× ×

05/04/24
FRIDAY

DAY - 5

Todays work
-> Complete Pre-Course
->

ARP - Mapping MAC address and IP address.

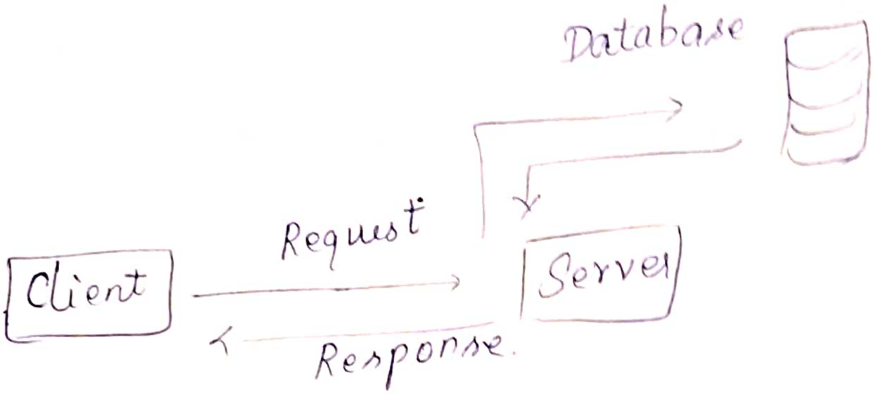
-> wire shark -> statistics

https
↳ TCP Handshake
↳ TLS handshake
↳ Encryption
↳ Data Transfer

* There are many flags available in Handshake.

1. Resered
2. Push
3. ACK
4. Fin
5. Urgent
6. SYN
7. Reset
8. Accurate

Packet Crafter tools
-> Packed design can be done.



HTTP methods

1. GET - Request
2. POST - No data in DB
3. PUT → Update DB
4. OPTIONS
5. DELETE

Response Code

→ 1 - Informational
2 - OK
3 - Redirection
4 - Client Error
5 - Server Error

Testing

Functional

→

Non-Functional

→ security

1. Production Environment
2. Staging Environment
3. QA Environment

Security test can be done

→ Live websites / web app

→ Real Copy

→ Test

SDLC → Each phase has different testing

Informational - Protocol changes

BURPSUITE

Client ---- PROXY --- Server
Burpsuite

* Data first move to - PROXY then Server
Server to - PROXY

* DARK Web - which is not available in google engine

Tor   .onion

Client ---> Proxy1 --- Proxy 2 -- Proxy 6 --- Server

Bitcoin 1b = 67,000 dollars.

Request	Response
	Response Code
HTTP method	

Useragent - Browser

above blank line - all are headers

Body

Interception

→ Gathering info and processing

[8080 Burpsuite]
⊗ ⊗

→ Burp - On

Edit virtual machine - 2GB RAM

Processor - 1
Core - 2 or 1

```
Cmd: sudo nmcli networking on
```

```
Cmd: sudo Service NetworkManager start
```

} working

do as a super user - sudo

```
Cmd: cat /etc/apt/sources.list
```

→ Read

Cmd : nano

[Ctrl + shift + c] - Copy
[ctrl + shift + v] - Paste

```
Cmd: nano /etc/apt/sources.list
```

Proxy refuse - Burp - ON [- To send traffic

```
Cmd: sudo service apache2 start
```

webserver starting

→ Import Certificate
→ burpsuite in browser
↓ Downlod CA certificat

URl - encoding

Cookies - Session Validates

By using Cookies we Can use

Cookies - enport - import

→ Burp - Repeater - Log out from all devices

→ Session Hijacking
→ Session Token

——— × ——————— × ———————

http : www. google. com / directory / filename.html

http/https - web protocol

TLD -

Domain - google.com

Subdomain - gmail. google. Com

```
ls var/www/html/
```

→ ls -l path

→ pwd - Path

Linux - - /var/www/html

windows - - C:\inetpub\wwwroot

→ http/2 - HTTPS

HTTP/1.1 - HTTP

Enumeration

* Finding step by step
* User enumeration.

Proxy - history

Repeater - Manual testing

Intruder - automatic Search

pass - select → add - Confirmation

→ Position

SNIPER ATTACK → ↳ Payloads - Paste

↓

Start attack

* The website will block it

Settings - Grep - Extract

↓

(Search) - Add - select ok

* Rate Limiting - [Per second How much Request the server]

FIREWALL

* Manages Request
* If more request hits, it drops the packets.

WAF + Rate Limiting

↓

Web application Firewall.

INTRUDER

→ SecList - Millions of words

→ discovery - web content

- Raft