Cheat Sheet (Quick Pentest)

by Muhammad Bilal

www.linkedin.com

https://www.linkedin.com/in/muhammad-bilal7276/

Information Gathering

Directory Busting and VHOST Enumeration

Dir Busting

> Find Directories and pages of a website

VHOST ENUMERATION

> Find subdomains of a website

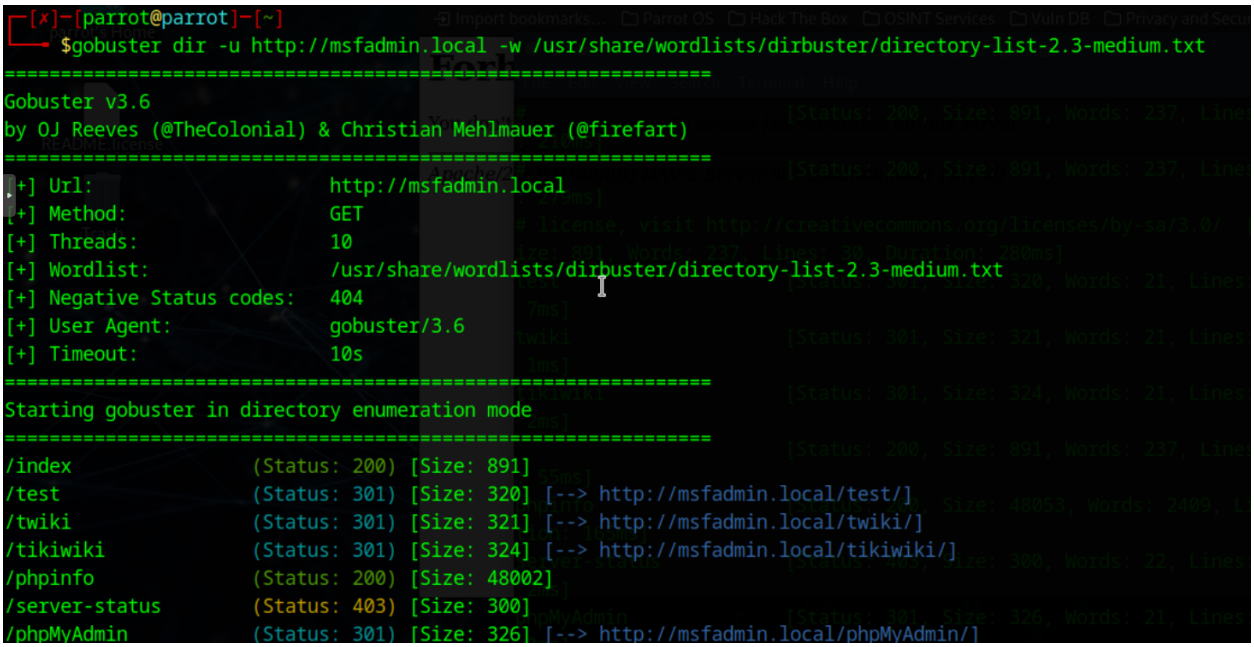
Wordlists

```
Sudo apt install seclists
```

DIR BUSTING

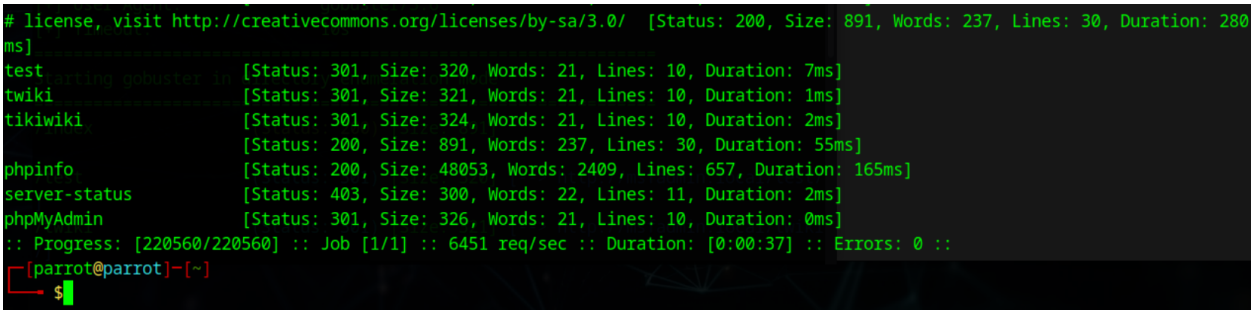
Gobuster

```
gobuster dir -u http://10.10.10.10 -w /usr/share/wordlists/dirbu
```



