Task 1

Passive information gathering for **Company: ServiceNow**
Founding with Search Engine:
Corporate Structure:
ServiceNow is a cloud computing company that provides a platform-as-a-service (PaaS) focused on IT service management and various enterprise operations. Its Chairman and CEO is Bill McDermott, with other key executives including Gina Mastantuono (CFO) and Chris Bedi (Interim Chief Product Officer). The founder, Fred Luddy, remains a board member. The company operates globally, with four primary subsidiaries: ServiceNow Americas, ServiceNow Asia Pacific, ServiceNow EMEA, and ServiceNow Technology.
Resources:
https://pitchbook.com/profiles/company/12239-02#overview
https://en.wikipedia.org/wiki/ServiceNow
https://www.theofficialboard.com/org-chart/servicenow

Social Media Presence:
ServiceNow maintains an active presence on platforms like LinkedIn and Twitter, where They engage with their audience by sharing updates about new product features, partnerships, and corporate achievements.
Linkedin: https://www.linkedin.com/company/servicenow/
Twitter: https://x.com/ServiceNow
Instagram: https://www.instagram.com/servicenow/?hl=en

Product and Service Offerings:
ServiceNow offers a variety of solutions targeting IT operations, employee workflows, and customer service management.The company's recent focus has shifted towards incorporating AI and machine learning to further streamline enterprise operations.
Resources:
https://www.theofficialboard.com/org-chart/servicenow
https://www.servicenow.com/company.html

Privacy and Compliance:
ServiceNow adheres to stringent privacy regulations across its operating regions. The company follows the General Data Protection Regulation (GDPR) in the European Union, ensuring that personal data is processed lawfully, and securely. ServiceNow also complies with the California Consumer Privacy Act (CCPA)
Furthermore, ServiceNow has incorporated advanced security measures such as encryption at rest and in transit, multifactor authentication, and role-based access control, ensuring that sensitive data is protected. These efforts are certified through global security standards, including ISO 27001 and SOC 2 compliance.
Resources:

https://docs.servicenow.com/bundle/vancouver-governance-risk-compliance/page/product/grc-privacy-management/concept/explore-privacy-management.html

Founding with Censys

https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=servicenow.com
Multiple IP addresses are associated with the domain servicenow.com. The spread of these IPs indicates that ServiceNow uses various data centers and services globally, such as the US, UK, India and Ireland.
The company is serving web traffic securely using HTTPS since we can see the common ports such as 80(HTTP) and 443 (HTTPS) are open.

Founding with Spiderfoot:

I used SpiderFoot to gather a variety of information related to ServiceNow, including Account on External Sites, Affiliate IP Addresses, Affiliate Domains, and Co-Hosted Sites. Each category provided valuable insights that helped me better understand the target's digital footprint.
For example,
Account on External Sites revealed user profiles and external affiliations connected to ServiceNow, potentially pointing to employees or affiliates.
The Affiliate IP Addresses and Domains helped map out the extended network of ServiceNow-related services, identifying potential infrastructure and partnerships.
Co-Hosted Sites indicated shared hosting environments, offering insights into external services that may be linked to ServiceNow's infrastructure.
These findings can help us to piece together a broader picture of ServiceNow's online presence and digital ecosystem, providing a strong foundation for further analysis.

