Configuration Manual

MSc Research Project

Masters in Cyber Security

Krishan Pal
Student ID:2225713

School of Computing

National College of Ireland

Supervisor: Khadija Hafeez

Krishan Pal
Student ID: 22205713

National College of Ireland

1 Introduction

1.1 1. 1 Overview

Smartphones have become one of the most essential utilities in today's society due to the fast advancement in which they undergo in the market and as such, they offer banking, communication, and entertainment among other activities. Nonetheless, it worth to admit the rise of its popularity made applications more exposed to attackers, especially through MITM type of attack. This is a type of cyber-attack where the attacker intervenes and can even modify the messages exchanged between two users which a very high risk of theft of information and data manipulation. These kinds of attacks are becoming more and more common, and that underlines the fact that better protection is needed for user data.
One of the most known platforms in the cybersecurity area, Kali Linux, provides the set of tools aimed to fulfill the tasks related to penetration testing and security auditing's. Detecting mechanism and preventive countermeasure to avoid MITM attack are quite essential in mobile applications due to tools such as Wireshark, Burp Suite, and Metasploit. The information presented in this manual is focused on describing how to set up these tools in Kali Linux to assess and mitigate MITM risks and thus improve mobile application protection.

2 System Specification

The System Specification Section provided the details of hardware and software fundamentals that requires setting up to create secure environment for analyzing and mitigating Man-in-the-Middle (MITM) attacks targeting mobile applications with through Kali Linux (Wangchuk *et al.* 2024). It determines the hardware requirements which are essential and recommended to meet the required tools' performance. Further, it explains the essential software parts such as Kali Linux ISO image, VMware Workstation Pro, and numerous security tools that are required to create a sound testing environment for vulnerability assessment and penetration testing.

2.1 Hardware Requirement

There are recommended hardware requirements that must be met in order to properly install Kali Linux and use it for activities such as penetration testing and security auditing (Heiding *et al.* 2023). Such requirements make that the system is capable of executing the requisites tools and processes, especially when working with more than one VM.

- **Processor:** To be more specific, it requires a compatible 64-bit x86 CPU of 2011 production and later. The processor must include minimum an operating core of at least 1. 3GHz. As for the Intel processors, Intel VT-x and Intel EPT technology should be enabled, for AMD processors, it should support the AMD-V and the RVI technologies.
- **Memory (RAM):** Most guest operating systems need at least 4 GB of RAM; 8 GB or more for better operation particularly when running several guests.
- **Hard Disk Space:** About one. 2 GB disk space is required for application. Each VM requires additional space for the particular guest OS and the applications that are to be installed there.

Graphics: A Graphic Processing Unit that has features compliant with DirectX 11 or OpenGL

4. It is important for 3D graphics, and 3D graphic required is 1. For better result, a have dedicated GPU memory and it is preferred to be a discrete one.

- **Network:** A standard Ethernet, or wireless Wi-Fi network card is necessary for network access.
- **Other Requirements:** Only at the level of BIOS can the popular HW virtualization support be enabled on the computer. A USB 2. 0/3. USB device support requires no controller; whereas, 0 controller is required for USB device support.

2.2 Software Requirement

In addition to the hardware, specific software components are necessary to set up the environment for testing and preventing MITM attacks:

- **Kali Linux ISO Image:** The first choice of operating system for conducting Penetration Testing and Security Auditing.
- **Android ISO Image:** Test Environment for Vulnerability of Android Applications is a virtualized environment to test Android apps and their possible vulnerabilities.
- **VMware Workstation Pro:** A program by which it is possible to install several virtual computers and test various configurations of operating systems.
- **Evil Droid:** A tool for creating malware that is blended into other genuine Android applications.
- **Metasploit:** A tactical approach towards identifying, elaborating, and verifying various kinds of attacks on a given entity.
- **XForce Terminal Emulator:** A terminal to run the commands with the facility of Kali Linux environment.
- **APK Tool:** A technique used in the reversal of the quantity of the spreading Android APK files for changing and rebuilding of the Android useful applications.
- **Apache Server:** A compromised web server that is employed in exposing the intending malware or files to the internet during pen testing.

3 Implementation

In this section, we also describe a set of steps for the configuration of the mentioned tools in Kali Linux for identifying and preventing MITM threats in mobile apps (Atılgan *et al.* 2023). All the tools are designed in a way that they are important in various facets of penetration testing, including traffic analysis and vulnerability exploitation.

3.1 Setting Up the Environment

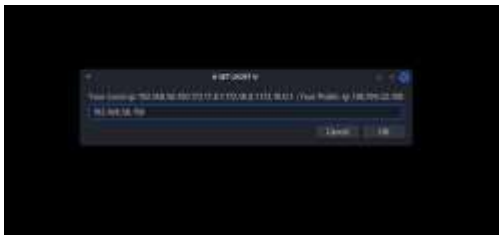

Figure 1: Setting up the listening host
(Source: Generated from Linux)

The first step therefore is to get the testing environment ready using VMware Workstation Pro. Kali Linux and Android ISO images should be installed as Guest Operating Systems. Make certain the configuration and setup of the Network resemble a ‘live’ environment where apps for mobile devices communicate over the internet with servers.

