# CHANDIGARH UNIVERSITY

## UNIVERSITY INSTITUTE OF NGINEERING

## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

| **Submitted By:** Vivek Kumar(21BCS8129) | **Submitted To:** Er. Himanshi (13362) |
|---|---|
| **Subject Name** | Web and Mobile Security Lab |
| **Subject Code** | 20CSP-338 |
| **Branch** | Computer Science and Engineering |
| **Semester** | 5th |

# Experiment - 6

**Student Name: Vivek Kumar** **UID: 21BCS8129**
**Branch: BE-CSE(LEET)** **Section/Group: WM-20BCS-616/A**
**Semester: 5th** **Date of Performance: 02/11/2022**
**Subject Name: Web and Mobile Security Lab** **Subject Code: 20CSP-338**

## 1. Aim/Overview of the practical:

Perform Penetration testing on a web application to gather information about the system (Foot Printing)

## 2. Task to be done/ Which logistics used:

To perform penetration testing and foot printing on any Web Application.

**3. Apparatus / Simulator Used:**

- Windows 7 & above version.
- Google Chrome
- D-Tech
- NMAP
- Metasploit

## INTRODUCTION

Web application penetration testing is the practice of simulating attacks on a system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure. These attacks are performed either internally or externally on a system, and they help provide information about the target system, identify vulnerabilities within them, and uncover exploits that could actually compromise the system. It is an essential health check of a system that informs testers whether remediation and security measures are needed.


Foot printing of any web side
Whos is Details
Software used and version
OS Details
Sub Domains
File Name and File Path
Scripting Platform & CMS Details
Contact Details

**DESCRIPTION:**
**D-TECT** is an All-In-One Tool for Penetration Testing. This is specially programmed for Penetration Testers and Security Researchers to make their job easier, instead of launching different tools for performing different task. **D-TECT** provides multiple features and detection features which gather target information and finds different flaws in it.

**Features:**

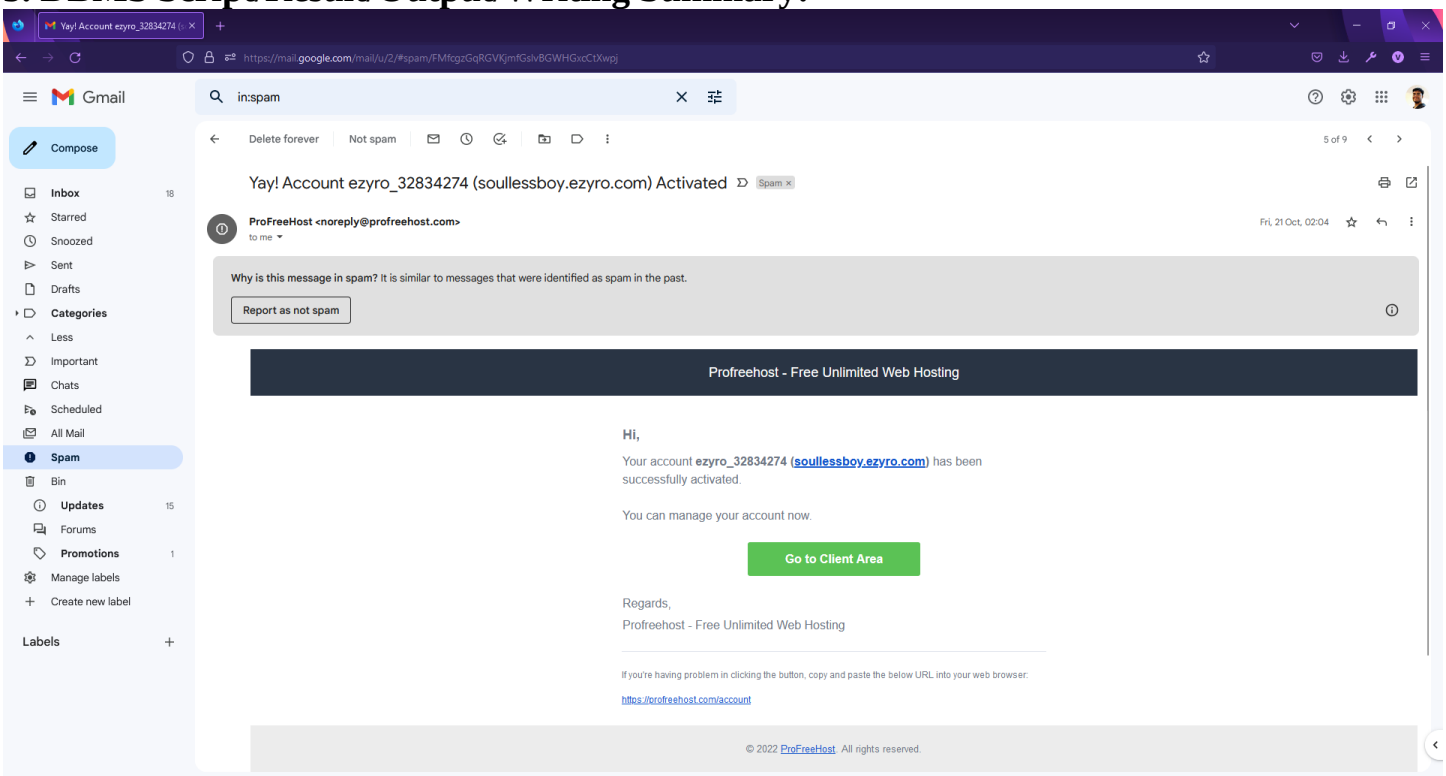
- Sub-domain Scanning
- Port Scanning
- WordPress Scanning
- WordPress Username Enumeration
- WordPress Backup Grabbing
- Sensitive File Detection
- Same-Site Scripting Scanning
- Click Jacking Detection
- Powerful XSS vulnerability scanning
- SQL Injection vulnerability scanning
- User-Friendly UI

