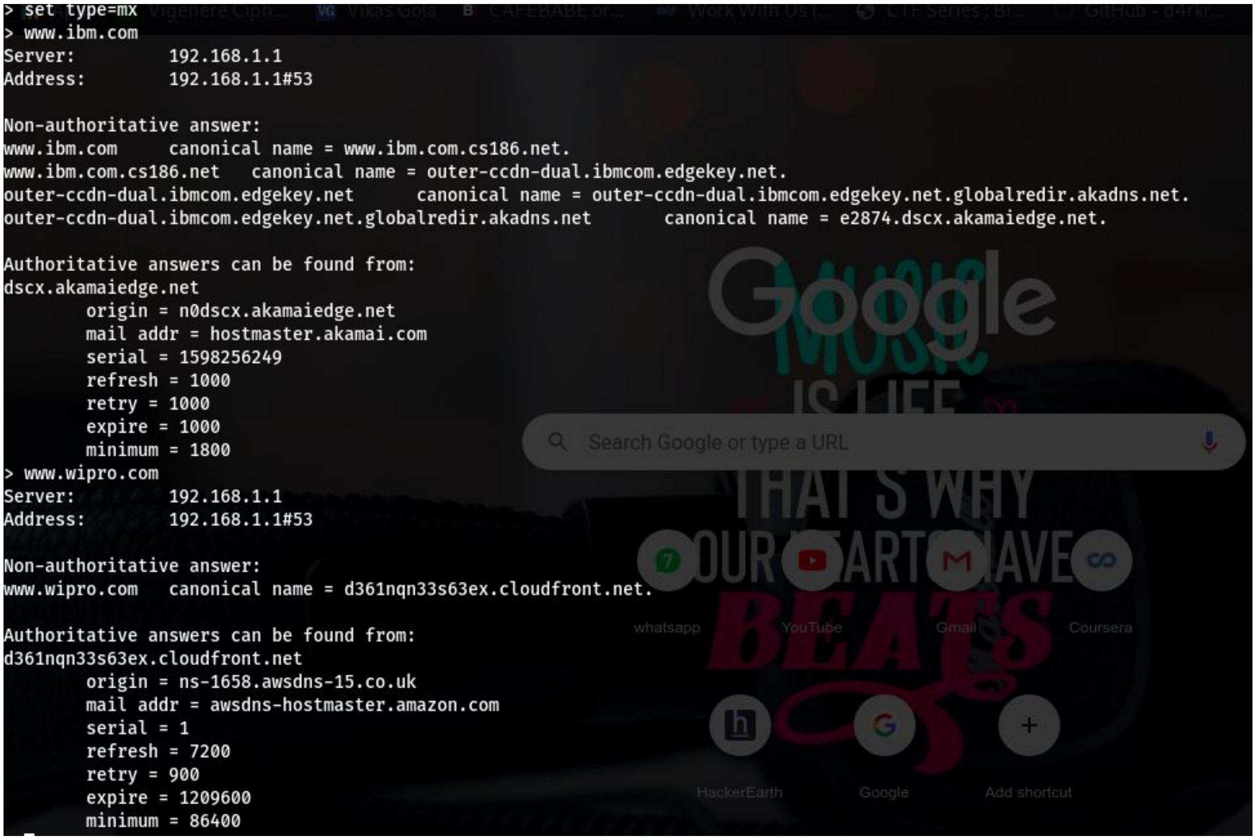
Assignment | Day 4 | Cybersecurity | LetsUpgrade

