

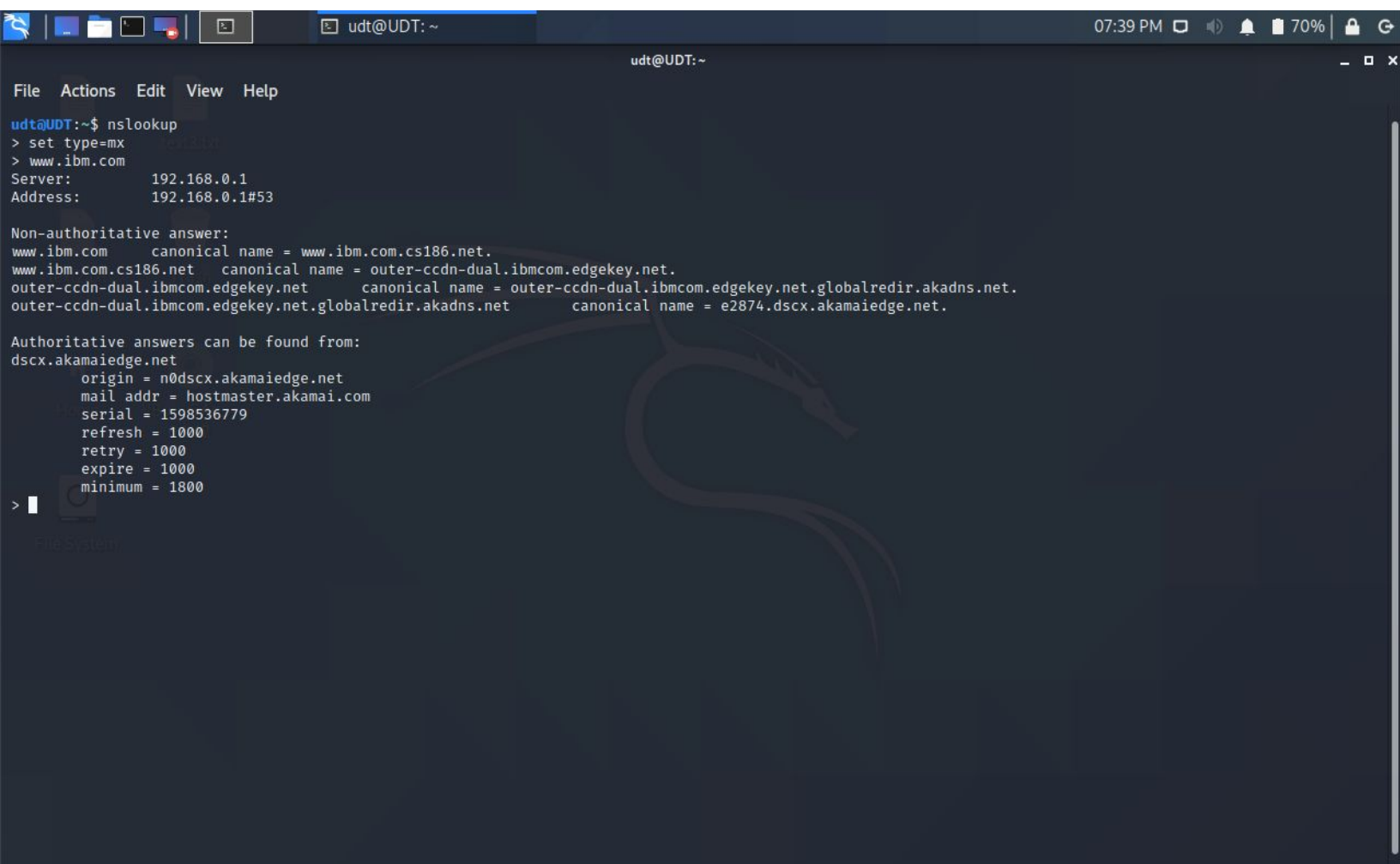
Assignment Day 4 | 23rd August 2020

Question 1:

Find out the mail servers of the following domain :

Ans: We will use nslookup along with the set type=mx to find out the mail servers

[Ibm.com](https://www.ibm.com)



```
udt@UDT: ~  
File Actions Edit View Help  
udt@UDT:~$ nslookup  
> set type=mx  
> www.ibm.com  
Server:      192.168.0.1  
Address:     192.168.0.1#53  
  
Non-authoritative answer:  
www.ibm.com canonical name = www.ibm.com.cs186.net.  
www.ibm.com.cs186.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.  
outer-ccdn-dual.ibmcom.edgekey.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net.  
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net canonical name = e2874.dscx.akamaiedge.net.  
  
Authoritative answers can be found from:  
dscx.akamaiedge.net  
origin = n0dscx.akamaiedge.net  
mail addr = hostmaster.akamai.com  
serial = 1598536779  
refresh = 1000  
retry = 1000  
expire = 1000  
minimum = 1800  
>
```

