SCHOOL OF ARCHITECTURE, COMPUTING AND ENGINEERING

Department of Engineering and Computing

CN6010 - Advanced Topic in Cyber Security and Networks

Application of Advanced Topics to solve Cyber Security Problem

U2197407George David Dandoczi

Supervisor: Dr.Umar Mukhtar Isamil

Table of Contents

Part One

Case Study

Business Type and Size:

Our company SecureTech Solutions has been contracted to perform a penetration test for a mediumsized clothing company called Fashion&Trendz working as retailer. This company operates in UK and it has multiple branches across UK. This company operates a web application where customers can browse and buy clothing items online. This company's website registers its customers by collecting personal information and store checkout process. They store information including names, addresses, email addresses and payment details. Payment processing of this company is handled by a third-party service provider, so this company does not directly store financial data.

Fashion&Trendz web application also gives access to its staff members to manage staff data that includes inventory, update product listings and process orders. Staff credentials are stored in the company's database including usernames and passwords and their access level according to their position.

In addition,Fashion&Trendz's also provides support their potential customers and inquiries via email. It also holds sensitive information, sizing information, their preference and contact details.

Type of Users:

Staff Users:

This company Fashion&Trendz'salso holds Information System, in their information system staff had different level of access for their staff members to manage their business according to their role and duties. All these information are stored in company's database.

- Clients/Customers
- Financial Staff
- Administrative staff (HR, accounting, IT department)

Customer Users:

Company had customers users by storing their personal information and store checkout process also including names, addresses, email addresses, customer preferences, Sizing information and contact information.

Customer Data:

Following data collected while customer registration and checkout processes.

Sr. No.	Column Name	Data type
1	Name	Varchar
2	Address	Varchar
3	Email	Varchar
4	Customer preferences	Varchar
5	Customer Sizing Information	Float

Staff Data:

Sr. No.	Staff Role	Department Name	Access Level
1	CEO	CEO Name	Admin (Full)
2	Directors	Director	Management (Limited to Management Level)

3	IT	IT department	IT Management (according to their job role)
4	Finance	Finance Department	Can see reports and financial transactions
5	Staff	Staff Name	Each staff has its own login

As company operated in United Kingdom, it operates with compliance to UK-GDPR. Penetrating testing assessment on the scenario defined above (based on the company's applications) and have now our penetration testing engagement aims to assessment of security level of Fashion&Trendz's web application, database and their information system. We will conduct a evaluation to identify existing vulnerabilities, weaknesses and any exploit that could potentially expose personal information of customers and staff. That can compromise the integrity of the company's web application or lead to unauthorized access to sensitive data.

Additionally, we will assess during penetration testing the effectiveness of Fashion&Trendz's security controls and provide recommendations for remediation to enhance the company's overall security posture and ensure compliance with data protection regulationsi.e UK-GDPR.

a. Client Report Requirement (Task 1):

1.1 Open Source Intelligence (OSINT) is a process of gatheringinformation from resources that are publicly available, for example internet, social media, public government data, professional networks. it is being used bycyber security professionals for an intelligence purpose. Followings are OSINT examples:

Sr. No.	Types	Example
1	Public Websites	Blogs, News, Corporate Website
2	Social Media Platforms	LinkedIn, Facebook, Twitter, Instagram, Reddit
3	Database and Directories	White pages, Legal filings, Public records, Professional associations
4	Satellite Imagery	Google Earth, Maps
5	Domain and IP information	WHOIS, DNS, Domain Ownership, Server Location

Following tools may contain useful information:

- Whois database
- Target's Website
- Perform Social Network scraping
- Google search results
- DNS information
- Review blogs, public forums, and Websites
- Search breach databases about the target

As OSINT are being used for different sources, three examples for case study are given below:

LinkedIn Profile of Company, which describes the company type and activities, company's number of employees, associate members, Headquarter location of company.

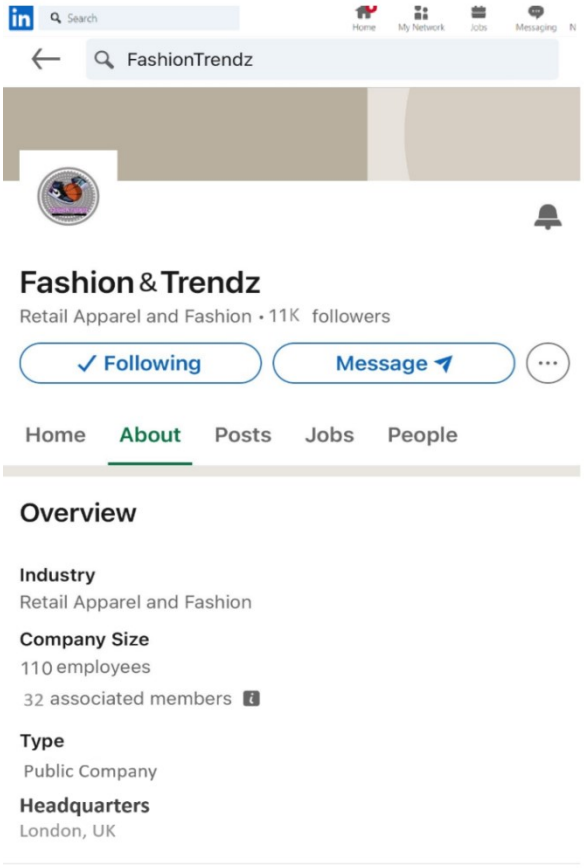


Fig-1 – Screenshot of Fashion&TrendzLinkenIn Profile and Company Information

This is example of search in exploit DB

These details are mentioned on profile of company, information can be include company's address, incorporated date, Nature of Business.

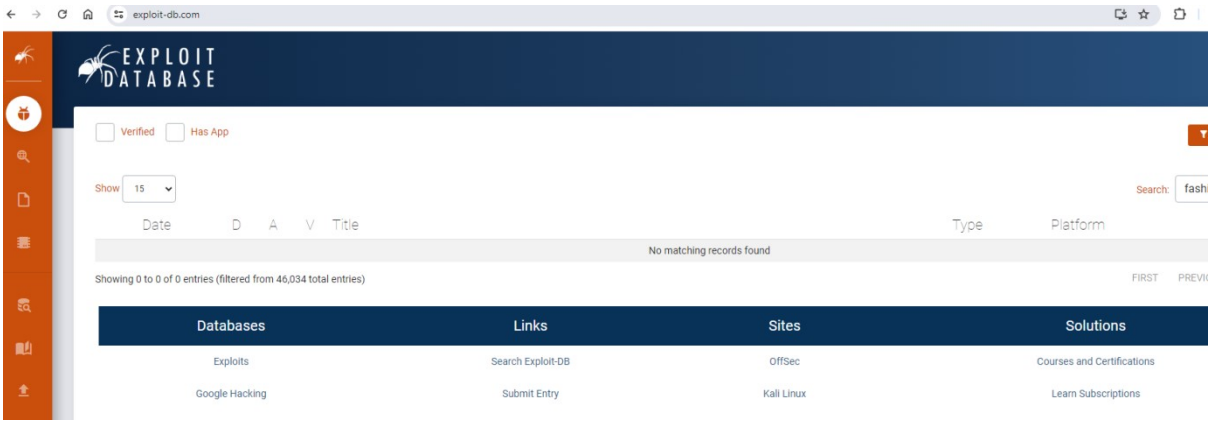


Fig 2 - Fashion&Trendzsearch on Exploit DB

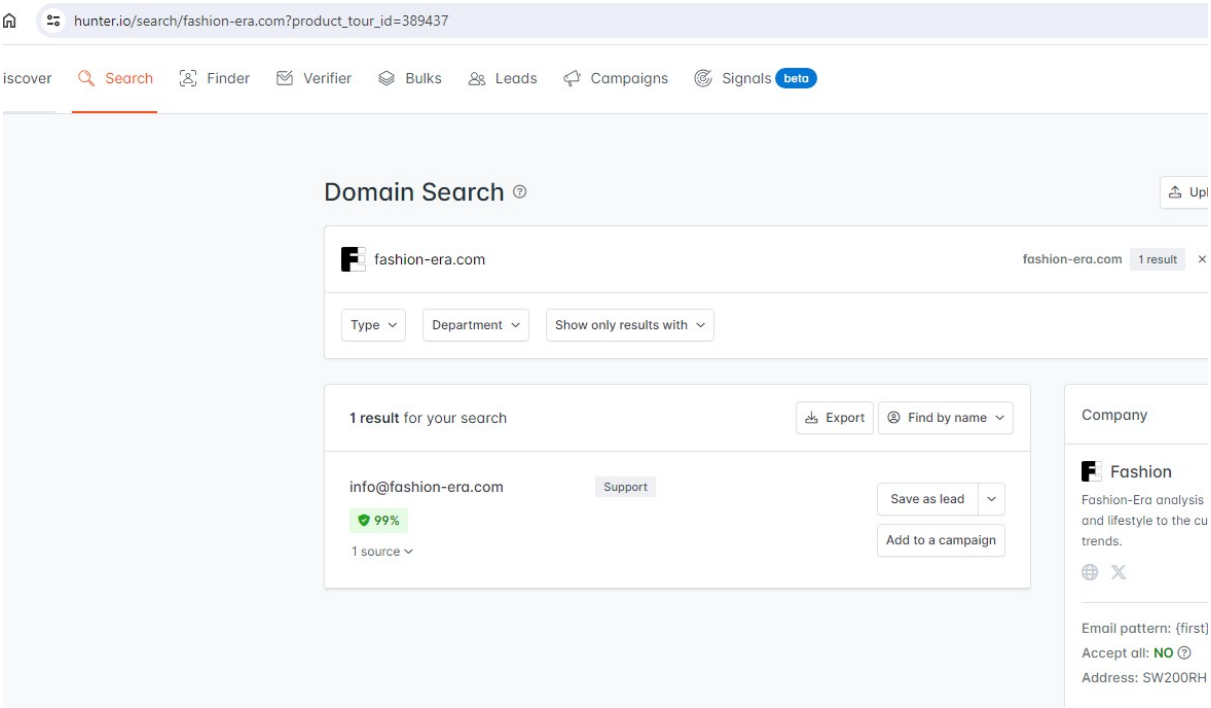


Fig: hunter.io search for email

Maps

By using the map, location information is available.

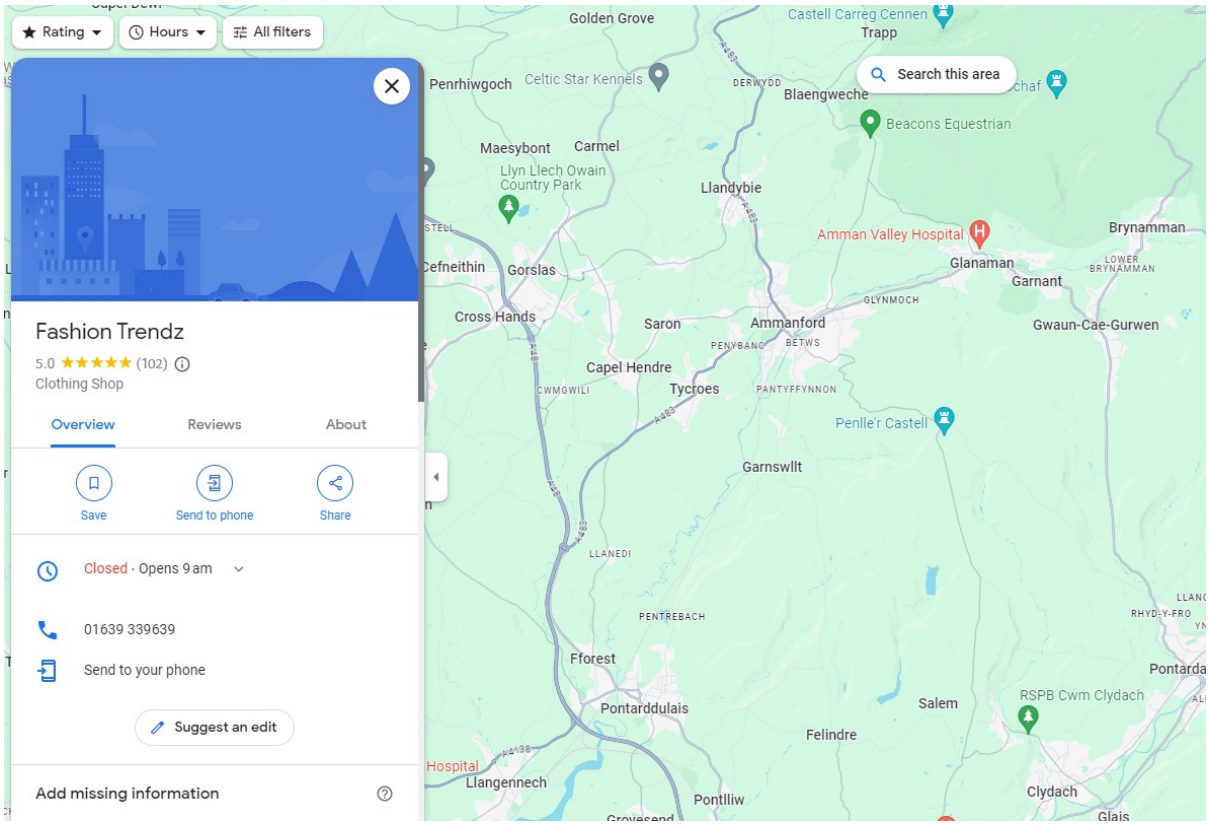


Fig-3 Map information of company

Instagram Profile of Company:

We also analyse the company on the instagram and it shows its number of posts, follower information.

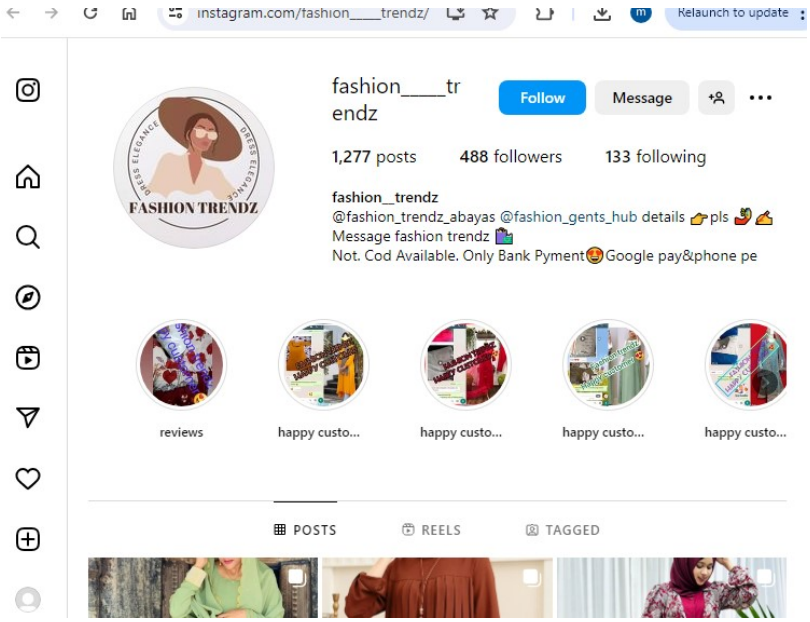


Fig4 – Instagram profile screen shot of company

Twitter Profile of company

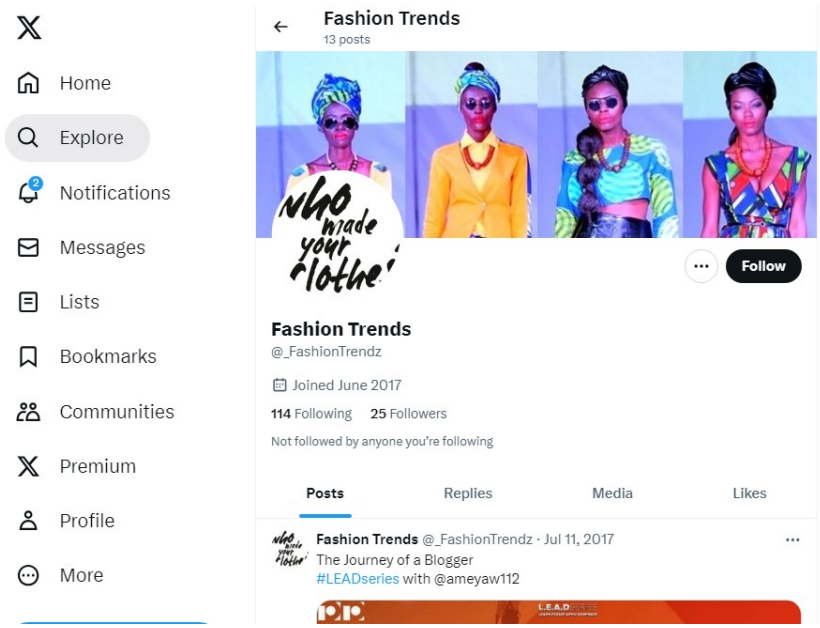


Fig-5 Twitter information of company.

