

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
FOOTPRINTING & RECONNAISSANCE



DI SUSUN OLEH

Nama : M Abdul Aziz
NIM : 21/474516/SV/18951
Hari, Tanggal : Selasa, 2 Mei 2023
Kelas : RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

Praktikum Keamanan Informasi 1

Footprinting & Reconnaissance

I. Tujuan

—

II. Latar Belakang

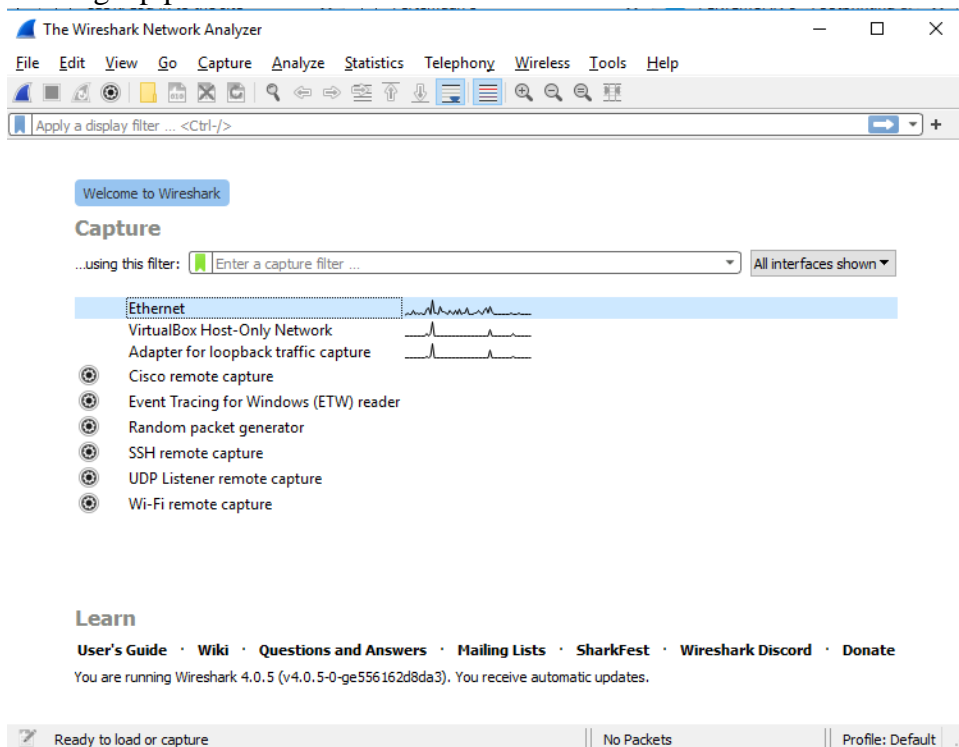
III. Alat & Bahan

— S

IV. Instruksi Kerja

TEKNIK CRAFTING

1. Buka server windows Start --> All Apps dan klik Wireshark untuk memulai aplikasi
2. Jendela utama Wireshark muncul. Klik dua kali pada Ethernet untuk mulai menangkap paket.



3. Wireshark mulai menangkap lalu lintas pada antarmuka Ethernet.
4. Masuk ke VM kalilinux
5. Cek IP PC Windows

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::1cf5:161a:795e:c9af%4
IPv4 Address. . . . . : 10.33.107.40
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.33.107.254
```

6. Buka terminal dan ketik `hping3 -c 3 10.33.107.40` dan tekan Enter.

