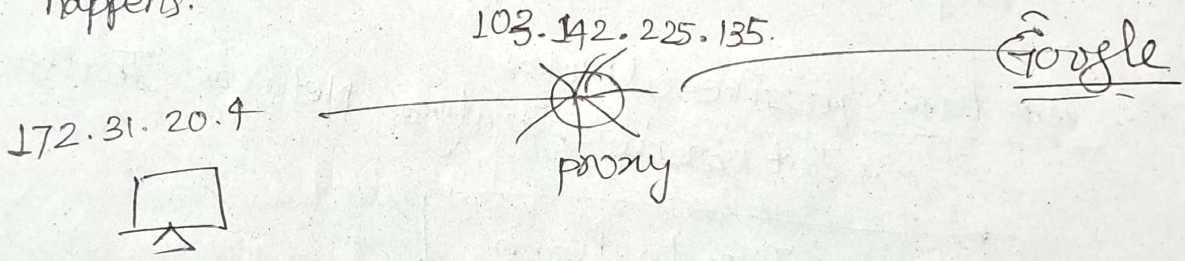
Venkatesh Sir

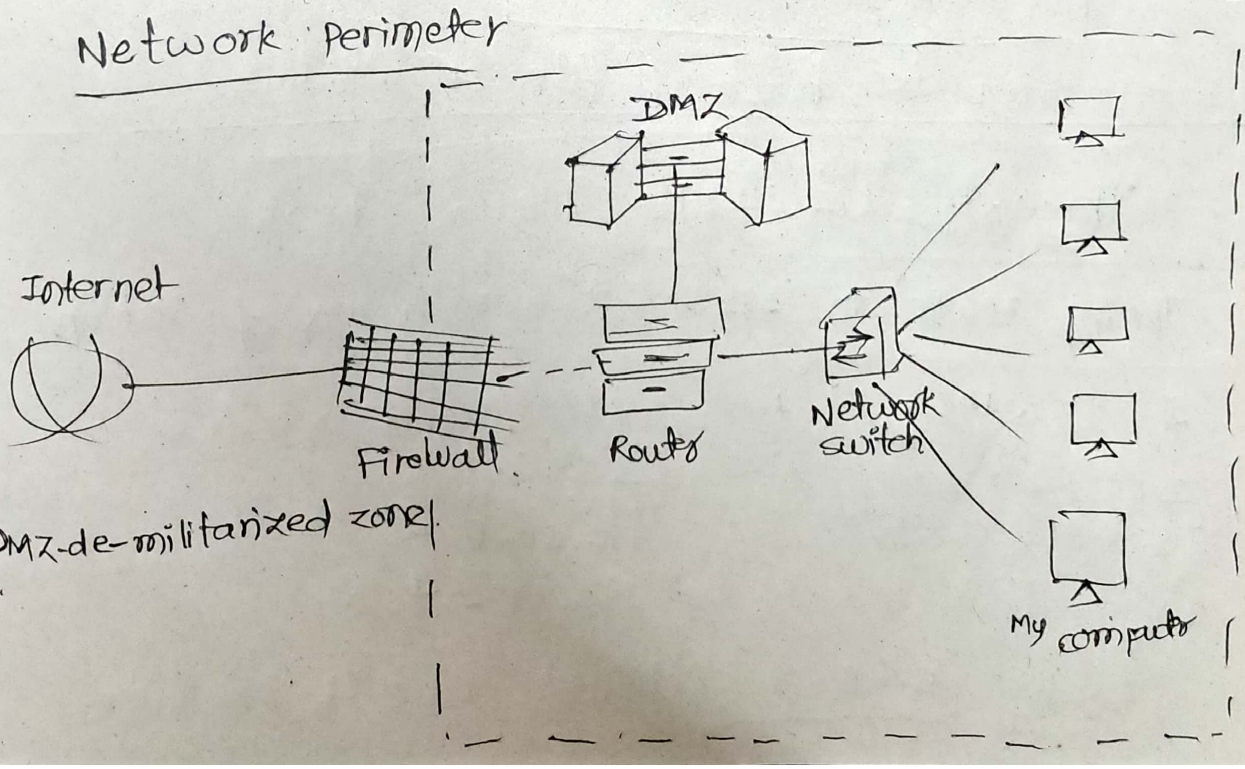
- IDS
- Firewall
- Wifi-security

- Intrusion - unauthorised access to system.
- Whenever there is Randomness, ML cannot be applied.
- ML needs cybersecurity, if someone poisons your data ex. AI will say cat instead of cat.

In case of VPN, there is global IP address.

When proxy is used NAN: Network address Translation happens.





OT- operational Technology (costly, long term)
IT- Information Technology

The perimeter defense prevents:-
- unauthorized access
- data breaches
- cyber threats from entering network.

Loopback → sender me Receiver me.
Ethernet → packages coming to you.
Wifi → —11—

Wireshark :- passive attacker
:- Just observe & analyse Network Traffic

TTL - Time to leave
- no. of hops

Tracert 172.31.2.4

Tracing route to 172.31.2.4 overal a max of 30 hops.

1	<1ms	1ms	172.20.35.1
2	< ms		172.20.1.9
3			172.20.0.1
4			172.31.2.4.

my device → proxy

common TTL values

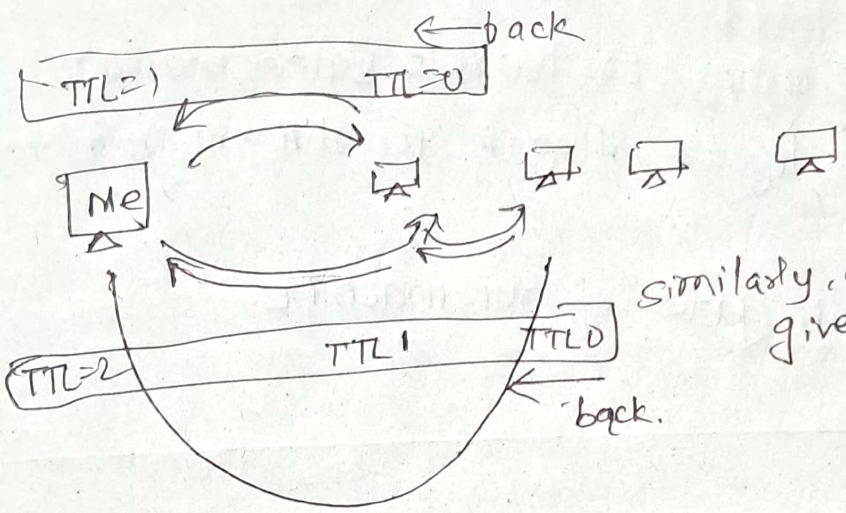
64 - Linux / MAC

128 - Windows system

256 - Network devices like routers.

