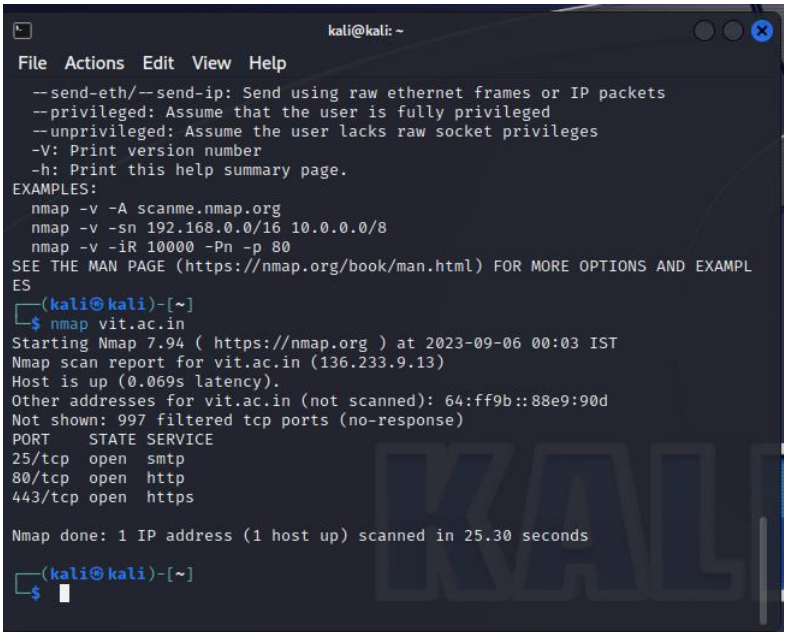
Stuti Maitra Sarkar
Assignment 2

Exploring tools in Kali Linux

N-Map:

Nmap, short for "Network Mapper," is a powerful network scanning tool used to discover and analyze devices and services on a network. It sends packets to target devices and interprets their responses to create a map of what's running on the network, including open ports, operating systems, and services, which can be valuable for network administrators and security professionals.

Using on vit.ac.in:



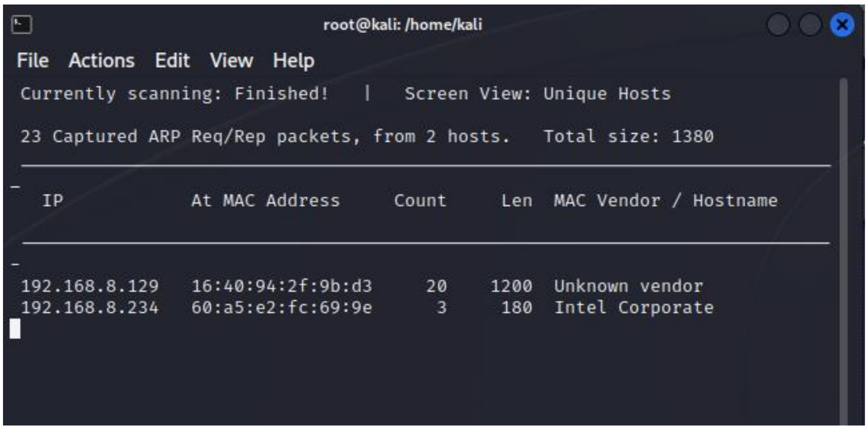
```
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPL
ES
┌──(kali㉿kali)-[~]
└─$ nmap vit.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 00:03 IST
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.069s latency).
Other addresses for vit.ac.in (not scanned): 64:ff9b::88e9:90d
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 25.30 seconds

┌──(kali㉿kali)-[~]
└─$
```

Netdiscover:

Netdiscover is a simple network scanning tool designed to help beginners find devices on a local network. It works by sending ARP (Address Resolution Protocol) requests to discover devices and their corresponding IP and MAC addresses. Netdiscover is often used for basic network reconnaissance and can be useful for identifying devices and their network configurations in a local area network (LAN).