SN RUNNING

Summary | Correlations | Browse | Graph | Scan Settings | Log

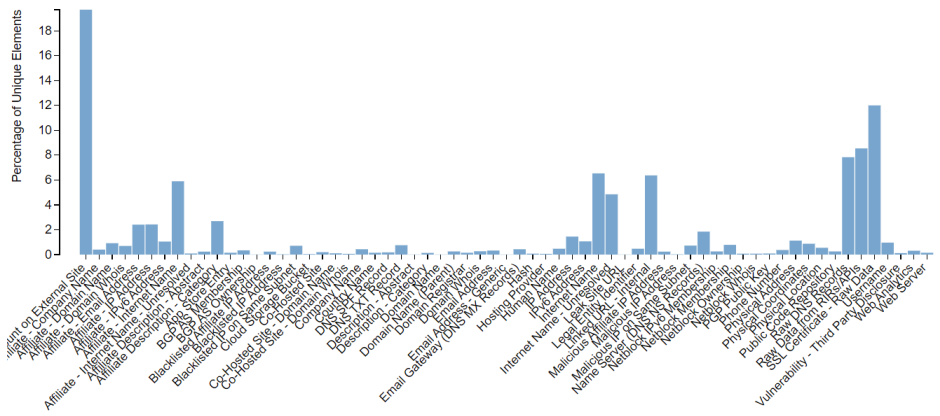
Scan Status

Total	Unique	Status	Errors
10399	6768	RUNNING	0

Correlations

High	Medium	Low	Info
0	0	0	0

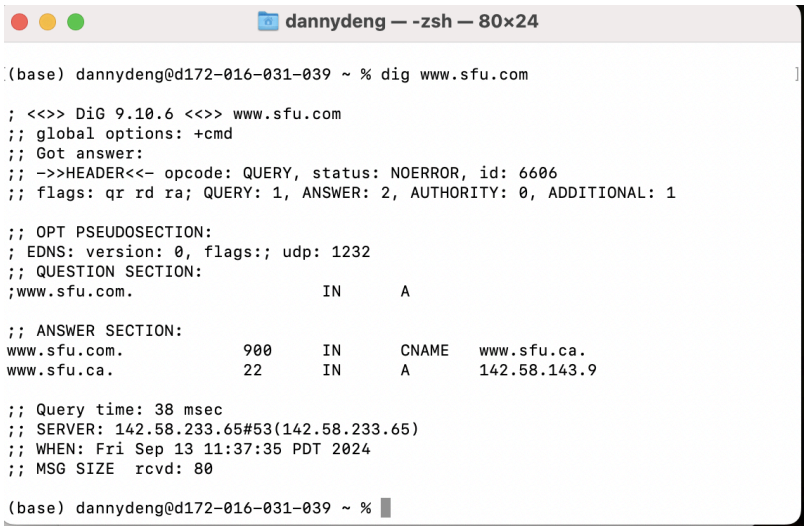
Data Types



Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	1333	1333	2024-09-12 19:43:38
Affiliate - Company Name	27	119	2024-09-12 19:42:05
Affiliate - Domain Name	62	241	2024-09-12 19:42:13
Affiliate - Domain Whois	47	47	2024-09-12 19:42:04
Affiliate - Email Address	163	528	2024-09-12 19:42:05
Affiliate - IP Address	164	300	2024-09-12 19:42:13
Affiliate - IPv6 Address	71	111	2024-09-12 19:42:02
Affiliate - Internet Name	399	640	2024-09-12 19:42:13
Affiliate - Internet Name - Unresolved	6	6	2024-09-12 19:06:13
Affiliate Description - Abstract	16	16	2024-09-12 19:01:13
Affiliate Description - Category	182	200	2024-09-12 19:01:13
App Store Entry	10	10	2024-09-12 16:51:31
BGP AS Membership	23	302	2024-09-12 19:42:02
BGP AS Ownership	1	2	2024-09-12 18:42:32
Blacklisted Affiliate IP Address	16	16	2024-09-12 19:39:16
Blacklisted IP Address	2	2	2024-09-12 17:53:24
Blacklisted IP on Same Subnet	48	48	2024-09-12 19:06:53
Cloud Storage Bucket	3	3	2024-09-12 16:51:40
Co-Hosted Site	13	40	2024-09-12 17:05:31
Co-Hosted Site - Domain Name	7	13	2024-09-12 18:49:03
Co-Hosted Site - Domain Whois	4	4	2024-09-12 18:49:02
Company Name	29	54	2024-09-12 19:06:51
Country Name	10	121	2024-09-12 19:42:03
DNS SPF Record	12	13	2024-09-12 19:06:13

1.2 DNS SERVER INTERROGATING

Task 2



The IP address is 142.58.143.9

Task 3

CNAME is the Canonical NAME
Whis is a type of DNS record used to alias one domain name to another. **www.sfu.com** is an alias for **www.sfu.ca**. So when someone accesses **www.sfu.com**, they will be redirected to **www.sfu.ca**. And then **www.sfu.ca** resolves to the IP address **142.58.143.9**.

