LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
PERTEMUAN 8 BAGIAN I
TEKNIK CRAFTING UDP DAN TCP PACKET DENGAN HPING3

DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

TEKNIK CRAFTING UDP DAN TCP PACKET DENGAN HPING3

A. TUJUAN

Dalam pemindaian jaringan, prosedur pertama Anda adalah memindai jaringan target untuk menentukan semua kemungkinan port terbuka, host langsung, dan layanan yang berjalan. Pengetahuan tentang teknik pembuatan paket dapat membantu Anda memindai jaringan di luar firewall atau IDS.

B. DASAR TEORI

Crafting packet UDP dan TCP mengacu pada proses pembuatan dan konfigurasi paket jaringan secara manual dengan mengatur header dan payload sesuai dengan protokol UDP (User Datagram Protocol) dan TCP (Transmission Control Protocol).

UDP dan TCP adalah dua protokol lapisan transport yang digunakan dalam komunikasi jaringan. UDP adalah protokol yang lebih sederhana dan kurang handal, sedangkan TCP adalah protokol yang lebih kompleks dan menjamin pengiriman data yang andal dan terurut.

Dengan crafting packet UDP atau TCP, pengguna dapat membuat paket khusus yang dapat dikirim melalui jaringan untuk berbagai tujuan, seperti pengujian jaringan, debugging, atau penelitian keamanan. Dalam proses crafting packet, pengguna dapat mengatur header paket dengan mengisi bidang seperti alamat sumber dan tujuan, nomor port, dan flag khusus yang terkait dengan protokol yang digunakan (misalnya, flag SYN untuk TCP).

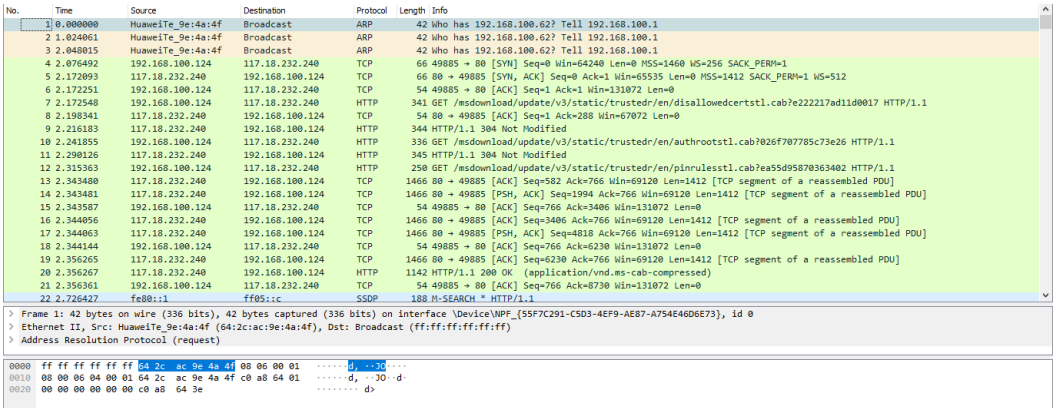
Dengan melakukan crafting packet UDP atau TCP, pengguna memiliki kontrol penuh terhadap isi dan karakteristik paket yang dikirimkan, termasuk data yang dimasukkan ke dalam payload. Hal ini memungkinkan pengguna untuk menguji dan menganalisis respons sistem terhadap jenis paket tertentu, atau memanfaatkan kerentanan atau celah keamanan yang mungkin ada dalam sistem.

