

# UNIVERSITY CYBER ATTACK PROJECT

Investigator: Terakala sai teja

## Client details

**Complete Name:** Samantha R.collen

**Personal email id:** Samantha.collen,r@gmail.com

**Official email id:**profsamantha@pu.edu.com

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

**Note:** Learners can use any platform like Kali Linux.

### 1. Install Nessus:

- Visit the Nessus download page: <https://www.tenable.com/products/nessus>
- Download and install Nessus for your platform.

### 2. Configure Nessus:

- Open Nessus in your web browser (usually <https://localhost:8834>).
- Complete the initial setup and create a user account.

### 3. Create a New Scan:

- Click on 'New Scan'.
- Select 'Basic Network Scan' template.
- Enter the scan details, including the IP range (e.g., 192.168.1.0/24).

### 4. Run the Scan:

- Start the scan and wait for it to complete.

### 5. Analyze the Results:

- View the scan results to identify the devices on the network.
- Look for details about the operating systems and any detected vulnerabilities.

```
Command Prompt
Microsoft Windows [Version 10.0.22631.3880]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::563:8903:be33:ca26%3
    IPv4 Address. . . . . : 192.168.1.76
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\HP>
```

tenable

Nessus Essentials

Scans

Settings

FOLDERS

My Scans

cyber attack

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

Improving Your Cloud Security Using JIT Access for...

Read More

cyber attack project

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 23

History 1

Filter

Search Hosts

1 Host

Host	Vulnerabilities
192.168.1.76	4

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 11:36 PM

End: Today at 11:41 PM

Elapsed: 6 minutes

Vulnerabilities

Critical

High

Medium

Low

Severity	Count
Critical	4
High	19
Medium	0
Low	0

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

Note: Learners can use any open-source data sets for vulnerability like NVD (National Vulnerability Database).

CVE - CVE

https://cve.mitre.org

CVE

CVE List

CNAs

WGs

Board

About

News

Search CVE List

Downloads

Data Feeds

Update a CVE Record

Request CVE IDs

TOTAL CVE Records: 240830

NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) and CVE Record Format JSON are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024. New CVE List download format is available now on CVE.ORG.

The mission of the CVE@ Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.  
[Go to new News page >>](#)

CVE Podcast

Podcasts have moved to the new CVE website.  
[Go to new Podcast page >>](#)

CVE Blog

Blogs have moved to the new CVE website.

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Join today!


Business benefits

No fee or contract

Few requirements

Easy to join

Go to new CVE website



[Learn How to Become a CNA >>>](#)

Newest CVE Records Feed

Feed of newly published CVE Records on X (formerly Twitter).  
[Go to new @CVEnew >>](#)

New & Updated CVE Records

cvelistV5 bulk downloads repository on GitHub includes a "Releases" feed of new & updated CVE Records.  
[Go to cvelistV5 "Releases" page >> > > >](#)

CVE - Search Results

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=2021-44228

CVE

Search CVE List

Downloads

Data Feeds

Update a CVE Record

Request CVE IDs

TOTAL CVE Records: 240830

NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) and CVE Record Format JSON are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024. New CVE List download format is available now on CVE.ORG.

HOME > CVE > SEARCH RESULTS

Search Results

There are 1 CVE Records that match your search.

Name	Description
<a href="#">CVE-2021-44228</a>	Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

BACK TO TOP


SEARCH CVE USING KEYWORDS:

Submit

You can also search by reference using the [CVE Reference Maps](#).

For More Information: [CVE Request Web Form](#) (select "Other" from dropdown)

← ↻ 🔒 https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE+2021-44228 🔍 ☆ 📄 ⌵ 🔄 🌐 ⚙️ ⋮



[CVE List ▾](#) [CNAs ▾](#) [WGs ▾](#) [Board ▾](#) [About ▾](#) [News ▾](#)

[Search CVE List](#) [Downloads](#) [Data Feeds](#) [Update a CVE Record](#) [Request CVE IDs](#)

**TOTAL CVE Records: 240830**

**NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) and CVE Record Format JSON are underway.**

**NOTICE: Support for the legacy CVE download formats ended on June 30, 2024.**  
**New CVE List download format is available now on CVE.ORG.**


HOME > CVE > SEARCH RESULTS

## Search Results

There are **18825** CVE Records that match your search.