```
(root@kali)~# hping3 -c 3 10.33.107.40
HPING 10.33.107.40 (eth0 10.33.107.40): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.33.107.40 ttl=127 DF id=1574 sport=0 flags=RA seq=0 win=0 rtt=7.8 ms
len=46 ip=10.33.107.40 ttl=127 DF id=1593 sport=0 flags=RA seq=1 win=0 rtt=15.8 ms
len=46 ip=10.33.107.40 ttl=127 DF id=1608 sport=0 flags=RA seq=2 win=0 rtt=11.6 ms

--- 10.33.107.40 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.8/11.8/15.8 ms
```

7. Untuk IP, cek PC windows pada cmd ketik `ipconfig` ganti IP pada command no 5
8. Perhatikan hasil tangkapan wireshark di Windows, ada berapa paket terkirim?

Capturing from Ethernet

No.	Time	Source	Destination	Protocol	Length	Info
2874	38.481503	13.107.6.171	10.33.107.40	TCP	1510	[TCP Out-Of-Order]
2875	38.481503	13.107.6.171	10.33.107.40	TLSv1.2	92	Application Data
2876	38.481546	10.33.107.40	13.107.6.171	TCP	54	49915 → 443 [ACK]
2877	38.481565	10.33.107.40	13.107.6.171	TCP	54	49915 → 443 [ACK]
2878	38.483538	10.33.107.40	13.107.6.171	TLSv1.2	96	Application Data
2879	38.511966	13.107.6.171	10.33.107.40	TCP	60	443 → 49915 [ACK]
2880	38.877588	Cisco_3a:64:14	Spanning-tree-(for-...	STP	60	Conf. Root = 3270
2881	39.171545	10.33.107.30	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.
2882	39.765187	10.33.107.39	10.33.107.255	BROWSER	227	Become Backup Br
2883	40.172248	10.33.107.30	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.
2884	40.635675	Routerbo_66:83:38	Broadcast	ARP	60	Who has 10.33.107.

9. Ketik `hping3 --scan 1-3000 -S x.x.x.x` (IP PC windows) dan ketik Enter.

```
(root@kali)-[/home/kali]
# hping3 --scan 1-3000 -S 10.33.107.40
Scanning 10.33.107.40 (10.33.107.40), port 1-3000
3000 ports to scan, use -V to see all the replies
```

port	serv name	flags	ttl	id	win	len
135	epmap	:.S..A...	127	58119	65392	46
139	netbios-ssn	:.S..A...	127	58375	8192	46
1521		:.S..A...	127	18952	65392	46
2030		:.S..A...	127	32008	65392	46
445	microsoft-d	:.S..A...	127	57864	65392	46