C. ALAT DAN BAHAN

a. PC
b. Koneksi internet
c. OS Windows
d. Kali Linux

D. HASIL DAN ANALISIS

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

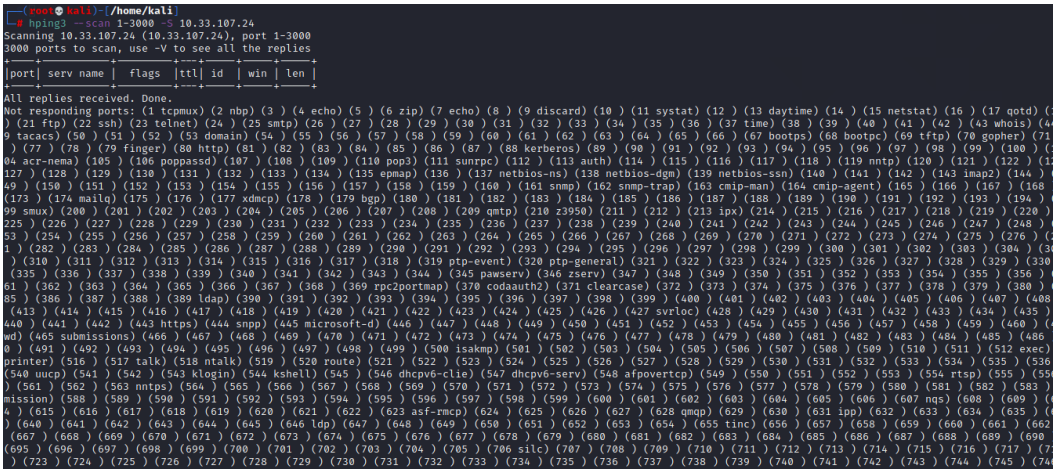


3. Wireshark mulai menangkap lalu lintas pada antarmuka Ethernet.
4. Masuk ke VM kalilinux
5. Buka terminal dan ketik **hping3 -c 3 10.33.107.46** dan tekan Enter

```
┌──(root💀kali)-[/home/kali]
└─# hping3 -c 3 10.33.107.24
HPING 10.33.107.24 (eth0 10.33.107.24): NO FLAGS are set, 40 headers + 0 data bytes

--- 10.33.107.24 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

6. Untuk IP , cek PC windows pada cmd ketik ipconfig ganti IP pada command no 5
7. Perhatikan hasil tangkapan wireshark di Windows, ada berapa paket terkirim?
8. Ketik **hping3 --scan 1-3000 -S x.x.x.x (IP PC windows)** dan ketik Enter.



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

```
┌──(root💀kali)-[/home/kali]
└─# hping3 10.33.107.24 --udp --rand-source --data 500
HPING 10.33.107.24 (eth0 10.33.107.24): udp mode set, 28 headers + 500 data bytes
^C
--- 10.33.107.24 hping statistic ---
858 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

10. 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.

11. Klik tombol **Restart Packet Capturing** dari bilah **menu** dan klik **Continue Without Saving** tombol masuk **Unsaved packets…**
12. Kirim permintaan TCP SYN ke mesin target, ketik **hping3 -S x.x.x.x -p 80 -c 5** dan tekan Enter.

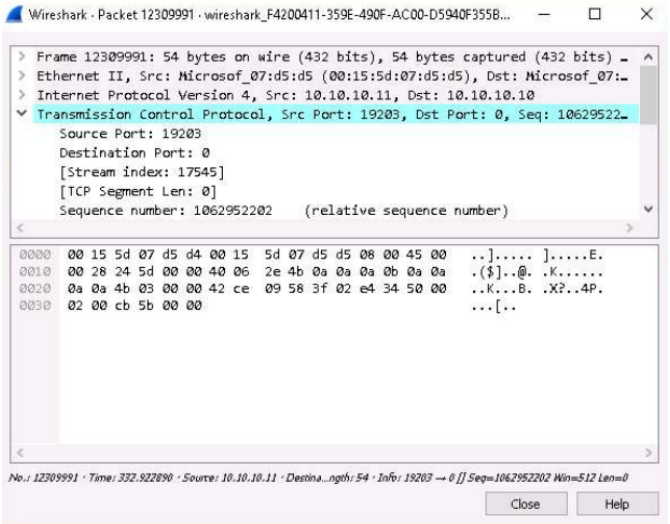
```
┌──(root💀kali)-[/home/kali]
└─# hping3 -S 10.33.107.24 -p 80 -c 5
HPING 10.33.107.24 (eth0 10.33.107.24): S set, 40 headers + 0 data bytes

--- 10.33.107.24 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

13. Sekarang beralih ke Windows 10 dan amati paket TCP pada Wireshark.
14. Beralih ke Kali Linux masuk ke terminal dan ketik **hping3 x.x.x.x --flood** dan tekan Enter

```
┌──(root💀kali)-[/home/kali]
└─# hping3 10.33.107.24 --flood
HPING 10.33.107.24 (eth0 10.33.107.24): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.33.107.24 hping statistic ---
10814802 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

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



PEMBAHASAN:

Command untuk mengirim packet UDP, misal

hping3 -2 -c 10 -p <port> -s <source port> -d <data size> <target IP>

Di sini, **-2** menunjukkan penggunaan protokol UDP, **-c 10** menunjukkan jumlah paket yang akan dikirim (misalnya, 10 paket), **-p**

<port> menunjukkan port tujuan, **-s <source port>** menunjukkan port sumber, dan **-d <data size>** menunjukkan ukuran data yang akan dikirim dalam paket.

