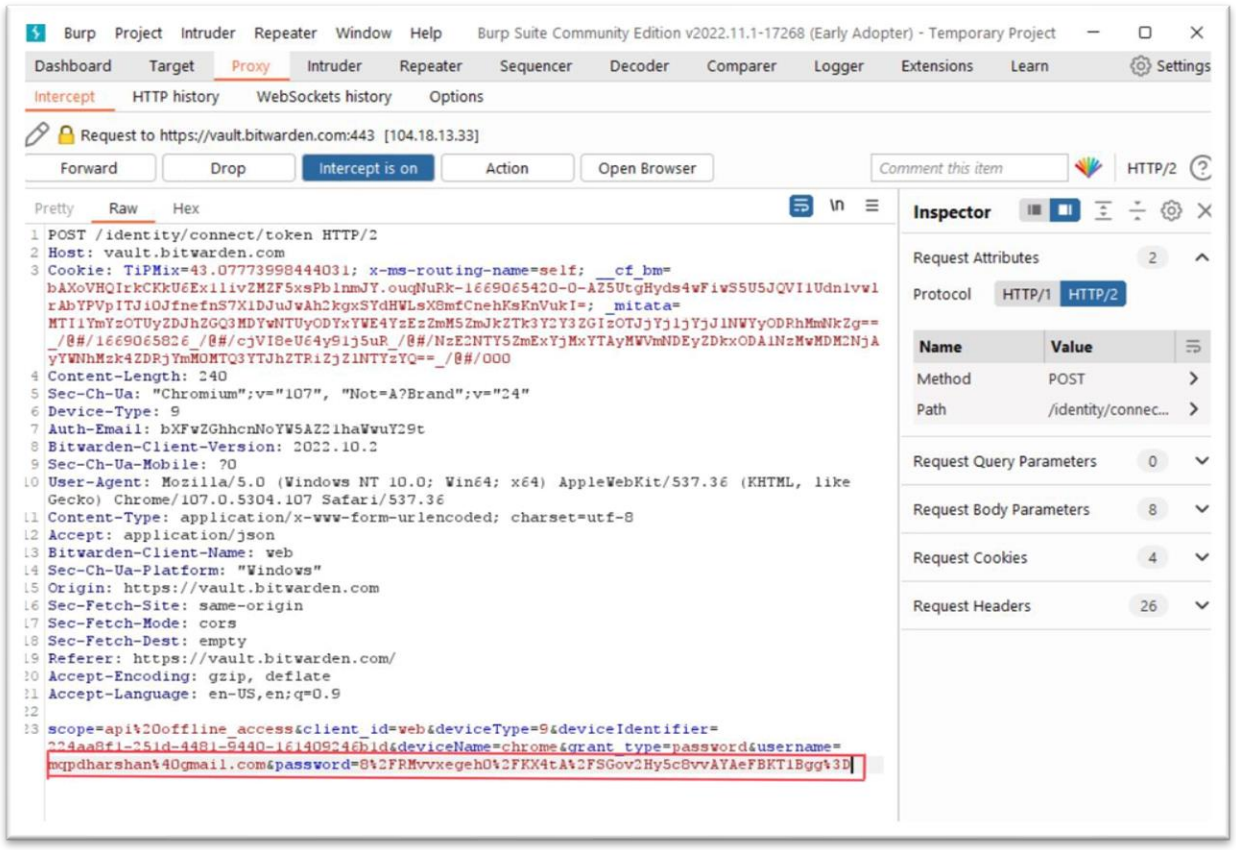
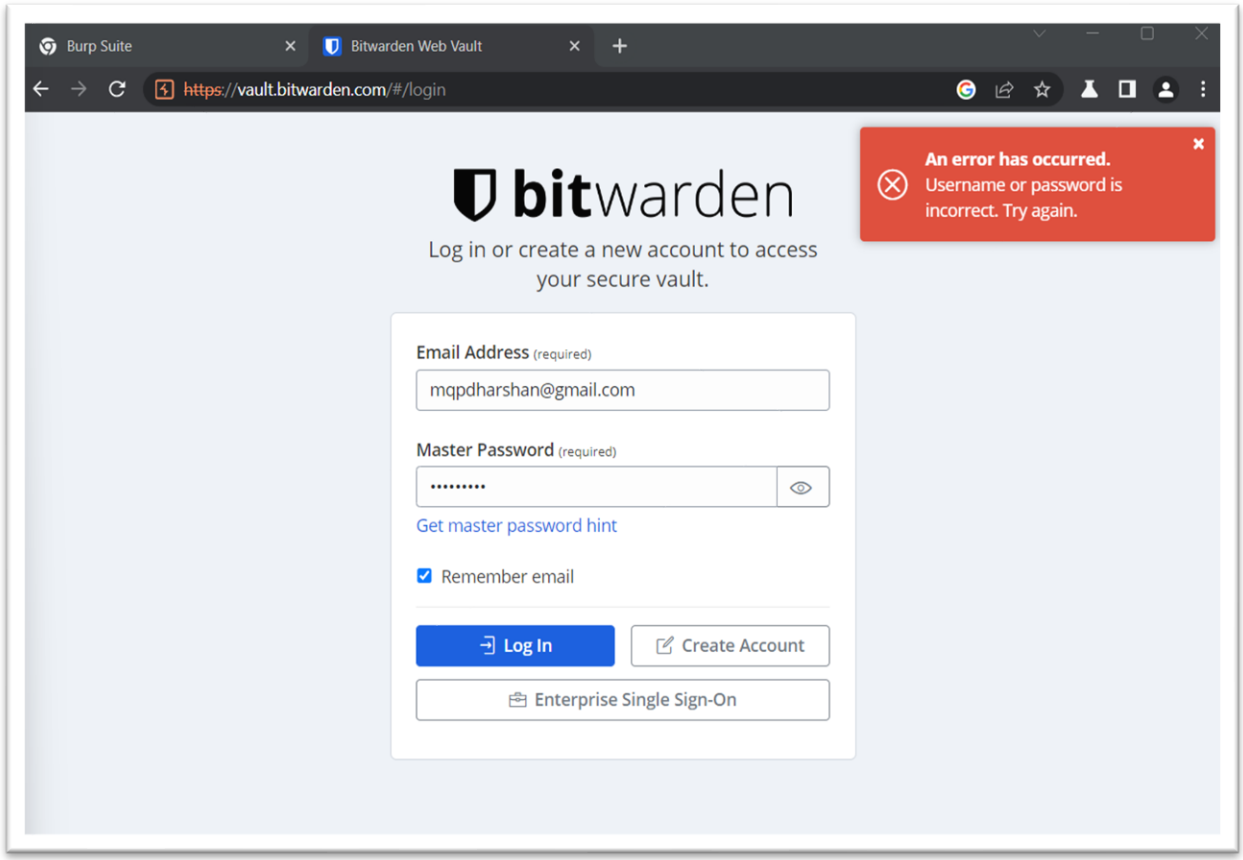
NSE 6120: CRYPTOGRAPHIC PROTOCOLS AND NETWORK SECURITY

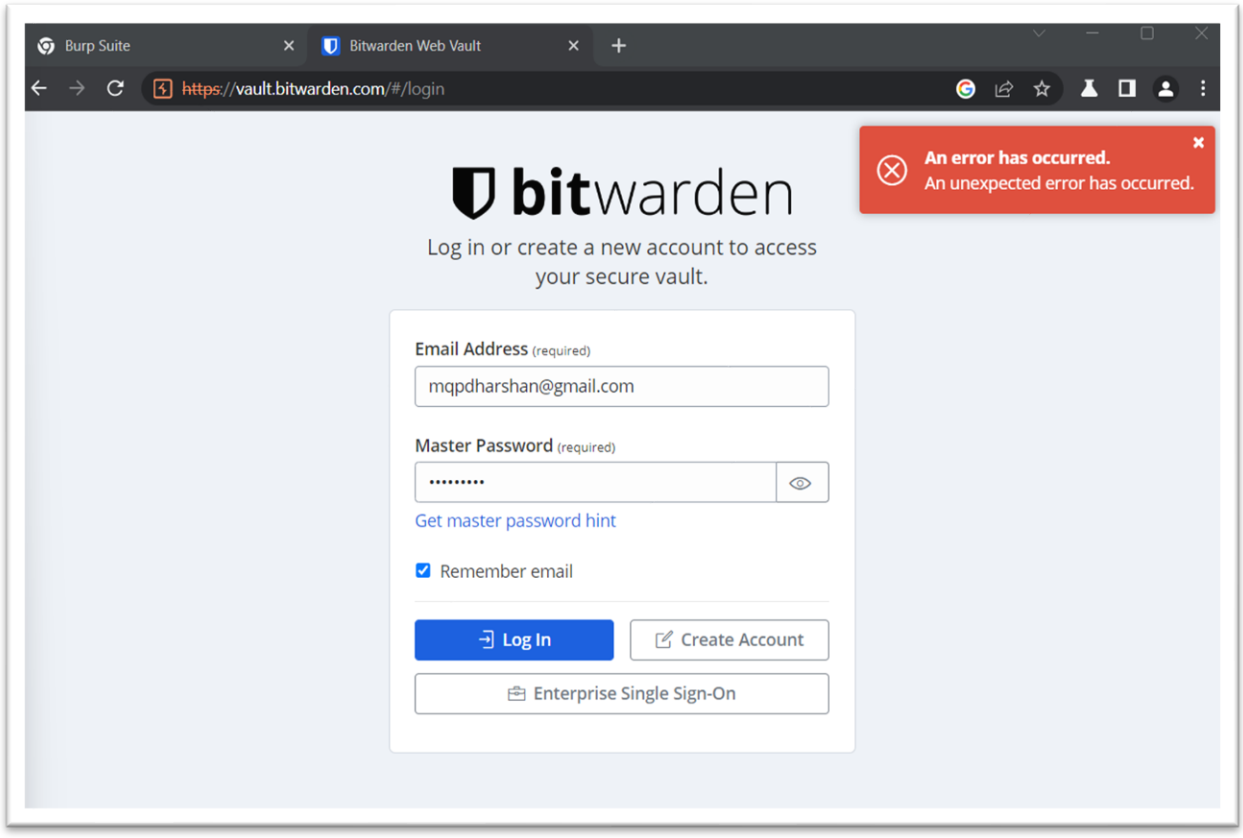
PROJECT REPORT ON PRIVACY AND SECURITY ANALYSIS OF ONLINE PRIVACY VAULTS

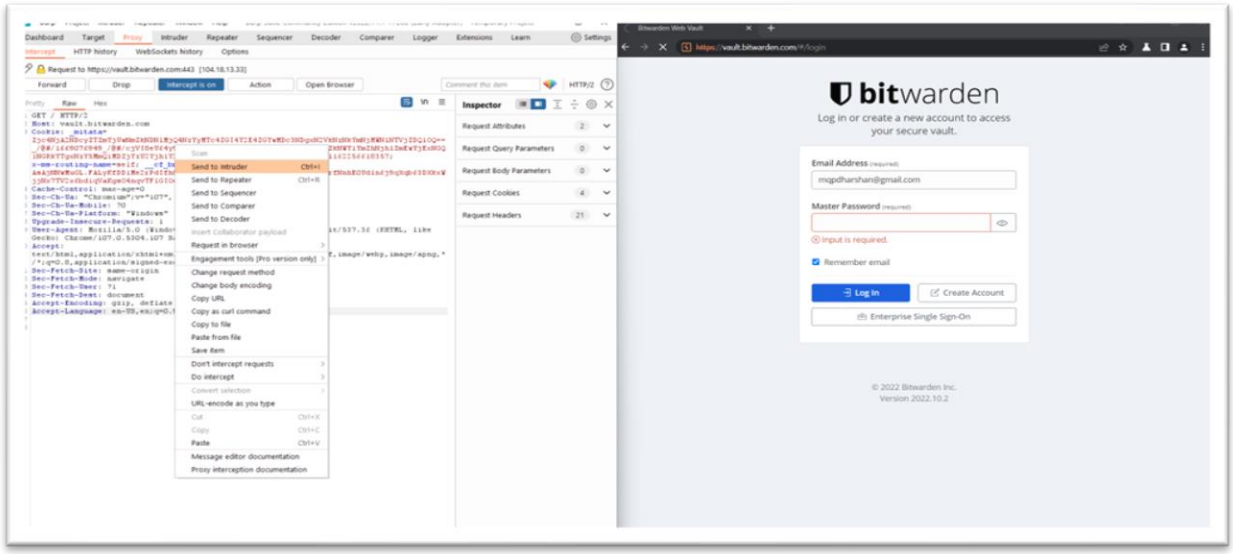
Screenshots:

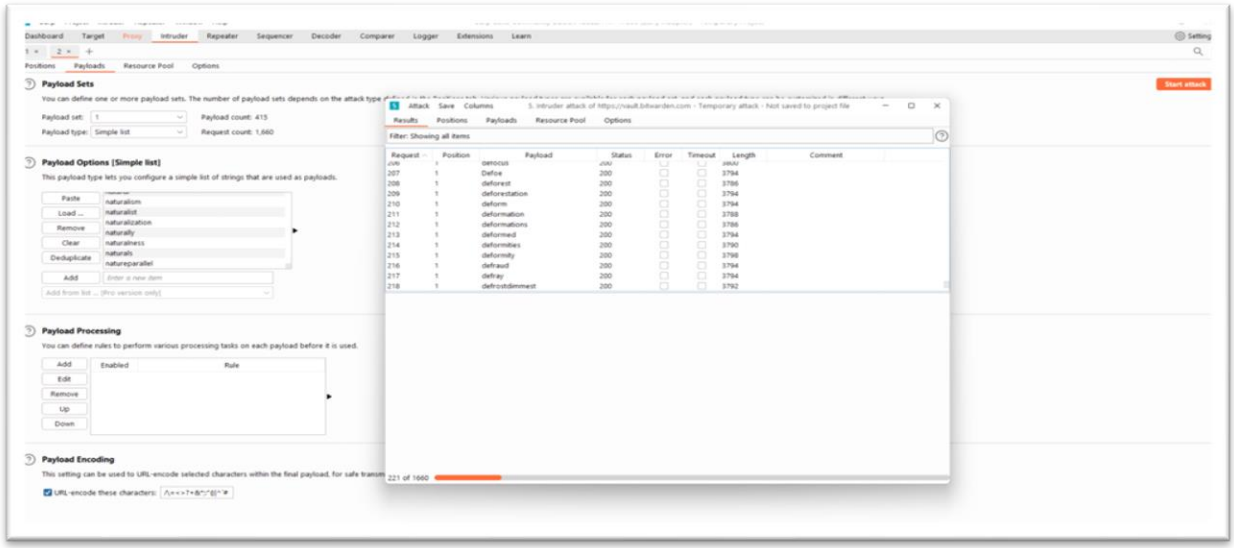
BitWarden:

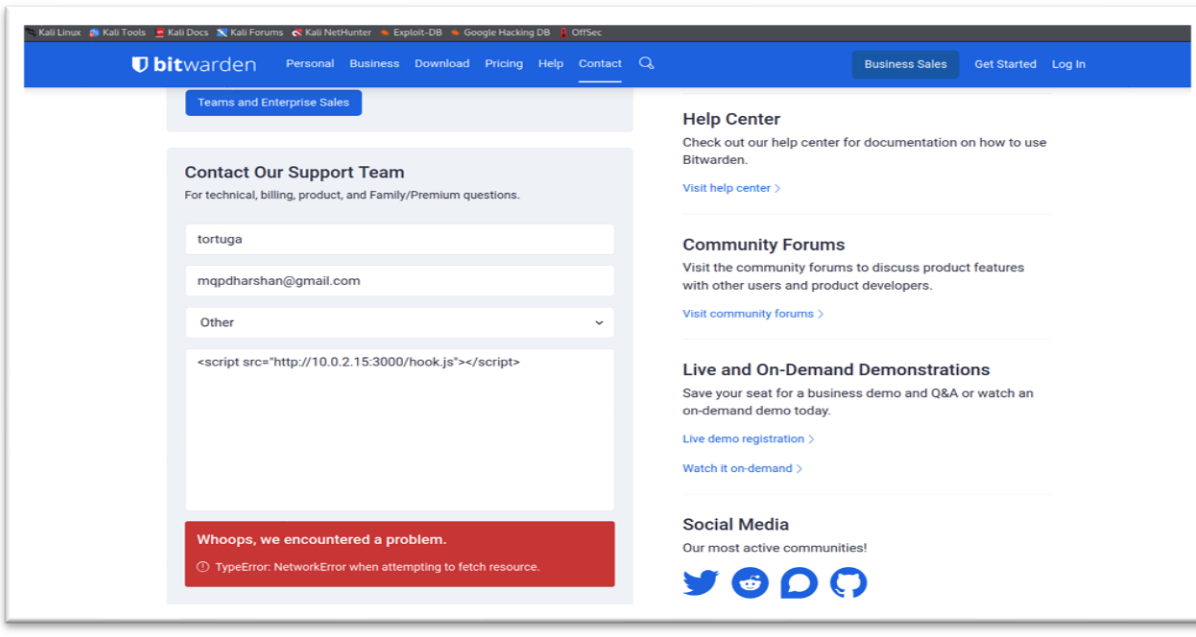



Burp Suite
Bitwarden Web Vault
https://vault.bitwarden.com/#/login
An error has occurred.
Username or password is incorrect. Try again.
bitwarden
Log in or create a new account to access your secure vault.
Email Address (required)
mqpdharshan@gmail.com
Master Password (required)
Get master password hint
Remember email
Log In
Create Account
Enterprise Single Sign-On

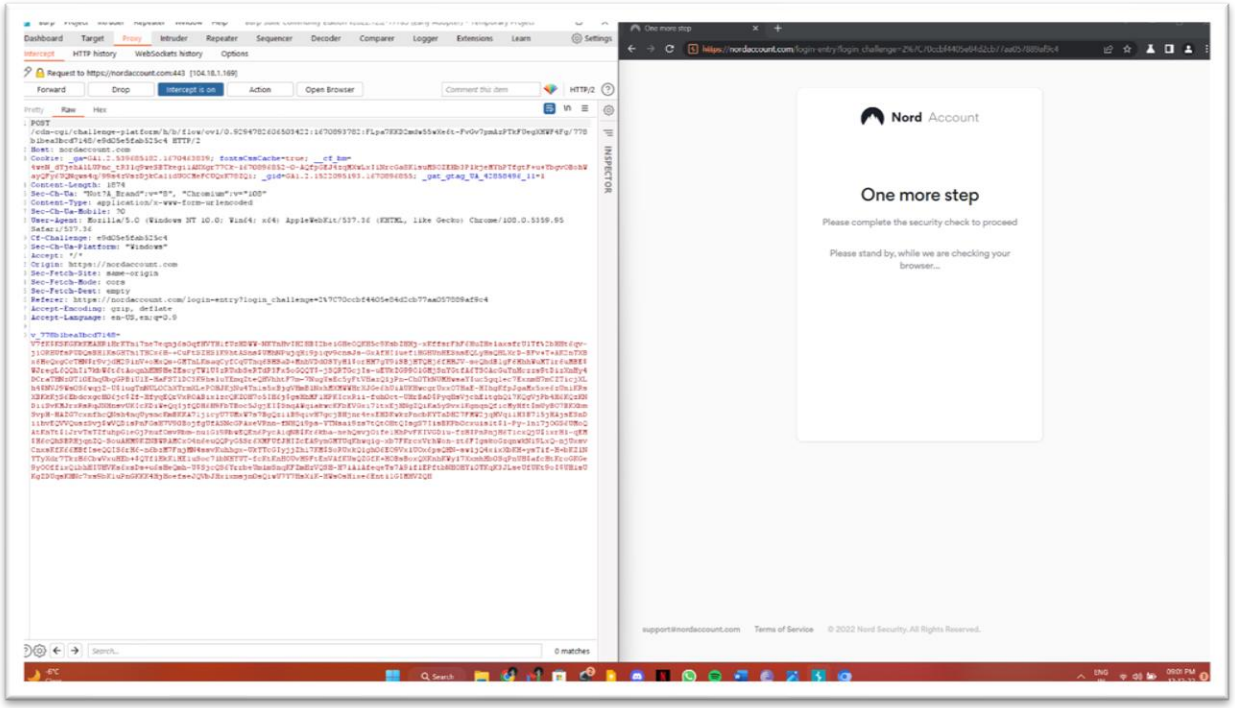

Burp Suite
Bitwarden Web Vault
https://vault.bitwarden.com/#/login
An error has occurred.
An unexpected error has occurred.
bitwarden
Log in or create a new account to access your secure vault.
Email Address (required)
mqpdharshan@gmail.com
Master Password (required)
Get master password hint
Remember email
Log In
Create Account
Enterprise Single Sign-On

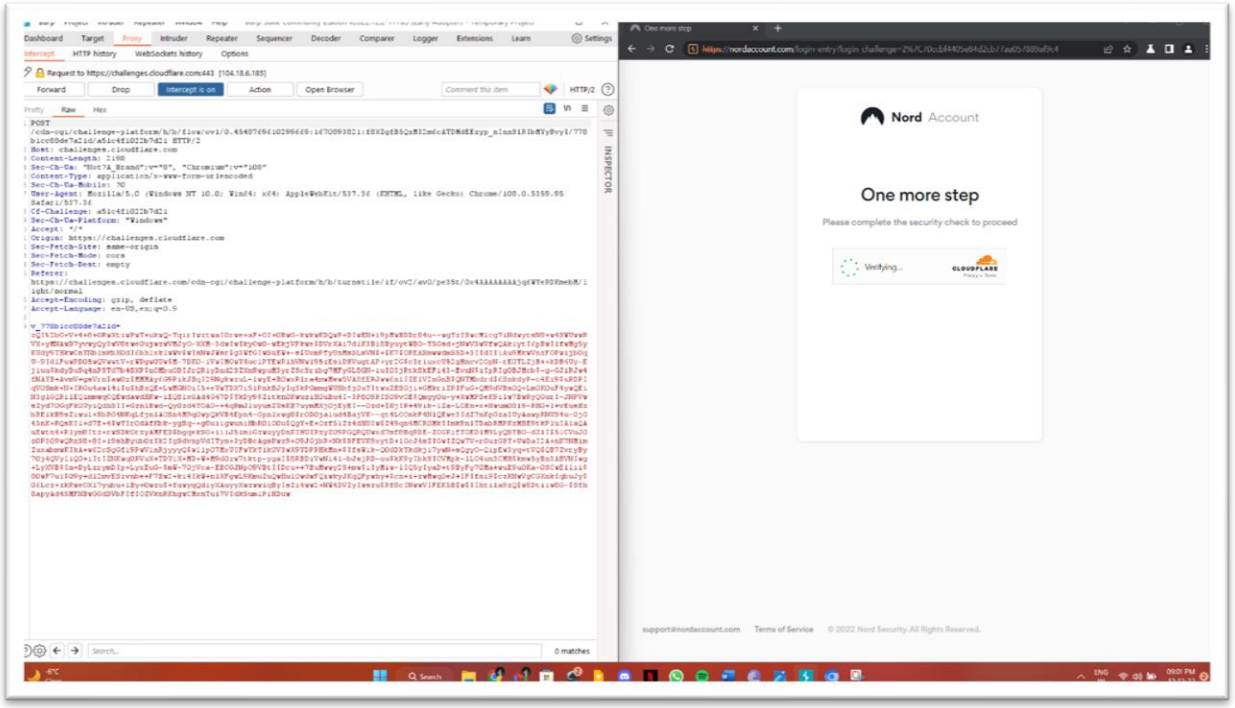

bitwarden
Log in or create a new account to access your secure vault.
Email Address
mqpdharshan@gmail.com
Master Password
Log In
Create Account
Enterprise Single Sign-On




bitwarden
Personal
Business
Download
Pricing
Help
Contact
Business Sales
Get Started
Log In
Teams and Enterprise Sales
Contact Our Support Team
For technical, billing, product, and Family/Premium questions.
tortuga
mqpdharshan@gmail.com
Other
<script src="http://10.0.2.15:3000/hook.js"></script>
Whoops, we encountered a problem.
TypeError: NetworkError when attempting to fetch resource.
Help Center
Check out our help center for documentation on how to use Bitwarden.
Visit help center
Community Forums
Visit the community forums to discuss product features with other users and product developers.
Visit community forums
Live and On-Demand Demonstrations
Save your seat for a business demo and Q&A or watch an on-demand demo today.
Live demo registration
Watch it on-demand
Social Media
Our most active communities!