FFUF

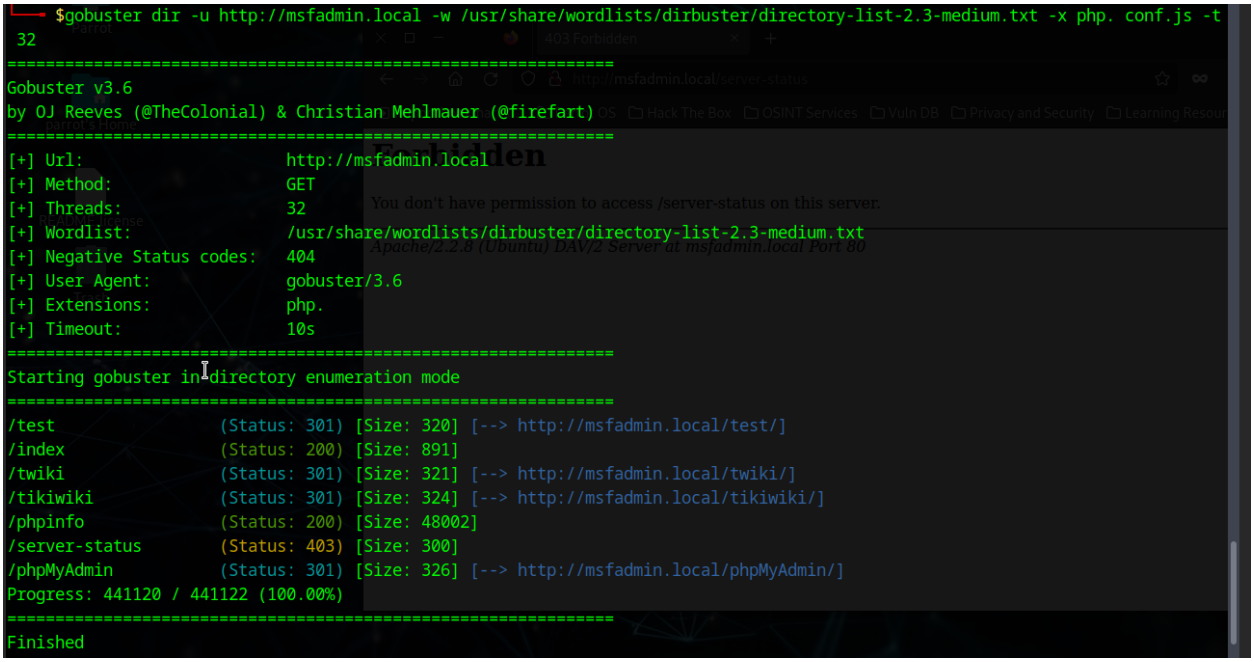
```
ffuf -u http://10.10.10.10/FUZZ -w /usr/share/wordlists/dirbuste
```



Finding Files

Gobuster

```
gobuster dir -u http://10.10.10.10 -w /usr/share/wordlists/dirbu
```



