

Case 3

Datum: 2025-06-01

Grupp - 42

1. Tjänsteidentifiering i nätverket 193.10.236.0/24

Under skanningen av nätverket identifierades följande aktiva servrar och deras tjänster:

Server grp60-serv1.grp60.lab.hv.se (IP: 193.10.236.246)

- HTTP-server på port 80
- HTTPS-server på port 443
- Cisco-protokoll för telefonsystem på port 2000
- SIP-protokoll för röstsamtal på port 5060
- XMPP-meddelandetjänst på port 8010

Server grp60-serv2.grp60.lab.hv.se (IP: 193.10.236.247)

- Samma tjänstekonfiguration som server 1
- Identiska öppna portar och protokoll

Server grp61-serv1.grp61.lab.hv.se (IP: 193.10.236.248)

- Även denna server har samma tjänsteuppsättning
- Alla fem tjänster är aktiva och tillgängliga

2. Operativsystemsidentifiering med Nmap

Teknisk bakgrund

Nmap innehåller en avancerad funktion för operativsystemsidentifiering som kallas OS-fingerprinting. Denna teknik aktiveras genom kommandoflaggan `-O` och fungerar genom att analysera nätverkssvar.

Processen innebär att Nmap sänder ut specialkonstruerade nätverkspaket till målsystemet. När svaren kommer tillbaka analyseras olika parametrar som TCP-sekvensnummer, paketens timing och felmeddelanden. Dessa data jämförs sedan mot Nmaps omfattande databas med operativsystemssignaturer.

Praktiska resultat

När OS-skanningen genomfördes mot våra målsystem erhöles följande information:

För IP-adress 193.10.236.131 visade analysen att systemet med 87% sannolikhet kör Linux med kernel version 3.X eller 2.6.X. De mer specifika gissningarna pekade mot Linux 3.2-3.8 (89% säkerhet) eller Linux 2.6.32-2.6.39 (84% säkerhet).

```
(kali@kali)-[~]
$ nmap -sT 193.10.236.99-250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 18:38 CEST
Nmap scan report for 193.10.236.102
Host is up (0.0027s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 193.10.236.130
Host is up (0.00085s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 193.10.236.131
Host is up (0.000058s latency).
All 1000 scanned ports on 193.10.236.131 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 152 IP addresses (3 hosts up) scanned in 24.04 seconds
```

```
(kali@kali)-[~]
$ sudo nmap -sS 193.10.236.99-250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 18:39 CEST
Nmap scan report for 193.10.236.102
Host is up (0.031s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: F8:39:18:B7:07:C0 (Unknown)

Nmap scan report for 193.10.236.130
Host is up (0.00093s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 48:21:0B:5F:40:A5 (Pegatron)

Nmap scan report for 193.10.236.131
Host is up (0.000060s latency).
All 1000 scanned ports on 193.10.236.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 152 IP addresses (3 hosts up) scanned in 32.67 seconds
```

3. Säkerhetsbedömning av servrarna

Ur säkerhetssynpunkt uppvisar alla tre servrar identiska risknivåer. Eftersom de har exakt samma konfiguration med identiska öppna portar och tjänster, finns inga påtagliga skillnader i säkerhetsprofilen mellan dem.

För en mer grundlig säkerhetsbedömning skulle man behöva genomföra djupare analyser, inklusive sårbarhetsscanning av de specifika tjänsterna och granskning av systemkonfigurationerna.

4. Nmaps huvudsakliga användningsområden

Nätverksupptäckt

Nmap excellerar inom nätverkskartläggning genom att identifiera aktiva enheter. Verktøget använder olika metoder som ICMP-ping och TCP SYN-paket för att upptäcka vilka system som är online inom ett nätverksområde.

Portscanning och tjänsteanalys

En av Nmaps kärnfunktioner är att kartlägga öppna portar på målsystem. Verktøget går dock längre än grundläggande portscanning - det kan identifiera specifika tjänster och till och med versionsnummer för mjukvaran som lyssnar på portarna.

Operativsystemsanalys

Genom avancerad fingerprinting-teknik kan Nmap med hög precision bestämma vilket operativsystem som körs på fjärrsystem, vilket är värdefullt för både säkerhetsbedömningar och systemadministration.

