

LAPORAN PRAKTIKUM

SCANNING NETWORKS AND ENUMERATION



DISUSUN OLEH :

Nama : Diki Candra
Nim : 2022903430010
Kelas : TRKJ 2 B
Jurusan : Teknologi Informasi dan Komputer
Program Studi : Teknologi Rekayasa Komputer Jaringan
Dosen Pengajar : Aswandi, S.Kom, M.Kom.

JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI
PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN
POLITEKNIK NEGERI LHOKSEUMAWE
TAHUN 2022/2023

LEMBARAN PENGESAHAN

Laporan Yang Berjudul : Scanning Networks And Enumeration
Disusun Oleh : Diki Candra
NIM : 2022903430010
Tanggal Praktikum : 18 September 2023
Tanggal Penyerahan : 25 September 2023
Jurusan : Teknologi Informasi & Komputer
Program Studi : Teknologi Rekayasa Komputer Jaringan
Mata Kuliah : Ethical Hacking
Tabel Penilaian :



Mengetahui,
Dosen Pembimbing,

Penyusun,

Aswandi, S.Kom, M.Kom
NIP. 197209242010121001

Diki Candra
NIM. 2022903430010

<p style="text-align: center;">LABORATORIUM: JARINGAN DAN MULTIMEDIA POLITEKNIK NEGERI LHOKSEUMAWE PENGUJIAN: SCANNING NETWORKS AND ENUMERATION</p>
--

I. Capaian Praktikum/Kompetensi

Setelah mengikuti praktikum *Scanning Networks and Enumeration*, diharapkan praktikan dapat:

1. Mahasiswa mampu mengidentifikasi host dan port dalam jaringan
2. Mahasiswa mampu mengidentifikasi informasi sistem operasi, services dan proses yang sedang berjalan dalam jaringan
3. Mahasiswa mampu mengidentifikasi keberadaan perangkat dan arsitektur keamanan pada sistem target
4. Mahasiswa mampu mengidentifikasi kerentanan sistem keamanan jaringan untuk mendukung persyaratan jaringan bisnis skala kecil hingga menengah
5. Mahasiswa diharapkan mampu menggunakan software enumeration dan melakukan koneksi pada target untuk mendapat informasi lebih.

II. Keselamatan Kerja

Praktikum *Scanning Networks and Enumeration* diharapkan mengikuti aturan keselamatan kerja, sebagai berikut:

1. Gunakanlah pakaian praktik!
2. Gunakan alas kaki yang terbuat dari karet untuk menghindari tersengat listrik
3. Bacalah dan pahami petunjuk praktikum pada setiap lembar kegiatan belajar!
4. Hati-hati dalam melakukan praktik!
5. Gunakanlah peralatan praktikum sesuai fungsinya!
6. Setelah selesai praktikum, matikan semua peralatan praktik dengan benar dan rapikan kembali posisi kursi maupun meja komputer.

III. Teori

Scanning Network adalah metode untuk mendapatkan informasi sebanyak-banyaknya serta menentukan target aktif/tidaknya dalam jaringan. Hasil scanning dapat berupa indentifikasi host, informasi port, IP, dan layanan dengan memindai

port dari jaringan komputer target. Scanning Network untuk menyelidiki jaringan target dan juga bisa mendapatkan informasi dari sebuah port dan layanan yang berjalan pada jaringan. Proses ini akan membantu penyerang membuat arsitektur jaringan yang lebih jelas tentang target. Jenis scanning ada 3(tiga), yaitu:

- a. Port Scanning untuk mengetahui service apa yang dijalankan oleh target berdasarkan *well known ports*
- b. Network Scanning untuk mengetahui aktifnya host dan IP Address
- c. Vulnerability Scanning untuk mengetahui sistem operasi apa yang digunakan, versi sistem operasi maupun service pack yang digunakan.