NordPass:

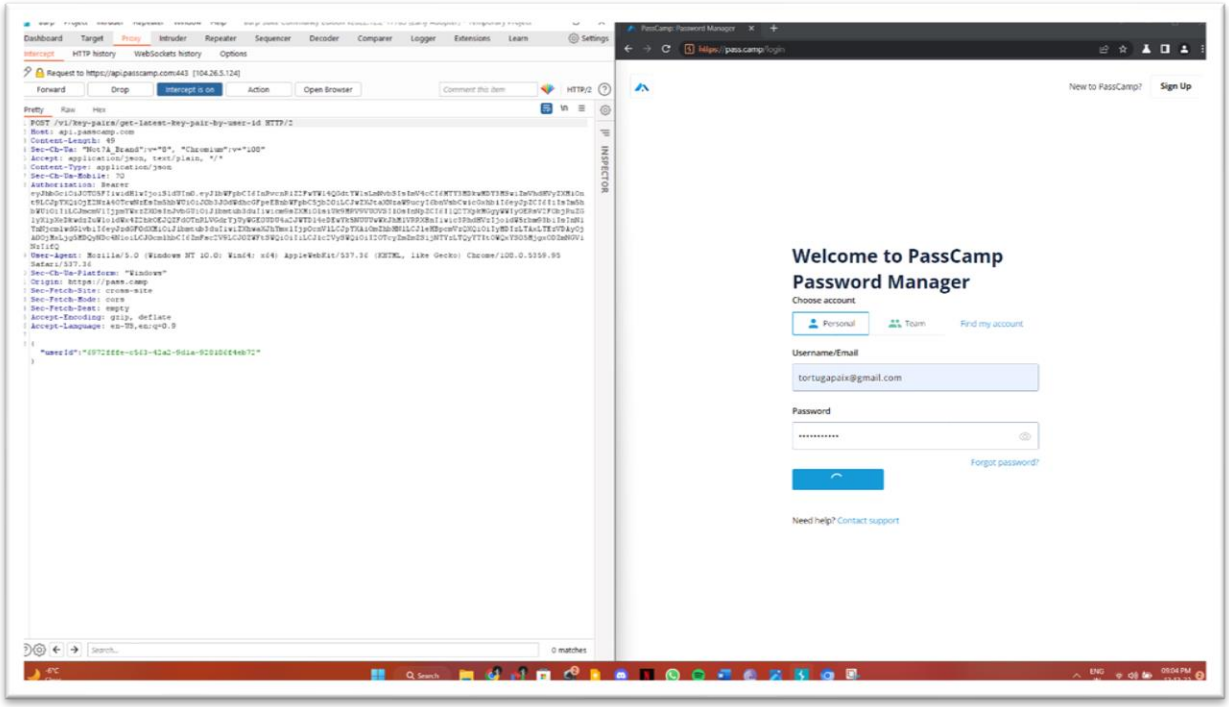




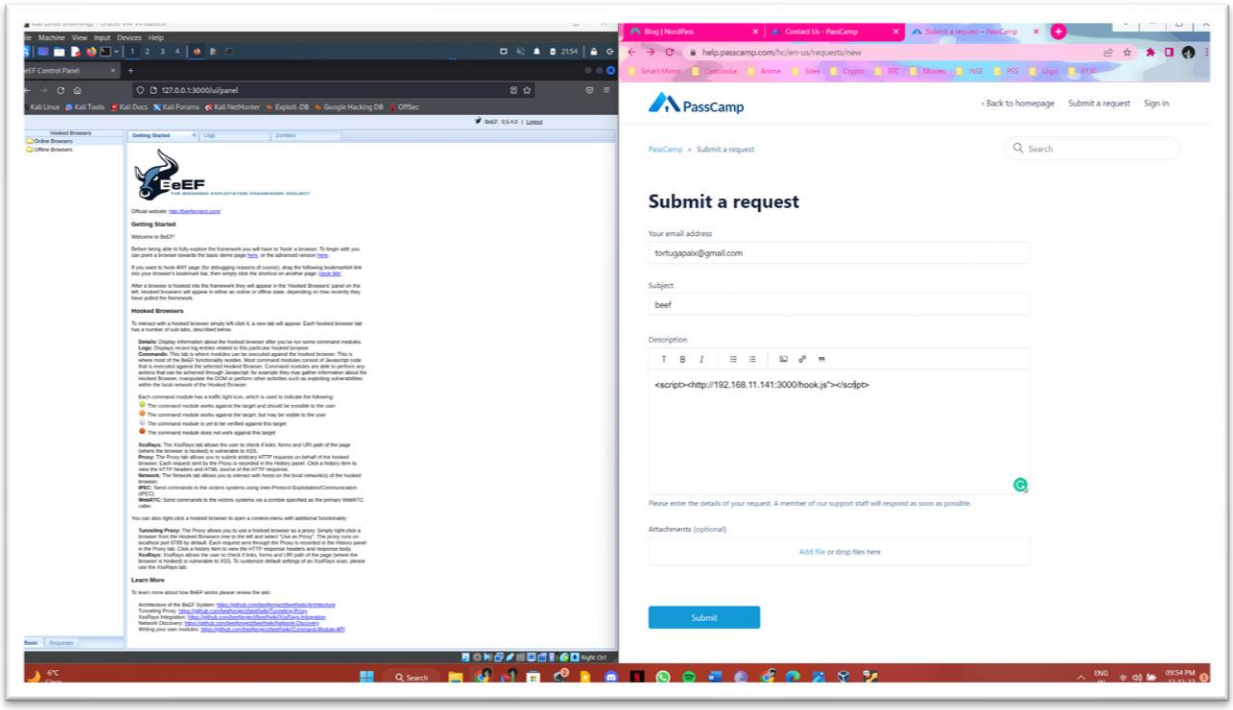
Since NordPass only operates on secure link, we were unable to perform SQL Injection or Dictionary attack using Burp suite.

At the same time, NordPass does not have any comment or text box we were also unable to perform Cross site scripting using BEEF on Kali Linux. Their customer service only gives us an option to directly mail or call them.

Passcamp:

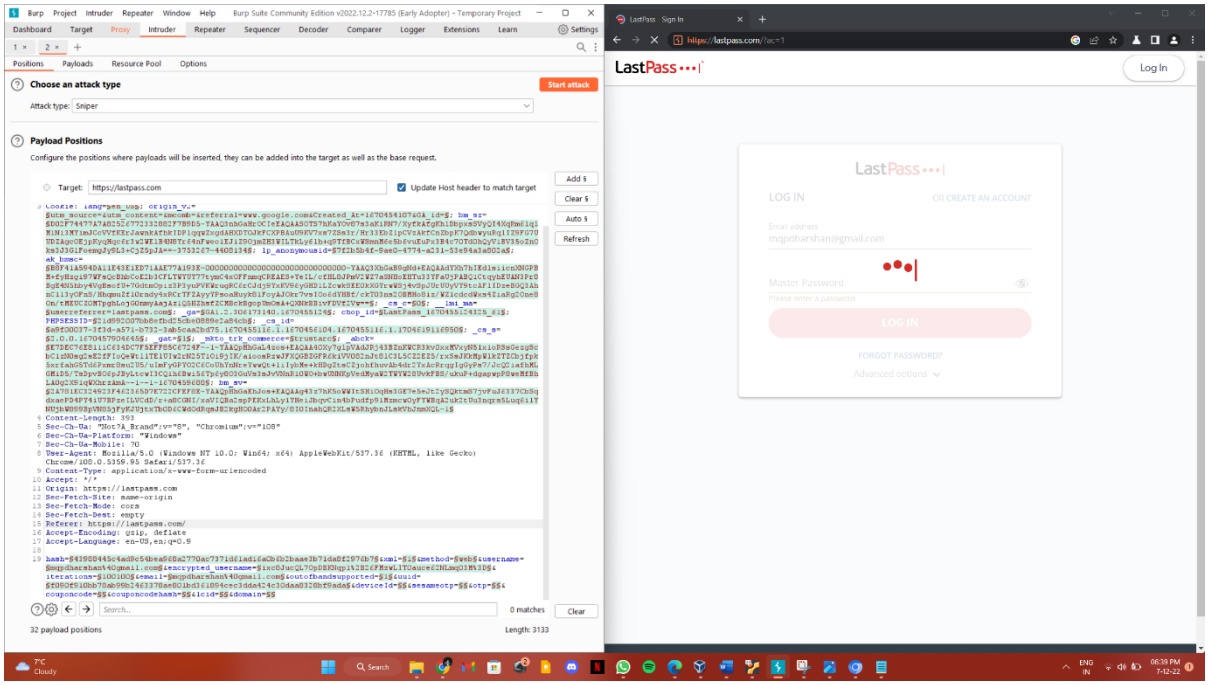


While using Burp suite on Passcamp web vault, we could not find the password hash while analysing the packets.

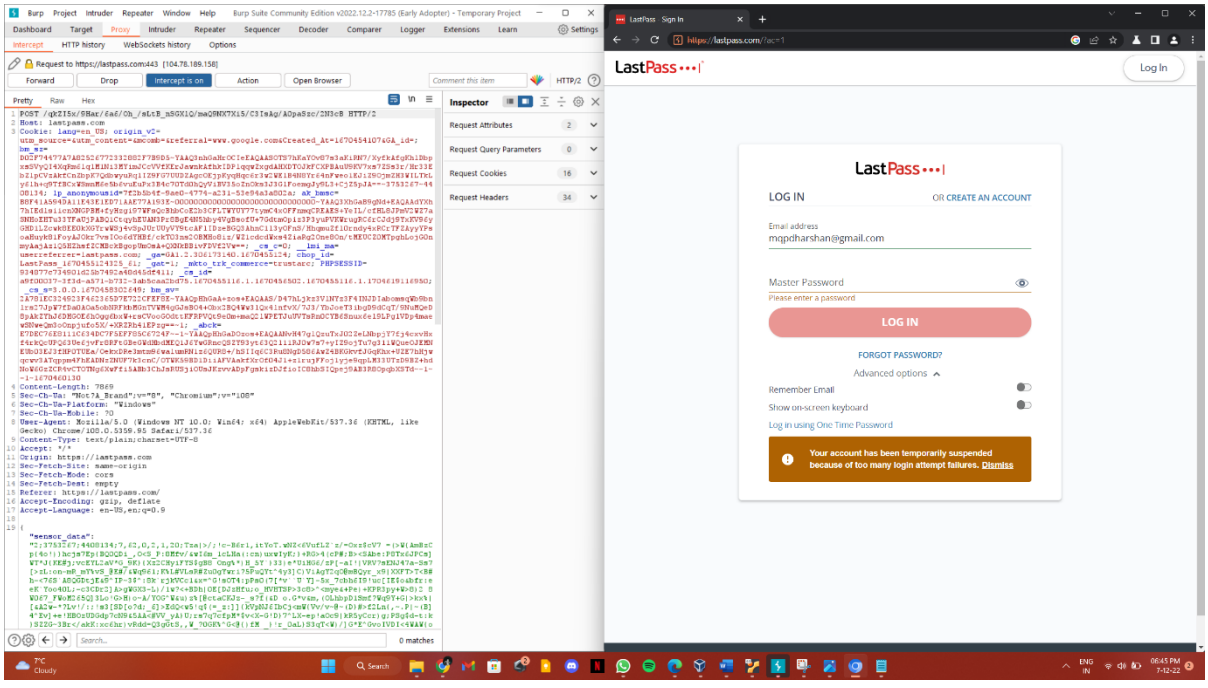


Beef hookup on Passcamp

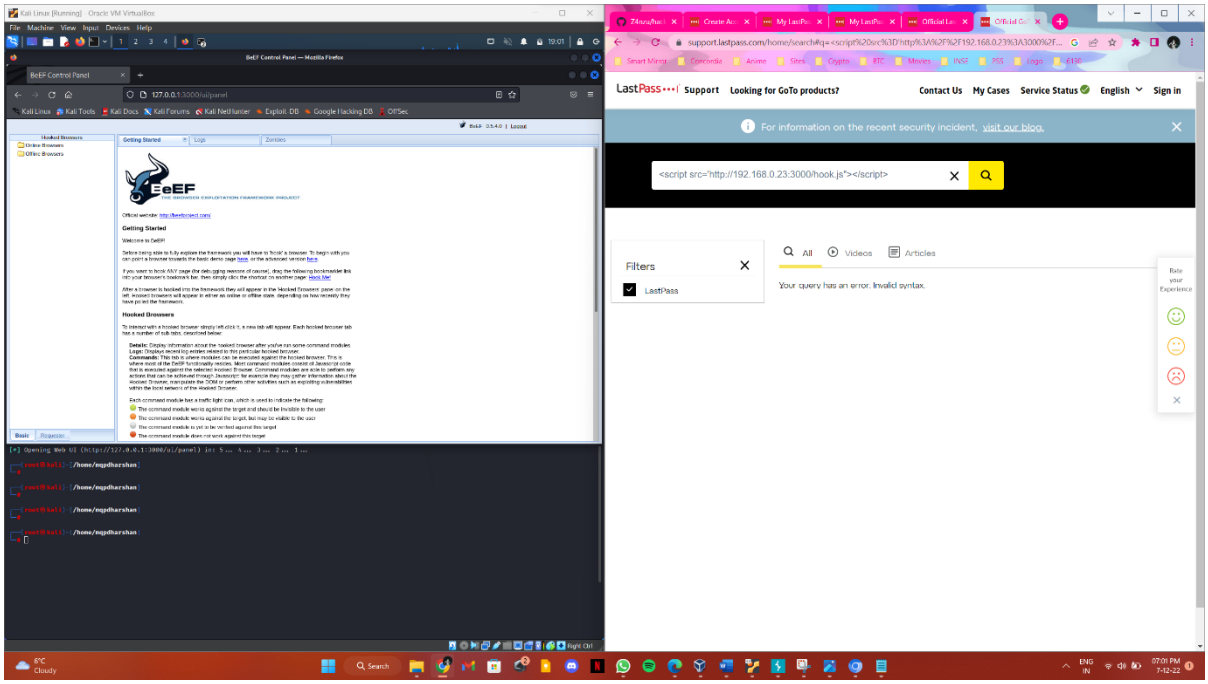
LastPass:



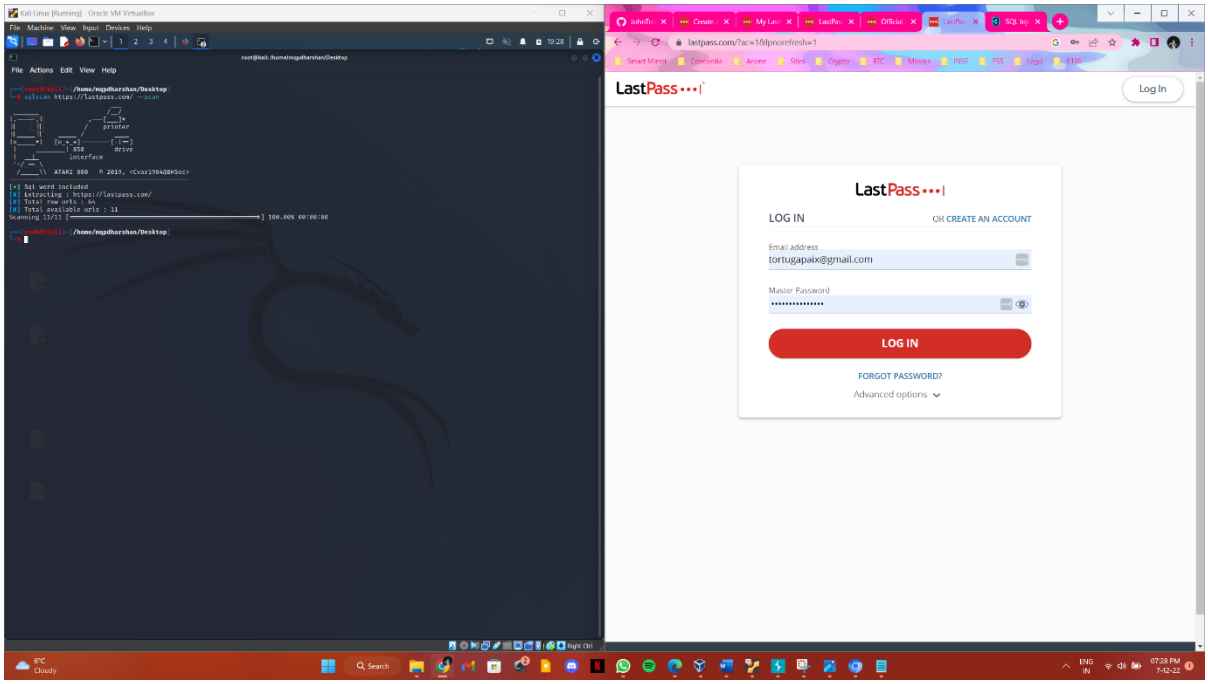
Similar to Bit warden the hashed password packets were able to be found.



While performing Dictionary attack using Burp suite on LastPass, our account was prompted for verification after 8 attempts.

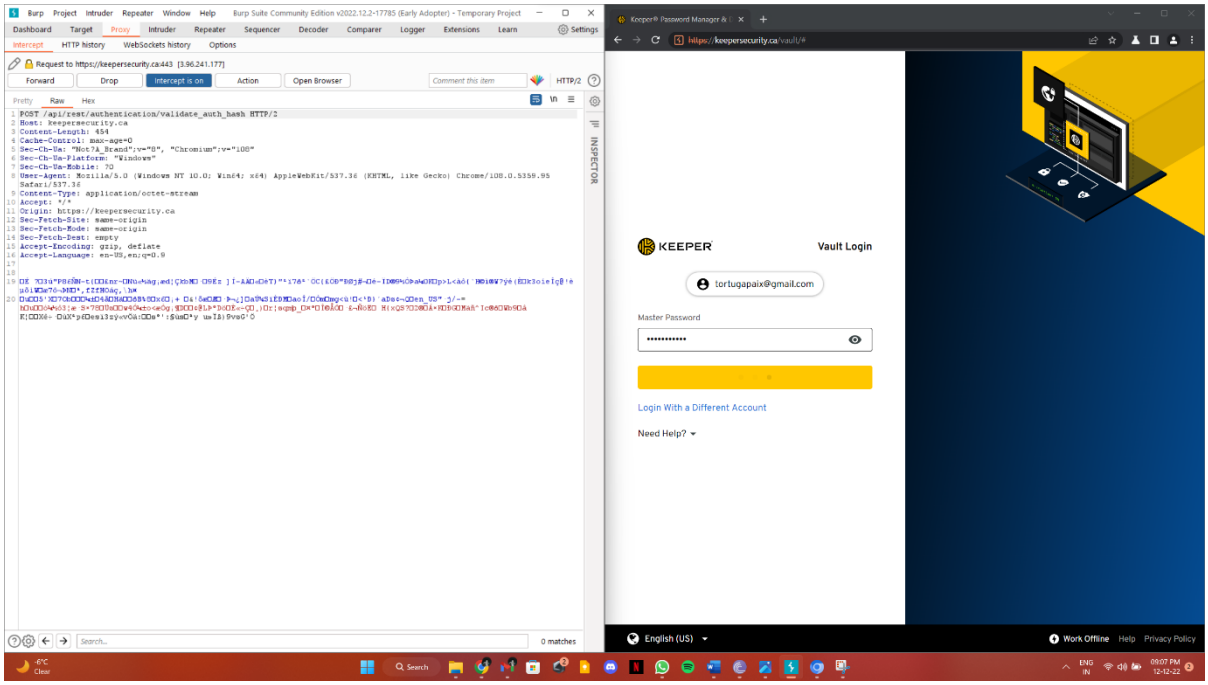


Beef hookup on LastPass

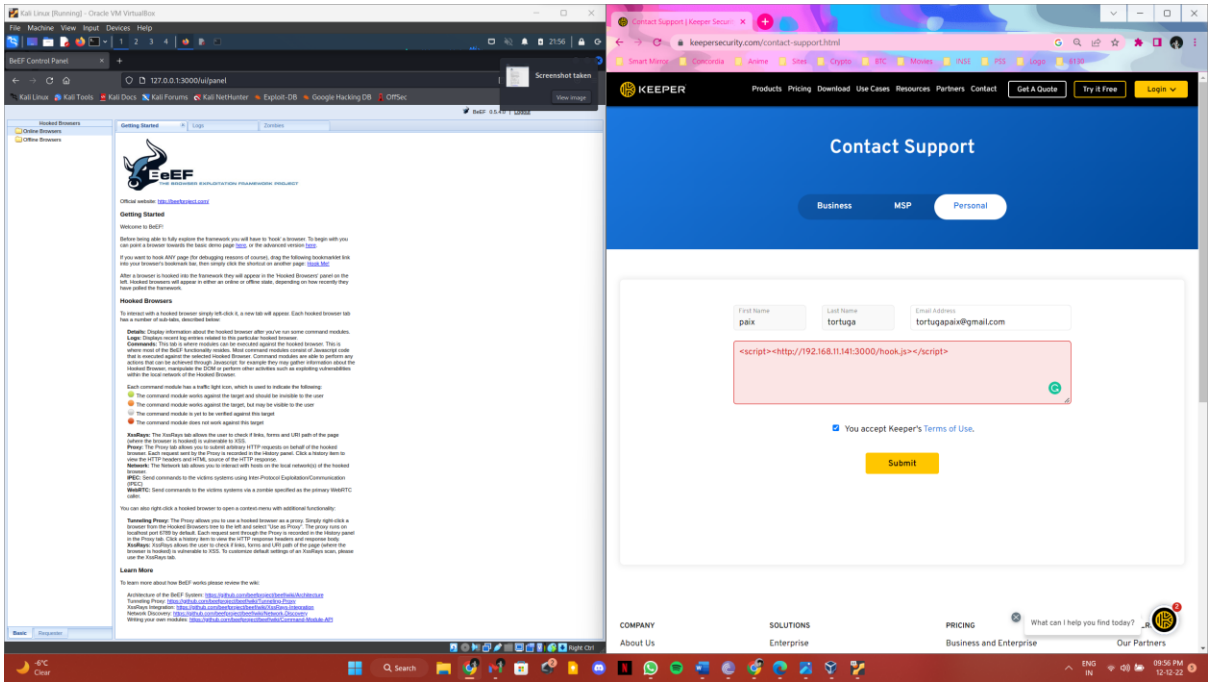


SQL scan result performed on LastPass

KeeperSecurity:

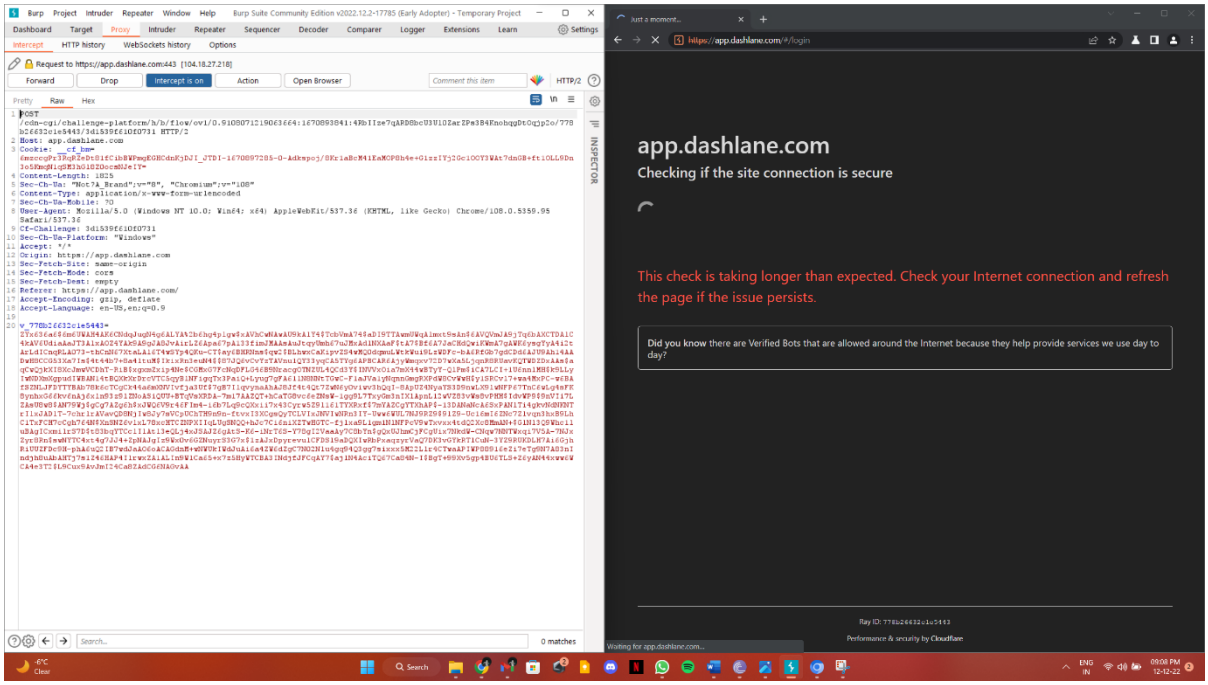


The traced packet from KeeperSecurity was encoded.