Task 4

Use dig @m.root-servers.net mail.sfu.ca +norecurse command
Could be any root server, I just picked a random one.

```
(base) dannydeng@d172-016-031-039 ~ % dig @m.root-servers.net mail.sfu.ca +norec
urse

; <<>> DiG 9.10.6 <<>> @m.root-servers.net mail.sfu.ca +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11880
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;mail.sfu.ca.                   IN      A

;; AUTHORITY SECTION:
ca.                     172800  IN      NS      any.ca-servers.ca.
ca.                     172800  IN      NS      j.ca-servers.ca.
ca.                     172800  IN      NS      c.ca-servers.ca.
ca.                     172800  IN      NS      d.ca-servers.ca.

;; ADDITIONAL SECTION:
any.ca-servers.ca.      172800  IN      A       199.4.144.2
j.ca-servers.ca.        172800  IN      A       198.182.167.1
d.ca-servers.ca.        172800  IN      A       45.142.220.101
c.ca-servers.ca.        172800  IN      A       185.159.196.2
any.ca-servers.ca.      172800  IN      AAAA    2001:500:a7::2
j.ca-servers.ca.        172800  IN      AAAA    2001:500:83::1
d.ca-servers.ca.        172800  IN      AAAA    2a0e:dbc0::101
c.ca-servers.ca.        172800  IN      AAAA    2620:10a:8053::2

;; Query time: 478 msec
;; SERVER: 202.12.27.33#53(202.12.27.33)
;; WHEN: Fri Sep 13 11:54:24 PDT 2024
;; MSG SIZE  rcvd: 297
```

The answer only gives the **ca.** Which makes sense since it's one of the top-level country domains.

Task 5

dig @m.root-servers.net sfu.ca NS +norecurse

```
; <<>> DiG 9.10.6 <<>> @a.root-servers.net sfu.ca NS +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43816
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sfu.ca.                            IN      NS

;; AUTHORITY SECTION:
ca.                     172800  IN      NS      d.ca-servers.ca.
ca.                     172800  IN      NS      any.ca-servers.ca.
ca.                     172800  IN      NS      c.ca-servers.ca.
ca.                     172800  IN      NS      j.ca-servers.ca.

;; ADDITIONAL SECTION:
d.ca-servers.ca.        172800  IN      A       45.142.220.101
d.ca-servers.ca.        172800  IN      AAAA    2a0e:dbc0::101
any.ca-servers.ca.      172800  IN      A       199.4.144.2
any.ca-servers.ca.      172800  IN      AAAA    2001:500:a7::2
c.ca-servers.ca.        172800  IN      A       185.159.196.2
c.ca-servers.ca.        172800  IN      AAAA    2620:10a:8053::2
j.ca-servers.ca.        172800  IN      A       198.182.167.1
j.ca-servers.ca.        172800  IN      AAAA    2001:500:83::1

;; Query time: 49 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Fri Sep 13 12:02:07 PDT 2024
;; MSG SIZE  rcvd: 288
```