Enumeration adalah suatu proses penggabungan informasi yang telah kita dapat dari proses sebelumnya, sehingga menghasilkan eksploitasi yang dapat digunakan untuk memulai koneksi aktif dengan sistem target. Dengan koneksi aktif ini, permintaan langsung dihasilkan untuk mendapatkan informasi lebih lanjut. Enumerasi untuk mengamati target lebih dekat untuk mendapatkan informasi lebih terperinci. Informasi ini sangat sensitif seperti informasi jaringan, sumber daya jaringan, jalur perutean, SNMP, DNS dan informasi terkait protokol lainnya, informasi pengguna dan grup, dll. Informasi ini membantu mengidentifikasi titik serangan sistem yang diakses secara tidak sah dengan menggunakan informasi yang dikumpulkan, seperti: (1) Informasi perutean; (2) Informasi SNMP; (3) Informasi DNS; (4) Informasi nama mesin; (5) Informasi pengguna; (6) Informasi group; (7) Aplikasi dan banner; (8) Informasi shared jaringan; (9) Sumber daya jaringan.

IV. Alat dan Bahan

Berikut ini merupakan alat dan bahan yang digunakan pada pelaksanaan praktikum *Scanning Networks and Enumeration*, adalah sebagai berikut:

1. VMWare
2. OS Server (Windows, Kali Linux)
3. OS Client (Windows XP/7/8/10)
4. Tools Software (*Hping Commands, Xmas Scanning, Mapper Tool, Nmap, SuperScan Tool dan SoftPerfect Network Scanner Tool*).

V. Prosedur Praktikum

Percobaan 1: Mendapatkan informasi menggunakan *Hping Commands*

Hping Commands merupakan command-line yang berorientasi pada pemrosesan paket TCP/IP. *Hping* dapat menggunakan zenmap tools aplikasi multi platform sebagai interface aplikasi nmap. Nmap (*Network Mapper*) sendiri adalah sebuah aplikasi open source untuk eksplorasi network dan audit keamanannya. *Zenmap* bersifat *multi platform*, bisa berjalan pada berbagai sistem operasi seperti Linux, Windows, Mac, FreeBSD, openBSD dan Sun OS. Dalam mendapatkan informasi menggunakan aplikasi Zenmap, prosedur praktikum sebagai berikut:

- a. Siapkan alat dan bahan
- b. Install software *Zenmap* pada laman web NMAP (<https://nmap.org/zenmap/>)
- c. Jalankan aplikasi *Zenmap* yang telah diinstall di komputernya masing-masing.
- d. Klik target untuk ping memindai jaringan (mis. 192.168.92.0/24).
- e. Pada command masukkan perintah: `nmap -sP 192.168.92.129/24`, untuk melakukan pemindaian ini, IP yang digunakan merupakan ip dari target.
- f. Kemudian klik button *scan*, silakan amati hasilnya.
- g. Untuk memindai target masukkan perintah: `nmap -O 192.168.92.2`.
- h. Kemudian klik button *scan*
- i. Silakan amati hasilnya yang ditampilkan.

Percobaan 2: Mendapatkan informasi menggunakan *Xmas Scanning*

Dalam proses mendapatkan informasi menggunakan *Xmas Scanning Kali Linux* dan *windows server*, prosedur praktikum sebagai berikut:

- a. Jalankan dan *login* sebagai *root* pada *OS Kali Linux*
- b. Jalankan dan *login OS Windows Server* menggunakan IP 192.168.198.138
- c. Kemudian pada windows server lakukan setting firewall diaktifkan
- d. Lalu jalankan *command terminal*, lalu ketikkan `nmap -sX -T4 192.168.198.138` pada terminal, lalu tekan tombol *enter*.
- e. Kemudian pada windows server lakukan setting firewall non-aktifkan
- f. Lalu jalankan *command terminal*, lalu ketikkan `nmap -sX -T4 192.168.198.138` pada terminal, lalu tekan tombol *enter*.