Wipro.com

```
udt@UDT: ~  
File Actions Edit View Help  
udt@UDT:~$ nslookup  
> set type=mx  
> www.wipro.com  
Server:      192.168.0.1  
Address:     192.168.0.1#53  
  
Non-authoritative answer:  
www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net.  
www.wipro.com.cdn.cloudflare.net canonical name = cdnetp-cdn-dual-ibwcdm.edgekey.net.  
Authoritative answers can be found from: canonical name = cdnetp-cdn-dual-ibwcdm.edgekey.net/globalredir.akadns.net;  
d361nqn33s63ex.cloudfront.net .net.globalredir.akadns.net canonical name = e2874.usca.akamaiedge.net;  
origin = ns-1658.awsdns-15.co.uk  
Authority mail addr = awsdns-hostmaster.amazon.com  
Serial = 1  
Refresh = 7200 .akamaiedge.net  
Retry = 900 hostmaster.akamai.com  
Expire = 1209600 /s  
Minimum = 86400  
> █  
Retry = 1800  
Expire = 1800  
Minimum = 1800  
> nslookup www.wipro.com
```

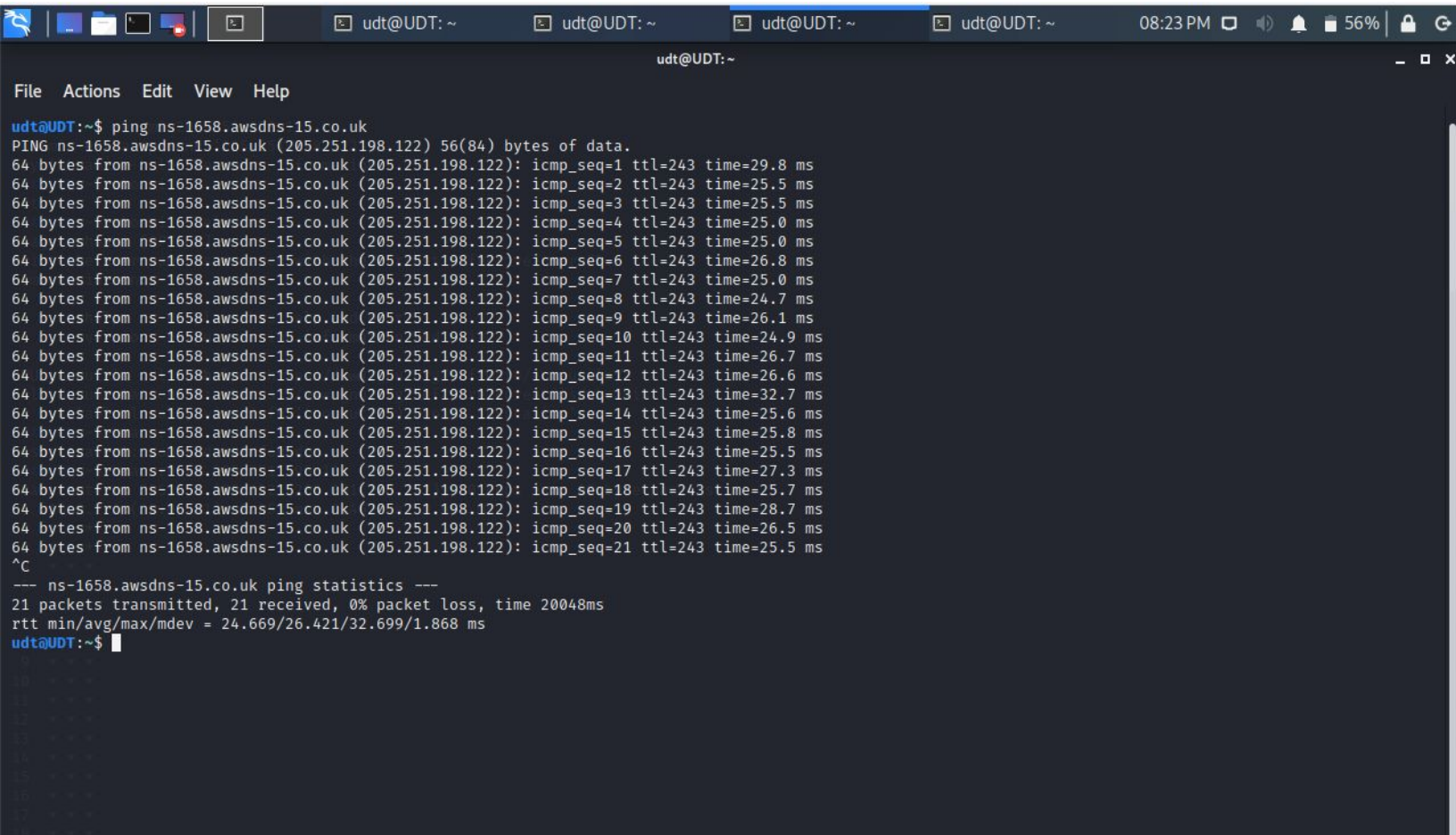
Question 2:

Find the locations, where these email servers are hosted.