Command untuk mengirim packet TCP, contohnya:

hping3 -S -c 10 -p <port> -s <source port> -d <data size> <target IP>

Di sini, **-S** menunjukkan penggunaan flag SYN untuk menginisiasi koneksi TCP, sedangkan opsi lainnya sama dengan pada langkah crafting UDP packet.

Sebelumnya harus dipastikan bahwa HPING3 sudah diinstal. Setelah mengirim command maka, periksa hasil yang diperoleh analisis tanggapan dari target dan melihat apakah ada anomali atau kerentanan yang dapat dieksplorasi lebih lanjut.

E. KESIMPULAN

- UDP adalah protokol yang sederhana tetapi kurang dapat diandalkan, sementara TCP adalah protokol yang kompleks namun dapat menjamin pengiriman data yang dapat diandalkan dan terurut.
- Informasi pada header packet dapat diatur. Seperti, alamat pengirim dan penerima, nomor port, dan juga flag khusus yang berkaitan dengan protokol yang digunakan.
- Teknik crafting packet UDP dan TCP ini memberikan pengguna kendali penuh dalam mengatur isi dan karakteristik paket yang dikirimkan.
- Pengguna dapat mengatur paket sesuai dengan kebutuhan dan memanfaatkannya sesuai keperluan.

LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
PERTEMUAN 8 BAGIAN 2
RECONNAISSANCE

DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA

2023

RECONNAISSANCE

A. TUJUAN

Praktikum ini bertujuan untuk mempelajari dan memahami metode-metode yang digunakan oleh para penyerang dalam tahap awal serangan terhadap sistem atau jaringan komputer. Pemetaan informasi, atau reconnaissance, adalah proses pengumpulan data dan informasi tentang target yang akan diserang. Dalam konteks keamanan informasi, ini berarti mencari tahu tentang sistem, jaringan, dan kelemahan yang mungkin dapat dieksploitasi.

B. DASAR TEORI

Dalam keamanan informasi, reconnaissance adalah proses secara diam-diam menemukan dan mengumpulkan informasi tentang suatu sistem. Ini adalah langkah penting dalam menemukan dan mencuri informasi rahasia. Reconnaissance digunakan dalam pengujian penetrasi dan sering digunakan dalam ethical hacking. Tujuan dari reconnaissance adalah untuk mengumpulkan sebanyak mungkin informasi tentang sistem target. Reconnaissance dapat bersifat aktif atau pasif. Reconnaissance aktif adalah proses mengumpulkan atau mengambil informasi dengan cara di mana sistem target dapat melihat tindakan yang dilakukan. Hal ini sebaiknya dilakukan dengan izin; jika tidak, korban dapat mengambil tindakan yang keras terhadap peretas. Reconnaissance pasif adalah proses mengumpulkan informasi tanpa berinteraksi dengan korban. Ini adalah pendekatan tidak langsung untuk terhubung dengan target. Reconnaissance pasif selalu bergantung pada data yang tersedia secara visual.

Reconnaissance umumnya mengikuti tujuh langkah: mengumpulkan informasi awal, menentukan rentang jaringan, mengidentifikasi mesin yang aktif, menemukan titik akses dan port terbuka, melakukan fingerprinting pada sistem operasi, mengidentifikasi layanan yang berjalan, dan mengambil banner. Salah satu teknik yang paling umum terkait dengan reconnaissance adalah pemindaian port, yang mengirimkan data ke berbagai port TCP dan UDP pada perangkat dan mengevaluasi responnya. Pemindaian port digunakan untuk mengidentifikasi port terbuka dan layanan yang berjalan pada sistem target.