Skriptbaserad utvidgning

Nmap Scripting Engine (NSE) erbjuder kraftfulla möjligheter för automatiserad testning. Skripten kan utföra allt från sårbarhetsscanning till lösenordsattacker och nätverkskonfigurationsanalys.

Brandväggtestning

Verktøget är effektivt för att utvärdera brandväggsregler och säkerhetskfigurationer genom att testa hur olika typer av nätverkstrafik hanteras av säkerhetssystem.

5. Mest värdefulla funktionen

OS-fingerprinting framstår som den mest praktiskt användbara funktionen i Nmap. Genom kommandot `nmap -O [IP-adress]` erhålls detaljerad information om målsystemets operativsystem.

Tekniken bygger på analys av nätverksprotokollbeteenden där Nmap sänder specialdesignade testpaket och utvärderar responserna. Parametrar som TCP-sekvensnummer, Round Trip Time (RTT) och Time To Live (TTL)-värden analyseras för att skapa en unik signatur för varje operativsystem.

Denna kapacitet är särskilt värdefull inom penetrationstestning och säkerhetsrevidering, eftersom olika operativsystem har specifika sårbarheter och säkerhetsegenskaper som påverkar teststrategin.

6. Mest utmanande funktionen

Den största utmaningen uppstod vid kombination av flera kommandoflaggor, specifikt när vi försökte integrera nmap -sS -p 21,23,53,80 -O -v 193.10.236.XX med additional parametrar.

Särskilda svårigheter uppstod med flaggan -IR (Random IP Scanning) och hur denna ska implementeras tillsammans med andra skanningsparametrar. Dokumentationen gav otillräcklig vägledning om hur slumpmässig IP-scanning interagerar med specifikt angivna målsystem.

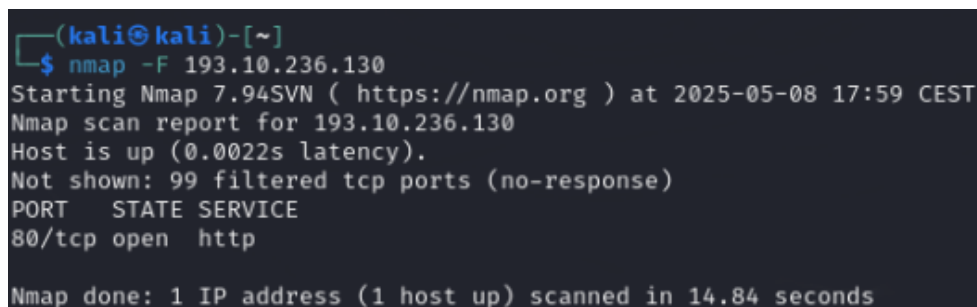
Den praktiska nyttan av -IR i laborationsmiljön var också svår att förstå, eftersom denna funktion går emot det vanliga arbetssättet där man specificerar exakta målsystem för scanning.

7. Fördjupad funktionsanalys: IP-protokollscanning

För att utforska Nmaps kapaciteter djupare undersöktes IP Protocol Scanning med kommandot nmap -sO [IP-adress].

Teknisk funktionalitet

Till skillnad från traditionell portscanning analyserar IP-protokollscanning vilka nätverksprotokoll som stöds av målsystemet på IP-lagret. Detta ger insikt i systemets nätverkskapaciteter på en mer fundamental nivå.



```
(kali@kali)-[~]
$ nmap -F 193.10.236.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 17:59 CEST
Nmap scan report for 193.10.236.130
Host is up (0.0022s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
```

Praktiska resultat

Testet genomfördes mot IP-adress 193.10.236.130

Skanningen identifierade stöd för tre huvudprotokoll:

- **ICMP** (Internet Control Message Protocol) - möjliggör nätverksdiagnostik och felmeddelanden
- **TCP** (Transmission Control Protocol) - standard för pålitlig dataöverföring
- **IGMP** (Internet Group Management Protocol) - hanterar multicast-gruppmedlemskap

Resultatet visar att målsystemet har en komplett nätverkskonfiguration med stöd för både standardkommunikation (TCP), nätverksdiagnostik (ICMP) och gruppkommunikation (IGMP).

