30 Sep 2024
Monday.

Lec-12 :-

Network Perimeter :- boundary b/w an organization's secured internal N/w and the Internet — or any other uncontrolled external N/w.

→ identifies mal functioning (or AI)
→ one application where ML can't be used?
cryptography as randomness, not pattern.

WOMK

one ~~scenario~~ application where CS can't be used?
↳ No such (☺)

→ CS uses ML
→ ML needs CS.

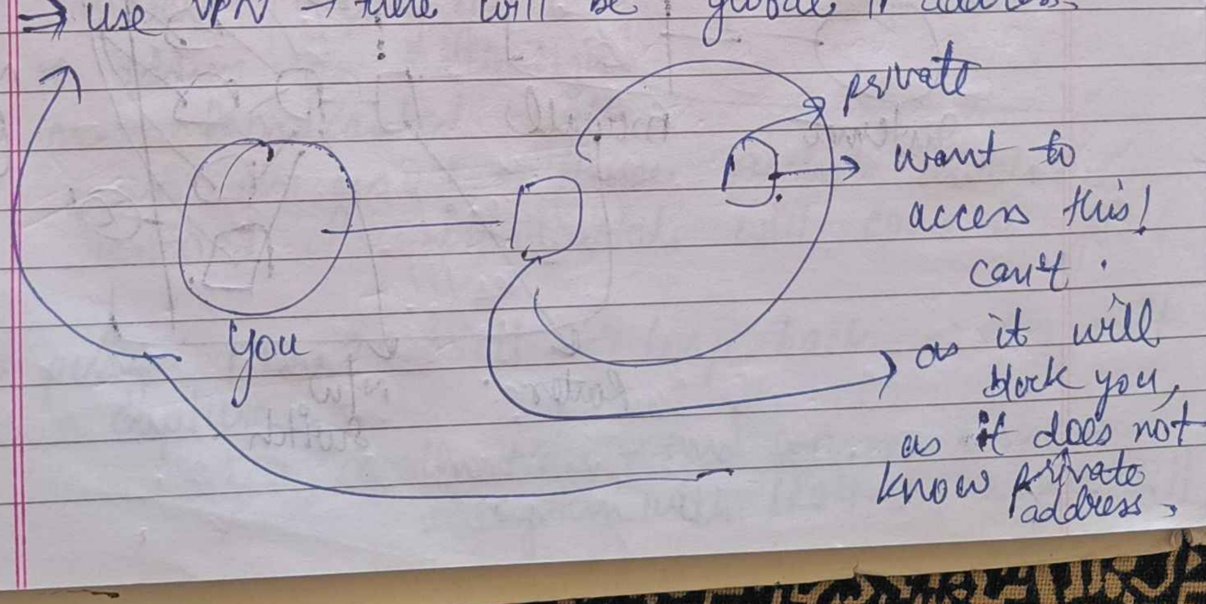
How our clg N/w setup is?
↳ we are in private N/w
↳ what is it?

How you will identify node is in private N/w or not?
↓
(by looking at IP address)
↓
as diff - 2 classes and har class ki IP is reserved.

→ we can access outside N/w like google, but they can't.
↳ as ur Id is (private) (not unique), but there is public.
So nobody can from outside, access your machine.

(ek IP meri ho skti, dusre N/w mein bhi kisi ki ho skti hai)

so
⇒ use VPN → there will be global IP address.



WJMK ☺

hmaare packet outside jaa skte hain but
~~wale~~ baahar wale nahi aa skte
siddha,
pehle DMZ ke paas filter honge,
fir N/W switch se filter honge!

Perimeter Security :-

N/w Infrastructure.

- IT ↓ Information Technology
- OT ↓ operational Technology ↑ industries mein use hota (????)
  → quality ↑, cost ↑, still holding window-7, but fir bhi advanced.
  ↓ time hi nahi milta update krne ka.

Intrusion :-

attack can be performed in 2 ways
- active
- passive

whatever having you IP address as destination or broadcasted will come to you! → those packets which are destined or broadcasted will come to you.

• ping 172.20.35.11 → loop back → won't capture.
↳ destination and source same → system with IPv4 → 172.20.35.11

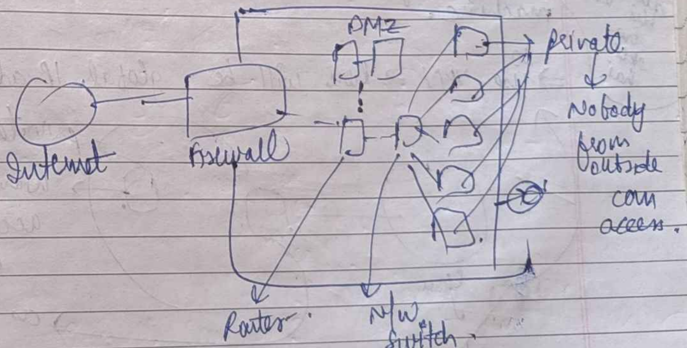
WJMK ☺

Proxy does NAT.
↳ N/w address translation

clg wale se connect krna, ghr se can't do
⇓
toh clg se pehle external se kro, fir ghr se jaakr uss external se, ab indirectly hm connect ho gye.
↓ but it can hack everything ☹

DMZ → Demilitarized Zone

Can't outsider access iiita.ac.in ?
↳ Yes!
So outsider can access DMZ not private N/W → for that come into N/W.



Sometimes B will stop communication / modify data / replace attack..etc.

↳ difficult agar cryptography use ho!!

Intrusion → loss of Reputation

↳ as kaam na kre, get kaam kre → reputation down. boli hai!! eg: window boot nahi ho rahi thi → flights bnd kri thi.

"ping 172.31.2.4" in system of 1804 → 172.20.35.1

↳ then TTL different

here "61" ms

here "128" ms

no. of hops

can trace using = "tracert 172.31.2.4".

64

here: → 172.20.35.1 → 172.20.1.9 → 172.20.0.1 → 172.31.2.4

63 62 62

63 61

→ at every node → (1) reduces.

→ toh 64 hoga starting mein.

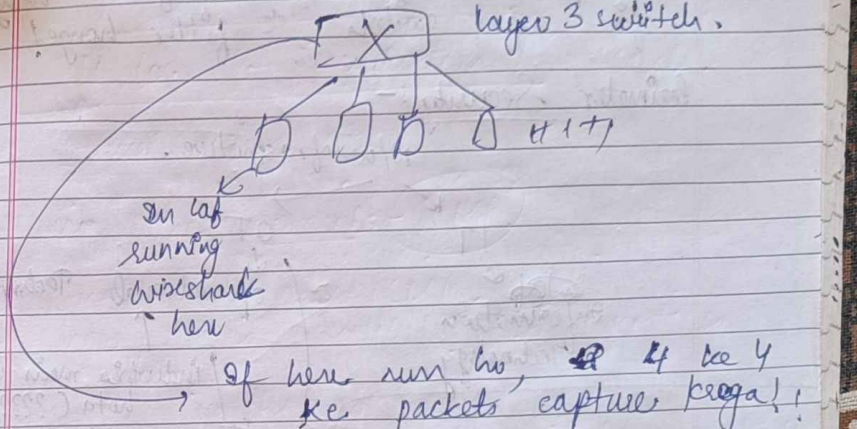
→ we do packet switching

→ route not fixed

→ to first identify path each time.