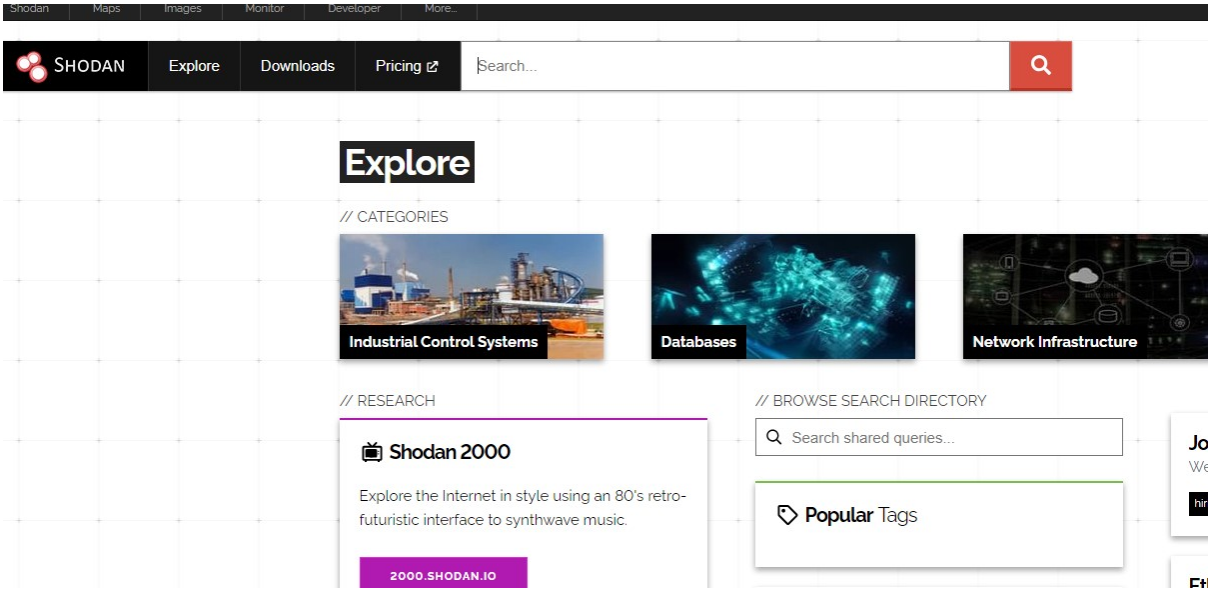
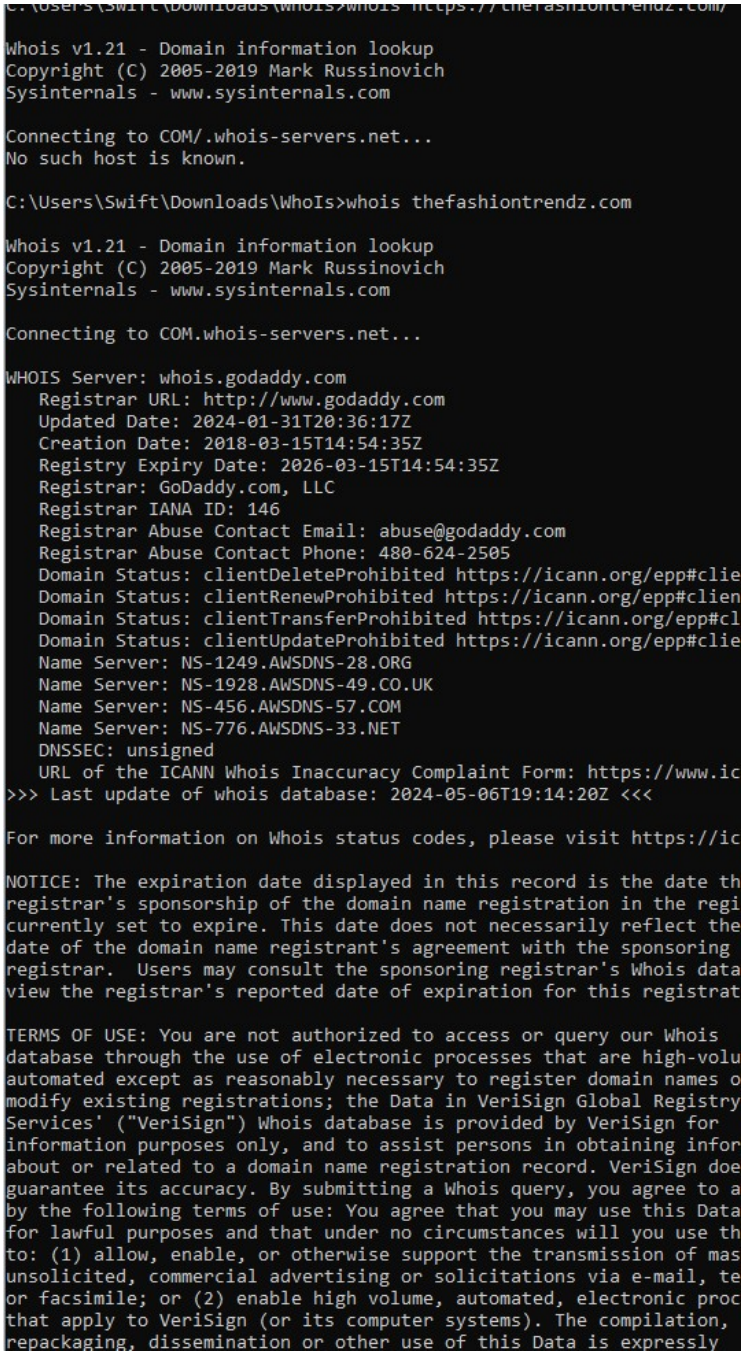


Fig6-shodan.io OSINT tool

Check DNS Records for specific target for OSINT purpose. Tools like dig andnslookupare being used to gather DNS information about the domain, such as A records (IP addresses), MX records (mail servers) and Name Server records.

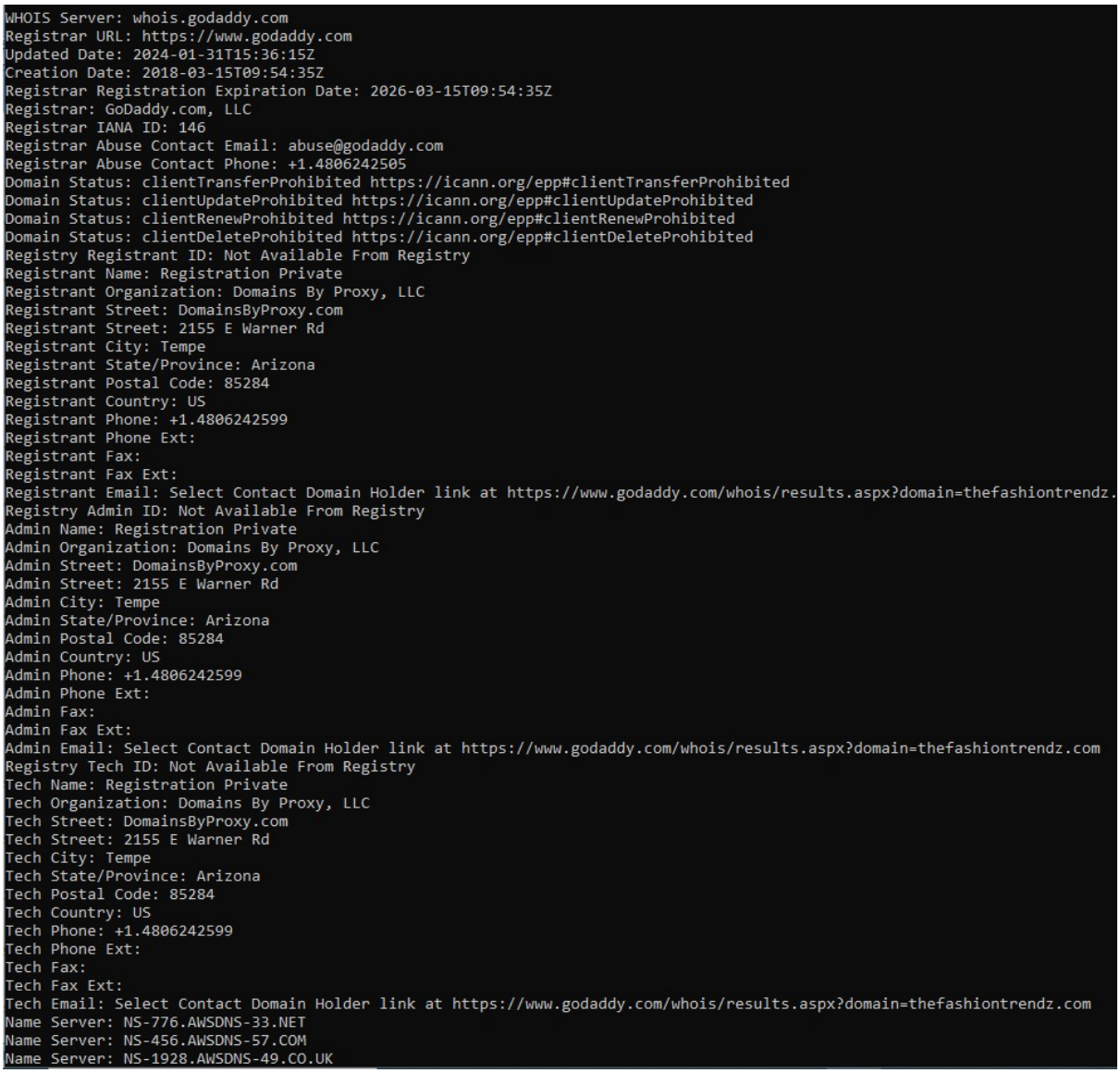
WhoisCompany’sinformation



```
C:\Users\Swift\Downloads\WhoIs>whois https://thefashiontrendz.com/

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM/.whois-servers.net...
No such host is known.

C:\Users\Swift\Downloads\WhoIs>whois thefashiontrendz.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2024-01-31T20:36:17Z
   Creation Date: 2018-03-15T14:54:35Z
   Registry Expiry Date: 2026-03-15T14:54:35Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clie
   Domain Status: clientRenewProhibited https://icann.org/epp#clien
   Domain Status: clientTransferProhibited https://icann.org/epp#cl
   Domain Status: clientUpdateProhibited https://icann.org/epp#clie
   Name Server: NS-1249.AWSDNS-28.ORG
   Name Server: NS-1928.AWSDNS-49.CO.UK
   Name Server: NS-456.AWSDNS-57.COM
   Name Server: NS-776.AWSDNS-33.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.ic
>>> Last update of whois database: 2024-05-06T19:14:20Z <<<

For more information on Whois status codes, please visit https://ic

NOTICE: The expiration date displayed in this record is the date th
registrar's sponsorship of the domain name registration in the regi
currently set to expire. This date does not necessarily reflect the
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois data
view the registrar's reported date of expiration for this registrat

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volu
automated except as reasonably necessary to register domain names o
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining infor
about or related to a domain name registration record. VeriSign doe
guarantee its accuracy. By submitting a Whois query, you agree to a
by the following terms of use: You agree that you may use this Data
for lawful purposes and that under no circumstances will you use th
to: (1) allow, enable, or otherwise support the transmission of mas
unsolicited, commercial advertising or solicitations via e-mail, te
or facsimile; or (2) enable high volume, automated, electronic proc
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
```

Fig-7Whois Domain server information

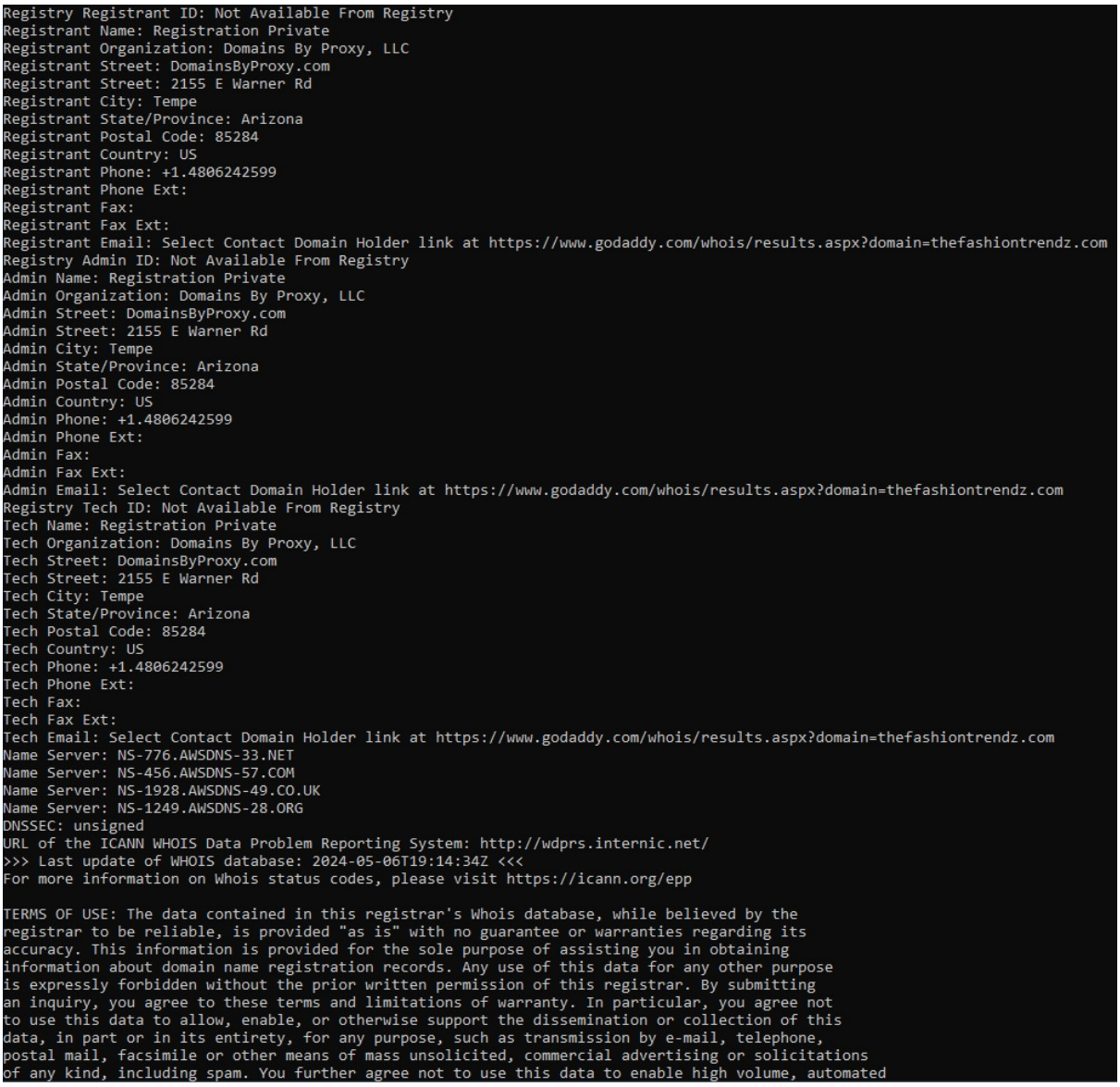
Whois server information



```
WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-01-31T15:36:15Z
Creation Date: 2018-03-15T09:54:35Z
Registrar Registration Expiration Date: 2026-03-15T09:54:35Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=thefashiontrendz.
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=thefashiontrendz.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=thefashiontrendz.com
Name Server: NS-776.AWSDNS-33.NET
Name Server: NS-456.AWSDNS-57.COM
Name Server: NS-1928.AWSDNS-49.CO.UK
```

Fig-8Whois Registration And Admin Information

Domain and registration information



```
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=thefashiontrendz.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=thefashiontrendz.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=thefashiontrendz.com
Name Server: NS-776.AWSDNS-33.NET
Name Server: NS-456.AWSDNS-57.COM
Name Server: NS-1928.AWSDNS-49.CO.UK
Name Server: NS-1249.AWSDNS-28.ORG
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-05-06T19:14:34Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

TERMS OF USE: The data contained in this registrar's Whois database, while believed by the
registrar to be reliable, is provided "as is" with no guarantee or warranties regarding its
accuracy. This information is provided for the sole purpose of assisting you in obtaining
information about domain name registration records. Any use of this data for any other purpose
is expressly forbidden without the prior written permission of this registrar. By submitting
an inquiry, you agree to these terms and limitations of warranty. In particular, you agree not
to use this data to allow, enable, or otherwise support the dissemination or collection of this
data, in part or in its entirety, for any purpose, such as transmission by e-mail, telephone,
postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations
of any kind, including spam. You further agree not to use this data to enable high volume, automated
```

Fig-9Whois Admin and Tech Information

1.2 Effectiveness of OSINT for penetration testing:

OSINT, in penetration testing-related investigations are mostly used to confirm certain pieces of information to map data points of an organization, which are typically useful to attackers e.g. IP addresses, Physical Address, hostnames, company's domain, email addresses, usernames, passwords, password hash values, URL paths. Attackers got information on basis of publically available data which can help them to do penetration test on the target. The example scenario detailed above demonstrates a mixture of various OSINT tools and techniques which can be combined to gain access to a system. This information is very much important and critical from attacker's point of view. That is why some OSINT is called a hacker's best friend.