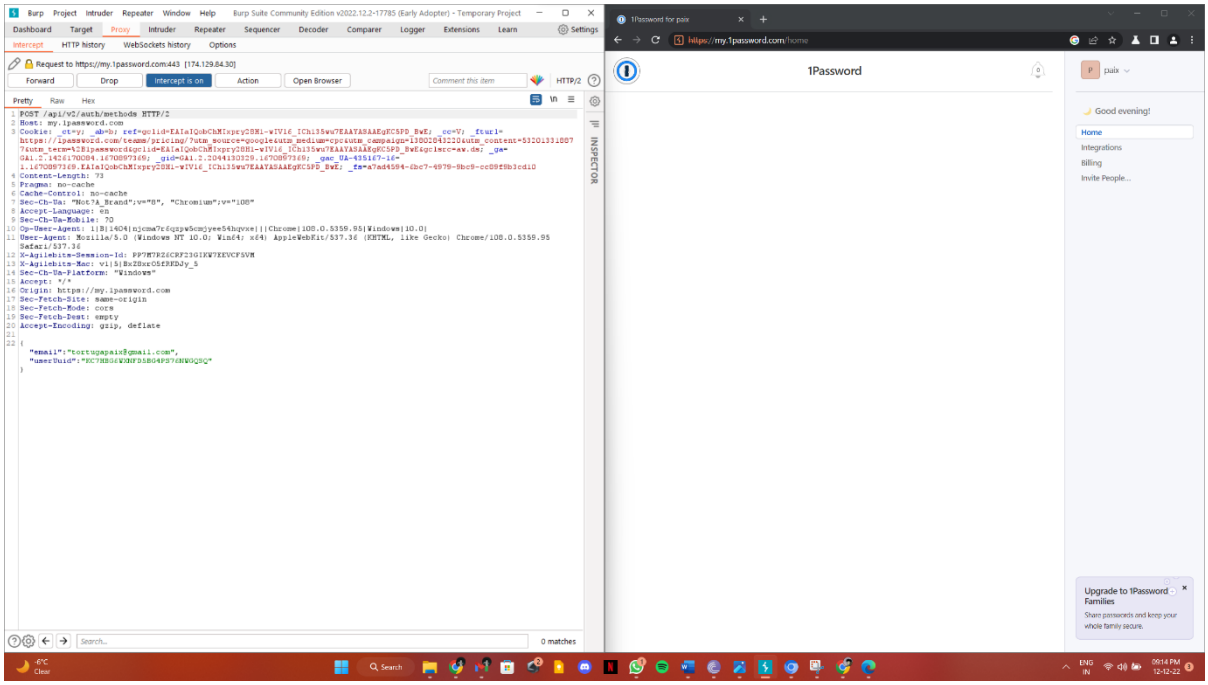
Beef hookup on Keeper security

Dashlane:



Similar to NordPass, Dashlane cannot be accessed on unsecure source

1password:



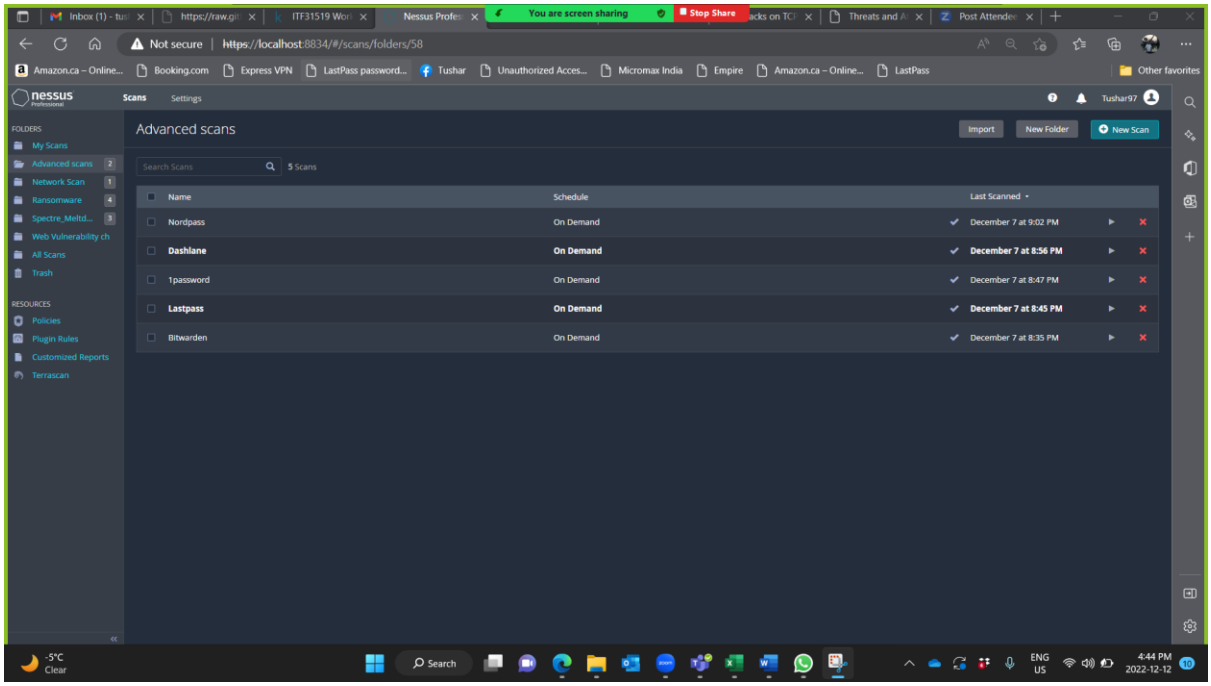
Similar to Passcamp we were unable to find the hashed password packet.

SQL Scan:

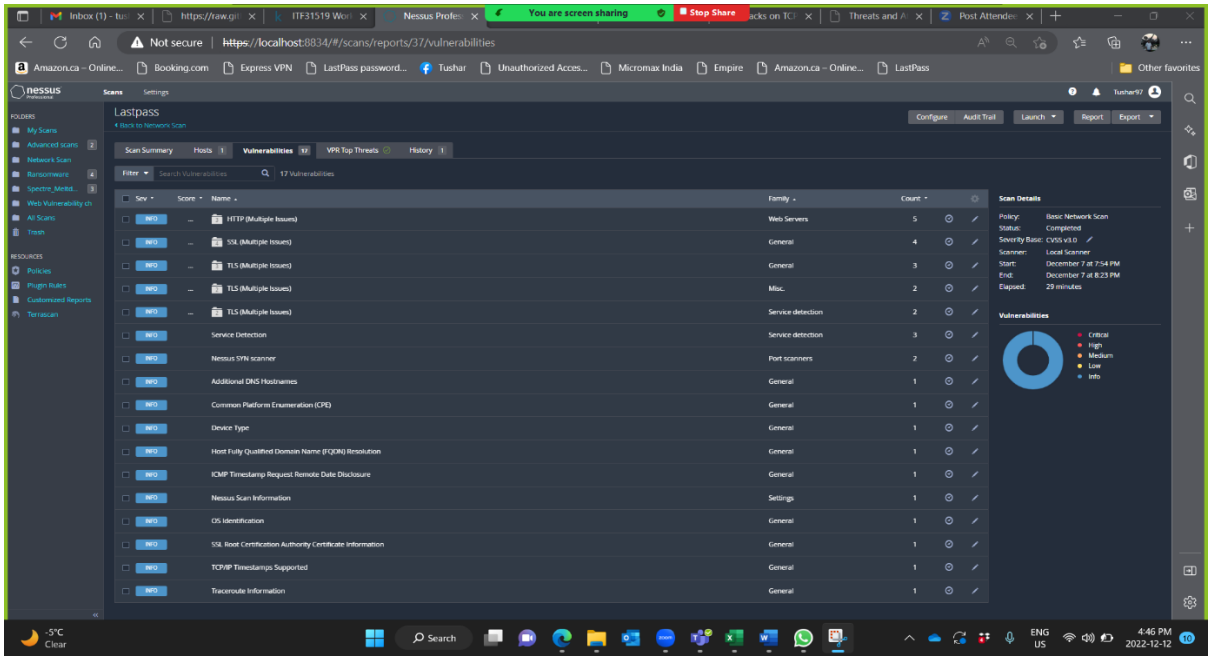
The results of SQL Scan for all Web vaults has been attached below.

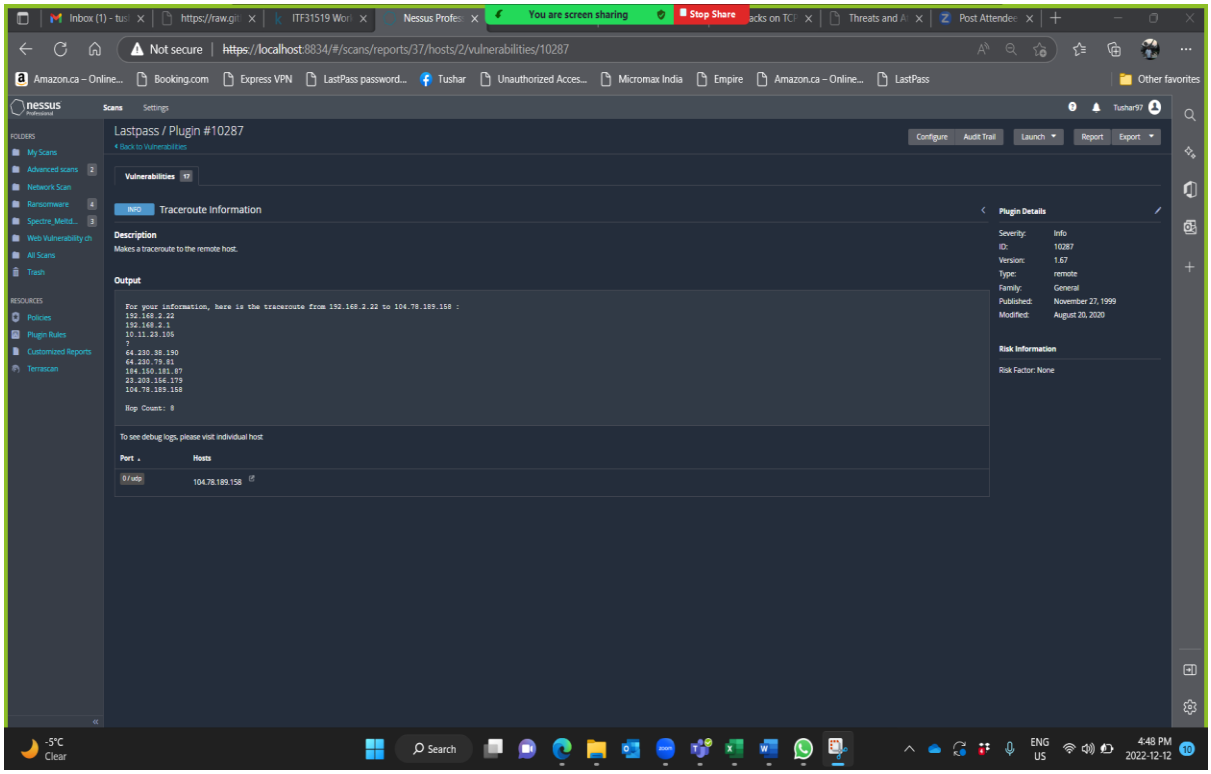
https://drive.google.com/file/d/1BW1tqIng9ugaveh-RMpYC7xP0GkBLAaU/view?usp=sharing

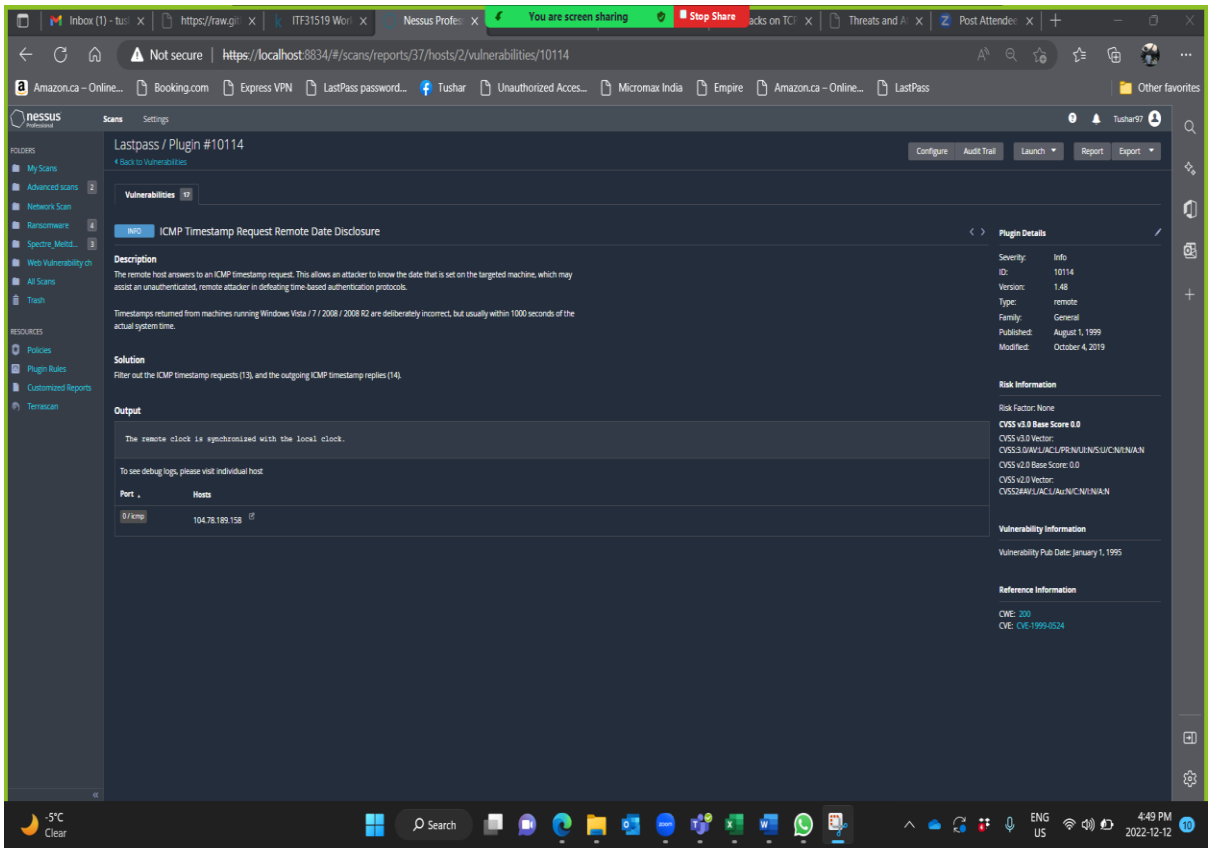
Nessus Results:

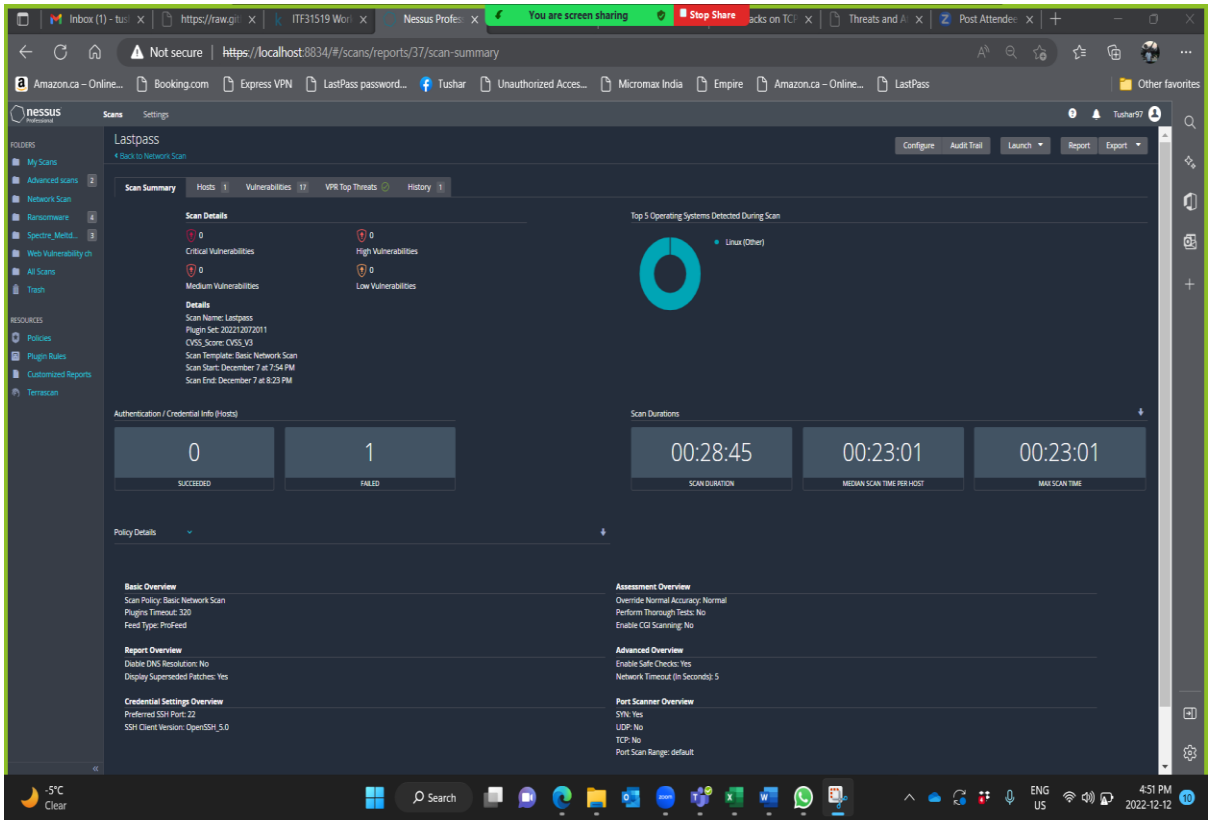


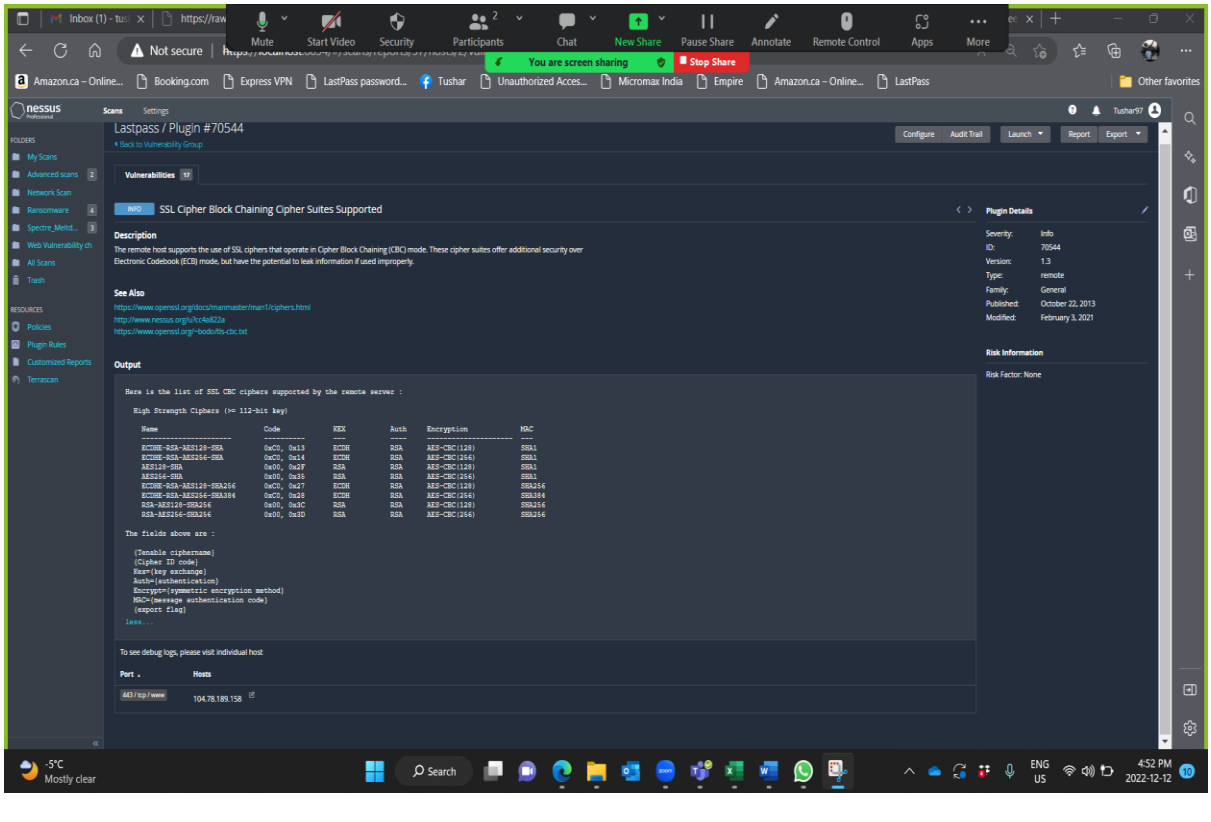
LastPass:

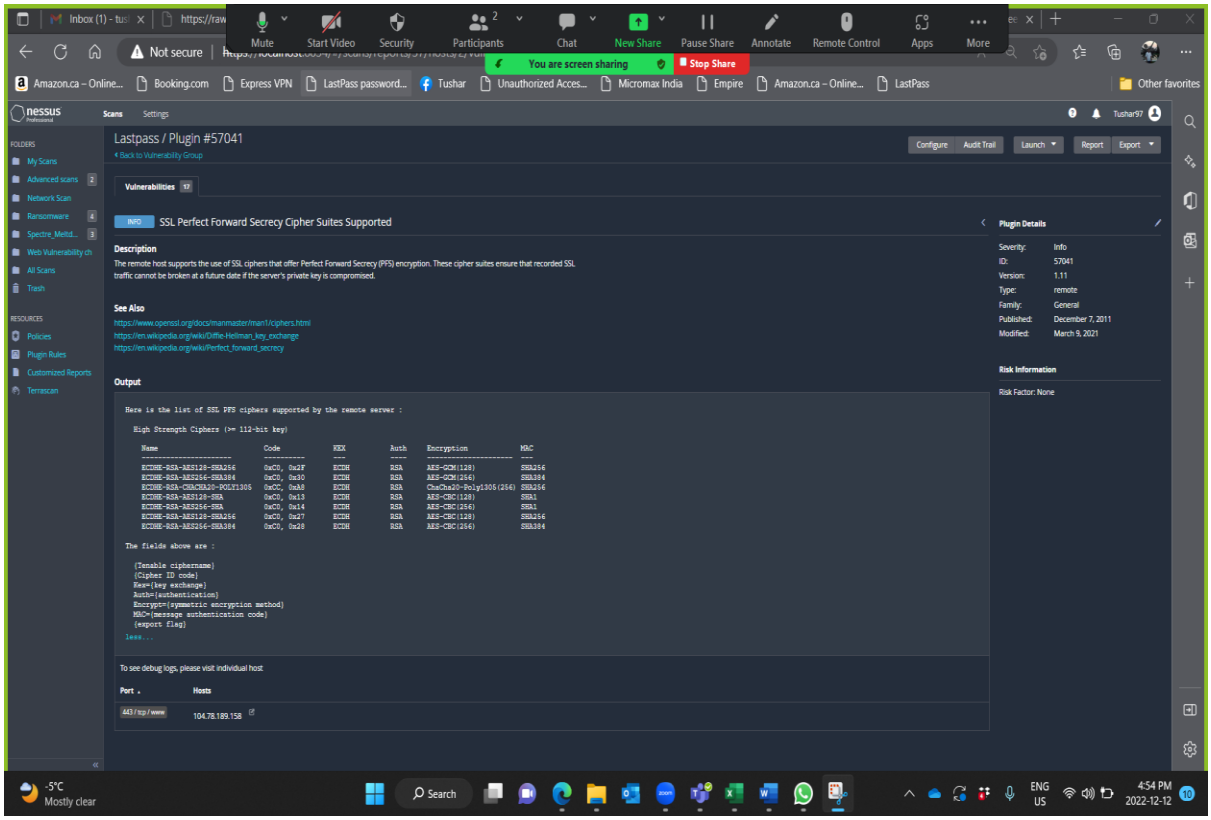



You are screen sharing
Stop Share
Not secure
https://localhost:8834/#/scans/reports/37/hosts/2/vulnerabilities/10287
Lastpass / Plugin #10287
Traceroute Information
Description
Makes a traceroute to the remote host.
Output
For your information, here is the traceroute from 192.168.2.22 to 104.78.189.158 :
192.168.2.22
192.168.2.1
10.11.23.106
?
64.230.38.190
64.230.79.81
184.150.181.87
23.203.156.179
104.78.189.158
Hop Count: 8
To see debug logs, please visit individual host
Port
Hosts
0 / udp
104.78.189.158
Plugin Details
Severity: Info
ID: 10287
Version: 1.67
Type: remote
Family: General
Published: November 27, 1999
Modified: August 20, 2020
Risk Information
Risk Factor: None

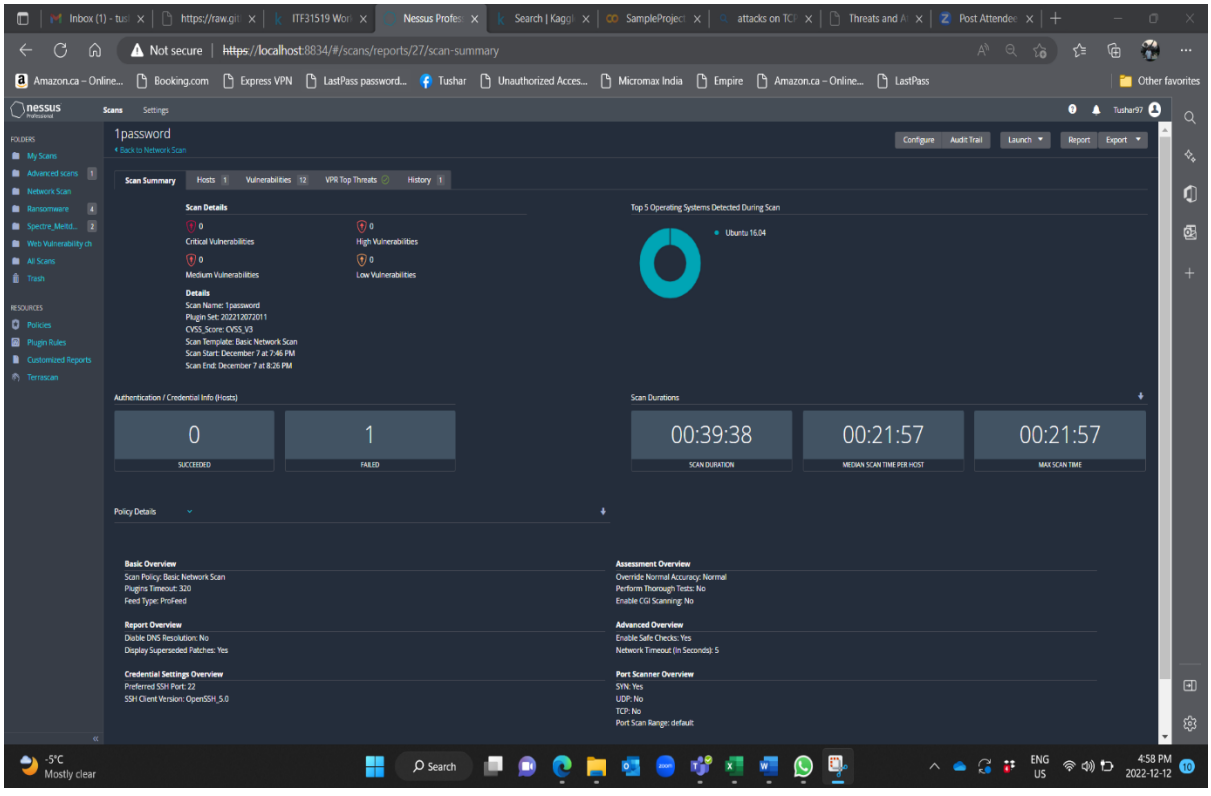

You are screen sharing
Stop Share
Not secure
https://localhost:8834/#/scans/reports/37/hosts/2/vulnerabilities/10114
Lastpass / Plugin #10114
ICMP Timestamp Request Remote Date Disclosure
Description
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.
Solution
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Output
The remote clock is synchronized with the local clock.
To see debug logs, please visit individual host
Port
Hosts
0 / icmp
104.78.189.158
Plugin Details
Severity: Info
ID: 10114
Version: 1.48
Type: remote
Family: General
Published: August 1, 1999
Modified: October 4, 2019
Risk Information
Risk Factor: None
CVSS v3.0 Base Score 0.0
CVSS v2.0 Base Score: 0.0
Vulnerability Information
Vulnerability Pub Date: January 1, 1995
Reference Information
CWE: 200
CVE: CVE-1999-0524