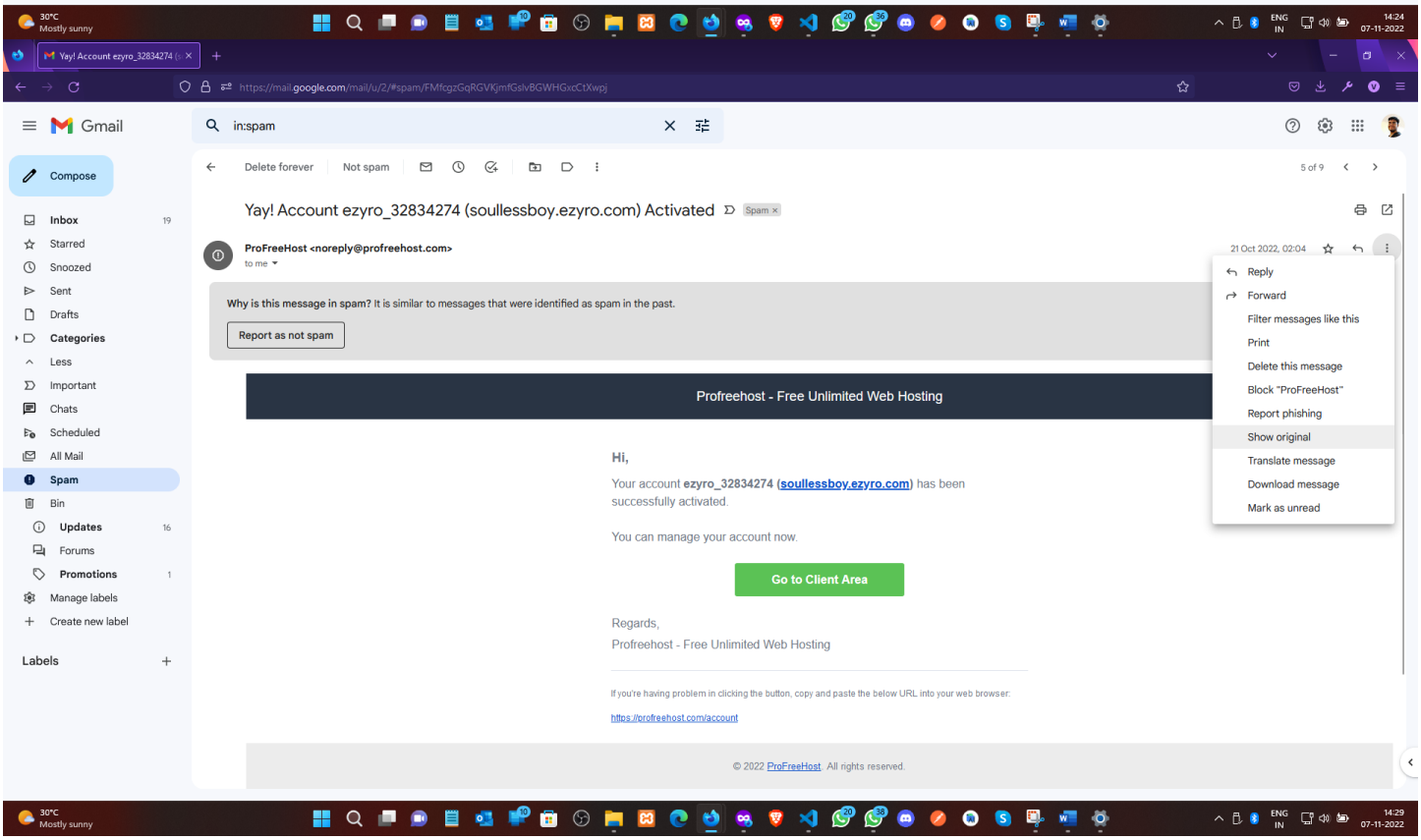
## 4. Program/ Steps/ Method:

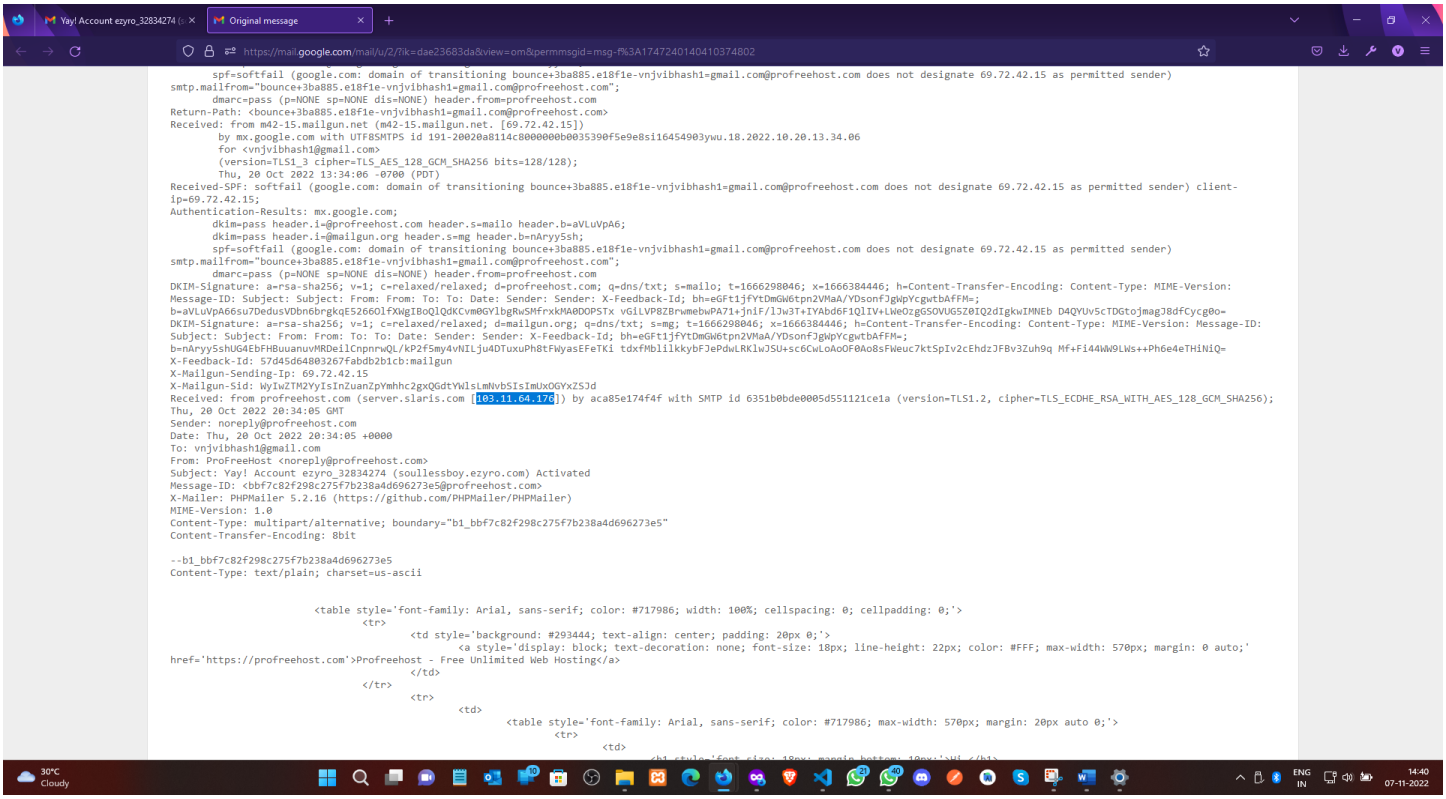
1. Install kali Linux virtual machine and D-tech tools Open Terminal.
2. git clone https://github.com/bibortone/D-Tech.git
3. ls
4. Check that D-tech tool is available on your system
5. cd D-tech and press Enter
6. D-Tech$ ls
7. D-Tech$ python d-tech.py(run the tools)