Which protocol is used by ping :- ICMP

Traceroot also uses ICMP.



similarly, all destinations give path of route.

All ports belongs to various apps.

80 - http.

443 - https

22 - SSH secure shell.
alternate of FTP.

Virus Total :- if you have doubt on any file put on this website.

~~The hash~~, The hash of virus has particular values.

To do tasks that can harm OS, use virtual machines, if any problem, delete VM.

IDS & antivirus does similar job.

For antivirus, if a message is illegal, its illegal for all.

For IDS, according to the role same message can be legal & illegal. for different machines

Firewall sits in gate of our machine.

IDS
- signature based (pattern).
- anomaly based (machine learning) (imp).

Keep updating Antivirus software, to identify new virus.

To compute hash of file on windows

```
certutil -hashfile filename MD5.
```

If u cannot verify through signature, we go through behavioural/dynamic analysis.
Test the code in SANDBOX

Every organisation should have a sandbox.

Intelligent attacker

malware behaves as normal code if it is getting executed in sandbox.

How? Normal machine – 8 cores – Attack Destroy
Sandbox – less cores, say 1 core – Mein gareeb hoon.

Hence, people mostly go for machine learning algos.

SHODAN : shows webcams available in India.
: made for genuine purpose.
: honeypot : Invite others to perform attack
: To find new bugs & techniques.
:- This is a trap for attackers.

Attackers do not attack honeypots.

H.W :- create ~~code~~ sandbox.

Indicators of Malware :-

In https, everything goes in encrypted form.

→ Rate of flow of packets
→ Repetition of packets

- ping uses "ICMP" protocol.
- ICMP – application layer.
- see format of ICMP:-
  - sender address
  - Receiver address,
  - payload, checksum, code type, etc.

default payload in Linux:- 0123456 7.

default payload in Windows:-
abcd--- ghi

sudo ping IP addres -s 128 -p 48692...2e

128 bit size

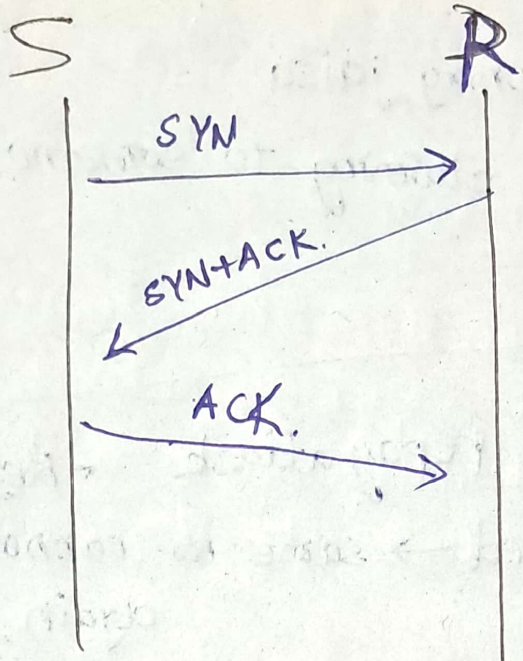
message in ASCII form

creating whitelist (:whitelist limited)

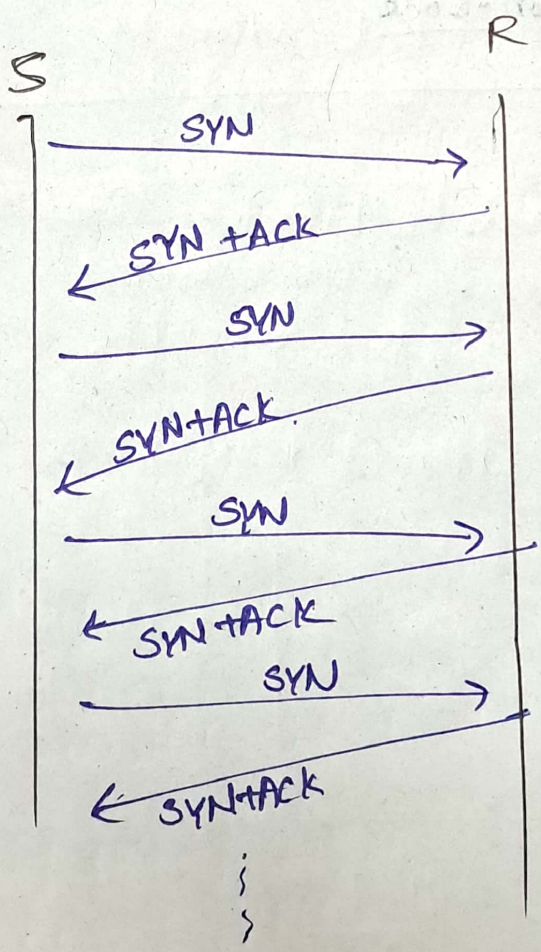
blacklist :- (not limited, large number)

Network Detrusion system : analyse header only

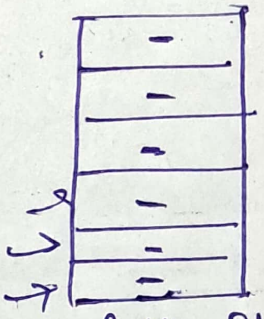
IDS, SNORT:- see header & payload.



* 3 way handshake for connection establishment.



TCB
Transfer control Block



fully filled.

Denial of service, if some new sender wants to establish connection.

