Scanning:

[+] Nmap

> nmap -sC -sV - oA *fileName* **IP_address**

> nmap -sC -sV -No *fileName* **IP_address**

> nmap -Pn -p 80,443 --script http-enum **IP_address**

> nmap -p 443 --script ssl-heartbleed **IP_address**

> nmap --script vuln -oA *fileName* **IP_address**

[+] Sparata

> GUI sanner

```
NOTE
-----
Port 53 tcp     | check zone transfer
port 443        | run SSL [heartbleed  nmap script]
```

[+] Sslyzer - Scannning SSL ports :

- ssylzer --heartbleed IP_Address
- when port 443 is open, run ssylzer against the port to determin if there is a heartbleed or poodle vulnerability

Service Enumeration :

DNS Enumeration

If TCP 53 is open could indicate a zone transfer

[+] NSlookup:

```
nslookup 172.0.0.1
```

```
nslookup IP_address of the machine
```

Start looking up local host; it may show up the host domain

[+] DNSrecon

```
dnsrecon   -r 10.10.10.0/24   -n machine_IP_address
```