1.3 Scenario Assessment

OSINT (Open Source Intelligence) plays very crucial role in penetration testing as it helps identify potential vulnerabilities and possible basic information by over viewing publicly available information/data about specific target. According to our case study we obtain following useful information about the company:

- Company Information
- Number of Employees
- Company Location
- Domain Name/Domain server information
- Contact and Web information (phone number/email/URL)
- Host Information

Information available in above mentioned company's platforms can expose weak points in network security, system configurations or employee information. Thus, information collected through OSINT is very critical and helpful for penetration testing for ethical hacker which minimize security risks.

b. Reconnaissance

1.4 Information obtained by testing the web applications

For using the active reconnaissance method, we use nmap command to discover the host on the network. We perform a ping scan to discover the live hosts in a network:

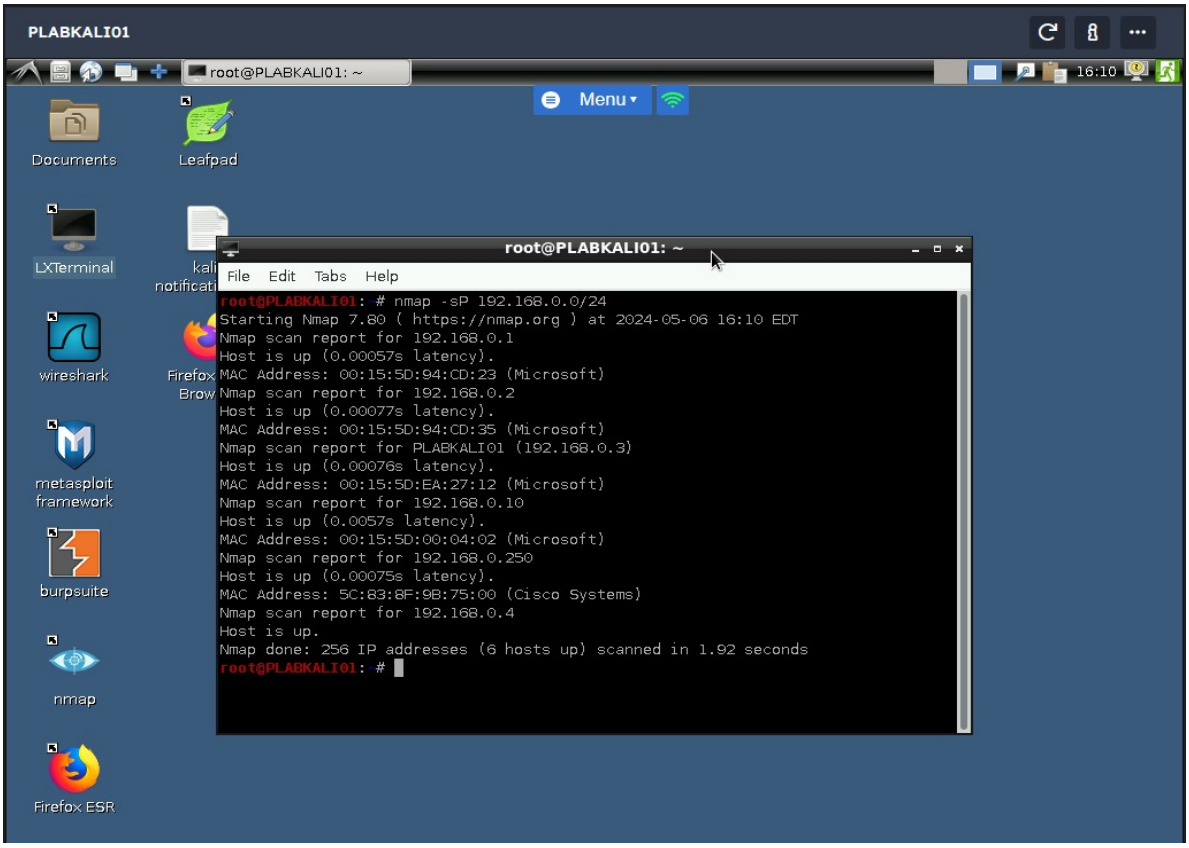


Fig-10 ping scan to discover live host

We used nmap tool to scan the live host on the network

Comman: *nmap –sP 192.168.0.0/24*

-sP- ping scanning

CIDR /24, then nmap will scan all 256 IP addresses on the network

Scanning the network without ping

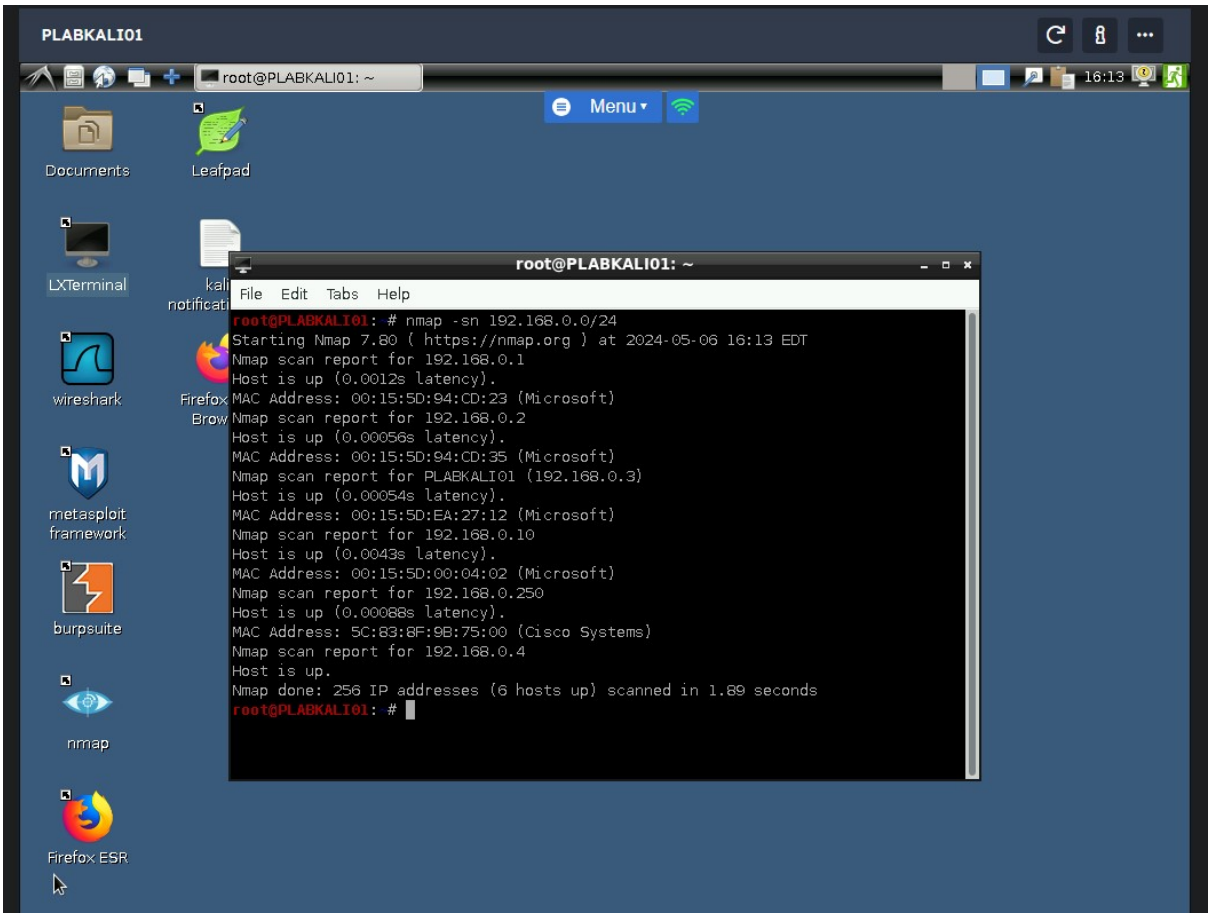


Fig-11 scan without ping to discover live host

To find number of live hosts on the network use following command

*nmap 192.168.0.**

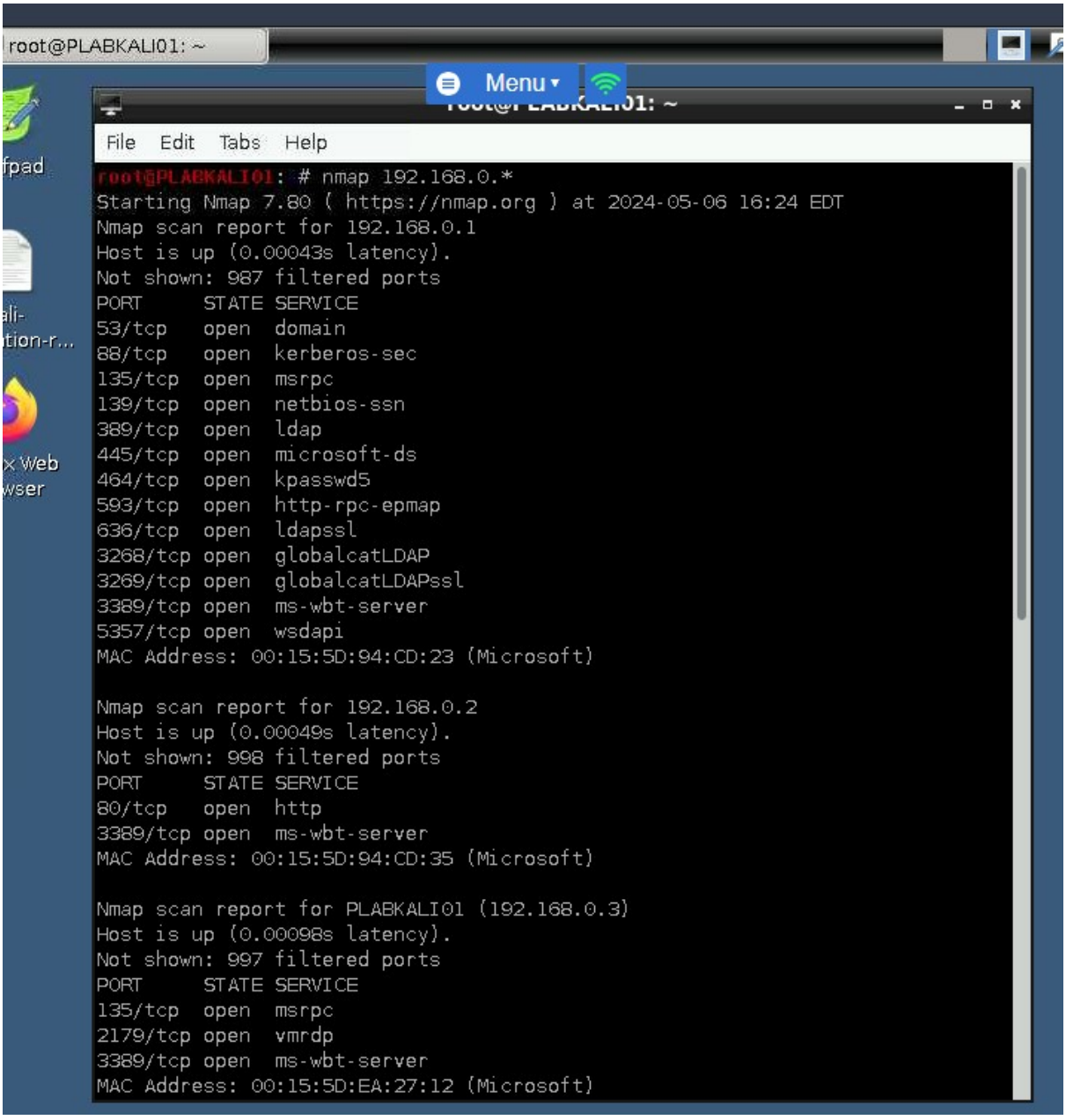


Fig-12 Number of all live host with their opening ports.

This displayed all the live hosts on the network with their open ports and active services.

Host Discovery: ARP Scan

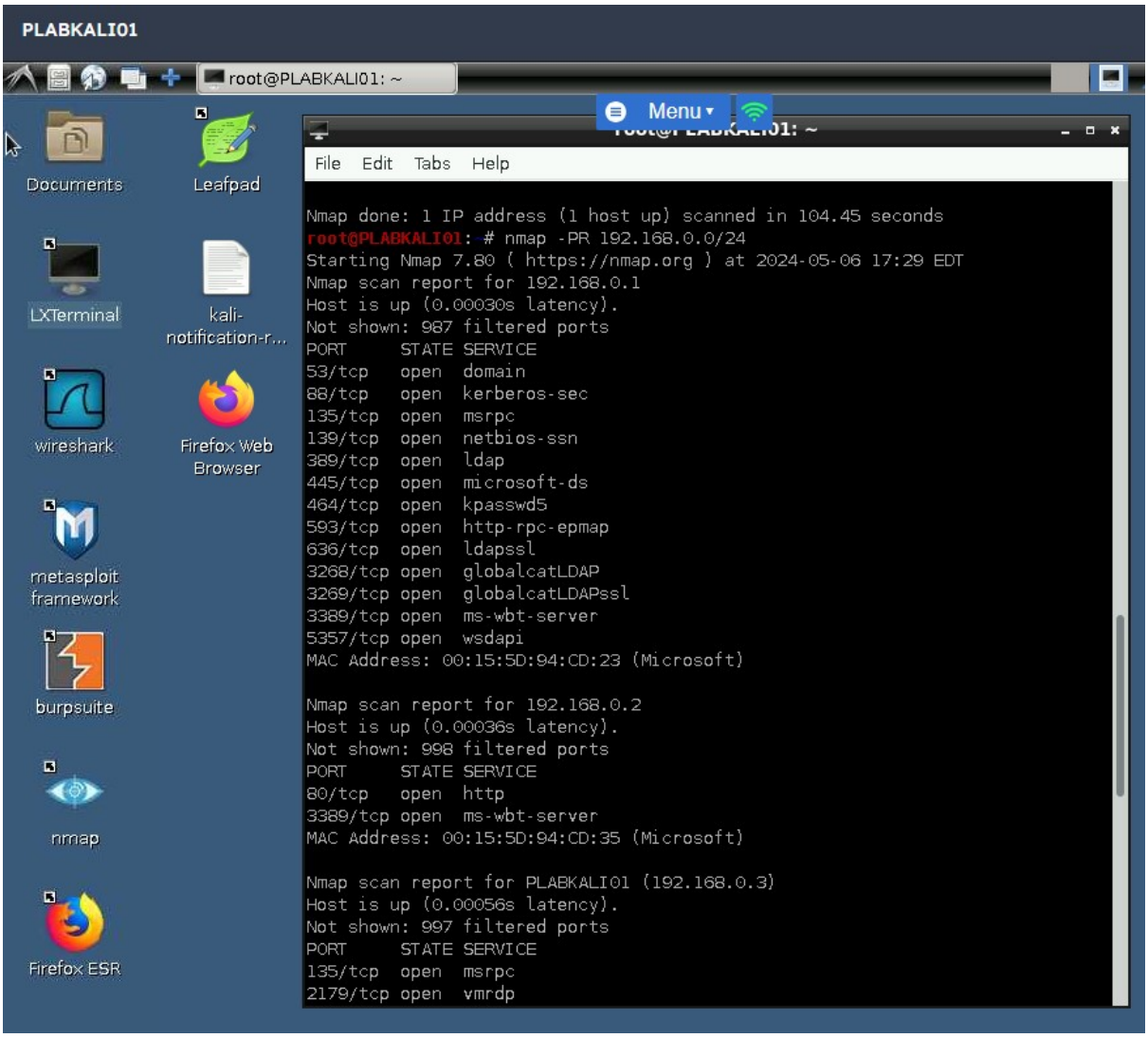


fig-13 ARP scan

ARP requests to the hosts on a given subnetand if the target system responds to these requests, then it means that it is alive.

This method, unlike the Ping scan method is not usually blocked by the firewall. Therefore, it is likely to get a better outcome.

In penetration testing host discovery is very critical step, it is very important especially whenever penetration tester finds on a targeted system that has a live systems or services which is up and running. This is the initial phase of penetration testing when a penetration tester map the network and find which IP addresses are reachable and active to penetrate. There are many methods which can be used for host discovery, ICMP, ping sweep, echo request and ARP scan.

After initial scanning, penetration testing includes to explore systems for vulnerabilities. By getting the information of live host and their active ports and services (such as HTTP servers, FTP servers, database services) that allows the tester to apply further specific vulnerability scanning and exploitation techniques suited to running services.

1.5 Scenario Assessment:

In our case study as penetration test, after the stage of finding the host discovery further penetration tester, it set out stage for further discovery using different intense scanning tools. After initial scanning, penetration testing includes to explore systems for vulnerabilities. By getting the information of live host and their active ports and services (such as HTTP servers, FTP servers, database services) that allows the tester to apply further specific vulnerability scanning and exploitation techniques suited to running services.

our host discovery finds many live system and services, including a web server running an outdated version of Apache on one 192.168.0.2 and a SQL database server on another IP 192.168.0.1. We as penetration tester uses this information to focus their efforts on these two systems to find further information. As our company Fashion&Trendz have web server with database, in our scenario assessment it may be exposed following two exploits:

- Web Server Exploitation
- Database Server Exploitation

The host discovery information by system scanning helps in identifying vulnerable systems present in network but also assists in planning the sequence of testing phases.

