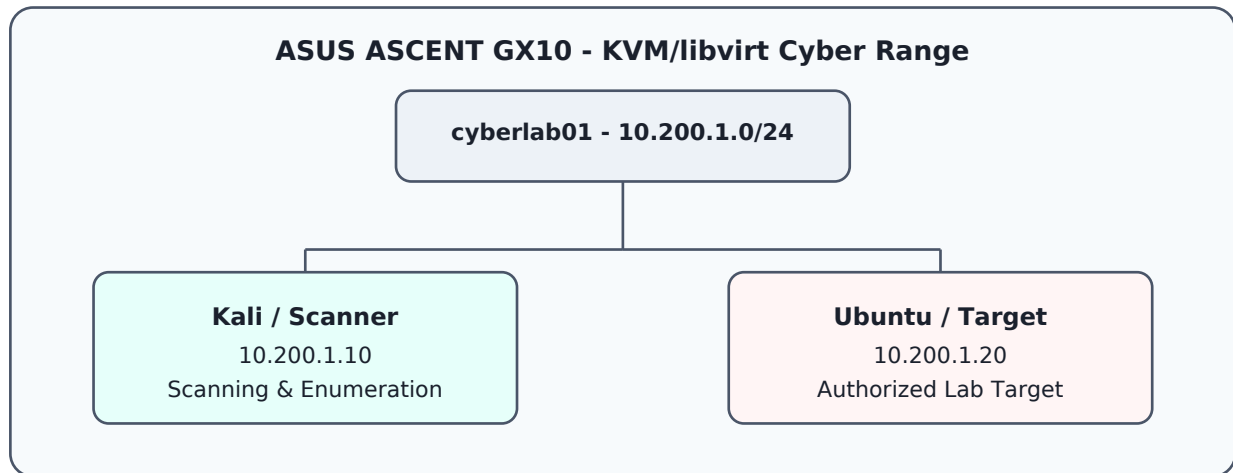


Scanning and Enumeration

Tutorial Praktikum Keamanan Siber pada Cyber Range Asus Ascent GX10



Mata Kuliah: Keamanan Siber (13S4121)

Lingkungan: Kali Linux sebagai scanner/pentester dan Ubuntu sebagai target laboratorium.

Scope utama: 10.200.1.0/24, dengan target 10.200.1.20.

Catatan etika: Seluruh perintah pada modul ini hanya untuk sistem laboratorium yang memiliki izin eksplisit. Jangan memindai jaringan kampus, Internet, atau host di luar scope.

1. Tujuan Pembelajaran

Setelah praktikum, mahasiswa diharapkan mampu:

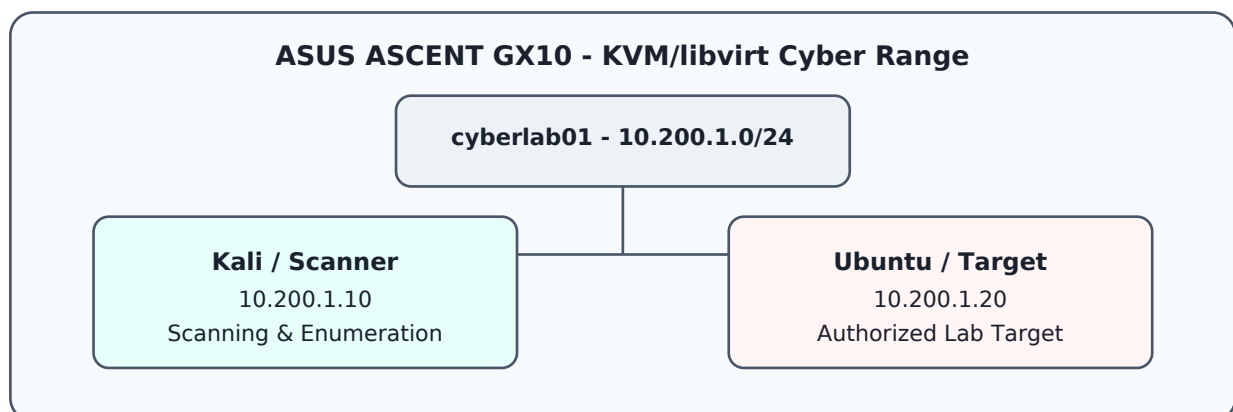
- menjelaskan perbedaan scanning dan enumeration;
- melakukan host discovery pada jaringan laboratorium;
- mengidentifikasi port terbuka, service, dan versi software;
- melakukan enumeration dasar terhadap HTTP dan SSH;
- membandingkan external view dari scanner dengan internal view pada target;
- mengubah hasil observasi menjadi attack-surface table dan rekomendasi hardening.

Scanning menjawab apa yang tersedia; enumeration menjawab apa yang berjalan dan informasi apa yang diekspos oleh service.

Alur Praktikum

Scope -> Network Identification -> Host Discovery
-> Port Scanning -> Service Detection
-> Enumeration -> Evidence
-> Attack Surface Analysis -> Defensive Control

Topologi Laboratorium



2. Persiapan Kali Linux

Pastikan Kali berada pada interface cyberlab dan mempunyai alamat 10.200.1.10/24.