Q 1. Find out the mail servers of the following domain:

a) Ibm.com b) Wipro.com

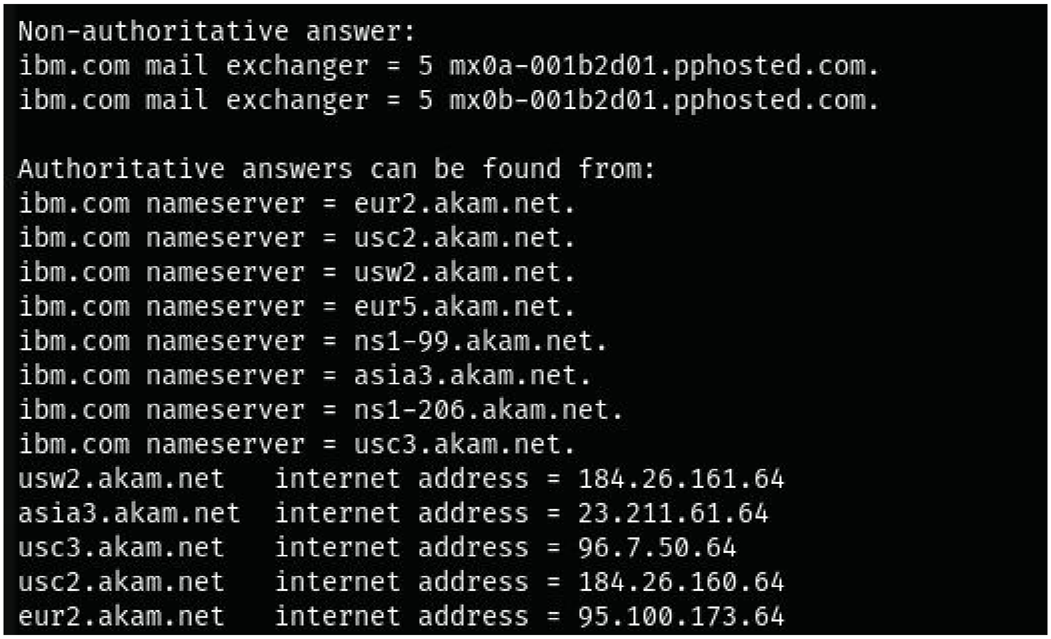
Answer 1:



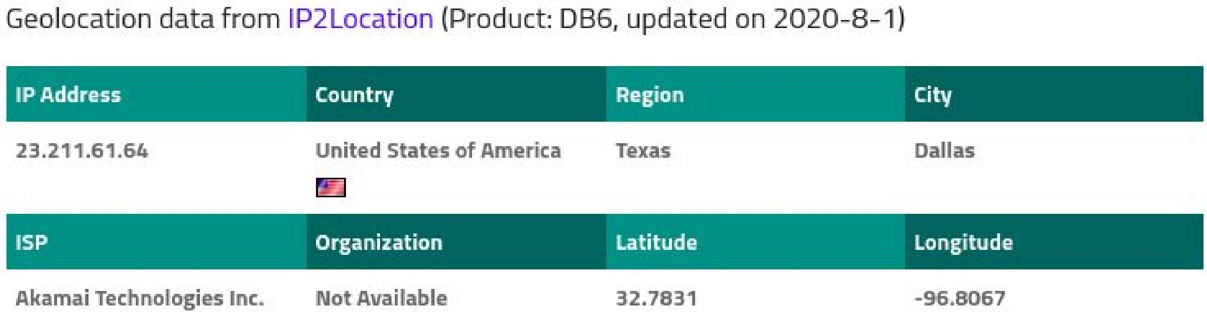
```
> set type=mx
> www.ibm.com
Server:         192.168.1.1
Address:        192.168.1.1#53

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 = 1598256249
        refresh = 1000
        retry = 1000
        expire = 1000
        minimum = 1800
> www.wipro.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.wipro.com   canonical name = d361nqn33s63ex.cloudfront.net.

Authoritative answers can be found from:
d361nqn33s63ex.cloudfront.net
        origin = ns-1658.awsdns-15.co.uk
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
```

Q 2. Find the locations, where these email servers are hosted.