1.6 Implementation of controls to minimize the threats found in reconnaissance:

To minimize the threats identified in reconnaissance phase and to also reduce threat level, following method can be implementedfor security controls. By implementing these procedures in security controls can reduce attacks probability and also increase the difficulty level for attacker to successful carry out any attack:

- Network Segmentation can limit lateral movement of attacker in network if attacker tried to compromise any specific segment.
- Strong Authentication and Authorization Measures by using multi layer of security. e.g implement multi-factor authentication (MFA), strong password policies and role-based access controls.
- Regular Updates and Patch Management can help to minimize threats intelligence during reconnaissance and also automate the procedure of applying un-patched vulnerabilities.
- Monitoring and Logging of system, create logging activity of network traffic and continuo's monitoring of network also minimize threats found in reconnaissance.

C. Port Scanning

1.7 Port discovery on the web server:

Our one host, 192.168.0.2, is running a Web server

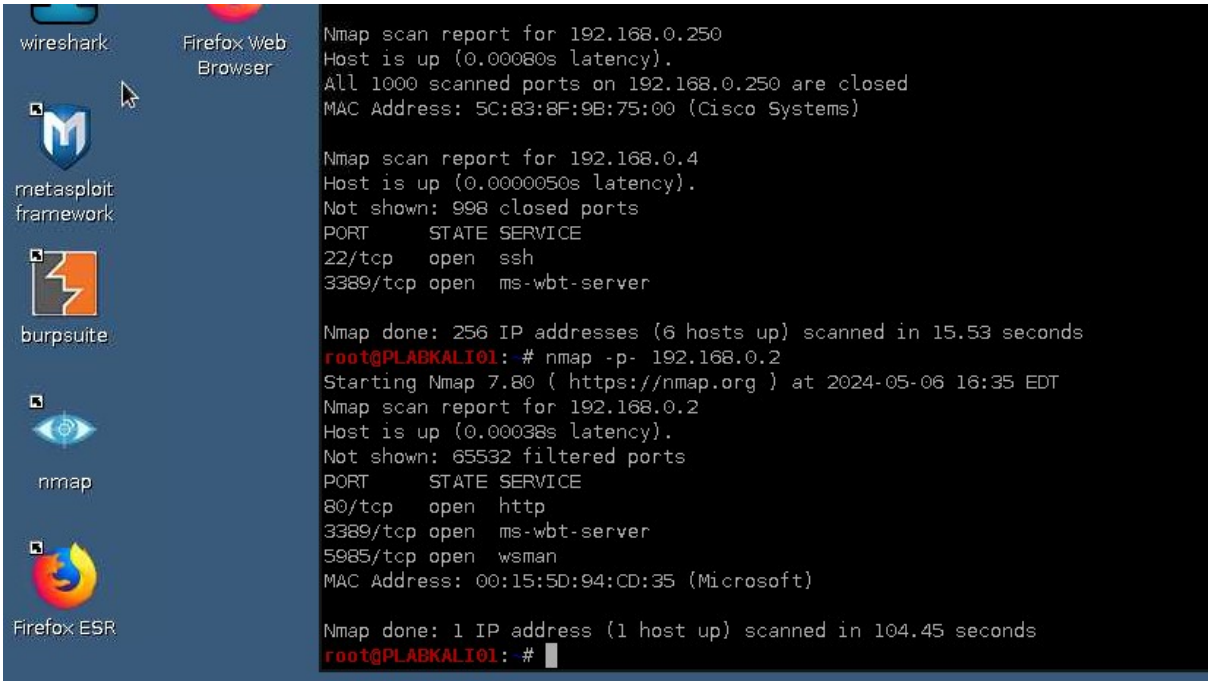


Fig-14nmap scan of all the port on live host i.e. 192.168.0.2

We can see that following ports are open 80/tcp having service http, 3389/tcp having service ms-wbt-server and 5985/tcp having service wsman.

1.8 Research and discuss on open port means and

Any open port on a server mean that server is configured and listening on that specific port. That port can receive connection and listen the data on that port. Open ports are considered as gateways of server thorough which they communicate with other devices. They can receive data or perform tasks according to given instructions. This ports are representated with numbers along with their services. Some of common ports are given below:

For web servers

HTTP on port 80

HTTPS on port 443

When a port is open the server is ready to accept data transmitted to assigned port, server can perform tasks like receiving user input, serving web pages and handling API requests.

Open ports can exposed to security risks if not properly managed. As these open ports can be used to listening and data transfer, they are act as entry points for attackers if outdated software, misconfigurations or unpatched security issuesare not resolved these ports left vulnerable. e.gan open HTTP port (80/tcp) might be vulnerable to attacks like cross-site scripting (XSS) or SQL injection if the web application is not securely coded. Attackers are can also perform reconnaissance on these open ports which give them information about services running on these servers that can be easily targeted for specific exploits. Ports left open can lead to data breaches, unauthorized access, and potentially, a full-scale network compromise if necessary security measures are not taken on time these security measures

are firewalls, strong authentication and traffic encryption over the network. It is therefore necessary to implement strong security policies in company, Security administrators should monitor open ports and implement security policies and that can reduce security risks and also to mitigate these risks effectively.

1.9Scenario Assessment:

As our host company Fashion&Trendzis running web server, during the testing of port scanning the information about web application can be used to exploit vulnerabilities,

Exploitation Scenarios for Open Ports:

Port	service	Vulnerability	Attack types
80/tcp	http	Web server open port 80	SQL injection (SQLi) Cross-Site Scripting (XSS) CrossSite Request Forgery (CSRF)
3389/tcp	ms-wbt-Server RDP	RDP,	Brute force attacks credential stuffing
5985/tcp	WSMan Windows Remote Management	implementation of the WS-Management Protocol	Unauthorized remote command execution

Table: Web application open ports exploits

Port 80 exploitation: An attacker can exploit our website to steal session cookies, inject malicious scripts using SQLi or even hijack user sessions.

Port 3389 exploitation: An attacker can gain unauthorized access to our web service by using RDP, that can escalate privileges to administrator levels.

Port 5985/tcp (WSMan)Exploitation: Attacker can execute random commands on our web server which can install malicious software like malwares, attacker can create new accounts with full user rights and then gain unauthorised access or alter system configurations to maintain full persistent access.

1.9.2Port knocking and protection against found vulnerabilities:

In an ethical context such as penetration testing to help our company's strengthen its security, we aim to use discovered information to patch and secure the systems before a malicious actor can exploit them. For example, findings from such tests should lead to:

- Patching outdated software
- Strengthening authentication mechanisms
- Configuring firewalls to limit access to sensitive ports
- Conducting regular security audits and updates.

Task 2 - Server-Side Exploits

a. Data Tampering

Data tampering is a server side exploit as it performs on the server machine by the attacker using different method to exploit this vulnerability.

2.1 Identifying application is vulnerable to data tampering and exploit.

Identifying for a web application is vulnerable to data tampering has involved in many steps which can be discoverable and weaknesses that could leads be exploited by attackers to manipulate data and data tampering in server side. Followings are the few type of test to check data tempering.

Type	Testing procedure	How to test
Input Validation Testing	Checking unexpected or malicious input	• Input non standard or malicious data into all input fields that • Check for error messages or system behaviour that indicates input is being executed or treated as data.
Error Handling and Messaging	Trigger errors intentionally by providing incorrect inputs or requests	assess result (database name, server path)
Tampering with HTTP Requests and Responses	Burp Suite OWASP ZAP Modify HTTP requests and responses	• Change parameters or tokens • Modify hidden field values • Alter session data
SQL Injection	Insert SQL syntax by manipulate its syntax	Check by input data in SQL

Table: Data Tempering testing types

Penetration Testing can also give information of data tampering vulnerability by performing different method to assess web application.

2.2 Data Tampering Vulnerability

Data tampering is unauthorised alteration of data. These activities can be during data in transit, at rest, or during the processing of data within a web application. When an application fails to adequately protect data integrity, allowing attackers to modify data such as user credentials, permissions, price information or any other sensitive data managed by the application then it results data tempering. (Aljawarneh, S,2010) Input validation very crucial yet often overlooked in web development which can be serious security issues like like unauthorized data access. This study finds vulnerabilities like SQL injection, reviewing common validation techniques and proposing a new semantic web-based data validation service to minimize data tempering.

Which Tenet of Cyber Security is Violated during Data Tampering:

Data integrity is very important in three basic cyber security rules. Data tampering affacts the integrity tenet of the cybersecurity. As we know confidentiality, integrity and availability are the important tenet of cyber security. As tampered data is due to unauthorised alternation that is why it can cause many problems. Tampered data does not have the authenticity of data and lost integrity completeness.

2.3 Scenario Assessment:

During the assessment, our company Fashion&Trendz has web server application that can be vulnerable to data tampering, various types of sensitive information could be at risk. We have customer information like Name, Address, Email, Customer preferences, Customer Sizing Information, Financial information. Vulnerable information in our scenario may involve following step:

- User Credentials
- Financial Information
- Sizing Data
- Customer Preferences
- Email
- Company information

This exploit can cause severe damage that including financial loss, legal liability, loss of customer trust and damage to reputation.

Strong validation can protectFashion&Trendz'sweb applications from data tampering. The Implementation of secure communication channels, installing firewall and define secure rules, ensuring robust authentication and authorization and utilize integrity checks. It is also recommended to use best security practices and regular security assessments for mitigate the risks associated with data tampering vulnerabilities.

b. SQL Injection

2.4 Identifying SQL Injection Vulnerabilities

To identify if a web application is vulnerable to SQL injection, We are performing the following tests:

Illustration of SQL Injection by GET/Search Method

SQL Injection (GET/Search) in web application

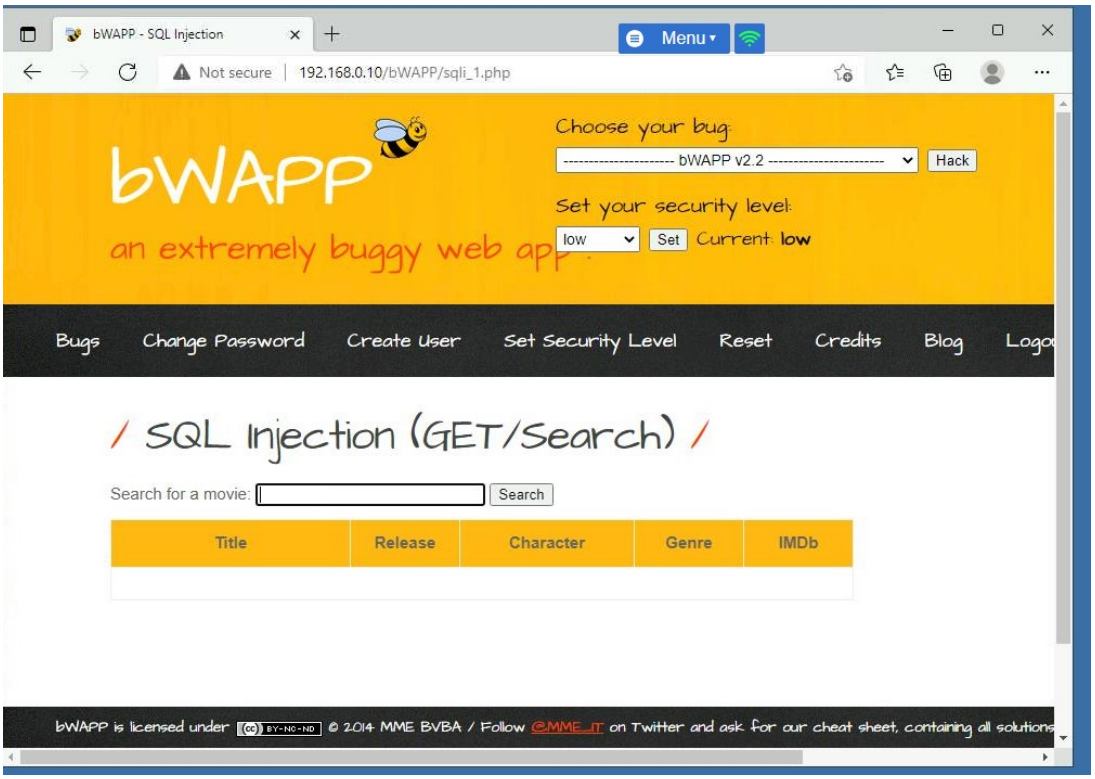


Fig-15 Input field of web application

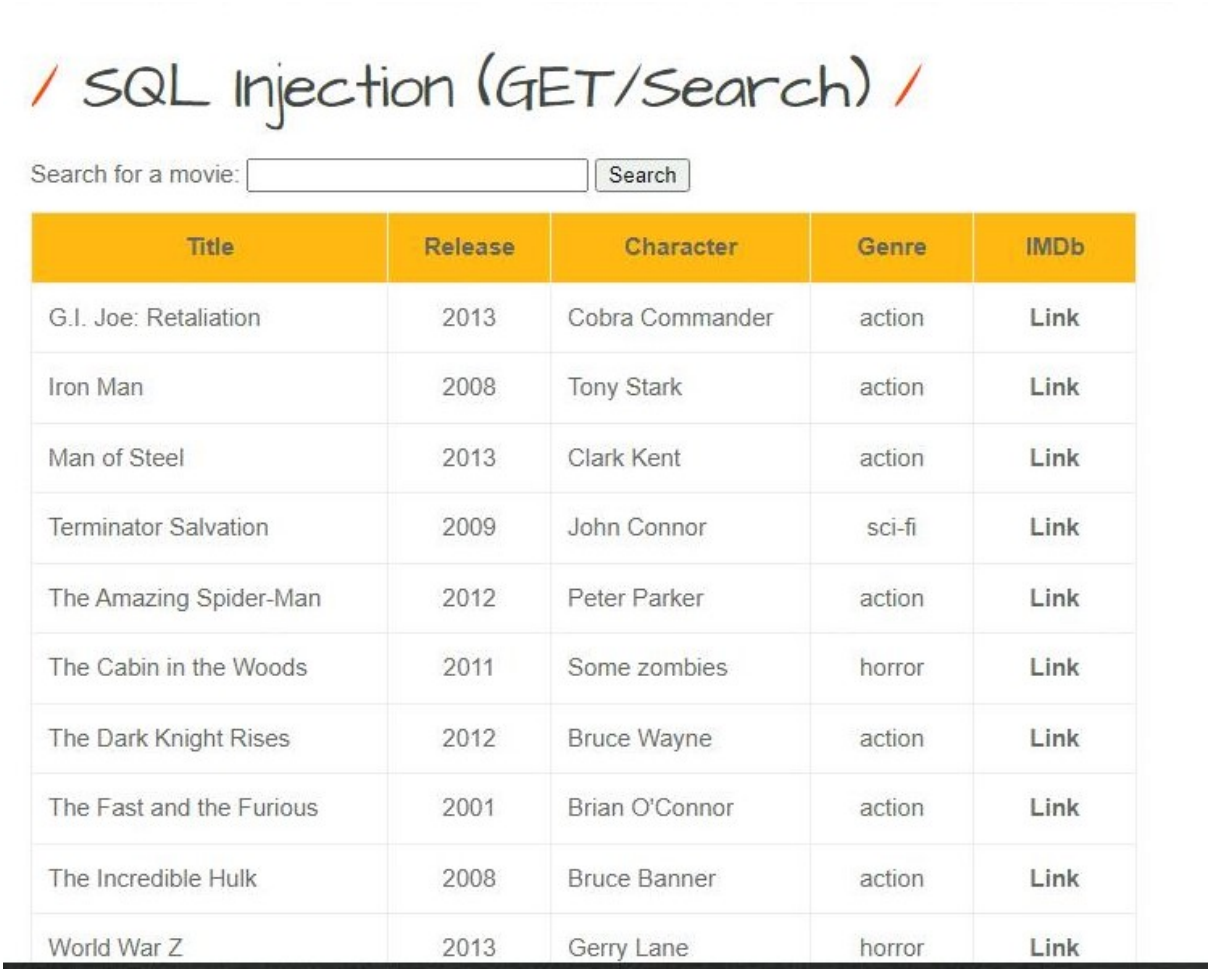


Fig-16 SQLi vulnerability fetch record from database

Type m' because this application is vulnerable to SQLi

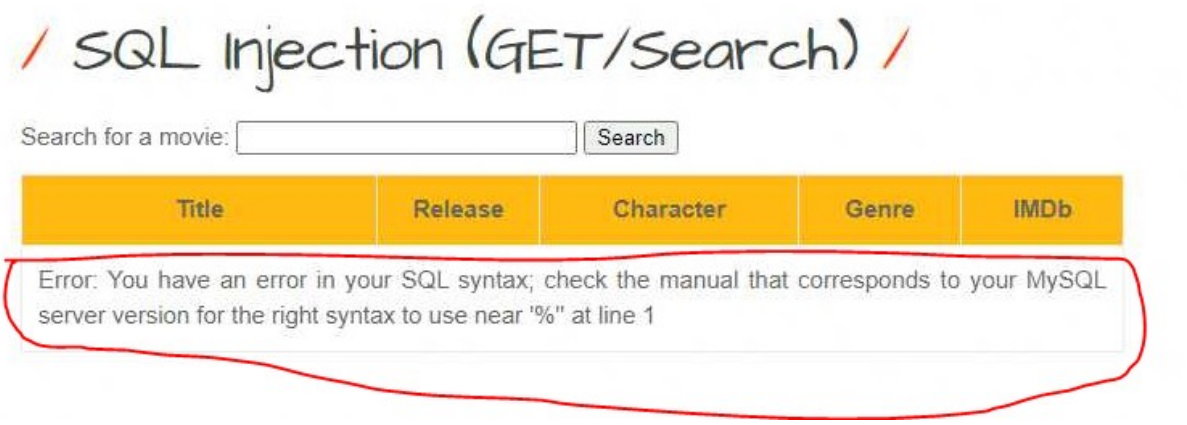


Fig-17 SQL injection web application interface

From the error message, it is giving too much information.