TCP has vulnerability of SYN flood attack.

Spoofing → proxy jaisa
→ claiming to someone else.

No rule for replay attack ← Research attack.

No. once used → same no. cannot be used again.

Fourozon-book

Firewall

Linux - normally all rules are not written
- no filtering rule by default.

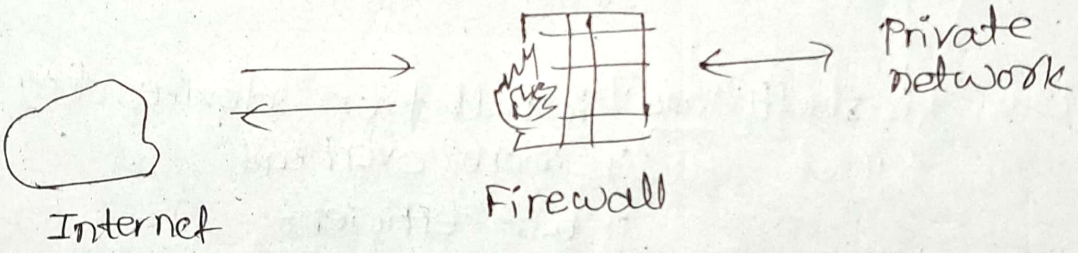
-

Windows - all rules are autoupdated.

Rules are for inbound as well as outbound rules

We have 3 profiles → Domain
→ Private
→ Public (airport, railways)

Firewall sits betn outside network and our network.



Firewall
- filters packets & see malicious packets
- There is outer & inner firewall for large network.

Router - routing the packets.

Sometimes in internal network, the packets need not pass through firewall or proxy.

ex: 172.20.35.1 → 172.20.1.9 → 172.20.0.1
↓
172.17.0.2
↓
172.17.15.65

Where should firewalls be put?

1) at Gateway
2) at every machine

ans- at Gateway (router), faces many attacks.
- applicable to complete network.
- The router handling person writes & modifies more rules than at machine level.

Types
- Hardware : independent of devices they protect
  : fast, efficient
  : less overhead.
- software : installed on devices they protect.
  :- more overhead
  :- less efficient

Q] How firewall different from IDS?

ans:-

Firewall	IDS
• works at the gate only.	• works internally also

Exam question

Host
- Anti-virus
- IDS
- firewall.

Inspection Types

- stateful
  - one rule can have dependency of another
  - can take decision for multiple packets
- stateless
  - takes decision for each packet
  - All rules for each packet.

- ping protocol for troubleshooting.

How to ping other devices.

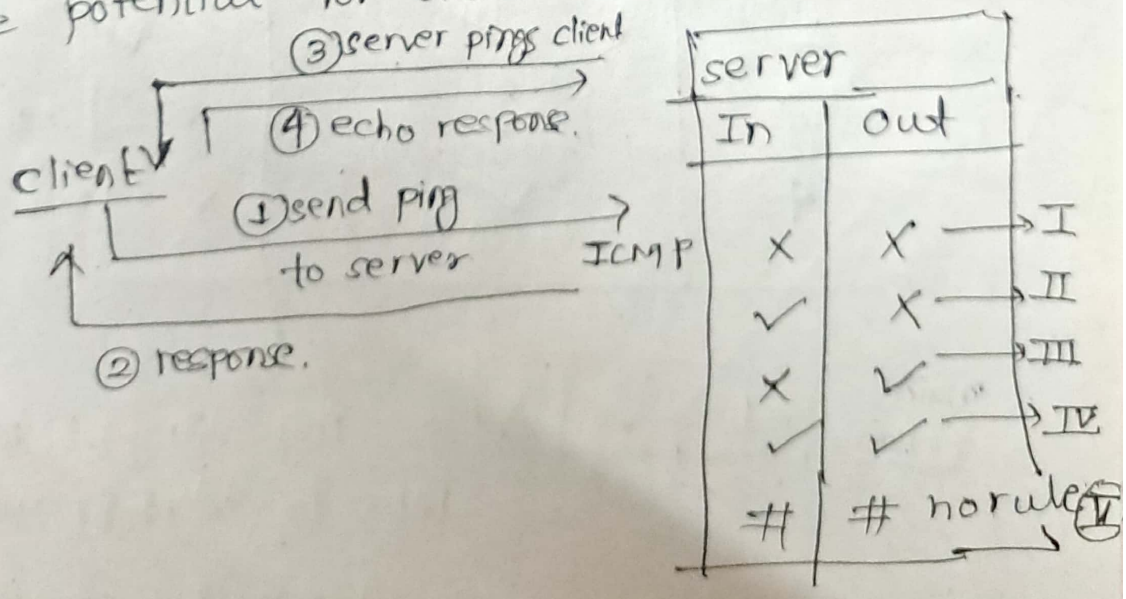
Firewall → [redacted] Outbound rules. & inbound rules

If no rules written for a scenario, will the packets allowed?

ans:- Not allowed in windows.

In outbound rules, going out, even if packet rule not present, the packet can go out

Hence potential for data leak.



ans

I) Block ① & ② .
③ & ④ .

II) ~~① ② ③ ④~~

III) since input itself blocked, output will not come
~~① ②~~ ③ ④

IV) ~~① ②~~ ③ ④

same as III

Above is according to windows.

How to find whether firewall is running in target machine?

ans:-

scenario	Firewall present	Rule present	
1	✓	X	
2	✓	✓	
3	X	✓	not possible
4	✓	X	not possible

main scenario → 1 ✓ X → You will get response. helps to identify whether firewall present?

