Table of Contents

1 Getting started

Here is set up 2 machines one target machine Kali Linux and is metasploitable Machine consisting DVWA web application which contains vulnerabilities so I will use kali machine to attack metasplotiable on portal DVWA web application

2 Building your Case Study:

In this case, "Creative Spark Digital" has developed DVWA emergency program as one way of keeping security training program inside as well as doing vulnerability testing. DVWA portlet, is distributed internally in a protected environment of the company. It can only be accessed via the company's intranet is thus used only by the agency's IT security team and employees attending training sessions. This configuration is meant to ensure that the trainees get necessary skills on spotting, targeting, and handling such threats in web apps.

The portal serves multiple functions:

Training Tool: It is used to carry out the practical part of the training of new and existing employees to teach a few different types of web security threats like SQL injection, XSS, and CSRF. Through simulation that can be performed in a safe environment, employees, for example, practice attacks, grasp the inner mechanism of exploits and how to protect against them.

Security Testing: The DVWA is also utilized for testing aspiring security advancements that are moving to be subsequently added to agency's official sites. IT employment employs it to emulate so-called "attacks" and watch defenses how they work in various circumstances.

Through offering their technical employees as well as the company secure web applications, "Creative Spark Digital" integrates DVWA into their security practice. The company thereby implicitly increases the security capabilities of the employees and the security posture of the web applications. By taking into account the possibility of threats and preventing them before they happen, the organization provides high level of security, thus securing not only clients' data, but also intellectual assets.

Task 1: Report Requirement for your Client

a. Information Gathering

1.1 OSINT Activities: Identify and explain how you have used three examples of Open-Source Intelligence (OSINT) investigation activities to carry out your test

For an OSINT based exercise "Creative Spark Digital Security Testing," effectively implementing this strategy is key to cybersecurity readiness. Initially, the Domain and Network Information Gathering is nearly akin to a simulator, which can be realized using WHOIS and nmap to draw the digital footprint of the organization, which is in fact the target for cyber-attack scenarios training. On the other hand, the process of the Public Code Repositories Analysis consists of scanning platforms like GitHub allowing the security personnel to discover accidental leaks of sensitive info and as a result the expertise of finding and stopping breaches is refined. Moreover, Social Media Analysis monitors various platforms such as LinkedIn and Twitter to collect data regarding public human vulnerabilities, and suggest any company's sensitive information that is obtainable. The whole OSINT cycle combined increases the assessment institution's resistance to and readiness to counter the cyber threats.

1.2 Research and evaluate how OSINT can be effective and explain why it is essential as one of the first activities carried out by penetration testers.

Open-Source Intelligence (OSINT) is a crucial tool for the Penetration Testers, particularly in the beginning of the cyber security assessment projects for the companies like "Creative Spark Digital". First OSINT can give wise reconnaissance to the tester via searching the target systems so no one will detect monitored organizations. Subsequently, use of compiled information on these entities by searching their domain names, server IPs, employee details and some other from WHOIS databases, professional networks and social platforms is included too. It is with such information that you can tell the probability of an occurrence of transferal of the system to an unsecured state such as having outdated software at weak points on the network infrastructure.

Also, in this context OSINT is useful in building social engineering techniques that capitalize on the behavioral and philosophical dynamics inside a corporation and should thus make the users more susceptible to spoofs such as phishing. In general, the OSINT-enriched information landscape complicates the strategic planning of penetration tests by implementing approach customization based on the technologies and security protocols deployed by the target organization.

Fundamentally, OSINT is cheap because it saves resources needed to collect data and lowers the degree of risks that might be associated with the issue of confidentiality or ethics since it relies on publically accessible information. Such initial gathering of intelligence may prove to be the basis on which the risks and dangers that the company is exposed to can be judged and corresponding defensive plans written up. Penetration testing is essential for the business like "Creative Spark Digital," draw on the OSINT heavily as its initial stage not only defines the scope but also determines the direction of the next security testing endeavors.

1.3 Scenario Assessment: according to your scenario, describe how critical or dangerous are the information you obtained.

In this scenario, the information gathered by "Creative Spark Digital" using OSINT in security assessment would invariably be of high importance and if in unregulated hands could obviously be harmful to the company. Infiltrating into the employee management system, hackers can access employees' information such as roles, contact details, and even personal preferences which might in turn be utilized in executing proficient phishing campaigns. These attacks may be specifically chosen to be targeted at individual employees; hence, the capability of them to exploit the systems is probable and thus become successful.

The specialized technical information on the company's internal IT infrastructure requirements, for instance the network architecture, IP addresses or software versions, also requires special attention and may contain serious danger. This is information that hackers use to locate weaknesses in the defenses, hence, berthing unauthorized entry and simulation of threats and malicious tampering with the system. Eg, the knowledge of a deprecated software component can give the attacker a hint to exploit the known exploits working for the versions against that component thus leading to a severe security breach.

Communication of publicly accessible data about internal projects and technologies can also result in precision attacks that, in turn, aim at the disruption of operations and the stealing of secret methods and projects data. The same can be said about internal information such the company's processes and culture, which can be also exploited by crafting extremely convincing spear-phishing attacks that mimic authentic correspondence. The comprehensive possibility for such intel may again be used in virtual harms to disturbed the safety of digital objects of organization as well as its financial standing and status. Therefore, a secure system like "Creative Spark Digital", which is responsible for implementing and sustaining the Internet of Things (IoT), should be more careful in managing their digital footprint and should develop strong security measures to prevent these possible threats.

b. Reconnaissance

1.4 Demonstrate some of the information you obtained by testing the web applications

Using Nmap, Nikto, ping tool to verify the vulnerabilities

In the process of recon, one commonly uses tools like Nmap, Nikto, and ping among others to probe for vulnerabilities in web apps. Nmap for TCP/IP ports scanning, Nikto to find out common web server vulnerabilities and ping to check for host availability are the examples of command line tools. These tools enable gaining important information about areas of possible security flaws and weaknesses, which can then be used when assessing security risks.