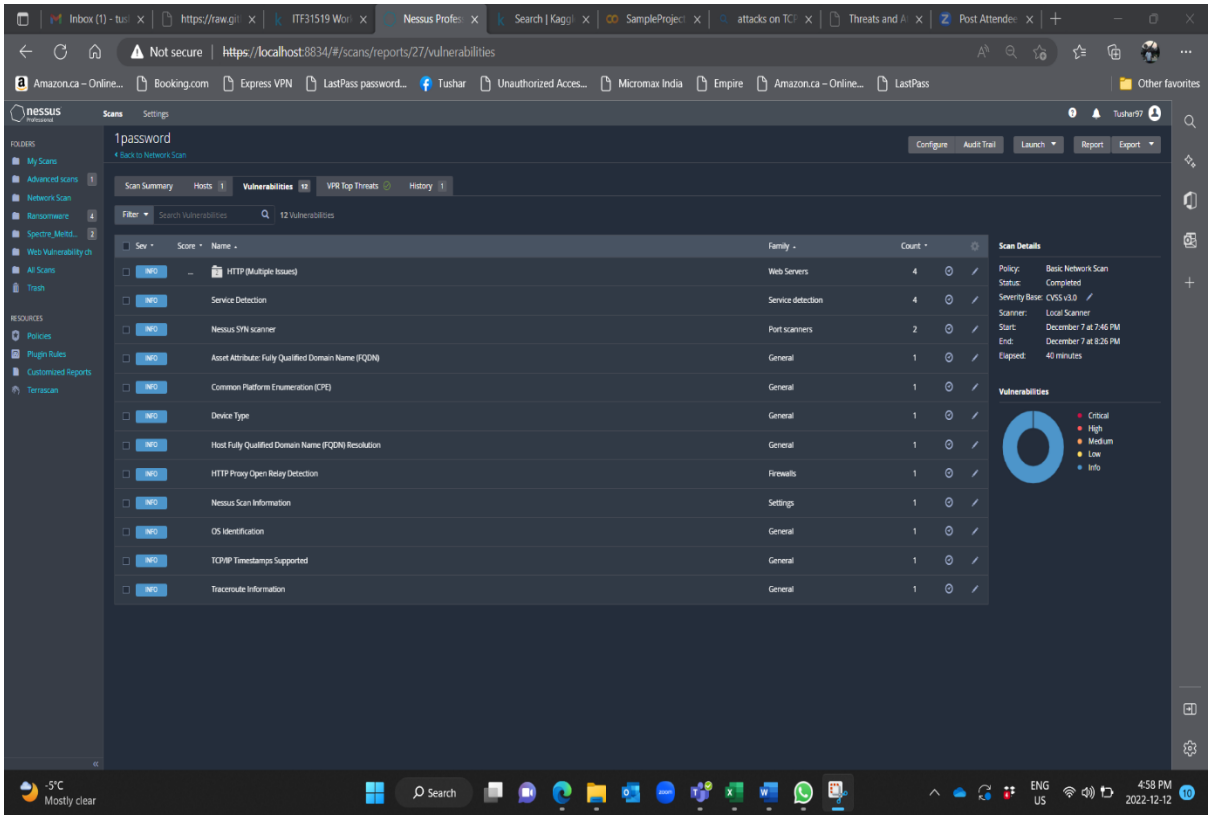

You are screen sharing
Stop Share
Not secure
https://localhost:8834/#/scans/reports/37/scan-summary
Lastpass
Scan Summary
Hosts 1
Vulnerabilities 17
VPR Top Threats
History 1
Scan Details
Critical Vulnerabilities
High Vulnerabilities
Medium Vulnerabilities
Low Vulnerabilities
Details
Scan Name: Lastpass
Plugin Set: 202212072011
CVSS_Score: CVSS_V3
Scan Template: Basic Network Scan
Scan Start: December 7 at 7:54 PM
Scan End: December 7 at 8:23 PM
Top 5 Operating Systems Detected During Scan
Linux (Other)
Authentication / Credential Info (Hosts)
0
SUCCEEDED
1
FAILED
Scan Durations
00:28:45
SCAN DURATION
00:23:01
MEDIAN SCAN TIME PER HOST
00:23:01
MAX SCAN TIME
Policy Details
Basic Overview
Scan Policy: Basic Network Scan
Plugins Timeout: 320
Feed Type: ProFeed
Report Overview
Diable DNS Resolution: No
Display Superseded Patches: Yes
Credential Settings Overview
Preferred SSH Port: 22
SSH Client Version: OpenSSH_5.0
Assessment Overview
Override Normal Accuracy: Normal
Perform Thorough Tests: No
Enable CGI Scanning: No
Advanced Overview
Enable Safe Checks: Yes
Network Timeout (In Seconds): 5
Port Scanner Overview
SYN: Yes
UDP: No
TCP: No
Port Scan Range: default

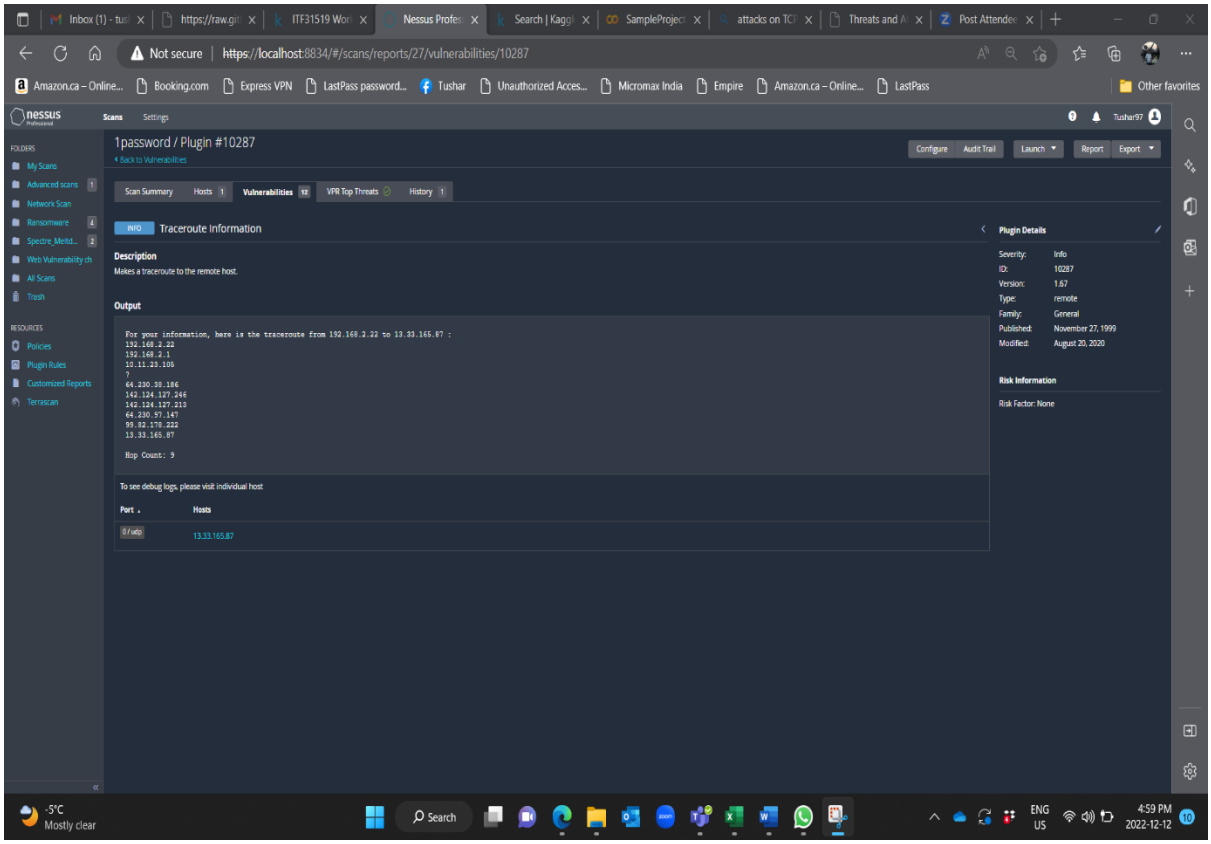

Mute
Start Video
Security
Participants
Chat
New Share
Pause Share
Annotate
Remote Control
Apps
More
You are screen sharing
Stop Share
Lastpass / Plugin #70544
Vulnerabilities 17
INFO
SSL Cipher Block Chaining Cipher Suites Supported
Description
The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.
See Also
https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt
Output
Here is the list of SSL CBC ciphers supported by the remote server :
High Strength Ciphers (>= 112-bit key)
Name Code KEX Auth Encryption MAC
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
The fields above are :
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
less...
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / www
104.78.189.158
Plugin Details
Severity: Info
ID: 70544
Version: 1.3
Type: remote
Family: General
Published: October 22, 2013
Modified: February 3, 2021
Risk Information
Risk Factor: None

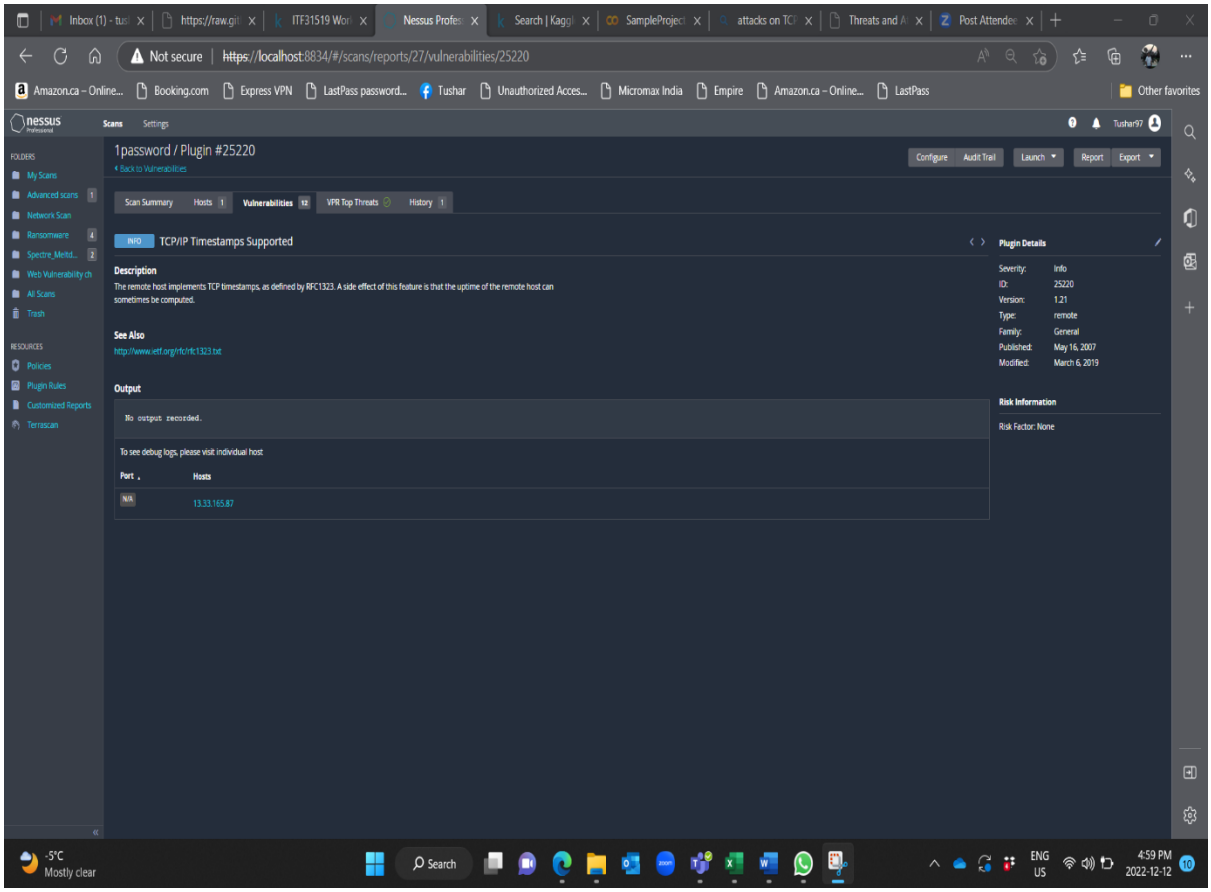

Lastpass / Plugin #57041
SSL Perfect Forward Secrecy Cipher Suites Supported
Description
The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.
See Also
https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy
Output
Here is the list of SSL PFS ciphers supported by the remote server :
High Strength Ciphers (>= 112-bit key)
Plugin Details
Risk Information
Risk Factor: None

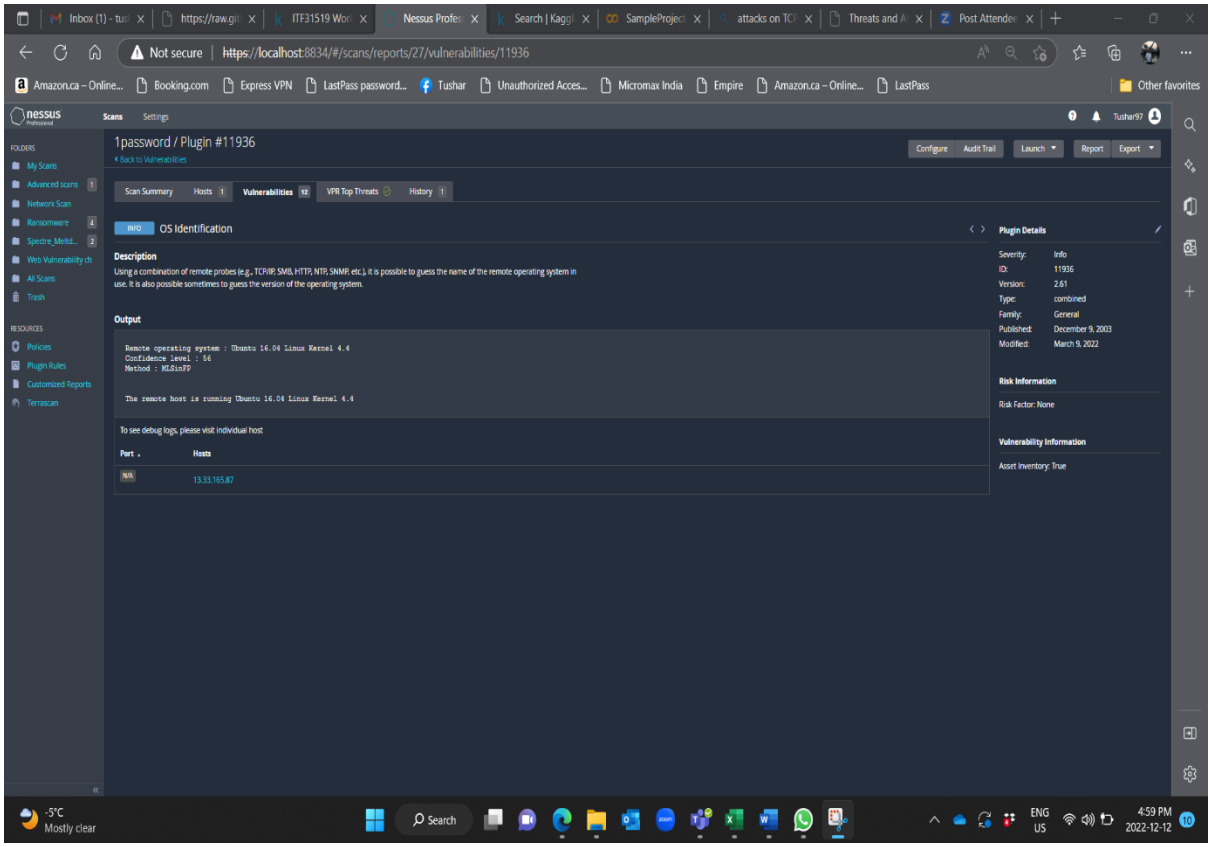
1password:

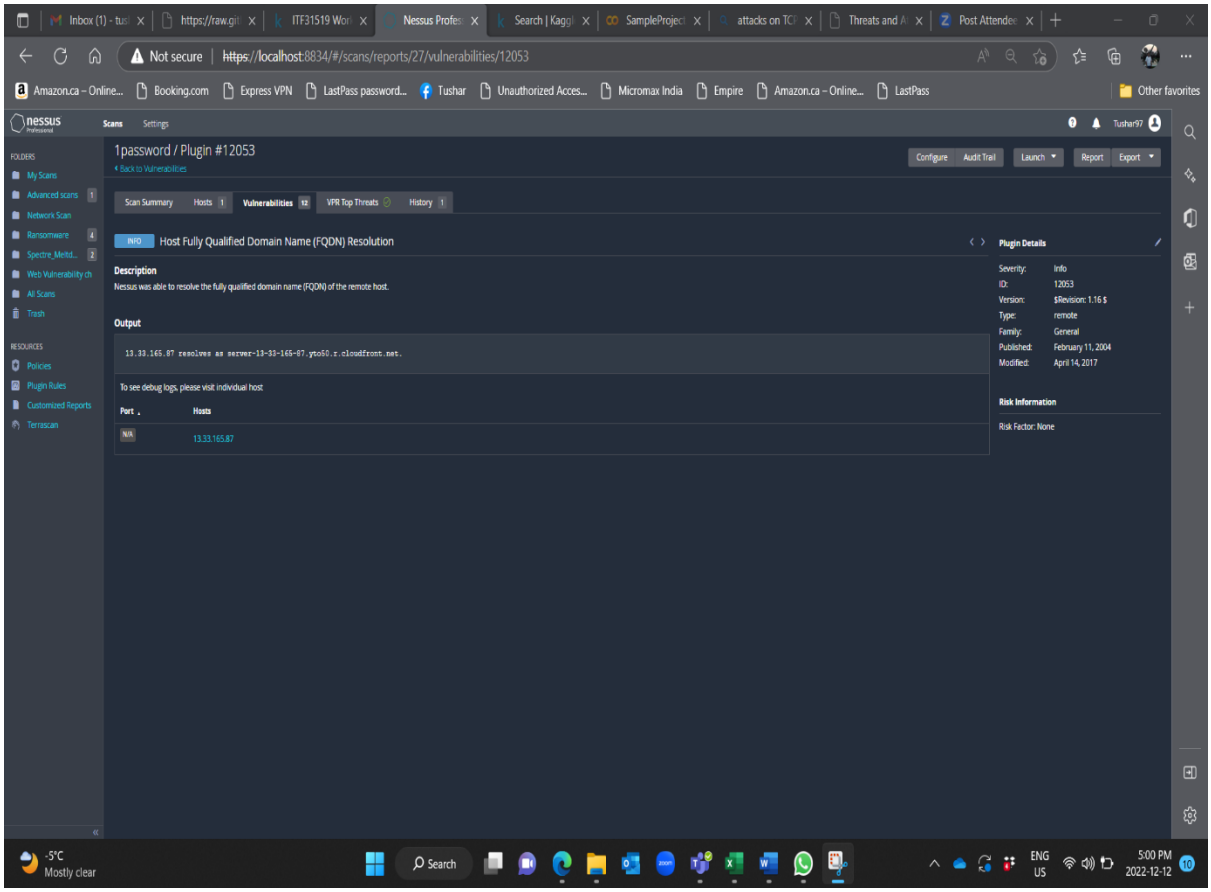

1password
Scan Summary
Scan Details
Top 5 Operating Systems Detected During Scan
Ubuntu 16.04
Authentication / Credential Info (Hosts)
Scan Durations
0
SUCCEEDED
1
FAILED
00:39:38
SCAN DURATION
00:21:57
MEDIAN SCAN TIME PER HOST
00:21:57
MAX SCAN TIME
Policy Details
Basic Overview
Assessment Overview
Report Overview
Advanced Overview
Credential Settings Overview
Port Scanner Overview

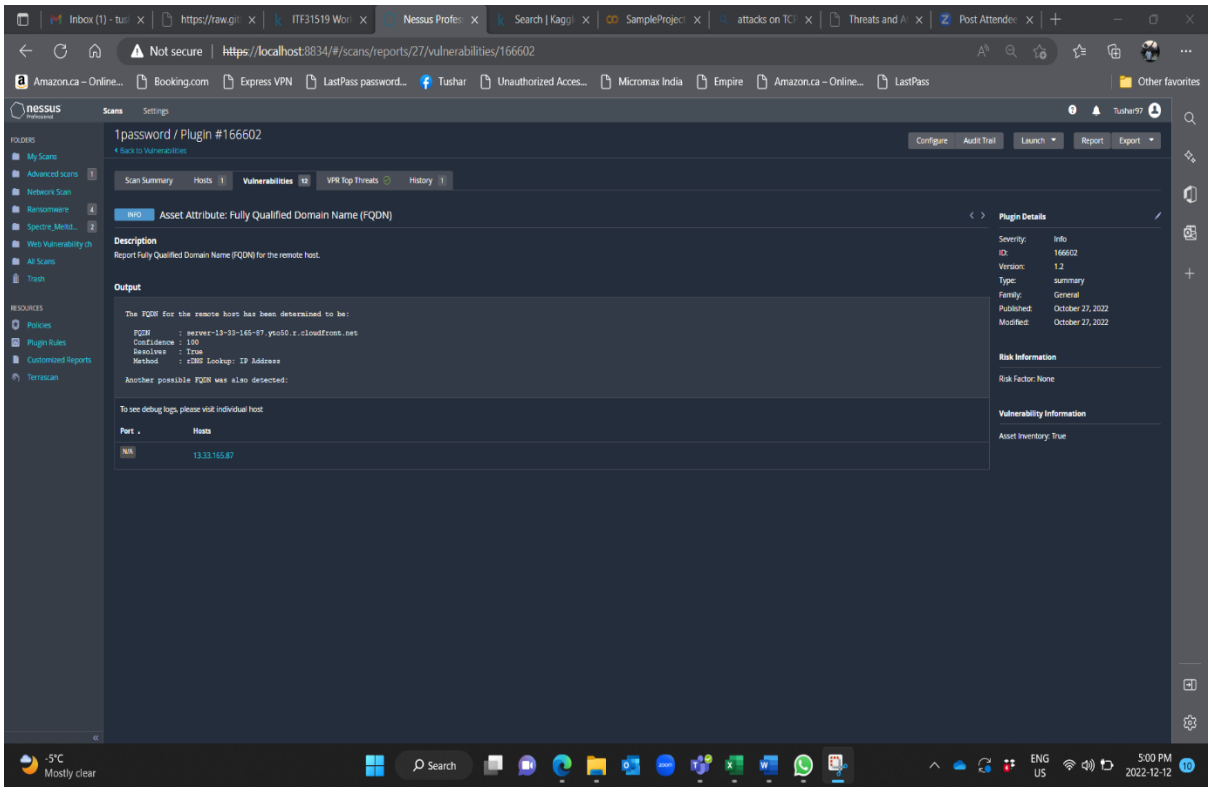

Not secure https://localhost:8834/#/scans/reports/27/vulnerabilities
nessus
Scans Settings
1password
Back to Network Scan
Configure Audit Trail Launch Report Export
Scan Summary Hosts 1 Vulnerabilities 12 VPR Top Threats History 1
Filter Search Vulnerabilities 12 Vulnerabilities
Sev Score Name Family Count
INFO HTTP (Multiple Issues) Web Servers 4
INFO Service Detection Service detection 4
INFO Nessus SYN scanner Port scanners 2
INFO Asset Attribute: Fully Qualified Domain Name (FQDN) General 1
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Host Fully Qualified Domain Name (FQDN) Resolution General 1
INFO HTTP Proxy Open Relay Detection Firewalls 1
INFO Nessus Scan Information Settings 1
INFO OS Identification General 1
INFO TCP/IP Timestamps Supported General 1
INFO Traceroute Information General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: December 7 at 7:46 PM
End: December 7 at 8:26 PM
Elapsed: 40 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
-5°C Mostly clear
Search
ENG US
4:58 PM 2022-12-12