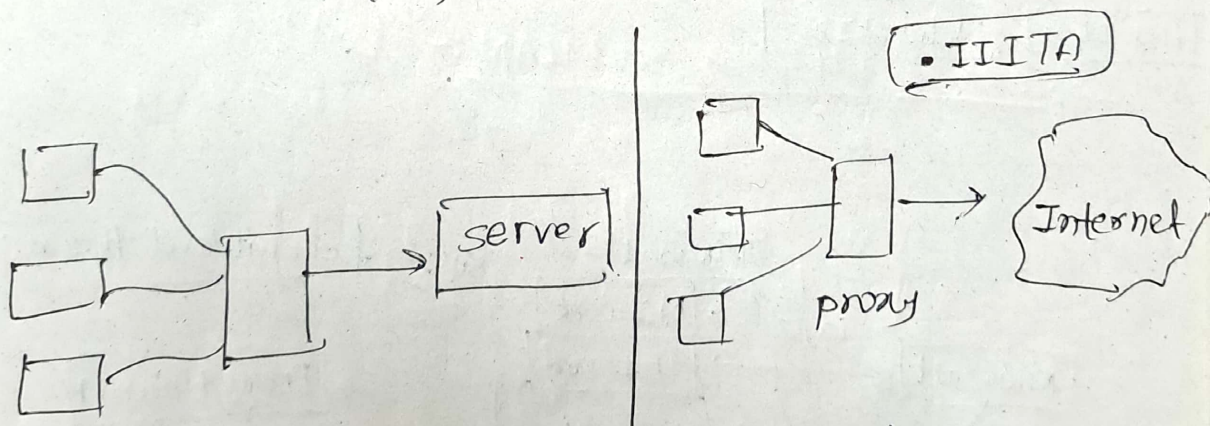
If message(/ping) is rejected, identifying whether firewall existed in target machine is tough.

'IP tables' in Linux is stateful & allows for writing rules.

The order of rules also matter.

Deep inspection firewall. — proxy
Not just header, but also check contents

Types of proxy → Reverse proxy
→ forward proxy.



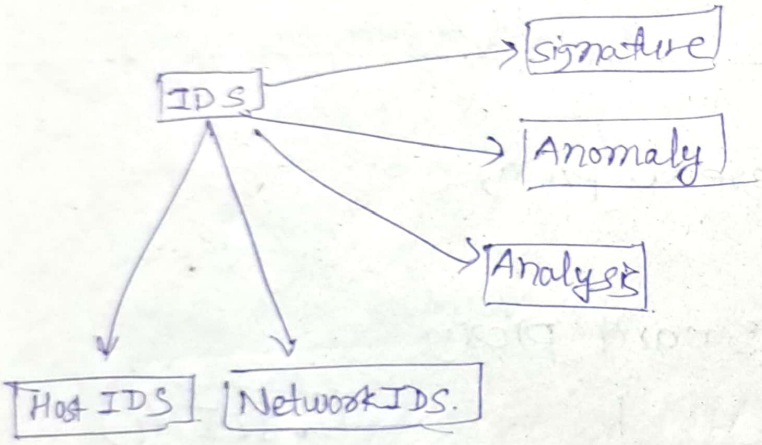
Reverse proxy

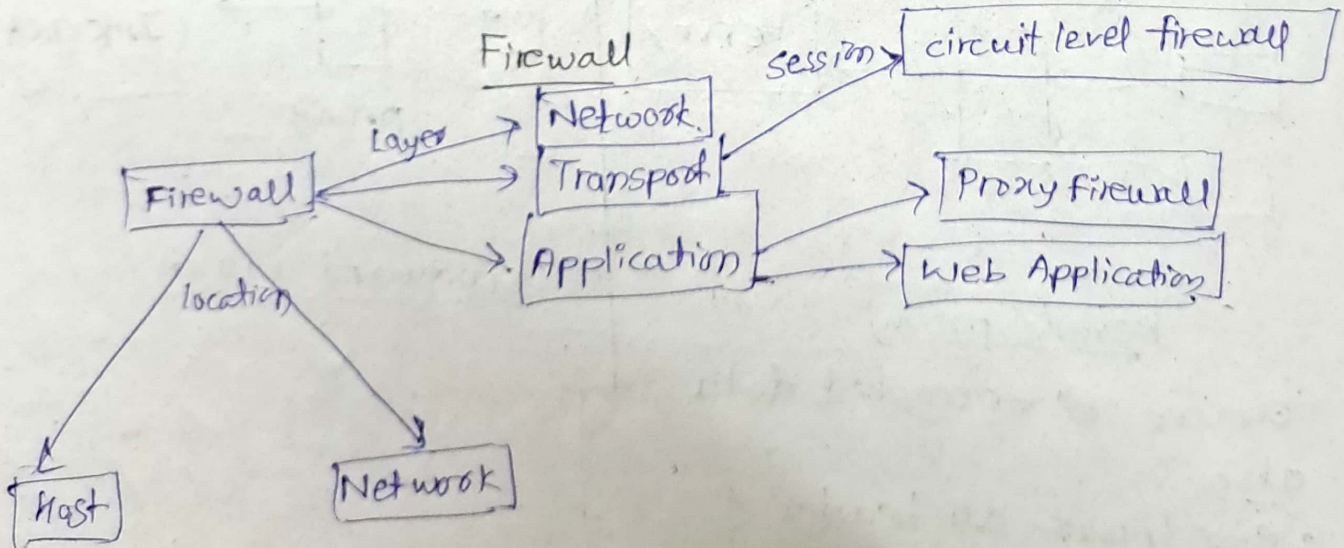
- can see & encrypted data also.
- Goes through all header & content.
- advantage - security to server
- drawback - overhead.

Forward proxy

WAF : Web application firewall
; identifies & monitors HTTP traffic between web applications and internet
; Normally, at service provider
: Bypassing WAF = Reaching / Attacking server
: can do deep inspection, because it has decryption keys.

IDS (applicable for IPS also)
↳ prevent





Antivirus

- similar to IDS (if host-based)
  - Firewall is at gate, so it cannot do activity of IDS or anti-virus.

- companies will never accept false positive

False Positive

- No malware but u say malware present
- costs time.
- signature-based never give FP
- Anomally-based gives both FP & FN

False Negative

- something present, but u are saying not present
- signature give FN always
- Anomaly based gives both FP & FN.

Why we need wireless security?

- anyone can capture packet
- anyone can connect.

https:- (http + SSL)
↳ (TLS)

IITA uses extended service set infrastructure

JAMMER - sends continuous data, to make collision & denial of service.