Wireshark

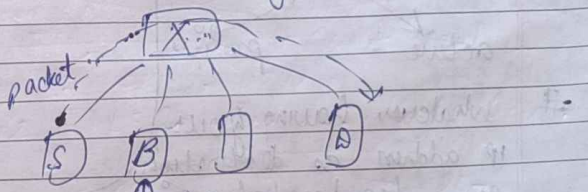
↳ capture ~~packets~~ packets going from you or coming to you.



→ If here sum ho, 4 ko 4 ke packets capture krega!!

wireshark → passive

↳ they only capture packets does not harm system.



→ I will say to S that I am switch or D → as S has no info.

→ This is active attack.

Prevention → report as well as block.

Intrusion Detection System :-

→ just reports does not blocks.

① n/w based
↳ run at n/w switch or firewall.

② If host based
↳ run at private host.

Virus Total → search.
↳ file mein virus dekhne ke liye compute hash, put here, ↳ will get answer
↳ may not always correct. ⇒ as uske paas kuchh particular hash hai jo virus hain → unse match kiya toh hi btaa paayega !!

Q. Difference b/w Host based IPS and Anti Virus and Firewall?

IPS → bas uthne ko kro quarantine

Anti Virus → sbko quarantine kro

FIREWALL
Inbound → something coming
Outbound → " going
↳ rules → who has to modify? → owner of machine
but any application can put rules here, eg: Zoom → can access firewall
why? ① Trusted. (No Harm)
② agar main khudh kroon time lgega. → and wo rules dusra user

Port belongs to layer which ??

443 → HTTP ??

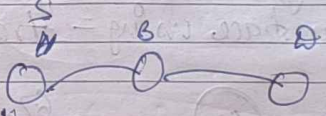
TTL = 128
↳ is starting
↳ no hop → to no reduction at all.

TTL for OS Identification → search.
↳ time to live.

"ping" uses protocol : ICMP

tracert also uses ICMP.

→ how path is identified? How tracert is working?
↳ $ / r to ping
↳ Pr. beech mein kbhi TTL = 0. error.



mainne TTL = 1 kiya, can't reach D, toh error aaya.
Fir TTL = 2 kiya ... that's how.

as beech mein hi TTL = 0 ho gya, error aa gya

Intrusion steps :-

① Reconnaissance ② Initial Exploitation
③ Maintain Persistence

→ port no. of SSH = 22.

WJMK©
35MM.

Shodan → search engin.

Sand Box → online compiler uses Sand Box:

putty.exe

trin
real time → sys

⇒ timeout 0.1s ./a.out

M-1: Static analysis → take code, do analysis.
M-2: do hash & check
M-3: Behavioural analysis

Can't put everything in Sand Box, jispe trust don't put that, bss doubtful put kro in Sand Box.

⇒ Create Sand box

Pattern Based — Compute Hash → Static → here attacker can escape more

Behavioural → Dynamic. ← can attacker escape here ??

Shodan → scan all public world wide devices → will say what vulnerabilities they have.

honeypot → anybody can come to my machine ← I invite and do attack ← why? → bug ← and solution nikaaloon for that nikaalo

WJMK©
35MM.

jab mera computer use kregi → usko fisa kna pdhega!

IDS → working
→ ① Signature - based detection → here vaar-2 update kro, d/w can't identify new virus
  → packet.
② Anomaly - based. " (ML used)
  → based on pattern
  → better! → as if pattern changed → can identify.
→ Antivirus k bhi same 2 types (??)

dir
ping 172.31.2.4 -n 20 → list

signature based → eg: "ping" present in file then virus, → just eg.
→ just block

→ CertUtil -hashfile a.txt md5 → Command.

→ say virus
dir
ls
ping 172.31.2.4 -n 20.
→ here no → as hash different !!!
but pattern wala dekh lega.

dir
ls
pinga 172.31.2.4 -n 20.

(Pavan sir)

WJMK ♡

black list → mushkil as many possibilities.

→ agar IP pta sender / receiver ki, fir toh "fire wall" se hi block ho jaata !! but 'ping' req toh koi bhi bhej skta hai.. Haan! You can block some ip → jo ping req na bhej skein but not all... maanlo apne hi kyun dur jaate jis command daalni ho, tab toh aap hi trouble main aa jaayoge.

⊙ NIDS → captures only packets (like Header, payload etc.) not file content or execution time etc!!

source → destination.

eg:

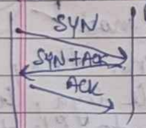
alert icmp any any → any any (msg: "ICMP Test"; sid: 1000001; rid: 11000001)

stiff mode
alert mode
logging mode } → 3 modes of ___?

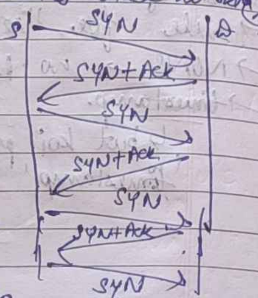
eg:

alert icmp any any → any any (msg: "MALWARE - BACKDOOR QAZ", content: "HI", metadata: ; classtype:).

→ TCP (3 way handshake) → Denial of service attack ho skta



↳ for establishment of connection
↳ agar break krna hai toh 'FIN'.



connection nahi bna

'S' trying to do attack on 'D'

↳ may be same port no. se na jaaye ⇒ TCB bharta jaayega!

genuine bnde tak request nahi jaayegi!

→ TCP se iss tarah Denial of service attack ho skta hai.

to SCTP → aaya!
↳ 4 way handshaking

WJMK ♡

So just show → normal machine → "honey pot" dikha, they won't attack as that's just for interaction
↳ as attacker ki bhut mehnat lgti hai!

→ agar bhut saari services run ho rahi hain → then honeypot OR MAC → (?????)

So 'sandbox' essa ho ki attacker identify naa kr paaye,

Indicators! → used to identify whether attack is happening or not.

HTTPS → encrypted data leta hai → so can not see.

① Rate of flow of packets
② Repetition of the packets. } → Replay.

↳ if some one sending massive no. of packets in short time → then wo attacker ho skta hai !!!

4/10/24
FRIDAY

Lec-13 WJMK ♡

protocol, root, signature,
↳ idk based on (????)

by default, payload = 01234567 (ubuntu)
payload = abcd.....wabc..i (window)
} one way to differ b/w OS.

* covert channel

⇒ sudo ping 172.17.15.75 -s 128 -p 48692068657265e.
↳ ASCII of msg.

kyi baari Denial of service attack ↳ k liye use hota.

how to identify msg?

↓ how can block such msgs?

By having "white list" → jo bhi skte bss aage "black list" bnaana very difficult

WJMK इंप्राम.

→ agar sirf (i) likhein toh pta hoga?

** alert tcp any any → any 22 (flags : S ; msg : "Possible" ; flow : Stateless ; detection_filter : track by_dst , count 70 , seconds 10 , ..)

