Lets Upgrade

Cyber Security | August 2020

Assignment Day 4 |

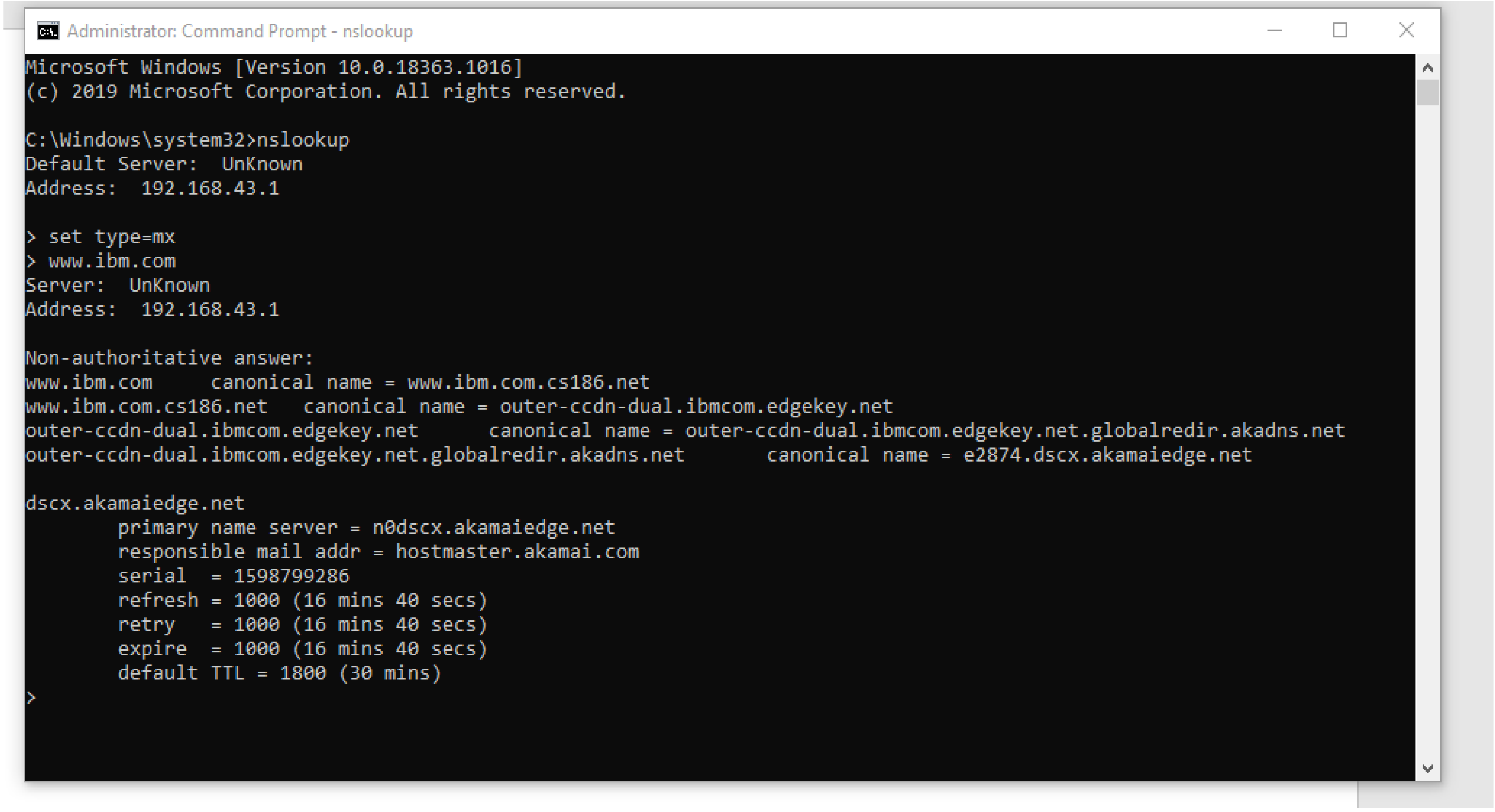
Name - Pritam Biswas **Emal id - pritambiswas1452@gmail.com**

Question 1:

Find out the mail servers of the following domain :
Ibm.com
Wipro.com

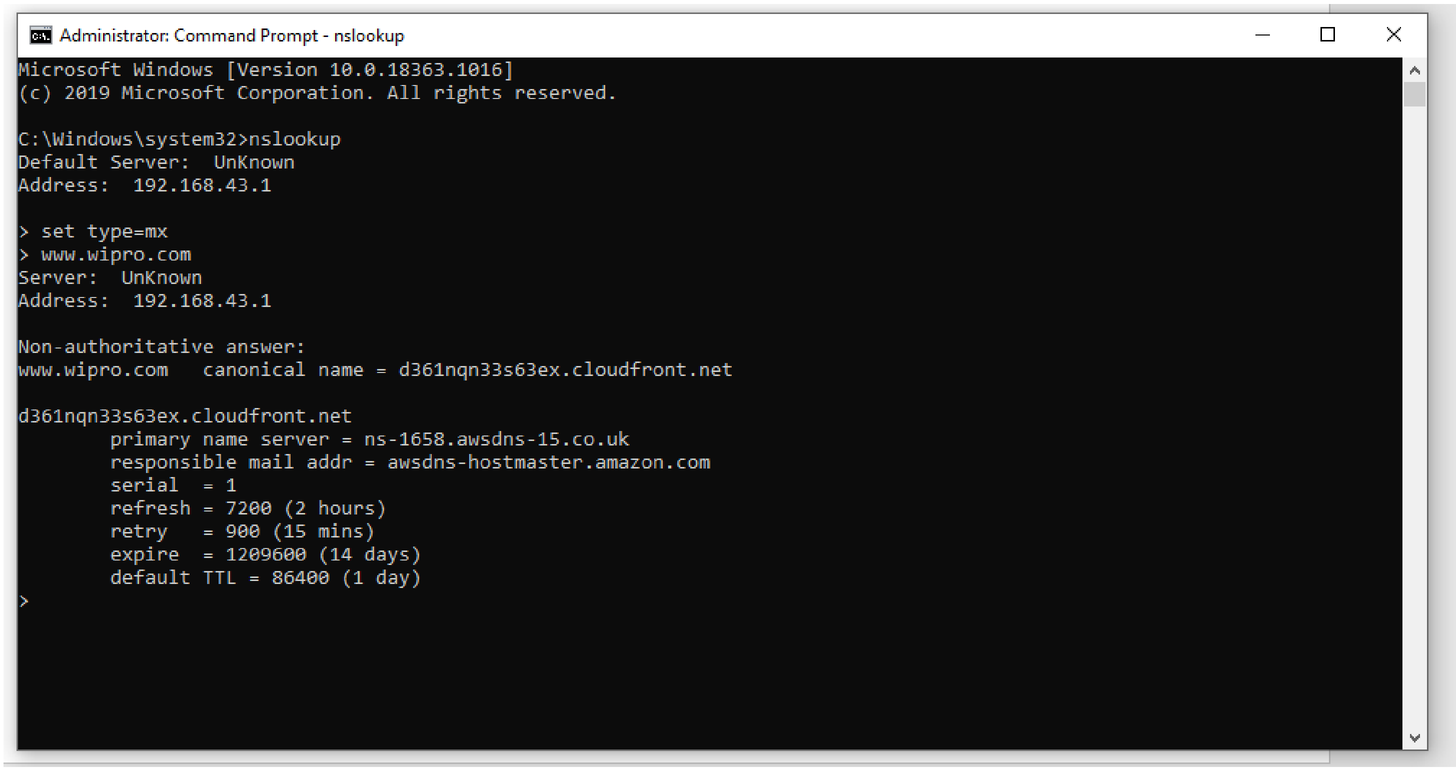
Solutions:

1.www.imb.com



```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> set type=mx
> www.ibm.com
Server:  UnKnown
Address:  192.168.43.1

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

dscx.akamaiedge.net
        primary name server = n0dscx.akamaiedge.net
        responsible mail addr = hostmaster.akamai.com
        serial  = 1598799286
        refresh = 1000 (16 mins 40 secs)
        retry   = 1000 (16 mins 40 secs)
        expire  = 1000 (16 mins 40 secs)
        default TTL = 1800 (30 mins)
>
```