Percobaan 3: Pendapatkan informasi menggunakan *Network Topology Mapper Tool*

Untuk mendapatkan informasi didalam jaringan dapat ditemukan topologi jaringan secara otomatis menggunakan aplikasi *Network Topology Mapper Tool*, prosedur praktikum sebagai berikut:

- a. Install dan jalankan aplikasi *Network Topology Mapper Tool*, bisa download link <https://www.solarwinds.com/network-topology-mapper>
- b. Kemudian buka lembar untuk men-scan, klik tombol button (*New ~ Scan*)
- c. Selanjutnya membuat password berguna untuk mengenkripsi map agar map aman serta map tersebut nantinya dapat diakses saat dipindah ke komputer lain.
- d. Kemudian lakukan *Configure Discovery Settings* terlebih dulu, berikan kredensial yang diperlukan jika diperlukan.
- e. Isikan alamat subnet mask jaringan yang akan di scan, untuk menambahkan alamat subnet dapat dilakukan dengan klik pada Add a New Subnet
- f. Kemudian isi IP Range yang terletak di sebelah tab Subnet.
- g. Jika sudah selesai semua konfigurasi scanning diisi, selanjutnya klik tombol scan, tunggu sampai selesai.
- h. Apabila proses pemindaian selesai, maka akan muncul daftar perangkat yang terdeteksi dimasukkan ke dalam topologi jaringan.

Percobaan 4: Mendapatkan informasi detail (*Services Enumeration*) menggunakan *Nmap*

Dalam mendapatkan informasi lainnya mengenai target tentang services, port dan informasi sistem operasi menggunakan aplikasi *Nmap*, prosedur praktikum sebagai berikut:

- a. Jalankan OS Kali Linux, lalu klik *Command Interface*
- b. Ketikkan perintah "*nmap -sP 192.168.92.0/24*".
- c. Lakukan ketik perintah "*nmap -sU -p untuk IP 192.168.92.2*".
- d. Lakukan perintah yang digunakan untuk melakukan pemindaian Stealthy pada host target 192.168.92.2, ketik "*nmap -sS 192.168.92.2*"
- e. Tampilan hasil dari perintah nmap -sSV -O dengan ip target 192.168.92.2 pada terminal kali linux, ketikkan "*nmap -sSV -O 192.168.92.2*".

Percobaan 5: Mendapatkan informasi (*Enumeration*) menggunakan *SuperScan Tool*

Untuk mendapatkan informasi lebih detail menggunakan aplikasi *SuperScan Tool* untuk *Windows*), prosedur praktikum sebagai berikut:

- a. Install aplikasi *SuperScan Tool* sampai finish, untuk versi windows silakan download link <https://www.hackingtools.in/free-download-superscan/>
- b. Jalankan aplikasi *SuperScan*, buka tab *Enumerasi* windows
- c. Masukkan nama *host*, isikan alamat ip target
- d. Centanglah *enumerasi type* yang diinginkan pada bagian kiri.
- e. Setelah selesai mengkonfigurasi, klik button *enumeration* untuk memulai proses dan tunggu beberapa saat hingga proses scan selesai, hasil scan bisa lihat pada gambar 5.

Percobaan 6: Mendapatkan informasi yang lebih detail (*Enumeration*) menggunakan *SoftPerfect Network Scanner Tool*

Untuk mengumpulkan lebih banyak informasi mengenai target di dalam jaringan menggunakan aplikasi *Metasploit Framework* pada *OS Kali Linux*, prosedur praktikum sebagai berikut:

- a. Siapkan sebuah komputer berbasis windows!
- b. Unduh *SoftPerfect Network Scanner Tool*, lalu install
- c. Jalankan *SoftPerfect Network Scanner Tool*
- d. Isikan range alamat ip (*Ipv4 From.... To.....*), kemudian klik tombol *start scanning*.
- e. Maka akan tampil beberapa alamat ip yang berhasil di scan.
- f. Pemeriksalah device yang berhasil di scan, dengan mengklik kanan lalu pilih *properties*.

