Hacking Web Applications & Servers

Identify Technology

Identify Technology (Footprint)

- Identifying the technology that is used by the web application would give us an idea on how to exploit that particular application.

List of tools used to identify the technology

1. httprecon
2. wappalyzer
3. whatweb (CLI)

Other Methods

- Using Telnet
- Using NetCat

Nmap Scripts

Normal HTTP Enumeration

```
nmap -sV --script=http-enum www.xyz.com
```

WAF Detection

```
nmap -p 80,443 --script=http-waf-detect www.xyz.com
```

Directory Brute force

Dirb

This is a really easy tool to use:

```
dirb http://target.com
```

Dirbuster

It is a GUI You start it with:

```
dirbuster
```

```
dirb http://192.168.1.5/dvwa
```

Gobuster -> tool

Service Bruteforce

Cracking FTP with Dictionary attack

```
nmap -p 21 [IP]
```

```
hydra -L usernames.txt -P passwords.txt ftp://[IP]
```

Hydra tool

`hydra -L /Path/To/Username/WordList -P /Path/To/Password/WordList 10.10.10.x ftp`

On Hydra, you can set your desired service to brute force, on the above command you can see I have set the brute force to FTP. Same as you can set for any service. Examples, SSH, RDP, SAMBA, etc...

Example 1: Bruteforcing Both Usernames And Passwords

Type the below command on the terminal and hit Enter.

```
hydra -L user.txt -P pass.txt 192.168.29.135 ssh -t 4
```

- **-l** specifies a username during a brute force attack.
- **-L** specifies a username wordlist to be used during a brute force attack.
- **-p** specifies a password during a brute force attack.
- **-P** specifies a password wordlist to use during a brute force attack.
- **-t** set to 4, which sets the number of parallel tasks (threads) to run.

medusa tool

`medusa -h 10.10.10.x -U /root/Documents/user_list.txt -p /root/Documents/pass_list.txt -M ftp -F`