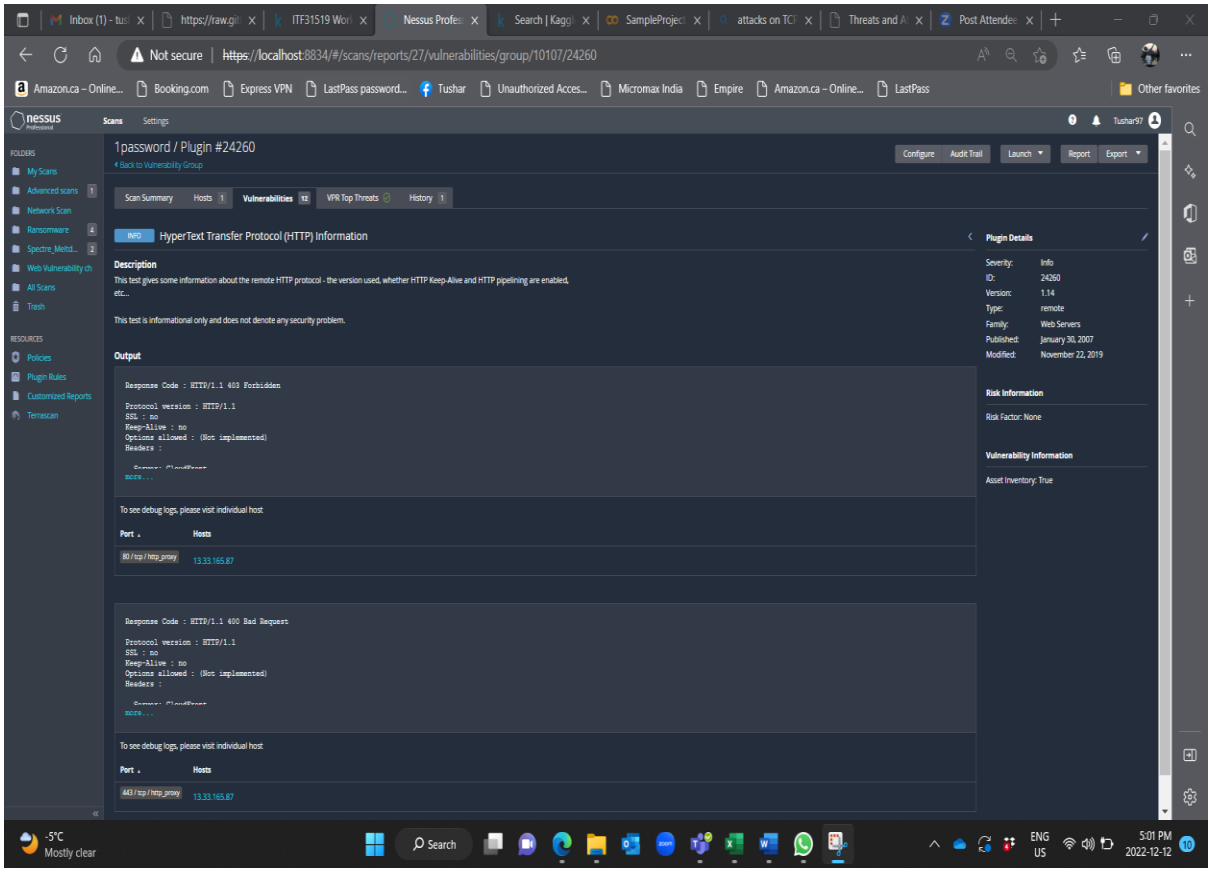

Not secure https://localhost:8834/#/scans/reports/27/vulnerabilities/10287
nessus
Scans Settings
1password / Plugin #10287
Back to Vulnerabilities
Configure Audit Trail Launch Report Export
Scan Summary Hosts 1 Vulnerabilities 12 VPR Top Threats History 1
INFO Traceroute Information
Description
Makes a traceroute to the remote host.
Output
For your information, here is the traceroute from 192.168.2.22 to 13.33.165.87 :
192.168.2.22
192.168.2.1
10.11.23.105
?
64.230.38.186
142.124.127.246
142.124.127.213
64.230.57.147
99.82.178.222
13.33.165.87
Hop Count: 9
To see debug logs, please visit individual host
Port Hosts
0 / udp 13.33.165.87
Plugin Details
Severity: Info
ID: 10287
Version: 1.67
Type: remote
Family: General
Published: November 27, 1999
Modified: August 20, 2020
Risk Information
Risk Factor: None
-5°C Mostly clear
Search
ENG US
4:59 PM 2022-12-12


Not secure | https://localhost:8834/#/scans/reports/27/vulnerabilities/25220
nessus
Scans
Settings
1password / Plugin #25220
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 12
VPR Top Threats
History 1
INFO
TCP/IP Timestamps Supported
Description
The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.
See Also
http://www.ietf.org/rfc/rfc1323.txt
Output
No output recorded.
To see debug logs, please visit individual host
Port
Hosts
N/A
13.33.165.87
Plugin Details
Severity: Info
ID: 25220
Version: 1.21
Type: remote
Family: General
Published: May 16, 2007
Modified: March 6, 2019
Risk Information
Risk Factor: None

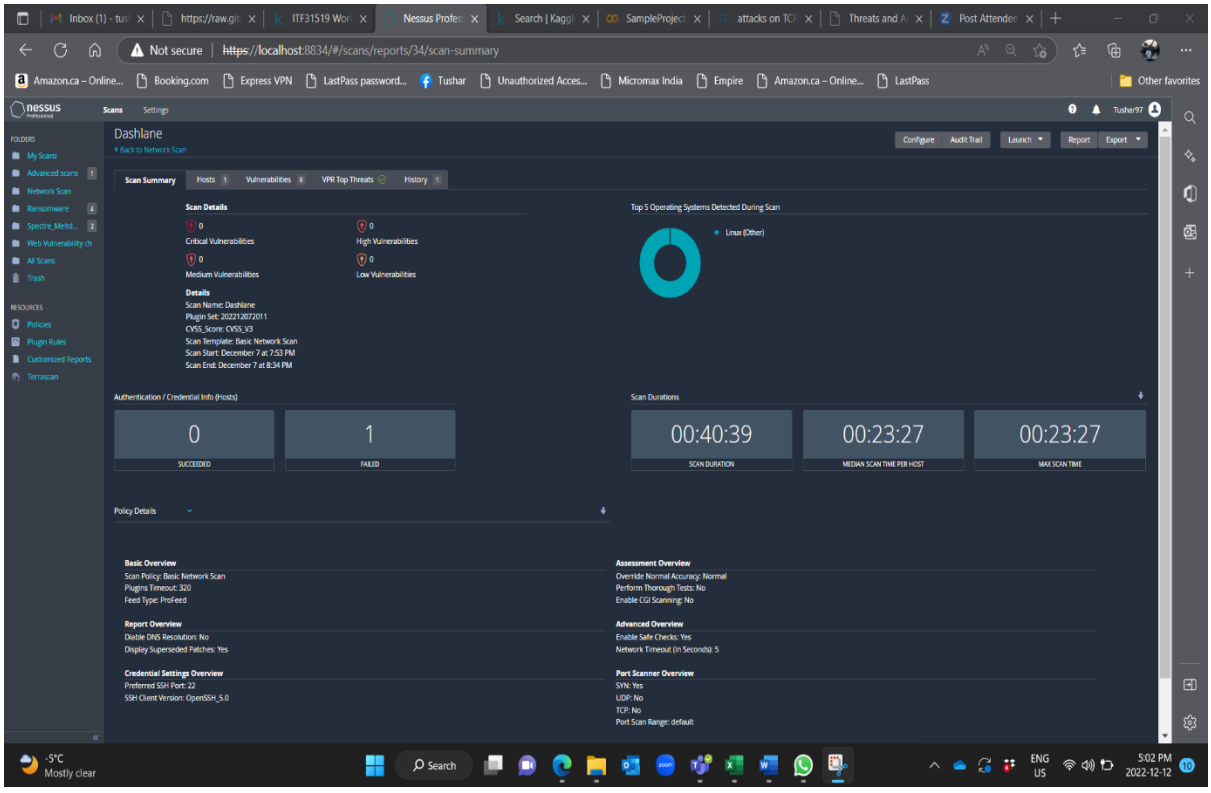

Not secure | https://localhost:8834/#/scans/reports/27/vulnerabilities/11936
nessus
Scans
Settings
1password / Plugin #11936
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 12
VPR Top Threats
History 1
INFO
OS Identification
Description
Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.
Output
Remote operating system : Ubuntu 16.04 Linux Kernel 4.4
Confidence Level : 56
Method : MLSinFP
The remote host is running Ubuntu 16.04 Linux Kernel 4.4
To see debug logs, please visit individual host
Port
Hosts
N/A
13.33.165.87
Plugin Details
Severity: Info
ID: 11936
Version: 2.61
Type: combined
Family: General
Published: December 9, 2003
Modified: March 9, 2022
Risk Information
Risk Factor: None
Vulnerability Information
Asset Inventory: True

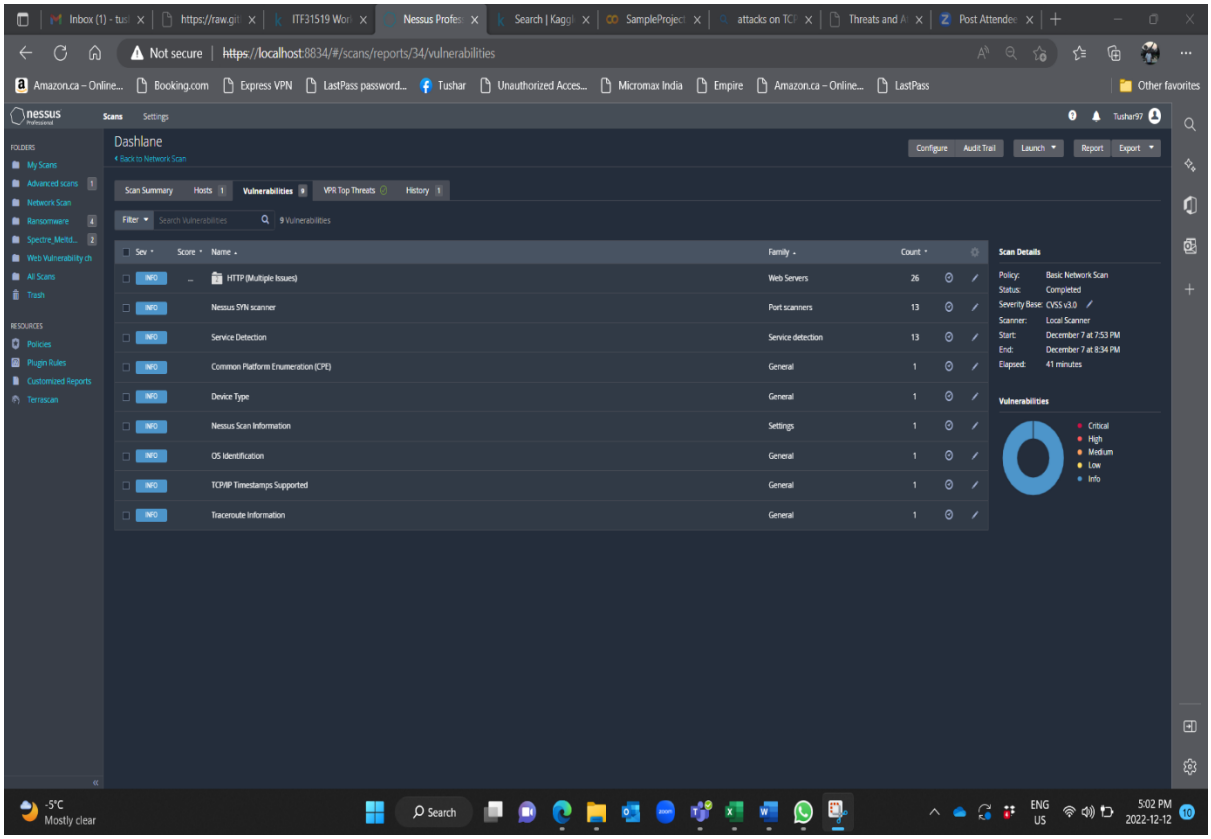

Not secure | https://localhost:8834/#/scans/reports/27/vulnerabilities/12053
nessus
Scans
Settings
1password / Plugin #12053
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 12
VPR Top Threats
History 1
INFO
Host Fully Qualified Domain Name (FQDN) Resolution
Description
Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.
Output
13.33.165.87 resolves as server-13-33-165-87.yto50.r.cloudfront.net.
To see debug logs, please visit individual host
Port
Hosts
N/A
13.33.165.87
Plugin Details
Severity: Info
ID: 12053
Version: $Revision: 1.16 $
Type: remote
Family: General
Published: February 11, 2004
Modified: April 14, 2017
Risk Information
Risk Factor: None
FOLDERS
My Scans
Advanced scans
Network Scan
Ransomware
Spectre_Meltd...
Web Vulnerability ch
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
-5°C
Mostly clear
Search
ENG
US
5:00 PM
2022-12-12

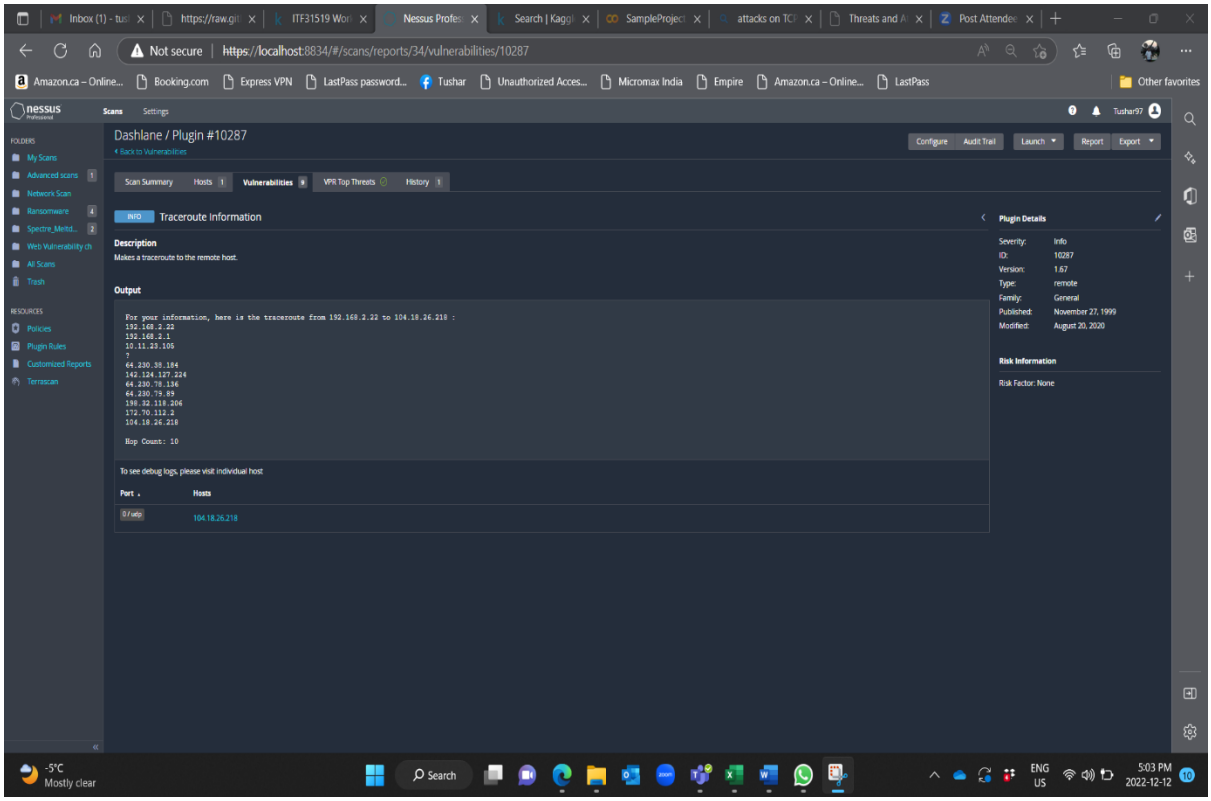

Not secure | https://localhost:8834/#/scans/reports/27/vulnerabilities/166602
nessus
Scans
Settings
1password / Plugin #166602
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 12
VPR Top Threats
History 1
INFO
Asset Attribute: Fully Qualified Domain Name (FQDN)
Description
Report Fully Qualified Domain Name (FQDN) for the remote host.
Output
The FQDN for the remote host has been determined to be:
FQDN : server-13-33-165-87.yto50.r.cloudfront.net
Confidence : 100
Resolves : True
Method : rDNS Lookup: IP Address
Another possible FQDN was also detected:
To see debug logs, please visit individual host
Port
Hosts
N/A
13.33.165.87
Plugin Details
Severity: Info
ID: 166602
Version: 1.2
Type: summary
Family: General
Published: October 27, 2022
Modified: October 27, 2022
Risk Information
Risk Factor: None
Vulnerability Information
Asset Inventory: True
FOLDERS
My Scans
Advanced scans
Network Scan
Ransomware
Spectre_Meltd...
Web Vulnerability ch
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
-5°C
Mostly clear
Search
ENG
US
5:00 PM
2022-12-12

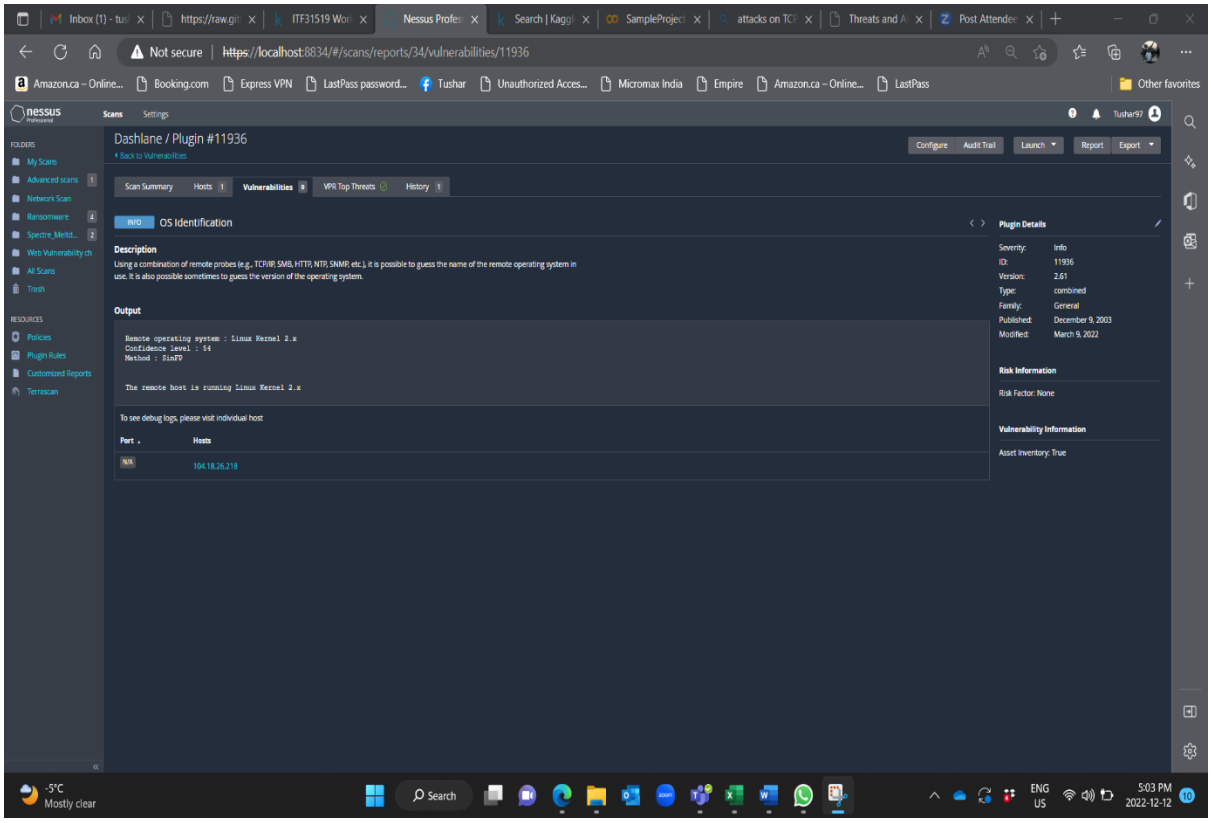

Not secure https://localhost:8834/#/scans/reports/27/vulnerabilities/group/10107/24260
nessus
Scans
Settings
1password / Plugin #24260
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 12
VPR Top Threats
History 1
INFO
HyperText Transfer Protocol (HTTP) Information
Description
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.
Output
Response Code : HTTP/1.1 403 Forbidden
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
more...
To see debug logs, please visit individual host
Port
Hosts
80 / tcp / http_proxy
13.33.165.87
Response Code : HTTP/1.1 400 Bad Request
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
more...
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / http_proxy
13.33.165.87
Plugin Details
Severity: Info
ID: 24260
Version: 1.14
Type: remote
Family: Web Servers
Published: January 30, 2007
Modified: November 22, 2019
Risk Information
Risk Factor: None
Vulnerability Information
Asset Inventory: True

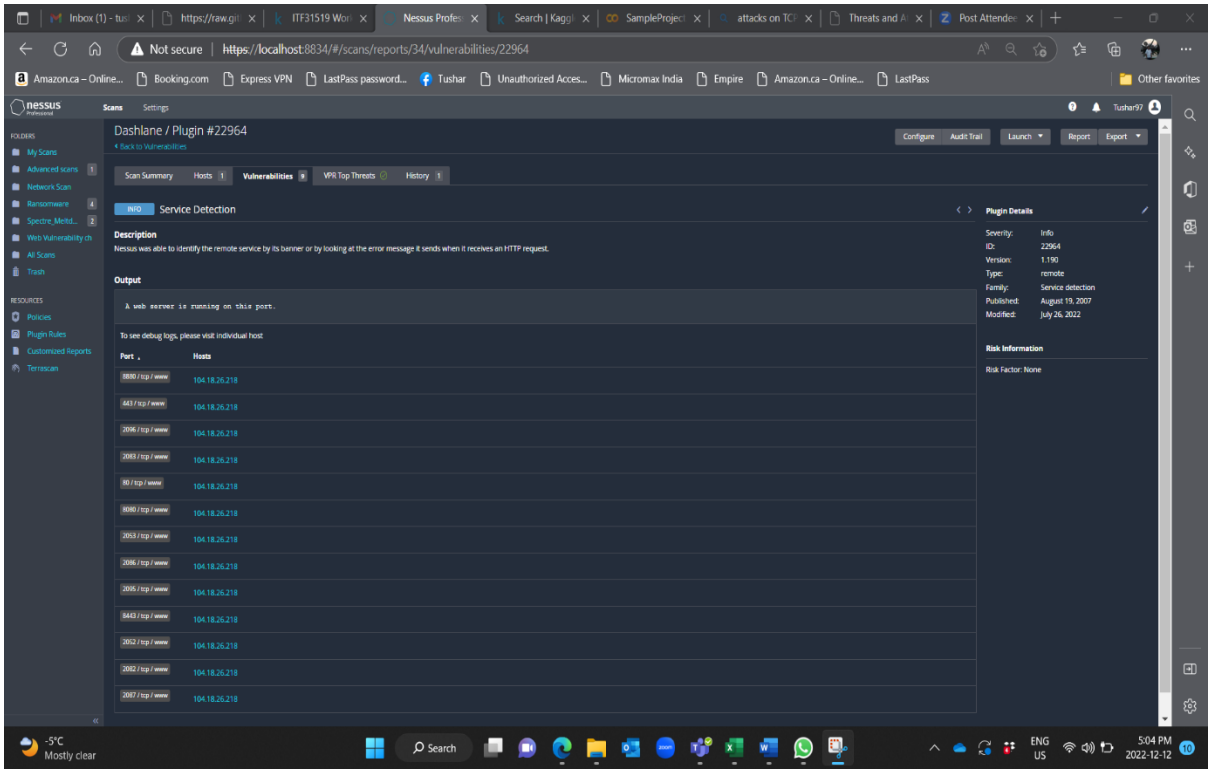
Dashlane:


Not secure https://localhost:8834/#/scans/reports/34/scan-summary
nessus
Scans
Settings
Dashlane
Back to Network Scan
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 9
VPR Top Threats
History 1
Scan Details
0 Critical Vulnerabilities
0 High Vulnerabilities
0 Medium Vulnerabilities
0 Low Vulnerabilities
Details
Scan Name: Dashlane
Plugin Set: 202212072011
CVSS_Score: CVSS_V3
Scan Template: Basic Network Scan
Scan Start: December 7 at 7:53 PM
Scan End: December 7 at 8:34 PM
Top 5 Operating Systems Detected During Scan
Linux (Other)
Authentication / Credential Info (Hosts)
0 SUCCEEDED
1 FAILED
Scan Durations
00:40:39 SCAN DURATION
00:23:27 MEDIAN SCAN TIME PER HOST
00:23:27 MAX SCAN TIME
Policy Details
Basic Overview
Scan Policy: Basic Network Scan
Plugins Timeout: 320
Feed Type: ProFeed
Report Overview
Diable DNS Resolution: No
Display Superseded Patches: Yes
Credential Settings Overview
Preferred SSH Port: 22
SSH Client Version: OpenSSH_5.0
Assessment Overview
Override Normal Accuracy: Normal
Perform Thorough Tests: No
Enable CGI Scanning: No
Advanced Overview
Enable Safe Checks: Yes
Network Timeout (in Seconds): 5
Port Scanner Overview
SYN: Yes
UDP: No
TCP: No
Port Scan Range: default