Ans: From the above we will get the email servers thus we will perform following actions to get location:

For wipro:

1. `ping ns-1658.awsdns-15.co.uk`, so that we get the ip address `205.251.198.122`



```
udt@UDT: ~  
File Actions Edit View Help  
udt@UDT:~$ ping ns-1658.awsdns-15.co.uk  
PING ns-1658.awsdns-15.co.uk (205.251.198.122) 56(84) bytes of data.  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=1 ttl=243 time=29.8 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=2 ttl=243 time=25.5 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=3 ttl=243 time=25.5 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=4 ttl=243 time=25.0 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=5 ttl=243 time=25.0 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=6 ttl=243 time=26.8 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=7 ttl=243 time=25.0 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=8 ttl=243 time=24.7 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=9 ttl=243 time=26.1 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=10 ttl=243 time=24.9 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=11 ttl=243 time=26.7 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=12 ttl=243 time=26.6 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=13 ttl=243 time=32.7 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=14 ttl=243 time=25.6 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=15 ttl=243 time=25.8 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=16 ttl=243 time=25.5 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=17 ttl=243 time=27.3 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=18 ttl=243 time=25.7 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=19 ttl=243 time=28.7 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=20 ttl=243 time=26.5 ms  
64 bytes from ns-1658.awsdns-15.co.uk (205.251.198.122): icmp_seq=21 ttl=243 time=25.5 ms  
^C  
--- ns-1658.awsdns-15.co.uk ping statistics ---  
21 packets transmitted, 21 received, 0% packet loss, time 20048ms  
rtt min/avg/max/mdev = 24.669/26.421/32.699/1.868 ms  
udt@UDT:~$
```

2. Now **use whois command or website** to get the location, here US country, Seattle city, 1918 8th Ave

```
udt@UDT:~$ whois 205.251.198.122
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#

NetRange: 205.251.192.0 - 205.251.255.255
CIDR: 205.251.192.0/18
NetName: AMAZON-05
NetHandle: NET-205-251-192-0-1
Parent: NET205 (NET-205-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS16509, AS39111, AS7224
Organization: Amazon.com, Inc. (AMAZON-4)
RegDate: 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/205.251.192.0

OrgName: Amazon.com, Inc.
OrgId: AMAZON-4
Address: 1918 8th Ave
City: SEATTLE
StateProv: WA
PostalCode: 98101-1244
Country: US
RegDate: 1995-01-23
Updated: 2020-03-31
Ref: https://rdap.arin.net/registry/entity/AMAZON-4

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
```

[Home](#) > [Whois Lookup](#) > 205.251.198.122

IP Information for 205.251.198.122

— Quick Stats

IP Location	United States Of America Seattle Amazon.com Inc.
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
Resolve Host	ns-1658.awsdns-15.co.uk
Whois Server	whois.arin.net
IP Address	205.251.198.122