VI. Data Percobaan

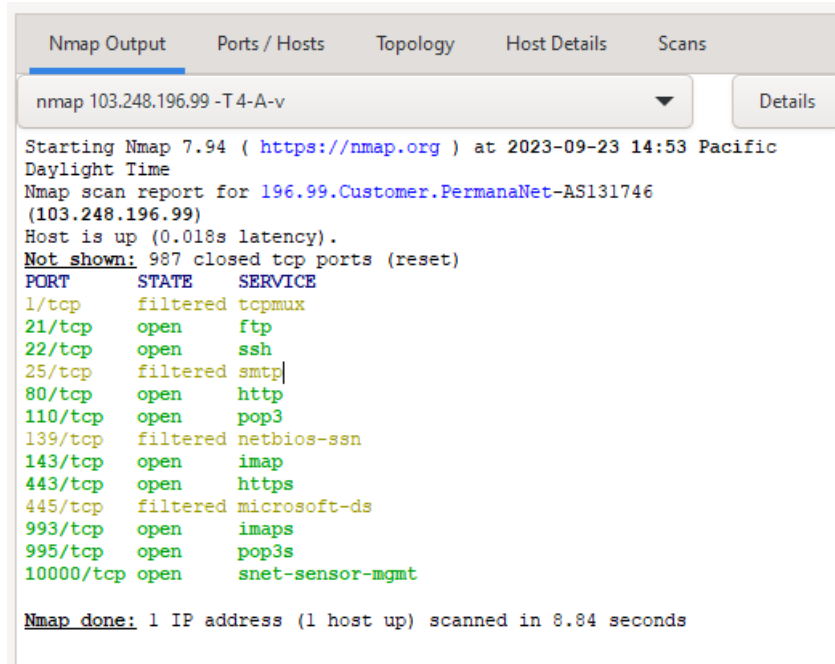
Setelah semua data diperoleh, maka data hasil pengamatan dan pengujian dimasukkan ke dalam tabel, sebagai berikut:

Percobaan 1:

Aplikasi:

Zenmap

Output:



```
nmap 103.248.196.99 -T4-A-v

Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 14:53 Pacific Daylight Time
Nmap scan report for 196.99.Customer.PermanaNet-AS131746 (103.248.196.99)
Host is up (0.018s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE      SERVICE
1/tcp     filtered  tcpmux
21/tcp    open       ftp
22/tcp    open       ssh
25/tcp    filtered  smtp
80/tcp    open       http
110/tcp   open       pop3
139/tcp   filtered  netbios-ssn
143/tcp   open       imap
443/tcp   open       https
445/tcp   filtered  microsoft-ds
993/tcp   open       imaps
995/tcp   open       pop3s
10000/tcp open       snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 8.84 seconds
```

Impact/Indicator:

Dalam percobaan dengan Zenmap (berbasis Nmap), dampaknya adalah pemindaian jaringan untuk mendapatkan informasi tentang perangkat, alamat IP, dan sistem operasi pada target, serta mendukung analisis keamanan. Penggunaan harus etis dan sah sesuai hukum.

Outcomes:

Percobaan ini memberikan manfaat berupa pemahaman jaringan, pemantauan keamanan, dan audit keamanan jaringan. Anda dapat mengidentifikasi host aktif, menguji penetrasi, dan memitigasi kerentanan.