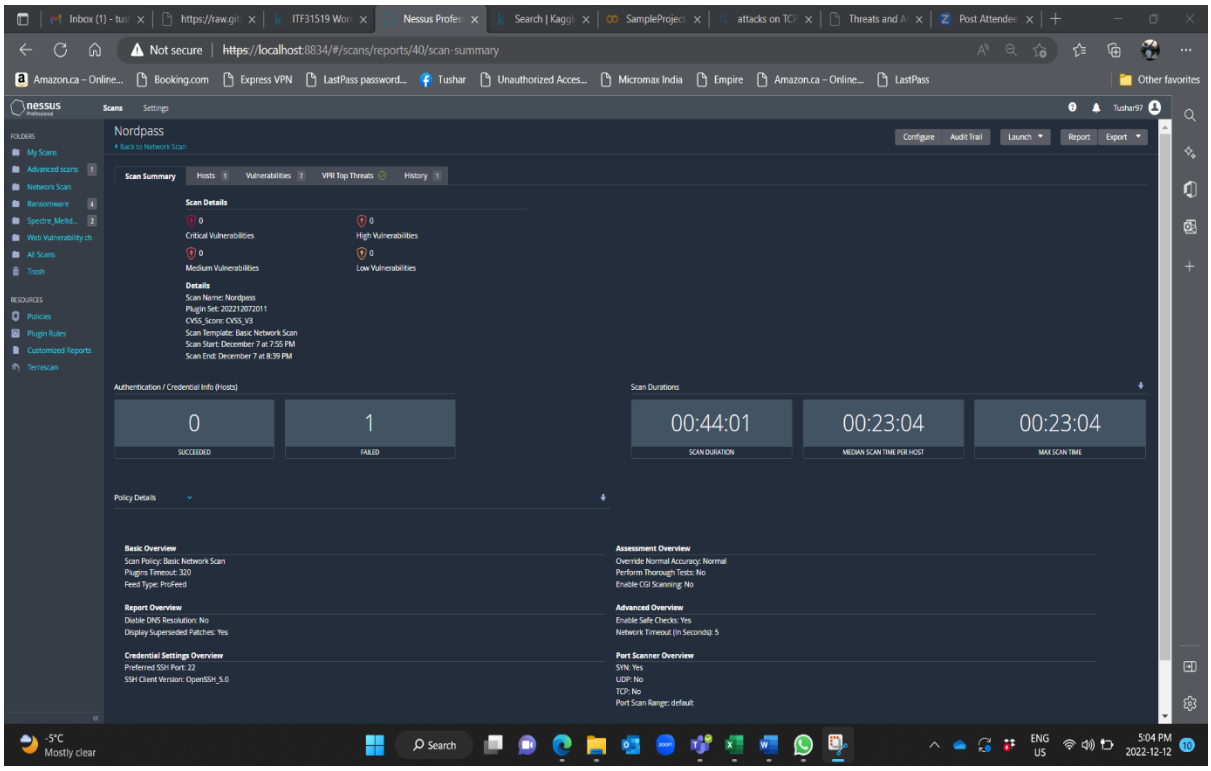

Not secure https://localhost:8834/#/scans/reports/34/vulnerabilities
nessus
Scans
Settings
Dashlane
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 9
VPR Top Threats
History 1
Filter
Search Vulnerabilities
9 Vulnerabilities
Sev
Score
Name
Family
Count
INFO
HTTP (Multiple Issues)
Web Servers
26
Nessus SYN scanner
Port scanners
13
Service Detection
Service detection
13
Common Platform Enumeration (CPE)
General
1
Device Type
General
1
Nessus Scan Information
Settings
1
OS Identification
General
1
TCP/IP Timestamps Supported
General
1
Traceroute Information
General
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: December 7 at 7:53 PM
End: December 7 at 8:34 PM
Elapsed: 41 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
-5°C
Mostly clear
Search
ENG
US
5:02 PM
2022-12-12

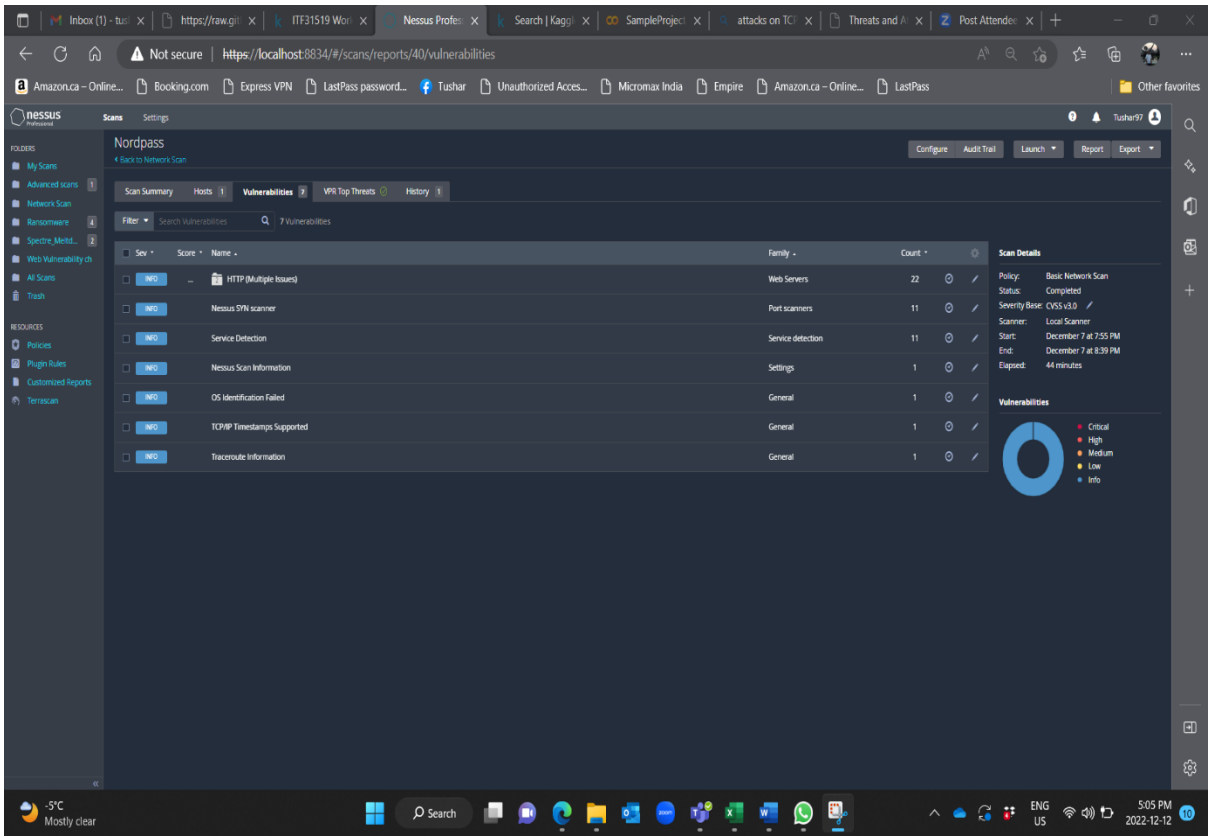

Not secure https://localhost:8834/#/scans/reports/34/vulnerabilities/10287
nessus
Scans
Settings
Dashlane / Plugin #10287
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 9
VPR Top Threats
History 1
INFO
Traceroute Information
Description
Makes a traceroute to the remote host.
Output
For your information, here is the traceroute from 192.168.2.22 to 104.18.26.218 :
192.168.2.22
192.168.2.1
10.11.23.105
?
64.230.38.184
142.124.127.224
64.230.78.196
64.230.79.89
198.32.118.206
172.70.112.2
104.18.26.218
Hop Count: 10
To see debug logs, please visit individual host
Port
Hosts
0 / udp
104.18.26.218
Plugin Details
Severity: Info
ID: 10287
Version: 1.67
Type: remote
Family: General
Published: November 27, 1999
Modified: August 20, 2020
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:03 PM
2022-12-12

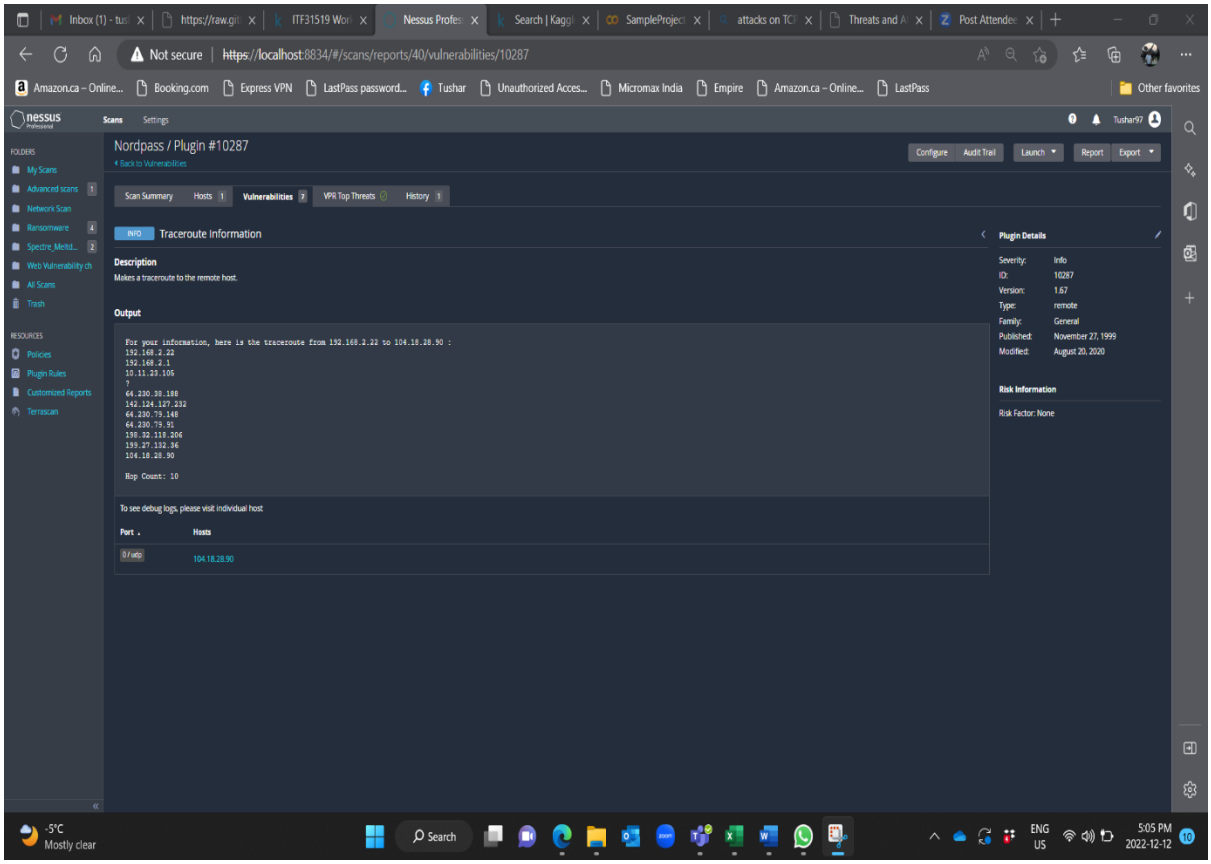

Not secure | https://localhost:8834/#/scans/reports/34/vulnerabilities/11936
nessus
Scans
Settings
Dashlane / Plugin #11936
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 9
VPR Top Threats
History 1
INFO
OS Identification
Description
Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.
Output
Remote operating system : Linux Kernel 2.x
Confidence Level : 54
Method : SinFP
The remote host is running Linux Kernel 2.x
To see debug logs, please visit individual host
Port
Hosts
N/A
104.18.26.218
Plugin Details
Severity: Info
ID: 11936
Version: 2.61
Type: combined
Family: General
Published: December 9, 2003
Modified: March 9, 2022
Risk Information
Risk Factor: None
Vulnerability Information
Asset Inventory: True
-5°C
Mostly clear
Search
ENG
US
5:03 PM
2022-12-12

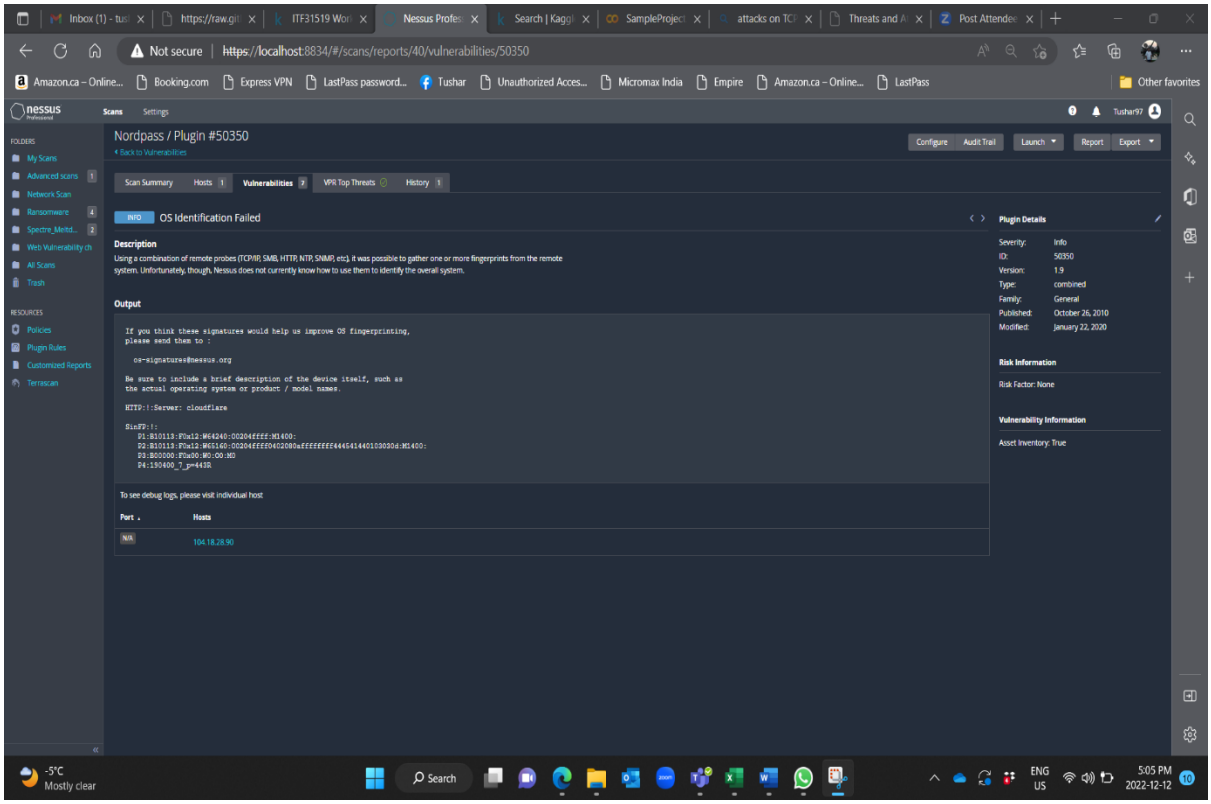

Not secure | https://localhost:8834/#/scans/reports/34/vulnerabilities/22964
nessus
Scans
Settings
Dashlane / Plugin #22964
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 9
VPR Top Threats
History 1
INFO
Service Detection
Description
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
Output
A web server is running on this port.
To see debug logs, please visit individual host
Port
Hosts
8880 / tcp / www
443 / tcp / www
2096 / tcp / www
2083 / tcp / www
80 / tcp / www
8080 / tcp / www
2053 / tcp / www
2086 / tcp / www
2095 / tcp / www
8443 / tcp / www
2052 / tcp / www
2082 / tcp / www
2087 / tcp / www
104.18.26.218
Plugin Details
Severity: Info
ID: 22964
Version: 1.190
Type: remote
Family: Service detection
Published: August 19, 2007
Modified: July 26, 2022
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:04 PM
2022-12-12

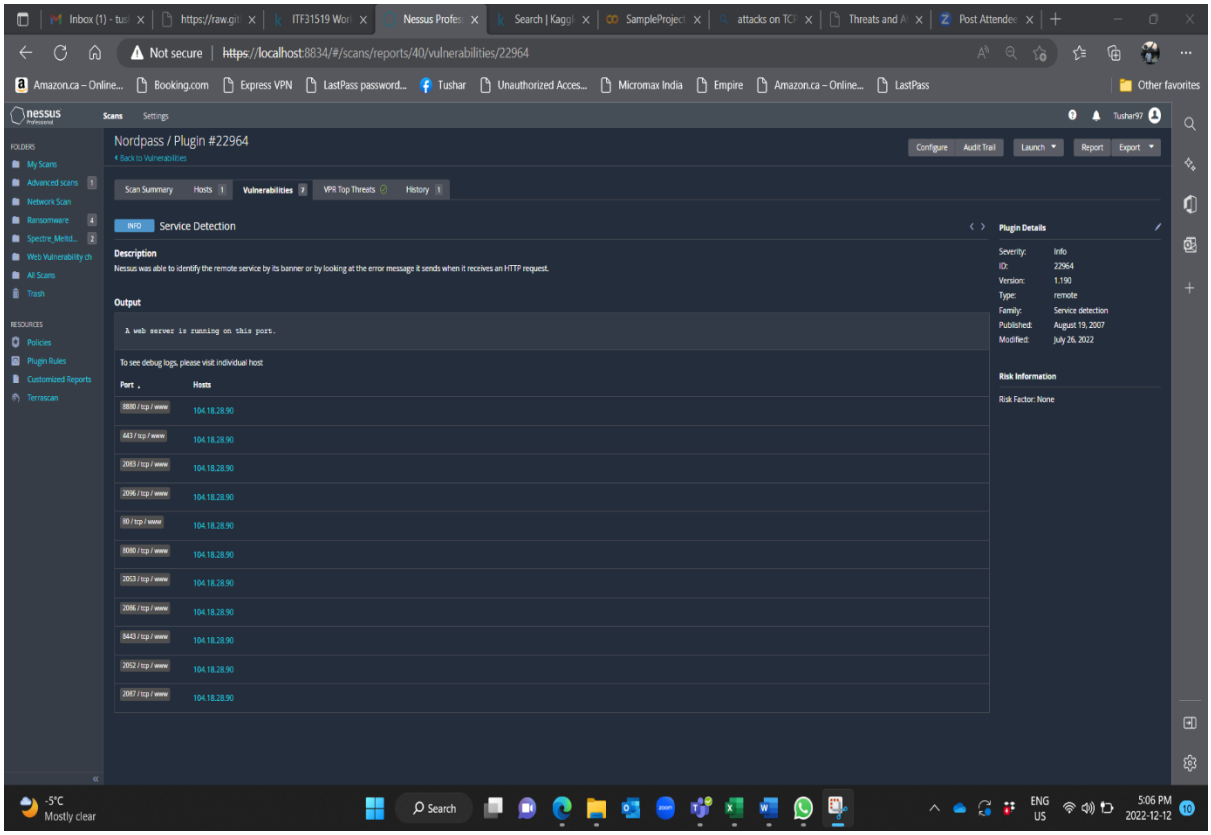
Nordpass:


Not secure | https://localhost:8834/#/scans/reports/40/scan-summary
nessus
Scans
Settings
Nordpass
Back to Network Scan
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 7
VPR Top Threats
History 1
Scan Details
0 Critical Vulnerabilities
0 High Vulnerabilities
0 Medium Vulnerabilities
0 Low Vulnerabilities
Details
Scan Name: Nordpass
Plugin Set: 202212072011
CVSS_Score: CVSS_V3
Scan Template: Basic Network Scan
Scan Start: December 7 at 7:55 PM
Scan End: December 7 at 8:39 PM
Authentication / Credential Info (Hosts)
0 SUCCEEDED
1 FAILED
Scan Durations
00:44:01 SCAN DURATION
00:23:04 MEDIAN SCAN TIME PER HOST
00:23:04 MAX SCAN TIME
Policy Details
Basic Overview
Scan Policy: Basic Network Scan
Plugins Timeout: 320
Feed Type: ProFeed
Assessment Overview
Override Normal Accuracy: Normal
Perform Thorough Tests: No
Enable CGI Scanning: No
Report Overview
Diable DNS Resolution: No
Display Superseded Patches: Yes
Advanced Overview
Enable Safe Checks: Yes
Network Timeout (in Seconds): 5
Credential Settings Overview
Preferred SSH Port: 22
SSH Client Version: OpenSSH_5.0
Port Scanner Overview
SYN: Yes
UDP: No
TCP: No
Port Scan Range: default
-5°C
Mostly clear
Search
ENG
US
5:04 PM
2022-12-12

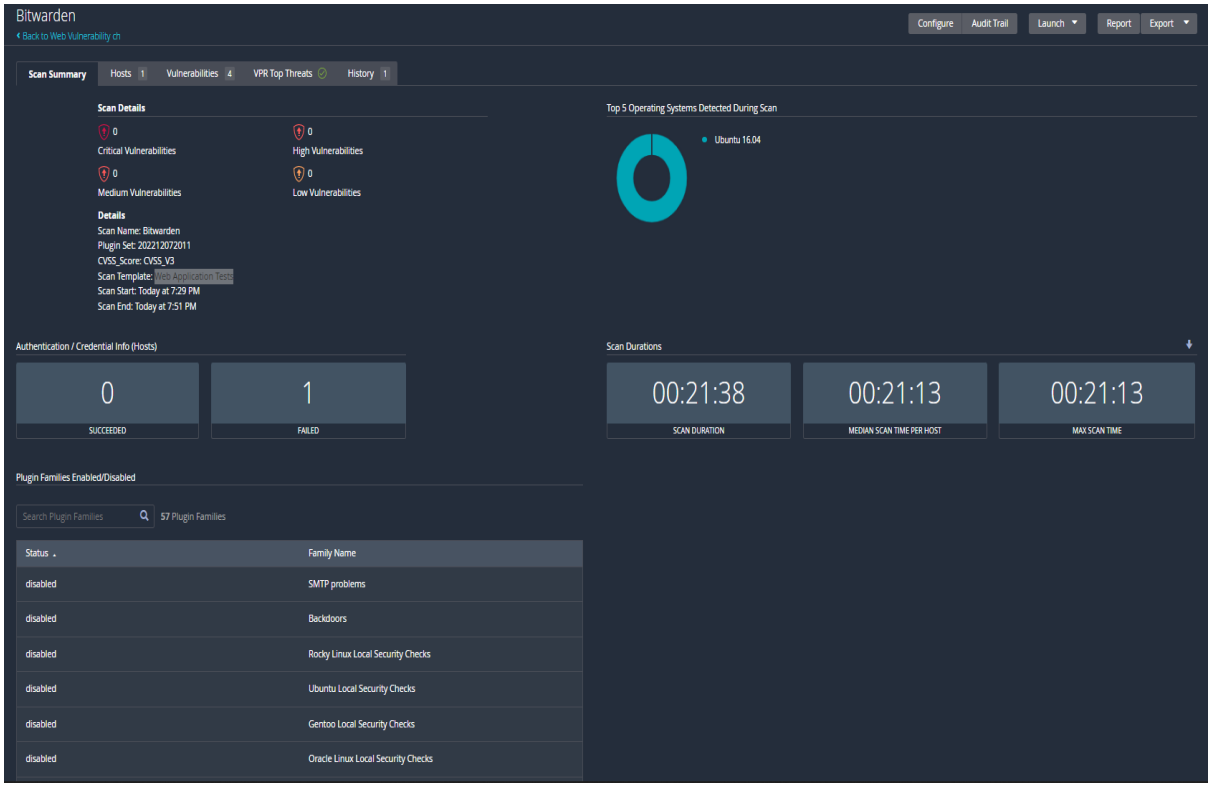

Not secure | https://localhost:8834/#/scans/reports/40/vulnerabilities
nessus
Scans
Settings
Nordpass
Back to Network Scan
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 7
VPR Top Threats
History 1
Filter
Search Vulnerabilities
7 Vulnerabilities
Sev
Score
Name
Family
Count
INFO HTTP (Multiple Issues) Web Servers 22
INFO Nessus SYN scanner Port scanners 11
INFO Service Detection Service detection 11
INFO Nessus Scan Information Settings 1
INFO OS Identification Failed General 1
INFO TCP/IP Timestamps Supported General 1
INFO Traceroute Information General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: December 7 at 7:55 PM
End: December 7 at 8:39 PM
Elapsed: 44 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
-5°C
Mostly clear
Search
ENG
US
5:05 PM
2022-12-12