In this case, identifying the type of database the web application uses (MySQL) lets potential hackers know to use only MySQL exploits. We need to make a hacker work harder for that type of information.

SQL Injection input validation

Input Validation Testing: Insert SQL control characters or SQL syntax into user inputs. Examples include inserting single quotes ('), double quotes ("), semicolons (;), and SQL keywords like OR '1'='1.

Error Messages: Observe the responses from the application. SQL errors or unusual responses when inserting SQL syntax can indicate vulnerability.

Behavioural Analysis: If the application behaves differently or returns more data than expected when SQL commands are inserted into inputs.

2.5 SQL Injection Vulnerability

SQL Injection (SQLi) is a of vulnerability that is injecting malicious SQL queries into an input field of a web application, This query act as a SQL query and get results from the database. If web application has this vulnerability then attacker can extract database entries without permission while executed query in the backend database. This can result in unauthorized access to the database that can allowing the attacker to view, modify, delete or update the record.

SQL injection attack techniques

Tutology - Injected code by conditional statement

Union Query - run an operator to combine result

Stored Procedures - running query by stored procedure in database

Piggy-backed queries - attack that compromises a database using a query delimiter, such as ";"

Timing Attacks - Attacker collects information by monitor timing delays in response

Blind Injection - attacker to compromise the database through asking aseries of logical questions through SQL statements

Cybersecurity Tenet Violated

SQL injection vulnerability affects and largely violates the confidentiality. As there are threeaspect of the CIA triad (Confidentiality, Integrity and Availability). SQLi allowing unauthorised access of data that compromises confidentiality. It is also impacting integrity of the same by altering data and availability by potentially corrupting data.

2.6 Scenario Assessment:

SQLi in our case study of Fashion&Trendz web application involves risks and potential damage threats due to text input fields.

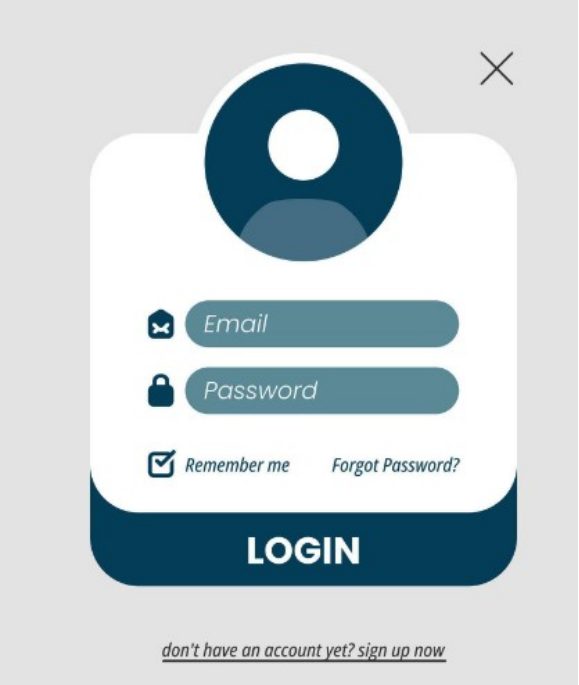


Fig –18 Login form

In our scenario if a SQL injection is successful, attackers could potentially have access Confidential Data,such as customer records, employee information, financial information, user information. Attacker can modify or destroy data: Leading to operational disruption and loss of trust. Attacker potentially privileges escalationand can gain administrative rights within the application by using SQLi. If SQLi is successful, then attacker can carry Out further attacks by using compromised server and can have further access to other systems.

2.7 Protecting Against SQL Injection

There are many procedural steps and technical controls to protecting Fashion&Trendzdatabase against SQL injection (SQLi).

- Prepared Statements (Parameterized Queries): This method can be used to ensure that SQL query are safely constructed before execution.
- ORM Frameworks: This process involves Object-Relational Mapping which abstract the database information by making object before executing the query without direct interaction of SQL statement from users.
- Implement input Validation: This is the process of validation of input before execution and make sure that no malicious code present in the SQL statement.
- Least Roles and Privilege is a process of that ensure that web application has right account privileges for accessing web application and only the permissions necessary to perform its tasks for every level.
- WAF implementation can also detect SQLi and block it from running before injection the query into database.
- Regularly update and apply patches also reduce the risk of SQLi, in this process regularly update and patches update company database and softwares from threats.
- Regularly perform security testing techniques also stop SQLi attack this security testing including vulnerability assessments, penetration testing.

C. OWASP Vulnerability

2.8 Identifying vulnerabilities in a machine that is part of an OWASP (Open Web Application Security Project) Vulnerable Machine are used for practices and to enhance skills in a controlled environment.Two common types of vulnerabilities are given blow:

Injection

Server-Side Request Forgery (SSRF)

These vulnerabilities can have significant implications for the security of web applications and their underlying servers.

Injection

In injection vulnerability an attacker sends malicious command or attack to an application. Example of such injection is SQLi, in which attacker uses SQL command to inject query in application input field and get result by fetching data from server. In SQLi attacker can obtain, data from tables, view admin user, manipulate data in tables.

SSRF exploits uses a server's request that has to make from attacker system for accessing external server access. Attackers use SSRF to force the server to send requests to unintended locations, for accessing external servers or services. These also including internal services that should not be accessible externally. In this method a request is sent to internal system so that by making the server send a request to internal systems to exploiting internal servicesand it can bypass firewall protections, exposing sensitive services to attackers. This can include services like databases, caching servers or administrative interfaces.

2.9 Scenario Assessment:

In scenario assessment of Fashion&Trendz web application can exposed to unauthorized access where attacker can gaining access to other confidential users' data, including personal information, customer email, customer sizing information.

If this web application is vulnerable to SQLi then by using SQLi attacker can manipulation or deletion, Modifying or deleting data belonging to other users, which could lead to data loss or corruption and affects integrity of data.

In Server Side Request Forgery (SSRF) can allow attackers to perform actions on server to obtain sensitive information by manipulate users rights and gain access by using external services. That can cause significant damage to the integrity of website and also users' trust for their data security.

Violated Tenet: In cyber security we know three triad is (Confidentiality, Integrity and Availability). These two vulnerabilities affectsthe confidentiality and integrity of data as unauthorized access to and manipulation of sensitive information.

Task 3 - Client-Side Exploits

Man in the Middle Attack (MiTM)

3.1 Show how an attacker can capture network traffic from a session a genuine user and the server side of the application.

To perform a MiTM attack, the specific location of the BWAPP application isn't critical as long as it's accessible from the network where the attack is being performed. Typically, the scope is to deploy BWAPP on a server accessible to both the client (Windows 10 workstation) and the attacker (Kali Linux workstation) within the same network.

Step to Configure Ettercap and to perform ARP spoofing by selecting the appropriate network interface (e.g., eth0) and specifying the target IP addresses for the Windows 10 workstation (PLABWIN10) and the BWAPP server in our case.

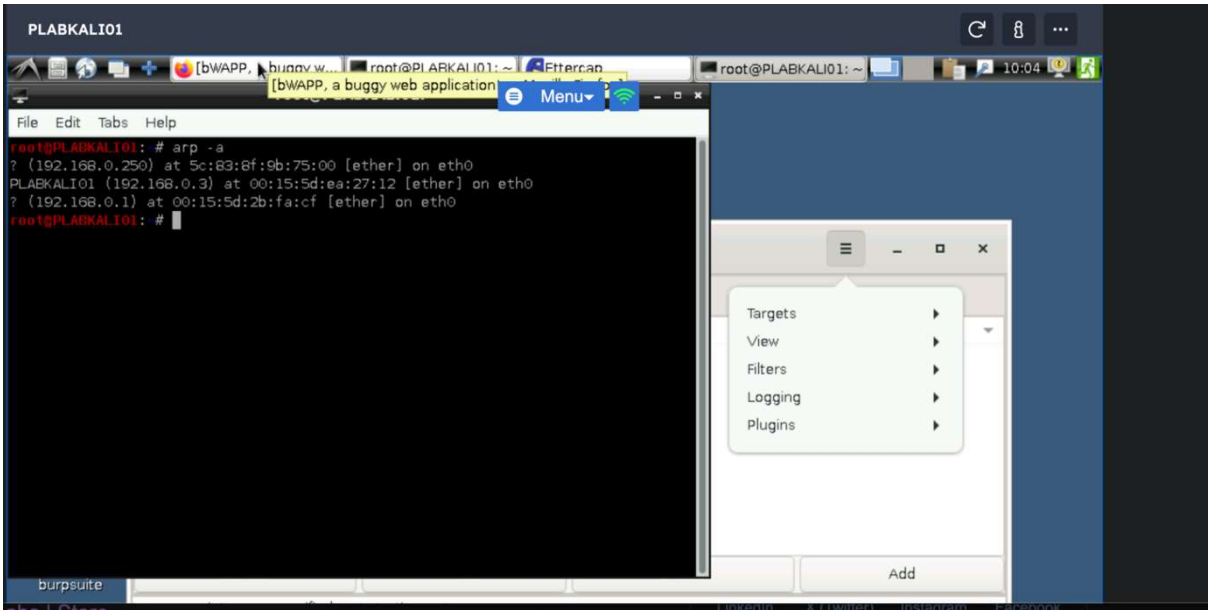


Fig-19

Fig-20, Ettercap interface

Fig-21 Scanning the hosts

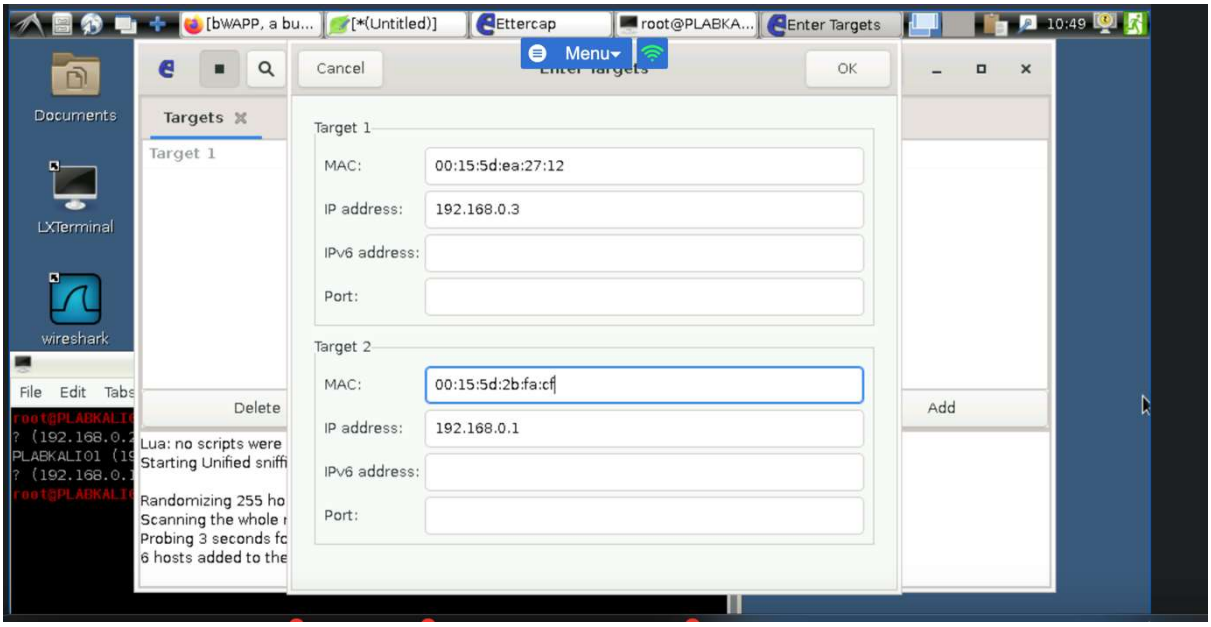


Fig-22 Target IP Address

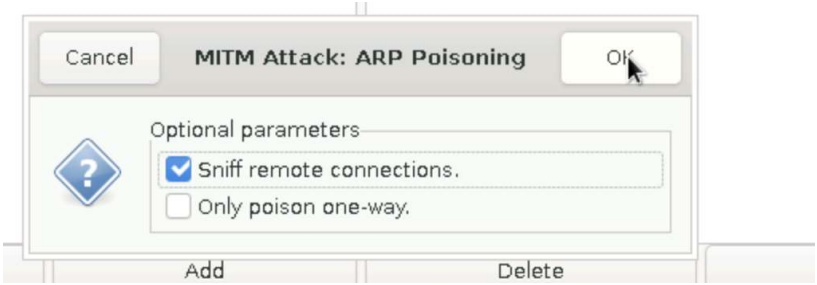


Fig-23 MITM Attack ARP Poisoning

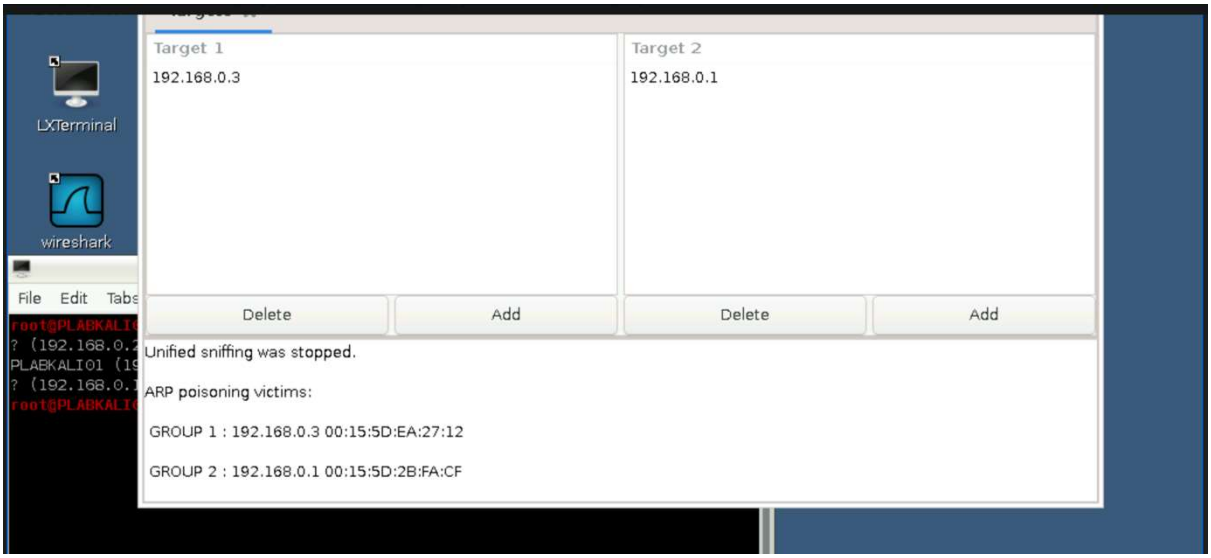


Fig-24 intercepted traffic

With ARP poisoning enabled, Ettercap is intercepting and redirecting traffic between the targeted hosts (PLABWIN10 and the server hosting BWAPP).

Capture packets by clicking on a relevant option in Ettercap's interface (e.g., "Start Sniffing" or "Capture Packets"). This allows monitoring the intercepted traffic.