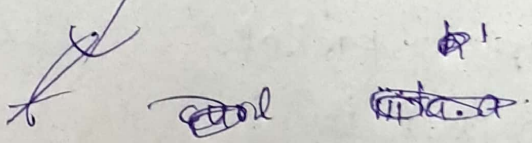
For 802.11
↳ security & noise control.

If channel is free, signal is like this

If data flow, difference in freq & amplitude after sensing chanel

Common Attacks on WLAN :- - Evil Twin
- Rogue Wireless devices - client isolation

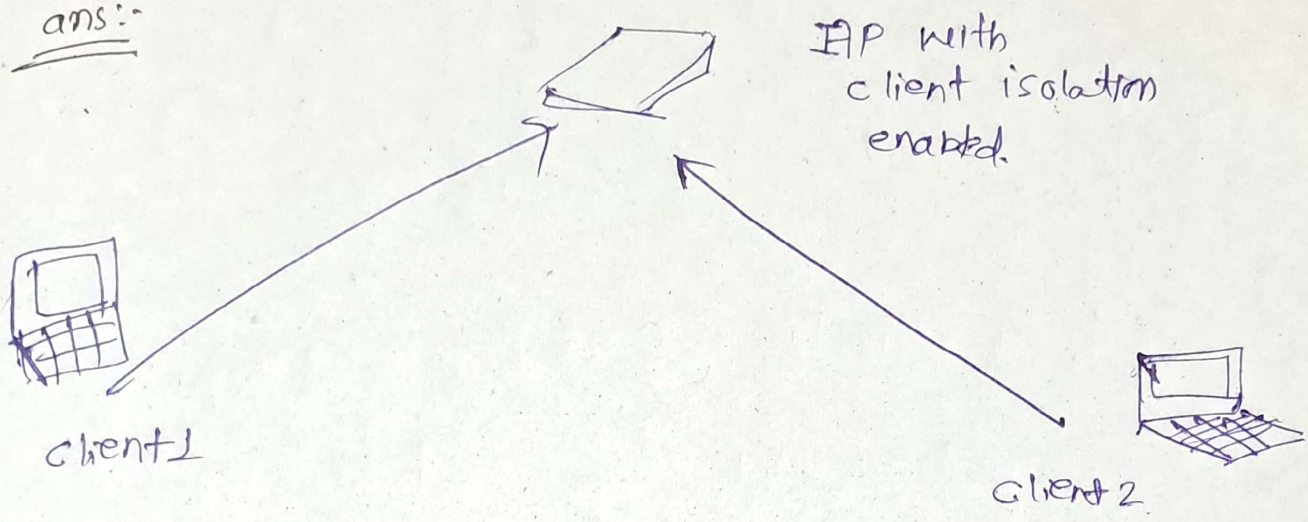
[use curl to destroy proxy, to play Valorant]



curl https://[redacted]iiita.ac.in

How to block people, but not owner/server?

ans:-

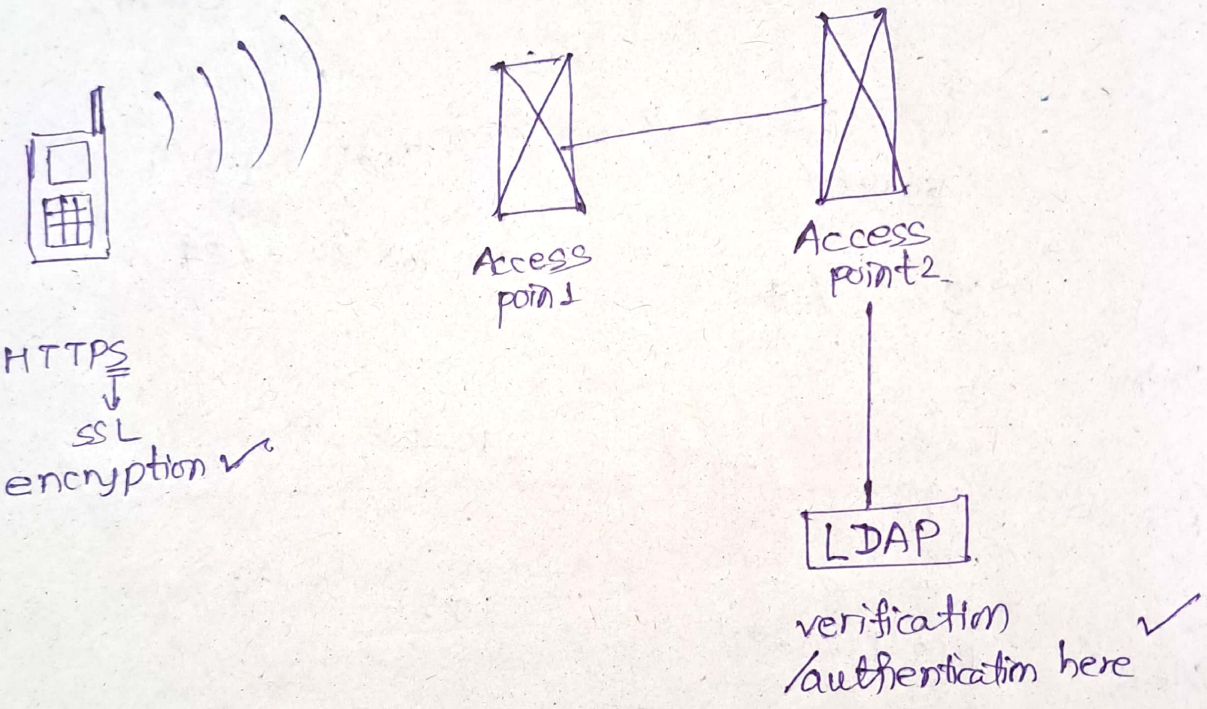


	Source	Dest.
(1) Reject / Drop	192.---/24	192.168.20.0/24
(2) Allow	192.---/24	192.168.20.1
(3) Allow	192.168.20.1	192.---/24

correct order :- 3,2,1.

802.11b Security services

- Two security services provided.
  - Authentication
    - shared Key Authentication
  - Encryption
    - wired Equivalence Privacy (WEP) – rejected later.