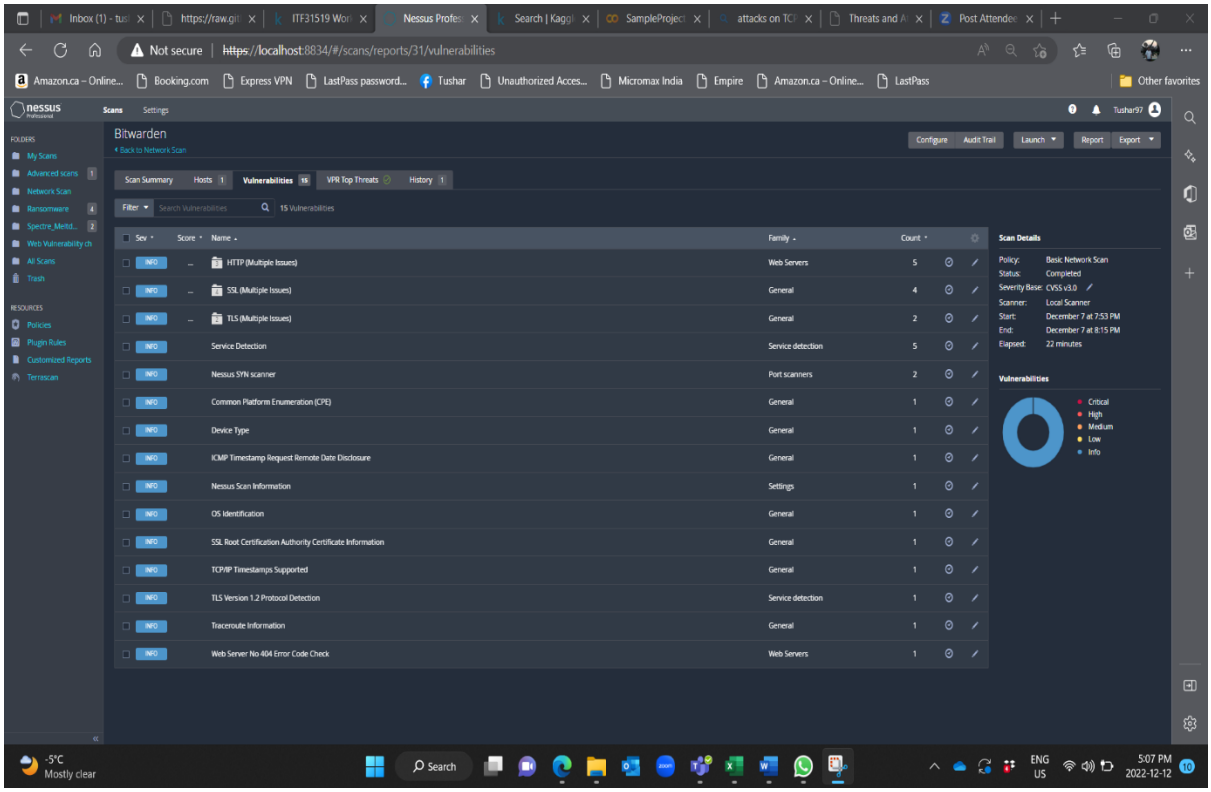

Not secure https://localhost:8834/#/scans/reports/40/vulnerabilities/10287
nessus
Scans
Settings
Nordpass / Plugin #10287
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 7
VPR Top Threats
History 1
INFO
Traceroute Information
Description
Makes a traceroute to the remote host.
Output
For your information, here is the traceroute from 192.168.2.22 to 104.18.28.90 :
192.168.2.22
192.168.2.1
10.11.23.105
?
64.230.38.188
142.124.127.232
64.230.79.148
64.230.79.91
198.32.118.206
199.27.132.36
104.18.28.90
Hop Count: 10
To see debug logs, please visit individual host
Port
Hosts
0 / udp
104.18.28.90
Plugin Details
Severity: Info
ID: 10287
Version: 1.67
Type: remote
Family: General
Published: November 27, 1999
Modified: August 20, 2020
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:05 PM
2022-12-12

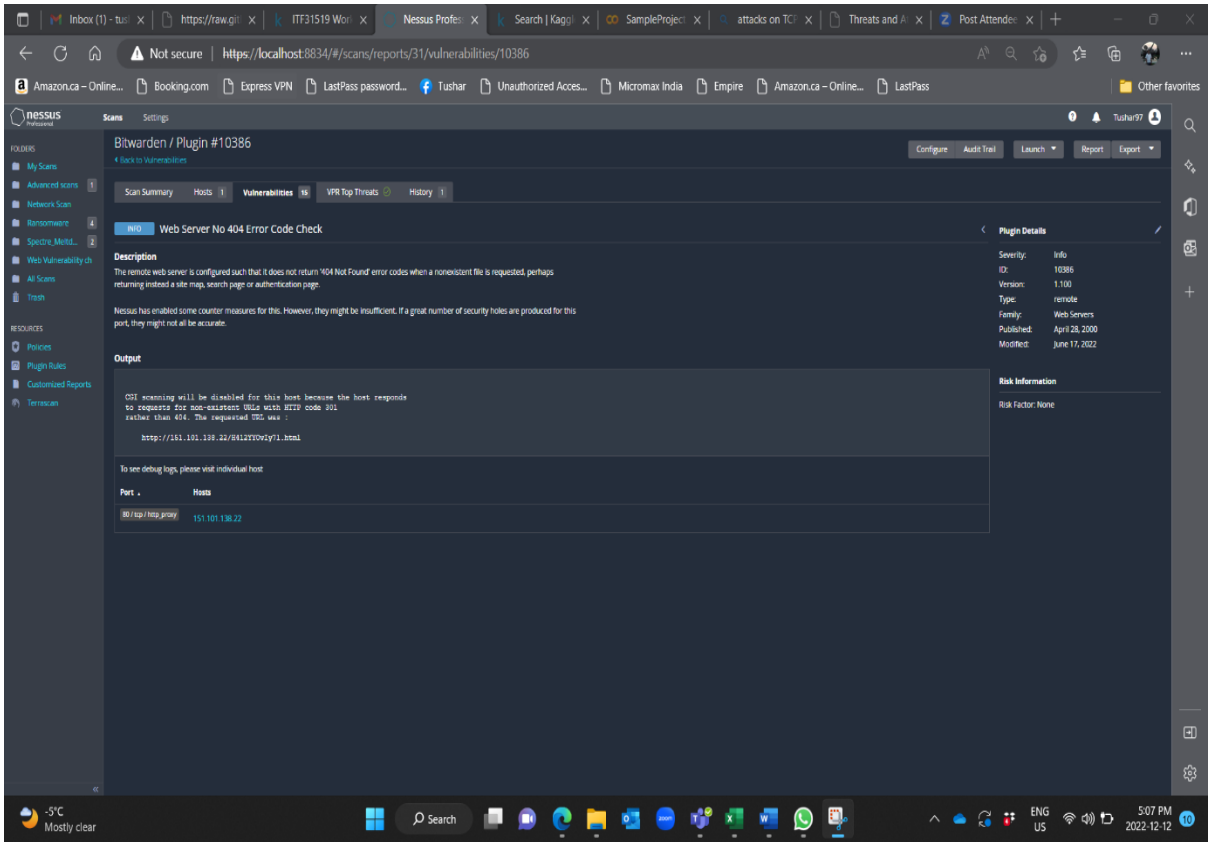

Not secure https://localhost:8834/#/scans/reports/40/vulnerabilities/50350
nessus
Scans
Settings
Nordpass / Plugin #50350
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 7
VPR Top Threats
History 1
INFO
OS Identification Failed
Description
Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.
Output
If you think these signatures would help us improve OS fingerprinting,
please send them to :
os-signatures@nessus.org
Be sure to include a brief description of the device itself, such as
the actual operating system or product / model names.
HTTP:!:Server: cloudflare
SinFP:!:
P1:B10113:F0x12:W64240:O0204ffff:M1400:
P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414403030d:M1400:
P3:B00000:F0x00:W0:O0:M0
P4:190400_7_p=443R
To see debug logs, please visit individual host
Port
Hosts
N/A
104.18.28.90
Plugin Details
Severity: Info
ID: 50350
Version: 1.9
Type: combined
Family: General
Published: October 26, 2010
Modified: January 22, 2020
Risk Information
Risk Factor: None
Vulnerability Information
Asset Inventory: True
-5°C
Mostly clear
Search
ENG
US
5:05 PM
2022-12-12

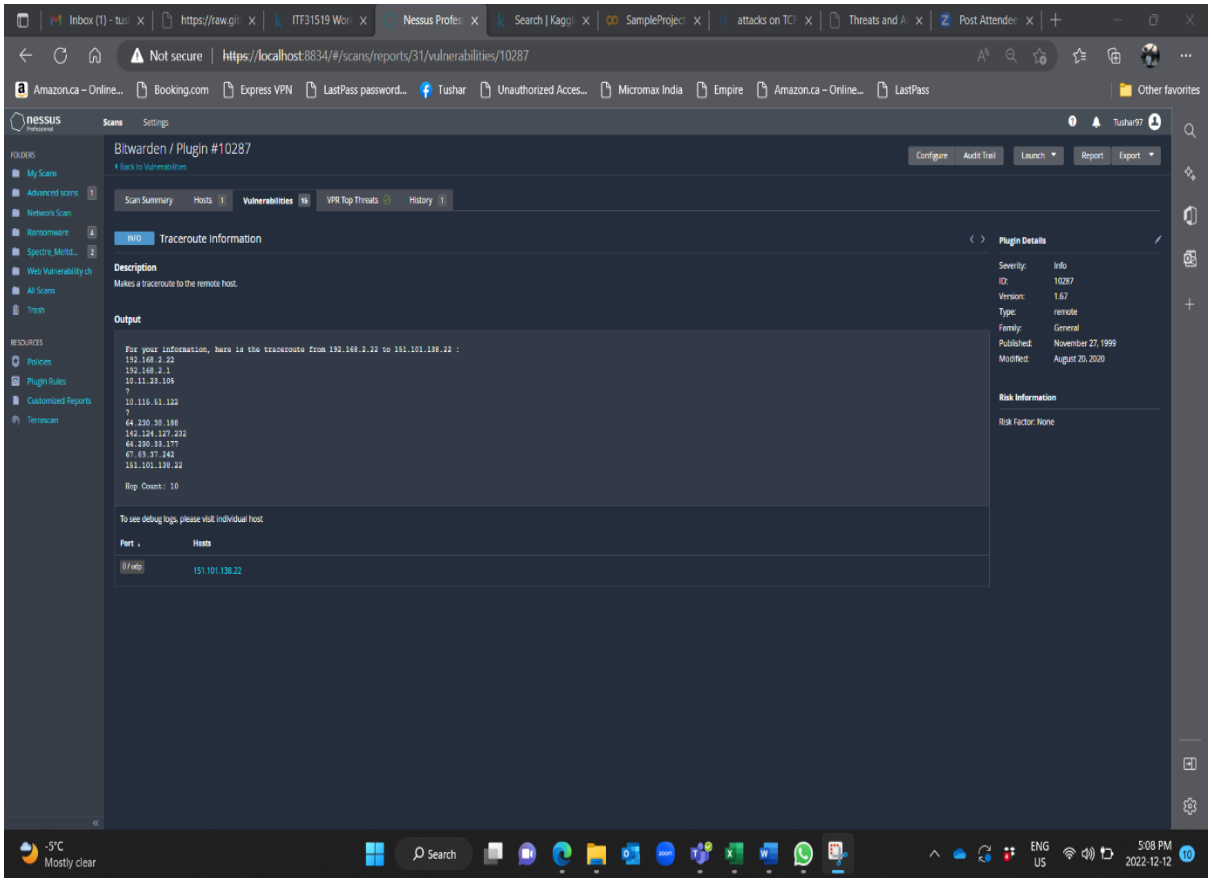

Not secure
https://localhost:8834/#/scans/reports/40/vulnerabilities/22964
nessus
Scans
Settings
Nordpass / Plugin #22964
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 7
VPR Top Threats
History 1
INFO
Service Detection
Description
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
Output
A web server is running on this port.
To see debug logs, please visit individual host
Port
Hosts
Plugin Details
Severity: Info
ID: 22964
Version: 1.190
Type: remote
Family: Service detection
Published: August 19, 2007
Modified: July 26, 2022
Risk Information
Risk Factor: None
104.18.28.90
-5°C
Mostly clear
Search
ENG
US
5:06 PM
2022-12-12

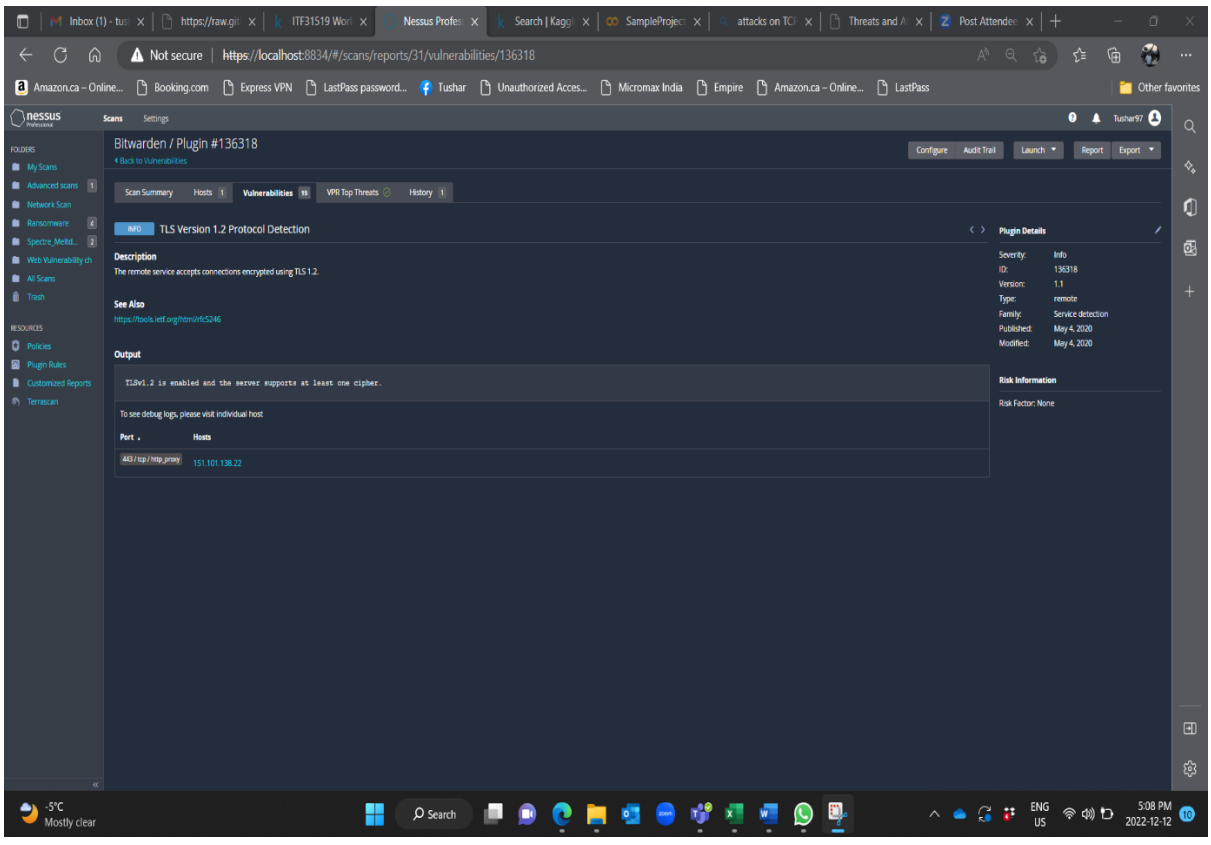
Bitwarden

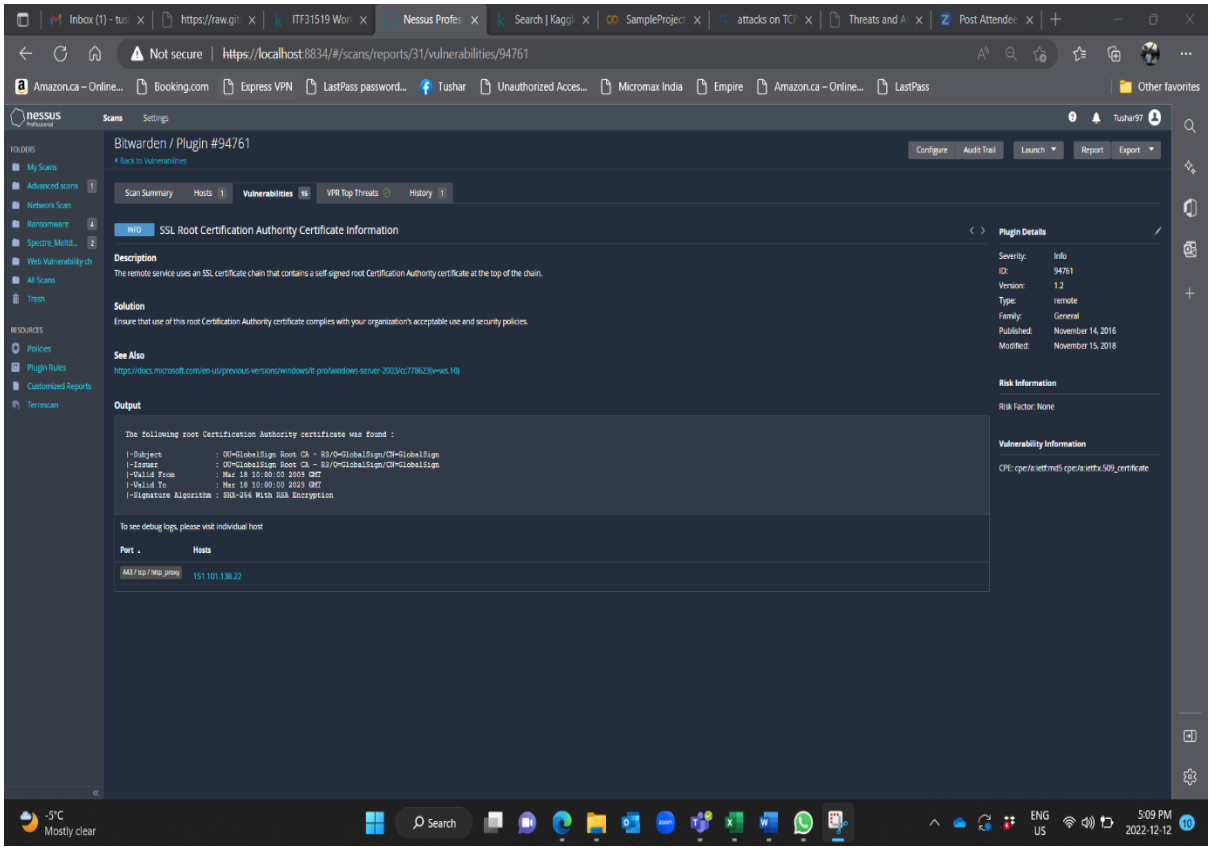

Bitwarden
Back to Web Vulnerability ch
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 4
VPR Top Threats
History 1
Scan Details
0
Critical Vulnerabilities
0
High Vulnerabilities
0
Medium Vulnerabilities
0
Low Vulnerabilities
Details
Scan Name: Bitwarden
Plugin Set: 202212072011
CVSS_Score: CVSS_V3
Scan Template: Web Application Tests
Scan Start: Today at 7:29 PM
Scan End: Today at 7:51 PM
Top 5 Operating Systems Detected During Scan
Ubuntu 16.04
Authentication / Credential Info (Hosts)
0
SUCCEEDED
1
FAILED
Scan Durations
00:21:38
SCAN DURATION
00:21:13
MEDIAN SCAN TIME PER HOST
00:21:13
MAX SCAN TIME
Plugin Families Enabled/Disabled
Search Plugin Families
57 Plugin Families
Status
Family Name
disabled
SMTP problems
disabled
Backdoors
disabled
Rocky Linux Local Security Checks
disabled
Ubuntu Local Security Checks
disabled
Gentoo Local Security Checks
disabled
Oracle Linux Local Security Checks

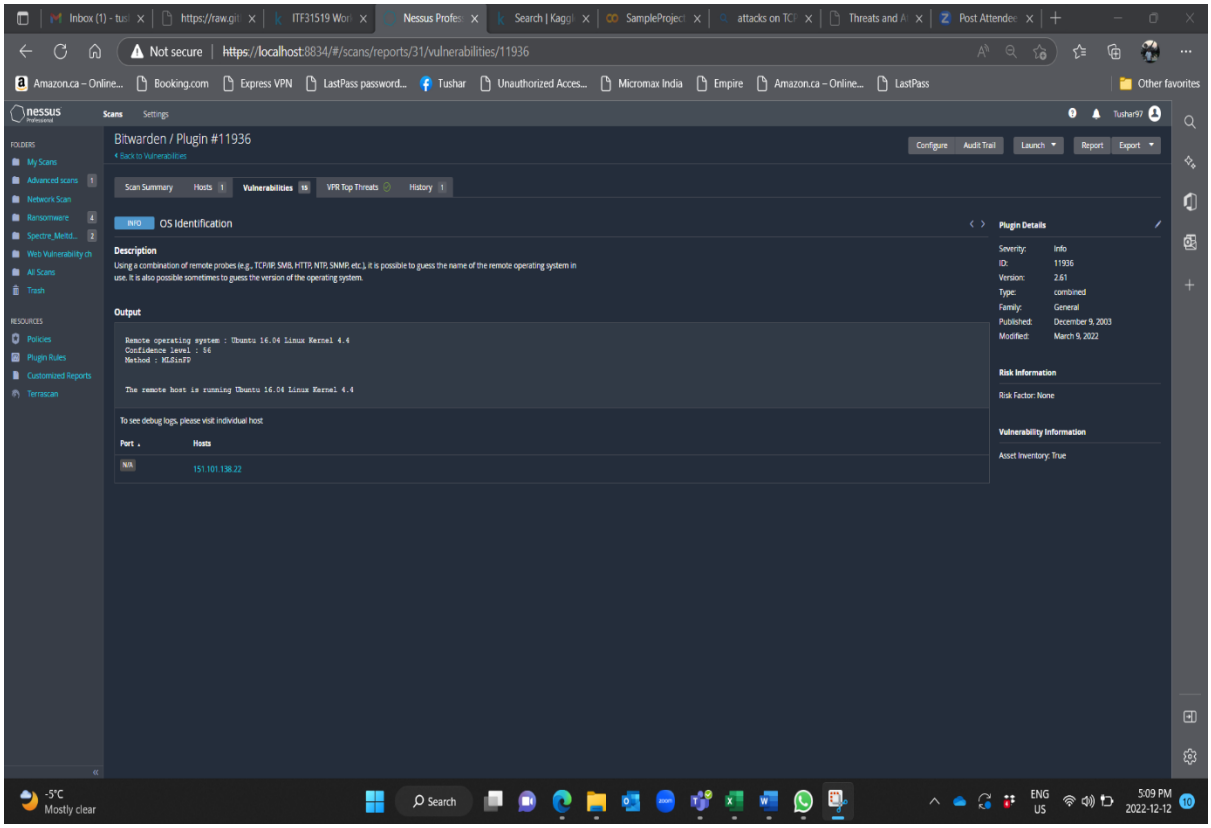

Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities
nessus
Scans
Settings
Bitwarden
Back to Network Scan
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
15 Vulnerabilities
Sev
Score
Name
Family
Count
HTTP (Multiple Issues)
Web Servers
SSL (Multiple Issues)
General
TLS (Multiple Issues)
Service Detection
Service detection
Nessus SYN scanner
Port scanners
Common Platform Enumeration (CPE)
Device Type
ICMP Timestamp Request Remote Date Disclosure
Nessus Scan Information
Settings
OS Identification
SSL Root Certification Authority Certificate Information
TCP/IP Timestamps Supported
TLS Version 1.2 Protocol Detection
Traceroute Information
Web Server No 404 Error Code Check
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: December 7 at 7:53 PM
End: December 7 at 8:15 PM
Elapsed: 22 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
-5°C
Mostly clear
Search
ENG
US
5:07 PM
2022-12-12

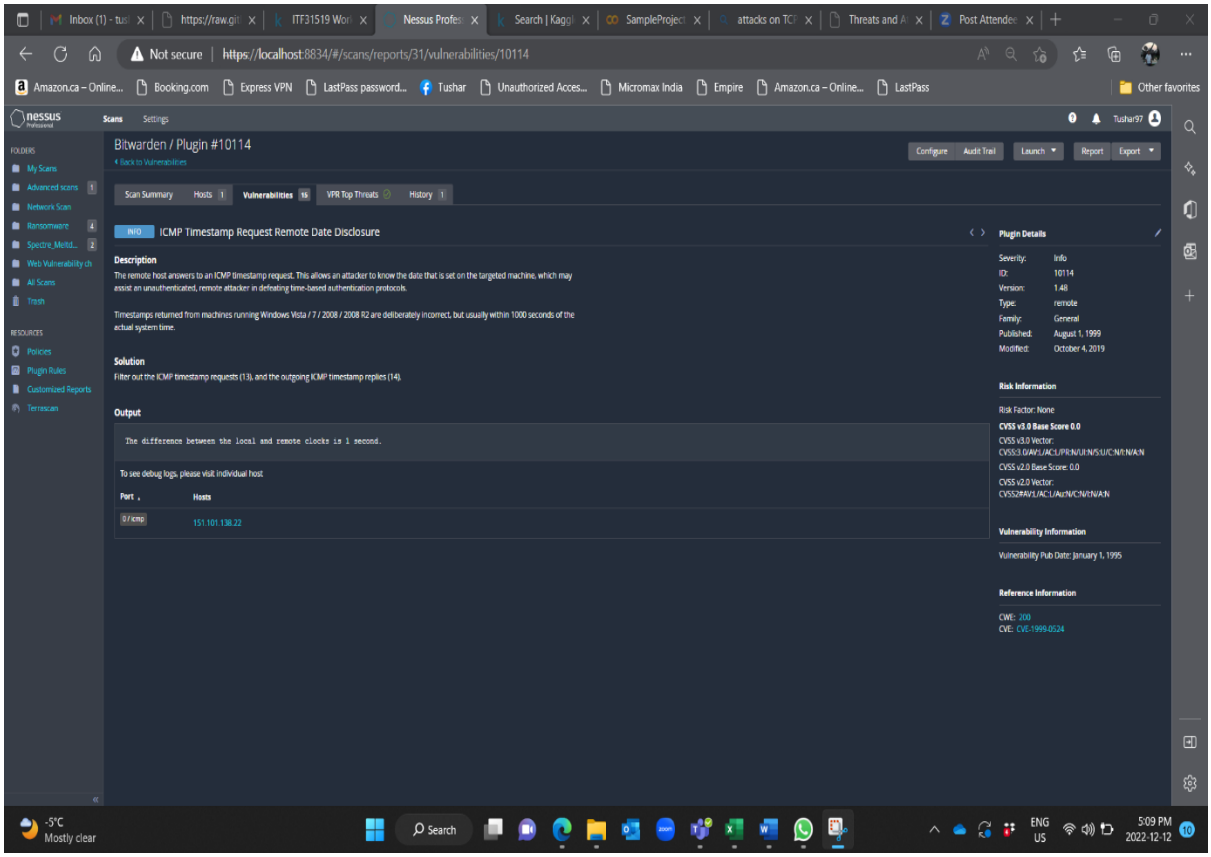

Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/10386
nessus
Scans
Settings
Bitwarden / Plugin #10386
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
INFO
Web Server No 404 Error Code Check
Description
The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.
Output
CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was :
http://151.101.138.22/E412YTOvlyY1.html
To see debug logs, please visit individual host
Port
Hosts
80 / tcp / http_proxy
151.101.138.22
Plugin Details
Severity: Info
ID: 10386
Version: 1.100
Type: remote
Family: Web Servers
Published: April 28, 2000
Modified: June 17, 2022
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:07 PM
2022-12-12