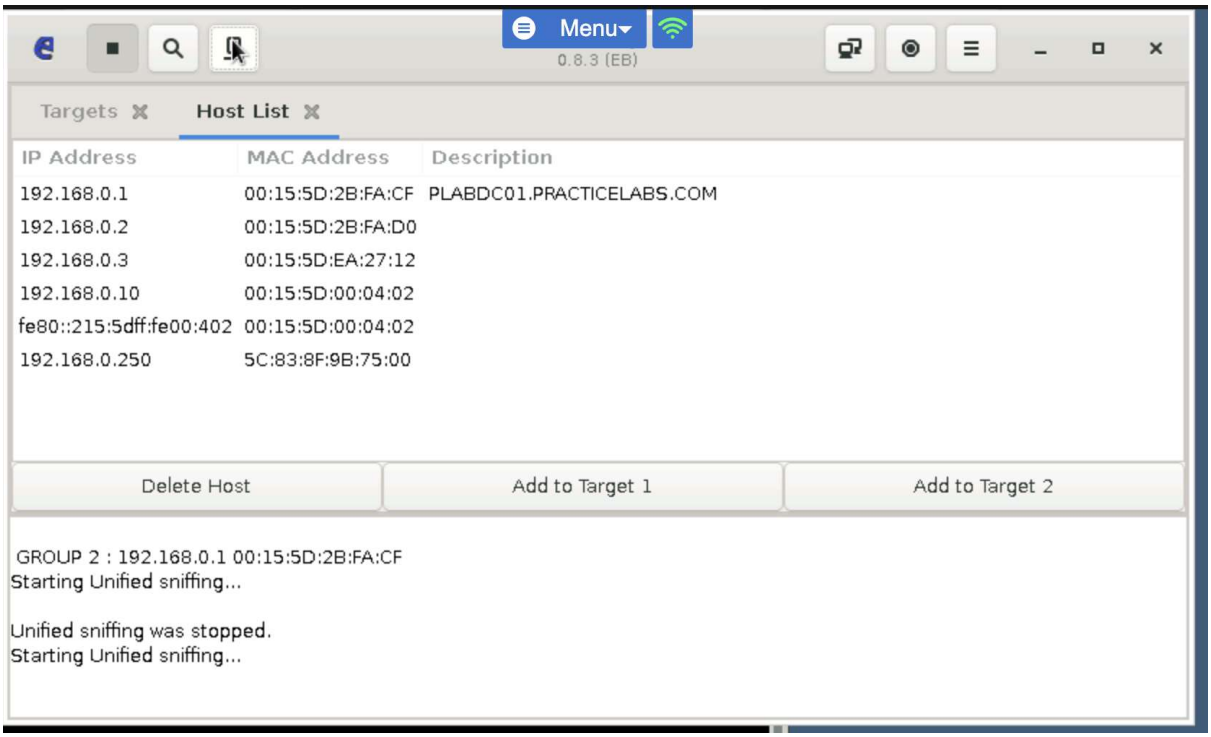


Fig-25 intercepted data

Analyse Traffic:

While the user session is active, we pressed "View" > "Connections" to view the intercepted connections.

As stated the Host 192.168.0.1 Port 49975 where the bWAPP session was running was intercepted.

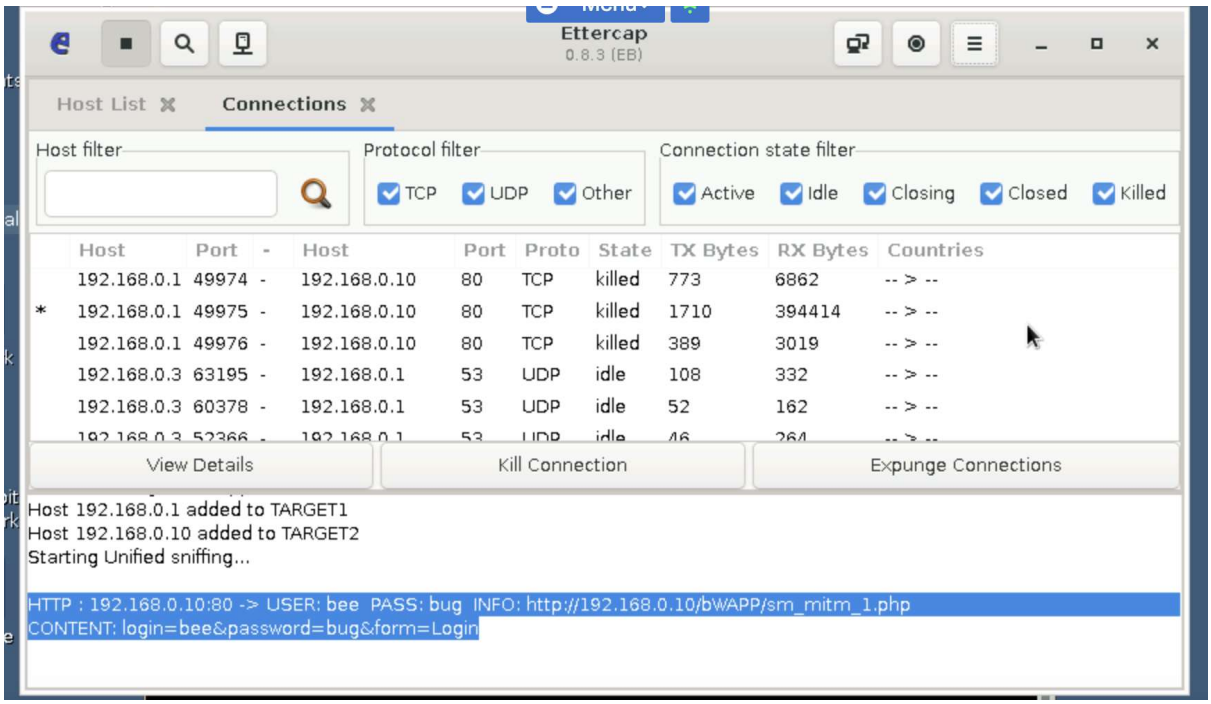


Fig-26 traffic capturing

Document Findings:

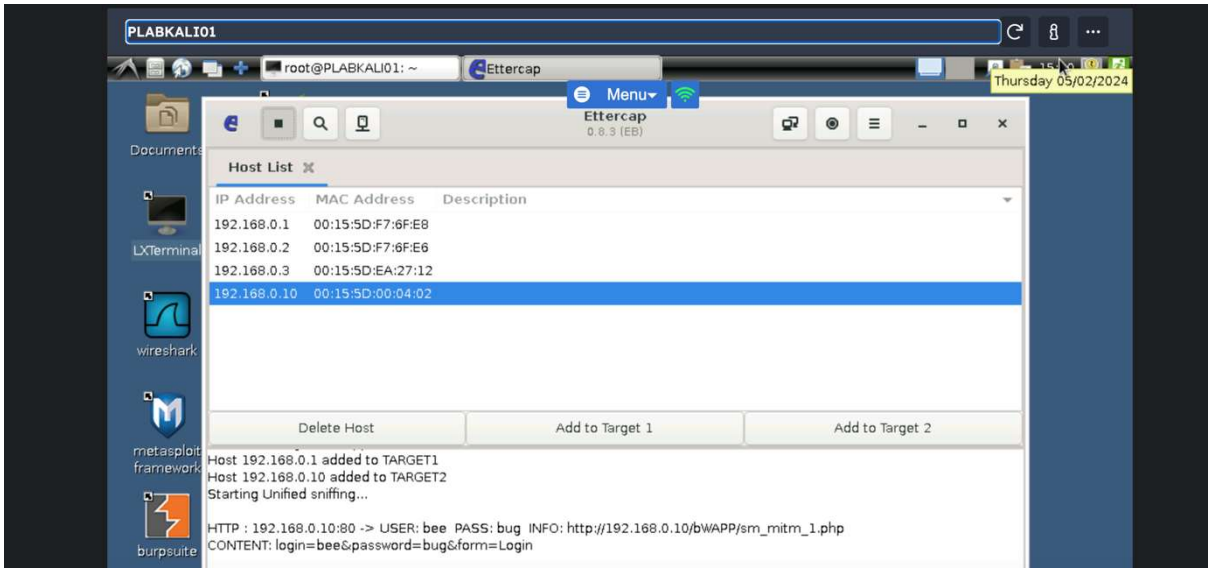


Fig-27 Ettercap screenshot

The server-client for Windows has been intercepted whilst a simluation of a user session was undergoing on its own VM. By applying "Mitm" > "ARP Poisoning" to launch ARP spoofing on the set targets, it generated an outcome from the HTTP Mitm traffic including the prescribed Username: bee and Password: bug.

Important:

In our scenario as a company this is known to be as sensitive data which must be recorded and used in accordance with Data Protection Protocols. Preferably on a secured pass-encrypted notepad.

3.2 Scenario Assessment:

In the scenario where the flaw linked to the "form=Login" parameter is exploited, an attacker can grab sensitive data like usernames, passwords and session cookies when they intercept the login traffic. This stolen information can let them access the web app as legitimate users, potentially causing harm by accessing private data or even carrying out further attacks.

Due to following reasons these are very critical activity:

- Allowing unauthorized access
- Risk of a data breach
- Opens the door for more attacks
- lead to compliance violations

Exploiting the "form=Login" parameter vulnerability poses a significant risk to the web app, its users and the organization as a whole.

3.3 Investigate and to protect the impact of MiTM.

To safeguard data transmitted between clients and servers, it's crucial to use secure communication protocols like HTTPS, which encrypt information. This prevents attackers from eavesdropping on sensitive data.

Using the provided details,configuring the web application (BWAPP) on PLABDC01 to enforce HTTPS encryption for all communications would be efficient. This can be achieved by configuring the web server software (e.g., Apache or IIS) to use SSL/TLS certificates and enable HTTPS. Additionally, Wireshark and tcpdump suggested to monitor.

Given scenario regular security audits and penetration tests using tools like Nessus or OpenVAS on devices for vulnerabilities. These scans can identify weaknesses such as outdated software, misconfigurations, or insecure network settings that could be exploited by attackers to conduct MitM attacks. By addressing these vulnerabilities promptly, it can reduce the risk of successful MitM attacks and enhance the overall security posture of the organisation.

b. Social Engineering Attack

3.4 Demonstration how attacker can lure a normal user.

The scope of such demonstration is large in its context. In our regards, supporting the latter, of the scenario; credentials harvester method can be an option. Typically

this involves creating a fake login page that mimics the legitimate login page of the target website (in this case, Fashion&Trendz's web application simulated on the bWAPP). The attacker then sends phishing emails or messages to the target users, directing them to this fake login page and prompting them to enter their credentials. When users enter their credentials on the fake page, the attacker captures and harvests these credentials for malicious purposes.

By demonstrating it effectively simulates how an attacker can lure users away from the legitimate server to the computer by tricking them into entering their credentials on a fake login page. This demonstrates the effectiveness of social engineering tactics in compromising user security and highlights the importance of user awareness and vigilance in detecting and avoiding such attacks.

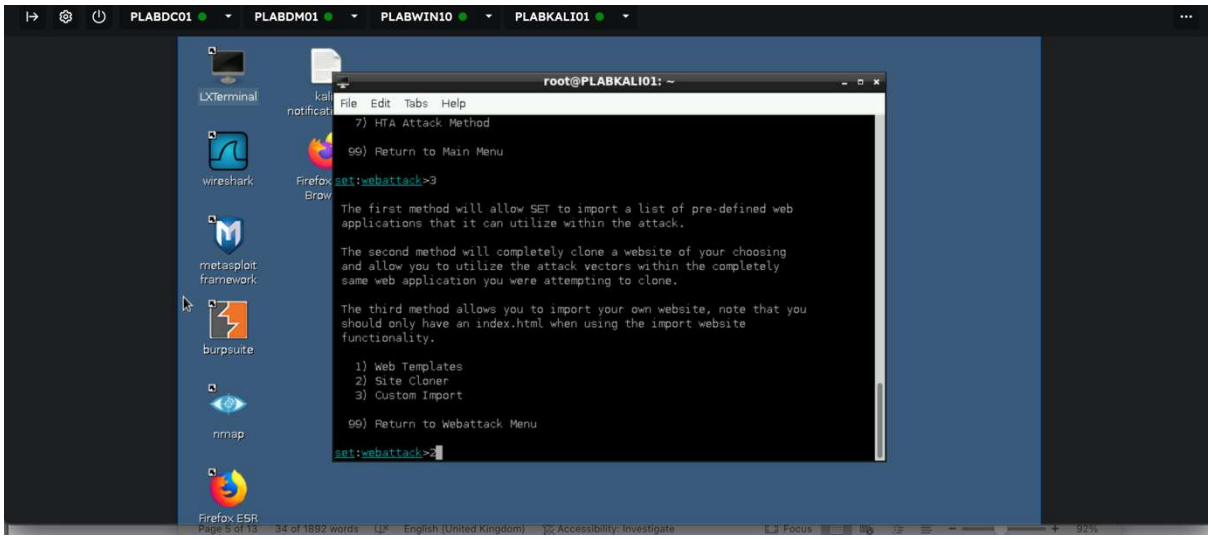


Fig-28 Social Engineering attack

For the task of simulating a social engineering attack using the credentials harvester method within BWAPP, you should choose the "Site Cloner" option. Here's why:

Site Cloner:

The Site Cloner option in the Credential Harvester Attack menu allows you to clone an existing website or web page, including its content and structure.

This option is suitable for replicating the login page of BWAPP or any other target website where you want to harvest credentials.

By cloning the login page, you can create a convincing phishing page that mimics the appearance and functionality of the original login page, increasing the likelihood of users falling for the phishing attempt.

Ensuringthat configuration cloned page to capture and store the entered credentials securely for analysis.

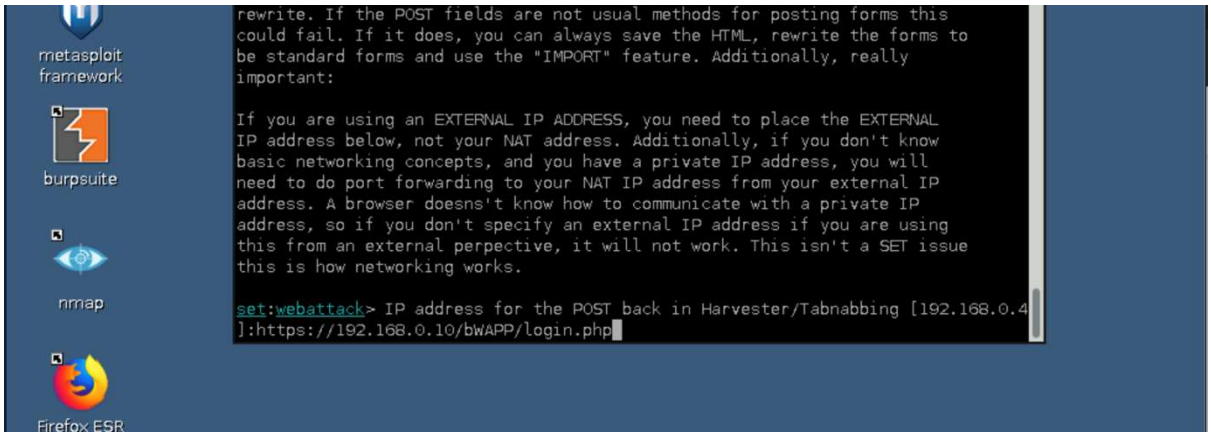


Fig-30 Social Engineering URL

Enter the URL of the target website whose login page you want to clone. In this case, enter the URL of the BWAPP login page hosted on PLABDC01.

In this case: htttp://192.168.10/bWAPP/login.php

This will create a phishing page that mimics its appearance and functionality for use in the social engineering attack.

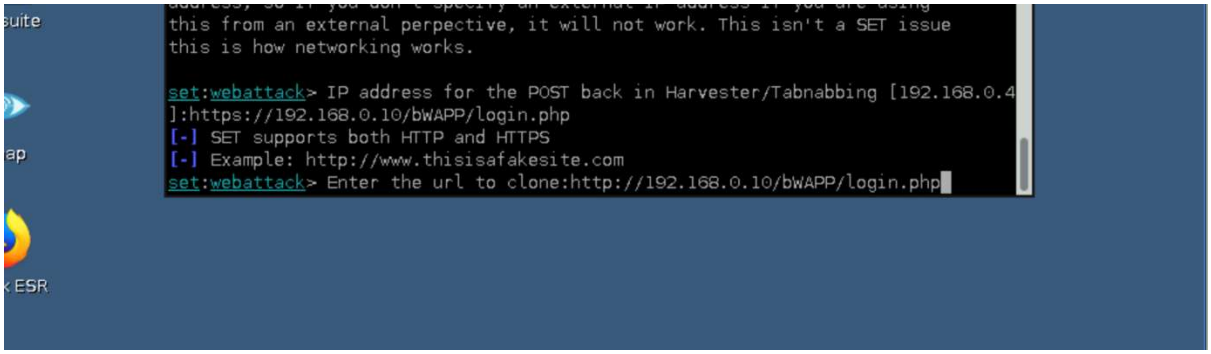


Fig-31 Phinsing screen shot

In the context of a phishing attack using the Social Engineering Toolkit (SET), the post-back URL is the location where captured credentials are sent after a user enters their login information on the cloned phishing page.

Cloning the login page of the BWAPP application, we can use the same URL for both the login page URL and the post-back URL. This ensures that captured credentials are sent back to the same location from where the phishing page was accessed.