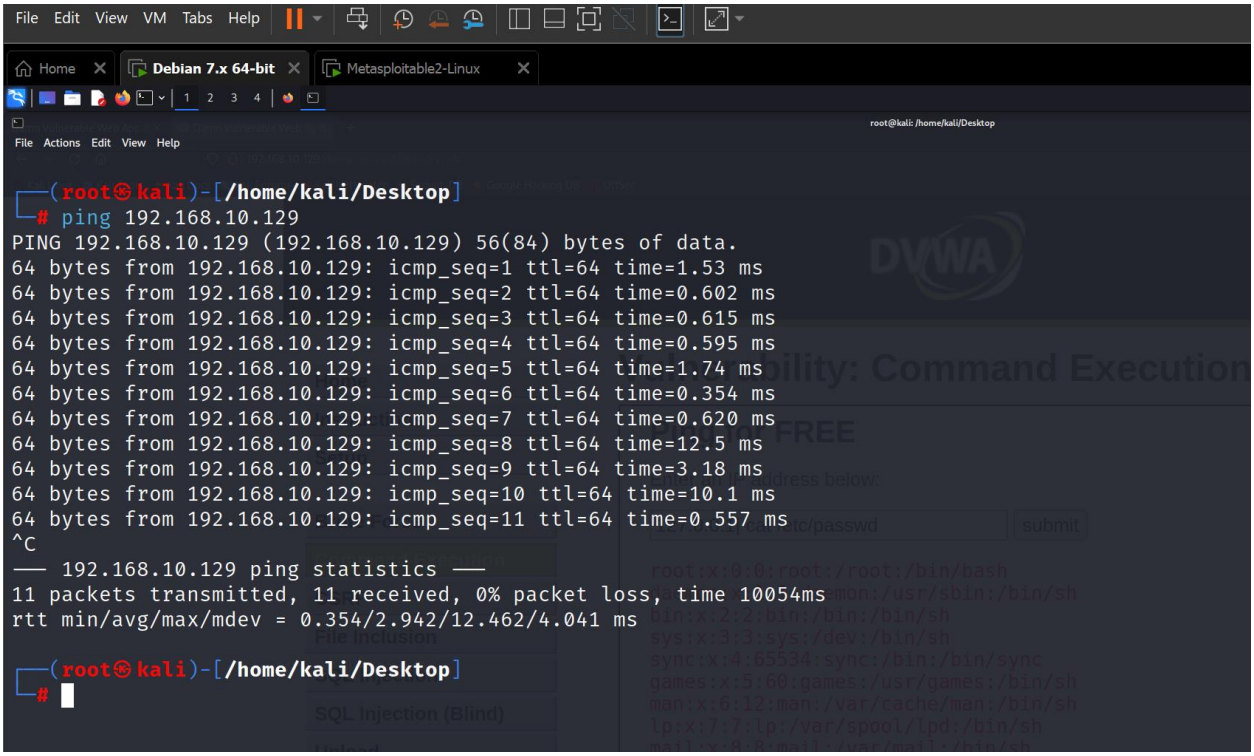


Figure-1 Ping connectivity check

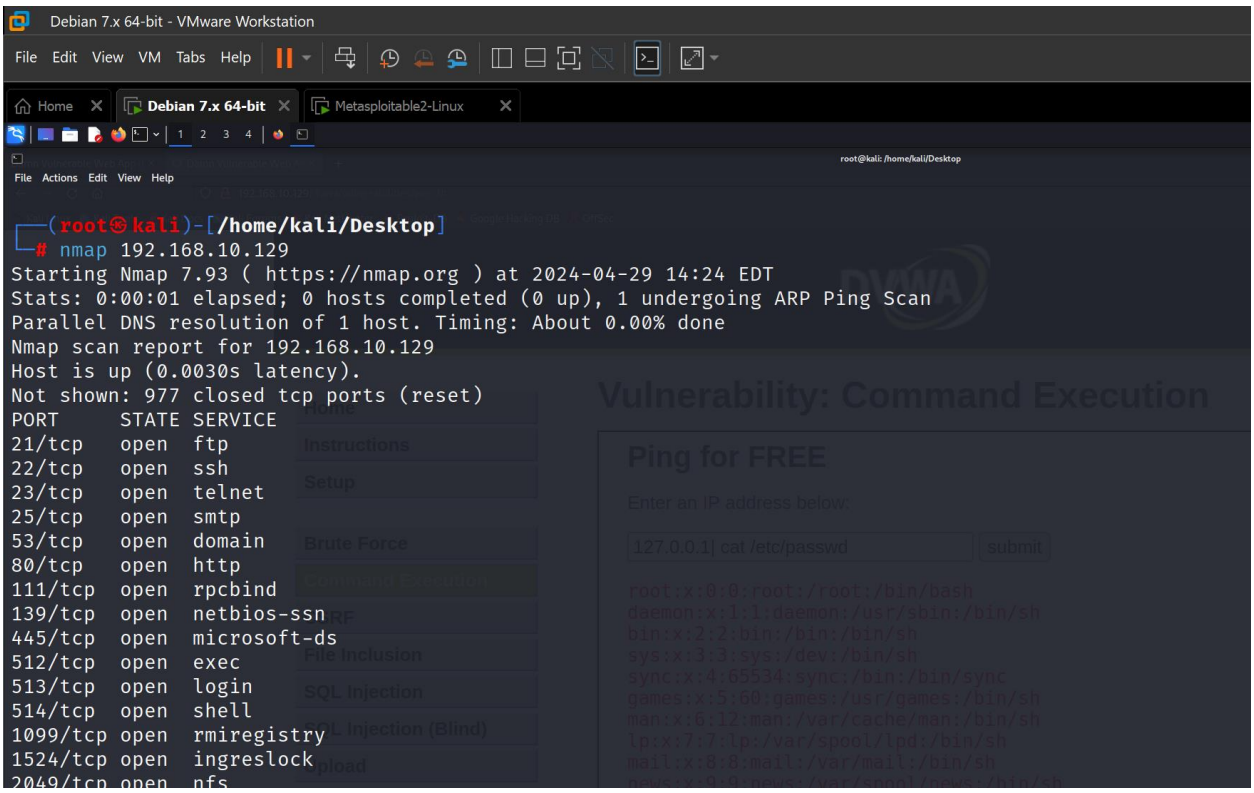


Figure-2 Basic Nmap scan

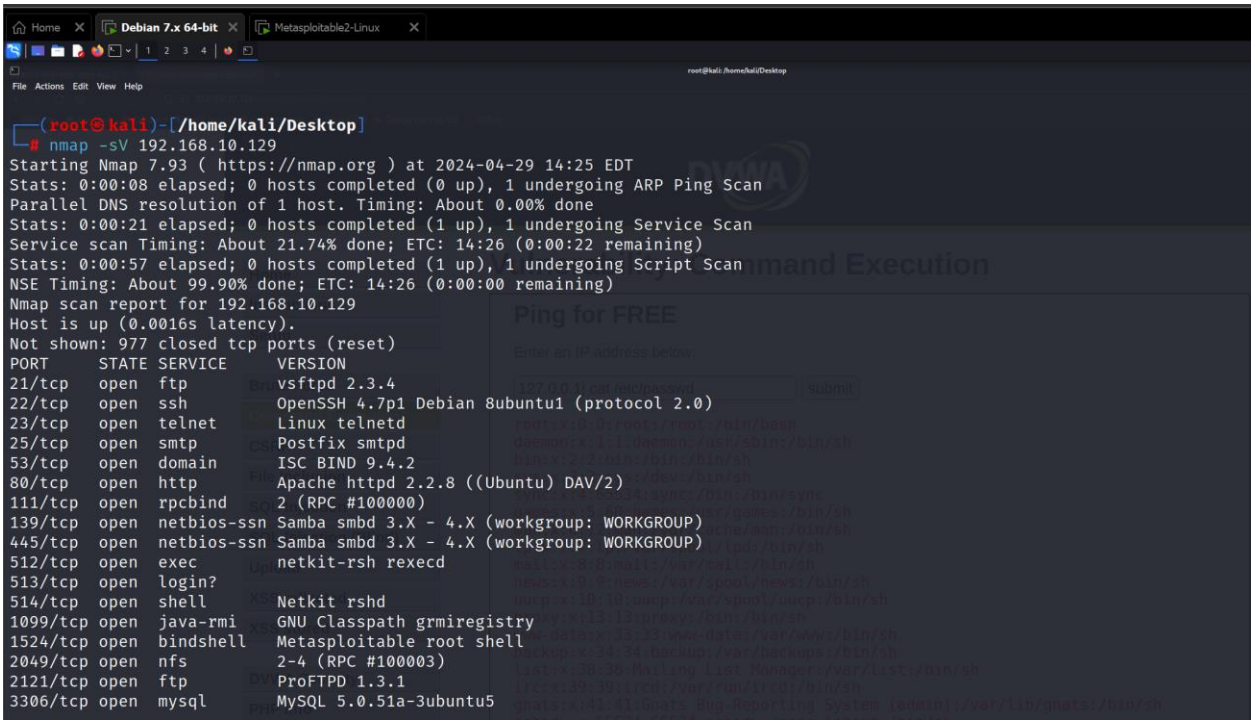


Figure-3 Detailed scan

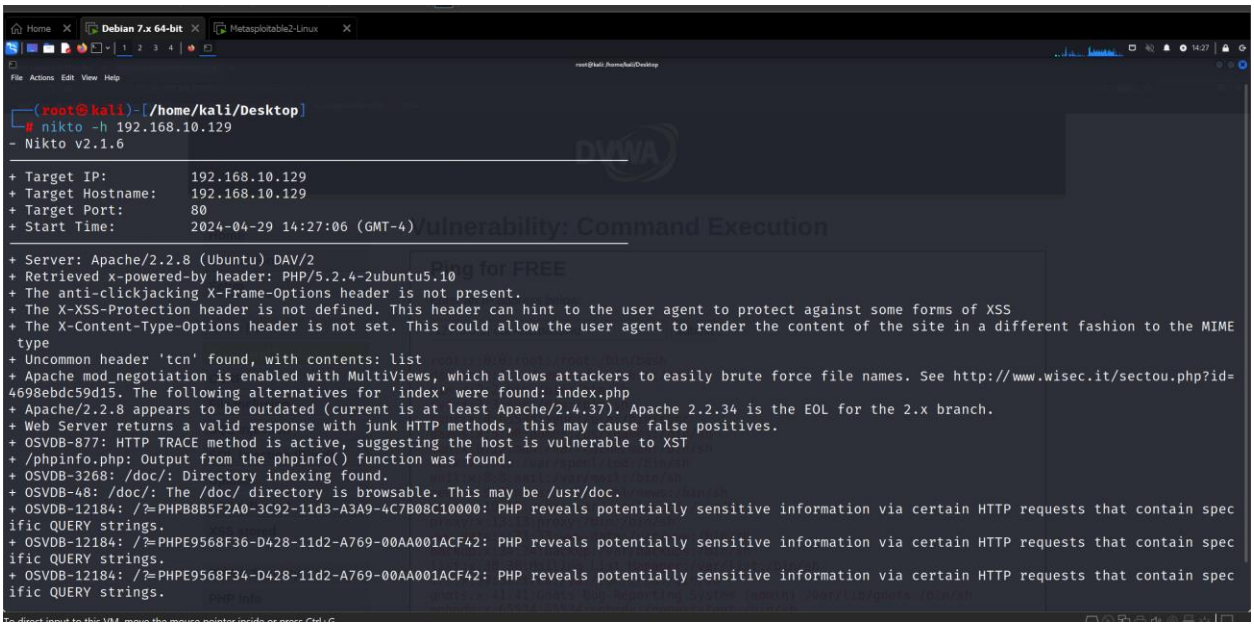


Figure-4 Nikto scan

1.5 Scenario Assessment: explain how the information obtained by testing the web applications can be used at a later stage to exploit company's web services, and give an example of some information that can be relevant to your scenario.

The data gathered while testing web applications in the reconnaissance step can in later phases be used to exploit a business organization's web services. For example, checking with Nmap and Nikto scans can

reveal the security of each open port and the possible presence of complexity. This data also can be utilized for the creation of the attacks that could eventually help to get unauthorized access to the systems of the company via the use of specific weaknesses of the servers, networks, or services.

1.6 Briefly explain the implementation courses of action (controls) to minimize the threats to the findings in the reconnaissance phase.

To handle or neutralize these risks, strengthening security mechanisms will be necessary. First of all, among the most important prevention measures is network segmentation which is aimed at isolating the critical systems from potential adversaries, restricting their access. Besides that, routine vulnerability detection and patch management bring prompt fixes to the detected vulnerabilities which enhance the security fortress considerably. The last, but not the least, enforcing strict access controls, incorporating the role-based access and strong authentication methodology, is the key to avoid the cases of unauthorized users.

Task 2: Server-Side Exploits

a. Data Tampering

2.1 Identify if the application is vulnerable to data tampering and exploit.

From searching the vulnerability scan on the target IP we can verify the machine can be vulnerable to attacks. using NMAP and nikto tools to search the version number of the service running on the server. Upon scanning we can confirm the service is vulnerable and data can be tempered. The exploitable NMAP and Nikto vulnerability scans confirm that the application services suffer from data manipulation vulnerability. Capitalizing on the system's Achilles heels, we can now forge ahead with our plan of action and create destructive requests or alter messy system parameters in order to manipulate the data maliciously.

2.2 Briefly explain data tampering vulnerability and explain which tenet of cyber vulnerability it Violates.

One type of common data vulnerability is data tampering in which unauthorized data alterations are made such as malicious actors modifying, deleting, or insertion of false data into systems. Through this breach the key principles of cyber integrity which assume that data shouldn't be modified or wiped out at any lifecycle stage should be respected.

2.3 Scenario Assessment: Describe the vulnerable information for data tampering that attackers could obtain when this activity is carried out.

Within data tampering like this, attackers could get through the private information like records of transactions, personal identity or secret businesses information. Using this type of information, criminals can achieve a robust result, which includes damage such as financial losses, identity thefts, and reputational injuries. This gap damages the entire system and makes it unsafe for the purpose that is supposed to guarantee the data always remains unchanged and refers to its integrity, the fundamental property in the production of information or data life cycle.

b. SQL Injection

2.4 Identify if the application is vulnerable to SQL injection and exploit

Enumeration is another important step during reconnaissance, hence use of tools such as Nmap, Nikto, and ping to disclose the loopholes in web apps. Nmap is one of the popular scanning tools mainly used for TCP/IP ports scanning, Nikto for detecting widely used web server flaws, and ping for avoiding host unavailability. They will be in the form of command-line language and is expected to output information on security flaws and vulnerabilities that are the crucial factor in computing for security risks.

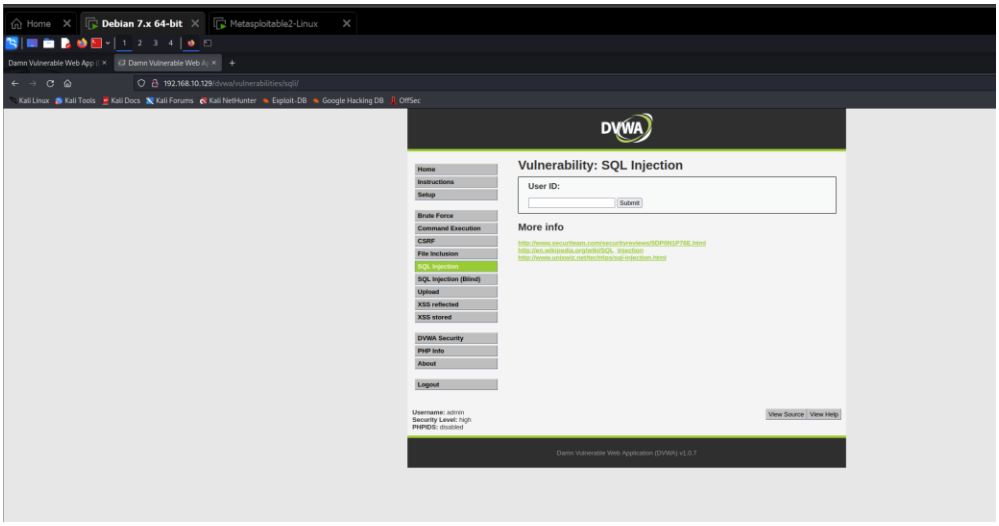


Figure-5 Starting application Webpage.