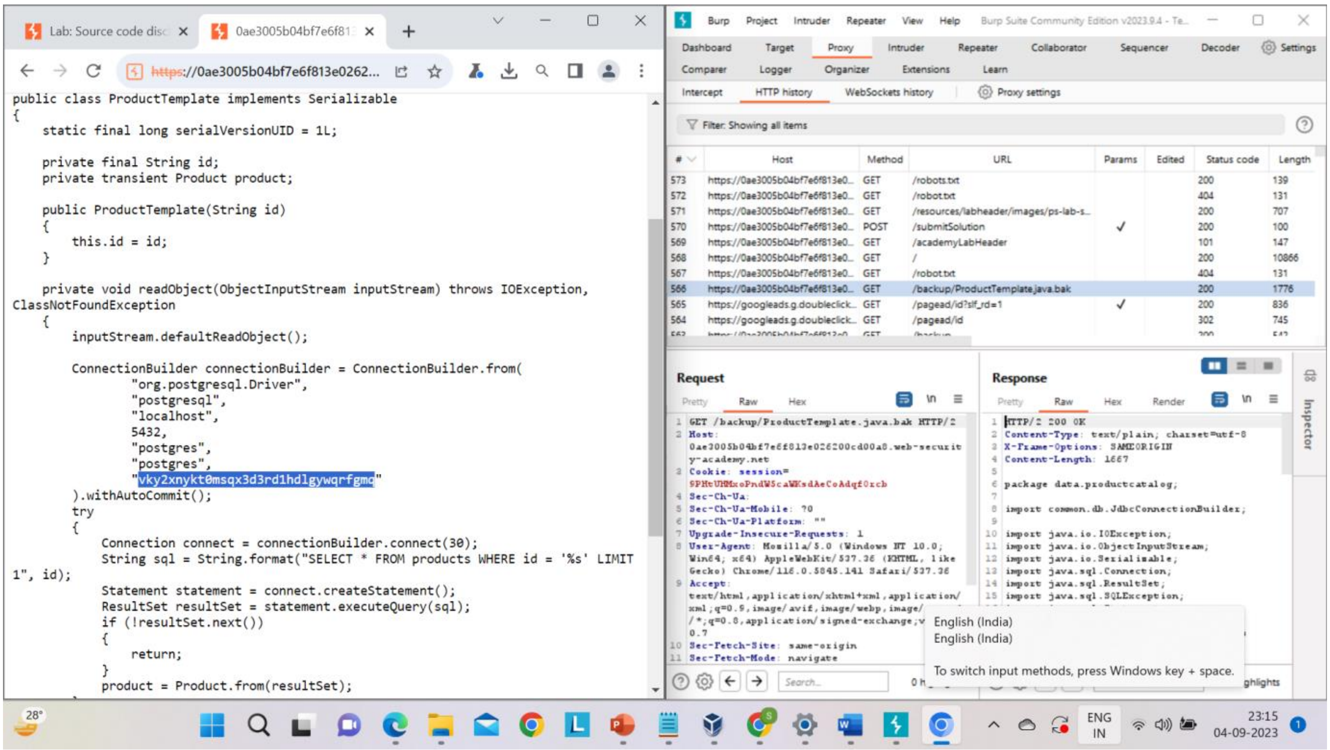
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 23 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 1380
 _____________________________________________________________________________
_
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
-
 192.168.8.129   16:40:94:2f:9b:d3     20    1200  Unknown vendor
 192.168.8.234   60:a5:e2:fc:69:9e      3     180  Intel Corporate
```

Stuti Maitra Sarkar
Assignment 2

Burpsuite:

Burp Suite is a comprehensive web application security testing tool used by security professionals and ethical hackers. It helps identify vulnerabilities in web applications by intercepting and analyzing web traffic, performing scans, and allowing users to manipulate requests and responses. Burp Suite assists in finding and fixing security issues like cross-site scripting (XSS) and SQL injection, making web applications more secure.


Lab: Source code disc
0ae3005b04bf7e6f81
https://0ae3005b04bf7e6f813e0262...
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.9.4 - Te...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter: Showing all items
English (India)
English (India)
To switch input methods, press Windows key + space.
ENG IN
23:15
04-09-2023