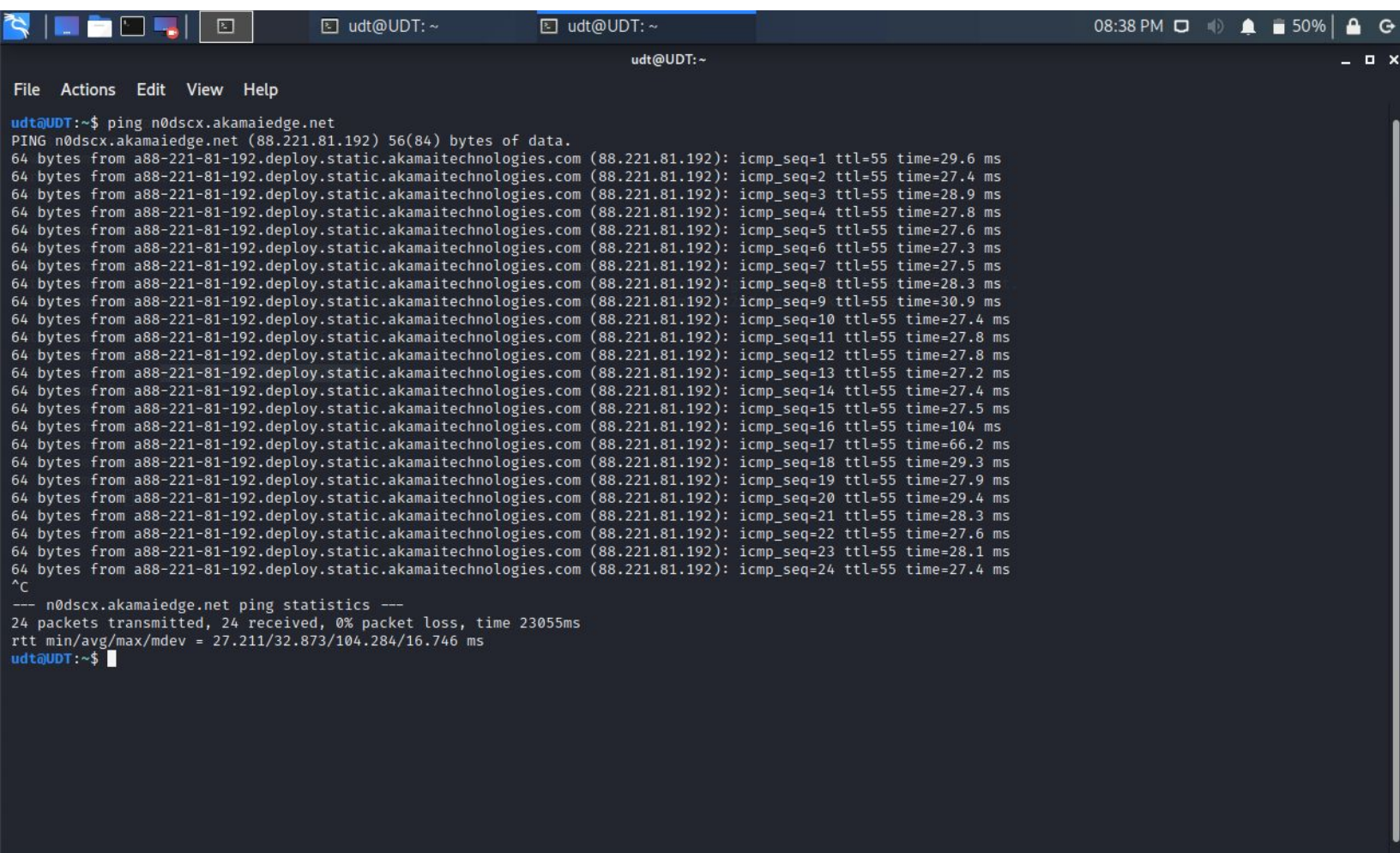
```
NetRange:      205.251.192.0 - 205.251.255.255
CIDR:          205.251.192.0/18
NetName:       AMAZON-05
NetHandle:     NET-205-251-192-0-1
Parent:        NET205 (NET-205-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS16509, AS39111, AS7224
Organization:  Amazon.com, Inc. (AMAZON-4)
RegDate:       2010-08-27
Updated:       2015-09-24
Ref:           https://rdap.arin.net/registry/ip/205.251.192.0

OrgName:       Amazon.com, Inc.
OrgId:         AMAZON-4
Address:       1918 8th Ave
City:          SEATTLE
StateProv:     WA
PostalCode:    98101-1244
Country:       US
RegDate:       1995-01-23
Updated:       2020-03-31
Ref:           https://rdap.arin.net/registry/entity/AMAZON-4

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName:  IP Routing
OrgRoutingPhone: +1-206-266-4064
OrgRoutingEmail: aws-routing-poc@amazon.com
```


For ibm:

1. ping `nodscx.akamaiedge.net` , so that we get the ip address `88.221.81.192`



```
udt@UDT: ~  
File Actions Edit View Help  
udt@UDT:~$ ping nodscx.akamaiedge.net  
PING nodscx.akamaiedge.net (88.221.81.192) 56(84) bytes of data:  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=1 ttl=55 time=29.6 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=2 ttl=55 time=27.4 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=3 ttl=55 time=28.9 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=4 ttl=55 time=27.8 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=5 ttl=55 time=27.6 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=6 ttl=55 time=27.3 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=7 ttl=55 time=27.5 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=8 ttl=55 time=28.3 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=9 ttl=55 time=30.9 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=10 ttl=55 time=27.4 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=11 ttl=55 time=27.8 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=12 ttl=55 time=27.8 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=13 ttl=55 time=27.2 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=14 ttl=55 time=27.4 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=15 ttl=55 time=27.5 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=16 ttl=55 time=104 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=17 ttl=55 time=66.2 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=18 ttl=55 time=29.3 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=19 ttl=55 time=27.9 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=20 ttl=55 time=29.4 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=21 ttl=55 time=28.3 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=22 ttl=55 time=27.6 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=23 ttl=55 time=28.1 ms  
64 bytes from a88-221-81-192.deploy.static.akamaitechnologies.com (88.221.81.192): icmp_seq=24 ttl=55 time=27.4 ms  
^C  
--- n0dscx.akamaiedge.net ping statistics ---  
24 packets transmitted, 24 received, 0% packet loss, time 23055ms  
rtt min/avg/max/mdev = 27.211/32.873/104.284/16.746 ms  
udt@UDT:~$
```