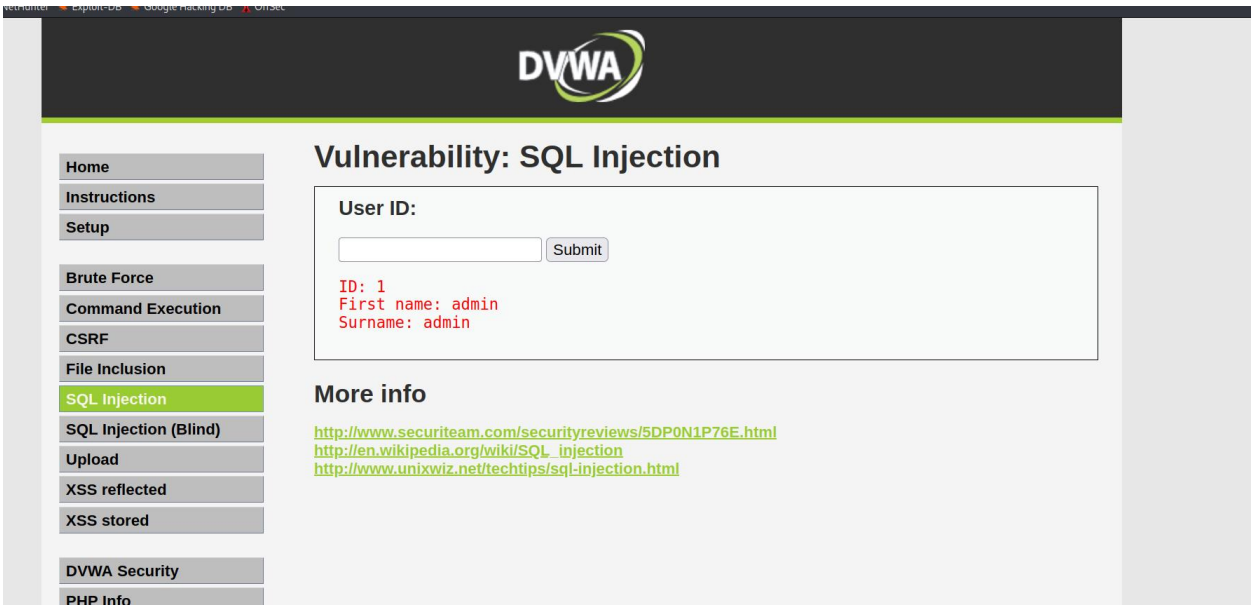


Figure-6 Normal functionality

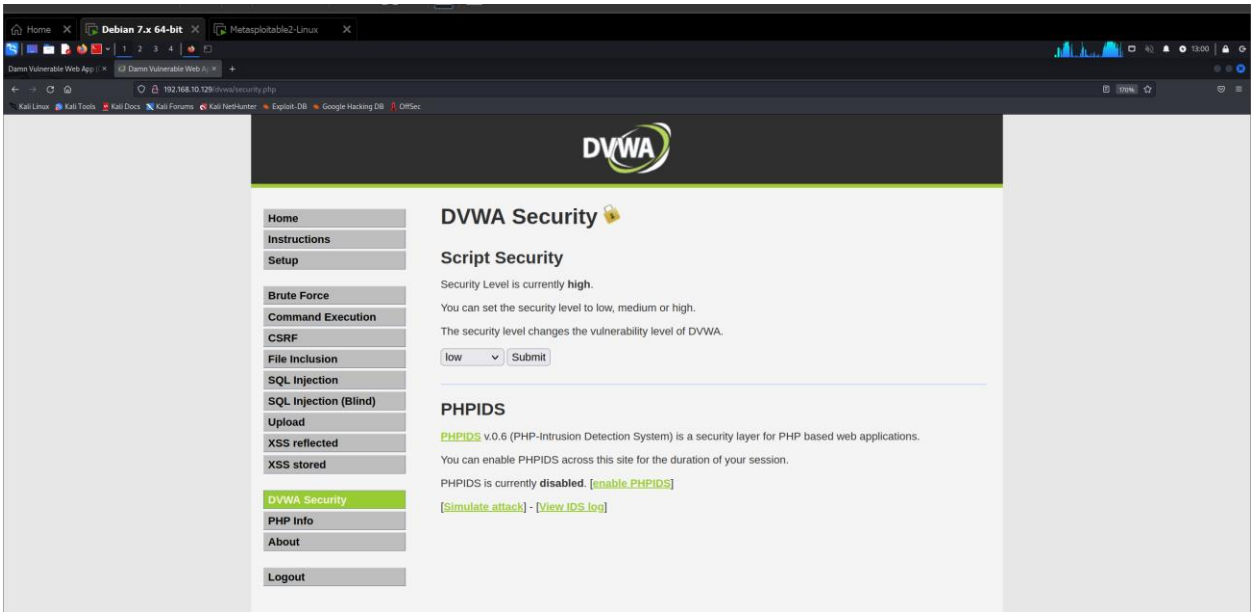


Figure-7 Security level low for testing

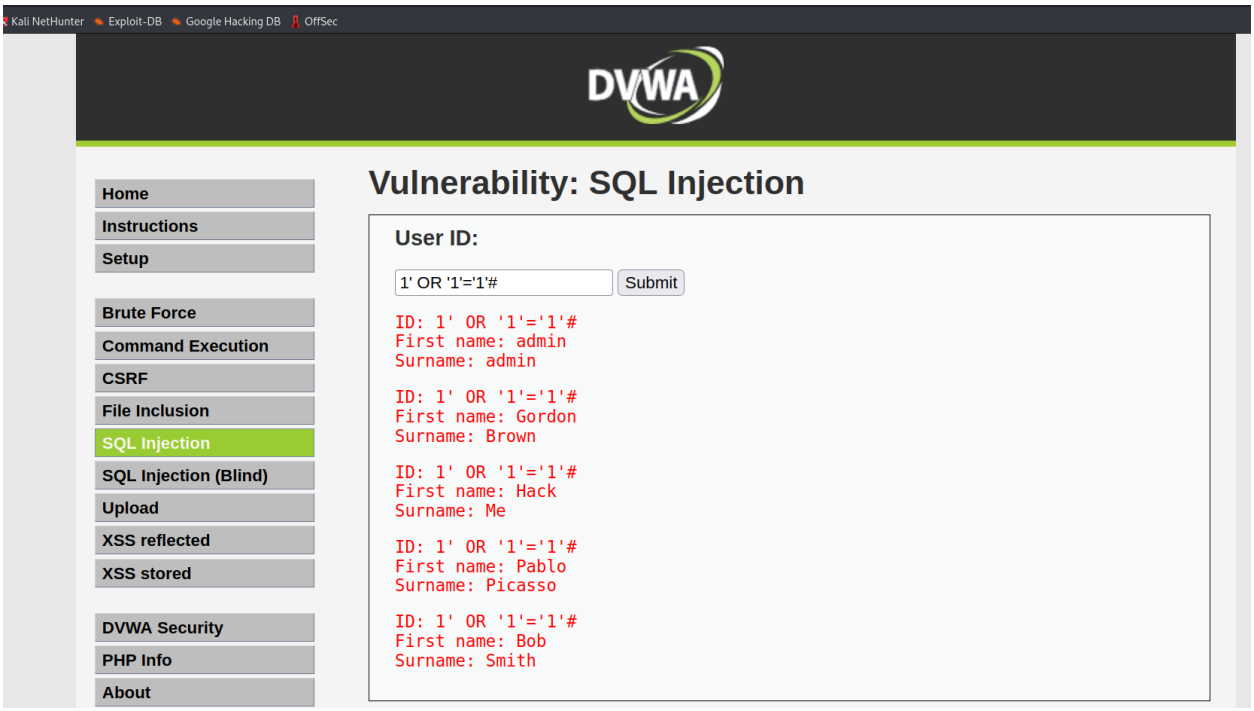


Figure-8 Trying input 1' OR '1'='1'#

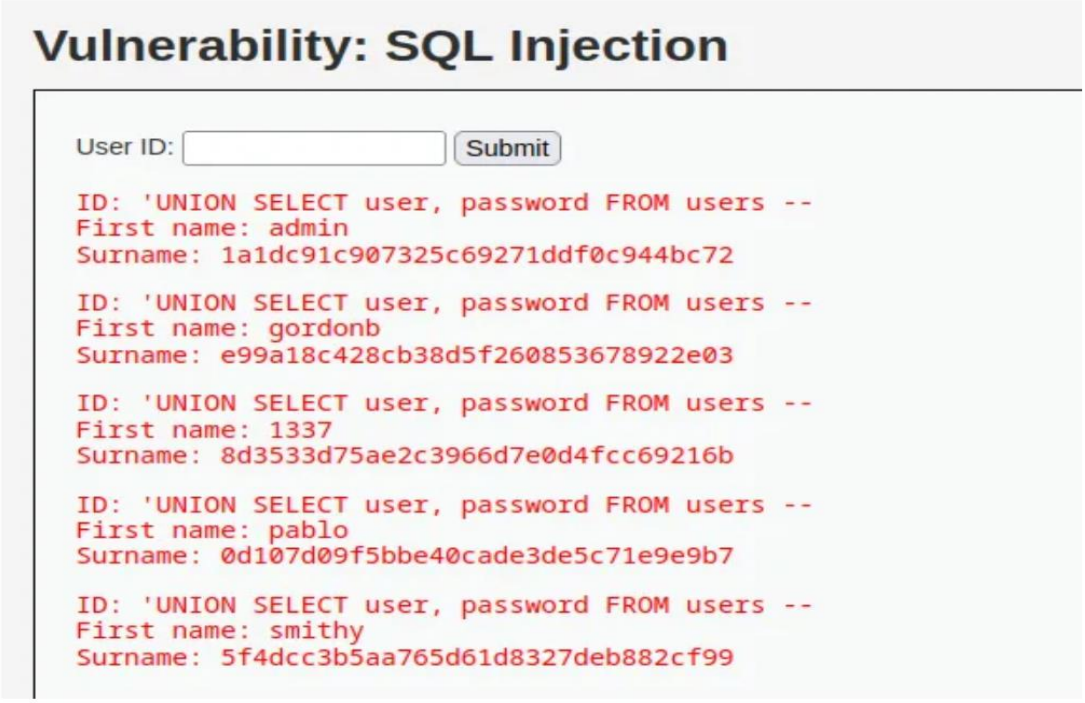


Figure-9 'UNION SELECT user, password FROM users –

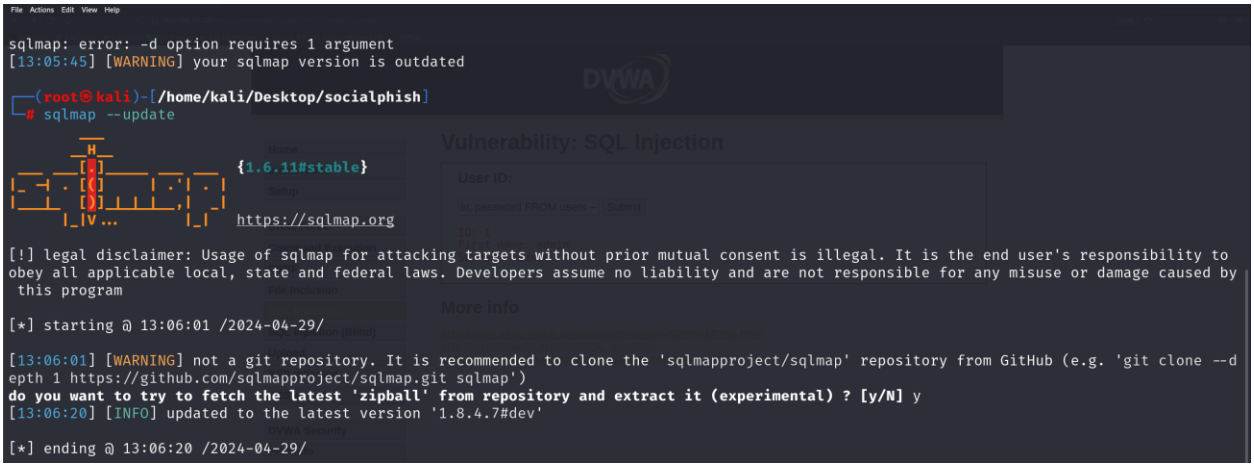


Figure-10 SQLmap to automate this

Figure-11 Detected strings.

2.5 Briefly explain SQL injection vulnerability and explain which tenet of cyber security this vulnerability exploits.

SQL injection is the security flaw that is exploited when hacker tries to change the SQL queries in through web application. This allow attackers to inject malicious input code that cause database to response with extra or valuable data that can be accessed by attackers. This vulnerability exploits the tenet of "data confidentiality" in security. By exploiting SQL injection, hackers can bypass access controls and view sensitive data stored in a database, compromising its confidentiality.

2.6 Scenario Assessment: Describe the information that attackers could obtain when this activity is carried, and how dangerous are they for your scenario

In this scenario of SQL injection attack, we have successfully conducted on web application attack that attackers could obtain a range of sensitive information from the targeted database. Using this vulnerability attacker can look around database system and look for sensitive data that is not by default be shown to normal users. As one perceives this, statistics leak will display all their personal details hence. Their purchase typical patterns are likely to be affected. This will happen, let's say, in the supermarket where they buy food and drinks, bank transactions of money sent as loses (as well) to the heart of the organization which is related to business transactions. Ethical dilemma, as such, applies to the authenticity of actors which face a burden like shading with the accuracy of the feedback, on the other hand, it is the path of using some fraudulent features as managing services features for operation disruption and information changes. Although murdered peoples may wield this infection like an instrument for their cruel plans, they can also easily apply it to the spread of the virus itself and the whole infrastructure of medical systems that should fight the infection

2.7 Briefly explain how to protect the company's database against SQL injection

SQL injections are one of the major types of vulnerabilities in web application security. Hence, validating and sanitizing the user inputs efficiently is needed to prevent SQL injection. The use of prepared statements and stored procedures helps a lot in improving the existing security measures in place by moving the SQL based logic from the user input section. As a plus, carrying out certain activities, like limiting user privileges, keeping all the systems up-to-date to have the latest software, and deploying a web application firewall greatly supports the web application in order to avoid being attacked. Integrating robust error handling and logging mechanisms ensures swift detection and response to any suspicious activity, bolstering overall database security.

The company can protect itself from the SQL injection attack by implementing various security controls

c. OWASP Vulnerable machine contains several other exploitable vulnerabilities.

2.8 Identify two other vulnerabilities that you identified in the vulnerable machine

1- XSS implies the malicious script injection into the target website, the data from which may provide an attacker with an unconditional access control of the website. Suppose a website will provide a non-guarded input data field like a comment box, username field, and email address field. Then the person who wants to attack others, he/she can inject malicious code script in the data like malicious script code.