Name	Description
<a href="#">CVE-2024-7081</a>	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been rated as critical. Affected by this issue is some unknown function: file expcatadd.php. The manipulation of the argument title leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272366 is the identifier assigned to this vulnerability.
<a href="#">CVE-2024-7080</a>	A vulnerability was found in SourceCodester Insurance Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /E-Insurance/. The manipulation leads to direct request. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272365 was assigned to this vulnerability.
<a href="#">CVE-2024-7079</a>	A flaw was found in the Openshift console. The /API/helm/verify endpoint is tasked to fetch and verify the installation of a Helm chart from a URI that is remote HTTP/HTTPS or local. Access to this endpoint is gated by the authHandlerWithUser() middleware function. Contrary to its name, this middleware function does not verify the validity of the user's credentials. As a result, unauthenticated users can access this endpoint.
<a href="#">CVE-2024-7069</a>	A vulnerability, which was classified as critical, has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects an unknown processing of the file /employee_gatepass/classes/Master.php?f=delete_department. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272351.
<a href="#">CVE-2024-7068</a>	A vulnerability classified as problematic has been found in SourceCodester Insurance Management System 1.0. This affects an unknown part of the file

← ↻ 🔒 https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE+2021-44228 🔍 ☆ 📄 ⌵ 🔄 🌐 ⚙️ ⋮



[CVE List ▾](#) [CNAs ▾](#) [WGs ▾](#) [Board ▾](#) [About ▾](#) [News ▾](#)

[Search CVE List](#) [Downloads](#) [Data Feeds](#) [Update a CVE Record](#) [Request CVE IDs](#)

**TOTAL CVE Records: 240830**

**NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) and CVE Record Format JSON are underway.**

**NOTICE: Support for the legacy CVE download formats ended on June 30, 2024.**  
**New CVE List download format is available now on CVE.ORG.**

HOME > CVE > SEARCH RESULTS

## Search Results

There are **18825** CVE Records that match your search.

Name	Description
<a href="#">CVE-2024-7081</a>	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been rated as critical. Affected by this issue is some unknown function: file expcatadd.php. The manipulation of the argument title leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272366 is the identifier assigned to this vulnerability.
<a href="#">CVE-2024-7080</a>	A vulnerability was found in SourceCodester Insurance Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /E-Insurance/. The manipulation leads to direct request. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272365 was assigned to this vulnerability.
<a href="#">CVE-2024-7079</a>	A flaw was found in the Openshift console. The /API/helm/verify endpoint is tasked to fetch and verify the installation of a Helm chart from a URI that is remote HTTP/HTTPS or local. Access to this endpoint is gated by the authHandlerWithUser() middleware function. Contrary to its name, this middleware function does not verify the validity of the user's credentials. As a result, unauthenticated users can access this endpoint.
<a href="#">CVE-2024-7069</a>	A vulnerability, which was classified as critical, has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects an unknown processing of the file /employee_gatepass/classes/Master.php?f=delete_department. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272351.
<a href="#">CVE-2024-7068</a>	A vulnerability classified as problematic has been found in SourceCodester Insurance Management System 1.0. This affects an unknown part of the file

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

**Note:** Learners can orchestrate any attacks like Denial-of-service attack and create reports based on it.

To identify if the victim's terminal is affected by a MiTM attack:

1. Monitor network traffic for unusual patterns.
2. Use tools like Wireshark to capture and analyze packets.
3. Look for signs of interception or manipulation.

Signs of MiTM Attack:

Unexpected ARP replies.

```
C:\Users\HP>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::866:39d4:3ce:beef%3
    IPv4 Address. . . . . : 192.168.1.76
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\HP>
```

zsh: corrupt history file /home/kali/.zsh\_history

(kali@kali)-[~]

\$ ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
inet6 fe80::f79f:4c5f:6cdb:a166 prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:d2:26:79 txqueuelen 1000 (Ethernet)  
RX packets 133 bytes 53128 (51.8 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 151 bytes 20331 (19.8 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

