**Penetration Testing Using Kali Linux**

Himamshu Aluru, Stephen Bickel, Siri Gundlapally, Meghana Meka, Yash Shah

Marist College – School of Computer Science and Mathematics   
3399 North Rd. Poughkeepsie, NY

**ABSTRACT**

Penetration testing is an essential part of modern cyber security and is crucial for effective vulnerability assessment within information systems. This tutorial paper provides a guide to penetration testing using Kali Linux, a versatile, powerful, and well-known toolkit for cyber security. Tools like Nmap, Wireshark, and Metasploit will be utilized. This paper will cover objectives, strategies, and legal considerations of penetration testing. This paper will guide readers through the phases of the penetration testing cycle including information gathering, target identification, vulnerability analysis, exploitation, and post-exploitation activities. Ultimately, this paper will be a valuable resource for aspiring and experienced IT professionals who want to enhance their knowledge of cyber security, Kali Linux, and its capabilities.

**Keywords:** Penetration Testing, Cyber Security, Vulnerability Assessment

**INTRODUCTION:**

**Information Gathering:**

"Information Gathering" is the first phase of the penetration testing cycle, which consists of multiple steps. During this stage, the target's IP addresses, domain names, subdomains, email addresses, and other pertinent data are methodically gathered by ethical hackers. Reconnaissance and enumeration techniques are employed to acquire an understanding of the target's infrastructure. The penetration tester can gain an understanding of the target environment, possible weaknesses, and prospective attack routes during this phase, which lays the groundwork for the succeeding processes of vulnerability scanning, exploitation, and post-exploitation operations. A thorough and successful penetration test is predicated on the collection of effective information, which aids in the identification of vulnerabilities and the assessment of the target systems' security.

**Target Identification:**

Target identification is a crucial phase in the penetration testing process because it aids in the selection and evaluation of the systems and networks that safety experts and ethical hackers will be examining. Potential targets can be found using a variety of methodologies while using Kali Linux, a widely utilized penetration testing system.It entails several procedures involving ping sweeps and network scanning. Web Scanning Technologies for DNS Enumeration and Vulnerability Enumeration Scanners Reconnaissance in Passive WiFi Inspection Target Lists for Social Engineering.

**Vulnerability Analysis:**

Vulnerability analysis is the utmost phase in the penetration testing it's a systemic process of relating, classifying, and assessing security weakness or vulnerabilities in computer systems, network, operations or any other information technology structure. The main precedence of Vulnerability analysis is to proactively identify implicit sins that could be exploited by vicious actors, allowing association to take correct action to alleviate these pitfalls before they were exploited. There are numerous of the software operations that assists to security professionals and associations in the process of detecting the vulnerabilities and managing the vulnerabilities. These tools also automate the process of scanning and assessing systems for known vulnerabilities and security sins. Some of the operations related to Vulnerability analysis are Nessus, Open VAS, Qualys, N expose, Metasploit, Wireshark, snort and vulnDB. In this study we are going to use the wireshark which is not a traditional tool for vulnerability scanner but it was a network protocol analyzer helps to identify network based vulnerabilities and anomalies by capturing and analyzing the network traffic.

**Exploitation and post exploitation studies:**

The exploitation phase of a penetration test is focused on gaining access to a system by bypassing security restrictions. Exploiting weak passwords, unpatched operating systems, or taking advantage of misconfigurations are some strategies used during cyber-attacks. If the vulnerability analysis phase is performed successfully, then the exploitation phase is a well-planned directed attack on a specific aspect of the system.

The period following unauthorized access to a system or network is referred to as post-exploitation in penetration testing. After access is gained, the emphasis switches to preserving control, raising privileges, and investigating the infiltrated environment to extract more data or carry out additional exploitation. Testers can carry out operations like lateral movement throughout the network, data exfiltration, privilege escalation, and access maintenance through backdoors other persistent mechanisms thanks to the range of capabilities Kali Linux offers for post-exploitation activities. It is imperative to remember that post-exploitation operations must only be carried out within a moral and legal framework and with the required license.

**PROCEDURE**

1. **Identifying and scanning target system**

First, we needed to identify the target machine. We went on the target machine to get the IP address. We identified the target IP address as 192.168.169.130. We then went onto our Kali Linux Operating system and pinged the target machine to establish a connection. We used NMAP to scan the target machine and identify the vulnerabilities and open ports. We used the following command:

**Nmap -sV -O 192.168.169.130**

The -sV command identified the version of services running on the target machine. The -O command was used to determine the operating system which the target system is operating on.