Vulnerability: Reflected Cross Site Scripting (XSS):

XSS injection is an indeed a weakness that were discussed and proposed by Open Web Application Security Project. XSS is one security weakness that enables one to inject any destructive codes on a web page that is seen by other users. These may be able to run in the context of the browser of the user to steal sensitive information, to hijack the session of the user, or to perform other bad actions.

Reflected Cross-Site Scripting (XSS) primarily violates the principle of integrity in cybersecurity.

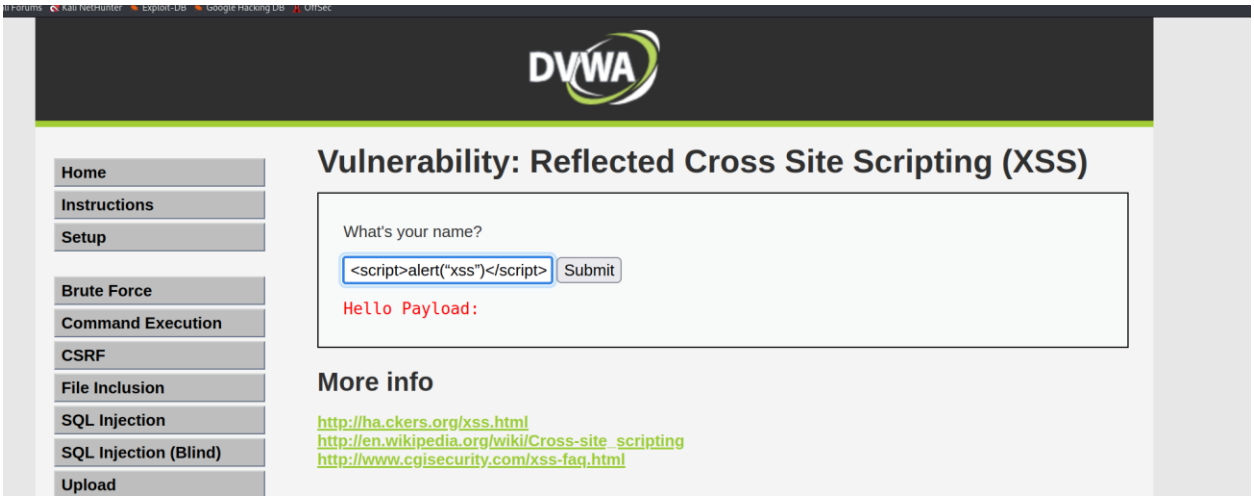


Figure-12 Payload: <script>alert("xss")</script>

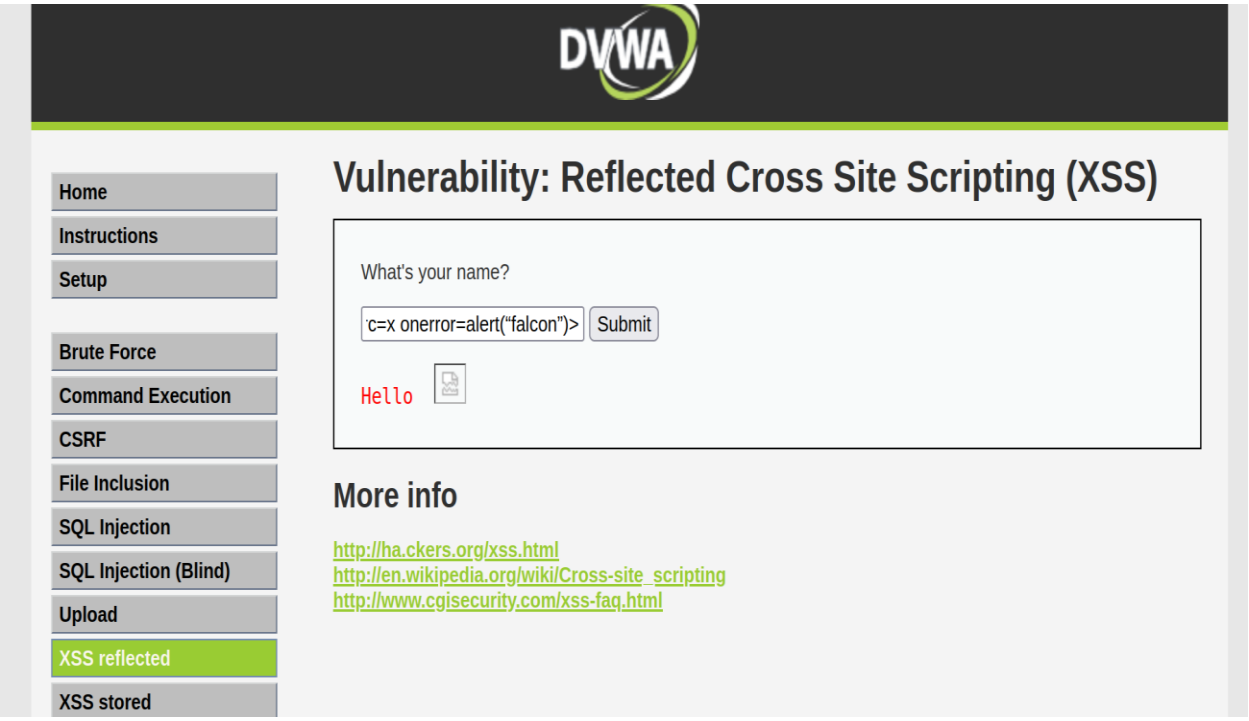


Figure-12 <img src=x onerror=alert("falcon")>

Vulnerability: Command Execution

Command execution vulnerability, as outlined by OWASP (Open Web Application Security Project), is a critical security flaw that allows an attacker to execute commands on a target system. This vulnerability

typically cause when an Web application accepts user input that includes shell commands or code, which is then executed by the system without appropriate validation or sanitization.
A command execution vulnerability primarily violates the principle of integrity in cybersecurity

Figure 13 127.0.0.1; ls -la /root

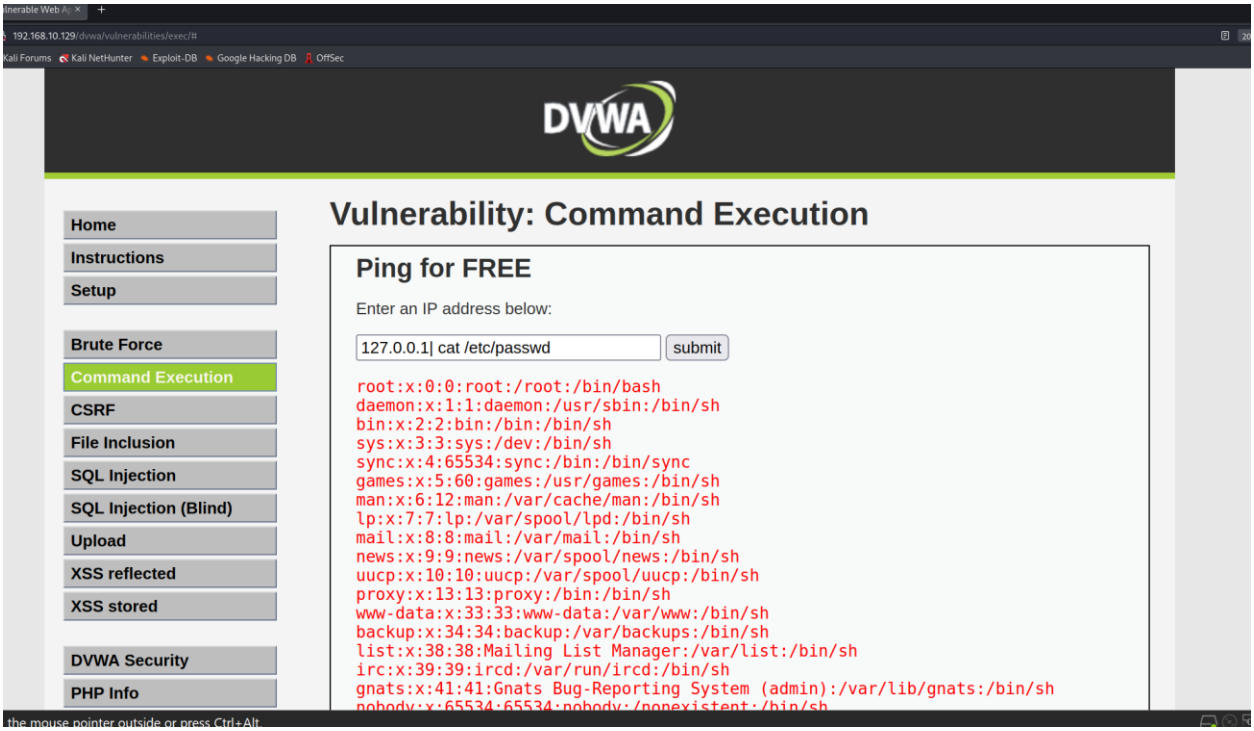


Figure-14 127.0.0.1| cat /etc/passwd

2.9 Scenario Assessment: Investigate and describe the threats of the exploitable vulnerabilities

identified and explain which cyber security tenet these vulnerabilities violate.

Vulnerabilities XSS and Command Execution, as indicated, represent a matter of concern to the company through its database security. XSS gives attackers a way of inserting malicious scripts into the website prejudicially, affecting the access to the sessions of the users and stealing their sensitive information. Users' integrity of privacy may also be violated. Likewise, the vulnerability of Command Execution allows attackers to execute arbitrary commands onto the victim computer which may be unfairly used resulting in data manipulation, unauthorized access and/or system compromise, again opposite to the principle of integrity. Therefore, this damage must elicit the implementation of concrete measures aimed at reducing the threats to the system confidentiality, the integrity of data, and the general system security as a whole.

Task 3: Client-Side Exploits

a. 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.

Man in the Middle attack is the attack in which attacker sits between the channel and intercepts the traffic for critical information. For this we will use tool called Ettercap that sends the arp requests to all hosts and intercepts the traffic from the network devices.

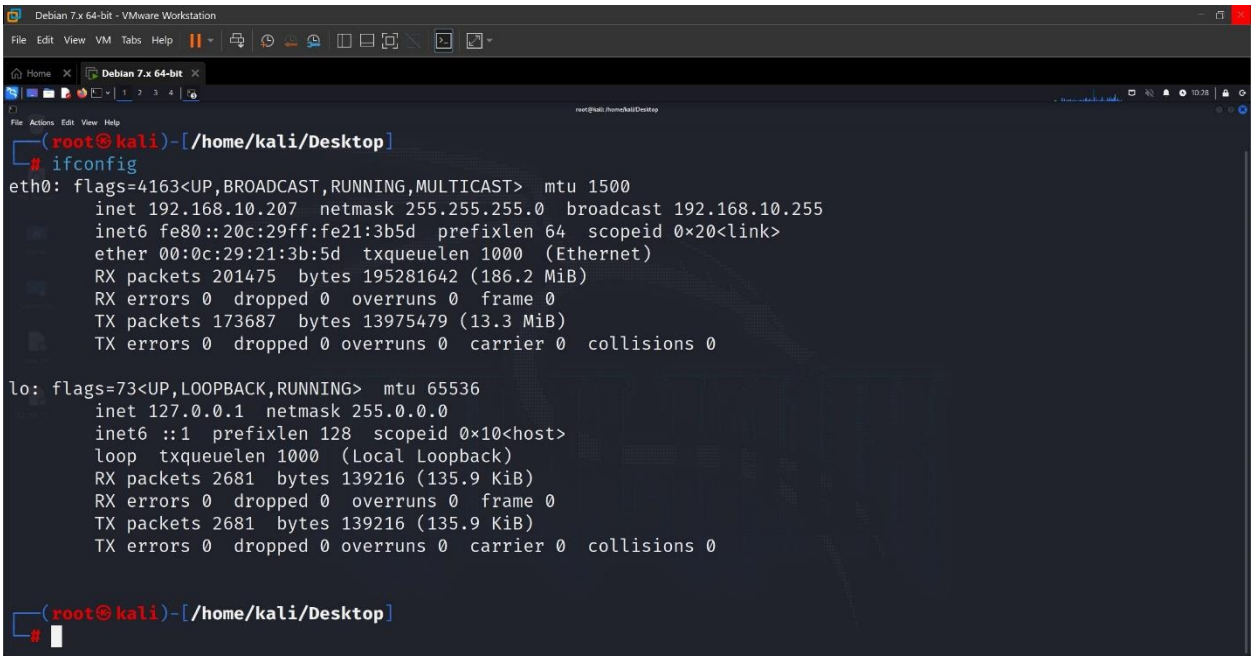


Figure-15 Kali Linux up.

