Pemindaian Keamanan Host Windows 10 dengan NMAP

1. Pendahuluan

Pemindaian keamanan dilakukan terhadap host Windows 10 (IP: 192.168.18.53) menggunakan NMAP pada Kali Linux (IP: 192.168.18.100). Tujuan utamanya adalah mengidentifikasi port terbuka, layanan aktif, dan potensi kerentanan.

2. Metodologi Pemindaian

Langkah	Perintah NMAP	Parameter Kunci
Host Discovery	ping 192.168.18.53	ICMP connectivity
OS Detection	nmap -O -Pn	Skip host discovery
Service Version	nmap -sV -sS -p 1-1000	SYN scan + version
SMB Vulnerability	nmap --script smb-vuln* -p 445	SMB-specific checks
UDP Scanning	nmap -sU -p 53,161,137	Key UDP ports
Vulnerability Scan	nmap --script vuln	General NSE scripts

3. Hasil Pemindaian

A. Host Discovery & OS Detection

- Konektivitas:

  64 bytes from 192.168.18.53: icmp_seq=1 ttl=128 time=0.711 ms

- Deteksi OS:
  - Sistem operasi terdeteksi: Windows 10/11/Server 2019 (akurasi 97%)
  - Alamat MAC: XX:XX:XX:XX:XX:XX

B. Port dan Layanan Terbuka

Tabel Port TCP Aktif:

Port	Layanan	Versi Layanan	Status
80	HTTP	Apache 2.4.54 (Win64)	Open
135	MSRPC	Microsoft Windows RPC	Open
139	NETBIOS-SSN	Microsoft Windows netbios-ssn	Open
443	HTTPS	Apache 2.4.54 (OpenSSL/1.1.1p)	Open
445	MICROSOFT-DS	-	Open
3306	MySQL	MariaDB ≤ 10.3.23 (unauthorized)	Open

Temuan UDP:

- Port 137/UDP (netbios-ns): Terbuka
- Port 53/UDP dan 161/UDP: Open|Filtered

C. Hasil Pemindaian Kerentanan

- SMB (Port 445):

  |_smb-vuln-ms10-061: Could not negotiate a connection

  |_smb-vuln-ms10-054: false

  - Tidak terdeteksi kerentanan MS17-010 (EternalBlue)
  - Gagal negosiasi koneksi untuk beberapa pemeriksaan
- Pemindaian Umum Kerentanan:

  | broadcast-avahi-dos: Hosts are all up (not vulnerable)

- Tidak ditemukan kerentanan kritis

4. Analisis Risiko

A. Layanan Berisiko Tinggi

1. Port 445 (SMB):
    - Meski tidak terdeteksi MS17-010, versi SMB yang digunakan berpotensi rentan jika tidak di-patch
    - Rekomendasi:
        - Nonaktifkan SMBv1 melalui PowerShell:

          Set-SmbServerConfiguration -EnableSMB1Protocol $false
            - Terapkan patch keamanan terbaru dari Microsoft
2. Port 3306 (MySQL):
    - Versi MariaDB ≤ 10.3.23 memiliki kerentanan dikenal (CVE-2021-27928)
    - Status "unauthorized" mengindikasikan konfigurasi tidak aman
    - Rekomendasi:
        - Upgrade ke versi terbaru
        - Terapkan autentikasi kuat
3. Port 80/443 (HTTP/HTTPS):
    - Apache 2.4.54 rentan terhadap CVE-2022-31813 (HTTP Smuggling)
    - Solusi: Upgrade ke Apache ≥ 2.4.56

B. Potensi Serangan

- NETBIOS (Port 137/139): Dapat dimanfaatkan untuk enumerasi sistem
- MySQL (Port 3306): Target brute-force atau SQL injection jika terpapar eksternal

5. Kesimpulan dan Rekomendasi

Temuan Utama

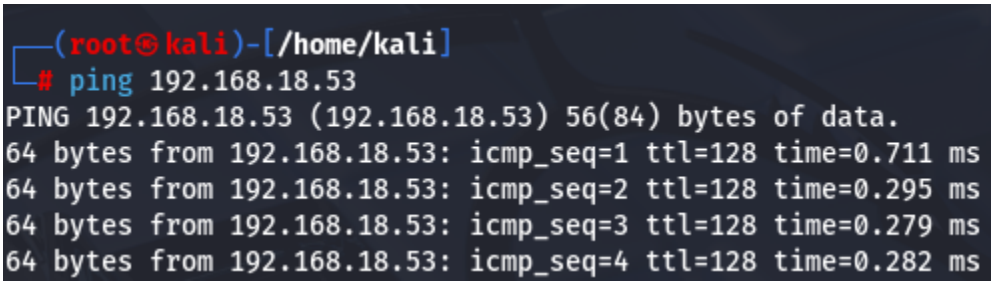
- 6 port TCP terbuka dengan 3 layanan berisiko (SMB, MySQL, Apache)
- 1 port UDP terbuka (NETBIOS)