(If count ≥ 70 ↳ then attack)

** ip spoofing ??

sudo hping3 -i u1 -a 192.168.50.52 -S -p 22 172.17.15.75

(u1: don't use my ip; -a: use this)

↳ kisi aur ki ip use karke msg. bhejna.
↳ can u identify?
↳ packets se toh nahi } ho skta IPv4, IPv6 mein possible only agar info daale → wo optional hoti hai.

(SSH port ko bs request jaaye)

→ how to filter? CC3 se sid = CC1 jaaye → can easily identify.
↳ but agar CC3 gateway compromise ho gya, toh LT gateway krega filter.

12 IP chahiye → 4 bits to bs
↳ ↑ toh attacker will misuse, as lot of free IP's available then, as ek ko black list kiya, then wo koi aur use kr lega.

nahi hai ☹

use of HOME_NET?
→ rule for "replay attack"? → with snort.
→ NONS → no 1's used.] → A ko bhejna tha, B ne le liya, how to identify?
→ timestamp.
↳ but koi protocol mein 'timestamp' nahi hota!

7 Oct 2024
Monday

Lec-

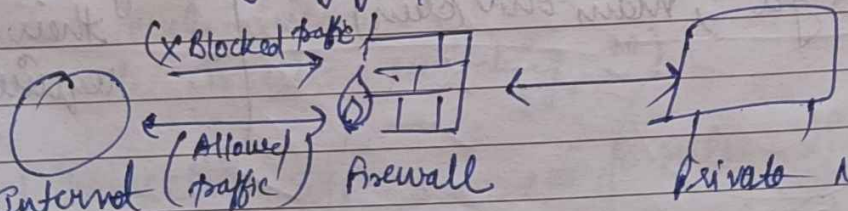
CYBERSECURITY :-

FIREWALL :-

Window
↳ when we download something, it has permission to update firewall.
↳ But Linux mein essa nahi hota.
↳ two types of rules :- (1) Inbound (2) outbound.

three types of profiles :-
(1) Domain
(2) Private profile → which to use when?
(3) public profile
↳ like hotspot wgera liya toh yeh use hogi.

Firewall → gated borders / gateways that manage travel of permitted and prohibited activity in private N/w.
↳ Filtering ka kaam krta hai, if route permits toh jaayega, o/w not.



WJMK ॐ

172.22.35.1
172.20.1.9
(172.20.0.1) → no firewall needed??
↳ why??
172.17.0.2
172.17.15.65

* Types of ~~Hardware~~ firewall :- (Based on system)
① Hardware ② Software
↳ jo hmaare computer (machines) mein hai.

(Based on Location) → ① N/w ② Host.

* Packet filtering :- firewall also like IDS goes to content, both perform same task, How different then?
↳ Firewall works at gate, but IDS can work internally!
↳ Host

(to look into IP address, port, data, transfer protocol)

* But how to differentiate N/w firewall and N/w IDS?
↳ as perform same task.

* How to differentiate b/w Antivirus, IDS and firewall?

Host → Antivirus, IDS, Firewall

N/w → IDS, firewall.

* Circuit level firewall works on Circuit switching (virtual circuit switching ??)

Inspection type
→ Stateful (have provision to look into past, future packets)
→ Static → jo rule likha, wo usi packet k liye applicable hoga, na jo chle gye, na jo aayenge.

WJMK ॐ

Firewall jiske liye wohi kaam kro →
↳ agar filtering kro routing bhi krwaayoge → 'overhead' aa jayega
routing ↳ router ko krne do, Don't merge both works

[tracert 172.17.15.65] → no proxy used, so not everything is routed through proxy.

* within campus, some devices does not have firewall.
↳ This attack can be done!
↳ How to avoid?

→ where to keep firewall, to avoid attack?
↳ individual machine or gateway?

↓ not every user knows all fact.

Drawbacks ↓
→ Not all users are aware and do changes
→ min level of protection
(ek ne kiya, dusre ko kaise pta chlega usne kiya, main bhi krun).

Adv :-
* ek bnda bdlega tbhi jo experienced hoga, and set individually bhi kr skein according to their requirement.

WORK 3/3 ...

X → block
✓ → send/allow
→ no rule exist.

	scenario 1	scenario 2	3	4
case 1	block	block	block	block
2	possible	possible	block	block
3	block	block	possible	possible
4	possible (allow)	possible	possible	possible
5	block	block	possible	possible

→ since 'input' itself blocked, output can't go.
so, firewall 'incoming pkt' pe more focus karta.
if 'input' trusted toh 'output' toh jaayega!

⇓

This all is according to windows
↳ (by default).
↳ rules can be changed.

for ①, ② scenario ⇒ client → source
server → destination

for ③, ④ scenario ⇒ client → "
server → source.

Q. * so how we can find out whether firewall is running or not?
↳ there will be some response which tells running or not.

WORK 3/3 ...

ping 172.20.35.11 → from 5206, sir trying to ping sir's cabin machine.
↳ but does not get ping
↳ firewall blocking ← bcoz
↓
which firewall?

is for trouble shooting

↳ if machine not running, nahi hoga ping,
but agar running, fir bhi ping na ho
↳ why?
→ which firewall is involved?

* agar SMTP protocol hai and firewall not having any rule for SMTP → then not allowed inside machine, (outbound mein nahi bhi h toh chalega)
but agar machine sending, chala jaayega!
→ So incoming ke liye rule must be written, (Inbound) mein hona chahiye
as attack ho sakta. ↳ (outbound) mein zaroori nahi
→ Haan leakage ho skti
↳ but utna itni importance nahi dete.

→ Jab andar aa raha hai → 'inbound' rule dekheinge.
Jab baahar jaa " " → 'outbound' " ".

Client → Send ping request → Server
④ response goes
② response comes
scenario ①
no rule sends ping request — ③ scenario (ping req.).

	Inbound	Outbound	
ICMP	X	X	case 1
	✓	X	2
	X	✓	3
	# no rule	✓ (#) no rule	4

WORK
DATE

* If access to src., Inbound mein rule ho and rule mein allowed likha hai, only then access will be given, if no rule present, then also can not access.
→ If rule saying 'not allowed', then also can't send packet.
→ then rule 'not allowing' wala rakhna hi kyun hai, rule hi mat rakho!
→ If want to block only one IP → then w/o rule not possible
↳ kyuki if no rule toh sare hi block ho jayenge.
↳ Same thing for outbound,
agar all not allowed krna hai ↳ then rules not ~~allowed~~! required!

* Prerouting → packet comes.
↳ fir dekho forward krna to next machine → 'fone kuch' or agar process krna → then consider as 'input' (as hmaare liye hai)
↳ then process hoga, output milega
↳ postrouting hogi, jisko bhejna hai, bhejdo!

→ If rule applied at prerouting, then we 'forward', 'input' . . . sb pass available.
→ If rule applied at 'Forward' → not applicable / available for prerouting.

WORK
DATE

Fp → Firewall present
Rp → Rule present or not
↳ means blocks or not.

	Fp	Rp
1 →	✓	X
2 →	✓	✓
3 →	X	✓
	X	X → so yeh toh hoga hi

→ not possible, if no firewall, i.e. no rule.

In all (3) different response

1. Ignore these
2. so pta chlega → firewall running or not.
↳ like (reject and drop) → Host no info/acknowledgement
↳ Inmein difference hain!
↳ getting some info/acknowledgement ki reject kiya.