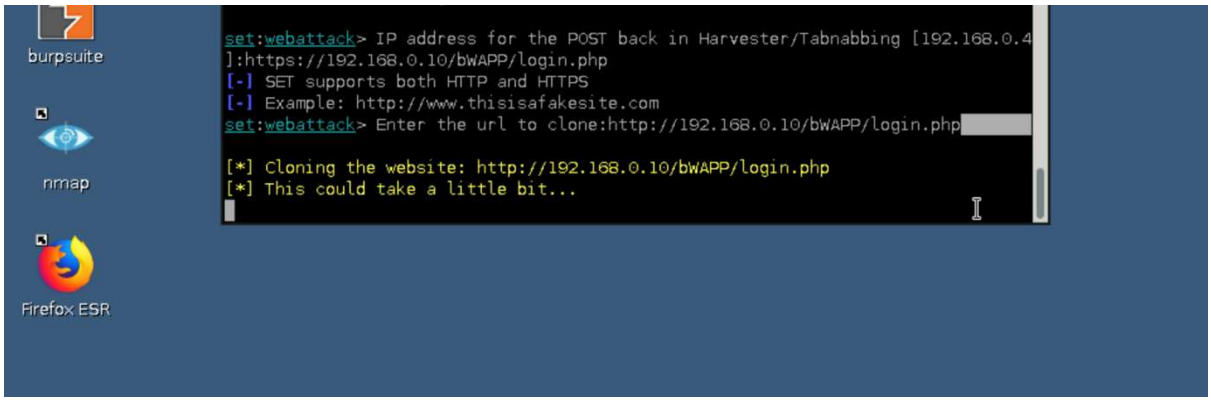


Fig-32 Cloing of websit screen shot

Since this process was unable to clone the target website, port forwarding may be necessary, as the target website is hosted on a remote server and I shall, in practicality, be accessing it from outside the local network.

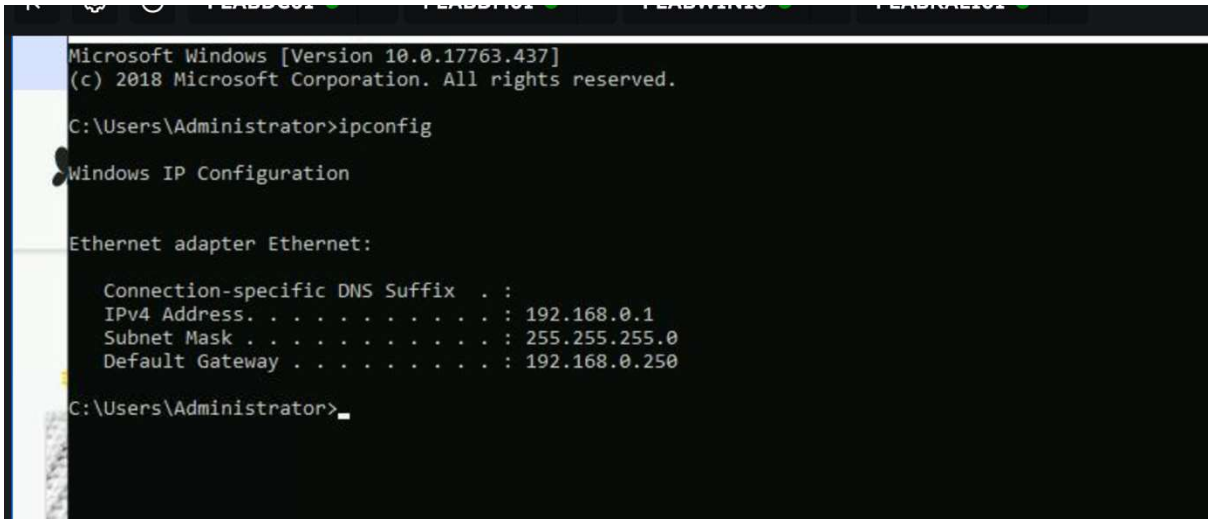


Fig-33 IP address

The default gateway should be typed in the URL to access the the router's administration panel.

Although since the parameters of the practice labs are set so robust, entering the default gateway it gave an error:

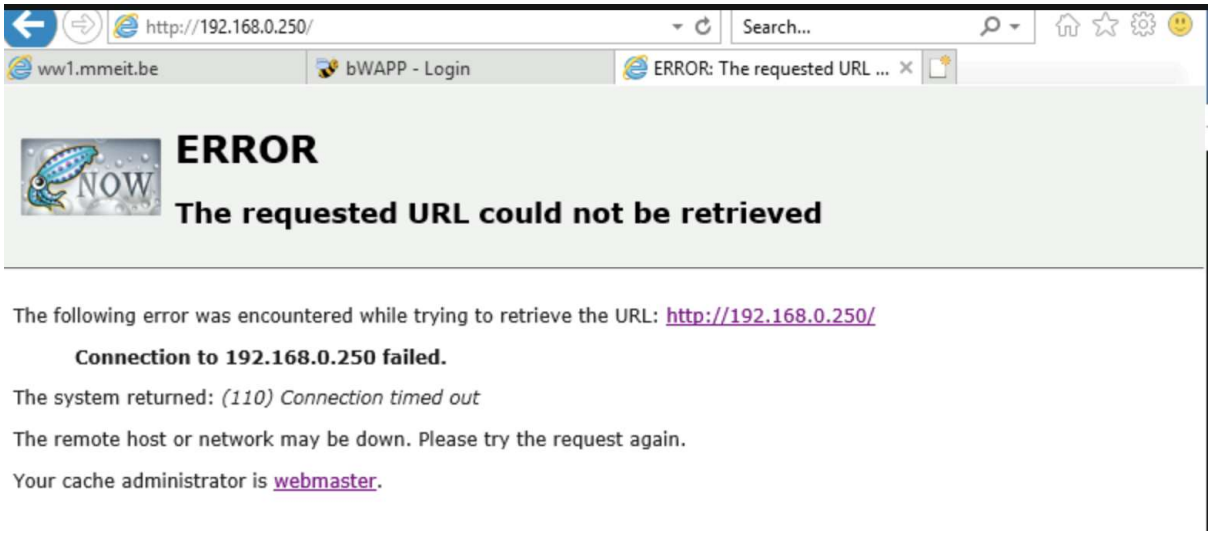


Fig-34- Access of Server

This occurrence is a factor upon the medium of the VM's used via the practice labs. Even though the step-by-step guidance was set to be completed correctly undergoing conduct.

Hence, for the continuation of this task we will still answer objectively to sustain the scope of our demonstration effectively.

Hence, we would proceed with a crafted persuasive phishing email on System. Pretending to be from Fashion&Trendz's IT support or a trusted authority figure and mention a security update or account verification process that requires users to log in to their accounts.

Example:

Subject: Urgent Security Update - Action Required Immediately

Dear Fashion&Trendz Staff and Customers,

As part of our commitment to ensuring the security and integrity of our systems, SecureTech Solutions has identified a critical security vulnerability within Fashion&Trendz's web application and database infrastructure. Our penetration testing engagement aims to assess the security level of Fashion&Trendz's systems, including the web application, database, and information system.

Given the nature of Fashion&Trendz's operations and the sensitivity of the data involved, it is imperative that immediate action be taken to address this vulnerability and mitigate potential risks. Failure to do so may compromise the confidentiality, integrity, and availability of personal information belonging to both customers and staff.

To address this security concern, please follow the instructions below to ensure that your devices are properly secured:

Consider enabling two-factor authentication for an additional layer of security.

Remain vigilant for any suspicious activity on your account and report any concerns to Fashion&Trendz support immediately.

Please note that these measures are essential for protecting your personal information and safeguarding Fashion&Trendz's systems against potential threats. Your cooperation in this matter is greatly appreciated.

Should you have any questions or require further assistance, please do not hesitate to contact our IT support team for guidance.

Thank you for your attention to this urgent matter.

Best regards, SecureTech Solutions Team.

This email provides clear instructions for staff members and customers to take proactive measures to enhance security. It emphasizes the importance of securing accounts and remaining vigilant for potential threats.

In simpler terms, it's like someone pretending to be a trusted colleague or service provider to trick you into giving them your login details, which they can then use to access sensitive information or systems.

3.5. Scenario Assessment:

In the context of our scenario, a potential attacker stands to gain access to login credentials through harvester method that is a social engineering attack. This will create a fake account having login pages that is similar to the original service, but the amin of the attacker to get username and password.

Depending on scenario should such an attack succeed within our case, the implications are dire because it can affect integrity of data. The attacker would have acquire sensitive information, including user name, on which a user access to their services and a the gateway to Fashion&Trendz's web application, database. This sensitive data may contain user information, their email, personal sizing information also staff user account present in the database.

The type of breach can impacted further due to implications of the scenario. Firstly, customers and employees like to be risk of identity theft, financial exploitation and invasion of privacy. With access to payment details and personal records, malicious actors could perpetrate fraudulent transactions, leading to monetary losses for both individuals and the company.

It can also damage in in terms of reputation and trust of the company. This security breach reduces the trust by the customers and image of our company

Fashion&Trendz's. Resultantly finance loss of the company also loss trust could precipitate a decline in customer loyaltyand credibility of business.

3.6 Investigate and explain the actions of scenario to be avoid:

Following step to be taken for investigate and explain the actions to avoid Social Engineering.

- Conduct Employee Training and Awareness to avoid social engineering attack.
- Implement Phishing Simulations to employees and train them for fake websites.
- Security purposes implement Email Filtering and Security methodology.
- Multi-Factor Authentication (MFA) help to reduce unauthorized access.
- Regular Software Updates and Patch Management also fix vulnerabilities and security flaws.
- Website Verification and HTTPS Encryption also introduced for security purposes.
- Incident Response Plan if any malicious traffic or activity observed over the network.
- Continuous Monitoring and Threat Intelligence also minimize the risk of social engineering.

c. Denial of Service Attacks: DoS the Web Server

3.7 Demonstration of DOS on Web server.

This is the demonstration of DoS Attack on the Web server that serves web pages. In this method we use Hping3 command to flood the web server and causing it to become overwhelmed for response to actual user.

Followings are the step:

1. Finding IP address of Fashion&Trendz web server for DoS Attack.
2. Nmap scan web server
3. Use Metasploit
4. Checking for web server is running and live for further attack.

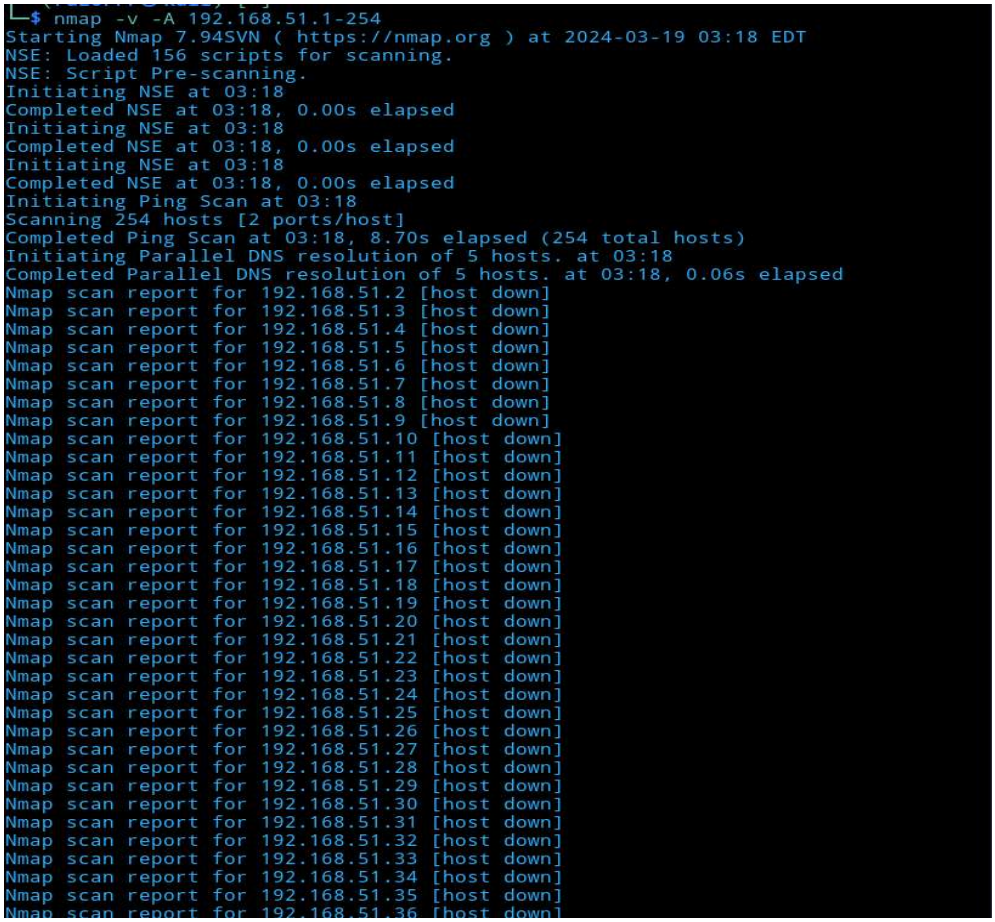
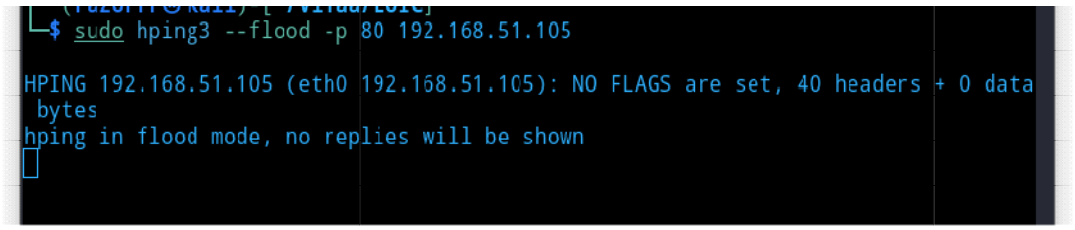


