Task 1: Obtain a scanning report of the entire network and identify how many terminals are connected with the Windows operating system and the Linux-based systems

we need to connect to a kali virtual machine and enter the credentials and login and then

Open the command prompt and enter

Ifconfig

Nmap -sn 10.10.10.0/24

Sudo nmap -ss -A 10.10.10.1

Enter password

And we get the output

There are two terminals connected one is a windows one and the other one is a kali they are

*10.10.10.1

*10.10.10.4

Output screenshots are attached at the end

Task 2: Identify CVE score of the victim's vulnerability.

Open google and enter cvedetails.com and then there select on Windows 10 21h2

And then click on **version 10.0.19045.3087 for x64**. And the screenshots are attached below

---

Task 3: Identify whether the victim's terminal is affected with MiMT attack or not and submit the incident report for the same.

we need to connect to a kali virtual machine and enter the credentials and login and then

Open the command prompt and enter

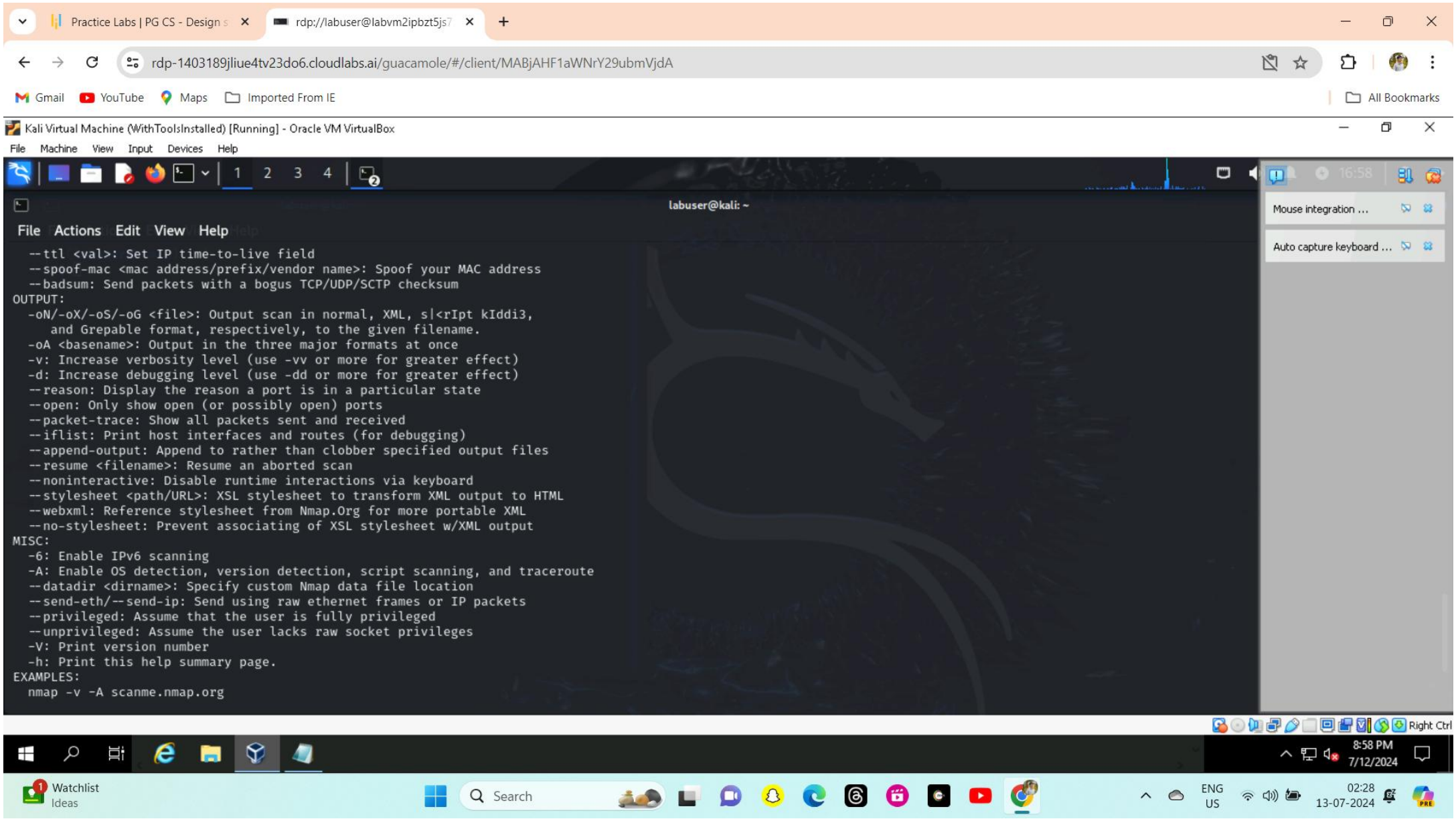
nmap -- script smb-flood.nse -p 445 10.10.10.1