- When we use mobile hotspot we used shared key authentication.

Is this right method?

Wired Equivalence Privacy (WEP)

- Extended service set
- No key management

RC4

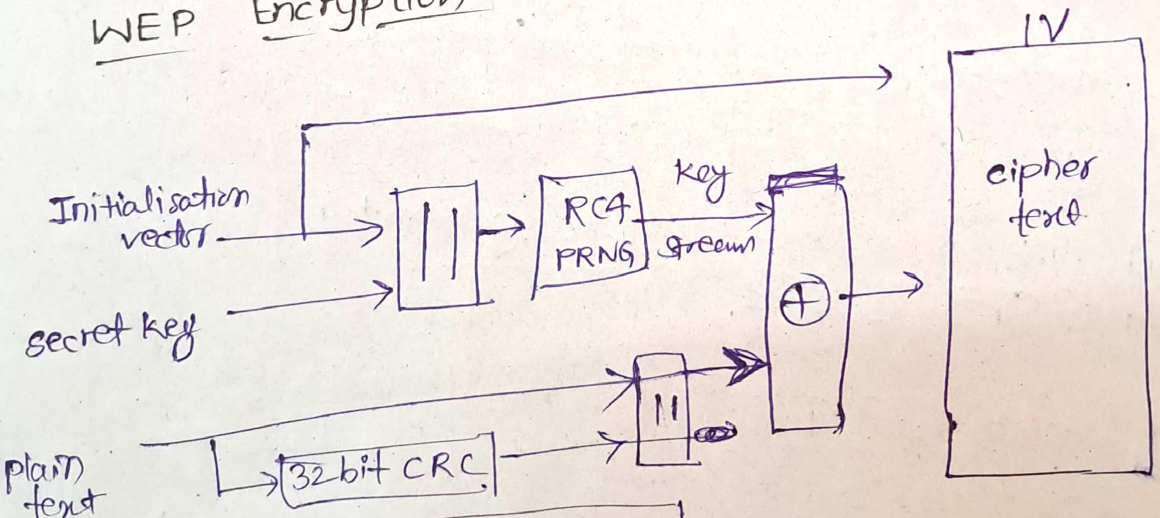
- Ron's Code number 4.
  - symmetric key encryption
  - XOR operator
  - 1 → 2048 bits.

WEP sending

- compute Integrity check vector. (32 bit CRC)
- plaintext encrypted via RC4.
- Ciphertext is transmitted.

IV in plain form

WEP Encryption :-



Before	Alice	Bob
secret key	✓	✓
plaintext	✓	○
IV	✓	○
Cypher text	✓	✓

Alice gives IV to Bob.

Decryption

• Assymetric Encrypt -Decrypt.

D (cipher text)

we shared ~~secret key~~ key-stream

Key-stream = RC4 PRNG (IV || SK).

Plaintext || CRC = ⊕ Keystream (ciphertext)

Keystream size = plain text size

↳ drawback of WEP decryption.

If unequal sizes, u will send plaintext partly

ex:- Keystream 1 1 1 1

plain text 1 1 1 1 0 0 0 1

⊕ 1 1 1 1 1 1 1 0.

• Each time new key must be generated

because $C_1 = P_1 \oplus K_1$

$C_2 = P_2 \oplus K_1$

$C_1 \oplus C_2$

$= P_1 \oplus K_1 \oplus P_2 \oplus K_1$

$= P_1 \oplus P_2$.

Hence, different key needed.

Hence, change IV again & again.

Also, keys will repeat, because limited size.

Port no. is of 16 bits

max ports $= 2^{16} - 1$

H.W. Viva again, from same questions.
with proper Justification

Initialisation vector

- some use pseudo random IV generator.
  ↳ may give IV repeatition
- some use simple ascending counter
- some switch between ascending & descending.

Passive WEP attack

- If 24bit IV is an ascending counter.
- If Access Point transmits at 11Mbps,
- All IVs are exhausted in roughly 5hours
- Passive attack (Phishing, Sniffing, Eavesdropping) (Man in middle)
  - Attacker collects all traffic.
  - Attacker could collect 2 messages :-
    - Encrypted with same key and same IV.
    - statistical attacks to reveal plaintext.
    - plaintext XOR ciphertext = keystream.

How? • IV goes in ~~text~~ form, secret key is common for all.
• same IV packet can be detected.

$P_1 \oplus K_1 \oplus P_2 \oplus K_1$

$\Rightarrow P_1 \oplus P_2$ → can be predicted by statistical analysis of characters in message.

- Active WEP attack :-
  - If attacker knows plaintext & ciphertext pair.
    - Keystream known
    - Attacker can create correctly encrypted message

- some uses Limited WEP keys, hence prone to Brute force.

$ARC_4 = RC_4$.

* special symbols may bring attacks :- SQL injection
  ex:- @, ., etc

Why passwords are hashed in database?

User	Password
Venkat	Venkat123

Rainbow Table.

↓

if this attacked.
password known
t_1

Hashed Password
abd3ac47i

↓

if this attacked.
password knowing
will take time
t_2

$t_1 < t_2$

but negligible difference.

we use salt

User	(Password || salt)
Venkat	

To increase complexity, we also use pepper.

password || salt || pepper

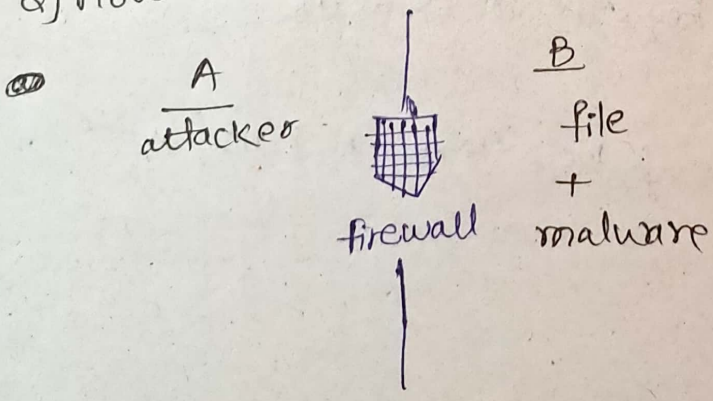
- pepper is not put in table, so it can't be stolen

Also, sometimes 4096 times hashing is done.