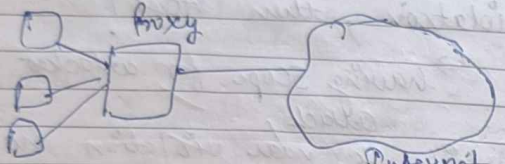
* If request something and service not running
↳ what response we'll get?

* IP table filter:-

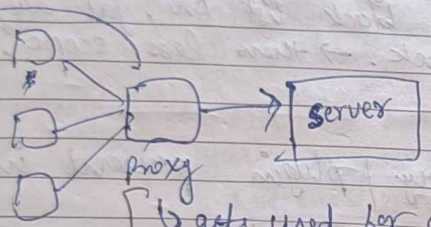
. Pre-Routing → route? → Forward → Post-Routing
↓
INPUT
↓
local process
↓
output → output → Post-Routing

Proxy

Reverse — Forward.



(Forward Proxy)



(Reverse Proxy)

↳ gets used for a server.

can have Firewall (Proxy Firewall).

↳ can go for deep inspection if able to decrypt the header, o/w can't see content.

→ having proxy before server → good or not?

↳ overhead

↳ performance issue

→ If performance efficient server, then not noticed much.

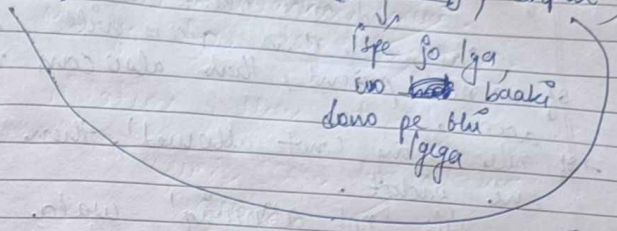
Mostly 'reverse proxy' is used.

web application Firewall (WAF)

↳ sirf web applications pe dhyan dega iska.

packet-state control.pdf

* Rule can be applied to Forwarding, Input, Forward.



↳ Input jo rule liya wo sirf Individually jispe lgaayega, sirf usi pe rahega.

Iptables → applications in linux to write rules for IP's.

↳ functionality?

* Why 'FORWARD' req?

↳ proxy ... does this only.

↳ tm saare use kr rahe, fir ka packet usko bhejo.

→ accept, reject, drop (sequence should be preserved).

→ In one second, one 'ping' request is to be sent.

↳ agar yehi kr rahe, then no violation.

How to add rule in iptable?

① Deep Packet Inspection firewall :-

Proxy Firewall

WORK

② fuzzy logic → uses fuzzy rules to detect malware

Anomaly → statistical
→ ML/DL
→ Graph Based
→ some uses (Rule-based) detection.

Firewall:-

can be at gate only) can't go inside, via cloud can't perform work of IDS and antivirus

firewall can work at any of layers:-
1) N/w → only pkt header dekhegi
2) Transport → ~~payload bhi dekegi~~ → connection dekhta
3) Application
↓
'payload' + 'data' but ~~and~~ agar encrypted and host based ?? (tab nhi dekh skte),

Anti Virus:-
↳ same as IDS if it is host based.
↳ if email comes, sometimes can see email ~~co~~ + attachments in email.

→ IDS costlier than Anti-Virus.
→ HIDS/HIPS performs efficiently agar firewall ho, as wo pehle hi filter kr dega, gate pe hi !!

Error 1: false positive → yeh tolerable nahi hai !!
Error 2: false Negative → but yeh for bhi
↳ malware hai, but 'No' bola, tolerable hai !!
malware nahi hai, but 'Yes' bola,
↳ toh faaltu ~~me~~ mein service roki etc.

WORK

here,
attacking WAP = attacking server.
→ can also go for 'deep inspection'.

once violation, then stops!
↳ having scope for attacker to attack
first ek vaar violation ho → fabhi block list ho, jab aaye fisse siddha block. → then less scope.

IP# → ??
↳ library / plugin present in Linux.

14/10/24 Monday

lec-

IDS :-
flow diagram of IDS is also applicable for IPS.

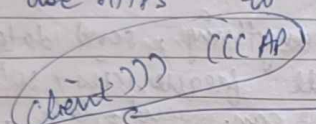
→ for pattern based IDS, we/we rules and patterns.

Anamoly → statical based
① route K 12 se yeh transaction
② kal 100 req, aaj 10,000
↑
may be aaj sirsat announce huya ho,
↳ dekho past year mein kitni requests thi,

client))) (((AP
Plain text → No security.

* SSL after 2.0 is TLS 1.0 etc..,
HTTPS → HTTP + SSL

→ we use HTTPS to connect to server :-



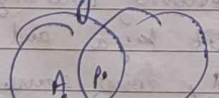
↳ then no need to worry of this, as already encrypted.
↳ worry only if HTTPS not used or weak encryption mechanism for key is used.

→ spoofing someone's AP as theirs.

802.11
↳ No N/w Layer.

① Wireless station also known as 'client'
↳ can transmit & receive
in wireless, dono same channel se nahi jaayenge, different channels se jayenge!

② BSS → has only one AP



Agar A, P pe aa jaaye, then access both signal of areas.

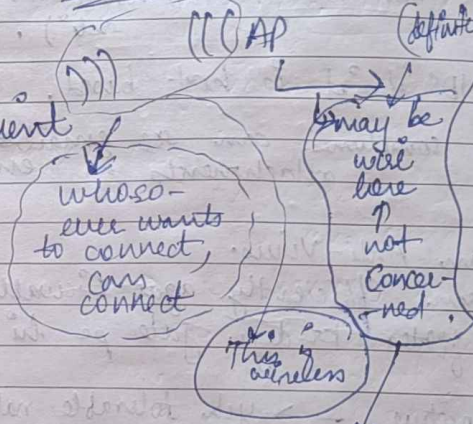
(agar nahi hai to nahi, tab)

③ IDS → signature-based
↳ false -ve ✓
↳ false +ve ✗
(agar match hoga bolega)

anomaly-based
↳ false -ve ✓
↳ false +ve ✓
That's why precision, recall wgera nikaalte hain!

WIRELESS SECURITY :-

Basics of wifi :-



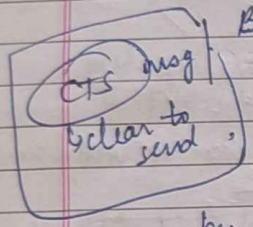
↳ why considering differently from security already studied??
① anyone can capture packet in atmosphere
② kitni bhi connect by state hain, wired mein limited.
→ no physical access needed, whosoever has capacity, can capture.

as NOT focus from source to destination, focus only from client to AP (access pt.).
↑
want security in this.

Hidden stations :- nodes which is not under coverage!

A, B both in AP range, but not in same range.

Thus, B is hidden station wrt A.



A se AP, AP se B.
now B tab tak talk start nahi krega, jab tak A na complete kr (say 1 sec given to A).

(x) agar B → jammer hota, wait na krta, continuously bhejta.

→ wired N/w throughput > wireless.

Joining a BSS :- client tunes to 'AP' channel.

↳ if 'AP' free, usko signal bhejta with its SSID, MAC address, indicating i m free.

