Linux Penetration Testing Report

Target Website: Confidential

Penetration Tester: SK ARIF BIN EKRAM

Executive Summary:

This report outlines the findings and steps taken during a comprehensive penetration test conducted on the target website. The test revealed several vulnerabilities, including issues with the Server Message Block (SMB) services, ProFTPD server, SSH key management, and privilege escalation via Set-User Identification (SUID). By exploiting these vulnerabilities, unauthorized access was gained to sensitive information and escalated privileges to root level, demonstrating significant security risks to the target website.

Table of Contents:

1. Introduction:

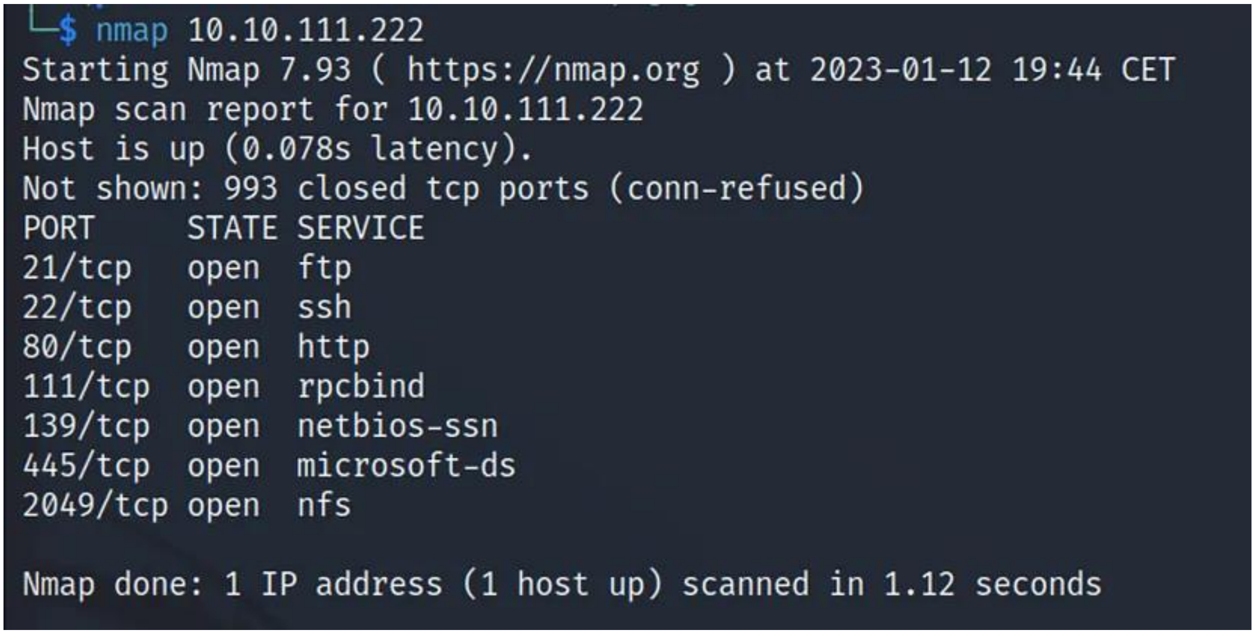
This penetration testing engagement was conducted to assess the security posture of the target website and identify potential vulnerabilities that could be exploited by malicious actors. The test was performed in a controlled environment to simulate real-world attack scenarios without causing harm to the production system.

2. Methodology:

The testing methodology followed industry-standard practices, including reconnaissance, vulnerability scanning, exploitation, and post-exploitation activities. Various tools and techniques were utilized, such as Nmap for port scanning, enumeration scripts for SMB services, searchsploit for identifying exploits, and manual inspection for privilege escalation opportunities.

