unreachable
Not running.

(iii) Hence it is error reporting msg. & of type 3
(As port is unreachable)

~~8 - Ech~~

* ICMP ping
8 - echo req.
0 - echo reply

* Smurf Attack
capture traffic ⇒ filter PKT ⇒ 8 ICMP-request
while (PKT-type == ECHO)
{ if (DST-IP == broadcast-IP)
Detect Attack as "ICMP smurf attack" }.
}

* ICMP Ping of Death
Attacker sends huge no. of "ECHO-REQ" ping
IP.4 ping pkts are much larger & can be as large as maximum allowable pkt. size of 65535 bytes.

Capture all traffic
{ Filter (PKT == ICMP_ECHO)
If (PKT_SIZE > 65535)
PKT_COUNT == 1000
Detect attack as "ICMP Ping of death attack"
}

ping command.

Page No. 8
Date 30 | 11 | 2020

* ICMP Flood Attack
  Capture all packets.
  { filter(ICMP_REPLY)
  if(PACKET_COUNT > 10 && PKT_SIZE => 65535)
  Detect attack as "ICMP Flood attack"
  } END;

- Attacker sends large vol. of ICMP echo req. pck. to victim
- Causes DoS attack.

* Tunnel Attack,
  (Install firewall / Set intrusion detection system)

* Twinge Attack
* ICMP Ping sweep

do attyack!!!

Cyber Crime

* Information Technology Act, 2000
- Provide legal recognition for the transactions carried out by means of electronic data interchange & other means of electronic communication, commonly referred to as 'Electronic Commerce' which involve use of alternatives to paper based methods.

- Law includes any Act of Parliament or of State legislature

* Article 240 - Power of President to make regulations for certain Union territories
* Article 357 : (1) (2)
* Article 21: Protection of life & Personal Liberty

- Protection of Life meaning
  - Right to life: livelihood, with dignity, Equality, without gender bias.
  - Socio-economic right; Right to Health & medical care
  - Social justice
  - No right to Die, Sentence of Death - Rarest of Rare Cases
  - Right to get Pollution Free Air & water
  - Right Against Noise Pollution
  - to know
  - to Privacy / Women's Right to make Reproductive Choice
  - Travel abroad
  - Right against Illegal Detention
  - Free Legal Aid & Right to Appeal.

Article → Constitution of India.
Section → Act

Page No.
Date

* Article 19:
Protection of freedom of speech
1. All citizens shall have the right:
(a) to freedom of speech & expression
(b) to assemble peaceably, without arms;
(c) to form associations.
(d) to move freely thro. out the territory of India.
(e) to reside & settle in any part of India.
(f) to practice any profession or to carry on any occupation

2. (a) To freedom of speech & expression.
Integrity of India, security of state, friendly relations with foreign states, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

(b) ——— × ——— × ——— × ——— × ———

- IT Act
- IPC - physical Attack
- Cr.PC
- Evidence Act

* Classification of Cyber crime.
a) Cyber crime against individual (Email spoofing, Phishing)
b) " against property (S/w piracy, Copyright infringement, Trademark infringement
organization, Email bombing, Salami Attack, DOS
society: Forgery, Web jacking, Logic bomb, Trojan Ho

Page No.
Date

* IT Act 2000 pdf

IMP ✓ Article 43 — 43 penalty & compensation for damage to computers, computer system, etc (Amended vide ITAA 2008)
(a) (b) (c) (d) (e) (f) (g) (h) (i)

ITAA 2006 Inserted

Network Attack Classification

DoS - apache, back, land, mailbomb, neptune
~~U2R~~
R2L
probe

Applicat²	DNS	SNMP	FTP & TFTP	HTTP	SMTP	
Transport	TCP	UDP			IMP (question will be asked)	
Internet	~~Interne~~ IP	ICMP	RIP, BGP, OSPF, EGP			
	ARP	RARP				
Network	SLIP	PPP	Ethernet			

Page No.
Date

* Exam Question

Q What are your rights to Life, Personal ~~liability~~, Liberty, Property, Freedom of Speech and profession?

Q what are the cyber crimes against these Rights? How IT Act 2000 is applicable to handle these cyber crimes.