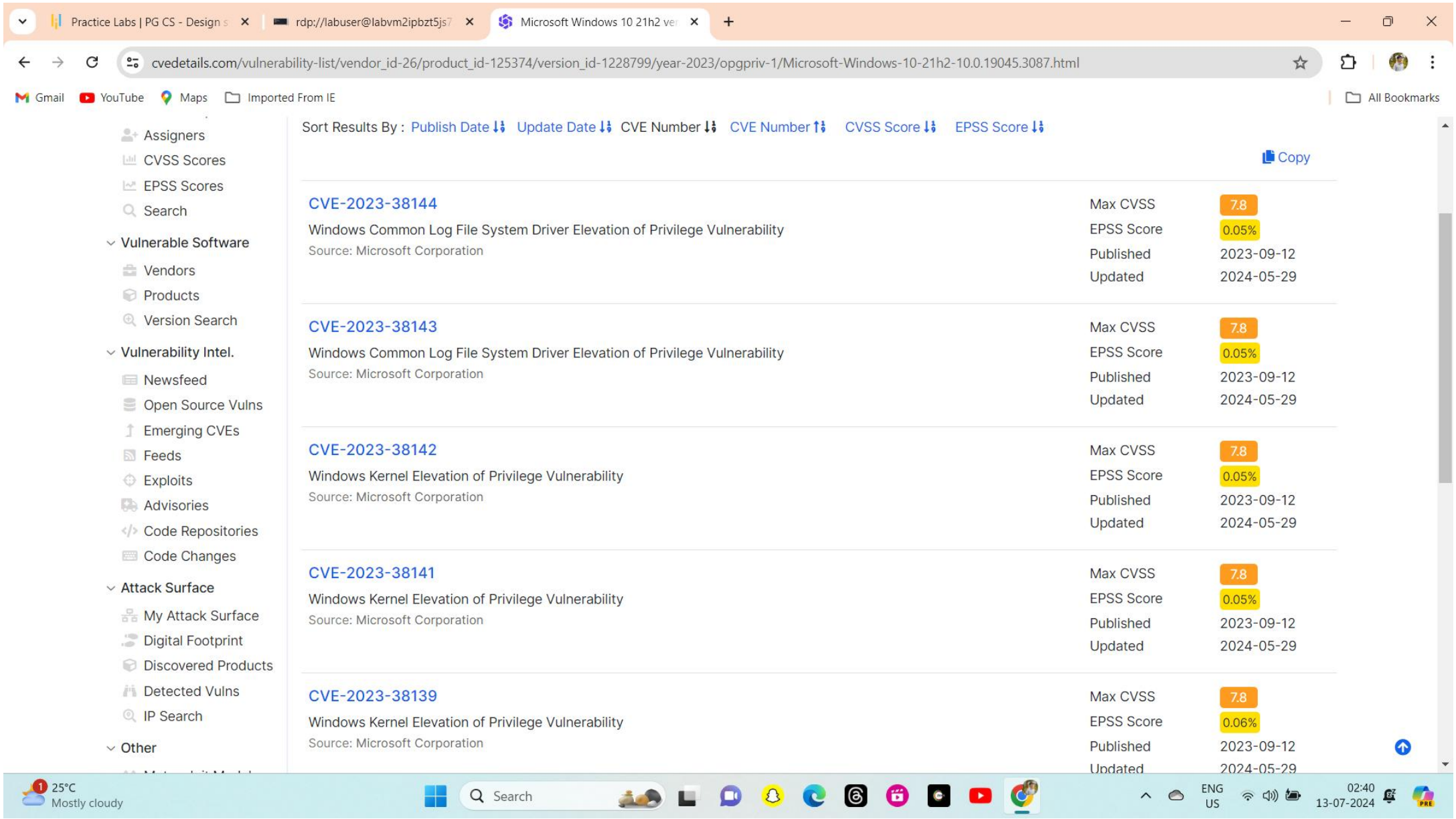
the Denial-of-service attack is successful and output screenshots are attached at the end