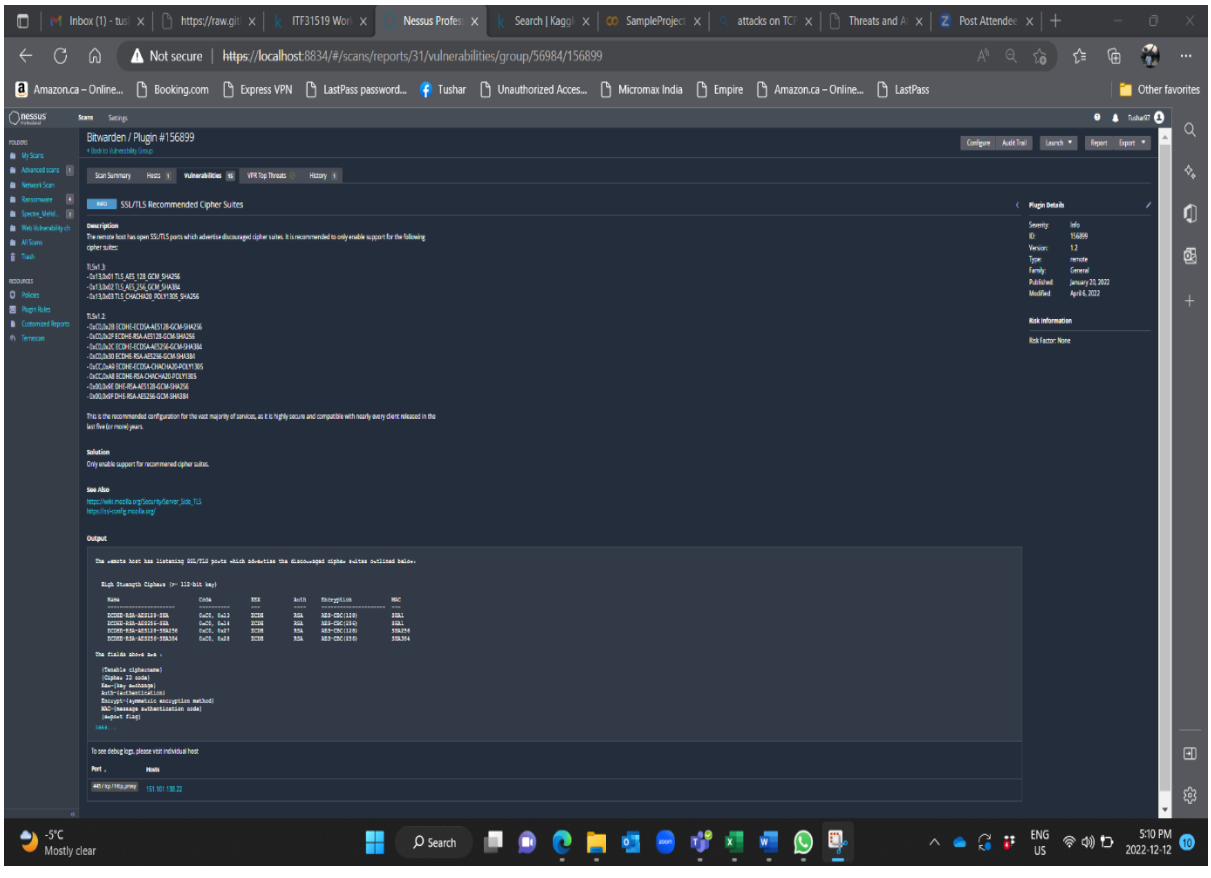

Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/10287
nessus
Scans
Settings
Bitwarden / Plugin #10287
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
INFO
Traceroute Information
Description
Makes a traceroute to the remote host.
Output
For your information, here is the traceroute from 192.168.2.22 to 151.101.138.22 :
192.168.2.22
192.168.2.1
10.11.23.105
?
10.116.61.122
?
64.230.58.188
142.124.127.232
64.230.33.177
67.69.37.242
151.101.138.22
Hop Count: 10
To see debug logs, please visit individual host
Port
Hosts
0 / udp
151.101.138.22
Plugin Details
Severity: Info
ID: 10287
Version: 1.67
Type: remote
Family: General
Published: November 27, 1999
Modified: August 20, 2020
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:08 PM
2022-12-12

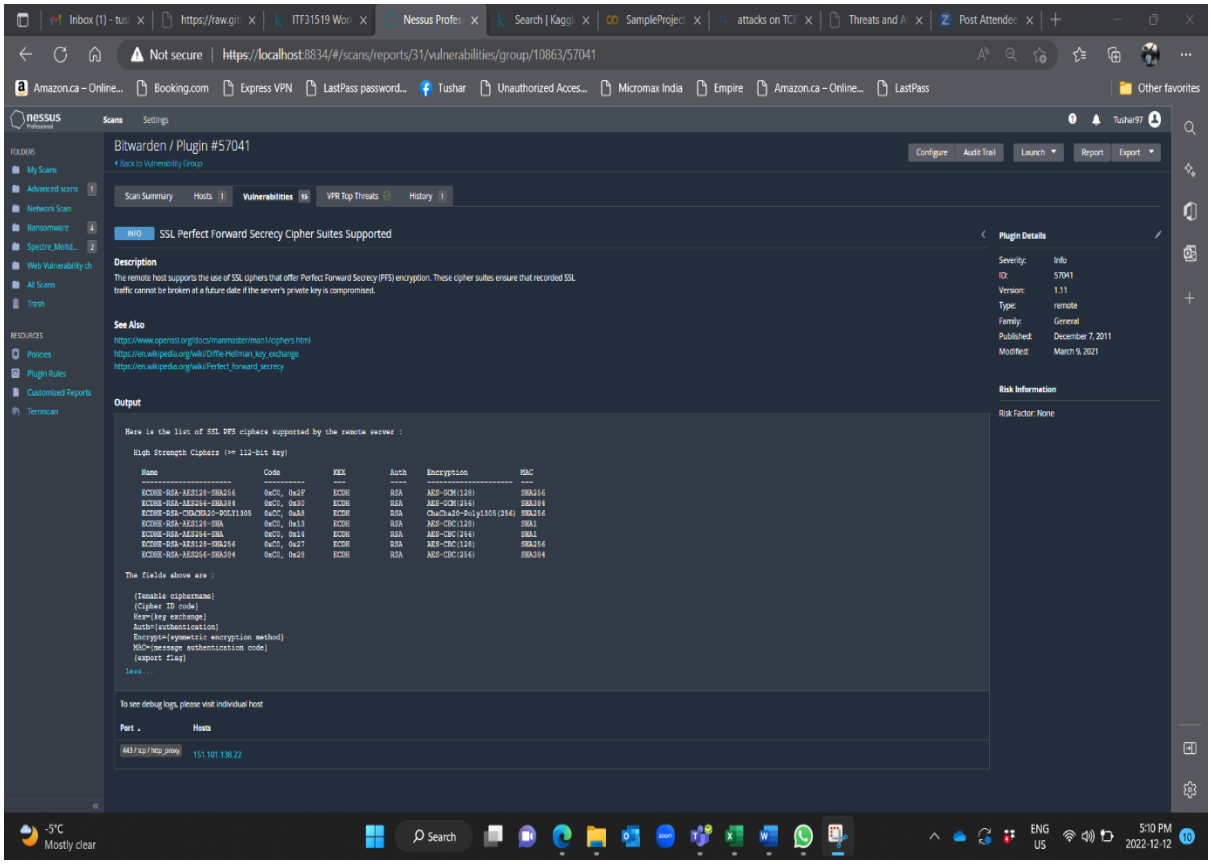

Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/136318
nessus
Scans
Settings
Bitwarden / Plugin #136318
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
INFO
TLS Version 1.2 Protocol Detection
Description
The remote service accepts connections encrypted using TLS 1.2.
See Also
https://tools.ietf.org/html/rfc5246
Output
TLSv1.2 is enabled and the server supports at least one cipher.
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / http_proxy
151.101.138.22
Plugin Details
Severity: Info
ID: 136318
Version: 1.1
Type: remote
Family: Service detection
Published: May 4, 2020
Modified: May 4, 2020
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:08 PM
2022-12-12

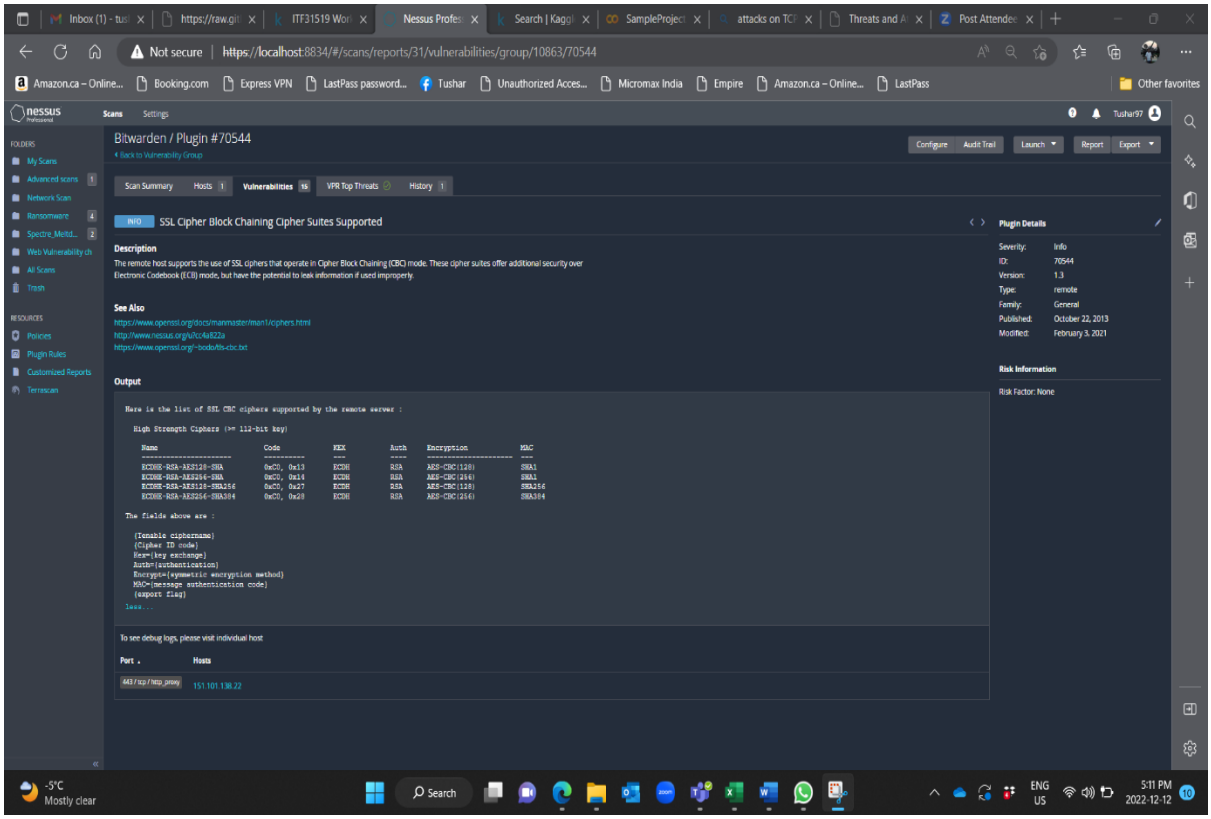

Not secure https://localhost:8834/#/scans/reports/31/vulnerabilities/94761
Bitwarden / Plugin #94761
SSL Root Certification Authority Certificate Information
Description
The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.
Solution
Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.
See Also
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)
Output
The following root Certification Authority certificate was found :
|-Subject : OU=GlobalSign Root CA - R3/O=GlobalSign/CN=GlobalSign
|-Issuer : OU=GlobalSign Root CA - R3/O=GlobalSign/CN=GlobalSign
|-Valid From : Mar 18 10:00:00 2009 GMT
|-Valid To : Mar 18 10:00:00 2029 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / http_proxy
151.101.138.22
Plugin Details
Severity: Info
ID: 94761
Version: 1.2
Type: remote
Family: General
Published: November 14, 2016
Modified: November 15, 2018
Risk Information
Risk Factor: None
Vulnerability Information
CPE: cpe:/a:ietf:md5 cpe:/a:ietf:x.509_certificate

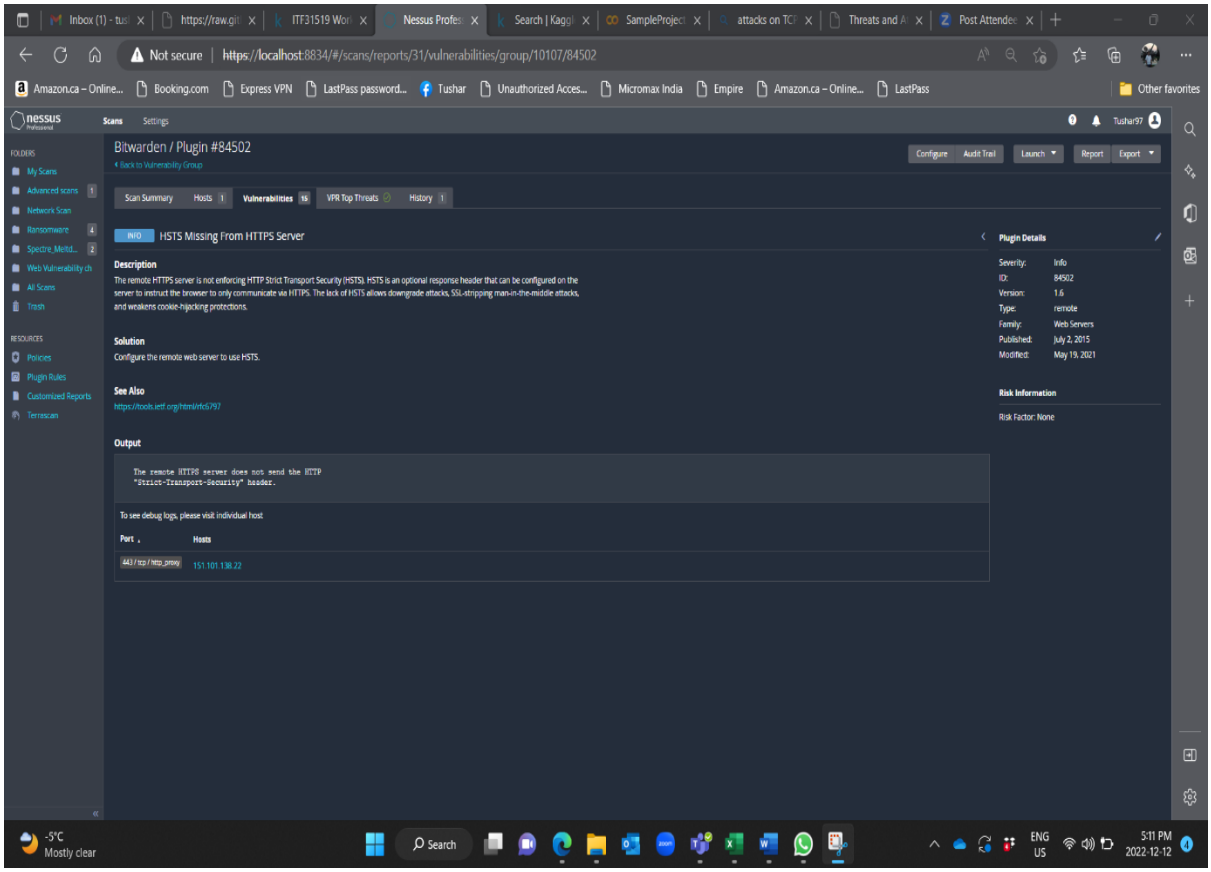

Not secure https://localhost:8834/#/scans/reports/31/vulnerabilities/11936
Bitwarden / Plugin #11936
OS Identification
Description
Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.
Output
Remote operating system : Ubuntu 16.04 Linux Kernel 4.4
Confidence Level : 56
Method : MLSinFP
The remote host is running Ubuntu 16.04 Linux Kernel 4.4
To see debug logs, please visit individual host
Port
Hosts
N/A
151.101.138.22
Plugin Details
Severity: Info
ID: 11936
Version: 2.61
Type: combined
Family: General
Published: December 9, 2003
Modified: March 9, 2022
Risk Information
Risk Factor: None
Vulnerability Information
Asset Inventory: True

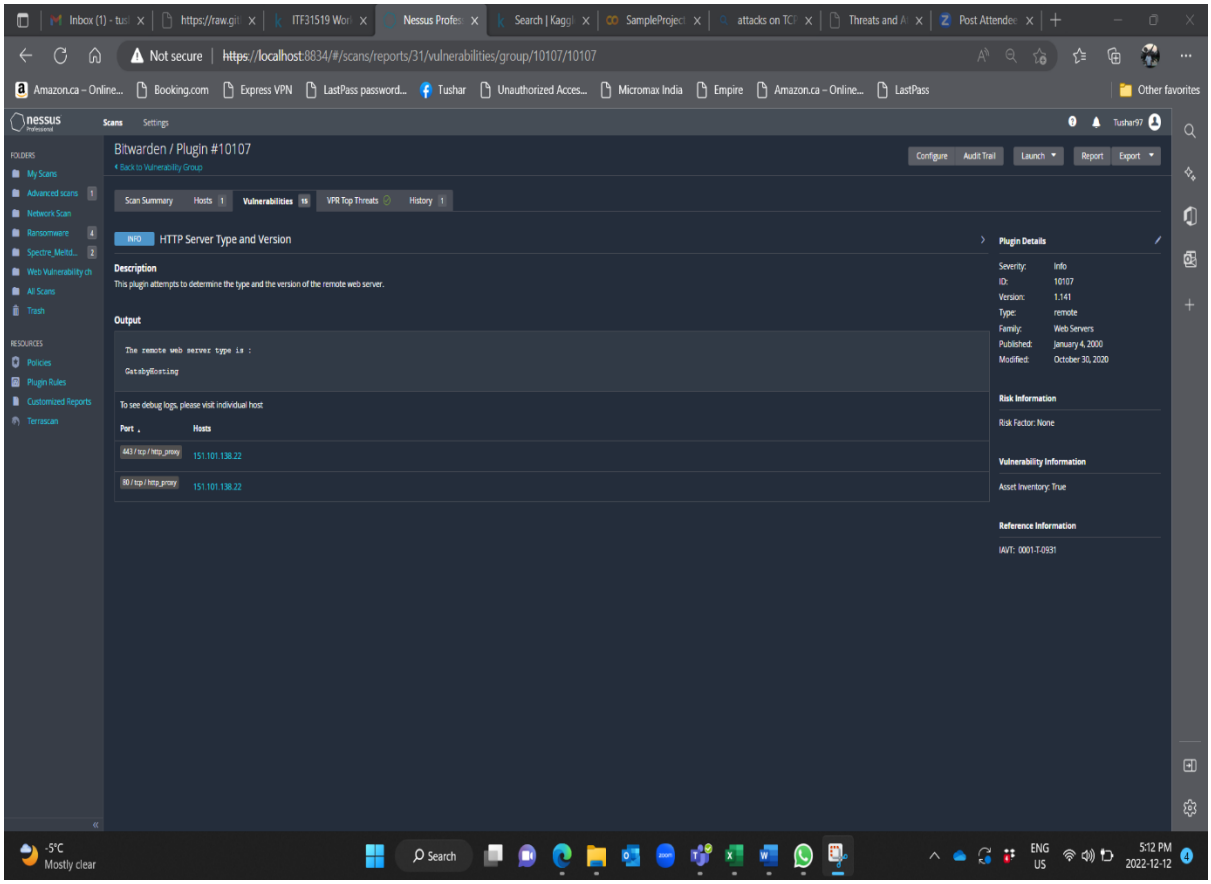

Not secure
https://localhost:8834/#/scans/reports/31/vulnerabilities/10114
Bitwarden / Plugin #10114
ICMP Timestamp Request Remote Date Disclosure
Description
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.
Solution
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Output
The difference between the local and remote clocks is 1 second.
To see debug logs, please visit individual host
Port
Hosts
0 / icmp
151.101.138.22
Plugin Details
Severity: Info
ID: 10114
Version: 1.48
Type: remote
Family: General
Published: August 1, 1999
Modified: October 4, 2019
Risk Information
Risk Factor: None
CVSS v3.0 Base Score 0.0
CVSS v3.0 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
CVSS v2.0 Base Score: 0.0
CVSS v2.0 Vector: CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N
Vulnerability Information
Vulnerability Pub Date: January 1, 1995
Reference Information
CWE: 200
CVE: CVE-1999-0524


Not secure
https://localhost:8834/#/scans/reports/31/vulnerabilities/group/56984/156899
Bitwarden / Plugin #156899
SSL/TLS Recommended Cipher Suites
Description
The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:
Solution
Only enable support for recommened cipher suites.
See Also
https://wiki.mozilla.org/Security/Server_Side_TLS
https://ssl-config.mozilla.org/
Output
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:
To see debug logs, please visit individual host
Port
Hosts
Plugin Details
Severity: Info
ID: 156899
Version: 1.2
Type: remote
Family: General
Published: January 20, 2022
Modified: April 6, 2022
Risk Information
Risk Factor: None


Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/group/10863/57041
nessus
Scans
Settings
Bitwarden / Plugin #57041
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
INFO
SSL Perfect Forward Secrecy Cipher Suites Supported
Description
The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.
See Also
https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy
Output
Here is the list of SSL PFS ciphers supported by the remote server :
High Strength Ciphers (>= 112-bit key)
Name Code KEX Auth Encryption MAC
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8 ECDH RSA ChaCha20-Poly1305(256) SHA256
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
The fields above are :
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
less...
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / http_proxy
151.101.138.22
Plugin Details
Severity: Info
ID: 57041
Version: 1.11
Type: remote
Family: General
Published: December 7, 2011
Modified: March 9, 2021
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:10 PM
2022-12-12


Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/group/10863/70544
nessus
Scans
Settings
Bitwarden / Plugin #70544
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 15
VPR Top Threats
History 1
INFO
SSL Cipher Block Chaining Cipher Suites Supported
Description
The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.
See Also
https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt
Output
Here is the list of SSL CBC ciphers supported by the remote server :
High Strength Ciphers (>= 112-bit key)
Name Code KEX Auth Encryption MAC
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
The fields above are :
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
less...
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / http_proxy
151.101.138.22
Plugin Details
Severity: Info
ID: 70544
Version: 1.3
Type: remote
Family: General
Published: October 22, 2013
Modified: February 3, 2021
Risk Information
Risk Factor: None
-5°C
Mostly clear
Search
ENG
US
5:11 PM
2022-12-12


Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/group/10107/84502
Bitwarden / Plugin #84502
HSTS Missing From HTTPS Server
Description
The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.
Solution
Configure the remote web server to use HSTS.
See Also
https://tools.ietf.org/html/rfc6797
Output
The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / http_proxy
151.101.138.22
Plugin Details
Severity: Info
ID: 84502
Version: 1.6
Type: remote
Family: Web Servers
Published: July 2, 2015
Modified: May 19, 2021
Risk Information
Risk Factor: None


Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/group/10107/10107
Bitwarden / Plugin #10107
HTTP Server Type and Version
Description
This plugin attempts to determine the type and the version of the remote web server.
Output
The remote web server type is :
GatsbyHosting
To see debug logs, please visit individual host
Port
Hosts
443 / tcp / http_proxy
151.101.138.22
80 / tcp / http_proxy
151.101.138.22
Plugin Details
Severity: Info
ID: 10107
Version: 1.141
Type: remote
Family: Web Servers
Published: January 4, 2000
Modified: October 30, 2020
Risk Information
Risk Factor: None
Vulnerability Information
Asset Inventory: True
Reference Information
IAVT: 0001-T-0931