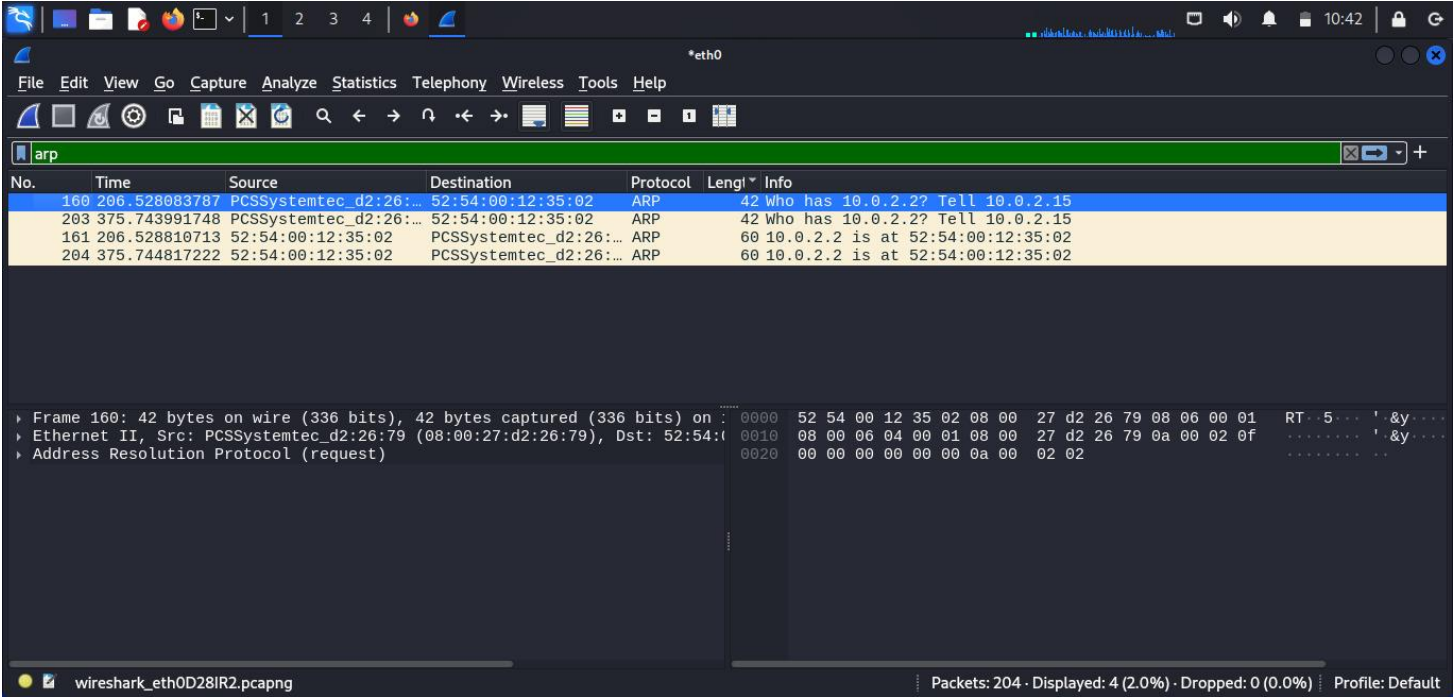
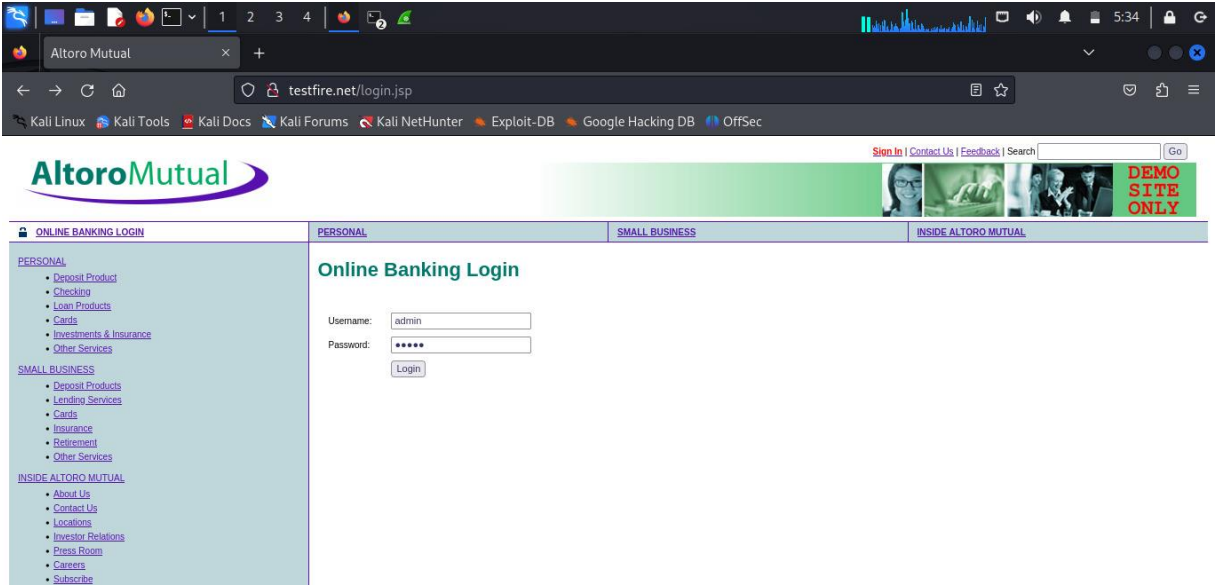
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 8 bytes 480 (480.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 8 bytes 480 (480.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