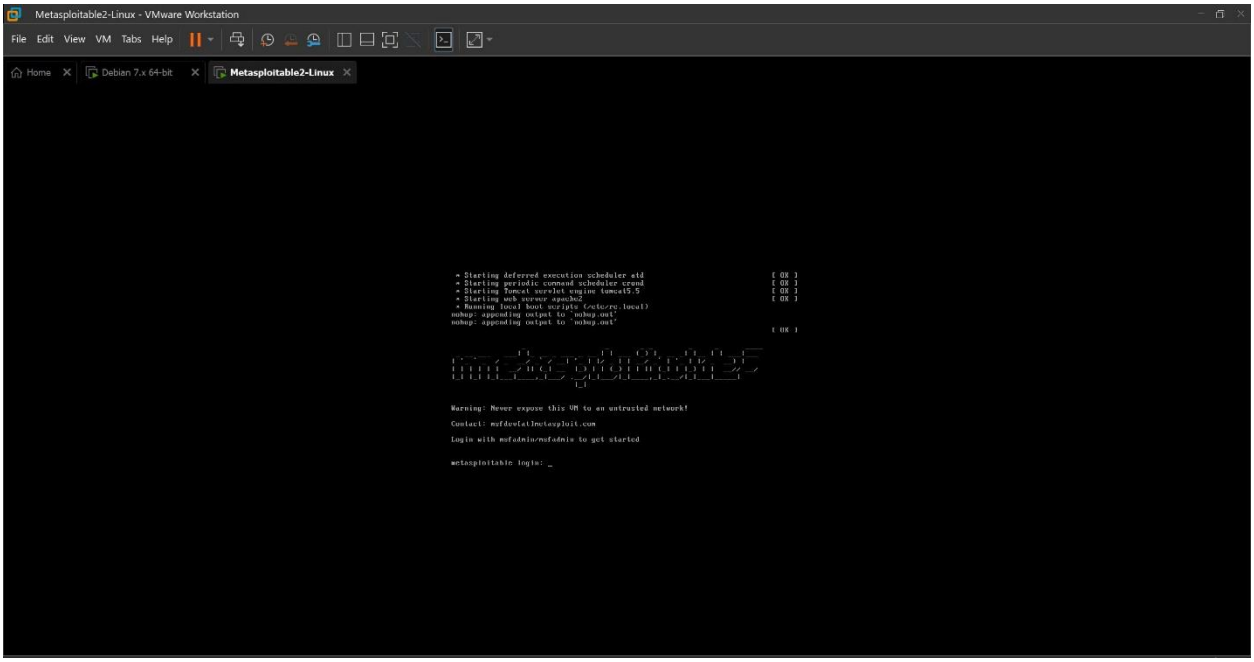


Figure-16 Metasplotable machine up.

Figure-17 Ettercap for attack.

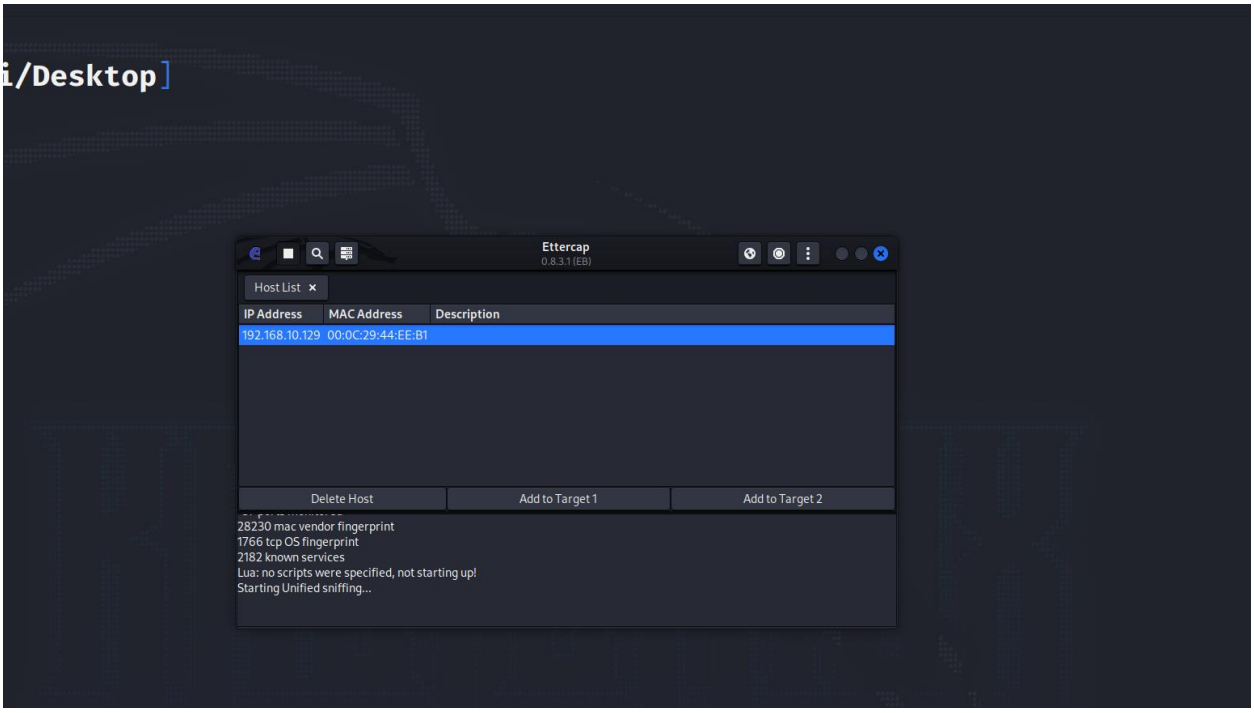


Figure-18 Host added

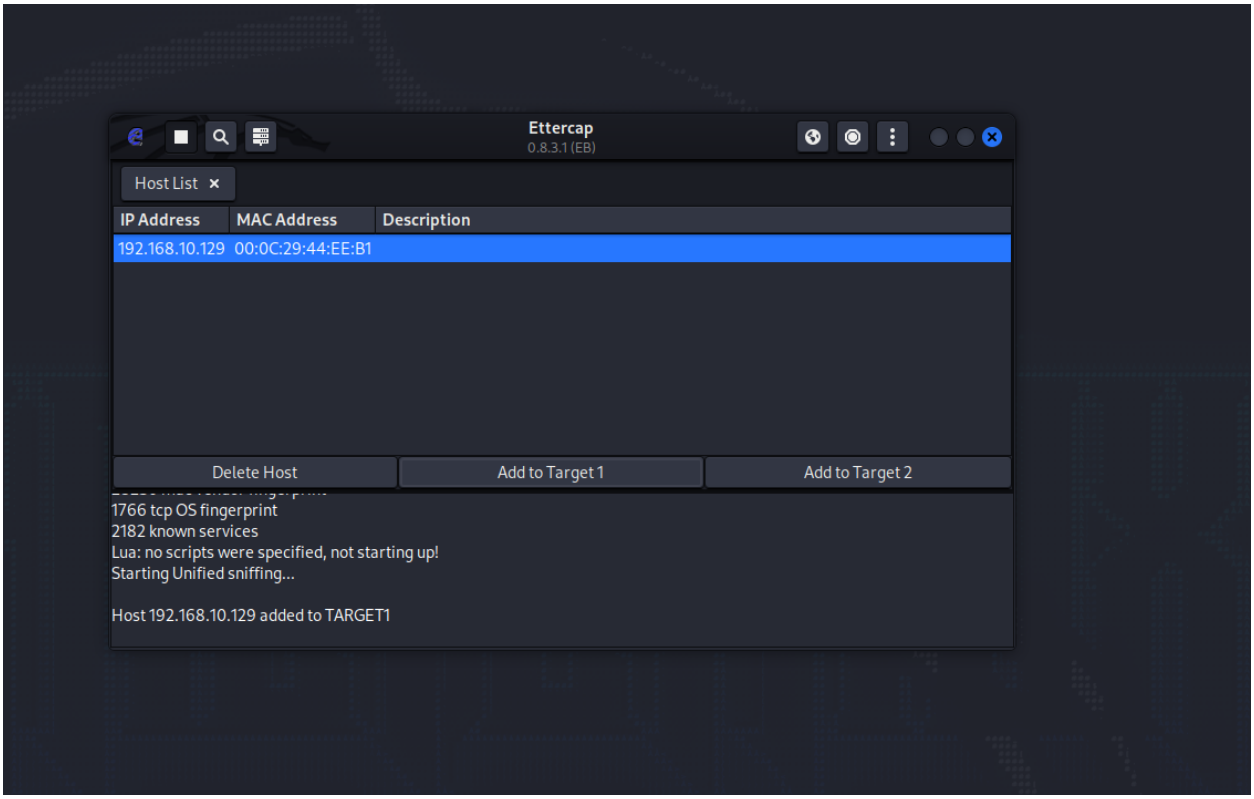


Figure-19 Host added to target.

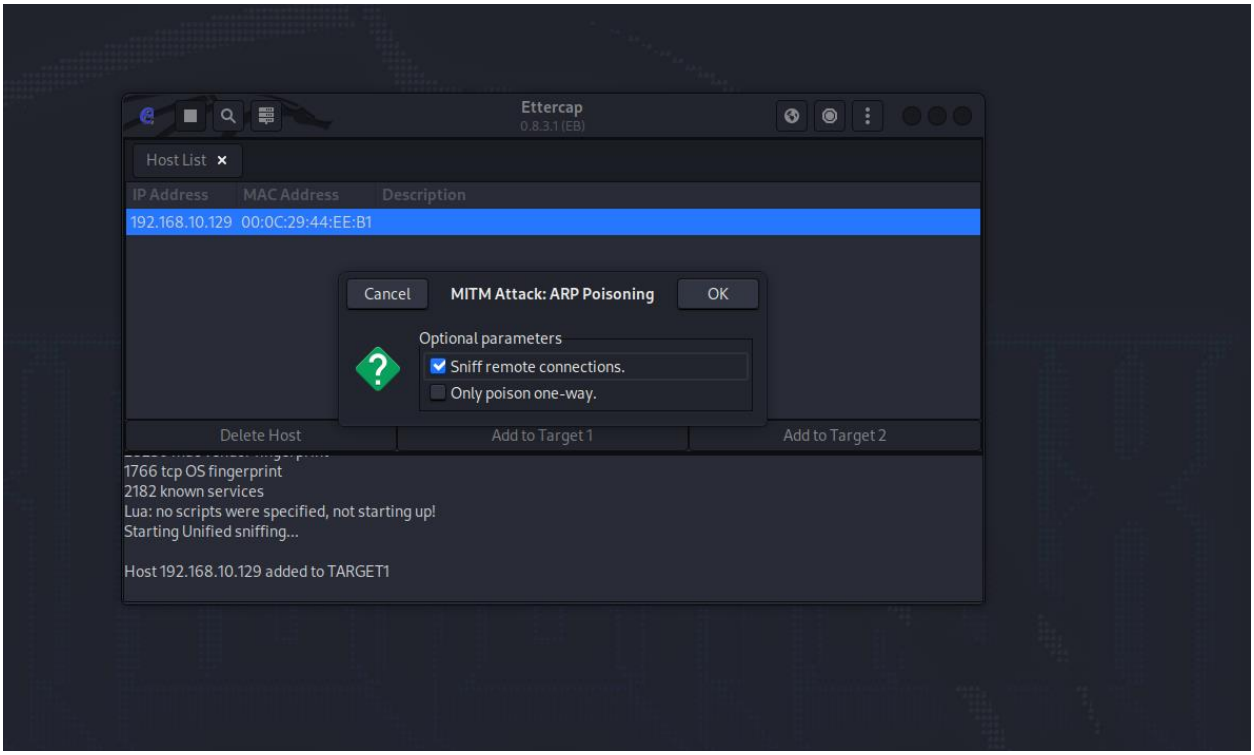


Figure-20 Attack started.