Q How ITA 2000 is applicable to handle these cyber crimes. [20]

* TCP header in Hex

0532 0017 0000 0001 0000 0000 5002 07FF 0000 0000

i) Src port No.? 1330
ii) Dest port No.? 23
iii) Seq. no.? 0000 0001
iv) Ack. No.? 0000 0000
v) ~~HLEN~~ HLEN? ~~4128~~ 20
vi) Type of segment?
vii) Window size?

Src : 16 → 0532
Dest : 16 → 0017
Seq. : 32 → 00000001
Ack : 32 → 0000 0000
HLEN : 4 → 5
Reserved : 6 →
Flag(6) : 6 →
Wnd : 16 → 07FF
Checksum : 16 → 02
Urgent Pointer : 16 →

nmap
wireshark
IPS/IPS
Firewall
} 10M

1-2 i) Src port : $(0532)_{16} = (0000\ 0101\ 0011\ 0010)_2 = (1330)_{10}$

3-4 ii) Dest port : $(0017)_{16} = (0000\ 0000\ 0001\ 0111)_2 = (23)_{10}$

5→8 iii) Seq : 1

9-12 iv) ACK = 0 (No ACK SYN Flood)

13th v) HLEN = $5_{16} = 5_{10} = 5*4 = 20$ byte

14th vi) Checksum = $02_{16} = 2_{10}$ B

vii) WND = $07FF_{16} = 2047_{10}$ bytes

* LAND ATTACKS

- Local Area Network Denial attack (DOS) attack in which attacker attacks the network by setting same TCP segment source & destination IPs & ports.
- Succeeds by forcing computer to respond to itself such that target host sends response, SYN-ACK pkt to itself until machine crash.

* LAND Attack Detection :- TCP

- Layer 4 DoS attack in which attacker sets src & destination info. of TCP segment to be same. A vulnerable machine will crash or freeze.
- [src_port == dest_port]

Algorithm : Capture the traffic
{ Filter the TCP pkt
{ if (SRC_IP == DST_IP && SRC_PORT == DST_PORT)
Detect as "TCP LAND attack"
}
END;
}

Page No.
Date

attack

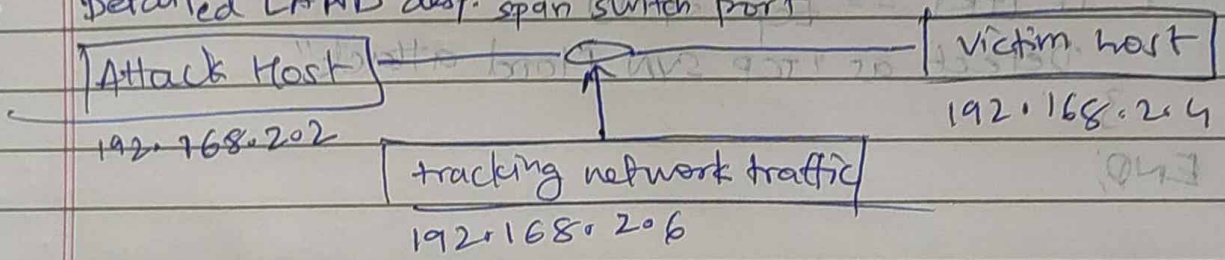
* Packet Capturing Tool: wisha WireShark

* Packet Generater Tool
1. Engage Pkt builder
2. Colasoft Pkt Builder.
3. Frame IP pkt generator.

* Packet Generator Tool?

* Packet Scanning Tool?

* Detailed LAND desp. span switch port



- Consider network that connects three hosts: Attack host, victim host & one is wired to SPAN port. i.e: monitoring port for tracking the network traffic shared bet² other two hosts.
- After switch conf. gen. land attack traffic.
- Use target host's IP & an open port as both src. & det. port.

* Detection & Prevention
- Multiple server & OS are vulnerable.
- Use Firewalls, Intrusion Detection & prevention prog., increase network speed, vendor fixes, reduce effects of LAND attacks.
- default TCP/IP stack conf. be modified a/c to security std.

2) TCP SYN Flood.

- SYN SYN+ACK SYN (SYN+ACK) ↓ Dropped.
- Flood victim machine with SYN.
- No three way handshake.

Algo : Capture traffic
{ Filter TCP pkt
- IF (PKT_COUNT >= 100)
  { IF (PKT == tcp.SYN)
    Detect as "TCP SYN flood attack"
  }
END;
}

3) XMAS Tree Attack