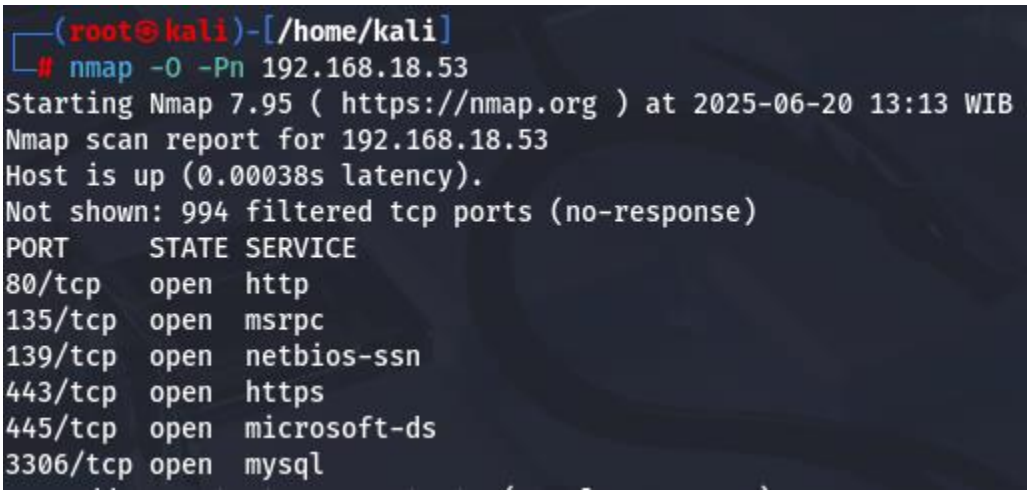
- Tidak terdeteksi kerentanan kritis, tapi konfigurasi layanan berpotensi rentan

Rekomendasi Keamanan

Prioritas	Langkah Mitigasi	Target
Tinggi	Patch SMB dan nonaktifkan SMBv1	Port 445
Tinggi	Upgrade Apache ke versi 2.4.56+	Port 80/443
Sedang	Upgrade MariaDB dan audit akses	Port 3306
Rendah	Batasi akses NETBIOS ke internal	Port 137/139

Lampiran





```
MAC Address:
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsof
t:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (97%), Microsoft Windows 10 19
03 - 21H1 (97%), Microsoft Windows 11 (94%), Microsoft Windows 10 1909 (91%), M
icrosoft Windows 10 1909 - 2004 (91%), Windows Server 2019 (91%), Microsoft Win
dows 10 1809 (91%), Microsoft Windows 10 20H2 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.46 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sS -p 1-1000 192.168.18.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 15:11 WIB
Nmap scan report for 192.168.18.53
Host is up (0.00033s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
80/tcp  open  http         Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/7.4.33)
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp open  ssl/http     Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/7.4.33)
445/tcp open  microsoft-ds?
MAC Address:
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -p 53,161,137 192.168.18.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 15:14 WIB
Nmap scan report for 192.168.18.53
Host is up (0.00040s latency).

PORT    STATE         SERVICE
53/udp  open|filtered domain
137/udp open          netbios-ns
161/udp open|filtered snmp
MAC Address: [redacted]

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.18.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 15:17 WIB
Nmap scan report for 192.168.18.53
Host is up (0.00041s latency).
MAC Address: [redacted]
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O 192.168.18.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 15:18 WIB
Nmap scan report for 192.168.18.53
Host is up (0.00034s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/7.4.33
)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/7.4.33
)
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MariaDB 10.3.23 or earlier (unauthorized)
```

```
MAC Address: 4C:49:6C:53:4A:4E (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open
 and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:wi
ndows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (97%), Microsoft Windows 10 1903 -
 21H1 (97%), Microsoft Windows 11 (94%), Microsoft Windows 10 1909 (91%), Microsoft
 Windows 10 1909 - 2004 (91%), Windows Server 2019 (91%), Microsoft Windows 10 1809
 (91%), Microsoft Windows 10 20H2 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.53 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script vuln 192.168.18.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 15:20 WIB
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -oN hasil_scan.txt 192.168.18.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 15:25 WIB
Nmap scan report for 192.168.18.53
Host is up (0.00038s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 4C:49:6C:53:4A:4E (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```