↑ with this, can get info of AP, can send msg w/o connecting.

BSS → Basic service set

Peer to peer → directly talk to each other

↑ Ad hoc mode (independent one)

IBSS

↑ so ~~can~~ anyone can anyone else directly.

Jammer ??

↳ w/o seeing anything, send data continuously with all frequencies, w/o sensing, so no one can send data, N/w ↑ congestion?

↑ Jamming not possible in wired,

Denial of service attack :- wired + wireless dono mein possible,

↑ 'jamming' bhi isi type ka hota hai.

* CSMA/CD

↳ how 'sensing' is done??

→ how can 'sense the 'channel' ??

↳ If channel is free, flow is different, if some data flowing, flow will be some what different.

↳ difference in frequency / amplitude.

→ let's say freq. ek limit tak jaa sakti hai, agar usse ↑ → then data present!

(x) go for random waiting, as agar same time k liye wait kiya and dono ne usko dekha, free mila, dono same time par data bhejenge fir.

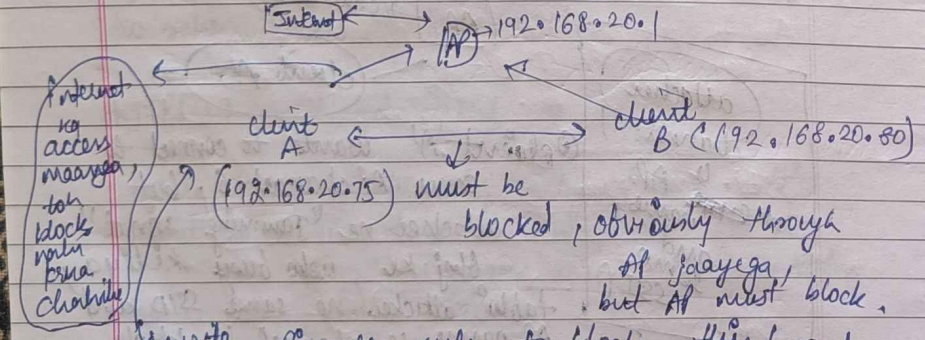
* like in some phones
↳ 2 wireless interfaces
↳ 1 se dusse ne hotspot liya hai → can capture packets.

→ 'curl' command. → try to connect through this command line.

curl url ?
↳ u can also pass user id and password and see whether proxy req. or not.

→ TLS 1.1 → then wo web browser nhi kholegaa, kam se kam TLS 1.2 hona chahiye, but command line se agar access le sake toh TLS 1.1 ka content bhi mil jaayega, as wheen itni security nahi chahiye.

2) Client Isolation :-
↳ this is also required.



↳ write firewall rule to block this!, and Internet access block na ho!

→ Isliye aaj kal saare info - nhi thejte, sirf bhaate hain ki main free hu, toh agar koi connect hona chahta hai wo kindly authenticated msg bheje.

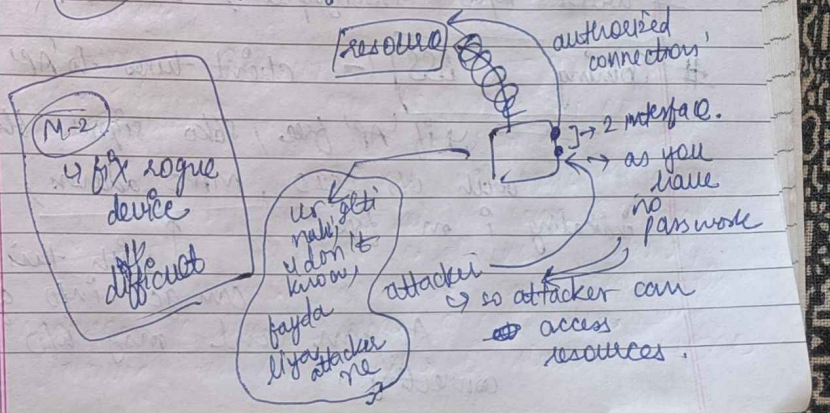
Interception Range :- ~~Range~~ Range within ~~the~~ which interception of packets can be done.

→ yehi problem :- agar within Interception range, they can capture our packets ; usually 'passive attack', but haan 'active attack' also possible.

WarDriving :-

Common Attacks on WLAN :-
1) Rogue wireless ~~dev~~
Rogue wireless devices :-
→ How possible?
→ In your laptop ; how possible?

M-1 → 2 interface :-



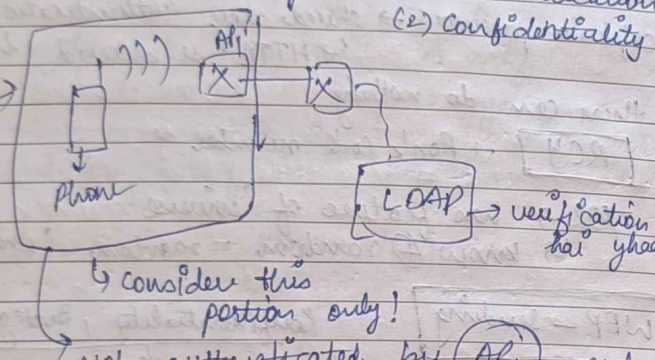
fake credentials bhee and attacker connect ho gya uss AP se !!

18 Oct 2024
FRIDAY

Lec - 6 :-

→ CSMA-CD can't be used in wireless as it uses different signals for receiving and transmitting.

Need 2 things :- (1) Authentication
(2) Confidentiality



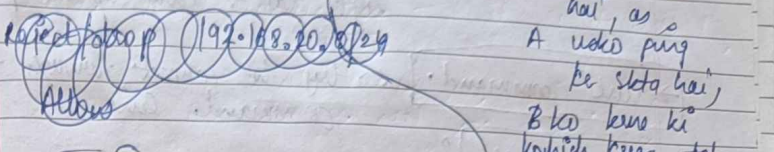
not authenticated by AP, only authenticated wired wale part ke liye ho sake hain, not for wireless.

HTTPS → tunnel get created as SSH used (22)

While HTTP → no tunnel, only flying mode,
→ want to ensure tunnel. b/w phone and AP,
↳ means encrypted form mein jaaye sab, with security.

Shared key Authentication → same password se saare devices connected (like in Hotspot).

192.168.20.0/24 ↳ but 'AP' ko exclude kiya hai, as A usko ping kr sakta hai, B ko kiya ki koshish karega toh AP block krega.



and AP can ping any client

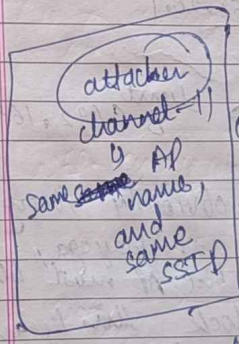
rule :-

can swap first	source	destination
Allow	192.168.20.0/24	192.168.20.1
Allow	192.168.20.1	192.168.20.0/24
reject/drop	192.168.20.0/24	192.168.20.0/24

↳ Order matters!

↑ in this way "client isolation" can be performed on our machine.