2.www.wipro.com

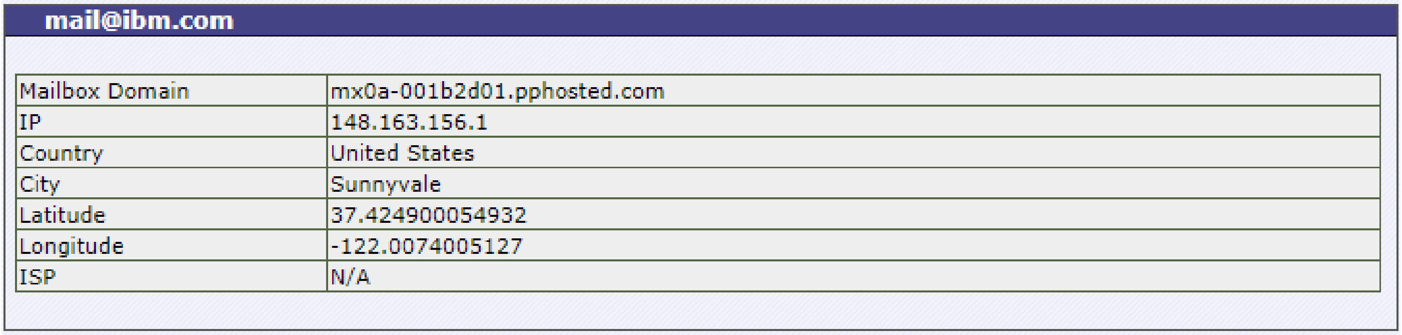


```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> set type=mx
> www.wipro.com
Server:  UnKnown
Address:  192.168.43.1

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

d361nqn33s63ex.cloudfront.net
        primary name server = ns-1658.awsdns-15.co.uk
        responsible mail addr = awsdns-hostmaster.amazon.com
        serial  = 1
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 86400 (1 day)
>
```

Question 2:

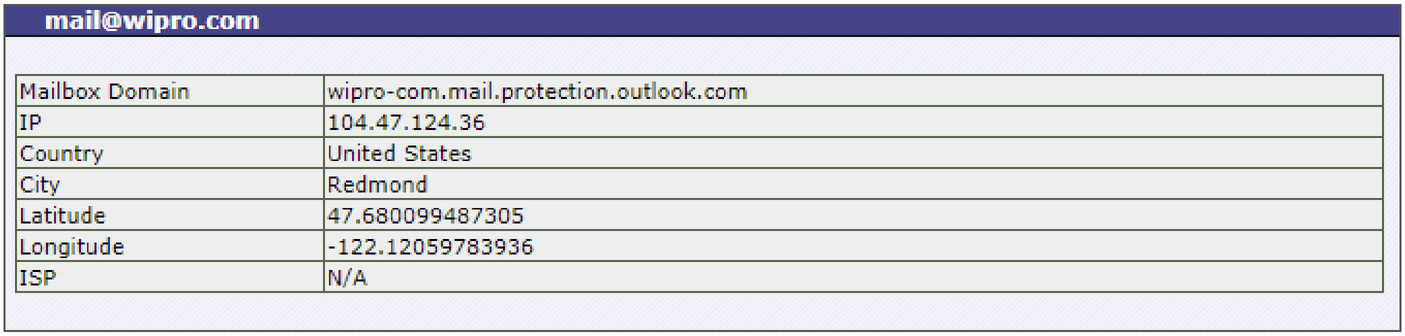
Find the locations, where these email servers are hosted.

Solutions:



mail@ibm.com

Mailbox Domain	mx0a-001b2d01.pphosted.com
IP	148.163.156.1
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