```
All replies received. Done.
Not responding ports: (680 ) (681 ) (682 ) (683 ) (684 ) (685 ) (686 ) (687 ) (688 ) (690 ) (771 )
(796 ) (797 ) (798 ) (799 ) (800 ) (807 ) (808 ) (809 ) (810 ) (811 ) (812 ) (813 ) (814 ) (815 )
(1031 ) (1032 ) (1033 ) (1034 ) (1035 ) (1036 ) (1037 ) (1038 ) (1039 ) (1040 ) (1041 ) (1042 ) (
) (1056 ) (1057 ) (1058 ) (1059 ) (1060 ) (1061 ) (1062 ) (1063 ) (1064 ) (1065 ) (1066 ) (1067 )
130 ) (1131 ) (1132 ) (1133 ) (1134 ) (1135 ) (1136 ) (1137 ) (1138 ) (1139 ) (1140 ) (1141 ) (11
) (1155 ) (1156 ) (1157 ) (1158 ) (1159 ) (1160 ) (1161 ) (1312 ) (1313 xtel) (1314 xtelw) (1415 )
28 ) (1429 ) (1430 ) (1431 ) (1432 ) (1433 ms-sql-s) (1434 ms-sql-m) (1435 ) (1436 ) (1437 ) (143
) (1451 ) (1452 ) (1453 ) (1454 ) (1455 ) (1456 ) (1457 ) (1458 ) (1461 ) (1560 ) (1562 ) (1563 ) (
) (1577 ) (1578 ) (1579 ) (1580 ) (1581 ) (1582 ) (1583 ) (1584 ) (1586 ) (1627 ) (1628 ) (1629
751 ) (1752 ) (1753 ) (1754 ) (1755 ) (1756 ) (1757 ) (1758 ) (1759 ) (1760 ) (1761 ) (1762 ) (17
) (1776 ) (1777 ) (1778 ) (1779 ) (1780 ) (1781 ) (1782 ) (1783 ) (1784 ) (1785 ) (1786 ) (1787 )
0 ) (1851 ) (1852 ) (1853 ) (1854 ) (1855 ) (1856 ) (1857 ) (1858 ) (1859 ) (2061 ) (2062 ) (2063
2126 ) (2127 ) (2128 ) (2129 ) (2130 ) (2131 ) (2132 ) (2133 ) (2134 ) (2135 gris) (2136 ) (2137
185 ) (2201 ) (2202 ) (2203 ) (2204 ) (2205 ) (2206 ) (2207 ) (2208 ) (2209 ) (2210 ) (2211 ) (22
) (2275 ) (2285 ) (2286 ) (2288 ) (2292 ) (2294 ) (2295 ) (2297 ) (2299 ) (2301 ) (2302 ) (2307 )
4 ) (2345 ) (2346 ) (2347 ) (2348 ) (2349 ) (2350 ) (2351 ) (2352 ) (2353 ) (2354 ) (2355 ) (2356
2469 ) (2470 ) (2471 ) (2472 ) (2473 ) (2474 ) (2475 ) (2476 ) (2477 ) (2478 ) (2479 ) (2480 ) (2
) (2592 ) (2595 ) (2596 ) (2597 ) (2598 ) (2599 ) (2600 zebrasrv) (2601 zebra) (2602 ripd) (2603
2612 ) (2613 ) (2614 ) (2615 ) (2617 ) (2618 ) (2619 ) (2620 ) (2621 ) (2623 ) (2624 ) (2625 ) (2
) (2787 ) (2788 ) (2789 ) (2790 ) (2791 ) (2792 f5-globalssi) (2793 ) (2794 ) (2795 ) (2796 ) (279
2860 ) (2861 ) (2862 ) (2863 ) (2864 ) (2865 ) (2866 ) (2867 ) (2868 ) (2869 ) (2870 ) (2871 ) (
```

- Untuk melakukan pembuatan paket UDP, ketik `hping3 x.x.x.x --udp --rand-source --data 500` dan tekan Enter.

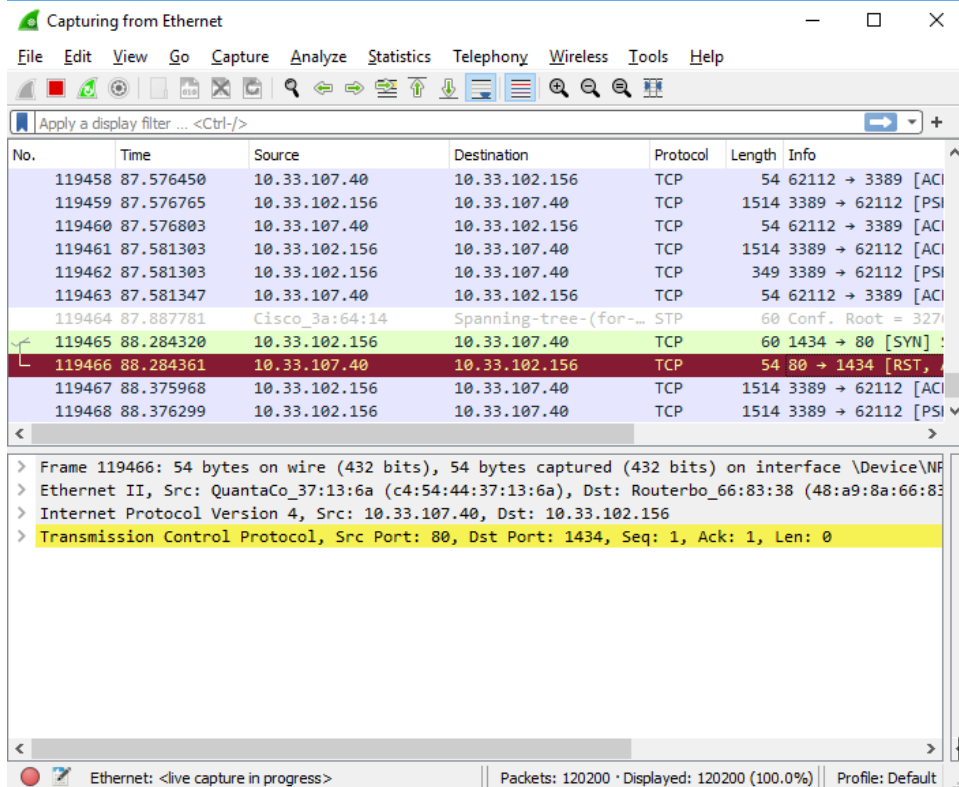
```
(root@kali)-[/home/kali]
# hping3 10.33.107.40 --udp --rand-source --data 500
HPING 10.33.107.40 (eth0 10.33.107.40): udp mode set, 28 headers + 500 data bytes
```

- Beralih ke mesin Windows dan klik paket UDP apa pun untuk melihat detail paket. Di panel detail paket, perluas bagian Data untuk melihat ukuran data paket.