3) Wireless Hijacking (Evil-Twin) :-



AP → (channel 6)

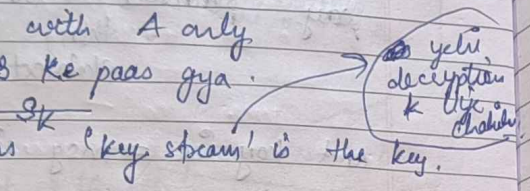
client A.

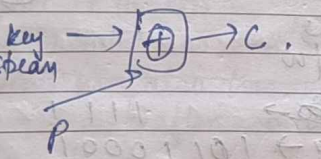
① client 'A' wants to connect to some AP channel-6, but attacker ne "jamming signal" bhej ke, usko busy kr diya, fabli attacker ne same SSID and AP name se channel 11 khola, hmne wo khola, usne credentials maange, le liye, chupke se chla gya, and jamming bnd ki, channel 6 khula, aapne

till now :- (SK)
Shared key known to both, but plaintext and initialisation vector (IV) is not only to sender (A), not receiver (B).

PRNG → is deterministic fn
↳ same input, same output
↳ random kaise ? when input pehle waala gya, can't guess output.

Ciphertext also with A only
↳ wo ab B ke paas gya.
~~Now as B knows SK~~
and for encryption 'key stream' is the key.





So (IV) req. only there can ~~detect~~ decrypt, so (IV) is going in plain with C, (and this is the major problem).
Now generate keystream.

keystream = PRNG (IV || SK)
↳ order matters

NOW B can decrypt and can get P.

* Sometimes AP will do authentication by itself, or 3rd person (like LDAP) doing that authentication.
* Shared Key Authentication :- Is it right method?
↳ NO!!
→ as who knows key and decrypt agar 2 log usi key se baat kr rahe hain!
→ all AP has same SSID in Extended service set,
→ safety ka password ⇒ shared key authentication.
↳ HTTPS se secured ho jayega, then can do nothing.

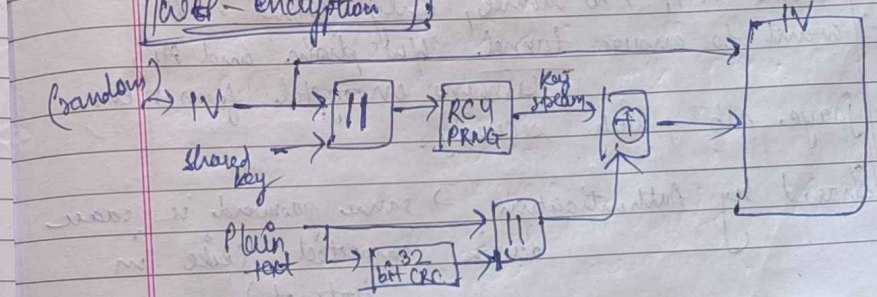
RC4 → Ron's code number 4

XOR → has feature of 'inverse'
↳ know ⊕ random = random (end feature)

WEP – Sending

Confidentiality, Integrity
we want when Alice want to communicate with Bob and Eve is present in the channel.
B → key
A ⊕ B = C
C ⊕ B = A
Ciphertext.

WEP – encryption



→ so should not use (IV) again!!

→ Youtube uses TCP.
↳ is it google product (????)
↳ sequence no. hota hai!
↳ kya wo repeat hota hai ??

say pehla seq no = 1
and data length = p
agla seq no = 1+p.
↳ in reality.

but here say :-
1st seq no = 1
2nd " " = 2
:
:

every parameter has size (like port → 16 bits
↳ total no. = $2^{16}-1$)

→ similarly, sequence no. also has bit,
↳ after reaches limit, will again go back to 1,
↳ similarly here (IV) will repeat, chahe size kitna bhi ho, as ek time baad toh limit reach ho jaayega!

19 Oct 2024
Saturday

Rec-

RC4 → can be used for secured communication.

→ alternate ascending - descending :-
1 → 2
last → last - 1
3 → 4
last - 1 → last - 2 . . .

Ciphertext = ⊕ keystream (Plaintext || CRC) → for encryption
(2222)

On receiving side :-
keystream = PRNG (IV || SK)
↳ same),

Plaintext || CRC = ⊕ keystream (ciphertext)

say plaintext → 100 bit
then,
Plaintext || CRC = 132 bit
↳ 32 bit

and key size = msg side (must)
↳ (also drawback)
↳ for XOR based solution

of wo

key → 1111
msg → 1010001
1011110
↳ msg ka kitna hissa toh mil hi gya (:')

→ Imp :- Same key should not be reused.
↳ WHY?

$C_1 = P_1 \oplus K_1$
$C_2 = P_2 \oplus K_1$

Now, $C_1 \oplus C_2 = P_1 \oplus P_2$ (with inverse property of XOR)
↳ can get easily,
as P_2 de diya khudh, P_1 dhoondh paayenge!

SQL Injection

detect modified (agar integrity ensured then can identify), (or agar fix pattern huge msg ke like only lower case alphabets, and attacker ne different msg bheja, then can identify).

Brute force Attack :- go with every possible combinations.

for 'n' bits → 2^n combination
↳ definitely koi ek toh pkka match hogi hi

* By using bits, brute force attack may take time but can't say secured as then statistical attack also possible.

WPA :- (???)

A → Abandoned (???) in ARC4, while mechanism same as of RC4.

A simple passphrase is combined with SSID and hashed 4096 times to produce 256 bit PSK.
↳ offline dictionary attack possible.
↳ Social Engineering attack possible.

Name	Password
Adati	Adati

→ WRONG way to keep, as Password should be in hash form.

Passive Web Attack :-
→ attacker just observes, just copies eg. packet sniffing/ sniffing.

eg. MIM attack as not changing packet

passive attack ↳ fishing website etc, as not changing anything.

attack
↳ take two packets with same key
(jabhi video key nhi pta, sirf C pta hai)
↳ kaise?

if 'IV' is same, as C ke saath 'IV' bhi jaa raha hai!
↳ then key stream will be same as :-

key stream = PRNG (IV || SK)

↳ as 'IV' kabhi nai kabhi toh repeat hoga hi !!

↳ then $C_1 \oplus C_2 = P_1 \oplus k_1 \oplus P_2 \oplus k_1$
$= P_1 \oplus P_2$
↳ now can perform statistical attack,

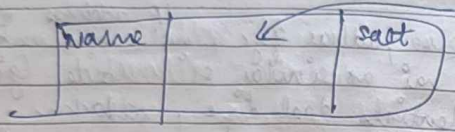
problem with one time padding
↳ key should not repeat.

Active WEP attack :-
(Our Assumption) ← If attacker know cipher and plain text pair :-
↳ can get keystream from this.
↳ can create correctly encrypted msg
↳ AP is deceived into accepting msg ⇒ as usne decrypt kiya, can

all passwords!!

↳ so (*) wale same table ka krega... some may match some not.

Now say pepper bhi add kiya ⇒



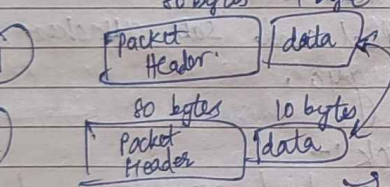
↓

Now more complicated for attacker.

→ that's why 4096 times hashing, thus more security, as har password ko 4096 times try krna pdhega... very much overhead for attacker.