Dig @d.ca-servers.ca sfu.ca NS +norecurse

```
(base) dannydeng@d172-016-031-039 ~ % dig @d.ca-servers.ca sfu.ca NS +norecurse

; <<>> DiG 9.10.6 <<>> @d.ca-servers.ca sfu.ca NS +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25541
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;sfu.ca.                                IN      NS

;; AUTHORITY SECTION:
sfu.ca.                 86400   IN      NS      ns1.sfu.ca.
sfu.ca.                 86400   IN      NS      ns2.sfu.ca.
sfu.ca.                 86400   IN      NS      ns3.sfu.ca.

;; ADDITIONAL SECTION:
ns3.sfu.ca.             86400   IN      A       142.58.103.140
ns2.sfu.ca.             86400   IN      A       142.58.103.2
ns1.sfu.ca.             86400   IN      A       142.58.103.1
```

dig @ns1.sfu.ca sfu.ca A +norecurse

```
(base) dannydeng@d172-016-031-039 ~ % dig @ns1.sfu.ca sfu.ca A +norecurse

; <<>> DiG 9.10.6 <<>> @ns1.sfu.ca sfu.ca A +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12946
;; flags: qr aa ra; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;sfu.ca.                                IN      A

;; ANSWER SECTION:
sfu.ca.                 300     IN      A       142.58.143.9
sfu.ca.                 300     IN      A       142.58.103.17
sfu.ca.                 300     IN      A       142.58.103.137
sfu.ca.                 300     IN      A       142.58.103.55

;; AUTHORITY SECTION:
sfu.ca.                 300     IN      NS      ns1.sfu.ca.
sfu.ca.                 300     IN      NS      ns2.sfu.ca.
sfu.ca.                 300     IN      NS      ns3.sfu.ca.

;; ADDITIONAL SECTION:
ns2.sfu.ca.             300     IN      A       142.58.103.2
ns1.sfu.ca.             300     IN      A       142.58.103.1
ns3.sfu.ca.             300     IN      A       142.58.103.140

;; Query time: 49 msec
;; SERVER: 142.58.103.1#53(142.58.103.1)
;; WHEN: Fri Sep 13 12:06:12 PDT 2024
;; MSG SIZE  rcvd: 201
```

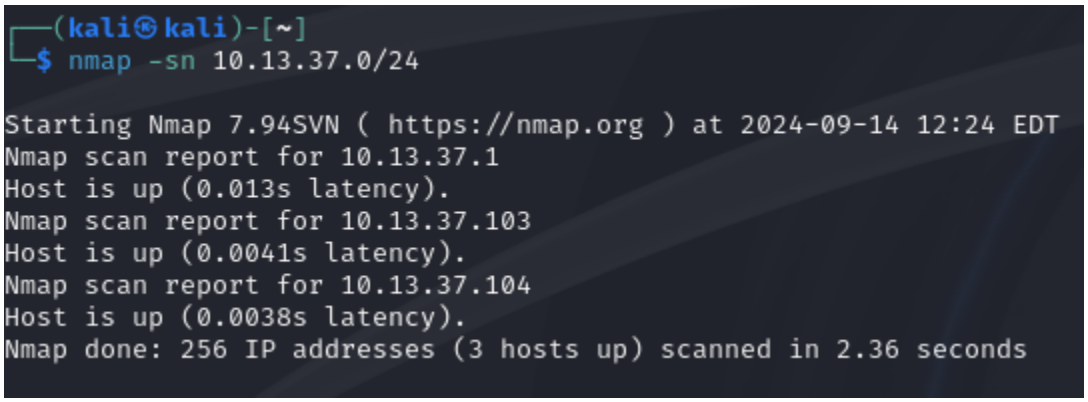
We got 4 IP address in the end
142.58.143.9
142.58.103.17
142.58.103.137
142.58.103.55

Task 6

On Kali use **ip route show**
On Window 7 use **route print**
We can know that the local network/netmask is **10.13.37.0/24**