Cek alamat interface:

```
ip -br addr
```

Cek routing:

```
ip route
```

Target yang benar seharusnya dapat dijangkau melalui jaringan 10.200.1.0/24.

Uji konektivitas:

```
ping -c 4 10.200.1.20
```

Catatan: host yang tidak membalas ICMP belum tentu mati. Firewall dapat memblok ping.

3. Network Identification

Identifikasi jaringan sebelum melakukan scanning.

```
ip addr show eth0
```

Jika alamat Kali adalah 10.200.1.10/24, maka subnet laboratorium adalah 10.200.1.0/24.

Mengetahui subnet tidak berarti semua host di luar scope boleh dipindai.

4. Host Discovery

Gunakan Nmap untuk mengetahui apakah target terdeteksi aktif tanpa melakukan port scan penuh.

```
nmap -sn 10.200.1.20
```

Untuk discovery seluruh subnet laboratorium yang memang diizinkan:

```
nmap -sn 10.200.1.0/24
```

5. ARP Discovery pada LAN

Karena Kali dan Ubuntu berada pada LAN yang sama, ARP dapat digunakan untuk menemukan pemetaan IP-MAC.

```
sudo apt update
sudo apt install arp-scan -y
sudo arp-scan --interface=eth0 10.200.1.0/24
```

Target Ubuntu yang digunakan pada lab ini memiliki alamat 10.200.1.20. Cocokkan hasil discovery dengan MAC address yang terlihat.

6. Basic Port Scanning

```
nmap 10.200.1.20
```

Interpretasi state port:

State	Makna
open	Ada service yang menerima koneksi.
closed	Host dapat dijangkau, tetapi tidak ada service pada port tersebut.
filtered	Nmap tidak dapat menentukan karena filtering/firewall.
open filtered	Tidak dapat dibedakan dengan pasti.

Scan port tertentu:

```
nmap -p 22,80 10.200.1.20
```

Scan port 1-1000:

```
nmap -p 1-1000 10.200.1.20
```

Scan seluruh TCP port pada target laboratorium:

```
nmap -p- 10.200.1.20
```

7. Service and Version Enumeration

Port terbuka belum cukup. Kita perlu mengetahui service dan versi yang berjalan.

```
nmap -sV 10.200.1.20
```

Untuk port tertentu:

```
nmap -sV -p 22,80,3000,8080 10.200.1.20
```

Informasi versi berguna untuk inventaris aset, patch management, dan penilaian apakah software sudah tidak didukung.

8. OS Detection

```
sudo nmap -O 10.200.1.20
```

OS detection adalah estimasi berdasarkan fingerprint TCP/IP. Hasil tidak selalu identik dengan OS sebenarnya.

Scan lebih komprehensif setelah mahasiswa memahami opsi dasar:

```
sudo nmap -sV -O 10.200.1.20
```

Alternatif yang lebih agresif pada LAB:

```
sudo nmap -A 10.200.1.20
```

Gunakan opsi agresif hanya setelah scope dan target diverifikasi.

9. Menyimpan Evidence

```
mkdir -p ~/cyberlab/evidence
```

```
nmap -sV 10.200.1.20 -oN ~/cyberlab/evidence/service-scan.txt
```

```
nmap -sV 10.200.1.20 -oA ~/cyberlab/evidence/ubuntu-services
```

Opsi -oA menghasilkan format .nmap, .xml, dan .gnmap. Ini lebih berguna daripada hanya mengandalkan screenshot.

10. HTTP Enumeration

Jika ditemukan port HTTP, mulai dari request sederhana.

```
curl http://10.200.1.20
```

Lihat header saja:

```
curl -I http://10.200.1.20
```

Lihat request dan response lebih detail:

```
curl -v http://10.200.1.20
```

Perhatikan status code, Server header, Content-Type, redirect, cookie, dan informasi lain yang memang diekspos oleh aplikasi.

11. Identifikasi Teknologi Web dengan WhatWeb

```
sudo apt install whatweb -y
whatweb http://10.200.1.20
whatweb http://10.200.1.20:8080
whatweb http://10.200.1.20:3000
```

12. Nikto untuk Web Server Assessment

```
sudo apt install nikto -y
nikto -h http://10.200.1.20
```

Temuan automated scanner harus diverifikasi. Scanner finding tidak sama dengan confirmed vulnerability.

13. Directory Enumeration

```
sudo apt install gobuster -y
```

```
gobuster dir -u http://10.200.1.20 -w /usr/share/wordlists/dirb/common.txt
```

Tujuannya adalah mengidentifikasi resource yang memang diekspos oleh server dalam ruang lingkup laboratorium.

14. Banner Grabbing dengan Netcat

```
nc -nv 10.200.1.20 80
```

Setelah terkoneksi, ketik:

```
HEAD / HTTP/1.1  
Host: 10.200.1.20
```

Tekan Enter dua kali. Response dapat menunjukkan status HTTP dan server banner.