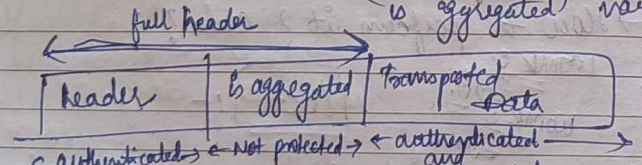
AGGREGATION ATTACK :-

eg:-



→ instead of this, dono ko ikatha bhejo :-

→ if aggregated multiple msgs/data, is aggregated variable ata hai.

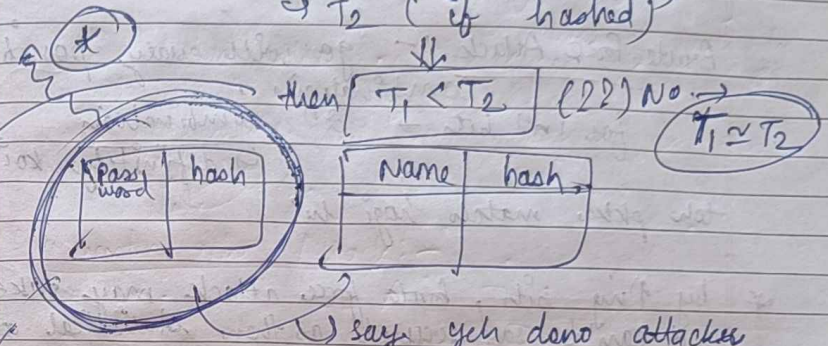


→ say table is stolen.

→ How much time admin have to inform everyone that change credentials as compromised,

↳ T_1 (if not hashed)

↳ T_2 (if hashed)



↳ say yeh dono attacker ko pta and usne ek particular password dekha

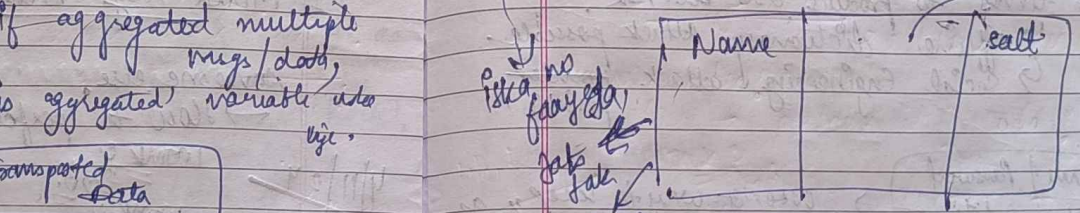
→ TC = O(size of table) ????

→ then why to hash?

↳ as admin ka bhi kaam bdha, password aaye, hash kro and compare!

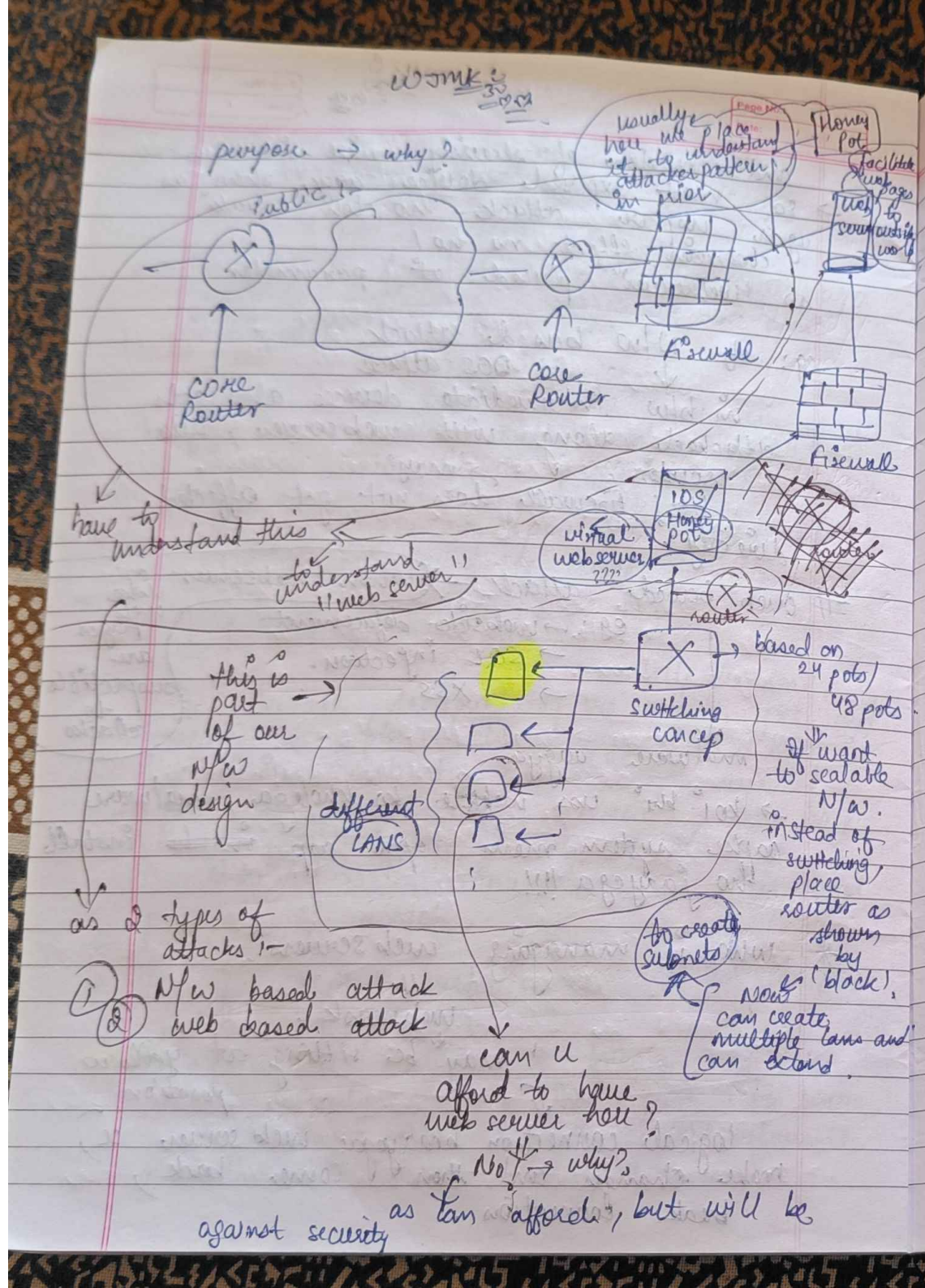
what to do now?

so add salt and pepper. → password || salt.



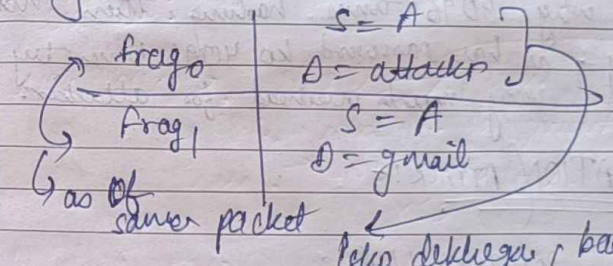
→ Now say yeh database table stolen, now much time attacker takes??

now attacker have to do || of salt with



Request only one but response are 2,
↳ one may contain
Dns response
↳ what happens, if wrong?
↳ IP address of somebody not known to us
ki attack hai as similar sa website ka name and hmne credentials daal diye, attacker ko pta chl gya

Fragment Cache Attack:-



Mixed-Key Attack:-
↳ actual request send to someone else.
→ How to perform it? code?