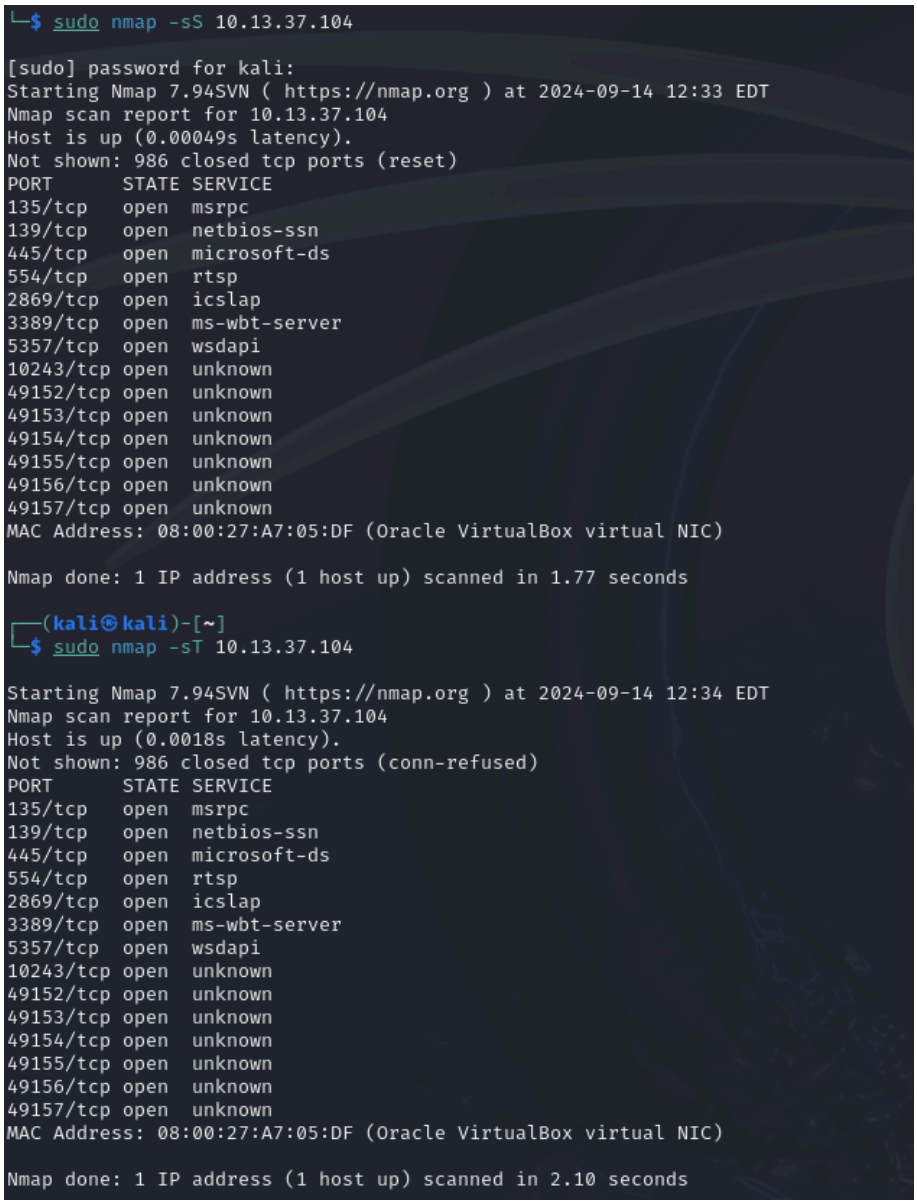
Task 7

Use **nmap -sn 10.13.37.0/24**



10.13.37.1: Active (The gateway/router).
10.13.37.103: Active (Kali)
10.13.37.104: Active (Windows 7 machine)

Task 8



TCP SYN Scan with Nmap (half-open scan)
nmap -sS 10.13.37.104
TCP Full Scan
nmap-sT 10.13.37.104
SYN Scan (`-sS`):