**Get menu after run the tools**
1. Word press username enumerator
2. Sensitive file detector
3. Cross-Site Scripting [ XSS ] Scanner:
4. SQL Injection [ SQLI ] Scanner:
5. Sub-domain Scanner:
6. Same Site Scripting detection:
7. Port scanner
8. Word press scanner
Step 6- [+] select any option from menu
>Enter 4 next
[+] enter domain
Demo.testfire.net
[+] checking Status…..
[] Not vulnerable
[+]exit or launch again?(e/a)

# 5. DBMS Script/Result/Output/Writing Summary:



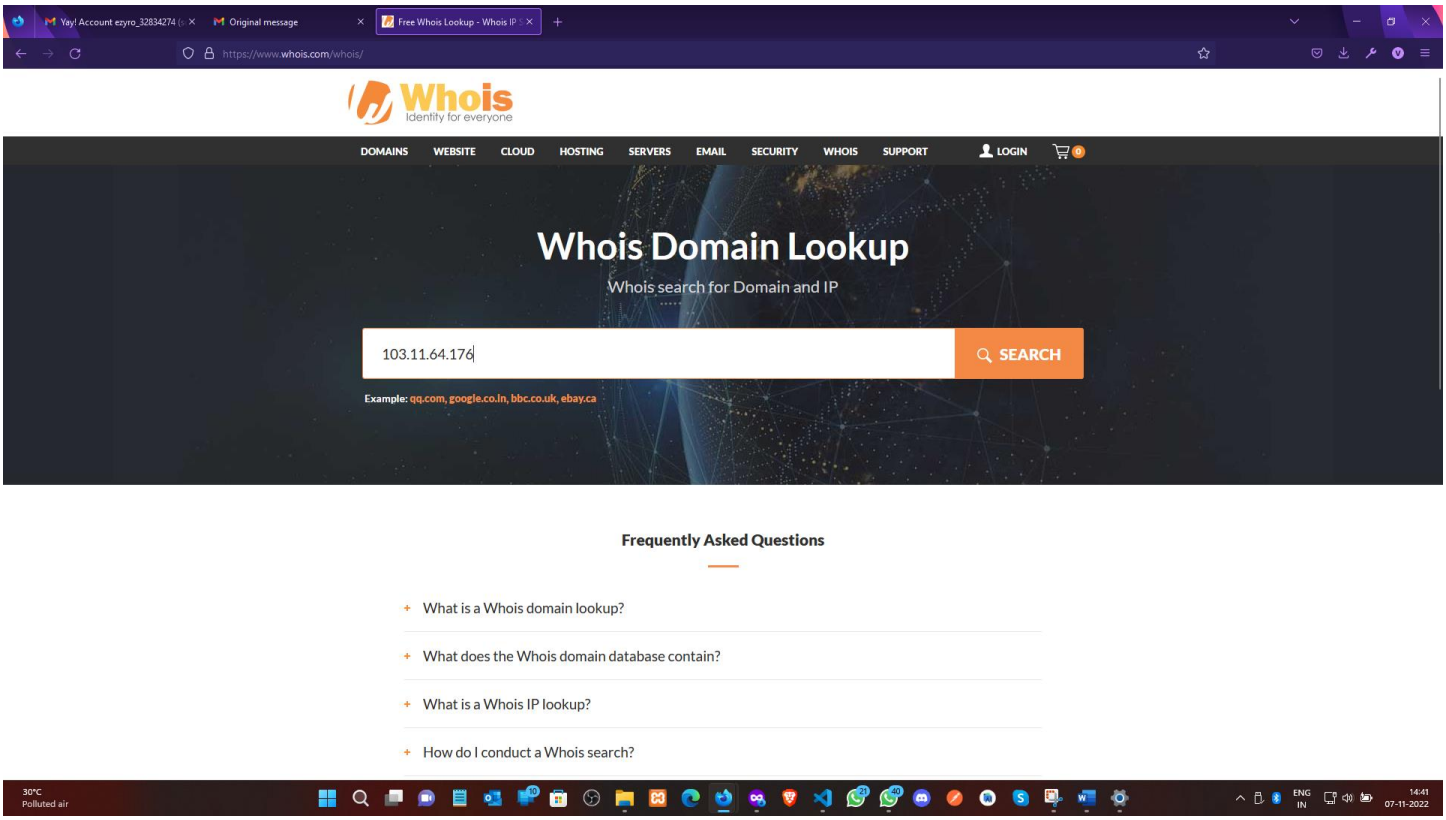


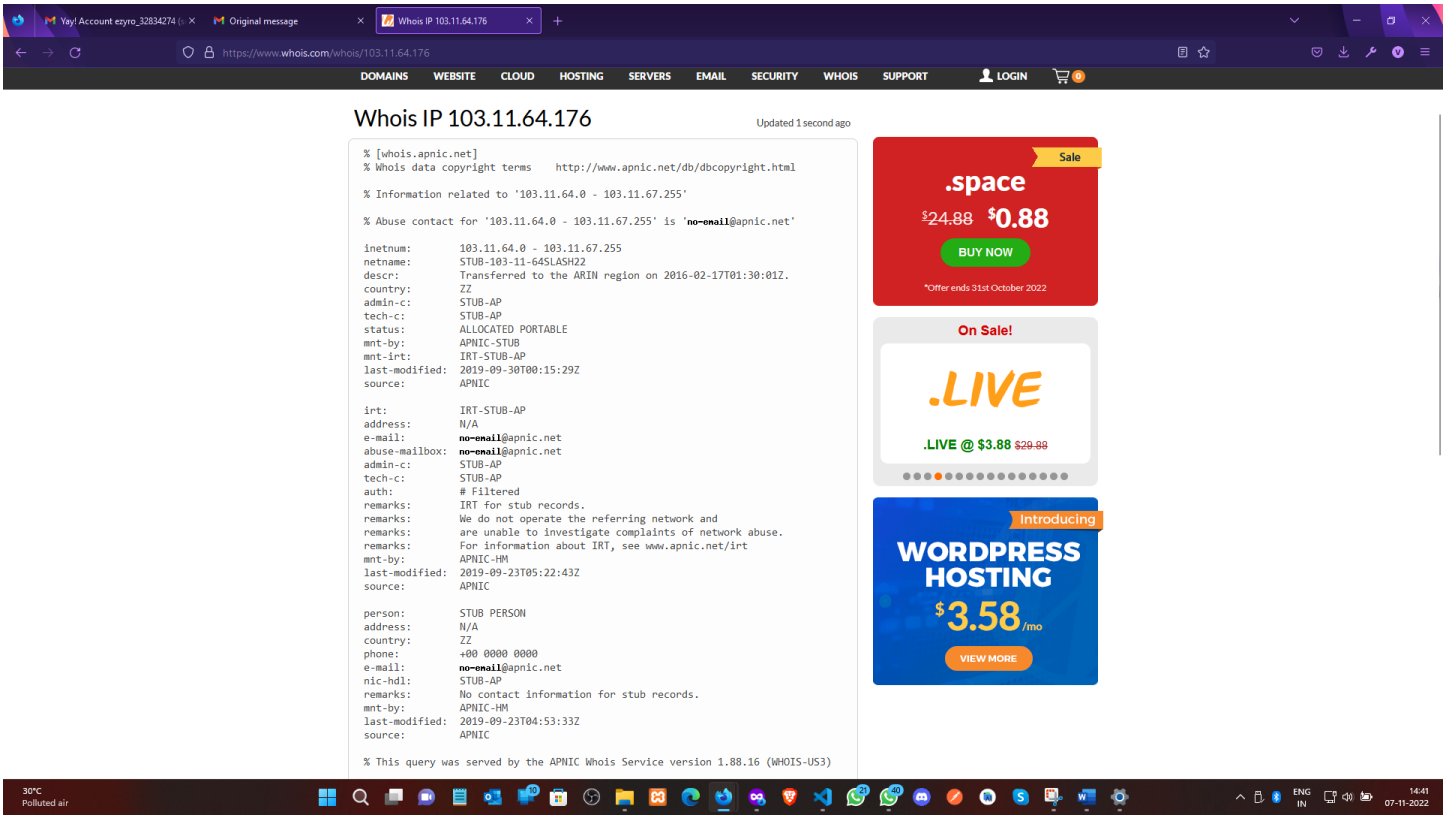
```
        spf=softfail (google.com: domain of transitioning bounce+3ba885.e18f1e-vnjvibhash1=gmail.com@profreehost.com does not designate 69.72.42.15 as permitted sender)
smtp.mailfrom="bounce+3ba885.e18f1e-vnjvibhash1=gmail.com@profreehost.com";
        dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=profreehost.com
Return-Path: <bounce+3ba885.e18f1e-vnjvibhash1=gmail.com@profreehost.com>
Received: from m42-15.mailgun.net (m42-15.mailgun.net. [69.72.42.15])
         by mx.google.com with UTF8SMTPS id 191-20020a8114c8000000b0035390f5e9e8si16454903ywu.18.2022.10.20.13.34.06
         for <vnjvibhash1@gmail.com>
         (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
         Thu, 20 Oct 2022 13:34:06 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning bounce+3ba885.e18f1e-vnjvibhash1=gmail.com@profreehost.com does not designate 69.72.42.15 as permitted sender) client-