FFUF can also be used to brute force the files

FFUF

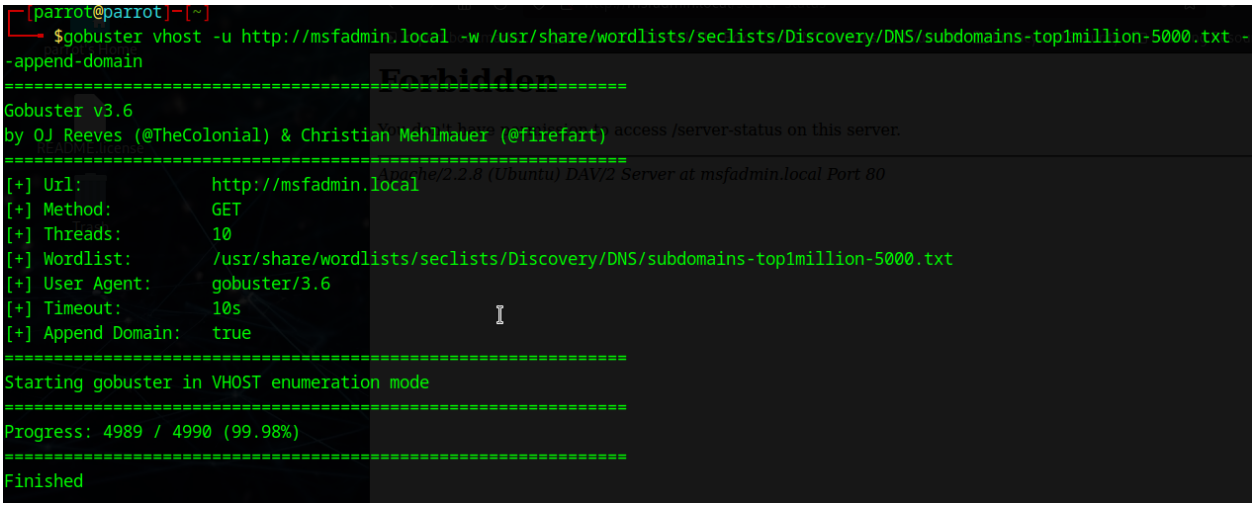
```
ffuf -u http://10.10.10.10/FUZZ -w /usr/share/wordlists/dirbuste
```

VHOST Enumeration

- VHOST enumeration is the process of identifying virtual hosts (VHOSTs) on a web server. A virtual host is a method of hosting multiple domain names on a single web server. Each domain name is associated with a unique IP address or port number, and the web server uses this information to route incoming requests to the appropriate website.

Gobuster

```
gobuster vhost -u http://example.com -w /usr/share/wordlists/Sec
```



FFUF

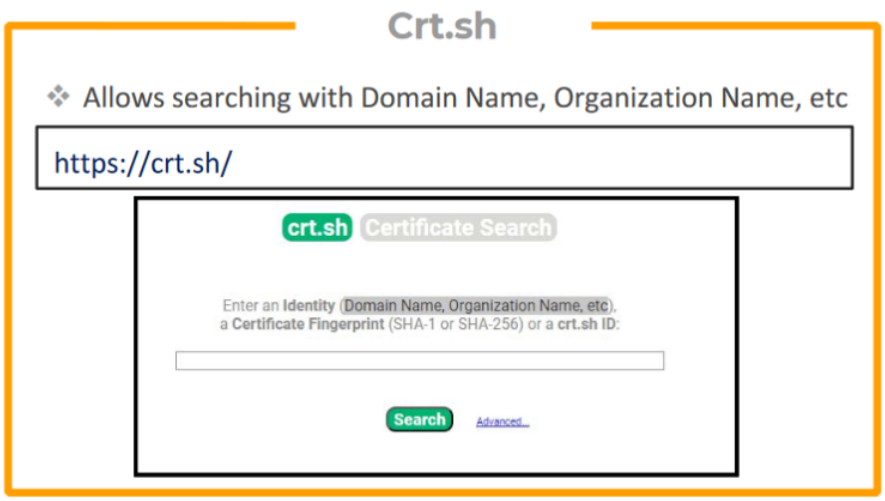
```
ffuf -u http://example.com -w /usr/share/seclists/Discovery/DNS/
```