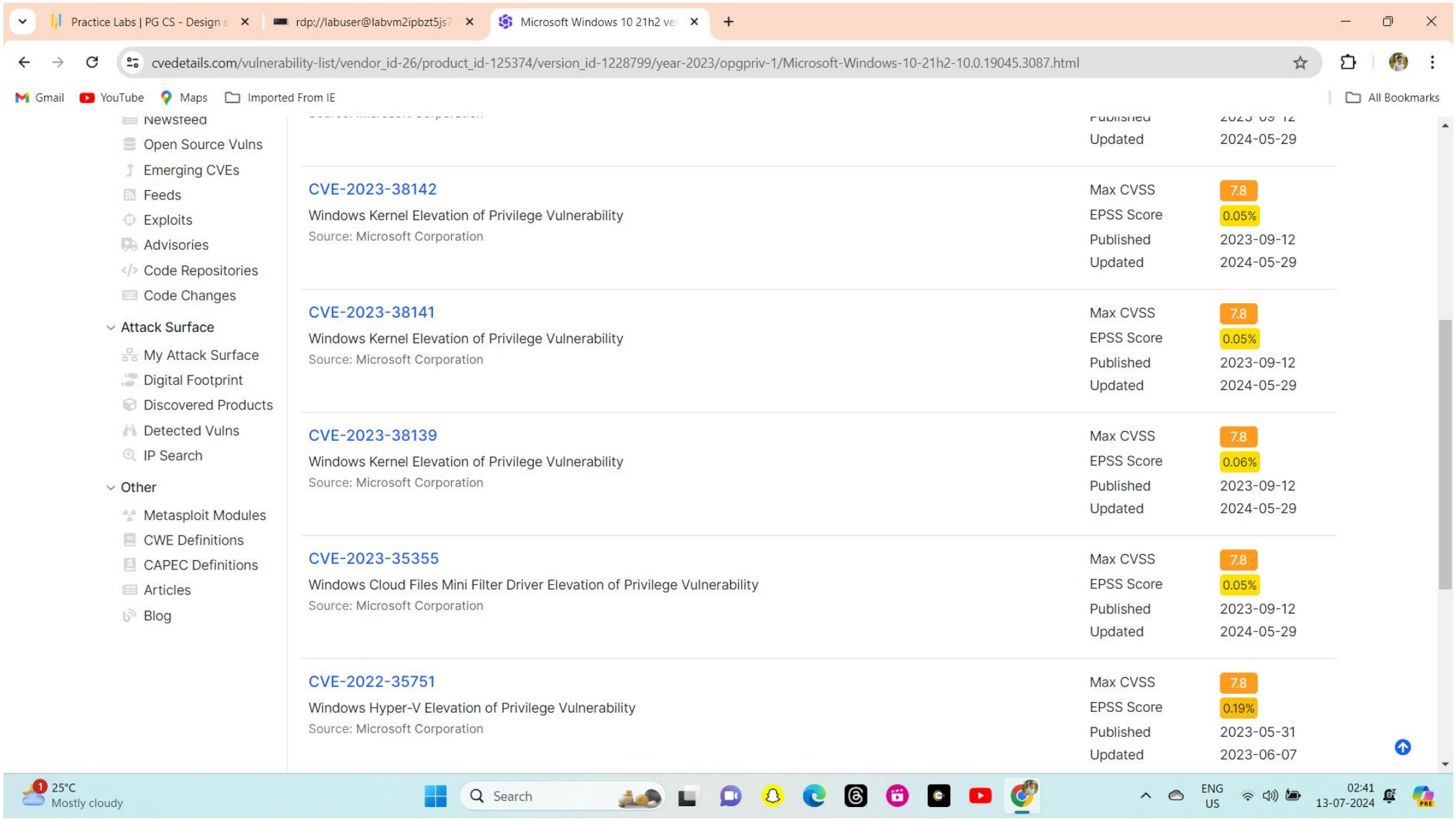
---

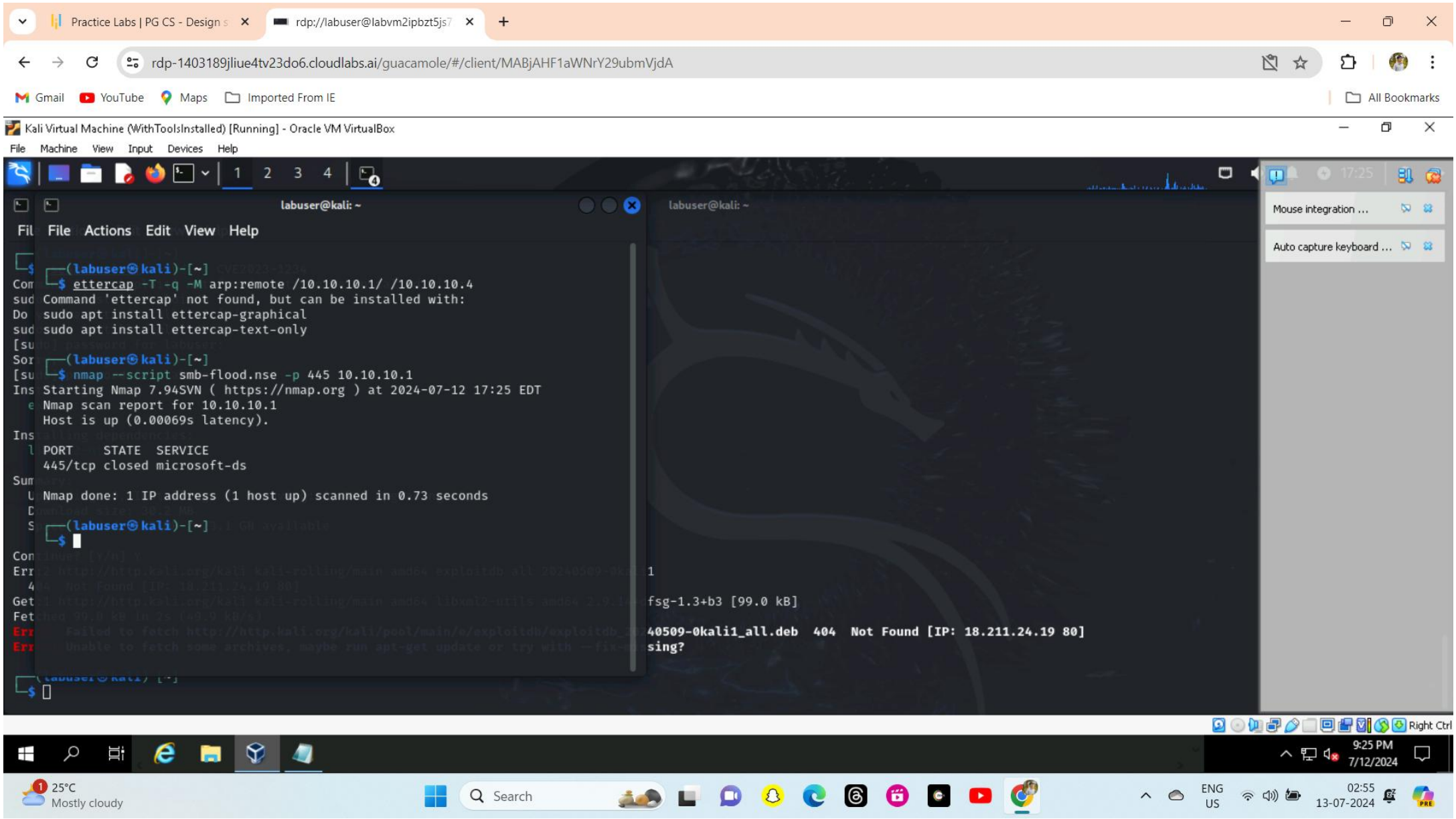
Task 4: Use email forensics analysis and identify the sender's IP address