```
(root@kali)~/home/kali
# hping3 -S 10.33.107.40 -p 80 -c 5
HPING 10.33.107.40 (eth0 10.33.107.40): S set, 40 headers + 0 data bytes
len=46 ip=10.33.107.40 ttl=127 DF id=14594 sport=80 flags=RA seq=0 win=0 rtt=15.7 ms
len=46 ip=10.33.107.40 ttl=127 DF id=14901 sport=80 flags=RA seq=1 win=0 rtt=11.7 ms
len=46 ip=10.33.107.40 ttl=127 DF id=14983 sport=80 flags=RA seq=2 win=0 rtt=11.6 ms
len=46 ip=10.33.107.40 ttl=127 DF id=15065 sport=80 flags=RA seq=4 win=0 rtt=11.2 ms

--- 10.33.107.40 hping statistic ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 11.2/12.6/15.7 ms
```

14. Sekarang beralih ke Windows 10 dan amati paket TCP pada Wireshark



15. Beralih ke Kali Linux masuk ke terminal dan ketik `hping3 x.x.x.x --flood` dan tekan Enter.

```
(root@kali)~/home/kali
# hping3 10.33.107.40 --flood
HPING 10.33.107.40 (eth0 10.33.107.40): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

16. Beralih ke Windows 10 dan amati Wireshark, yang menampilkan paket TCP yang membanjiri dari mesin penyerang.

No.	Time	Source	Destination	Protocol	Length	Info
824138	190.270893	10.33.102.156	10.33.107.40	TCP	60	[TCP Previous se
824139	190.270893	10.33.102.156	10.33.107.40	TCP	60	34760 → 0 [<None:
824140	190.270893	10.33.102.156	10.33.107.40	TCP	60	34761 → 0 [<None:
824141	190.270893	10.33.102.156	10.33.107.40	TCP	60	34759 → 0 [<None:
824142	190.270893	10.33.102.156	10.33.107.40	TCP	60	34766 → 0 [<None:
824143	190.270893	10.33.102.156	10.33.107.40	TCP	60	34762 → 0 [<None:
824144	190.270893	10.33.102.156	10.33.107.40	TCP	60	34763 → 0 [<None:
824145	190.270893	10.33.102.156	10.33.107.40	TCP	60	34765 → 0 [<None:
824146	190.270893	10.33.102.156	10.33.107.40	TCP	60	34764 → 0 [<None:
824147	190.270893	10.33.102.156	10.33.107.40	TCP	60	[TCP Previous se
824148	190.270893	10.33.102.156	10.33.107.40	TCP	60	34767 → 0 [<None:

17. Klik dua kali paket TCP pada aliran paket untuk mengamati informasi paket TCP. Aliran Paket TCP menampilkan informasi lengkap paket TCP yang ditransmisikan ke mesin penyerang dan paket yang diterima.

```

> Frame 3171533: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on inte
> Ethernet II, Src: Routerbo_66:83:38 (48:a9:8a:66:83:38), Dst: QuantaCo_37:13:6a
> Internet Protocol Version 4, Src: 104.208.16.89, Dst: 10.33.107.40
  Transmission Control Protocol, Src Port: 443, Dst Port: 62436, Seq: 18811, Ack:
    Source Port: 443
    Destination Port: 62436
    [Stream index: 65293]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 18811 (relative sequence number)
    Sequence Number (raw): 1849384490
    [Next Sequence Number: 18811 (relative sequence number)]
    Acknowledgment Number: 263764 (relative ack number)
    Acknowledgment number (raw): 2602209296
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 2053
    [Calculated window size: 525568]
    [Window size scaling factor: 256]
    Checksum: 0xcc2c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
    [Time since first frame in this TCP stream: 186.366770000 seconds]
    [Time since previous frame in this TCP stream: 0.231074000 seconds]
  > [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 3171529]
    [The RTT to ACK the segment was: 0.231074000 seconds]
    [iRTT: 0.228021000 seconds]
  0000  c4 54 44 37 13 6a 48 a9 8a 66 83 38 08 00 45 00  ·TD7·jH· ·f·8··E·
  No.: 3171533 · Time: 301.724467 · Source: 104.208.16.89 · Destinati... 60 · Info: 443 → 62436 [ACK] Seq=18811 Ack=263764 Win=525568 Len
  [x] Show packet bytes
  Close Help
  
```

18. Berapa banyak paket yang telah dikirim ke mesin target?

No.	Time	Source	Destination	Protocol	Length	Info
3171538	301.878817	10.33.107.42	239.255.255.250	UDP	698	52615 → 3702
3171539	301.894415	fe80::ffc8:eea1:76f...	ff02::c	UDP	718	52616 → 3702
3171540	301.907241	13.107.6.171	10.33.107.40	TLSv1.2	596	Application
3171541	301.907511	13.107.6.171	10.33.107.40	TLSv1.2	92	Application
3171542	301.907530	10.33.107.40	13.107.6.171	TCP	54	49874 → 443
3171543	301.926021	10.33.107.31	239.255.255.250	SSDP	217	M-SEARCH * H
3171544	302.103478	169.254.10.10	169.254.255.255	UDP	86	57621 → 5762
3171545	302.129653	QuantaCo_37:13:d1	Broadcast	ARP	60	Who has 10.3
3171546	302.436071	Cisco_3a:64:14	Spanning-tree-(for-	STP	60	Conf. Root =
3171547	302.937149	10.33.107.31	239.255.255.250	SSDP	217	M-SEARCH * H

RECONNAISSANCE

1. Masuk ke Kali Linux
- 2.

```
(root@kali)-[/home/kali]
# dnsrecon -d www.acme.com
[*] Performing General Enumeration of Domain: www.acme.com
[-] DNSSEC is not configured for www.acme.com
[*] NS dns2.name-services.com 216.40.47.201
[*] NS dns2.name-services.com 2604:4000:0:d:216:40:47:201
[*] NS dns1.name-services.com 64.98.148.137
[*] NS dns1.name-services.com 2604:4000:2800:2000:64:98:148:137
[*] NS dns4.name-services.com 216.40.47.202
[*] NS dns4.name-services.com 2604:4000:0:d:216:40:47:202
[*] NS dns5.name-services.com 64.98.148.139
[*] NS dns5.name-services.com 2604:4000:2800:2000:64:98:148:139
[*] NS dns3.name-services.com 64.98.148.138
[*] NS dns3.name-services.com 2604:4000:2800:2000:64:98:148:138
[-] Could not Resolve MX Records for www.acme.com
[*] CNAME www.acme.com acme.com
[*] A acme.com 23.93.76.124
[*] Enumerating SRV Records
[+] 0 Records Found
```