ip=69.72.42.15;
Authentication-Results: mx.google.com;
        dkim=pass header.i=@profreehost.com header.s=mailo header.b=aVLuVpA6;
        dkim=pass header.i=@mailgun.org header.s=mg header.b=nAryy5sh;
        spf=softfail (google.com: domain of transitioning bounce+3ba885.e18f1e-vnjvibhash1=gmail.com@profreehost.com does not designate 69.72.42.15 as permitted sender)
smtp.mailfrom="bounce+3ba885.e18f1e-vnjvibhash1=gmail.com@profreehost.com";
        dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=profreehost.com
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=profreehost.com; q=dns/txt; s=mailo; t=1666298046; x=1666384446; h=Content-Transfer-Encoding: Content-Type: MIME-Version:
Message-ID: Subject: Subject: From: From: To: To: Date: Sender: Sender: X-Feedback-Id; bh=eGFt1jfYtDmGW6tpn2VMaA/YDsonfJgWpYcgwtbAFFM=;
b=aVLuVpA66u7DeDusVDbn6brgKqE5266OlfXWgIBoQlQdKCvm0GV1bgRuSMfrkkNAODOPSTx vGiLVP8ZBrwmebwPA71+jnIf/lJw3T+IYAbd6F1QlIV+LWeOzgGSOVUG5Z0IQ2dIgkwIMNEb D4QYUv5cTDGtojmagJ8dfCycg0o=
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mailgun.org; q=dns/txt; s=mg; t=1666298046; x=1666384446; h=Content-Transfer-Encoding: Content-Type: MIME-Version: Message-ID:
Subject: Subject: From: From: To: To: Date: Sender: Sender: X-Feedback-Id; bh=eGFt1jfYtDmGW6tpn2VMaA/YDsonfJgWpYcgwtbAFFM=;
b=nAryy5shUG4EbFHBuuanuvMRDeilCnpnrwQL/kP2f5my4vNILju4DTuxuPh8tFWyasEFeTKi tdxfMblilkkybFJePdwLRKlwJSU+sc6CwLoAoOF0Ao8sFWeuc7ktSpIv2cEhdzJFBv3Zuh9q Mf+Fi44WW9LWs++Ph6e4eTHiNiQ=