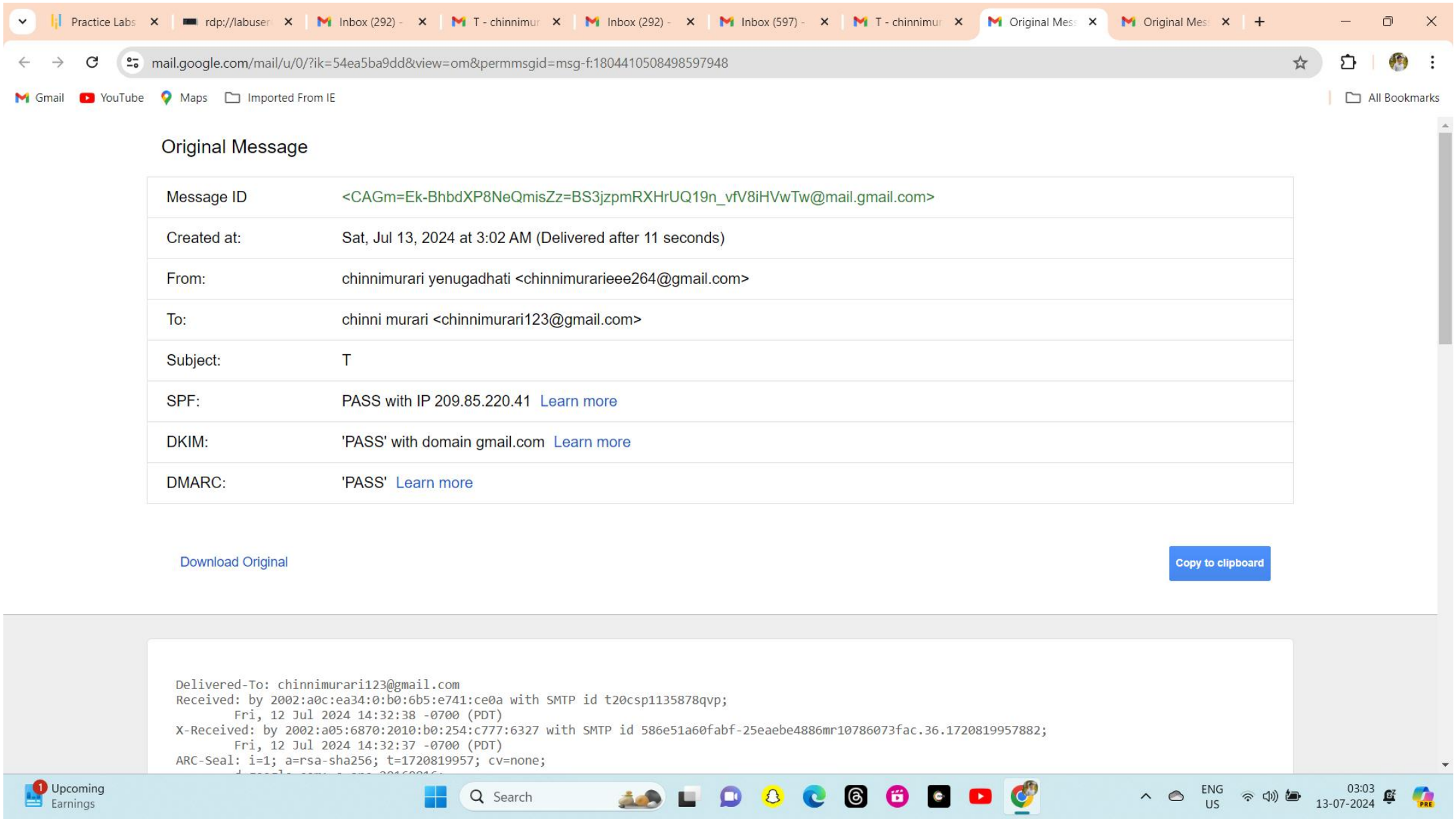
Open Gmail and compose an mail to your other gmail and send it and the open the mail in which it was received and then click on show originals and we can find the IP address and take a screenshots which are attached below.