```
public class ProductTemplate implements Serializable
{
    static final long serialVersionUID = 1L;

    private final String id;
    private transient Product product;

    public ProductTemplate(String id)
    {
        this.id = id;
    }

    private void readObject(ObjectInputStream inputStream) throws IOException,
ClassNotFoundException
    {
        inputStream.defaultReadObject();

        ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
                "org.postgresql.Driver",
                "postgresql",
                "localhost",
                5432,
                "postgres",
                "postgres",
                "vky2xnykt0msqx3d3rd1hdlgywqrfgmq"
        ).withAutoCommit();
        try
        {
            Connection connect = connectionBuilder.connect(30);
            String sql = String.format("SELECT * FROM products WHERE id = '%s' LIMIT
1", id);
            Statement statement = connect.createStatement();
            ResultSet resultSet = statement.executeQuery(sql);
            if (!resultSet.next())
            {
                return;
            }
            product = Product.from(resultSet);
```

#	Host	Method	URL	Params	Edited	Status code	Length
573	https://0ae3005b04bf7e6f813e0...	GET	/robots.txt			200	139
572	https://0ae3005b04bf7e6f813e0...	GET	/robot.txt			404	131
571	https://0ae3005b04bf7e6f813e0...	GET	/resources/labheader/images/ps-lab-s...			200	707
570	https://0ae3005b04bf7e6f813e0...	POST	/submitSolution	✓		200	100
569	https://0ae3005b04bf7e6f813e0...	GET	/academyLabHeader			101	147
568	https://0ae3005b04bf7e6f813e0...	GET	/			200	10866
567	https://0ae3005b04bf7e6f813e0...	GET	/robot.txt			404	131
566	https://0ae3005b04bf7e6f813e0...	GET	/backup/ProductTemplate.java.bak			200	1776
565	https://googleads.g.doubleclick...	GET	/pagead/id?slf_rd=1	✓		200	836
564	https://googleads.g.doubleclick...	GET	/pagead/id			302	745

Request

```
GET /backup/ProductTemplate.java.bak HTTP/2
Host:
0ae3005b04bf7e6f813e026200cd00a8.web-securit
y-academy.net
Cookie: session=
9PHtUHMxoPndW5caWKsdAeCoAdqf0rcb
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/116.0.5845.141 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/
/*;q=0.8,application/signed-exchange;v
0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