3. Findings:

3.1 Nmap Port Scanning and SMB Enumeration:



```
└─$ nmap 10.10.111.222
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-12 19:44 CET
Nmap scan report for 10.10.111.222
Host is up (0.078s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

Affected Component: Network Services (Port 445 - SMB)

Proof of Concept: Using Nmap with SMB enumeration scripts, three SMB shares were discovered on the target system. Access to one of the shares revealed a log.txt file containing sensitive information, including SSH private key.

Technical Details: The enumeration of SMB shares exposed sensitive files, highlighting potential misconfigurations in the server's file-sharing settings. Access to the log.txt file provided valuable credentials for further exploitation.

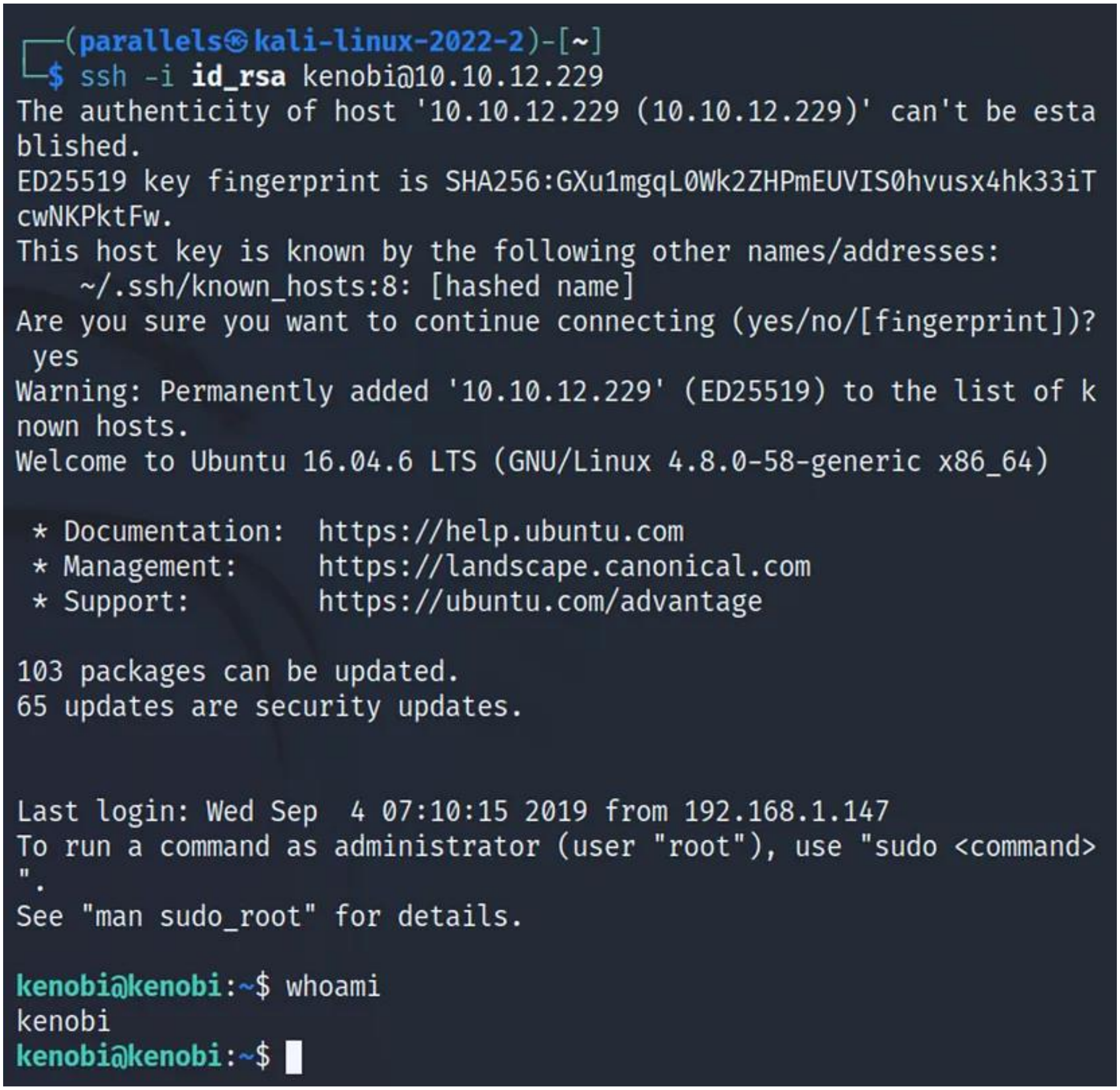
3.2 ProFTPD Vulnerability:

Affected Component: ProFTPD Server

Proof of Concept: Exploiting a known vulnerability in ProFTPD (version 1.3.5), unauthorized access was gained to the server. This allowed retrieval of sensitive information, including user credentials.

Technical Details: The ProFTPD vulnerability provided a foothold for attackers to access the system, underscoring the importance of timely software updates and patch management.

3.3 SSH Key Management:



```
┌──(parallels㉿kali-linux-2022-2)-[~]
└─$ ssh -i id_rsa kenobi@10.10.12.229
The authenticity of host '10.10.12.229 (10.10.12.229)' can't be esta
blished.
ED25519 key fingerprint is SHA256:GXu1mgqL0Wk2ZHPmEUVIS0hvusx4hk33iT
cwNKPktFw.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])?
 yes
Warning: Permanently added '10.10.12.229' (ED25519) to the list of k
nown hosts.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

103 packages can be updated.
65 updates are security updates.


Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147
To run a command as administrator (user "root"), use "sudo <command>
".
See "man sudo_root" for details.

kenobi@kenobi:~$ whoami
kenobi
kenobi@kenobi:~$ 
```

Affected Component: SSH Configuration

Proof of Concept: Extracting the SSH private key from the SMB share, unauthorized access was obtained to the server as the "kenobi" user.

Technical Details: Insecure SSH key management facilitated unauthorized access to the server, highlighting the need for proper key handling practices and access controls.

3.4 Privilege Escalation via SUID:

Affected Component: SUID Binary

Proof of Concept: Exploiting a vulnerable SUID binary (/usr/bin/menu), root-level access was achieved through path manipulation and command execution.

Technical Details: The exploitation of the SUID binary demonstrated the importance of securely configuring setuid permissions and conducting regular security audits to identify potential risks.

4. Recommendations:

- Implement proper access controls and authentication mechanisms to prevent unauthorized access to sensitive resources.
- Regularly update and patch software to address known vulnerabilities and mitigate potential security risks.
- Improve SSH key management practices, including encryption, rotation, and access control.
- Review and restrict permissions for SUID binaries to minimize the risk of privilege escalation attacks.

5. Conclusion:

In conclusion, the penetration test revealed significant vulnerabilities within the target website, including issues with SMB services, ProFTPD server, SSH key management, and SUID binaries. Addressing these vulnerabilities is critical to enhancing the overall security posture of the website and protecting against potential cyber threats. Continued vigilance, regular security assessments, and proactive risk mitigation strategies are essential for maintaining a secure and resilient IT environment.

Disclaimer: This report is intended for internal use only and should not be disclosed to unauthorized individuals. The findings and recommendations provided herein are based on the results of the penetration testing engagement and may require further investigation and validation.