Passive Reconnaissance with Digital Certificates

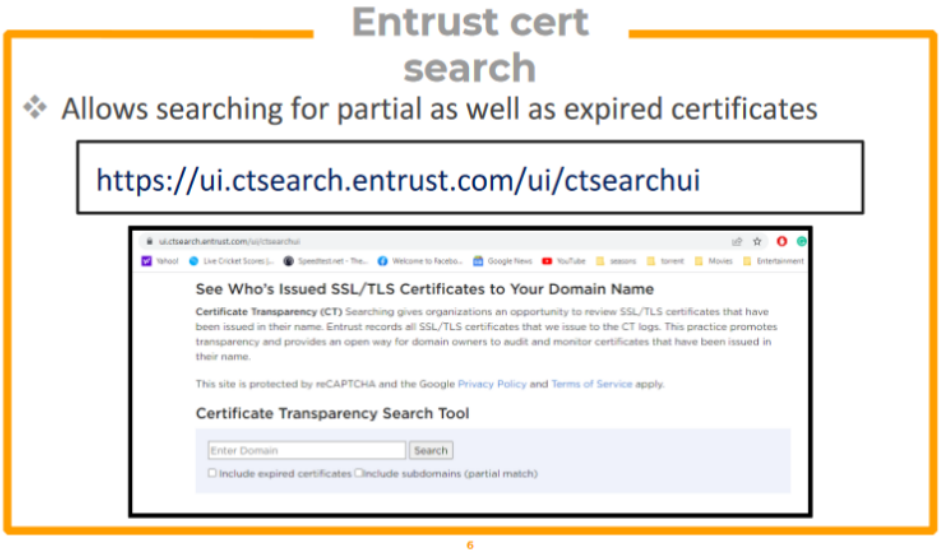
Digital certificates are primarily used to ensure the security and authenticity of websites. They help to establish a secure connection between a user's browser and the website they are trying to access, by verifying that the website is legitimate and encrypting the data that is exchanged between the two parties.
Digital certificates can also be used to discover subdomains of a website. When a certificate is issued for a specific domain, it is typically issued for that domain and any of its subdomains. Therefore, by searching for certificates issued to a particular domain, it is possible to discover subdomains that are associated with that domain.

Digital Certs search engines

Crt.sh



Entrust cert search



Censys

DNS Enumeration

DNS enumeration, also known as DNS recon, is the process of gathering information about a domain name system (DNS) infrastructure and its associated records. DNS is responsible for translating human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.168.1.1). DNS enumeration involves querying DNS servers to obtain various types of DNS records, which can reveal valuable information about the target domain including hidden or internal subdomains

The primary purpose of DNS enumeration is to gather intelligence about a target's DNS infrastructure. It can be used by security professionals, penetration testers, or malicious actors to identify potential vulnerabilities, misconfigurations, or targets for further attacks. By gathering information about the target's DNS infrastructure, an attacker can potentially identify subdomains, mail servers, or other potential entry points for further attacks

Record Types

Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

Axfr	Zone transfer. Includes all records about a domain

Dig

Most common DNS Enumeration tool DNS Enumeration swiss army knife

❖ Dig can be used for simple domain lookup

```
>dig zonetransfer.me
```

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ dig zonetransfer.me

; <<>> DiG 9.18.8-1-Debian <<>> zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2143
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 939460665727bbb3010000006486aed7fd6efd81b896fe69 (good)
;; QUESTION SECTION:
;zonetransfer.me.               IN      A

;; ANSWER SECTION:
zonetransfer.me.        7200    IN      A       5.196.105.14
```

Dig 1.0

❖ We can also specify the type of record with dig command

>dig ns zonetransfer.me	(Name server)
>dig mx zonetransfer.me	(Mail server)
>dig cname zonetransfer.me	(cname record)

```
┌──(kali㉿kali)-[~]
└─$ dig ns zonetransfer
```

Host

Simplest DNS Enumeration tool

Host

- Host provides a simple way to perform DNS lookups and retrieve DNS records.

```
>host zonetransfer.me
```

```
┌──(kali㉿kali)-[~]
└─$ host zonetransfer.me
zonetransfer.me has address 5.196.105.14
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.
```

- Host can be used to map IP address to the website with reverse lookup