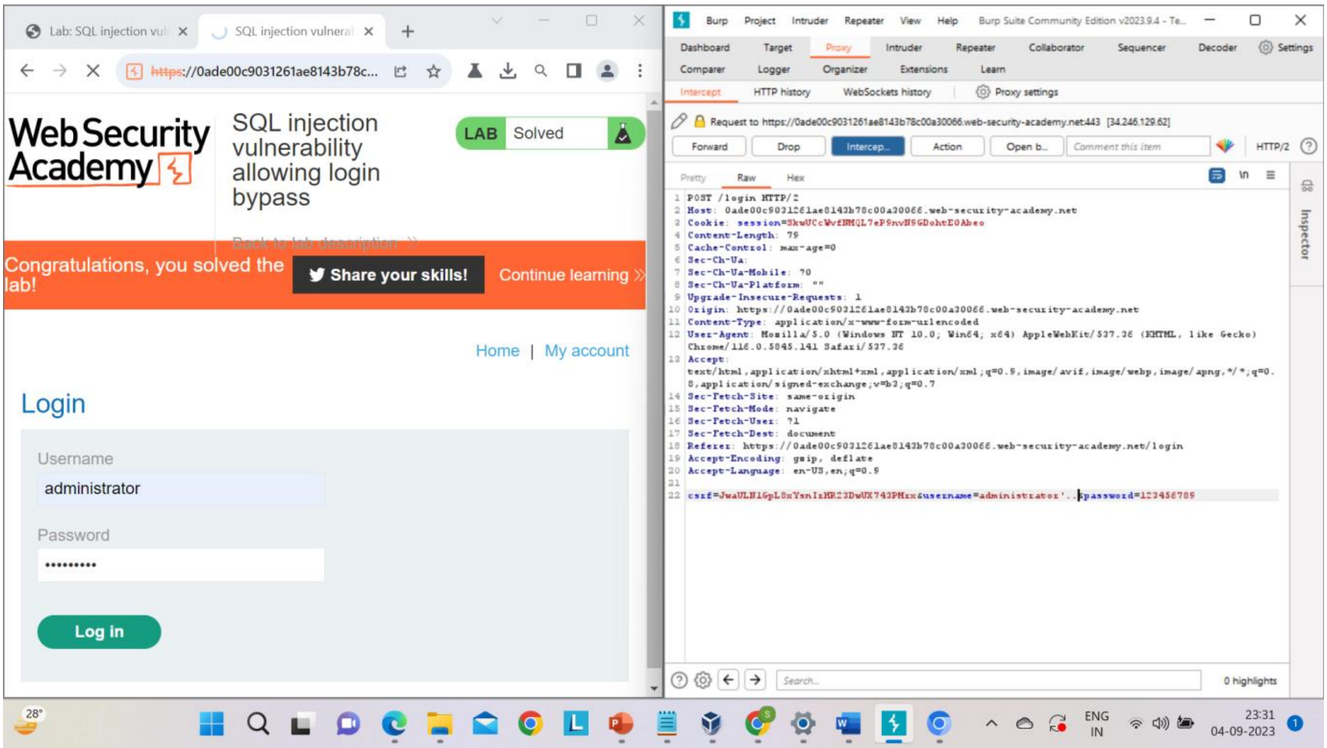
Response

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 1667

package data.productcatalog;

import common.db.JdbcConnectionBuilder;

import java.io.IOException;
import java.io.ObjectInputStream;
import java.io.Serializable;
import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.SQLException;
```


Lab: SQL injection vul
SQL injection vulnera
https://0ade00c9031261ae8143b78c...
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.9.4 - Te...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercep... Action Open b... Comment this item HTTP/2
Pretty Raw Hex
0 highlights
ENG IN
23:31
04-09-2023

Web Security Academy

SQL injection vulnerability allowing login bypass

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home | My account

Login

Username
administrator

Password
•••••••••

Log in

Request to https://0ade00c9031261ae8143b78c00a30066.web-security-academy.net:443 [34.246.129.62]

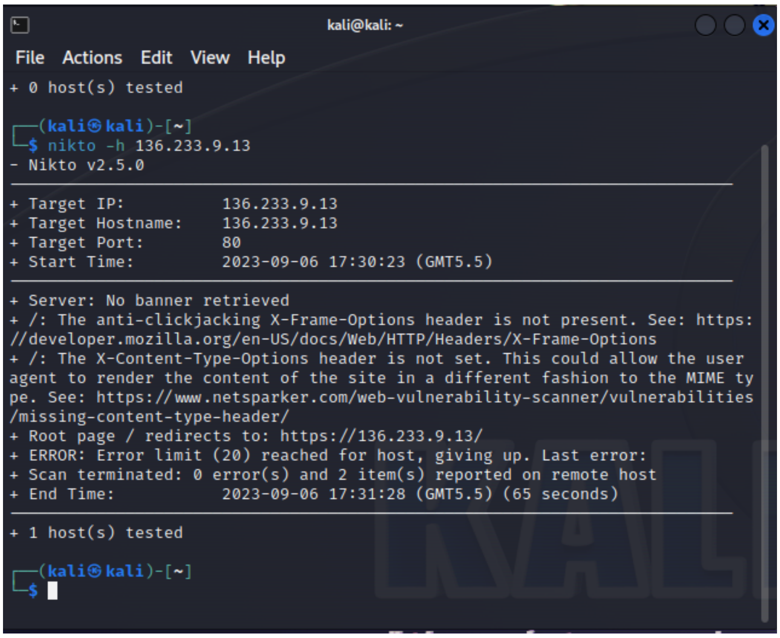
```
POST /login HTTP/2
Host: 0ade00c9031261ae8143b78c00a30066.web-security-academy.net
Cookie: session=SkwUCcWvfNMQL7eP9nvN9GDohtE0Abeo
Content-Length: 79
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://0ade00c9031261ae8143b78c00a30066.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.141 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ade00c9031261ae8143b78c00a30066.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