2. Now use whois command or website to get the location, here US country, Cambridge MA 02142 , Akamai Technologies

```
File Actions Edit View Help
% To receive output for a database update, use the "-B" flag.
% Information related to '88.221.81.0 - 88.221.81.255'
% Abuse contact for '88.221.81.0 - 88.221.81.255' is 'abuse@akamai.com'

inetnum: 88.221.81.0 - 88.221.81.255
netname: AKAMAI-PA
descr: Akamai Technologies
country: EU
admin-c: NARA1-RIPE
tech-c: NARA1-RIPE
status: ASSIGNED PA
mnt-by: AKAM1-RIPE-MNT
mnt-routes: AKAM1-RIPE-MNT
created: 2013-10-11T16:59:42Z
last-modified: 2013-10-11T16:59:42Z
source: RIPE

role: Network Architecture Role Account
address: Akamai Technologies
address: 8 Cambridge Center
address: Cambridge, MA 02142
phone: +1-617-938-3130
abuse-mailbox: abuse@akamai.com
admin-c: NF1714-RIPE
admin-c: CKAK-RIPE
tech-c: NF1714-RIPE
tech-c: JP1944-RIPE
tech-c: APB15-RIPE
tech-c: CKAK-RIPE
tech-c: TBAK-RIPE
tech-c: NB782-RIPE
tech-c: RM4844-RIPE
tech-c: AKAY-RIPE
nic-hdl: NARA1-RIPE
mnt-by: AKAM1-RIPE-MNT
created: 2002-03-06T09:02:17Z
last-modified: 2019-04-15T17:17:53Z
source: RIPE # Filtered
```

[Home](#) > [Whois Lookup](#) > 88.221.81.192

IP Information for 88.221.81.192

— Quick Stats

IP Location	 United States Of America Middletown Akamai Technologies Inc.
ASN	 AS21342 AKAMAI-ASN2, EU (registered Nov 05, 2001)
Resolve Host	a88-221-81-192.deploy.static.akamaitechnologies.com
Whois Server	whois.ripe.net
IP Address	88.221.81.192