3.2 Making a Malicious Application

Figure 2: Choosing the reverse TCP meterpreter shell
(Source: Generated from Linux)

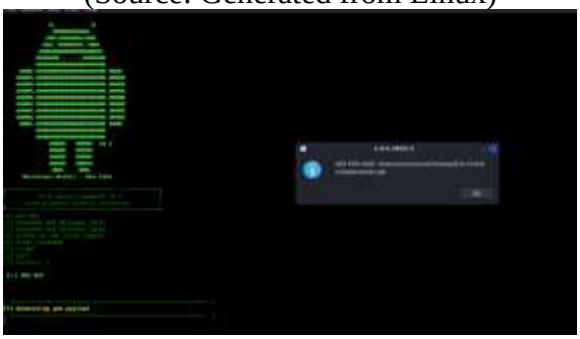

Figure 3: Successfully generated a malicious app
(Source: Generated from Linux)

Once the environment is set up, the next thing that is done is to create a bad, dangerous Android app. This process includes, the use of application such as Evil Droid, which is used in placing a bug within another normal application. The payload intends to create a reverse TCP meterpreter shell that means the attacker gets full control of the device. On the Kali Linux Machine, the setup of listening host is shown in Figure 1 below: Figure 1: Listening Host setup on Kali Linux Machine The options selected in penetrated mobile during the creation of the malicious app are shown in Figure 2 above.

3.3 Connecting the Reverse Shell

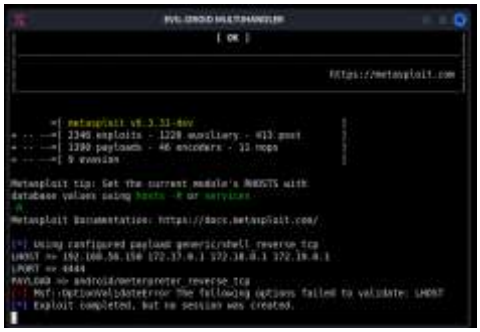

Figure 4: Opening the Metasploit framework for reverse shell connection
(Source: Generated from Linux)

Thus, the further steps pertain to the process of moving the generated app to the targeted Android device. In this type of attack, once the victim downloads the created App the attacker gains control of their device with the use of the Metasploit framework for instance to create a reverse shell connection. Figure 4 shows the process of running the Metasploit Framework to configure the listener while the figure 5 and Figure 6 show the IP address of the host machine and the Android phone. These steps are very important in achieving the objective of establishing a connection between the attacker and the victim's device so as to intercept and arbitrate communication between the mobile app and the server.

Step 1: Begin by opening Burp Suite in Kali Linux and start setting it as an operative proxy.

Step 2: Proxy the traffic of the Android VM through the burp suite to be able to intercept requests and responses.
Step 3: The significance of the interception of the traffic to identify the flaws, for example, inadequate SSL/TLS configurations together with invalid certificate validation.
Step 4: One needs to modify the intercepted traffic to mimic an MITM attack to analyses the application's reaction.

3.4 Exploitation with Metasploit

Metasploit can be described as a full-featured toolbox that encompasses the means, ways, and goals of penetrating and compromising a target system. Using the tool, an MITM proxy attack is possible as it involves the injection of wrong or malicious data into the Mobile application.

Step 1: Open the Metasploit in the Kali Linux and set the attack to the Android Virtual Machine.

Step 2: Exploit/multi/HTTP/mitm_proxy – exploits the system to impersonate a Man in the Middle Proxy.

Step 3: Spy the traffic going through the proxy to incorporate infected codes.

Step 4: one has to evaluate the attack's consequences on the mobile application from the data integrity and the user's privacy perspectives.

3.5 Implementing Countermeasures

After learning more about the threats and the feasibility of the MITM attack, it will be necessary to learn about the countermeasures that can be employed to safeguard the mobile application (Daka *et al.* 2023). Another strategy was observed to be certificate pinning, in that the application only communicates with trusted servers.

Step 1: It is important to further alter some of the content of the mobile application by applying the certificate pinning. This involves placing the server's public key or its certificate in code form with the application and making it become a part of its source code.

Step 2: Verify it consistently refuses to connect to any server unless explicitly trusted, even when the SSL certificate looks splendid.

Step 3: Perform another traffic analysis and vulnerability scanning test to ascertain that an MITM attack is no longer feasible.

4 Conclusion

Therefore, as the use of MITM attacks on mobile applications grows, it is important to take action to protect the mobile application. Security experts are in a position to use the effective applications in Kali Linux including Wireshark, Burp Suite, and Metasploit to dissect mobile

applications to look for weaknesses. This manual has described the hardware and software requisites and the procedures to apply these tools to enter into the identification and counteraction of international MITM threats.

Thus, when other countermeasures, including certificate pinning, are implemented, the security of mobile applications is enhanced, and the user's confidential information will not be compromised during communication. Cyber threats are continuously developing and security measures and technologies must be also adapted as well as possible attackers. This manual offers a detailed way for security testing environment setup and deployment of a proper defence against MITM in mobile applications.

1. References

Daka,M.,2023. *Strengthening web application security through technical measures* (Doctoral dissertation, The University of Zambia.).

Makulova, A., Sharipova, B., Othman, M., Pyrkova, A. and Ordabayeva, G., 2024. Defection of operating system vulnerabilities and network traffic analysis methods. *Journal of Mathematics, Mechanics and Computer Science*, *121*(1), pp.99-109.

Şimşek, M.M. and Atılgan, E., 2023. Attacks on Availability of IoT Middleware Protocols: A Case Study on MQTT. *Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi*, *4*(2), pp.16-27.

Süren, E., Heiding, F., Olegård, J. and Lagerström, R., 2023. PatrIoT: practical and agile threat research for IoT. *International Journal of Information Security*, *22*(1), pp.213-233.

Thankappan, M., Rifà-Pous, H. and Garrigues, C., 2024. A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. *IEEE Access*.

Wangchuk, T., Tshering, Y., Mandela, N. and Rughani, P., 2024. Forensic analysis of Scientific Linux image using commercial and opensource forensic tools. *Journal of Applied Engineering, Technology and Management*, *4*(1), pp.68-82.