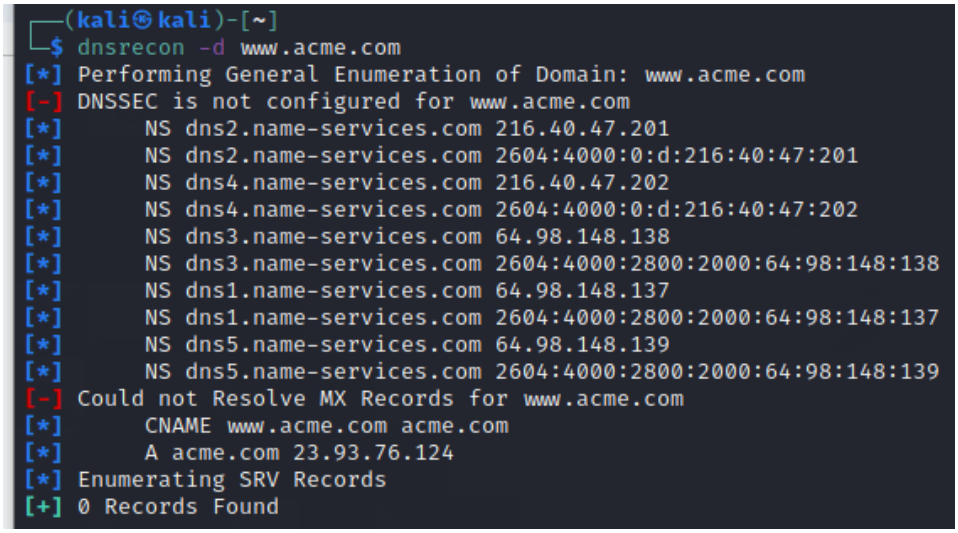
Reconnaissance adalah langkah penting dalam keamanan informasi karena membantu mengidentifikasi kerentanan dalam sistem. Penting juga untuk dicatat bahwa reconnaissance dapat dilakukan secara manual atau menggunakan alat otomatis. Namun, penting untuk memastikan bahwa hasil yang diinginkan dicapai saat melakukan normalisasi dan persiapan log file secara manual. Skrip normalisasi yang buruk dapat mengubah data, secara langsung mempengaruhi pekerjaan analis.

C. ALAT DAN BAHAN

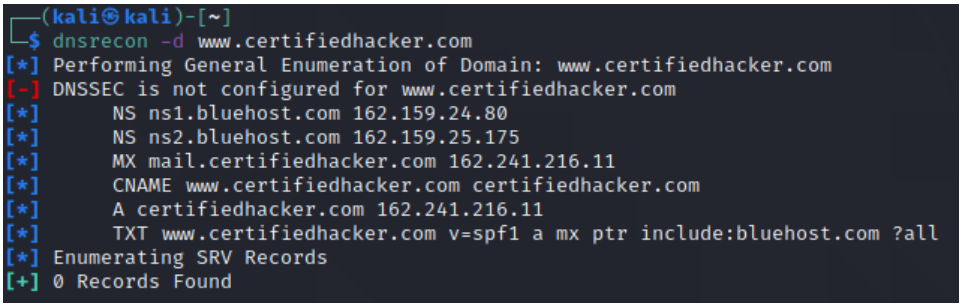
a. PC
b. OS Windows
c. Jaringan internet
d. Kali linux

D. HASIL DAN ANALISIS

1. Ketik **dnsrecon -d www.acme.com** dan ketik Enter.



2. Ketik **dnsrecon -d www.certifiedhacker.com** dan ketik Enter.



3. Ketik **dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt** dan ketik Enter.

4. Ketik **dnsrecon -d www.acme.com -t zonewalk** dan ketik Enter.

```
┌──(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
```

5. Ketik **dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt** dan ketik Enter.

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

6. Ketik **dnsrecon -d www.acme.com -t axfr** dan ketik Enter.

```
┌──(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 dns2.name-services.com 216.40.47.201
[*]     NS dns2.name-services.com 2604:4000:0:d:216:40:47:201
[*]     NS dns4.name-services.com 216.40.47.202
[*]     NS dns4.name-services.com 2604:4000:0:d:216:40:47:202
[*]     NS dns3.name-services.com 64.98.148.138
[*]     NS dns3.name-services.com 2604:4000:2800:2000:64:98:148:138
[*]     NS dns5.name-services.com 64.98.148.139
[*]     NS dns5.name-services.com 2604:4000:2800:2000:64:98:148:139
[*]     NS dns1.name-services.com 64.98.148.137
[*]     NS dns1.name-services.com 2604:4000:2800:2000:64:98:148:137
[*] 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 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
[*]
[*] Trying NS server 64.98.148.137
[-] Zone Transfer Failed for 64.98.148.137!
[-] Port 53 TCP is being filtered
```

```
[*] Trying NS server 2604:4000:2800:2000:64:98:148:137
[-] 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
[*]
[*] 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 64.98.148.138
[-] Zone Transfer Failed for 64.98.148.138!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:139
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:139!
[-] 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 216.40.47.201
[-] Zone Transfer Failed for 216.40.47.201!
[-] Port 53 TCP is being filtered
```