3. dnsrecon -d www.certifiedhacker.com

```
(root@kali)-[/home/kali]
# dnsrecon -d www.certifiedhacker.com
[*] Performing General Enumeration of Domain: www.certifiedhacker.com
[-] DNSSEC is not configured for www.certifiedhacker.com
[*] NS ns2.bluehost.com 162.159.25.175
[*] NS ns1.bluehost.com 162.159.24.80
[*] MX mail.certifiedhacker.com 162.241.216.11
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[*] TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
```

4. dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt

```
(root@kali)-[/home/kali]
# dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt
[-] Could not resolve NS server provided and server doesn't appear to be an IP: ns_server
[-] Please specify valid name servers.
```

5. dnsrecon -d www.acme.com -t zonewalk


```

(root@kali)~/home/kali
# dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt
[-] Could not resolve NS server provided and server doesn't appear to be an IP: ns_server
[-] Please specify valid name servers.

(root@kali)~/home/kali
# dnsrecon -d www.acme.com -t zonewalk
[*] Performing NSEC Zone Walk for www.acme.com
[*] Getting SOA record for www.acme.com
[-] This zone appears to be misconfigured, no SOA record found.
[*] CNAME www.acme.com acme.com
[*] A acme.com 23.93.76.124
[+] 2 records found

```

6. dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt

```

(root@kali)~/home/kali
# dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt
[-] File /path/to/dict.txt does not exist!

```

7. dnsrecon -d www.acme.com -t axfr

```

(root@kali)~/home/kali
# dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt
[-] File /path/to/dict.txt does not exist!

(root@kali)~/home/kali
# dnsrecon -d www.acme.com -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for www.acme.com name servers
[*] Resolving SOA Record
[*] Resolving NS Records
[*] NS Servers found:
[*] NS dns5.name-services.com 64.98.148.139
[*] NS dns5.name-services.com 2604:4000:2800:2000:64:98:148:139
[*] NS dns2.name-services.com 216.40.47.201
[*] NS dns2.name-services.com 2604:4000:0:d:216:40:47:201
[*] NS dns3.name-services.com 64.98.148.138
[*] NS dns3.name-services.com 2604:4000:2800:2000:64:98:148:138
[*] NS dns1.name-services.com 64.98.148.137
[*] NS dns1.name-services.com 2604:4000:2800:2000:64:98:148:137
[*] NS dns4.name-services.com 216.40.47.202
[*] NS dns4.name-services.com 2604:4000:0:d:216:40:47:202
[*] Removing any duplicate NS server IP Addresses ...
[*] Trying NS server 216.40.47.202
[-] Zone Transfer Failed for 216.40.47.202!
[-] Port 53 TCP is being filtered
[*] Trying NS server 64.98.148.138
[-] Zone Transfer Failed for 64.98.148.138!
[-] Port 53 TCP is being filtered

```

```

[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:138
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:138!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:139
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:139!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 64.98.148.137
[-] Zone Transfer Failed for 64.98.148.137!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:0:d:216:40:47:202
[-] Zone Transfer Failed for 2604:4000:0:d:216:40:47:202!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 216.40.47.201
[-] Zone Transfer Failed for 216.40.47.201!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:0:d:216:40:47:201
[-] Zone Transfer Failed for 2604:4000:0:d:216:40:47:201!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:137
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:137!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 64.98.148.139
[-] Zone Transfer Failed for 64.98.148.139!
[-] Port 53 TCP is being filtered

```

8. `dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com`

```

(root@kali)-[/home/kali]
# dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 208.67.222.200 to 208.67.222.255
[+] PTR dns.umbrella.com 208.67.222.222
[+] PTR dns.opendns.com 208.67.222.222
[+] PTR resolver1.opendns.com 208.67.222.222
[+] PTR resolver3.opendns.com 208.67.222.220
[+] 4 Records Found

```

V. Pembahasan

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

- 1.

VII. Daftar Pustaka

Klopmart. (February 23, 2021). 2 Kegunaan Solder, Komponen Beserta Jenis-Jenisnya. Retrieved August 21, 2022, from <https://www.klopmart.com/article/detail/kegunaan-solder>