15. SSH Enumeration

Jika port 22 terbuka, lakukan enumeration pasif terlebih dahulu - bukan brute force.

```
nmap -sV -p 22 10.200.1.20
```

```
nmap --script ssh-hostkey -p 22 10.200.1.20
```

```
nmap --script ssh2-enum-algos -p 22 10.200.1.20
```

Mahasiswa dapat mencatat versi SSH, host key, dan algoritma kriptografi yang ditawarkan.

16. HTTP Enumeration dengan Nmap NSE

```
nmap --script http-title -p 80 10.200.1.20
```

```
nmap --script http-headers -p 80 10.200.1.20
```

```
nmap -sV -p 80,3000,8080 --script http-title,http-headers 10.200.1.20
```

17. UDP Scanning

UDP tidak menggunakan three-way handshake seperti TCP. Karena itu hasil scan sering lebih lambat dan dapat berupa open|filtered.

```
sudo nmap -sU -p 53,67,68,123,161 10.200.1.20
```

18. Perspektif Defender: Melihat Scan dari Target

Saat Kali melakukan scanning, buka terminal pada Ubuntu target.

```
sudo tcpdump -ni any host 10.200.1.10
```

Kemudian ulangi dari Kali:

```
nmap -sV 10.200.1.20
```

Mahasiswa dapat mengamati SYN, SYN/ACK, dan RST sebagai bukti bahwa scanning meninggalkan telemetry.

Kali / Scanner	Ubuntu / Target
nmap	----- SYN -----> tcpdump
	<----- SYN/ACK -----
	----- RST ----->

19. External View vs Internal View

Pada Kali:

```
nmap -sV 10.200.1.20
```

Pada Ubuntu:

```
sudo ss -ltnp
```

Contoh: service yang hanya listen pada 127.0.0.1 mungkin tidak terlihat dari Kali.

Listening service tidak selalu berarti externally reachable service.

20. Dari Enumeration ke Attack Surface

Mahasiswa menyusun tabel attack surface berdasarkan evidence.

IP	Port	Protocol	Service	Versi	Exposure
10.200.1.20	22	TCP	SSH	hasil scan	Remote administration
10.200.1.20	80	TCP	HTTP	hasil scan	Web service
10.200.1.20	3000	TCP	HTTP/App	hasil scan	Web application
10.200.1.20	8080	TCP	HTTP/App	hasil scan	Web application

- Apakah service tersebut memang diperlukan?
- Apakah service seharusnya exposed ke jaringan?
- Apakah versi software masih didukung dan sudah dipatch?
- Apakah authentication dan authorization memadai?
- Apakah logging dan monitoring aktif?

21. Skenario Praktikum Lengkap

```
STEP 1  Verify scope          -> 10.200.1.20
STEP 2  Host discovery        -> nmap -sn
STEP 3  Port discovery        -> nmap
STEP 4  Service enumeration   -> nmap -sV
STEP 5  OS estimation         -> nmap -O
STEP 6  Protocol enumeration  -> curl / WhatWeb / NSE
STEP 7  Defender observation  -> ss / tcpdump
STEP 8  Attack-surface table
STEP 9  Recommend controls
STEP 10 Re-test after hardening
```

22. Quick Reference Perintah

Tujuan	Perintah
Cek interface	<code>ip -br addr</code>
Cek route	<code>ip route</code>
Test konektivitas	<code>ping -c 4 10.200.1.20</code>
Host discovery	<code>nmap -sn 10.200.1.20</code>
Scan umum	<code>nmap 10.200.1.20</code>
Semua TCP port	<code>nmap -p- 10.200.1.20</code>
Service/version	<code>nmap -sV 10.200.1.20</code>
OS detection	<code>sudo nmap -O 10.200.1.20</code>
HTTP header	<code>curl -I http://10.200.1.20</code>
HTTP detail	<code>curl -v http://10.200.1.20</code>
Web technology	<code>whatweb http://10.200.1.20</code>
Banner grabbing	<code>nc -nv 10.200.1.20 80</code>
Simpan Nmap	<code>nmap -sV -oA hasil 10.200.1.20</code>

23. Deliverable Mahasiswa

- identitas target dan scope;
- bukti host discovery;
- daftar port terbuka;
- identifikasi service dan version;
- hasil enumeration HTTP dan/atau SSH;
- perbandingan hasil Nmap dengan ss -ltnp pada target;
- attack-surface table;
- minimal tiga rekomendasi hardening yang dapat diuji;
- evidence dalam bentuk file hasil scan, bukan hanya screenshot.

Kesimpulan

Scanning dan enumeration bukan tujuan akhir. Keduanya adalah proses mengubah observasi jaringan menjadi informasi yang dapat digunakan untuk memahami attack surface, menilai risiko, memilih defensive control, dan melakukan re-test.

Discovery -> Scanning -> Enumeration
-> Attack Surface -> Risk
-> Defensive Control -> Re-test

Stop condition: hentikan kegiatan jika target salah, scope tidak jelas, service kritis terdampak, atau terjadi efek yang tidak diharapkan.