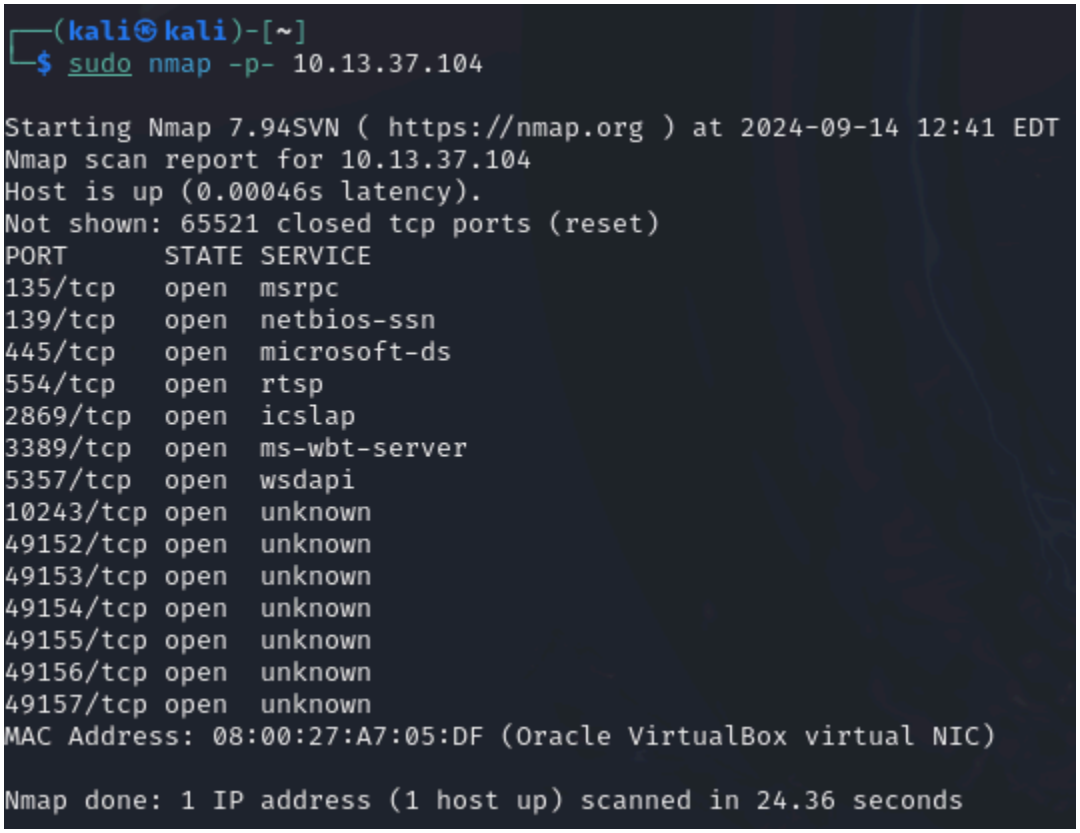
- This scan is faster (1.77 seconds) and only sends a SYN packet, receiving a SYN-ACK from open ports and then terminating the connection..
- Detected 14 open ports on the target machine.

TCP Connect Scan (`-sT`):

- This scan takes slightly longer (2.10 seconds) and completes the full TCP handshake (SYN, SYN-ACK, ACK), meaning the connection is fully established.
- The same 14 open ports were detected as in the SYN scan.

Task 9

sudo nmap -p- 10.13.37.104



Yes, we can infer the OS, you can see Microsoft there so it's probably a Windows system. With further research we can know

