

LetsUpgrade

Cyber Security Essentials

Day 4 Assignment

Darshan

+91 7022086560

darshanbangera1612@gmail.com

1. Finding mail servers of the domains :

- **ibm.com**
- **wipro.com**

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Acer>nslookup
Default Server: UnKnown
Address: 192.168.1.1

> set type=mx
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com
> wipro.com
Server: UnKnown
Address: 192.168.1.1

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

wipro.com nameserver = ns3.webindia.com
wipro.com nameserver = ns1.webindia.com
wipro.com nameserver = ns2.webindia.com
>
```

2.a. Finding location of the mail server of ibm.com :

Nessus Professional / Folders / \ | My Basic Network Scan | eMailTrackerPro Report | +

File | C:/Users/Administrator/eMailTrackerPro/V8/reports/report-20200827-2005-1.html

eMailTrackerPro® Report

[How to Report Email Abuse](#) | [eMailTrackerPro Manual](#) | [FAQ](#) | [Visualware Home](#) | [eMailTrackerPro Website](#) | [Purchase eMailTrackerPro](#)

Identification Report for 148.163.156.1

You are on day 2 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to [purchase a product license](#) from the Visualware website or authorized reseller.

Emails from 148.163.156.1 are passed to the server identified on the Internet by **148.163.156.1**. This report details that server, which is probably owned or maintained by the sender's company or Internet service provider. If you would like information on the computer on which the email was actually composed, then use eMailTrackerPro's Advanced Email Trace facility).

Note that email addresses are very easy to fake. If you have received a spam or scam email pertaining to be from 148.163.156.1, then it almost certainly does not come from that address. You can find the real source of the email using the Advanced Email Trace facility.

Computer **148.163.156.1** has been found. It is almost certainly located in **Sunnyvale, California, USA** as it has an exact match in the eMailTrackerPro database.

This system is a mail server (click [here](#) for details).

Network Contact Information: The following details refer to the network that the system is on.

Proofpoint, Inc.
 abuse@proofpoint.com
 +1-801-748-4494
 892 Ross Drive Sunnyvale CA 94089 US

[Click here to hide the route map](#) ([more info](#))


The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.

Nessus Professional / Folders / \ | My Basic Network Scan | eMailTrackerPro Report | +

File | C:/Users/Administrator/eMailTrackerPro/V8/reports/report-20200827-2005-1.html

[Click here to hide the route map](#) ([more info](#))

The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.



[Click here to hide information on each hop along the route](#) ([more info](#))

The table below identifies the Internet route taken to reach the destination requested.

This is valuable data when tracking the end location because it helps qualify the actual final position. In some instances the final location has been derived from the network registration details, which is often the head office location for the Internet Service Provider (ISP). The ISP location is often local to the destination traced, but sometimes also located elsewhere, particularly in the case of large national ISPs. The physical (authoritative) locations of systems in last 2 or 3 hops of the route provide helpful location information as they are often in the vicinity of the destination being traced. Authoritative locations are shown in **bold**. Locations derived from registration details appear in *italic*.

Address of Hop	Name of Hop	Location
192.168.		(Private)
-	(unnamed)	
148.163.156.1	mx0a-001b2d01.pphosted.com	Sunnyvale, California, USA

2.b. Finding location of the mail server of wipro.com :

Nessus Professional / Folders / \ X | My Basic Network Scan X | eMailTrackerPro Report X | eMailTrackerPro Report X +

File | C:/Users/Administrator/eMailTrackerPro/V8/reports/report-20200827-2004-0.html

eMailTrackerPro® Report

[How to Report Email Abuse](#) | [eMailTrackerPro Manual](#) | [FAQ](#) | [Visualware Home](#) | [eMailTrackerPro Website](#) | [Purchase eMailTrackerPro](#)

Identification Report for 104.47.125.36

You are on day 2 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to [purchase a product license](#) from the Visualware website or authorized reseller.

Emails from 104.47.125.36 are passed to the server identified on the Internet by **104.47.125.36**. This report details that server, which is probably owned or maintained by the sender's company or Internet service provider. If you would like information on the computer on which the email was actually composed, then use eMailTrackerPro's Advanced Email Trace facility).

Note that email addresses are very easy to fake. If you have received a spam or scam email pertaining to be from 104.47.125.36, then it almost certainly does not come from that address. You can find the real source of the email using the Advanced Email Trace facility.

Computer **104.47.125.36** has been found. It is almost certainly located in **Singapore, Singapore** as it has an exact match in the eMailTrackerPro database.


This system is a mail server (click [here](#) for details).

Network Contact Information: The following details refer to the network that the system is on.

see <http://www.iana.org>.


[Click here to hide the route map \(more info\)](#)

The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.



Nessus Professional / Folders / \ X | My Basic Network Scan X | eMailTrackerPro Report X | eMailTrackerPro Report X +

File | C:/Users/Administrator/eMailTrackerPro/V8/reports/report-20200827-2004-0.html



[Click here to hide information on each hop along the route \(more info\)](#)

The table below identifies the Internet route taken to reach the destination requested.

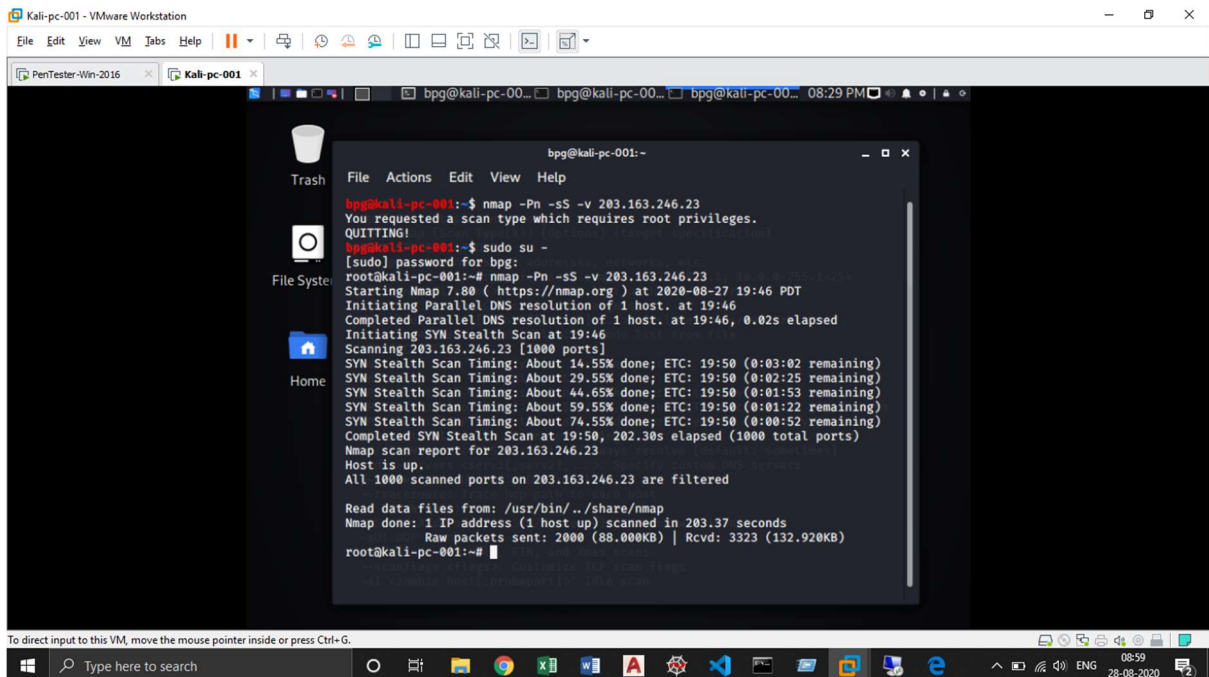
This is valuable data when tracking the end location because it helps qualify the actual final position. In some instances the final location has been derived from the network registration details, which is often the head office location for the Internet Service Provider (ISP). The ISP location is often local to the destination traced, but sometimes also located elsewhere, particularly in the case of large national ISPs. The physical (authoritative) locations of systems in last 2 or 3 hops of the route provide helpful location information as they are often in the vicinity of the destination being traced. Authoritative locations are shown in **bold**, locations derived from registration details appear in *italic*.

Address of Hop	Name of Hop	Location
192.168.		(Private)
-	(unnamed)	
104.47.125.36	mail-sg2apc010036.inbound.protection.outlook.com	Singapore, Singapore

[Click here to hide further owner details \(more info\)](#)

Network Owner Information	Domain Owner Information
The following information refers to the network on which this system lies. This is useful information.	

3. Finding open port numbers in 203.163.246.23 using NMAP:



```
bpg@kali-pc-001: ~  
File Actions Edit View Help  
bpg@kali-pc-001:~$ nmap -Pn -sS -v 203.163.246.23  
You requested a scan type which requires root privileges.  
QUITTING!  
bpg@kali-pc-001:~$ sudo su -  
[sudo] password for bpg:  
root@kali-pc-001:~# nmap -Pn -sS -v 203.163.246.23  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 19:46 PDT  
Initiating Parallel DNS resolution of 1 host. at 19:46  
Completed Parallel DNS resolution of 1 host. at 19:46, 0.02s elapsed  
Initiating SYN Stealth Scan at 19:46  
Scanning 203.163.246.23 [1000 ports]  
SYN Stealth Scan Timing: About 14.55% done; ETC: 19:50 (0:03:02 remaining)  
SYN Stealth Scan Timing: About 29.55% done; ETC: 19:50 (0:02:25 remaining)  
SYN Stealth Scan Timing: About 44.65% done; ETC: 19:50 (0:01:53 remaining)  
SYN Stealth Scan Timing: About 59.55% done; ETC: 19:50 (0:01:22 remaining)  
SYN Stealth Scan Timing: About 74.55% done; ETC: 19:50 (0:00:52 remaining)  
Completed SYN Stealth Scan at 19:50, 202.30s elapsed (1000 total ports)  
Nmap scan report for 203.163.246.23  
Host is up.  
All 1000 scanned ports on 203.163.246.23 are filtered  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 203.37 seconds  
Raw packets sent: 2000 (88.000KB) | Rcvd: 3323 (132.920KB)  
root@kali-pc-001:~#
```

4. Installing Nessus in VM and scanning vulnerabilities :