7. Ketik **dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com** dan ketik Enter.

```
┌──(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 resolver1.opendns.com 208.67.222.222
[+] PTR dns.opendns.com 208.67.222.222
[+] PTR dns.umbrella.com 208.67.222.222
[+] PTR resolver3.opendns.com 208.67.222.220
[+] 4 Records Found
```

PEMBAHASAN:

Hasil dari DNSrecon dapat mencakup:

- Server DNS: Informasi tentang server DNS yang bertanggung jawab untuk domain target.
- Catatan DNS: Catatan DNS yang terkait dengan domain target, seperti catatan A (alamat IP), catatan MX (server email), catatan NS (server nama), dll.
- Alamat IP: Daftar alamat IP yang terkait dengan domain target.

- Server email: Informasi tentang server email yang digunakan oleh domain target.

Periksa hasil yang diperoleh dari DNSrecon untuk mengidentifikasi informasi penting. Antara lain:

- Identifikasi server DNS yang digunakan: Mengetahui server DNS yang bertanggung jawab dapat memberikan wawasan tentang infrastruktur jaringan target.
- Menganalisis catatan DNS: Memeriksa catatan DNS seperti catatan A, MX, dan NS dapat memberikan pemahaman tentang alamat IP, server email, dan server nama yang terkait dengan domain target.
- Identifikasi alamat IP terkait: Mengetahui daftar alamat IP yang terkait dengan domain target dapat membantu dalam memahami infrastruktur jaringan dan mengidentifikasi host yang mungkin menjadi sasaran serangan.

E. KESIMPULAN

Reconnaissance merupakan proses yang dilakukan secara diam-diam dalam keamanan informasi untuk mengumpulkan informasi tentang suatu sistem. Tujuannya adalah untuk memperoleh informasi yang diperlukan guna mencapai tujuan tertentu, seperti pencurian data rahasia atau merusak sistem. Reconnaissance dapat dilakukan secara aktif atau pasif. Reconnaissance aktif melibatkan interaksi langsung dengan sistem target, sedangkan reconnaissance pasif dilakukan tanpa berinteraksi secara langsung.

Dalam praktik reconnaissance, terdapat serangkaian langkah yang umumnya dijalankan. Langkah-langkah tersebut meliputi pengumpulan informasi awal, penentuan jangkauan jaringan, identifikasi mesin yang aktif, penemuan titik akses dan port yang terbuka, pengenalan sistem operasi, identifikasi layanan yang sedang berjalan, dan pengambilan informasi banner.

Hasil dari DNSrecon dapat mencakup

- Server DNS
- Catatan DNS
- Alamat IP

Periksa hasil yang diperoleh dari DNSrecon untuk mengidentifikasi informasi penting.

F. DAFTAR PUSTAKA

Blumira. (n.d.). *What is Reconnaissance?* Blumira. Diakses pada May 6, 2023, dari https://www.blumira.com/glossary/reconnaissance/

Fitzpatrick, K. (n.d.). *Lab5- Lab Assignment - a) UDP and TCP packet crafting using Hping In this lab, you will perform*. Studocu. Diakses pada May 6, 2023, dari https://www.studocu.com/en-us/document/kennesaw-state-university/securing-enterprise-infrastructure/lab5-lab-assignment/17422291

Shankdhar, P. (2018). *15 best free packet crafting tools | Infosec Resources*. Infosec Resources. Diakses pada May 6, 2023, dari https://resources.infosecinstitute.com/topic/15-best-free-packet-crafting-tools/

Tech Target Contributor. (n.d.). *What is active reconnaissance? | Definition dari TechTarget*. TechTarget. Diakses pada May 6, 2023, dari https://www.techtarget.com/whatis/definition/active-reconnaissance

Vazquez, M. (n.d.). *How to craft TCP and UDP Packets with HPING3*. Knowledge Base. Diakses pada May 6, 2023, dari https://kb.marcorvazquez.com/topics/ethical-hacking/hacking-tools/hping3/how_to_craft_tcp_and_udp_packets_with_hping3