% Abuse contact for '88.221.81.0 - 88.221.81.255' is ' abuse@akamai.com '

```
inetnum:      88.221.81.0 - 88.221.81.255
netname:      AKAMAI-PA
descr:        Akamai Technologies
country:      EU
admin-c:      NARA1-RIPE
tech-c:       NARA1-RIPE
status:       ASSIGNED PA
mnt-by:       AKAM1-RIPE-MNT
mnt-routes:   AKAM1-RIPE-MNT
created:      2013-10-11T16:59:42Z
last-modified: 2013-10-11T16:59:42Z
source:       RIPE

role:         Network Architecture Role Account
address:      Akamai Technologies
address:      8 Cambridge Center
address:      Cambridge, MA 02142
phone:        +1-617-938-3130
e-mail:       ip-admin@akamai.com
abuse-mailbox: abuse@akamai.com

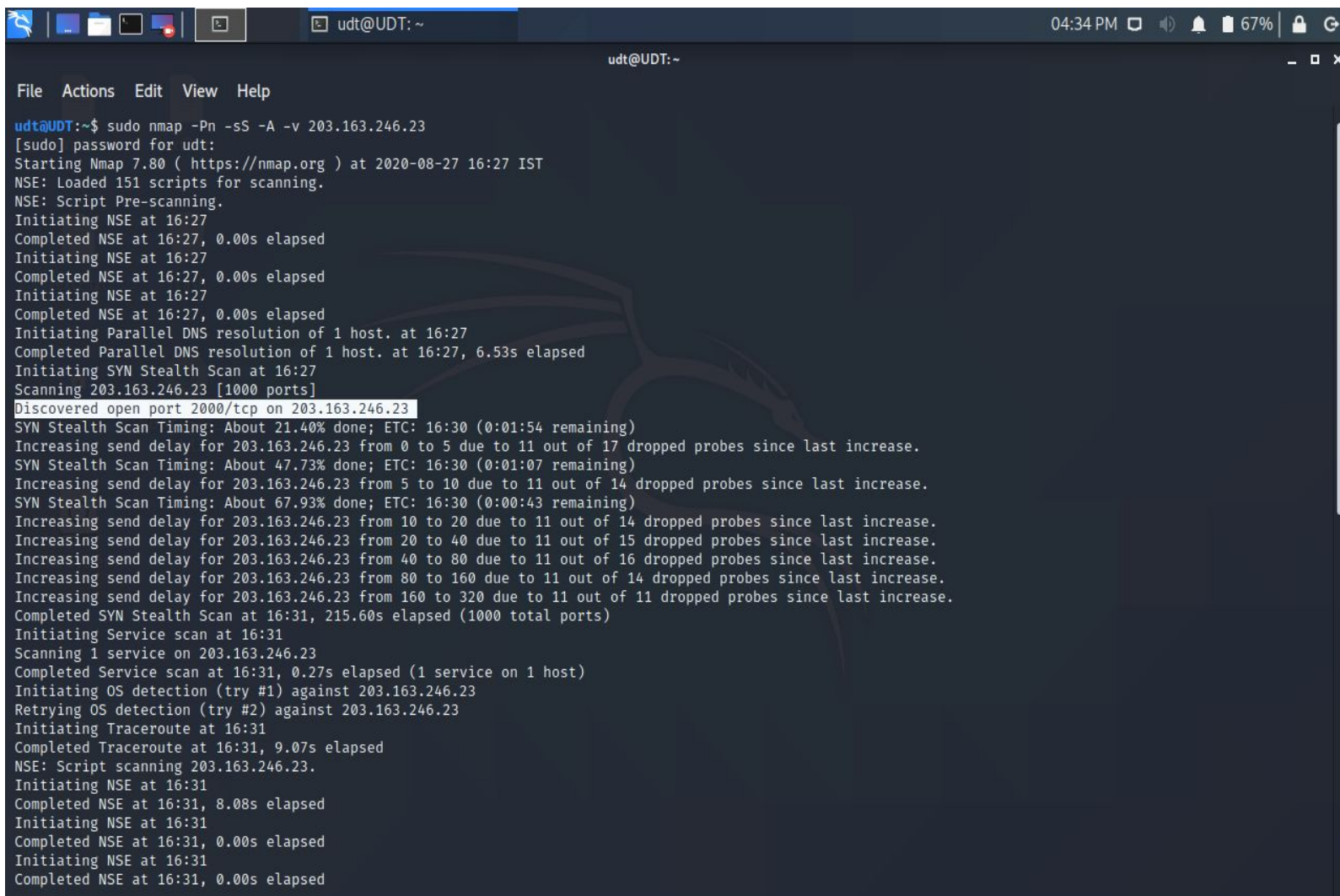
admin-c:      NF1714-RIPE
admin-c:      CKAK-RIPE
tech-c:       NF1714-RIPE
tech-c:       JP1944-RIPE
```


Question 3:

Scan and find out port numbers open 203.163.246.23

Ans: Here we will use the **nmap** to scan for the open port for 203.163.246.23

- ss is for stealth scan
- v is for verbose mode
- A aggressive scan
- Pn to scan behind a firewall

