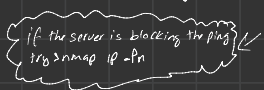
information Gathering

1. Target site : any.com
2. find subdomains
   - Virustotal.com
3. rank subdomains by unpopularity
4. find ip_address
   - ping any.com
5. which programming language the site is using
   - whatweb any.com
     - x-powered-by [-----]
6. find open ports and services
   - nmap ip_address {normal scanning}
   - nmap ip_address -sV {agressive scanning}
   - nmap ip | nmap -sC ip
     - to detailed infos about target.

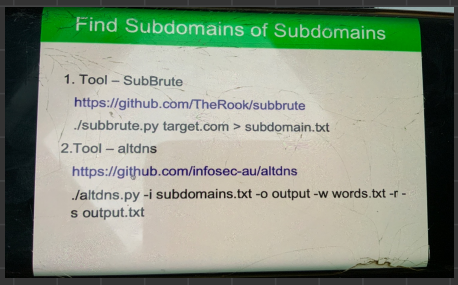
   

7. Server info
   IIS or apache or tomcat or nginx
   - whatweb ip
     - HTTPServer [----]

Recon

- Find subdomains using virustotal or a tool subbrute from github

And some times subdomains has also subdomains so for that use altdns



Scanning target:

- whois
- Reverse IP lookup (yougetsignal.com)
- Subdomain Enumeration (knock-github, virustotal)
- OS Detection (ping: TTL ≤ 60 → linux , TTL ≥ 110 → window
- Builtwith.com or wappalazyer

* Shodan.io

  webcam

  City: "New York"

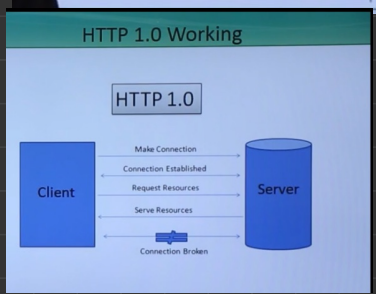
  Country: "CA"

  OS: "Linux"

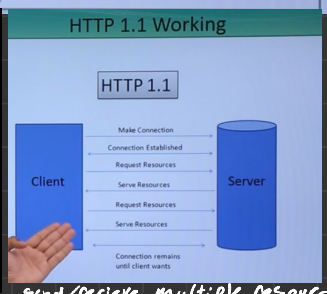
  port: 443

HTTP Basics:

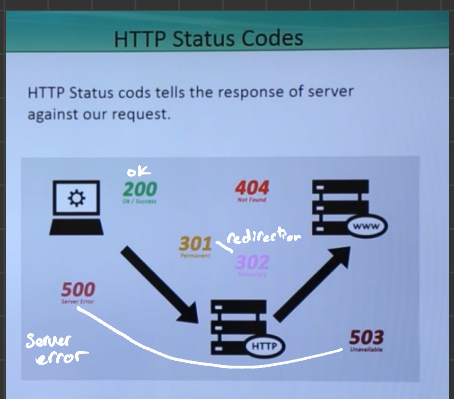
HTTP 1.0	HTTP 1.1
•HTTP 1.0 It is older version	• Latest version
•Use single request to get resource from the server then close the connection.	•It uses single connection to request resources from the server , multiple times.



only one request can be handled.



send/recieve multiple resources in one connection



HTTP Methods

HTTP Methods are types of request which we want to send . Different HTTP Methods are as follows –

SAFE METHODS — NO ACTION ON SERVER	GET	HTTP/1.1 MUST IMPLEMENT THIS METHOD
	HEAD	INSPECT RESOURCE HEADERS
MESSAGE WITH BODY — SEND DATA TO SERVER	PUT	DEPOSIT DATA ON SERVER – INVERSE OF GET
	POST	SEND INPUT DATA FOR PROCESSING
	PATCH	PARTIALLY MODIFY A RESOURCE
	TRACE	ECHO BACK RECEIVED MESSAGE
	OPTIONS	SERVER CAPABILITIES
	DELETE	DELETE A RESOURCE – NOT GUARANTEED

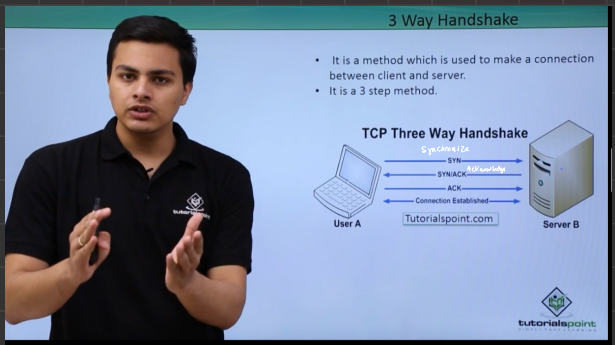
Get: for accessing any resource or fetching any resource with no action on Server.

Head: for seeing the server http header but not the html data. with no action on server.

put, Post: for sending an input to the server.

Options: to know what kind of http methods are enabled on a remote server. (user send http request by using options method)

delete: Dangerous, because if delete Method is enable on any server, a user can delete any particular resource on the server. by sending http request using delete method.



handshake a 3-way handshake is the first
process before requesting any resource

So used to make connection

How to use netcat:

```
> nc any.com/IP port
GET / HTTP/1.0
Host: any.com
```

Server made only one connection and cancelled = one connection on time

```
> NC google.com 80
GET / HTTP/1.1
Host: google.com
```

Server made one connection and still connected to make another connection = multiple connection one time

Curl Overview

- Curl is small computer utility which is used for transferring data from various protocols.
- Libc curl is a free client-side URL transfer library.
- It supports cookies , HTTP , HTTP/2 , FTP and Gopher etc.
- It also performs SSL certificate verification.

Gopher is a protocal, that has been used before http for requesting resaurce but nowadays it's not used.

With the help of curl we can send http request by using different http methods.

> curl -v -X http_method any.com -L -o file.txt

-v : for more details.

-L : if site has redirection, so curl follow that redirection

Cookies Basics

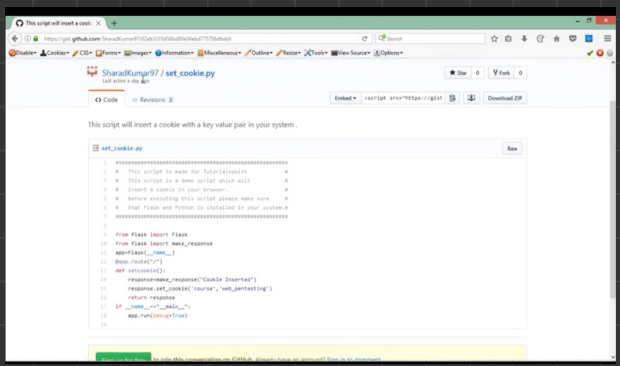
- Cookies are small file which contains information
- Not an executable file
- Stored on a client side
- Sometimes used for user preferences
- Name Value Pair
- Sometime contains user session ,login information

Cookies Internal

Information inside a cookie is in the form of name value pair.
E.g. – [Name : Value]

Important Fields in cookies –

1. Domain
2. Path
3. Secure — like https to use
4. Expires
5. Httponly — if this presents inside a cookie, which mean cookie can't be stolen by using js.



Sessions Basics

- Session Id is a long, random alpha-numeric string
- It uniquely identifies user on a website
- Sometime it get stored in cookie

Session vs Cookies

- Cookie is stored on client side
- Sessions are stored on server side
- Values are hidden in session which make them more secure than cookies

if server stored my session ID in DB, then there should be not a session file created.