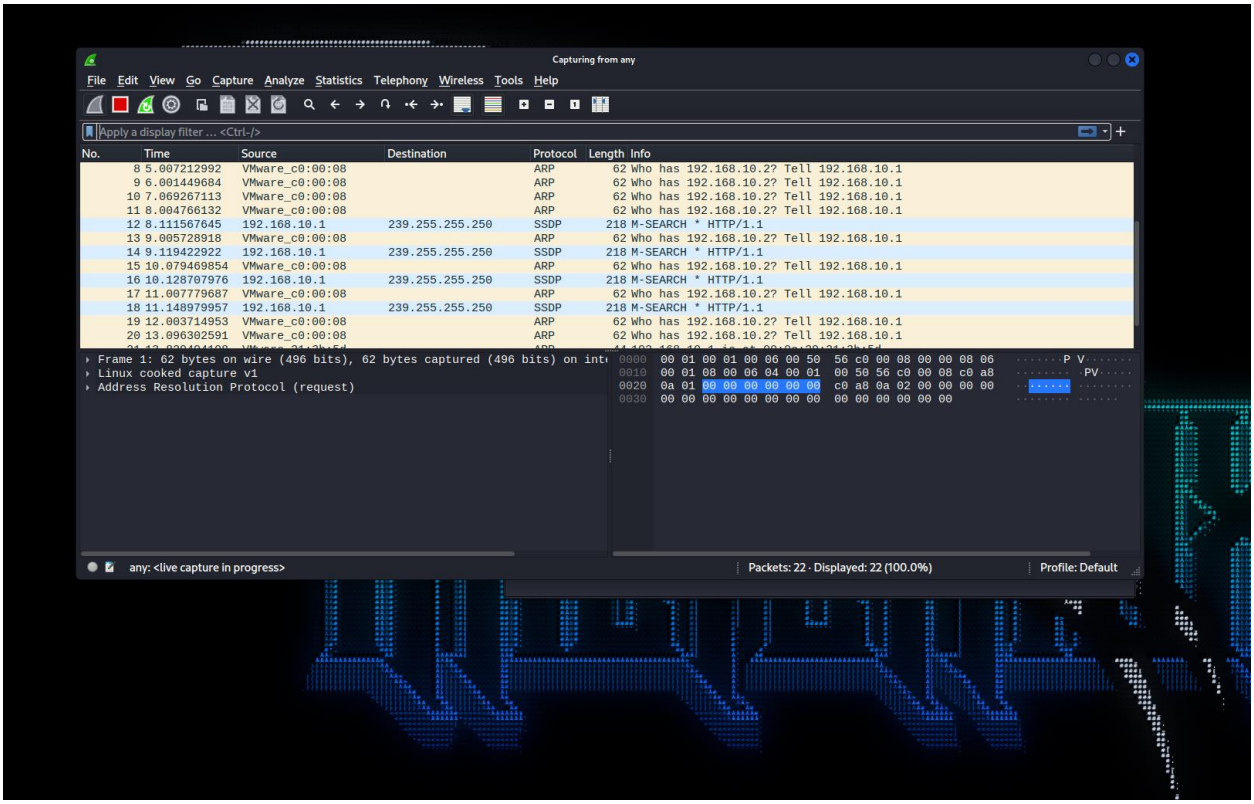


Figure-21 Wireshark for detection

Figure-22 Login in

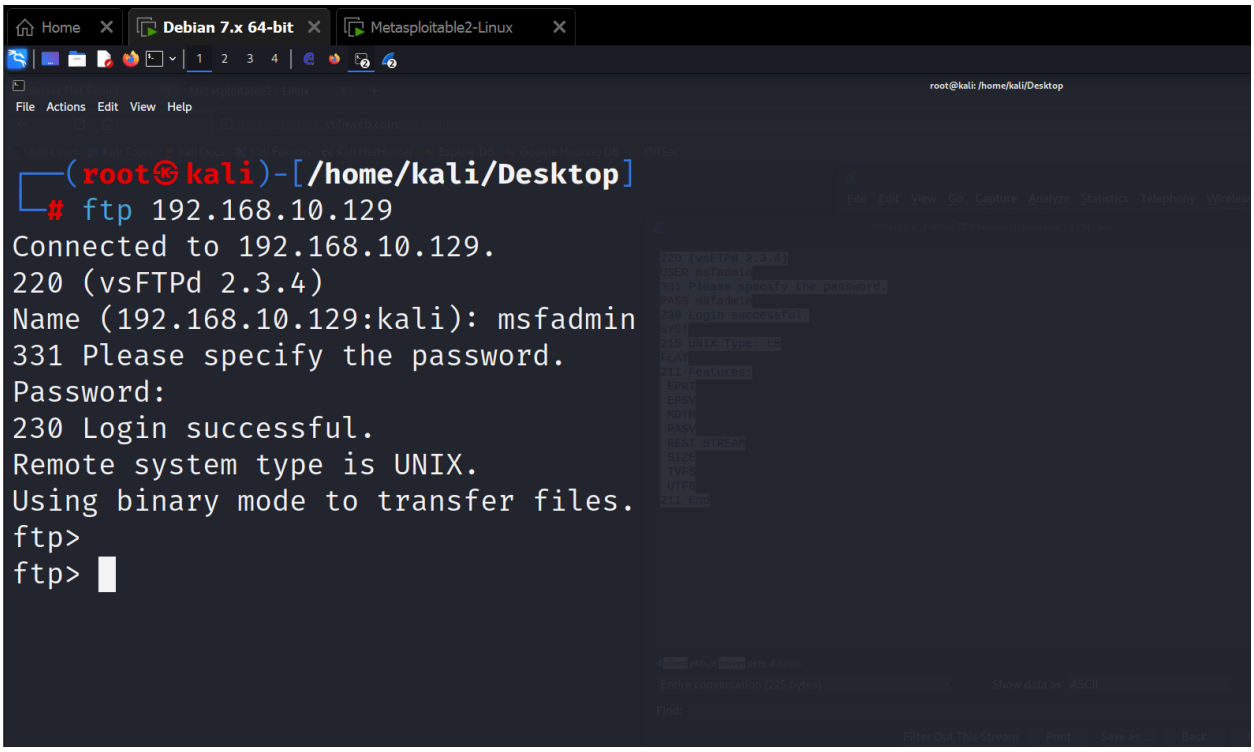
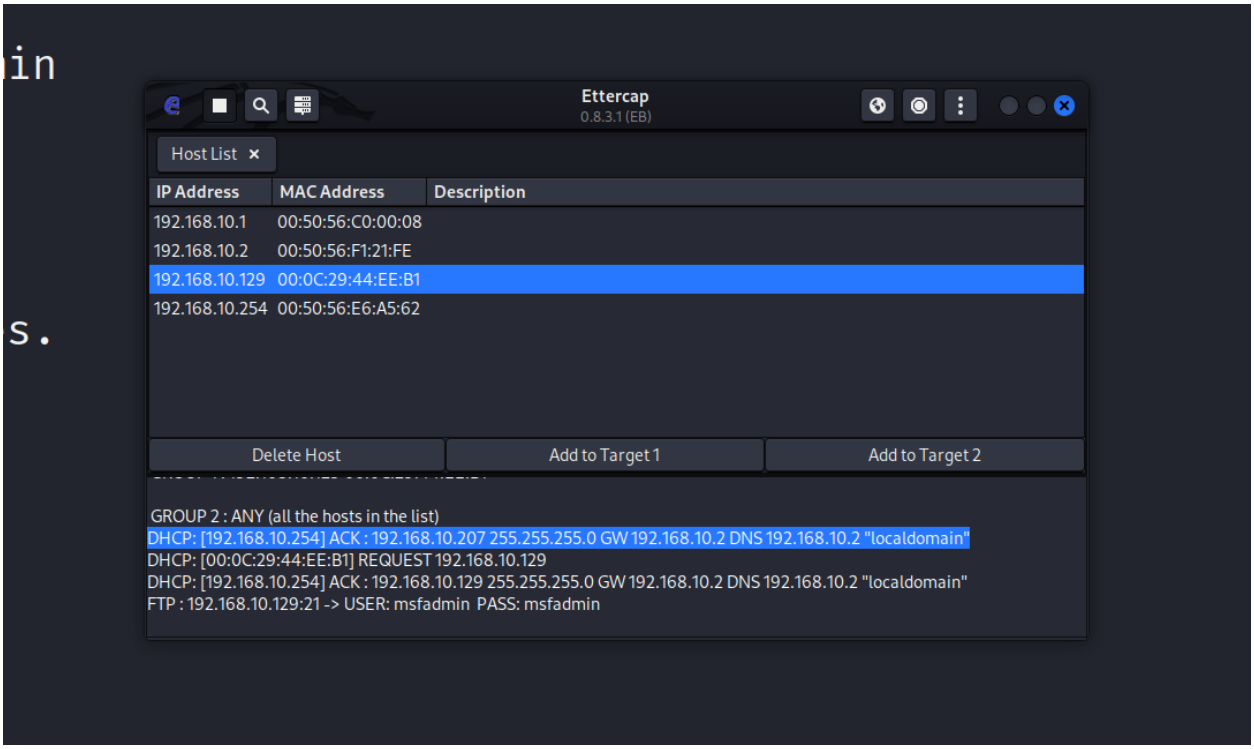


Figure-23 FTP login connection



Msfadmin password fetched.

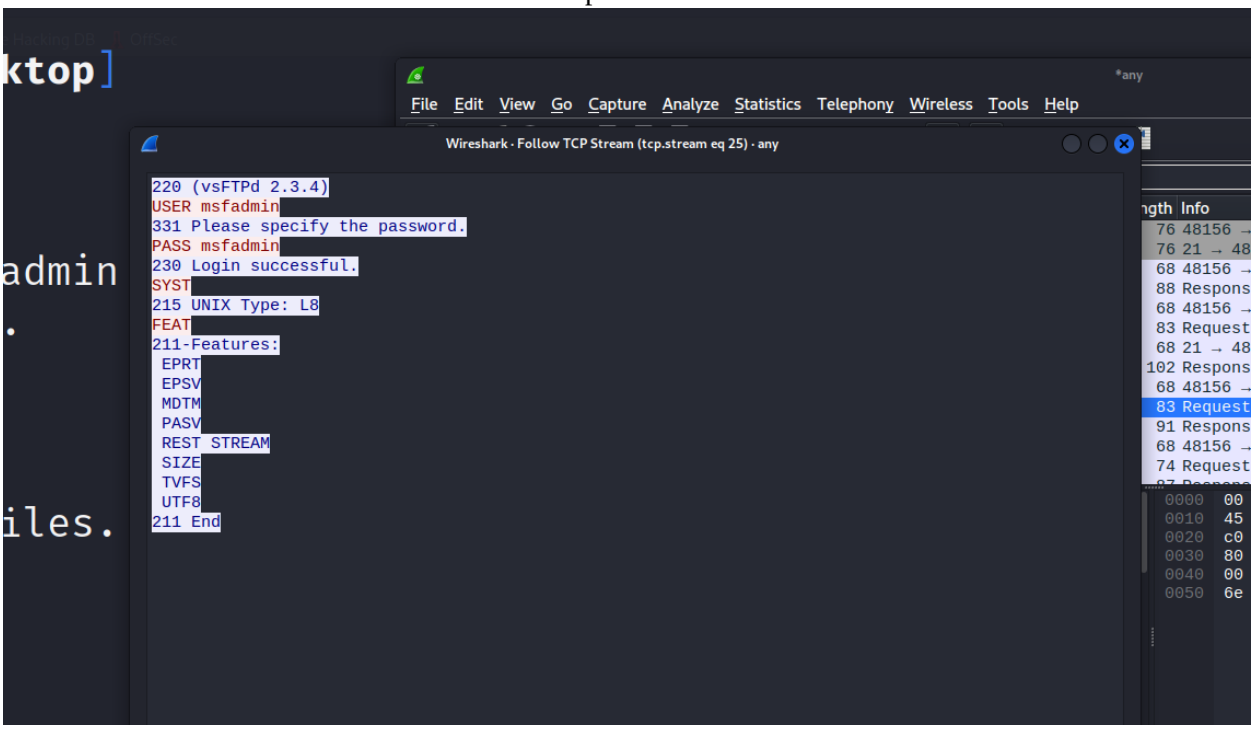


Figure-24 On Wireshark TCP Stream

3.2 Scenario Assessment: What information a potential attacker can obtain when this activity is

carried out, and how dangerous is this activity for your scenario

From the scenario we have obtained the login credintials of user while he is trying to login to ftp server. Using Wireshark tool, we can extract the ftp packets to search for login credintials that can be furthered used for malicious purpose. Additionally, the discovery of plaintext credentials underscores the importance of implementing encryption mechanisms like TLS/SSL for securing FTP communications to prevent such data interception and exploitation by attackers.