A terminal window titled 'udt@UDT: ~' showing the execution of an nmap scan. The command 'sudo nmap -Pn -ss -A -v 203.163.246.23' is entered. The output shows the scan progress, including NSE script pre-scanning, parallel DNS resolution, and a SYN Stealth Scan. The scan discovers an open port 2000/tcp on 203.163.246.23. The terminal also shows service scanning and OS detection attempts.

```
udt@UDT:~$ sudo nmap -Pn -ss -A -v 203.163.246.23
[sudo] password for udt:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 16:27 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 16:27
Completed Parallel DNS resolution of 1 host. at 16:27, 6.53s elapsed
Initiating SYN Stealth Scan at 16:27
Scanning 203.163.246.23 [1000 ports]
Discovered open port 2000/tcp on 203.163.246.23
SYN Stealth Scan Timing: About 21.40% done; ETC: 16:30 (0:01:54 remaining)
Increasing send delay for 203.163.246.23 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
SYN Stealth Scan Timing: About 47.73% done; ETC: 16:30 (0:01:07 remaining)
Increasing send delay for 203.163.246.23 from 5 to 10 due to 11 out of 14 dropped probes since last increase.
SYN Stealth Scan Timing: About 67.93% done; ETC: 16:30 (0:00:43 remaining)
Increasing send delay for 203.163.246.23 from 10 to 20 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 203.163.246.23 from 20 to 40 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 203.163.246.23 from 40 to 80 due to 11 out of 16 dropped probes since last increase.
Increasing send delay for 203.163.246.23 from 80 to 160 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 203.163.246.23 from 160 to 320 due to 11 out of 11 dropped probes since last increase.
Completed SYN Stealth Scan at 16:31, 215.60s elapsed (1000 total ports)
Initiating Service scan at 16:31
Scanning 1 service on 203.163.246.23
Completed Service scan at 16:31, 0.27s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 203.163.246.23
Retrying OS detection (try #2) against 203.163.246.23
Initiating Traceroute at 16:31
Completed Traceroute at 16:31, 9.07s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 16:31
Completed NSE at 16:31, 8.08s elapsed
Initiating NSE at 16:31
Completed NSE at 16:31, 0.00s elapsed
Initiating NSE at 16:31
Completed NSE at 16:31, 0.00s elapsed
```

```
udt@UDT: ~  
File Actions Edit View Help  
Completed NSE at 16:31, 0.00s elapsed  
Initiating NSE at 16:31  
Completed NSE at 16:31, 0.00s elapsed  
Nmap scan report for 203.163.246.23  
Host is up (0.022s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE VERSION  
113/tcp   closed ident  
2000/tcp  open  tcpwrapped  
Device type: firewall  
Running (JUST GUESSING): Fortinet embedded (87%)  
OS CPE: cpe:/h:fortinet:fortigate_100d  
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)  
No exact OS matches for host (test conditions non-ideal).  
  
TRACEROUTE (using port 113/tcp)  
HOP RTT ADDRESS  
1 ... 30  
  
NSE: Script Post-scanning.  
Initiating NSE at 16:31  
Completed NSE at 16:31, 0.00s elapsed  
Initiating NSE at 16:31  
Completed NSE at 16:31, 0.00s elapsed  
Initiating NSE at 16:31  
Completed NSE at 16:31, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
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 248.77 seconds  
Raw packets sent: 3342 (153.064KB) | Rcvd: 25 (1.008KB)
```

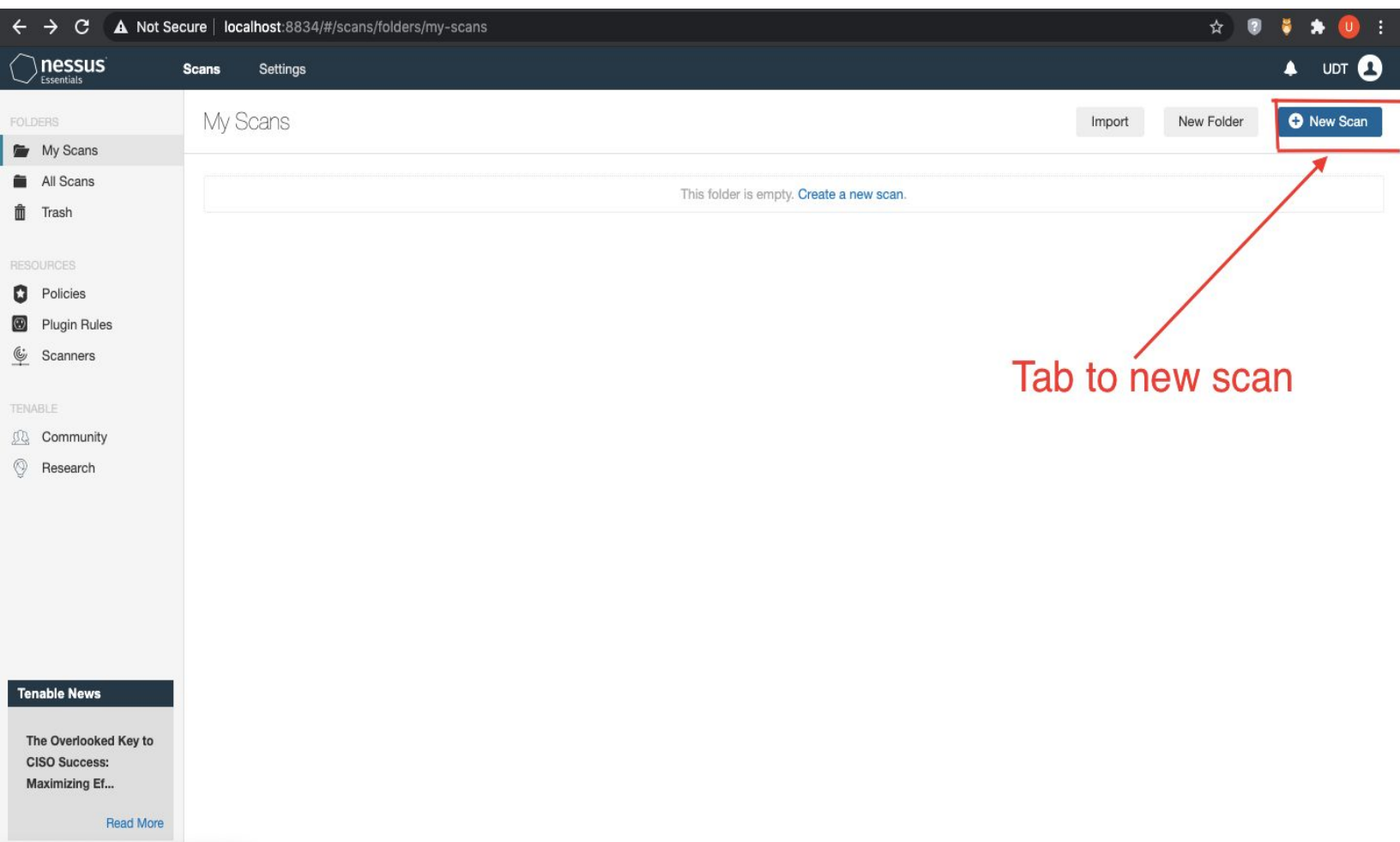
Here we can see that 998 ports are filtered and 1 port is closed as well as 1 port is open.