Our first task was to exploit FTP port 21. We launched Metasploit using the command below.

**msfconsole**

1. **Exploiting FTP port 21**

We searched the for the exploit on FTP port 21 by using the command below:

**search vsftpd**

Metasploit was able to identify an exploit. We executed the exploit by using the following command:

**use exploit/unix/ftp/vsftpd\_234\_backdoor**

We then set the remote host to our target system using the following command:

**set RHOST 192.168.169.130**

We then used the command “run” to run the exploit. This exploit gave us access to the target system. We used the command “whoami” in order to confirm that we were given root access to the target system.

1. **Exploiting port 5900**

We used metaploit to search for exploits by using the command:

**search vnc login**

Metasploit was able to identify an export and we used the following command to execute the exploit:

**use auxillary/scanner/vnc/vnc\_login**

we then set our remote host to our target system and ran the exploit using the commands:

**set RHOST 192.168.169.130**

**run**

1. **Exploiting Samba Server**

Once again we used Metasploit to exploit the Samba Server. We used the following command to search for the exploit:

**search usermap script**

Metasploit identified the exploit and we ran the following commands to gain access:

**exploit/multi/samba/usermap\_script**

After access to the target system was gained, we used the following commands to check for our privileges.

**Whoami**

We got the response “root” which means that we were given root access to the target machine.

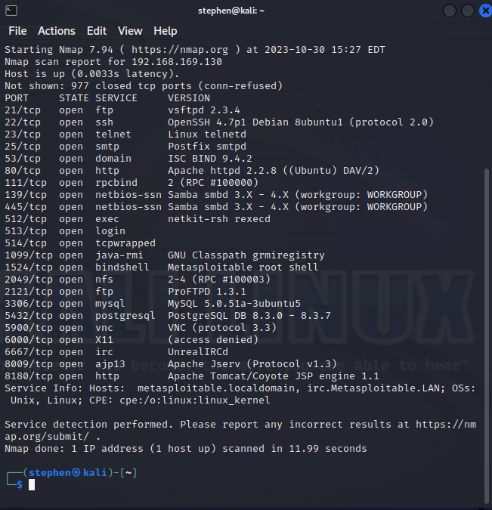
**RESULTS**

**Exploiting Port 21**

A screenshot of a computer program

Description automatically generated

We were able to ping and establish a connection with the target system.



We used Nmap to scan the target system for open ports, as well as the version of the services running on the target system.

A screenshot of a computer

Description automatically generated

We opened up Metasploit.

A screenshot of a computer

Description automatically generated

We searched for exploits on FTP port 21 which we identified as open using Nmap.

A computer screen with white text

Description automatically generated

We used the exploit identified by Metasploit to gain access to the target system. We set our remote host as our target system and then we ran the exploit.

**Exploiting port 5900**

A screenshot of a computer

Description automatically generated

For this we used Metasploit again to search for exploits on port 5900. We were able to extract login and password and gain access to the target system.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

The two pictures above show that we were able to gain access to the target system.

**Exploiting Samba Server Vulnerability**

The last vulnerability we exploited was the Samba server. This vulnerability will give use access to a TCP shell which a hacker could use to perform malicious activity on the target system.

A screenshot of a computer

Description automatically generated

We used Metasploit to search for exploits. We set the remote host to the target machine and gained access.

**Conclusion**

This project provided hands-on experience in applying penetration testing methodologies with Kali Linux. By systematically conducting reconnaissance, vulnerability analysis, exploitation, and post-exploitation, we successfully demonstrated how common system weaknesses can be identified and exploited. Using tools such as Nmap, Wireshark, and Metasploit, we gained root access to the target system through FTP, VNC, and Samba vulnerabilities. These findings underscore the importance of proactive vulnerability management and patching in maintaining secure information systems. Ultimately, this project enhanced our technical knowledge of ethical hacking practices and reinforced the critical role of penetration testing in strengthening cybersecurity defenses.

**References**

Muthii, K. (2022, April 3). *Learn hacking with metasploitable 2 [step-by-step]*. GoLinuxCloud. https://www.golinuxcloud.com/learn-hacking-using-metasploitable-2/

Tiwari, G. (2023, July 3). *The exploitation phase in penetration testing: What should it include?*. Gaurav Tiwari. https://gauravtiwari.org/exploitation-phase-in-penetration-testing/