- Mathy Vanhoef discovered new vulnerabilities each time

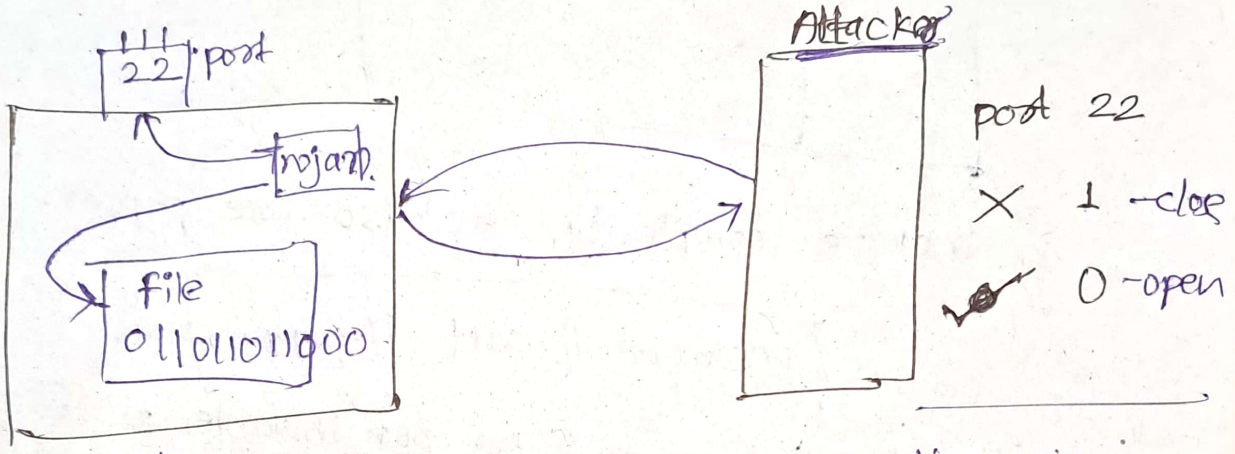
Monday discuss trojan horse & compromise

Q] How to steal file from others? How to get file



Advantage of Trojan :-

1) Read file
2) Open and close port.



victim

encoding using port open, close

can Hacker decrypt messages?

ans:- Yes, if shared key authentication is used. (we know key)

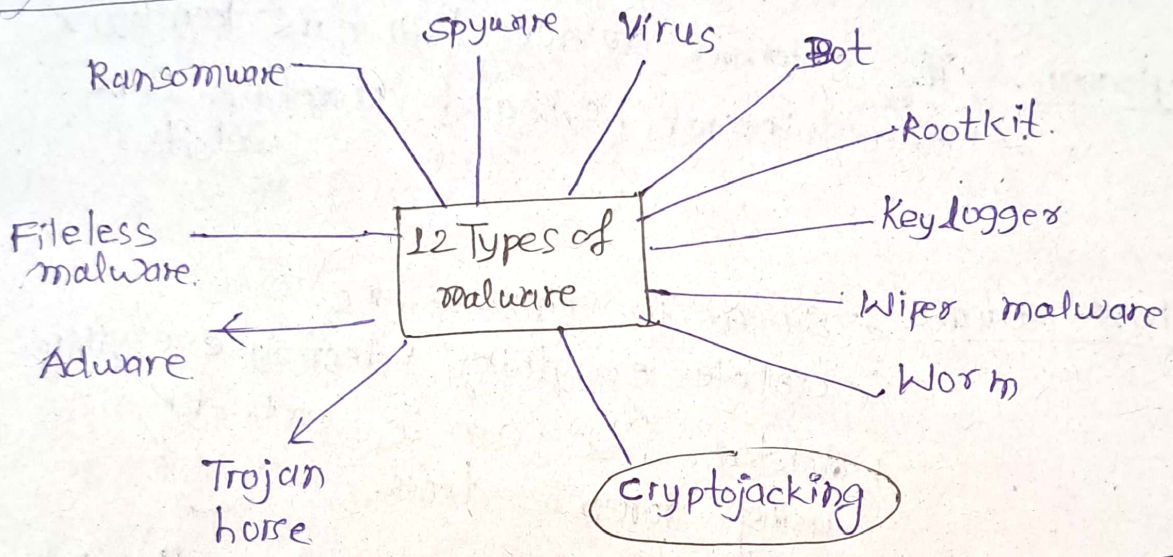
No, if shared key authentication + Deffie Hellman is used.

IV weakness

- If IV is weak, key stream is weak
- Passive attack.
- If first few bits of keystream is known all key stream is known.

Radius server - maintains authentication
- bass all passwords & username.

Why CSMA/CA ?



Bitcoin → mining a block → successfully accepted by all
↓
Block is considered successful.

cryptojacking → pirated apk files
→ runs mining on your device
→ gives bitcoins to attacker.

Ransomware:- Encrypts all files (except bootable files)
:- Asks for money, if u give money, they will give key.
:- Hackers payment wanted in bitcoin
:- Govt. looks at account transaction
:- Wannacry -2017, very few disclosed
:- Ransom - money.

Spyware:- focuses on credit card details, passwords etc

Bot:- Perform denial of service

Rootkit:- • Why not wait until antivirus?
• Start before anti-virus, & kill anti-virus.
• Bios start → Rootkit → OS → Anti-virus.

Keylogger:- • The external devices can have keylogger
:- Hence virtual keyboards used on Bank websites

Wiper malware:- :- similar to Ransomware
:- delete everything & destroy everything
:- deleted files can be extracted using forensic tools.
:- delete means just removing the index
:- file is still present on disc, until overwritten by others

Virus	worm
• needs human being to move from 1 computer to another.	• propagates by itself.

Safety - Precaution - Gun. - done by myself

Security - Prevention - Guard - provided by others.

Risk - what will be the damage.

Threat -

Vulnerability - weakness of system.