Answer 2:
ibm.com

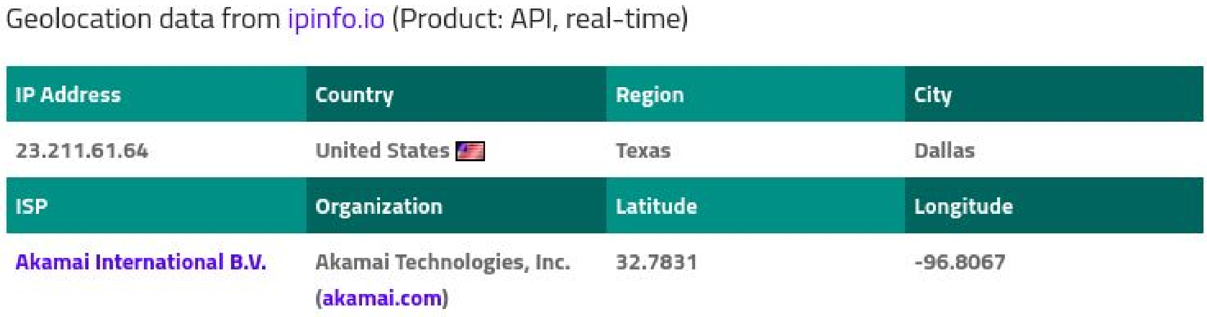


```
Non-authoritative answer:
ibm.com mail exchanger = 5 mx0a-001b2d01.pphosted.com.
ibm.com mail exchanger = 5 mx0b-001b2d01.pphosted.com.

Authoritative answers can be found from:
ibm.com nameserver = eur2.akam.net.
ibm.com nameserver = usc2.akam.net.
ibm.com nameserver = usw2.akam.net.
ibm.com nameserver = eur5.akam.net.
ibm.com nameserver = ns1-99.akam.net.
ibm.com nameserver = asia3.akam.net.
ibm.com nameserver = ns1-206.akam.net.
ibm.com nameserver = usc3.akam.net.
usw2.akam.net   internet address = 184.26.161.64
asia3.akam.net  internet address = 23.211.61.64
usc3.akam.net   internet address = 96.7.50.64
usc2.akam.net   internet address = 184.26.160.64
eur2.akam.net   internet address = 95.100.173.64
```



Geolocation data from IP2Location (Product: DB6, updated on 2020-8-1)

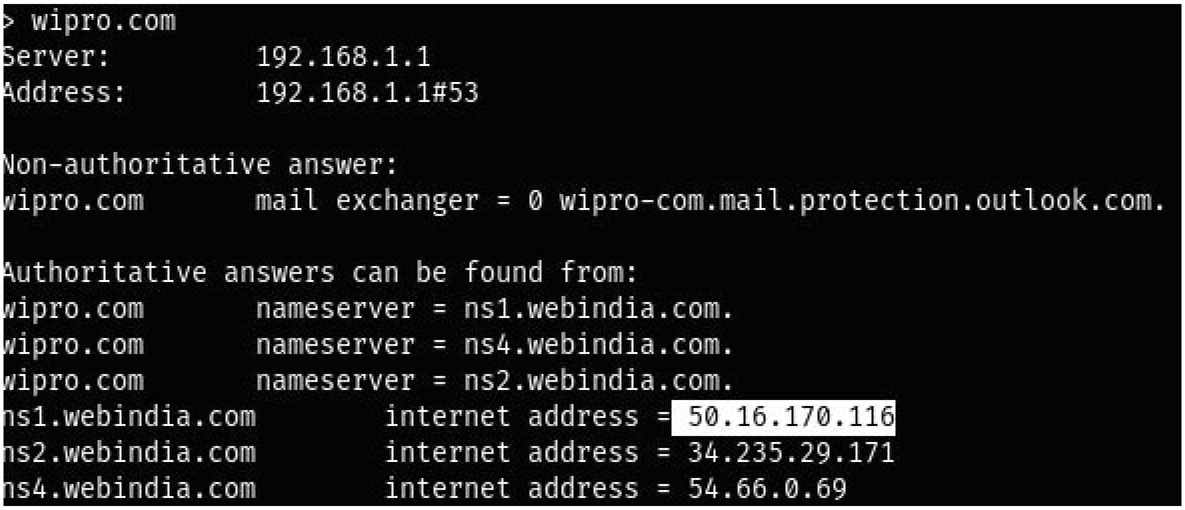
IP Address	Country	Region	City
23.211.61.64	United States of America 🇺🇸	Texas	Dallas
ISP	**Organization**	**Latitude**	**Longitude**
Akamai Technologies Inc.	Not Available	32.7831	-96.8067