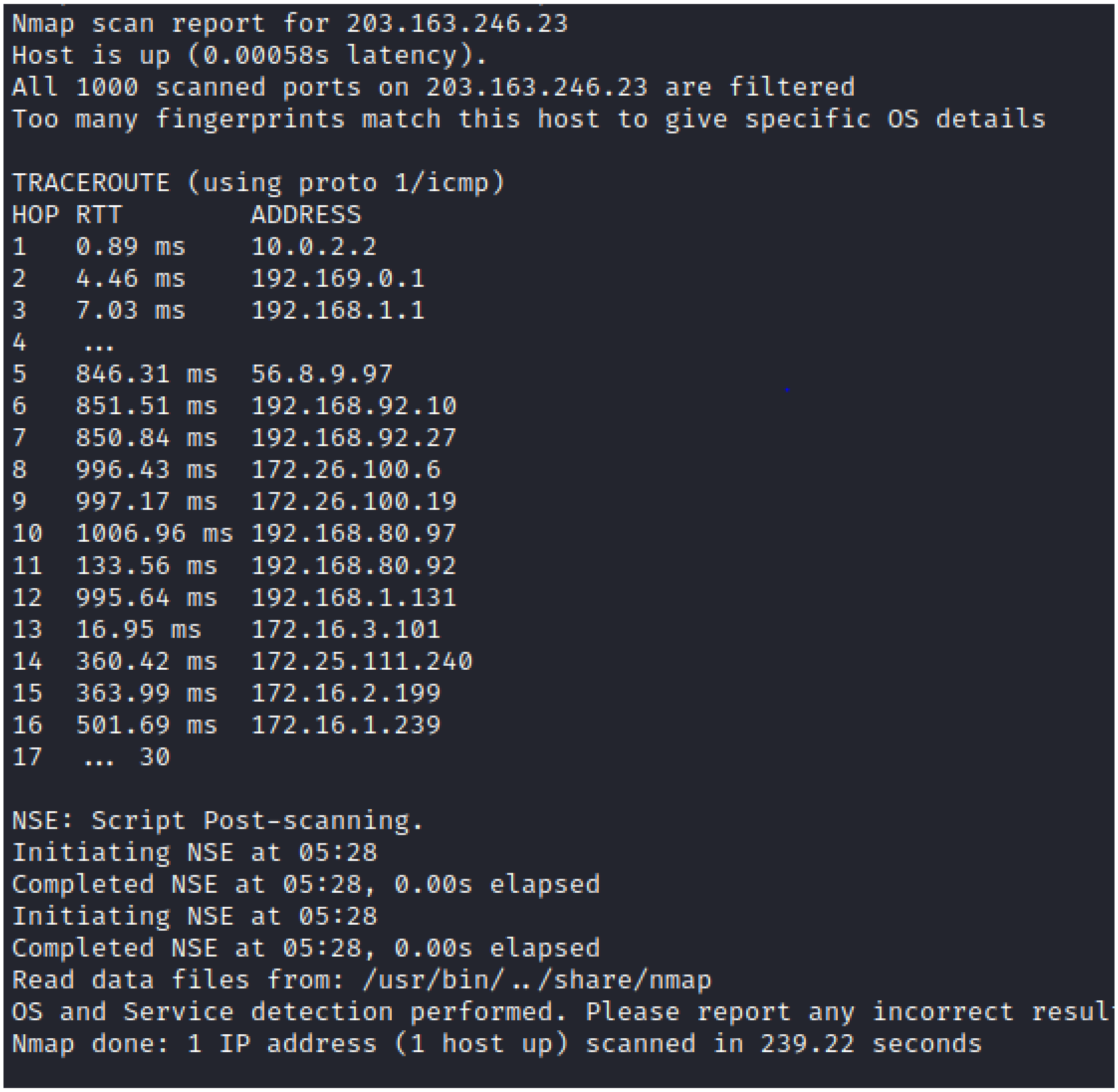


mail@wipro.com

Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.124.36
Country	United States
City	Redmond
Latitude	47.680099487305
Longitude	-122.12059783936
ISP	N/A

Question 3:

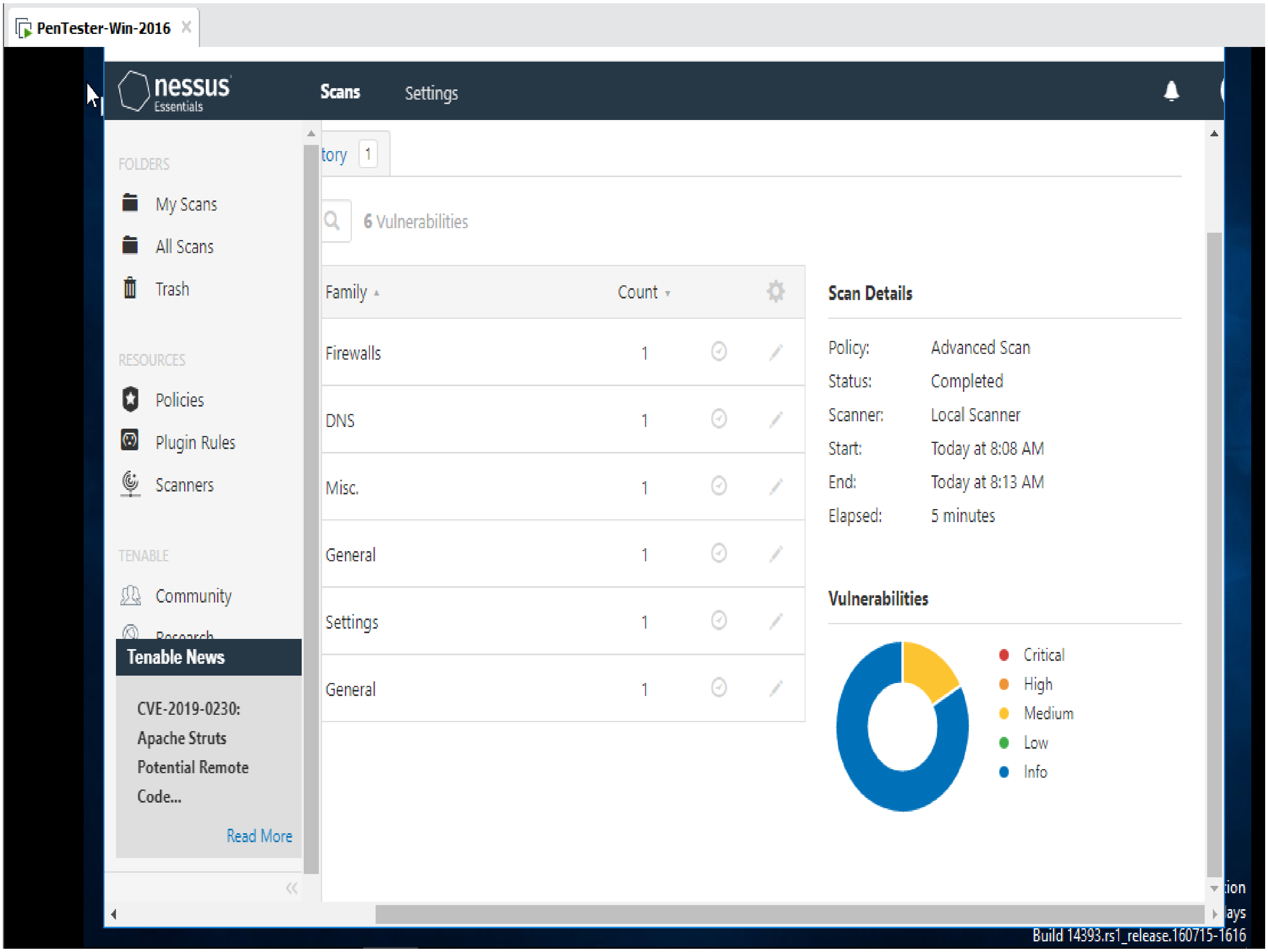
Scan and find out port numbers open 203.163.246.23



```
Nmap scan report for 203.163.246.23
Host is up (0.00058s latency).
All 1000 scanned ports on 203.163.246.23 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT         ADDRESS
1   0.89 ms     10.0.2.2
2   4.46 ms     192.169.0.1
3   7.03 ms     192.168.1.1
4    ...
5   846.31 ms   56.8.9.97
6   851.51 ms   192.168.92.10
7   850.84 ms   192.168.92.27
8   996.43 ms   172.26.100.6
9   997.17 ms   172.26.100.19
10  1006.96 ms 192.168.80.97
11  133.56 ms   192.168.80.92
12  995.64 ms   192.168.1.131
13  16.95 ms    172.16.3.101
14  360.42 ms   172.25.111.240
15  363.99 ms   172.16.2.199
16  501.69 ms   172.16.1.239
17   ... 30

NSE: Script Post-scanning.
Initiating NSE at 05:28
Completed NSE at 05:28, 0.00s elapsed
Initiating NSE at 05:28
Completed NSE at 05:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect resul
Nmap done: 1 IP address (1 host up) scanned in 239.22 seconds
```

Question 4:

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



Tenable News

CVE-2019-0230: Apache Struts Potential Remote Code...

6 Vulnerabilities

Family ▲	Count ▾
Firewalls	1
DNS	1
Misc.	1
General	1
Settings	1
General	1

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 8:08 AM
End:	Today at 8:13 AM
Elapsed:	5 minutes

Vulnerabilities

Build 14393.rs1_release.160715-1616