msrpc : Microsoft implementation of the RPC protocol

ms-wbt-server: Microsoft Remote Desktop Protoco

are indicators that the target is using a modern Windows version

Task 10

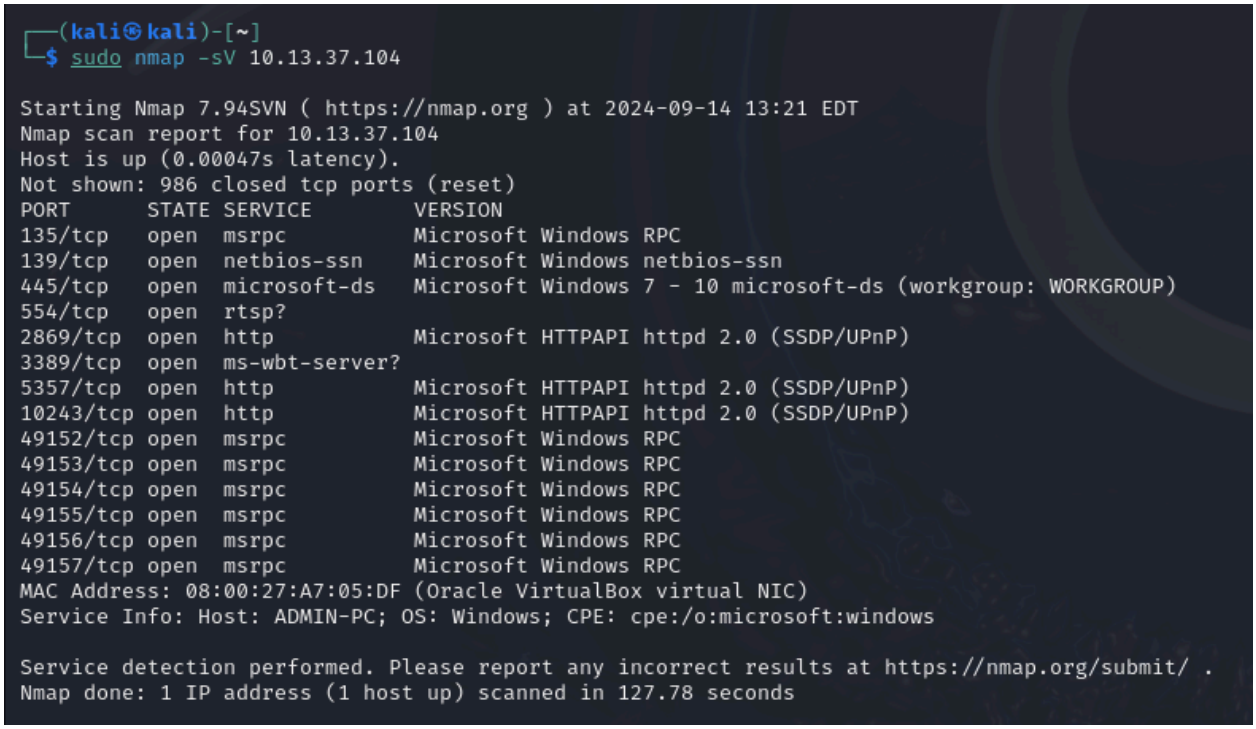
First method: **sudo nmap -O 10.13.37.104 to detect OS directly**

```
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 13:17 EDT
Nmap scan report for 10.13.37.104
Host is up (0.0030s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:A7:05:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:m
icrosoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Up
date 1
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 3.17 seconds
```

You can see it directly show the target's OS is Windows 7

Second method: **sudo nmap -sV 10.13.37.104 to perform service version detection**