Attack - damaging

Exploit - exploiting vulnerability

0-day vulnerability :- not yet known, even to manager.

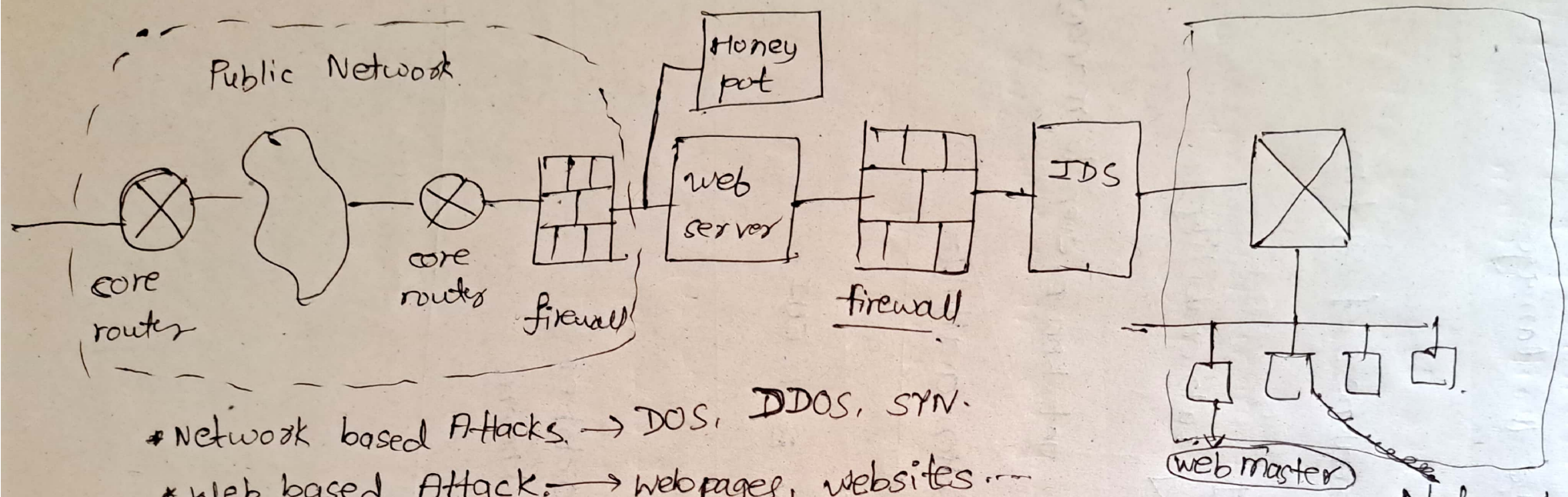
0-day attack :- no solution available.

SIEM Tools

SNORT is in console, SIEM is in GUI.

- Abhishek sir onwards
- 1 Lab evaluation left
- cyber sec awareness - October
  * Quiz - prize known.

:- Abhishek Vaish sir :-



* Network based Attacks → DOS, DDOS, SYN.
* Web based Attack → webpages, websites ...

These are susceptible to multiple attacks

- website
- XSS
- SQL injection

• Database server should be at end (inside security)

1) Keep web server is on perimeter.
It has to give info to public.

Scope of work → Network based Attacks
→ Application based Attacks.

Most common attacks :- Infect website with malware.
:- ~~Infect~~ Malware

Q) Who manages web server? ans- Web Master

So, Traffic flows website to web master
IF Hacker gains access to this machine, it can enter the webserver.

Q) which port number should be open in firewall to facilitate web traffic.?

ans:- 80 443 port
↓ ↓
http. https

- Web servers are constantly under Attacks
- Unprofessional programmers developing websites overnight, are making their cyberspace vulnerable.

Netstumbler → get all access points with SSID & passwords.

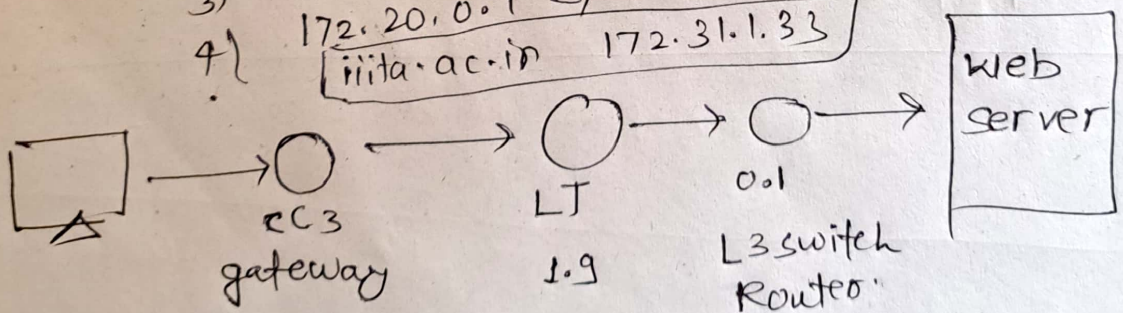
cisco password:-Tsunami123
Leads to switch level.

---

ping iiita.ac.in ⇒ gives IP addrs

tracert 172.31.1.33 ⇒ gives devices/hops between our device & iiita.ac.in (web server)

Scope
1) 172.20.35.1 ⇒ cc3
2) 172.20.1.9 ⇒ LT
3)
4) 172.20.0.1 ⇒ iiita.ac.in 172.31.1.33



∴ Passive attack done.

Now, OS fingerprinting, active information gathering.
Use tools to scan live ports, hosts & services.

Vulnerability Assessment :-

- Use automated tools (Nessus, open VAS) to scan known vulnerabilities

- web site
  - URL embedded
    - Active URL
    - Dormant URL

port 21 – FTP
port 22 – SSH - ~~indicates used by attacker~~

OWASP

Most recognized and widely used OWASP resources.

- OWASP Top Ten.
- OWASP ZAP.
- OWASP Dependency-check.
- OWASP SAMM.

DVWA – emulator for attacking web server.
– has ~~so~~ critical vulnerabilities in it.
  - Injection flaws
  - Broken Authentication
  - sensitive

(given in slides.