Percobaan 2:

Aplikasi:

Xmas Scanning

Output:

Sebelum Mematikan Firewall

```
(root@kali)-[~]  
# nmap -sX -T4 192.168.100.99  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 15:50 WIB  
Nmap scan report for 192.168.100.99  
Host is up (0.00051s latency).  
All 1000 scanned ports on 192.168.100.99 are in ignored states.  
Not shown: 1000 open|filtered tcp ports (no-response)  
MAC Address: 08:00:27:32:7A:0B (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 36.59 seconds
```

Setelah Mematikan Firewall

```
(root@kali)-[~]  
# nmap -sX -T4 192.168.100.99  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 15:51 WIB  
Nmap scan report for 192.168.100.99  
Host is up (0.00081s latency).  
All 1000 scanned ports on 192.168.100.99 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
MAC Address: 08:00:27:32:7A:0B (Oracle VirtualBox virtual NIC)
```

Impact/Indicator:

Dalam percobaan dengan Xmas Scanning antara Kali Linux dan Windows Server, dampaknya adalah pengujian keamanan Windows Server dan pemahaman tentang kerentanan potensial. Penggunaan harus etis dan sah sesuai hukum.

Outcomes:

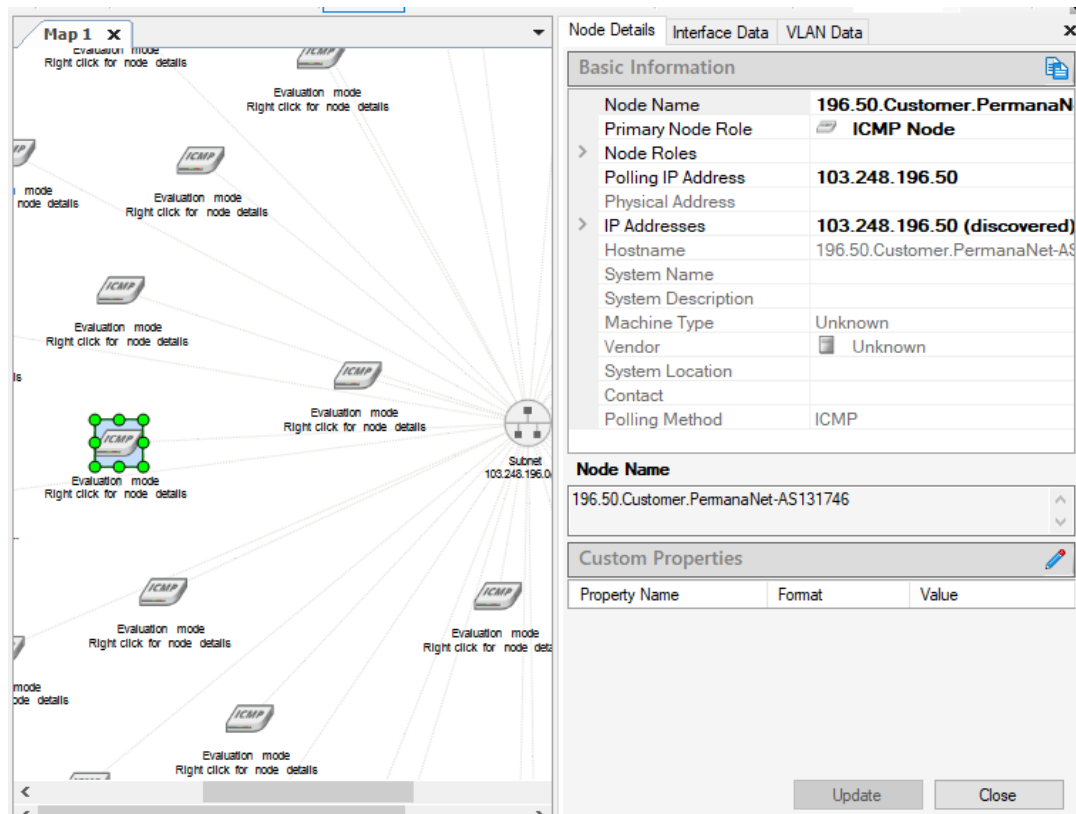
Manfaat dari percobaan menggunakan Xmas Scanning adalah identifikasi kerentanan pada sistem Windows Server, pemahaman firewall, dan analisis keamanan jaringan. Penggunaan harus etis, sah, dan mematuhi hukum yang berlaku.