92.168.1.255	ff-ff-ff-ff-ff-ff	static
24.0.0.22	01-00-5e-00-00-16	static
24.0.0.251	01-00-5e-00-00-fb	static
24.0.0.252	01-00-5e-00-00-fc	static
39.255.102.18	01-00-5e-7f-66-12	static
39.255.255.250	01-00-5e-7f-ff-fa	static
55.255.255.255	ff-ff-ff-ff-ff-ff	static

Internet Address	Physical Address	Type
192.168.1.65	3c-57-6c-2e-15-df	dynamic
192.168.1.66	be-37-92-39-22-99	dynamic
192.168.1.78	52-5b-2c-93-be-05	dynamic
192.168.1.86	10-5a-17-c5-48-db	dynamic
192.168.1.98	74-97-79-05-be-e3	dynamic
192.168.1.254	78-17-25-06-1b-50	dynamic



```
-> sudo nmap -sn 10.0.2.15/24
[sudo] password for kali:
aliSorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 10:
Nmap scan report for 10.0.2.2
Host is up (0.00014s latency).
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00012s latency).
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Nmap scan report for 10.0.2.15
```

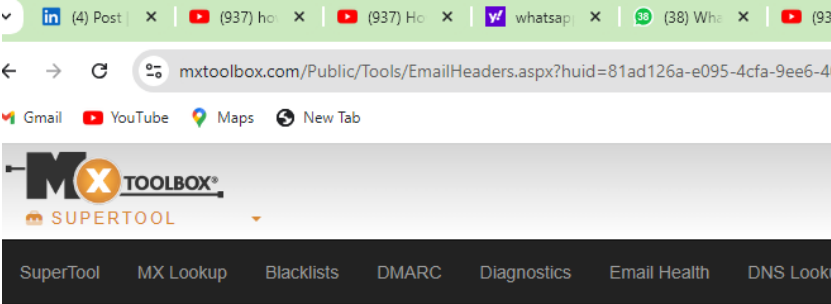


**Task 4:** Use email forensics analysis and identify the sender's IP address

**Note:** Learners can create a dummy email ID, perform this task, or send an email to anyone. They can identify the sender's IP address.

To identify the sender's IP address from an email:

- 1. Open the email and view its headers.
- 2. Look for the 'Received: from' field to find the sender's IP address.
- 3. Tools like Email Header Analyzer can help in parsing the headers.



**Header Analyzed**  
Email Subject: [Cybersecurity project](#)

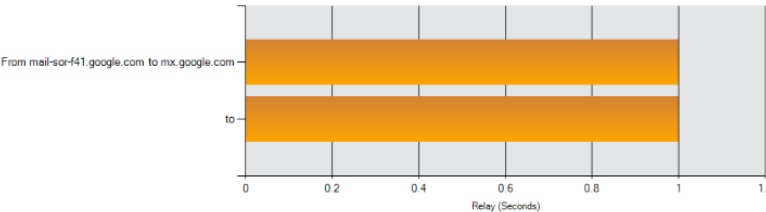
**Delivery Information**

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

**Relay Information**

Received	0 seconds
----------	-----------

Delay:



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mail-sor-f41.google.com 209.85.220.41	mx.google.com	SMTPS	7/26/2024 4:24:28 PM	✓
2	0 seconds		2002:a05:7010:2010:b0:3ea:bfbef8e1	SMTP	7/26/2024 4:24:28 PM	

**SPF and DKIM Information**

dmarc:gmail.com

Show

Solve Email Delivery Problems



```
→ sudo nmap -sn 10.0.2.15/24
[sudo] password for kali:
kaliSorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 10:
map scan report for 10.0.2.2
Host is up (0.00014s latency).
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
map scan report for 10.0.2.3
Host is up (0.00012s latency).
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
map scan report for 10.0.2.4
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
map scan report for 10.0.2.15
```

**Task5:** Submit the complete incidence report