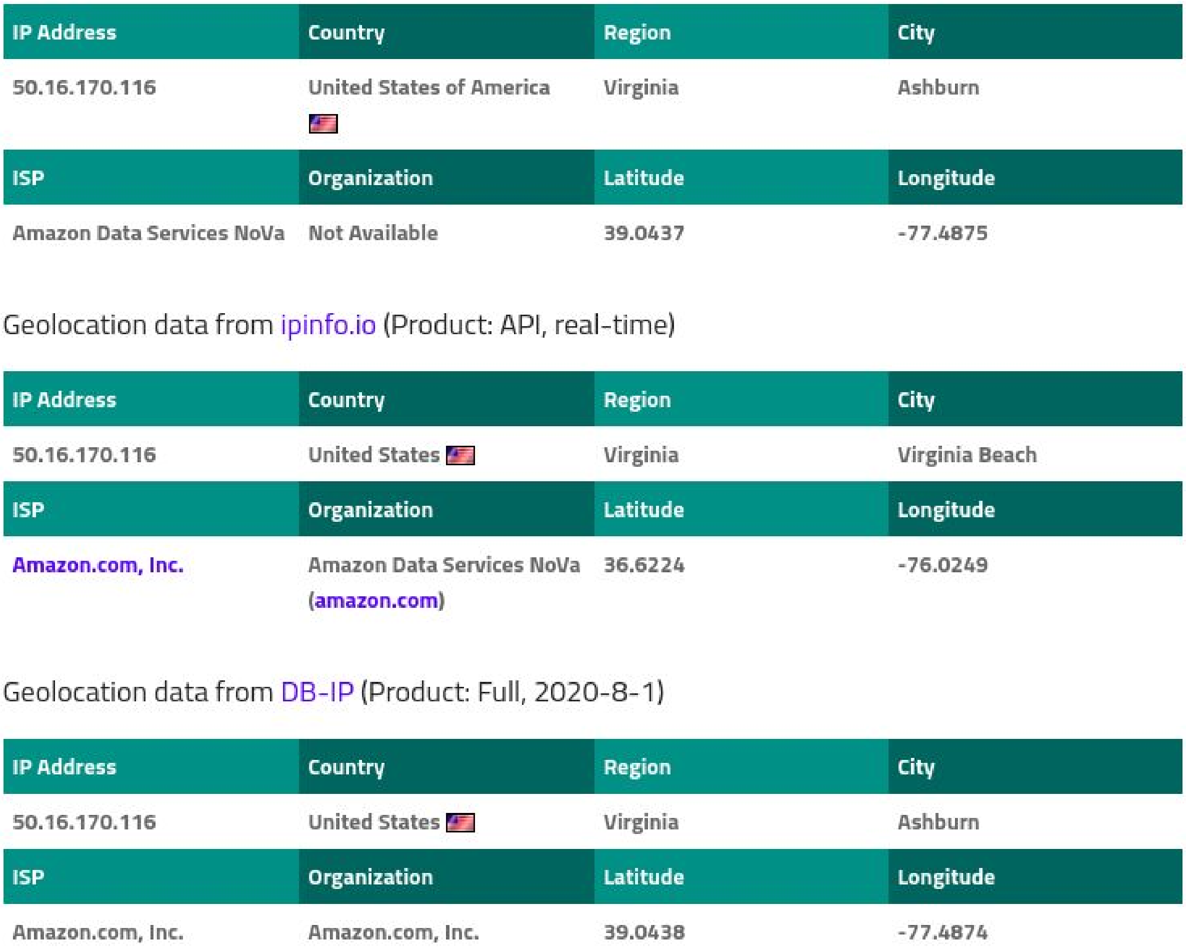
Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
23.211.61.64	United States 🇺🇸	Texas	Dallas
ISP	**Organization**	**Latitude**	**Longitude**
Akamai International B.V.	Akamai Technologies, Inc. (akamai.com)	32.7831	-96.8067