Practice Labs | PG CS - Design
rdp://labuser@labvm2ipbzt5js7
rdp-1403189jliue4tv23do6.cloudlabs.ai/guacamole/#/client/MABjAHF1aWNrY29ubmVjdA
Gmail
YouTube
Maps
Imported From IE
All Bookmarks
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~
File Actions Edit View Help
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
8:58 PM
7/12/2024
Watchlist
Ideas
Search
ENG
US
02:28
13-07-2024


Practice Labs | PG CS - Design
rdp://labuser@labvm2ipbzt5js7
Microsoft Windows 10 21h2 ver
cvedetails.com/vulnerability-list/vendor_id-26/product_id-125374/version_id-1228799/year-2023/opgpriv-1/Microsoft-Windows-10-21h2-10.0.19045.3087.html
Gmail
YouTube
Maps
Imported From IE
All Bookmarks
Assigners
CVSS Scores
EPSS Scores
Search
Vulnerable Software
Vendors
Products
Version Search
Vulnerability Intel.
Newsfeed
Open Source Vulns
Emerging CVEs
Feeds
Exploits
Advisories
Code Repositories
Code Changes
Attack Surface
My Attack Surface
Digital Footprint
Discovered Products
Detected Vulns
IP Search
Other
Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score
Copy
CVE-2023-38144
Windows Common Log File System Driver Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.05%
Published 2023-09-12
Updated 2024-05-29
CVE-2023-38143
Windows Common Log File System Driver Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.05%
Published 2023-09-12
Updated 2024-05-29
CVE-2023-38142
Windows Kernel Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.05%
Published 2023-09-12
Updated 2024-05-29
CVE-2023-38141
Windows Kernel Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.05%
Published 2023-09-12
Updated 2024-05-29
CVE-2023-38139
Windows Kernel Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.06%
Published 2023-09-12
Updated 2024-05-29
25°C
Mostly cloudy
Search
ENG
US
02:40
13-07-2024