Fig-35 nmap scan of host

```
Nmap scan report for 192.168.51.105
Host is up (0.0063s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.51.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETR
N, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA
/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPro
vinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
|_SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2024-03-19T07:06:42+00:00; -13m15s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

Fig-Screenshot of metasplitable

5. Start hping3 for flooding on target

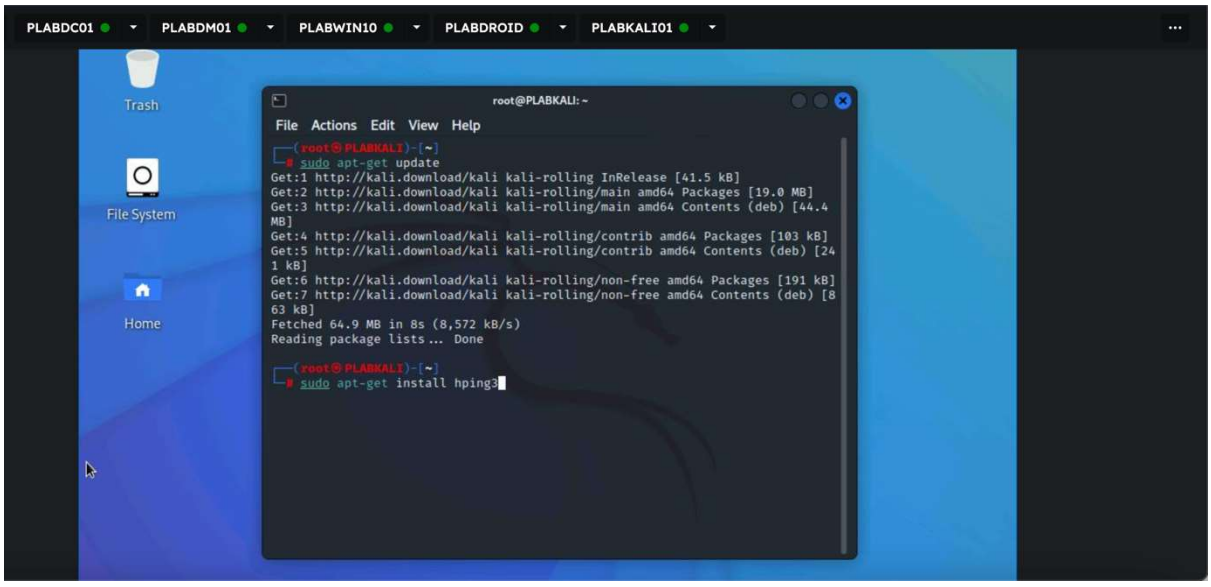


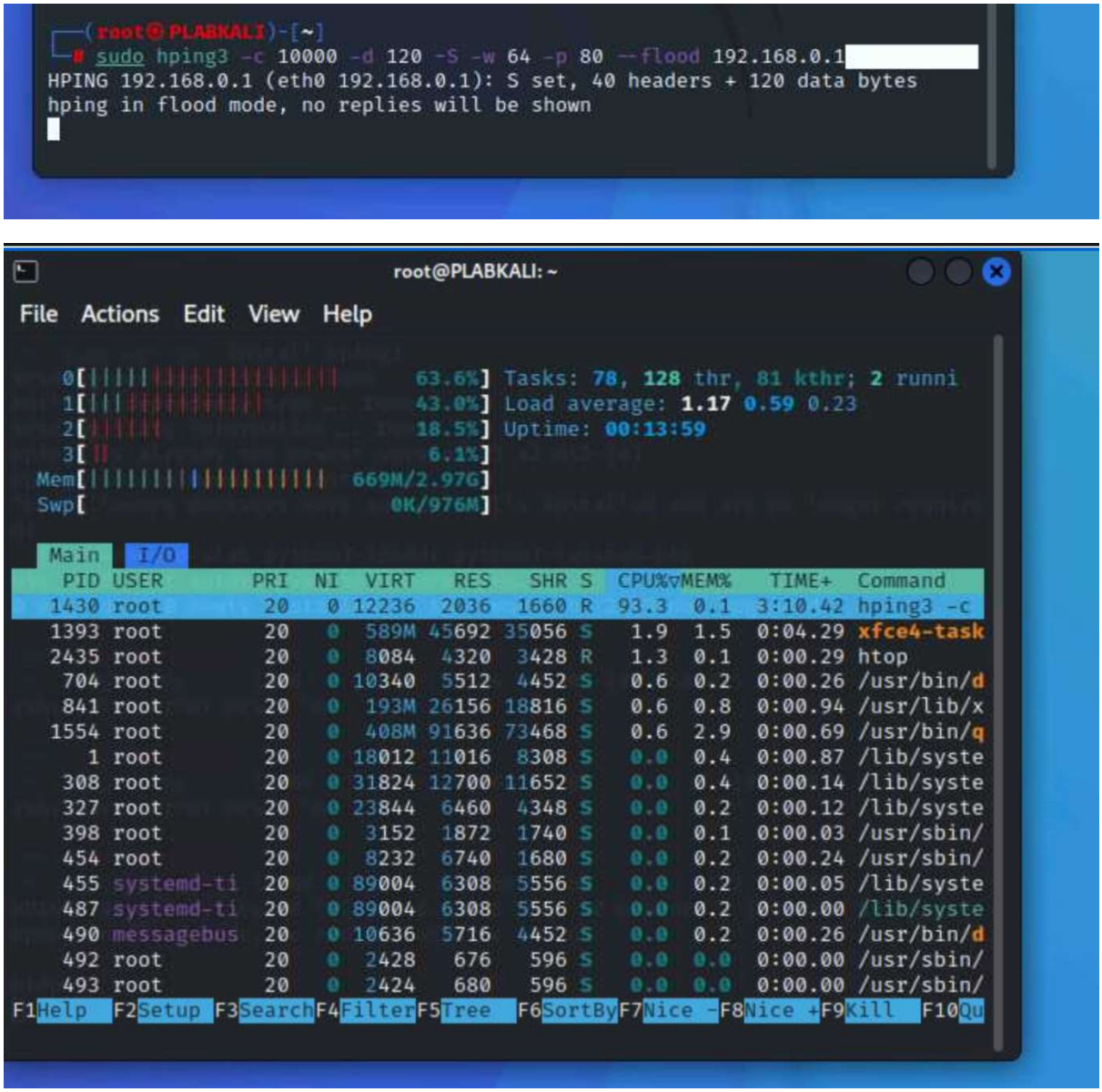
6. After flooding attack, check the server where service is running.

Fig-Sever Response

From the figure it is shown that server is not responding and it take so long.

Step 1: Determine the IP address of the web server hosting bWAPP. In this case, it's the IP address of PLABDC01, which is 192.168.0.1.

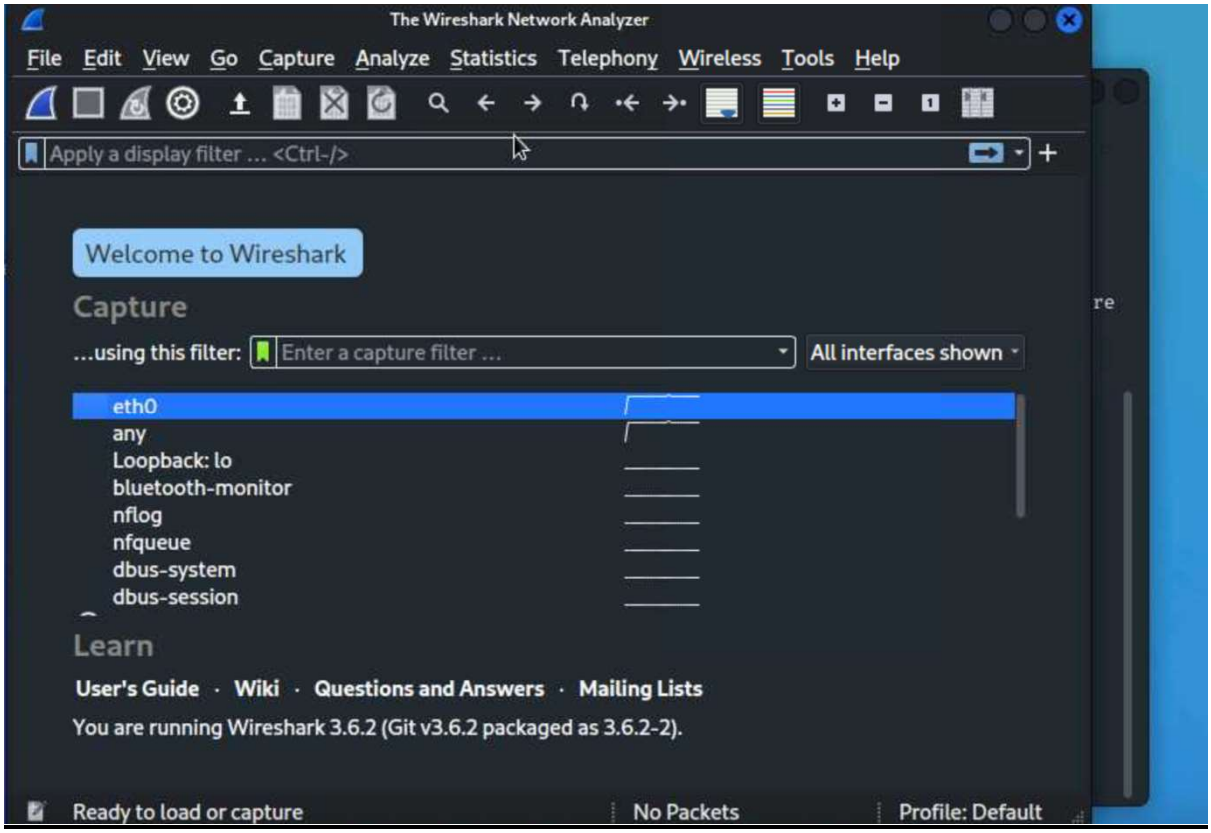


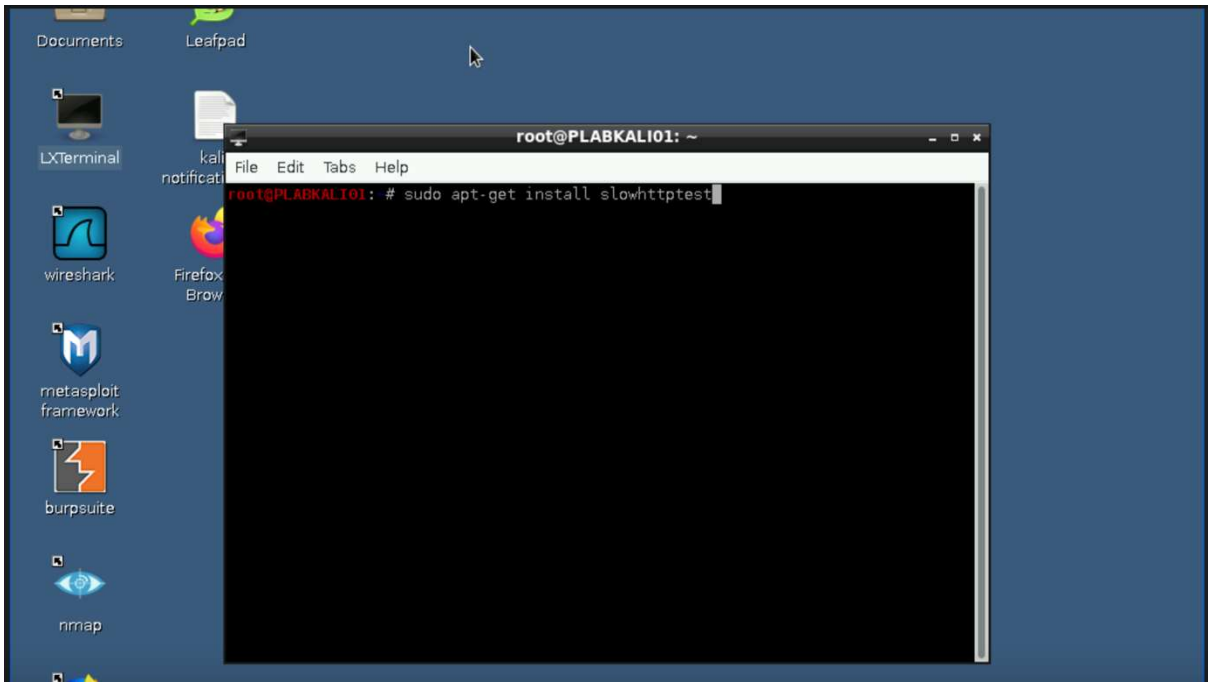


Capturing Network Traffic Using Wireshark

Choose the appropriate network interface eth0 that is connected to the network where the target web server resides.

- The XML bomb is designed to consume significant server resources, such as CPU cycles, memory, and network bandwidth.





Techniques can be used for DOS attack Hping3 and xml bomb

Analyse the network infrastructure to mitigate and the impact of DoS attacks, by adopting procedures including the firewalls, IDS/IPS and monitor network bandwidth limitations.

3.8 Tenet of cyber security in this vulnerability

This vulnerability goes against the principle of cybersecurity called "Availability." It's about ensuring that systems, data, and services are accessible and usable when needed by authorized users. When there's an XML bomb vulnerability, it disrupts this availability. It can cause a denial-of-service (DoS) situation where the server becomes unresponsive or very slow. This means legitimate users can't access the services they need, impacting their ability to do their tasks. Attackers exploit this vulnerability to disrupt the system, causing interruptions in services and preventing users from accessing resources. Fixing this vulnerability is crucial to maintain the availability of systems and ensure that users can access them without interruption.

Layer 2 – Network	Attackers can attack edge routers and firewalls with DoS attacks. If not configured properly, switches can be flooded with requests to overflow their CAM tables. Attackers also attempt to sniff network traffic./td>

3.9Scenario Assessment

The impact of this attack on our scenario can be significant. It disrupts the normal functioning of the web server hosting, making it unavailable or slow to respond. This affects the ability of legitimate users, such as employees or customers of the clothing company, to access the website and its services. It could lead to frustration among users who rely on the website for various tasks like browsing products, making purchases, or managing inventory. Additionally, if the website is unavailable for an extended period, it could result in financial losses for the company due to lost sales opportunities. Moreover, the company's reputation may suffer if customers experience difficulties accessing the website or completing transactions, potentially leading to a loss of trust and credibility. Overall, the impact of this attack could be detrimental to the company's operations, finances, and reputation.

3.10 Toprotect web services from DoS attack

To protect their web services against DoS attacks following measures be taken:

- Implement Rate Limiting to check number of request on the network.

- Use Web Application Firewalls (WAFs) for monitoring traffic.
- Enable DDoS Mitigation Services to filter malicious traffic.
- Regularly Update Software and Patches also reduce DoS attack.
- Monitor Network Traffic by implement IPS /IDS to observe traffic patterns.
- Implement CAPTCHA on web pages.

By implementing above mentioned measures we can minimize the DoS attack on the system.

Task 4: Laws and Ethics

4.1 Law and Ethics on unethical and Illegal activities as Pen Testers.

As a penetration testing assessment of Fashion&Trendz many issued related unethical and illegal activities which can be identified and their Impacts and practicing during penetration testing.

Unauthorized Access of Fashion&Trendz's systems without privileges breaches breach ethical standards. It also violate the legal framwork of Computer Misuse Act 1990, this act prohibits anyone to gain unauthorized access.

Data Manipulation includes tampering with or altering data within Fashion&Trendz's systems without consent constitutes unethical behaviour. This tempering of data or any part of data can compromise the integrity of data also violate data protection laws like the UK-GDPR.

Deception involved fake representation and engagedeceptive practices like social engineering attacks or sending phishing emails or trying to pretend for malicious purposes. These practices damage trust and also result a legal action by violate laws and frauds.

If attacker deliberately disrupting Fashion&Trendz's web application by DoSattacks or DDoS attack is also unethical and illegal. In the UK DoS attacks are prohibited under the Computer Misuse Act 1990 and can cause damage operations and financial losses of the businessFashion&Trendz.

Invading privacy of customers or employees or any other information related to Fashion&Trendz'swithout consent and keeping is unethical and illegal. This policy violation can lead result in legal consequences and damage the reputation of the penetration testing firm or any other personnel involving invading of privacy.

4.2 Consideration of National and International laws as a penetration tester in UK based company.

Laws and Regulations in the UK

There are four critical legislations that govern cybersecurity, dataprivacy and data protection in the UK

- Data Protection Act 2018
- UK General Data Protection Regulation (UK-GDPR)
- Network and Information Security Regulations 2018 (NIS Regulations)
- Computer Misuse Act 1990

As a penetration tester operating in the United Kingdom, it is very important to follow national and international laws governing cybersecurity and data protection while based in the UK. By understanding and compliance with these legal frameworks, as a penetration testersit is to be ensuredthat conduct activities ethical and mitigate legal risks within legal framework.

The foundation of data protection legislation in the UK is the Data Protection Act 2018 (DPA), this law governs the processing and protection of personal data. Penetration tester must make sure that any personal data accessed or processed during assessments is handled in accordance with the law in the UK. Proper This also having a proper consent to be obtained for security purpose against unauthorised access and follow the rules and regulations.

As Fashion&Trendz is a medium-sized business who sells clothing to its customer, it operates a web application where buying transaction carried out by customers online. Their web application collects information and data from customers and store in their database including names, addresses, email addresses, sizing information and payment details. Staff also access database by logging into accounts according to their roles and database also had staff information in the system. They also manage the system for inventory, update product listings and process orders. The company'smust have commitment to compliance with the DPA ensures that personal data should be securely processed with lawfulness and transparently.

General Data Protection Regulation (GDPR): Ensuring Data Protection in Penetration Testing

The General Data Protection Regulation (GDPR) stands as a foundation of data protection legislation in the European Union (EU) including the United Kingdom. As penetration testers engaged in the assessment the security of Fashion&Trendz's web application compliance with the GDPR is mandatory that ensuring that protection of personal data processed by the company.

The GDPR imposes several key obligations on organizations handling personal data, which directly influence our penetration testing activities:

Lawfulness, Fairness and Transparency in data handling and make sure personal data must be kept or processed or kept lawfully, fairly and transparently with the explicitly consent of Fashion&Trendz.

Purpose Limitation and Data Minimization during the handling of personal data and use it for legitimate purposes only. Adhere the principal minimization and to ensuring access that data to fulfil our objectives within law framework.

Data Security and Integrity involves step to ensure that security and integrity of personal data, prioritize data security by employing encryption, access controls, and other security measures to protect sensitive information during our assessments.

U2197407 George David Dandoczi Development Plan

ITEM	DETAILS		
Student ID	2197407		
Student Name	George David Dandoczi		
Course	BSc (Hons) Computer Science	BSc (Hons) Computing for Business	BSc (Hons) Cyber Security & Networks
Post UEL Email	georgedavid.dandoczi@gmal.com		
LinkedIn Profile (URL)	https://www.linkedin.com/in/george-dandoczi-6033a6159/?originalSubdomain=uk		
Evidence of completing careers zone pathway			
Evidence of engagement with BCS Special Interest Groups	I have made an account and will pay subscription to become an official member. Assisted workshop talk at UEL in regards to BCS.		
Post-Graduation Plans (e.g., further study, skills development, job applications etc.)	I am interested in two domains entailing my programme. First is fintech merely that my dissertation evolved around threats and vulnerabilities in the banking system. I have found on Santander banking career undergraduate prospects. Secondly I am planning to obtain a certificate fromEC-Council either in a data protection field or Business Continuity.		
UEL PG Computing Courses	Please place a tick against any of the following UEL MSc courses you might be interested in		
	☐MSc Computer Science	☐MSc Artificial Intelligence	
	☐MSc Big Data Technologies	☐MSc Information Security & Digital Forensics	
	☐MSc Cloud Computing	☐MSc Blockchain & Financial Technologies	
	☐MSc Digital Education	☐Other (please state)	

References:

Alazab, A., Alazab, M., Abawajy, J. and Hobbs, M., 2011, November. Web application protection against SQL injection attack. In Proceedings of the 7th international conference on information technology and applications (pp. 1-7).

Aljawarneh, S., Alkhateeb, F. and Maghayreh, E.A., 2010. A semantic data validation service for web applications. Journal of theoretical and applied electronic commerce research, 5(1), pp.39-55.

Data protection act 2018 Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed: 29 March 2024).

OWASP, 2021a. Cross Site Scripting (XSS). OWASP. Available at: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery [Accessed 19April 2024].

OWASP, 2021b. SQL Injection. OWASP. Available at: https://owasp.org/www-community/attacks/SQL_Injection [Accessed 28 March 2024].

Sharp, K. (2023). The importance of OSINT in cyber security. [online] Evalian®. Available at: https://evalian.co.uk/the-importance-of-osint/. (Accessed 10-April-2024).

What is GDPR, the EU's new Data Protection Law? (2023) GDPR.eu. Available at: https://gdpr.eu/what-is-gdpr (Accessed: 03April 2024).