```
>host 192.168.2.2
```

```
┌──(kali㉿kali)-[~]
└─$ host 5.196.105.14
Host 14.105.196.5.in-addr.arpa. not found: 3(NXDOMAIN)
```

nslookup (A cross platform tool for DNS Enumeration)

❖ We can use nslookup on windows to enumerate dns records

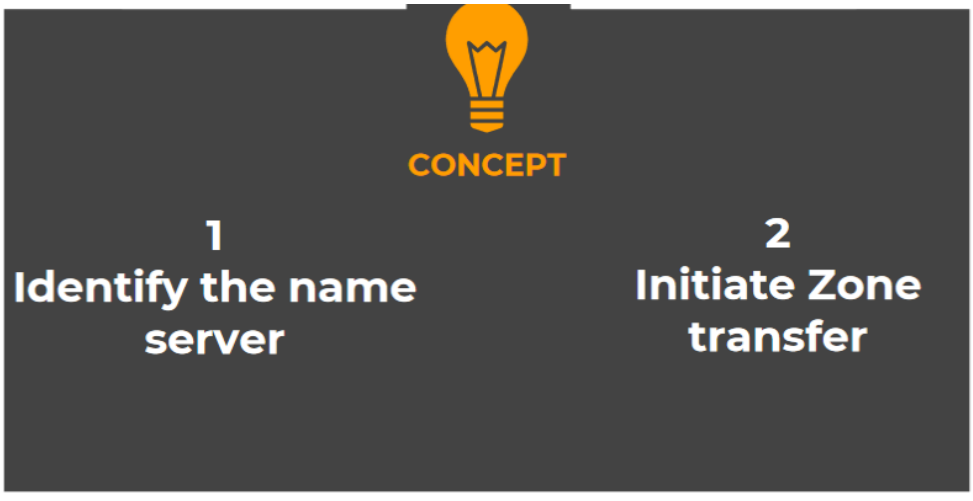
```
>nslookup zonetransfer.me
```

```
C:\Users\Ammar>nslookup zonetransfer.me
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  fe80::1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    zonetransfer.me
Address:  5.196.105.14
```

Zone Transfer

Zone transfer is a mechanism in DNS for sharing and synchronizing DNS database information between servers. Pentesters and hackers can leverage zone transfer to gather intelligence about a target's DNS infrastructure. Zone transfers provide a comprehensive list of DNS records, including subdomains, IP addresses, and mail servers



- Host tool can be used to initiate zone transfer. First look for the name server and then check if it supports zone transfer. Try all listed name servers for best results

```
>host -t ns zonetransfer.me
```

```
┌──(kali㉿kali)-[~]
└─$ host -t ns zonetransfer.me
zonetransfer.me name server nsztm2.digi.ninja.
zonetransfer.me name server nsztm1.digi.ninja.
```

- Dig can also be used to initiate zone transfer

```
>dig ns zonetransfer.me
>dig axfr zonetransfer.me @nsztm2.digi.ninja
```

```
┌──(kali㉿kali)-[~]
└─$ dig axfr zonetransfer.me @nsztm1.digi.ninja

; <<>> DiG 9.18.8-1-Debian <<>> axfr zonetransfer.me @nsztm1.digi.ninja
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209
600 3600
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04V
lMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
```

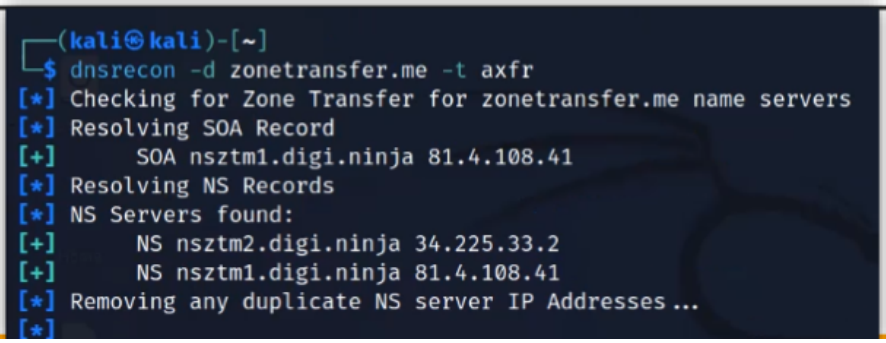
s

Automated tools for DNS

DNS Recon

- DNSRECON is designed to automate and streamline the process of querying DNS servers, retrieving DNS records, and conducting various types of DNS-related scans