Question 4:

Install nessus in a VM and scan your laptop/desktop for CVE.

Ans: We will first of all install nessus and complete the login process with user id and password and activation key

1. Now will select the New Scan



2. Select the Advance Scan

The screenshot shows the Nessus Essentials web interface. The browser address bar indicates the URL is `localhost:8834/#/scans/reports/new`. The interface has a dark blue header with the Nessus logo and navigation tabs for 'Scans' and 'Settings'. On the left, there is a sidebar with sections: 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Scanners), and 'TENABLE' (Community, Research). The main content area is titled 'Scan Templates' and includes a 'Back to Scans' link and a search bar. It is divided into three sections: 'DISCOVERY' (containing 'Host Discovery'), 'VULNERABILITIES' (containing a grid of 15 scan templates), and 'UPGRADE' (containing 'Mobile Device Scan'). A red arrow points from the text 'Tab to advance scan' to the 'Advanced Scan' template in the 'VULNERABILITIES' section. The 'Advanced Scan' template is described as 'Configure a scan without using any recommendations.' Other templates include 'Basic Network Scan', 'Advanced Dynamic Scan', 'Malware Scan', 'Web Application Tests', 'Credentialed Patch Audit', 'Badlock Detection', 'Bash Shellshock Detection', 'DROWN Detection', 'Intel AMT Security Bypass', 'Shadow Brokers Scan', 'Spectre and Meltdown', and 'WannaCry Ransomware'.

Scan Templates

[Back to Scans](#)

Scanner

Search Library

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

DROWN Detection
Remote checks for CVE-2016-0800.

Intel AMT Security Bypass

Shadow Brokers Scan

Spectre and Meltdown

WannaCry Ransomware

Tenable News

Teltonika Gateway TRB245 Multiple Vulnerabilities

[Read More](#)

3. Add name and the ip address of target system

← → ↻ ⚠ Not Secure | localhost:8834/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/basic/general ☆ ? 🐱 ⚙️ UDT 👤

nessus Essentials Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- ★ Policies
- 📄 Plugin Rules
- 🔍 Scanners

ENABLE

- 👤 Community
- 💡 Research

Tenable News

Ubiquiti UniFi Protect Username Discovery

[Read More](#)

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name Windows 10

Description

Folder My Scans

Targets 10.0.2.2

Upload Targets [Add File](#)

Save Cancel

Add name and target ip address

4. Enter the credentials and launch the scan

Enter details here

Launch scan from here

Save Cancel

Launch

5. From here we can get the report of the scan which we have performed

The screenshot displays the Nessus Essentials web interface. The browser address bar shows 'localhost:8834/#/scans/reports/6/history'. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', 'Scanners', 'Community', and 'Research'. The main content area is titled 'Windows 10' and shows a table of scan history. A red arrow points from the 'Report' dropdown menu to the text below.

Windows 10

Configure Launch Report Export

PDF HTML CSV

Start Time	Last Modified	Status	Scan Details
<input type="checkbox"/> Current Today at 5:14 PM	Today at 5:14 PM	✓ Completed	Policy: Advanced Scan Status: Completed Scanner: Local Scanner Start: Today at 5:14 PM End: Today at 5:14 PM Elapsed: a few seconds
<input type="checkbox"/> Today at 5:08 PM	Today at 5:08 PM	✓ Completed	
<input type="checkbox"/> Today at 5:07 PM	Today at 5:07 PM	✓ Completed	

Here we will get the report of our scans also and study it to resolve the vulnerabilities.