csrf=JwaULN1GpL8xYsnIzHR23DwUX743PMxx&username=administrator'..&password=123456789
```

Stuti Maitra Sarkar
Assignment 2

Nikto

Nikto is an open-source web server scanner used for assessing the security of web servers and identifying potential vulnerabilities. It does this by sending various HTTP requests and inspecting the server's responses, looking for known security issues, misconfigurations, and potential risks such as outdated software or exposed directories. Nikto is commonly used by security professionals to perform quick security assessments of web servers and web applications to ensure they are protected against common web-based threats.



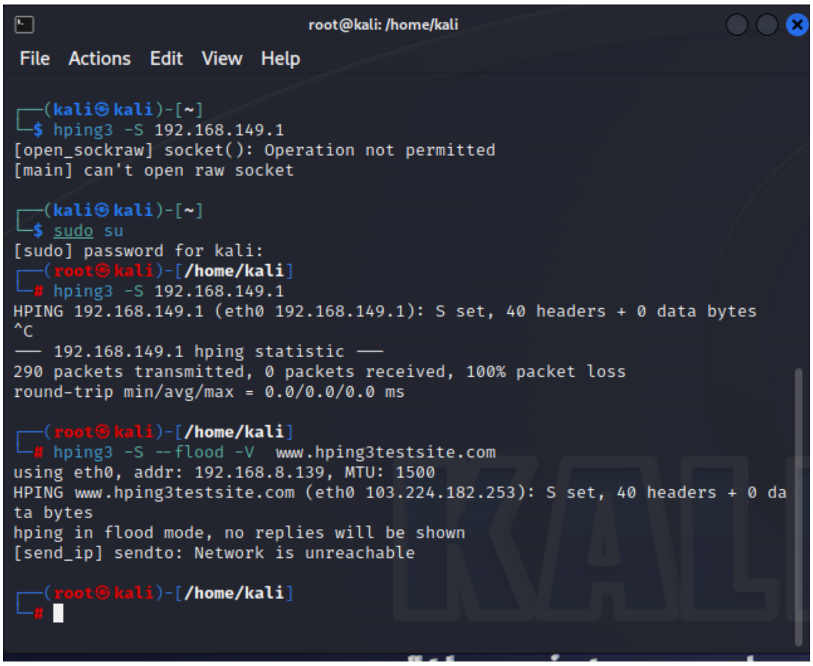
```
+ 0 host(s) tested

┌──(kali㉿kali)-[~]
└─$ nikto -h 136.233.9.13
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          136.233.9.13
+ Target Hostname:    136.233.9.13
+ Target Port:        80
+ Start Time:         2023-09-06 17:30:23 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ Root page / redirects to: https://136.233.9.13/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2023-09-06 17:31:28 (GMT5.5) (65 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

Hping3

Hping3 is a command-line tool used for network exploration and security auditing. It enables users to craft and send custom packets to target hosts, making it a versatile utility for tasks like network scanning, ping testing, and firewall testing. Hping3 can be used to test network behavior, discover open ports, and assess network security by sending specially crafted packets to a target and analyzing the responses, making it a valuable tool for network administrators and security professionals.



```
┌──(kali㉿kali)-[~]
└─$ hping3 -S 192.168.149.1
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S 192.168.149.1
HPING 192.168.149.1 (eth0 192.168.149.1): S set, 40 headers + 0 data bytes
^C
--- 192.168.149.1 hping statistic ---
290 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿kali)-[/home/kali]
└─# hping3 -S --flood -V  www.hping3testsite.com
using eth0, addr: 192.168.8.139, MTU: 1500
HPING www.hping3testsite.com (eth0 103.224.182.253): S set, 40 headers + 0 da
ta bytes
hping in flood mode, no replies will be shown
[send_ip] sendto: Network is unreachable

┌──(root㉿kali)-[/home/kali]
└─# 
```