Wipro.com



```
> wipro.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
wipro.com       mail exchanger = 0 wipro-com.mail.protection.outlook.com.

Authoritative answers can be found from:
wipro.com       nameserver = ns1.webindia.com.
wipro.com       nameserver = ns4.webindia.com.
wipro.com       nameserver = ns2.webindia.com.
ns1.webindia.com        internet address = 50.16.170.116
ns2.webindia.com        internet address = 34.235.29.171
ns4.webindia.com        internet address = 54.66.0.69
```



IP Address	Country	Region	City
50.16.170.116	United States of America 🇺🇸	Virginia	Ashburn
ISP	**Organization**	**Latitude**	**Longitude**
Amazon Data Services NoVa	Not Available	39.0437	-77.4875

Geolocation data from ipinfo.io (Product: API, real-time)

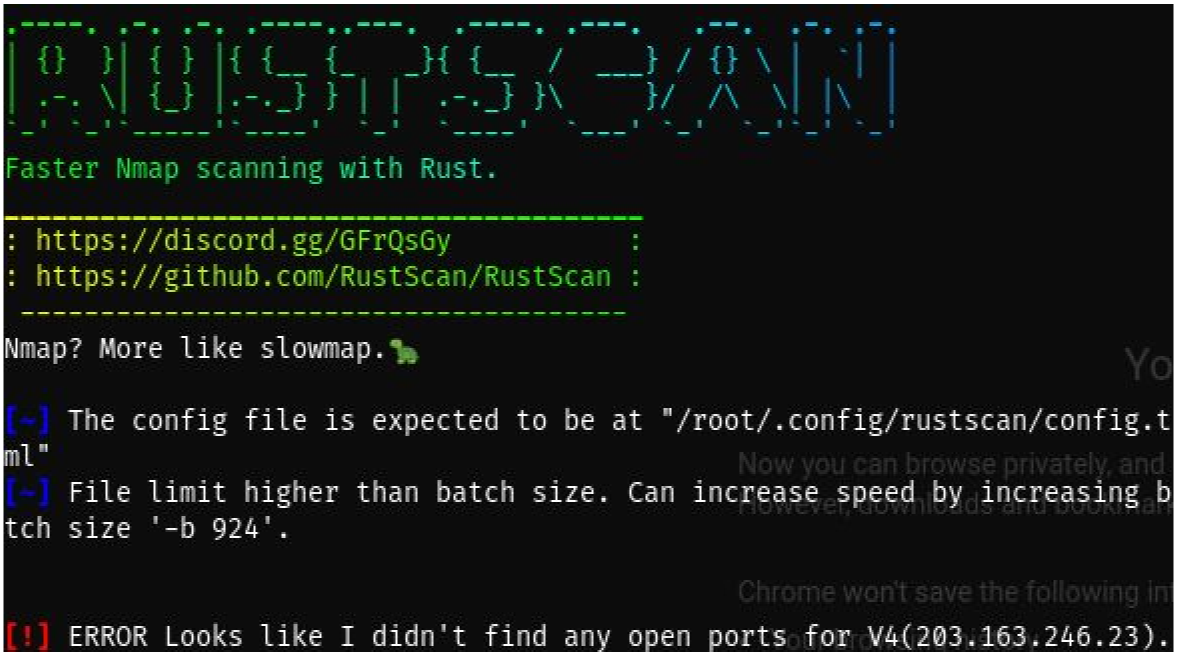
IP Address	Country	Region	City
50.16.170.116	United States 🇺🇸	Virginia	Virginia Beach
ISP	**Organization**	**Latitude**	**Longitude**
Amazon.com, Inc.	Amazon Data Services NoVa (amazon.com)	36.6224	-76.0249

Geolocation data from DB-IP (Product: Full, 2020-8-1)

IP Address	Country	Region	City
50.16.170.116	United States 🇺🇸	Virginia	Ashburn
ISP	**Organization**	**Latitude**	**Longitude**
Amazon.com, Inc.	Amazon.com, Inc.	39.0438	-77.4874