3.3 Investigate what activities a security analyst can conduct to protect the impact of man-in-the middle attack in the case of the scenario

To protect against MITM attack, security analyst can create a security plan that include implementing of VPSs to secure FTP connections. Security Analyst can also perform network segmentation and traffic monitoring by utilizing IDS/IPS can limit the attack surface for attackers. After implementing technology solutions, Security analyst can Educating users about MITM risks and secure communication practices through security awareness training. Implementing certificate pinning to prevent attackers from intercepting SSL/TLS connections.

b. Social Engineering Attack

3.4 Demonstrate how the attacker can lure a normal user of the server to your computer instead of the server machine.

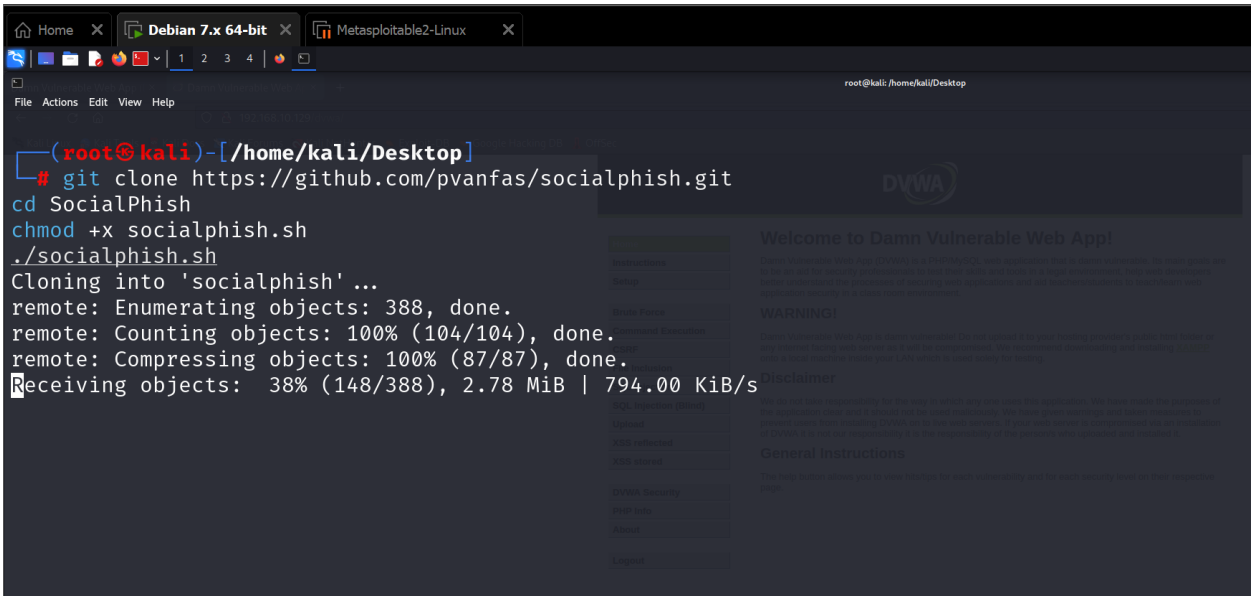


Figure-25 Installing social phish tool

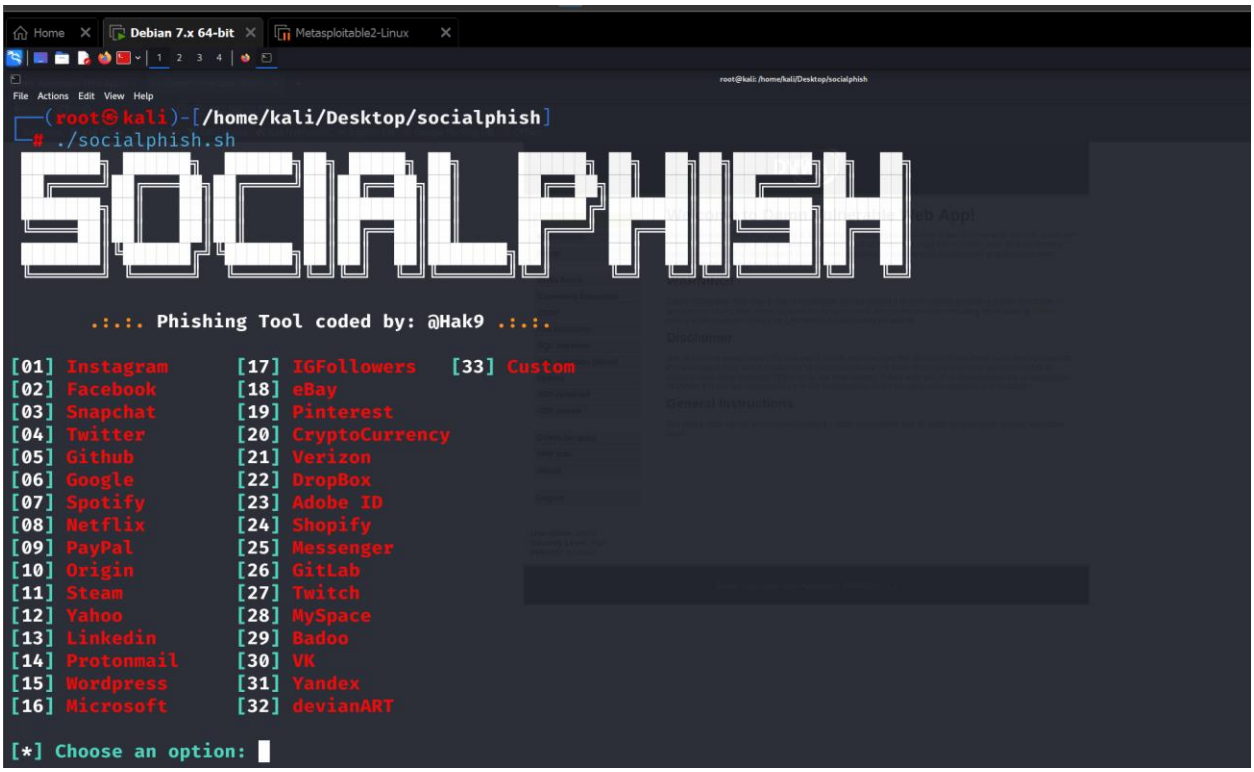
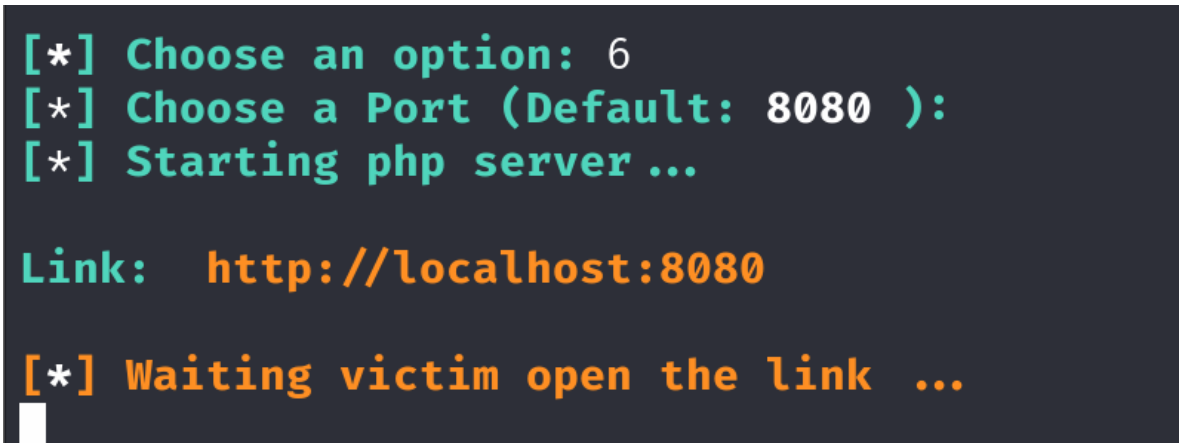


Figure-26 Starting tool



Creating phishing link (demonstrated on local host)

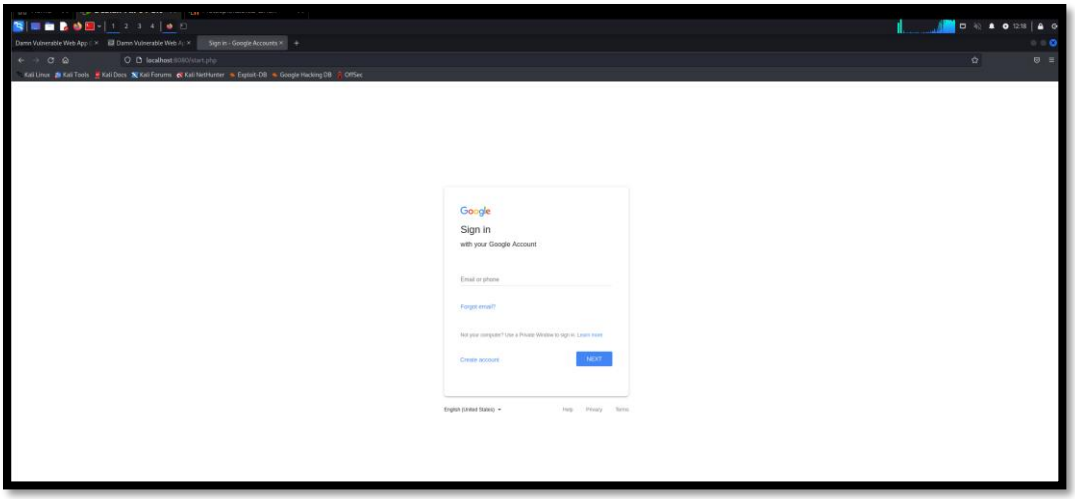


Figure-27 Opening phishing link

Figure-28 Entering credentials

Figure-29 We got the credentials

3.5 Scenario Assessment: What information a potential attacker can obtain when this activity is carried out, and how dangerous is this activity for your scenario.

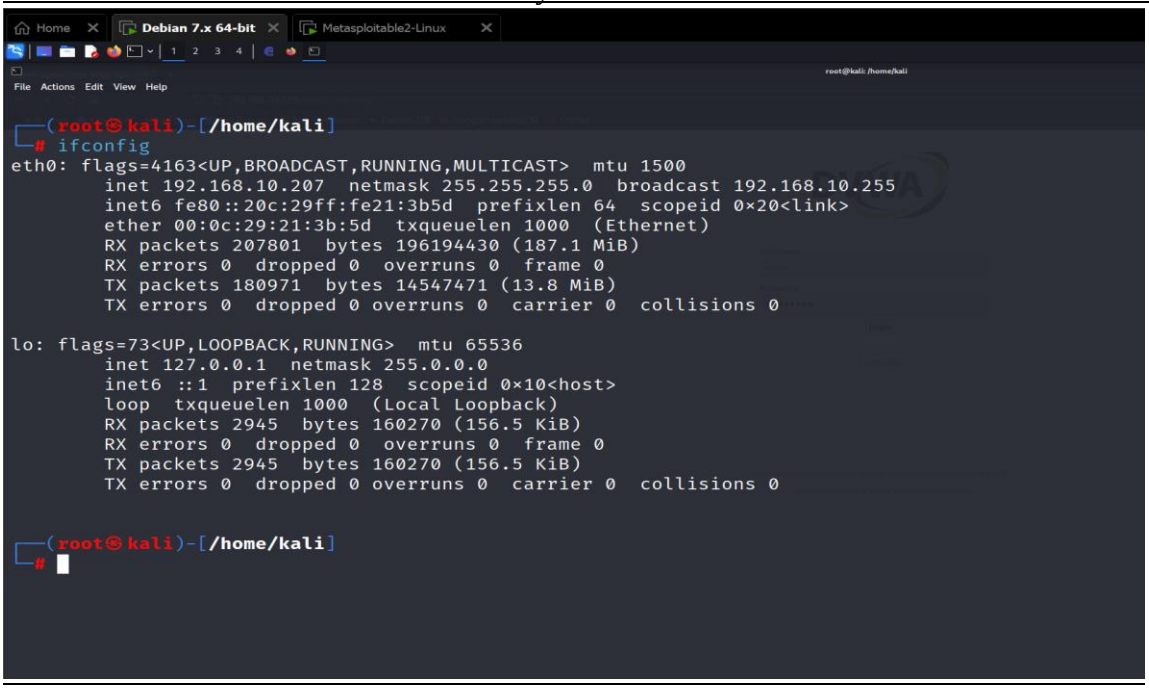
Through this scenario we have performed a social engineering attack in which attacker can create a phishing page of a legit website and trick user to enter sensitive credentials. This is very dangerous because the credentials entered by the user can be misused by the attackers or can be leaked over the databases. All accounts like bank accounts can be used by hackers to get unauthorized access

3.6 Investigate and explain the actions your scenario must do to ensure that users do not fall victims to social engineering attacks similar to the attack you carried out.