X-Feedback-Id: 57d45d64803267fabdb2b1cb:mailgun
X-Mailgun-Sending-Ip: 69.72.42.15
X-Mailgun-Sid: WyIwZTM2YyIsInZuanZpYmhhc2gxQGdtYWlsLmNvbSIsImUxOGYxZ5Jd
Received: from profreehost.com (server.slaris.com [103.11.64.176]) by aca85e174f4f with SMTP id 6351b0bde0005d551121ce1a (version=TLS1.2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256);
Thu, 20 Oct 2022 20:34:05 GMT
Sender: noreply@profreehost.com
Date: Thu, 20 Oct 2022 20:34:05 +0000
To: vnjvibhash1@gmail.com
From: ProFreeHost <noreply@profreehost.com>
Subject: Yay! Account ezyro_32834274 (soullessboy.ezyro.com) Activated
Message-ID: <bbf7c82f298c275f7b238a4d696273e5@profreehost.com>
X-Mailer: PHPMailer 5.2.16 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="b1_bbf7c82f298c275f7b238a4d696273e5"
Content-Transfer-Encoding: 8bit

--b1_bbf7c82f298c275f7b238a4d696273e5
Content-Type: text/plain; charset=us-ascii


                        <table style='font-family: Arial, sans-serif; color: #717986; width: 100%; cellspacing: 0; cellpadding: 0;'>
                                <tr>
                                        <td style='background: #293444; text-align: center; padding: 20px 0;'>
                                                <a style='display: block; text-decoration: none; font-size: 18px; line-height: 22px; color: #FFF; max-width: 570px; margin: 0 auto;'
href='https://profreehost.com'>Profreehost - Free Unlimited Web Hosting</a>
                                        </td>
                                </tr>
                                        <tr>
                                                <td>
                                                        <table style='font-family: Arial, sans-serif; color: #717986; max-width: 570px; margin: 20px auto 0;'>
                                                                <tr>
                                                                        <td>
```

C






## Learning outcomes (What I have learnt):

Finally, as a penetration tester, you should collect and log all vulnerabilities in the system. Don't ignore any scenario considering that it won't be executed by the end-users.If you are a penetration tester, please help our readers with your experience, tips, and sample test cases on how to perform Penetration Testing effectively.

## Evaluation Grid (To be created per the faculty's SOP and Assessment guidelines):

| Sr. No. | Parameters | Marks Obtained | Maximum Marks |
|---|---|---|---|
| 1. | Worksheet completion including writing learning objectives/Outcomes. (To be submitted at the end of the day). | | |
| 2. | Post-Lab Quiz Result. | | |
| 3. | Student Engagement in Simulation/Demonstration/Performance and Controls/Pre-Lab Questions. | | |
| | Signature of Faculty (with Date): | Total Marks Obtained: | |