Q 3. Scan and find out port numbers open 203.163.246.23

Answer 3:



```
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
Faster Nmap scanning with Rust.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/root/.config/rustscan/config.t
ml"
[~] File limit higher than batch size. Can increase speed by increasing b
tch size '-b 924'.


[!] ERROR Looks like I didn't find any open ports for V4(203.163.246.23).
```

No ports open or the host is down

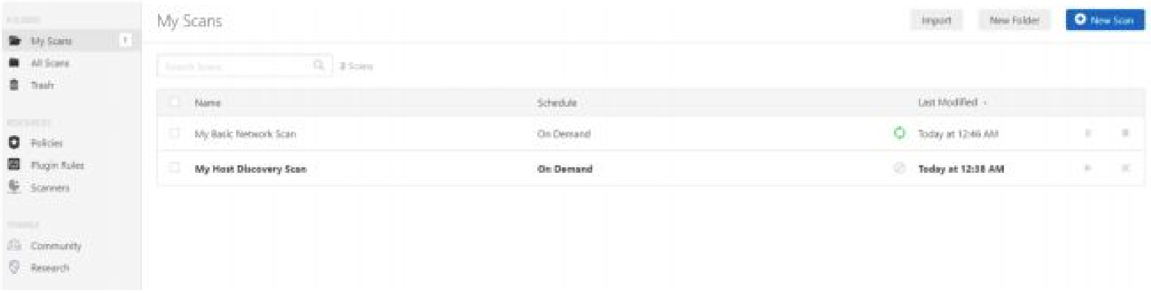
Q 4. Install Nessus in a VM and scan your laptop/desktop for CVE

Answer 4:

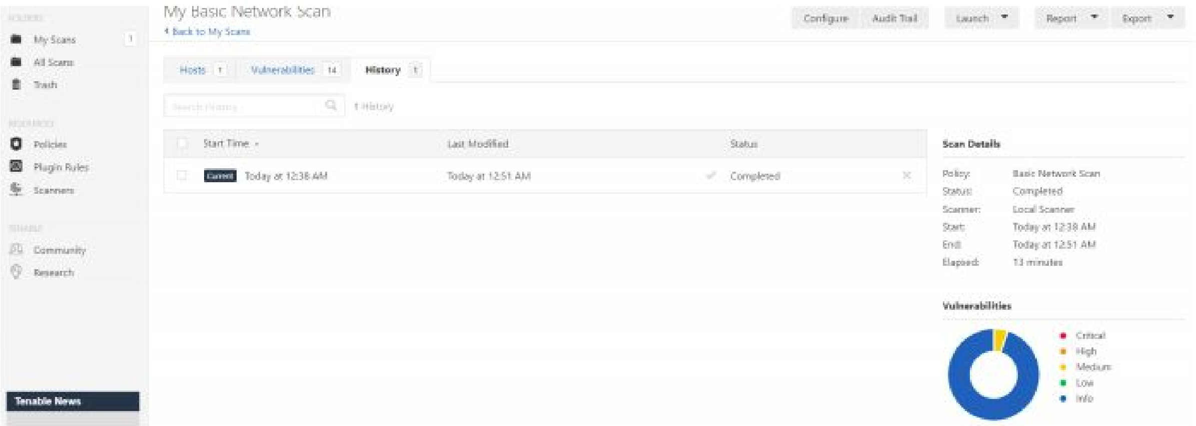
Step 1: Open Pentester-Win 2016 VM and install Nessus in it and open it in a suitable browser. Step 2: Enter the Ipv4 address of your machine in the popup box and start Scanning.

Step 3: The scan is now running. Wait for few seconds until the scan is over.

Step 4: Once the Scan is over, we can see the reports. (Click the Vulnerabilities tab to view the reports)



Name	Schedule	Last Modified
My Basic Network Scan	On Demand	Today at 12:46 AM
My Host Discovery Scan	**On Demand**	**Today at 12:38 AM**



Start Time	Last Modified	Status
Current Today at 12:38 AM	Today at 12:51 AM	Completed

Scan Details

Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 12:38 AM
End: Today at 12:51 AM
Elapsed: 13 minutes