4/11/24 Monday

Lec:-

We can not harden up security from N/w

→ webserver
↳ perimeter device
↳ 1st line of defence
↳ most susceptible to attack

→ In order to facilitate access of webserver w/o restriction → (port no = 80, 443) should be open in firewall.
http, https (22)

→ attacker know that these 2 ports are open for them, so they will encapsulate pkt in such way that payload mein malicious script encapsulate hoga with http header, toh pura pkt encapsulated lgega http packet and wo accept ho jayega ⇒

[payload | 80]
↳ http header

So firewall, decapsulates the whole pkt and signature se pta chl jayega that there is malicious content and hence rejected.

→ But attackers are more advanced, thus aage 'Honey pot' lgaaya, firewall k baad, which takes some time to understand pattern of attack.

* 70% of infected websites are used to distribute malware. ∴ so,

→ Jo log website owner right bnaake host krte hain, not only affecting their own web server, but making whole cyber space vulnerable as such websites have malwares.

and burden of security will increase
→ so most exposed device aage rkho as agar uspar attack ho toh baaki cheezein effect na ho!
so 'webserver' placed at parameter,

eg: of N/w based attack
↳ DOS attack
in b/w Intermediate devices also gets attacked along with webserver, like router, → 'may'
Yes! Firewall does not get affected directly.

web based attack → (when webserver or like web pages are susceptible to attacks)
eg: → webside defacement
→ SQL infection.
→ XSS
↓
malware aagya
→ koi bhi uss website ko kholega, malware aapke system mein apne aap ~~kro ko~~ install ho jayega !!!

* who is managing web servers?
↓
web mask.
↓ may be sitting at yellow position
↓
logical connection bnaayega web server se, make changes and then come back, break connection.

WJMK

Page No.
Date:

'script' sun kake koi, can attack internal info like 'mail'

(*) Types of web Application Security Testing :-

1) Black box 2) white box 3) Gray box
4) N/W penetration 5) web Application penetration
6) Mobile Application penetration.

→ visibility of testing very imp
↳ means how many info client is providing you for the testing purpose.

→ means client provided no info, may even not given 'url' of webserver
so want you to do testing as hacker / attacker and try to gain info as much as possible (blind testing)

Black box
↑ (visibility ↓s)
white box

(4) # N/W penetration :- methodology to perform testing of N/W based attack.

→ client b4 giving u any task, may ask your methodology !!

⇒ what will be methodology for black box testing ??

Vulnerability Assessment and Penetration Testing :- (VAPT)

WJMK

Page No.
Date:

Governing Security Principles applicable to web security :-

1. least privelege
2. Defense in Depth
3. Input Validation.

Racky matrix,
has which privelege, contains info like what

(*) URL attached to web server are attached to important servers eg. mail server, file server.

so problem is not only web server!

(as organisation use FTP to upload file)

to esse & 'internal info' of organization tak jaa skta attacker, and can affect them.

Mail server → uses SMTP (25).
↳ connected to data base server.

web server → login (RBAC) → mail (SMTP (25)) → data base server → prone to SQL injection !!!

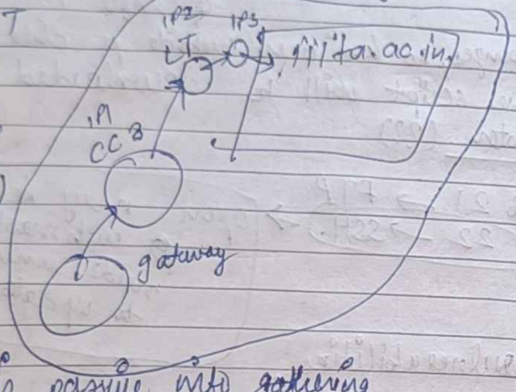
Input box (like mail, password of user) should be restricted !
(like size of variable)
↳ o/w mail server vagera crash ho skta hai !!

→ so agar input validation nahi hai toh

WJMK 30

→ ping www.iiita.ac.in
→ tracert 172.31.1.33.
↳ gives no. of hopes and scope of my work.

IP1 → CC3
IP2 → LT
IP3 → L3 switch or router (perhaps) 172.20.0.1



↳ this is passive info gathering
Now want to know:-
OS fingerprinting devices, by which will get list of vulnerabilities

active gathering se doubt hota hai, n/w administrative ko ki koi toh scanning kr raha hai

passive gathering se nahi hota.

→ so 'ping' req. should not reveal IP address!!!!

③ VA → hardware level
→ software level.
↳ important parameters that we will give are IP address of that particular machine or range of IP addres.

→ list of known vulnerabilities:-
① SQL injection
② XSS
③ CSRF
④ session hijacking ... so on!

VIPRO

WJMK 30

team performs security testing of other team

1) Planning and Scope definition
2) Info gathering ↔ active gathering / passive
3) Vulnerability assessment (VA)
4) Exploitation
5) post - "
6) Reporting
7) Remediation and Re-testing
8) Continuous monitoring

techniques used:- 1) social media etc, as want to know more about organization

N-Map
↳ generates traffic for both TCP and UDP
↓
Thus making active website busy???

→ trying to find weaknesses in webserver by acting like a hacker/attacker.
↳ create N/w map, tell scope
↳ like no. of IP addresses/ or geographical location or nothing
↳ Blackbox

If wireless want to know all rogue AP
↳ thus want all IP and MAC

Problem:- ① Saari info dedi pehle (WRONG)
② Signal strength, can sniff and have access to AP outside till 500m (WRONG)
③ able to enter switch level using by default CISCO password (WRONG).
④ Now as at switch level, can perform any type of attack eg. DoS attack.

OWASP → not talking of any software but of websites as SAMM included hai!

(*) Key features of OWASP ZAP:-
1) Automated scanning
2) Manual Testing tools
3) Passive scanning
4) Active Scanning 5) Spidering / Crawling
6) Session Management and Authentication
7) ZAP HUD
8) API integration
9) Reporting and Results

(*) OWASP Dependency check:-

1) Vulnerability Identification.

⊙ Database Integration :-
1) NVD 2) Github Advisory database

→ web servers
↳ has URL embedded
↳ contains 2 imp class of info (???)
→ URL mein changes, so kisi aur website pe click karenge from where script will be downloaded.
→ resp. of web master (??)

port 21 → FTP
22 → SSH. → open may be bcoz. web master needs remote login to update website

⊙ OWASP vulnerabilities

8/11 Friday

lec

→ SQL injection works only with SQL database.

OWASP :- some flagship projects include:
1) Top Ten 2) ZAP 3) Dependency-check
4) SAMM (Software Assurance Maturity Model)

(*) what will be security implication if doing on real environment?
↳ as there it will be like DOS attack,
So need an "Illuminator"?

(*) what are top Ten critical vulnerabilities with which OWASP deals?