Practice Labs | PG CS - Design
rdp://labuser@labvm2ipbzt5js7
Microsoft Windows 10 21h2 ver
cvedetails.com/vulnerability-list/vendor_id-26/product_id-125374/version_id-1228799/year-2023/opgpriv-1/Microsoft-Windows-10-21h2-10.0.19045.3087.html
Gmail
YouTube
Maps
Imported From IE
All Bookmarks
Newsfeed
Open Source Vulns
Emerging CVEs
Feeds
Exploits
Advisories
Code Repositories
Code Changes
Attack Surface
My Attack Surface
Digital Footprint
Discovered Products
Detected Vulns
IP Search
Other
Metasploit Modules
CWE Definitions
CAPEC Definitions
Articles
Blog
Updated 2024-05-29
CVE-2023-38142
Windows Kernel Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.05%
Published 2023-09-12
Updated 2024-05-29
CVE-2023-38141
Windows Kernel Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.05%
Published 2023-09-12
Updated 2024-05-29
CVE-2023-38139
Windows Kernel Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.06%
Published 2023-09-12
Updated 2024-05-29
CVE-2023-35355
Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.05%
Published 2023-09-12
Updated 2024-05-29
CVE-2022-35751
Windows Hyper-V Elevation of Privilege Vulnerability
Source: Microsoft Corporation
Max CVSS 7.8
EPSS Score 0.19%
Published 2023-05-31
Updated 2023-06-07
25°C
Mostly cloudy
Search
ENG
US
02:41
13-07-2024


Practice Labs | PG CS - Design
rdp://labuser@labvm2ipbzt5js7
rdp-1403189jliue4tv23do6.cloudlabs.ai/guacamole/#/client/MABjAHF1aWNrY29ubmVjdA
Gmail
YouTube
Maps
Imported From IE
All Bookmarks
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~
File Actions Edit View Help
(labuser㉿kali)-[~]
$ ettercap -T -q -M arp:remote /10.10.10.1/ /10.10.10.4
Command 'ettercap' not found, but can be installed with:
sudo apt install ettercap-graphical
sudo apt install ettercap-text-only
(labuser㉿kali)-[~]
$ nmap --script smb-flood.nse -p 445 10.10.10.1
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-12 17:25 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00069s latency).
PORT STATE SERVICE
445/tcp closed microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
(labuser㉿kali)-[~]
$
labuser@kali: ~
Mouse integration ...
Auto capture keyboard ...
fsg-1.3+b3 [99.0 kB]
40509-0kali1_all.deb 404 Not Found [IP: 18.211.24.19 80]
sing?
Right Ctrl
9:25 PM
7/12/2024
25°C
Mostly cloudy
Search
ENG
US
02:55
13-07-2024


Practice Labs
rdp://labuser
Inbox (292) -
T - chinnimur
Inbox (292) -
Inbox (597) -
T - chinnimur
Original Mes
Original Mes
mail.google.com/mail/u/0/?ik=54ea5ba9dd&view=om&permmsgid=msg-f:1804410508498597948
Gmail
YouTube
Maps
Imported From IE
All Bookmarks
Original Message
Message ID
<CAGm=Ek-BhbdXP8NeQmisZz=BS3jzpmRXHrUQ19n_vfV8iHVwTw@mail.gmail.com>
Created at:
Sat, Jul 13, 2024 at 3:02 AM (Delivered after 11 seconds)
From:
chinnimurari yenugadhati <chinnimurarieee264@gmail.com>
To:
chinni murari <chinnimurari123@gmail.com>
Subject:
T
SPF:
PASS with IP 209.85.220.41 Learn more
DKIM:
'PASS' with domain gmail.com Learn more
DMARC:
'PASS' Learn more
Download Original
Copy to clipboard
Delivered-To: chinnimurari123@gmail.com
Received: by 2002:a0c:ea34:0:b0:6b5:e741:ce0a with SMTP id t20csp1135878qvp;
Fri, 12 Jul 2024 14:32:38 -0700 (PDT)
X-Received: by 2002:a05:6870:2010:b0:254:c777:6327 with SMTP id 586e51a60fabf-25eaebe4886mr10786073fac.36.1720819957882;
Fri, 12 Jul 2024 14:32:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1720819957; cv=none;
Upcoming
Earnings
Search
ENG
US
03:03
13-07-2024