```
>dnsrecon –d zonetransfer.me –t axfr
```



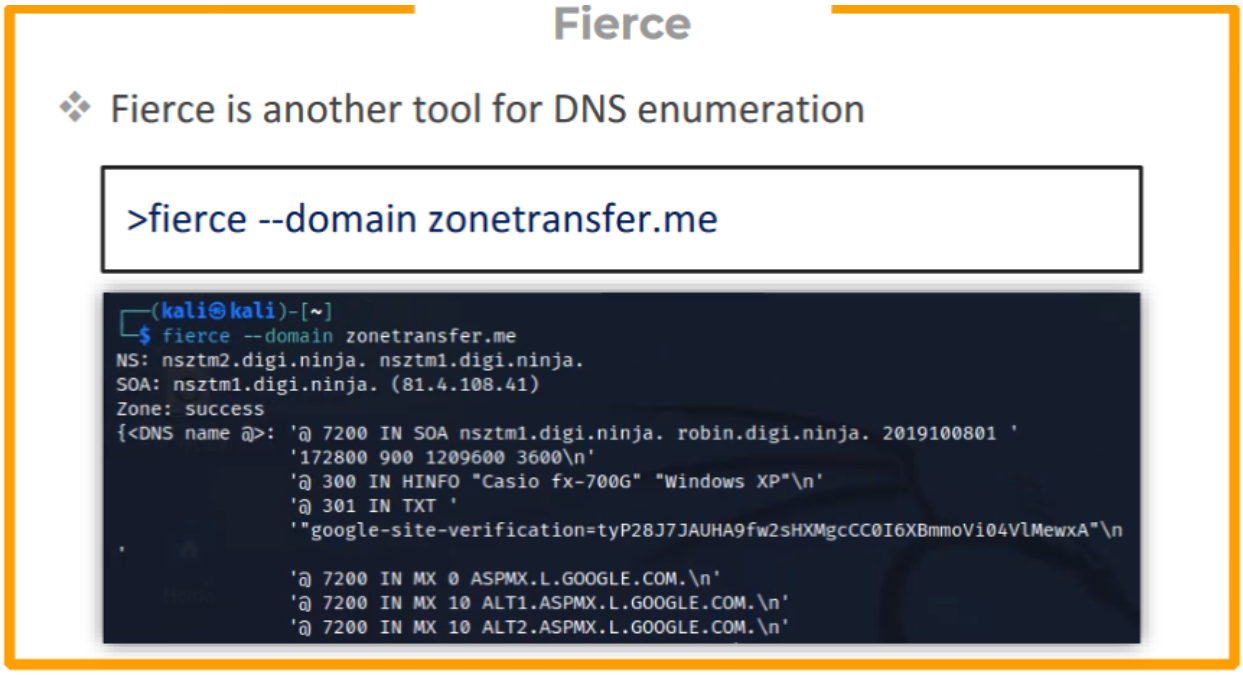
DNS Recon

DNS Enum

- DNSenum is another automated tool that collects all possible information about the target

```
>dnsenum zonetransfer.me
```

DNS ENUM



Fierce

Scanning

Host Discovery

Identifying Live Hosts

Host Discovery is the always the first step in any ethical hacking certification exam and in CTFs. It involves enumeration IP addresses of the systems available in the test environment

Netdiscover is used to scan for the live hosts on the network

```
netdiscover -i (network interface name)
```

Ping scan is used to scan for the live hosts on the network

```
nmap –sn 192.168.18.1/24
```

Arp scan is another method to scan for the live hosts on the network

```
nmap -sn -PR 192.168.18.0-255
```

To find Ip addressed

```
=>  arp-scan -l
=> netdiscover -r 182.14.4.0/24
```

Nmap has a vast variety of scans aval. Some of the most useful scans for host discovery are listed below

```
nmap -sn -PU 192.168.18.110 //UDP ping scan
nmap -sn -PE 192.168.18.1-255 //ICMP Echo Ping scan
nmap -sn -PM 192.168.18.1-255 //Mask Ping scan (use if ICMP is
nmap -sn -PP 192.168.18.1-255 //ICMP timestamp scan
nmap -sn -PS 192.168.18.1-255 //tcp syn ping scan
nmap -sn -PO 192.168.18.1-255 //IP protocol scan.use different
```

Service and OS Discovery

Service Discovery

- Identify Open Ports
- dentify Services Running on the ports

Nmap is the go to tool for identifying open ports and services running on these ports

```
nmap –sS –sV 192.168.18.1/24
```

Nmap Command

```
#scan whole subnet

nmap 192.168.17.0/24


# TCP Scan
sudo nmap -T4 -p- -A 192.168.18.73

# UDP Scan

nmap -sU -T4 -p- 192.168.18.73

# For ports only
nmap --script=banner  10.129.228.159
```

Nikto scan

```
nikto -h http://192.168.18.73
```

Exploitation

Password Brute force

Hydra

```
hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords
```

Post Exploitation

Windows credentials dumps

```
hashdump
```