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.13.37.104

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 13:21 EDT
Nmap scan report for 10.13.37.104
Host is up (0.00047s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server?
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:A7:05:DF (Oracle VirtualBox virtual NIC)
Service Info: Host: ADMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.78 seconds
```

We can see clearly the target using Windows 7

Task 11

https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html

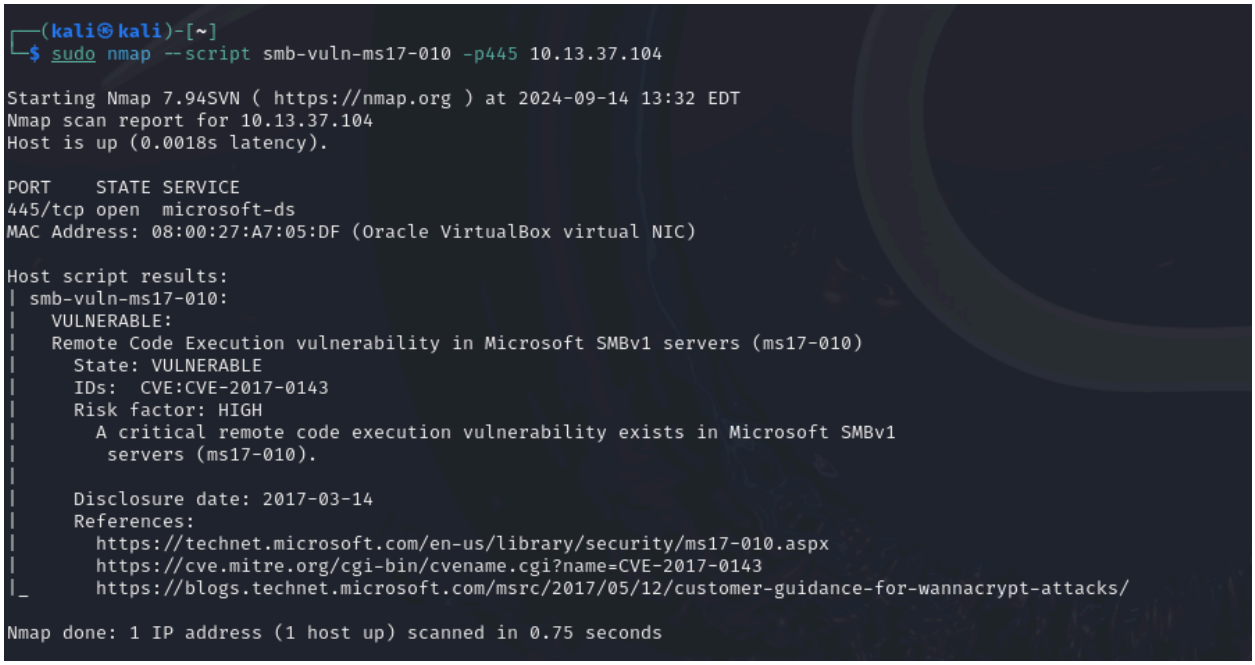
Script used: **smb-vuln-ms17-010**

Command: sudo nmap --script smb-vuln-ms17-010 -p445 10.13.37.104

SMB is running on **port 445**

https://www.varonis.com/blog/smb-port#:~:text=SMB%20uses%20either%20IP%20port,other%20on%20the%20same%20network.

Result:



Nmap scan has identified that the target machine is **vulnerable** to the **EternalBlue** exploit (CVE-2017-0143).

Task 12

By creating new scan we can find following Vulnerabilities

10.13.37.104

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	5	9	2	36

Vulnerabilities Total: 55

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.7	0.9748	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentia check)
CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.3	0.826	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remo Code Execution (2509553) (remote check)
HIGH	8.8	7.4	0.9675	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Coc Execution (2992611) (uncredentialed check)
HIGH	8.1	9.7	0.964	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	4.2	0.0111	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	9.3*	9.6	0.6791	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Re Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	6.0	0.0192	90510	MS16-047: Security Update for SAM and LSAD Remote Proto (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	2.5	0.0127	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakne
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.0054	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.0	-	-	58453	Terminal Services Doesn't Use Network Level Authentication (Only
MEDIUM	4.3*	-	-	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

Microsoft RDP RCE (BlueKeep), **EternalBlue**, **MS14-066**, and **MS12-020** can be directly used to exploit the system and gain control. These vulnerabilities allow **remote code execution** and are highly critical.

Vulnerabilities like **SSL Weaknesses**, **SMB Signing Not Required**, and **RDP Encryption Weaknesses** are more likely to be exploited for **information gathering** or **man-in-the-middle attacks**. While not used for direct access, they can increase the risk of other attacks.