Percobaan 3:

Aplikasi:

Network Topology Mapper Tool

Output:



Impact/Indicator:

Dalam percobaan dengan Network Topology Mapper Tool, dampaknya adalah pemahaman topologi jaringan, pengelolaan jaringan yang lebih baik, dan pemantauan keamanan. Penggunaan harus etis dan sah sesuai hukum, serta memperhatikan privasi dan hak cipta.

Outcomes:

Manfaat dari percobaan dengan Network Topology Mapper Tool adalah pemahaman jaringan yang lebih baik, manajemen yang efisien, peningkatan keamanan jaringan, dan kemampuan pemulihan bencana yang lebih baik. Ini membantu dalam pemantauan, pemecahan masalah, dan perencanaan jaringan.

Percobaan 4:

Aplikasi:

Nmap

Output:

```
(root@kali)-[~]
# nmap -sU -P 192.168.92.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 17:18 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.16 seconds

(root@kali)-[~]
# nmap -sS 192.168.92.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 17:18 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.24 seconds

(root@kali)-[~]
# nmap -sSV -O 192.168.92.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 17:20 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.46 seconds
```

Impact/Indicator:

Dalam percobaan dengan Nmap, dampaknya adalah pemahaman layanan, port, dan sistem operasi pada target, yang membantu dalam analisis keamanan dan identifikasi kerentanan.

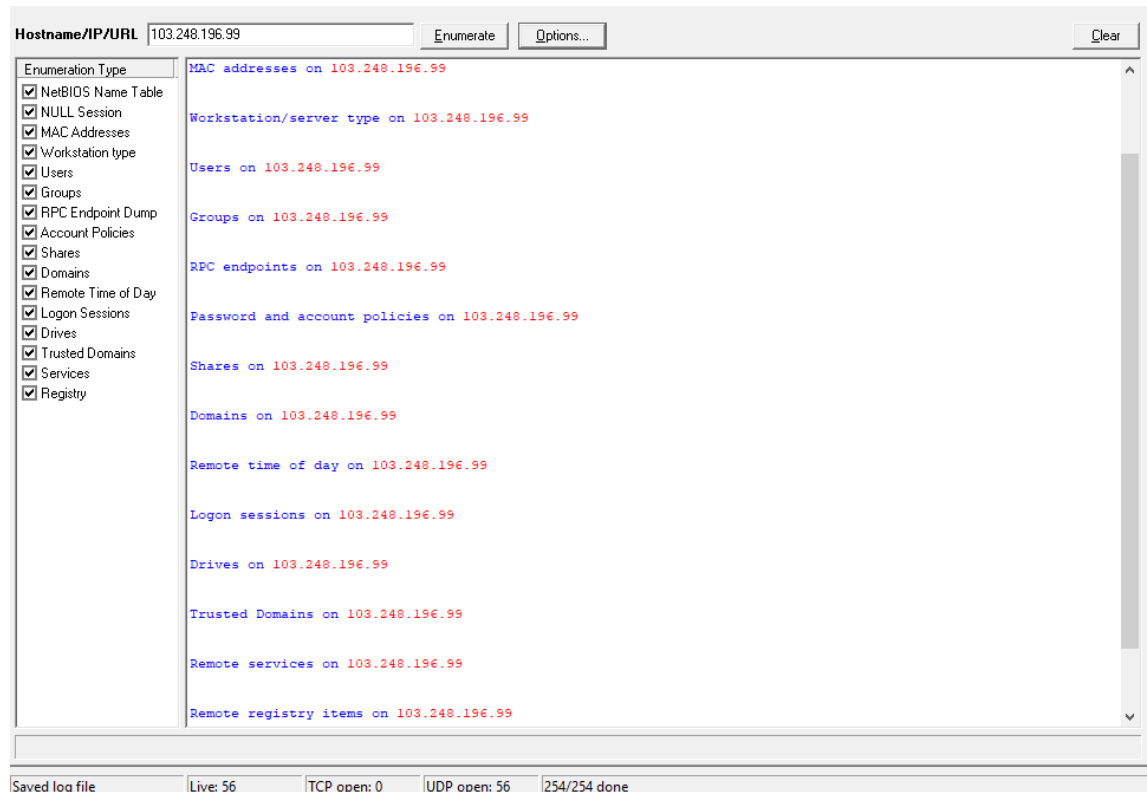
Outcomes:

Manfaat dari percobaan dengan Nmap adalah pemahaman mendalam tentang layanan dan port pada target, identifikasi sistem operasi, pemindaian jaringan untuk identifikasi kerentanan, dan pemecahan masalah. Dengan Nmap, Anda dapat meningkatkan pemahaman, keamanan, dan pemantauan jaringan.

Percobaan 5:

Aplikasi:

Output:



Impact/Indicator:

Dalam percobaan dengan SuperScan Tool, dampaknya adalah pengumpulan informasi detail tentang target, pemahaman jaringan yang lebih baik, dan analisis keamanan yang mendalam.

Outcomes:

Manfaat dari percobaan dengan SuperScan Tool adalah mendapatkan informasi rinci tentang jaringan, mengidentifikasi kerentanan, menganalisis keamanan, dan memantau jaringan.

Percobaan 6:

Aplikasi:

SoftPerfect Network Scanner Tool

Output:

IP address	MAC address	Response Time	Host name
192.168.100.1	AC-75-1D-58-FD-B1	2 ms	1.100.168.192.in-addr.arpa
192.168.100.32	F0-79-E8-1E-9C-D5	22 ms	32.100.168.192.in-addr.arpa
192.168.100.99	08-00-27-32-7A-0B	0 ms	DESKTOP-8QDC8UL
192.168.100.114	EA-20-07-03-08-3D	130 ms	114.100.168.192.in-addr.arpa
192.168.100.167	F4-7B-09-4D-29-07	0 ms	167.100.168.192.in-addr.arpa
192.168.100.198	8C-AA-CE-37-B4-18	350 ms	198.100.168.192.in-addr.arpa
192.168.100.210	08-00-27-F9-CD-B3	1 ms	210.100.168.192.in-addr.arpa

Properties	
Shared Resources	
● IP address	192.168.100.210
● MAC address	08-00-27-F9-CD-B3
● Response Time	1 ms
● Host name	210.100.168.192.in-addr.arpa

Impact/Indicator:

Dalam percobaan dengan SoftPerfect Network Scanner Tool, dampaknya adalah pengumpulan informasi detail tentang perangkat dan layanan dalam jaringan, yang membantu dalam analisis keamanan dan pemahaman jaringan yang lebih baik.

Outcomes:

Manfaat dari percobaan dengan SoftPerfect Network Scanner Tool adalah pengumpulan informasi detail tentang perangkat di dalam jaringan, pemahaman yang lebih baik tentang jaringan, pengelolaan yang efisien, analisis keamanan yang lebih baik.

VII. Analisa dan Kesimpulan

Percobaan "Scanning Networks and Enumeration" melibatkan pemindaian jaringan dan pengumpulan informasi tentang target. Hasil pemindaian memberikan wawasan tentang layanan yang berjalan, port yang terbuka, dan sistem operasi yang digunakan pada komputer target. Penting untuk menjalankan aktivitas ini dengan etis dan sah. Kesimpulannya, pemindaian jaringan dan enumeration membantu meningkatkan pemahaman keamanan dan manajemen jaringan.

VIII. Daftar Pustaka

Kurniawan, Agus. (2012). *Network Forensics – Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta: ANDI

Mitchell, John. (2015), "*Computer and Network Security*", Spring

Saeed, A., Khan, Nouman Ahmed, Yousuf, M. (2018), *CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs*, Vol. 10, United Kingdom, IPSpecialis LTD.