To Protect against social engineering attacks requires a different approach that encompasses education, technology, and organizational policies. First there should be a complete awareness session to all employees to train them for phishing link identification and not to enter sensitive information on the suspicious links. The implementation of MFA ensures that there is an extra shielding in case hackers manage to break through. Hence, even if the passwords are intercepted the attackers will not be able to access secure information. When a range of technologies is adopted, a cybersecurity apparatus consisting of these measures becomes robust equipping organizations to detect as well as avert social engineering attacks and steal data unjustly.

c. Denial of Service Attacks: DoS the Web Server

3.7 Demonstrate how an attacker can carry out a denial-of-service attack on the web server .



Fgure-30 Kali Linux to perform DOS attack.

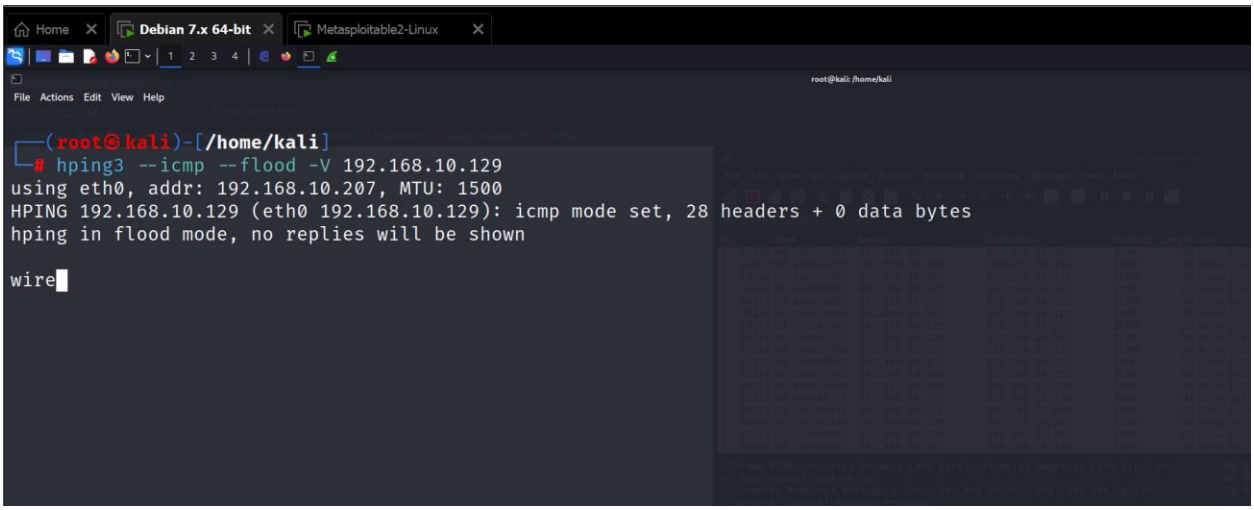


Figure-31 Hping tool to perform DOS attack on server

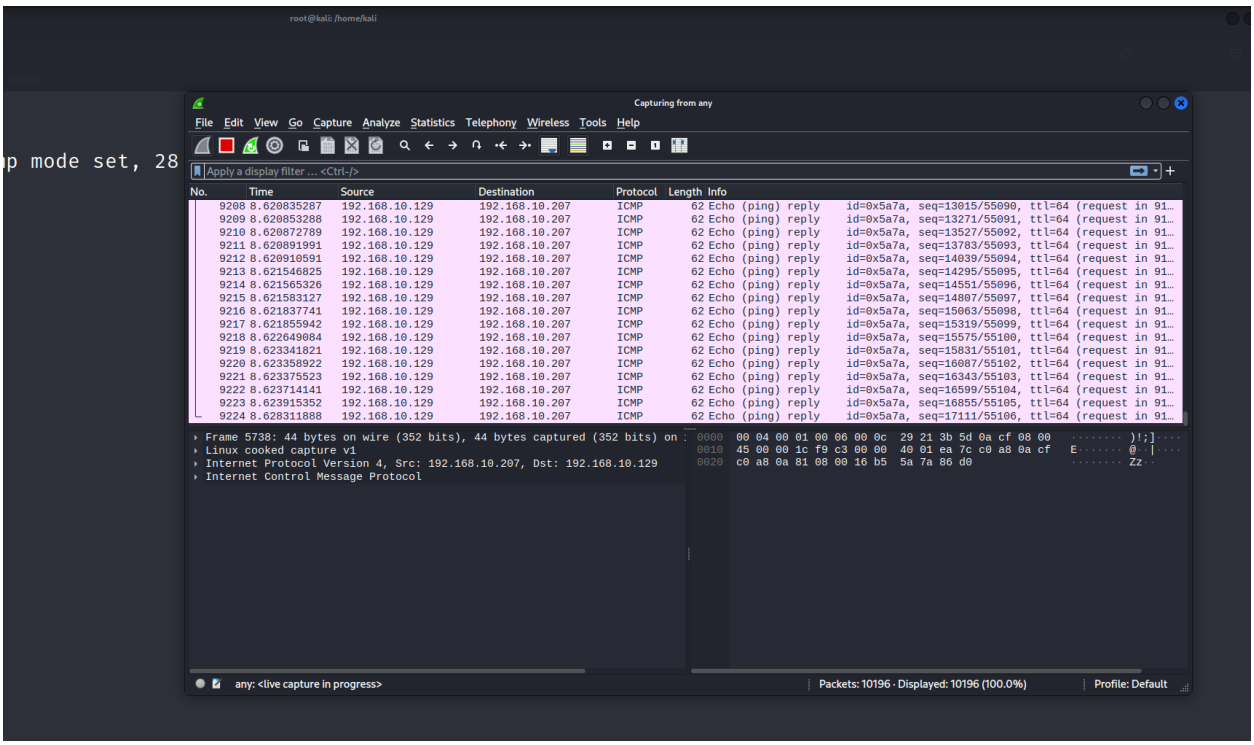


Figure-32 On Wireshark we can confirm the ping requests flooding.

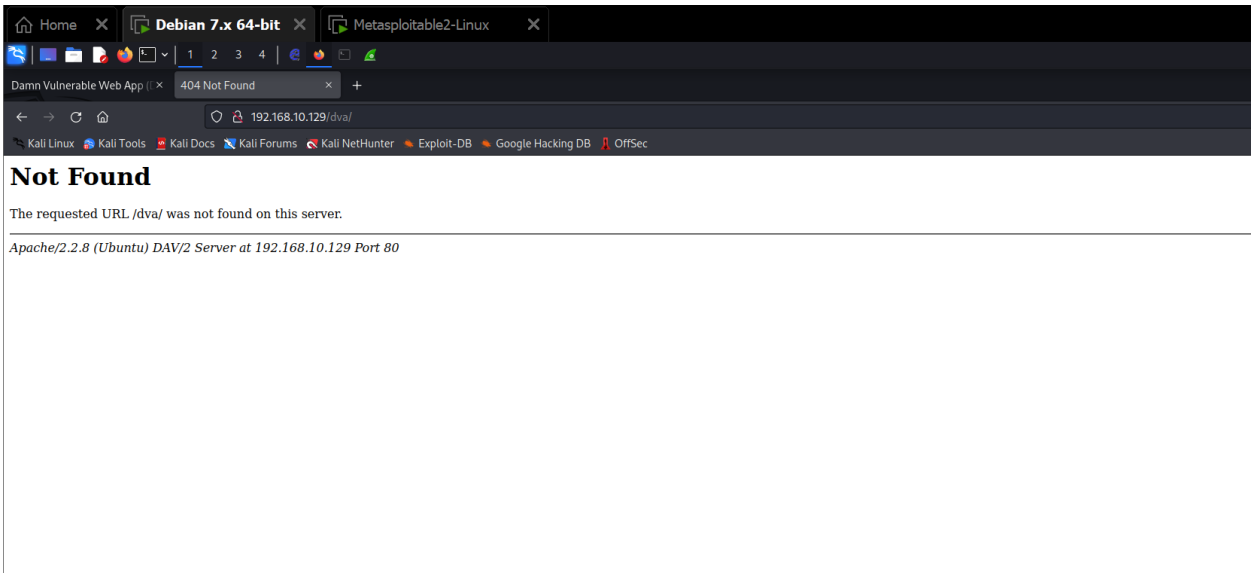


Figure-34 Unavailability of service.

3.8 Explain which tenet of cyber security this vulnerability violates?

The tenet of cyber security this vulnerability violates is Availability. This vulnerability allows for a DoS attack disrupt this availability by flooding a system, network, or service with excessive traffic or requests, this violation directly undermines the availability aspect of cybersecurity, as it prevents users from accessing the resources they need.

3.9 Scenario Assessment: what is the impact of this attack on your scenario?

In our scenario the impact is Denial of Service (DoS) attack disrupts service availability, causing the unavailability of webpage in our machine. This can cause the users to cannot access the server dashboard to perform their tasks causing to lose of service.

3.10 Explain what the company must to protect their web services against DoS attack similar to what you carried out

To protect against DoS attacks, the company should implement a multi-layered defense strategy. This includes deploying intrusion detection and prevention systems (IDPS) to detect and block suspicious traffic patterns indicative of DoS attacks. Implementing rate limiting measures, such as CAPTCHA challenges or IP address rate limiting, can also help mitigate the impact of DoS attacks by limiting the rate of incoming requests from potential attackers. Regularly updating and patching software and systems, along with conducting thorough security assessments and penetration testing, are essential to identify and address vulnerabilities before attackers can exploit them.

Task 4: Laws and Ethics (10 Marks)

4.1 Discuss the categories of unethical and illegal activities and how can affect your practice as a penetration tester.

As a penetration tester, it's crucial to understand and be aware of the categories of unethical and illegal activities to ensure that your work is conducted ethically, legally, and responsibly. Here

are some common categories of unethical and illegal activities that can affect your practice as a penetration tester:

1-Unauthorized Access: As such, hackers will use tactics such as compromise of the computer systems, networks, and data without the due authorization. Penetration testers must ask for a written approval from the owners of the systems they would be testing and only after an agreement can they commit any type of attack. An illegal access to a system or a software use, for example, may induce legal sanctions, including prosecutions on the ground of any computer crime acts.

2- Data Breaches and Theft: Testers need to remember that they need not expose themselves to much risk of creating data breaches or purloining protected information during their penetration pen tests. Excluding or poisoning the data without touching it is illegal and immoral. Create an engaging and informative narrative about the history of beer brewing in a specific region or country. Describe the cultural and societal significance of beer, explain the various brewing processes and ingredients used, and highlight the role of this process in the historical development of the area. It can influence incessant legal consequences and bad reputation for the potential penetration tester and the committed clients.

3- Denial of Service (DoS) Attacks: Instigating a DoS attack without legal permission is a criminal and an unethical activity. The job of a penetration tester requires the person not to perform any activity that results in systems and networks failing as they are supposed to work. DoS attack is very harmful to business and has the capability of losing huge amount of financial money.

4.2 What national and international laws must you consider when completing your engagement as a penetration tester assuming the company is based in the UK?

Considering penetration testers' adherence to the Foundations of the UK Data Protection Act of 2018 (GDPR), the Computer Misuse Act of 1990 and international concerns like the Budapest Convention. This process helps maintain strict legal and ethical standards, creating an increased level of security ensuring that there is no exposure of data during consultations. Moreover, compliance with the requirements from the institutions of like representing security niche, for example NCSC and CIISec is essential for responsible testing practices.

References:

1- Chauhan, A.S., 2018. Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus. Packt Publishing Ltd.
2- Miyamoto, Y., Shi, D., Nakajima, M., Ozaki, K., Sudo, A., Kotani, A., Uchida, A., Tanaka, T., Fukui, N., Tsunoda, T. and Takahashi, A., 2008. Common variants in DVWA on chromosome 3p24. 3 are associated with susceptibility to knee osteoarthritis. Nature genetics, 40(8), pp.994-998.
3- Zhang, L., Zhang, D., Wang, C., Zhao, J. and Zhang, Z., 2019. ART4SQLi: The ART of SQL injection vulnerability discovery. IEEE Transactions on Reliability, 68(4), pp.1470-1489.
4- Huovila, V., 2024. Improving the Security of SQL Server using SQL-Map Tool.