HackTheBox Beep

HackTheBox penetration test report

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

19-5-2023

Contents

1 HackTheBox “Beep” penetration test report **1**

1.1 Introduction 1

1.2 Objective 1

1.3 Requirements 1

2 High-Level Summary **2**

2.1 Recommendations 2

3 Methodologies **3**

3.1 Information Gathering 3

3.2 Service Enumeration 3

3.3 Penetration 3

3.4 Maintaining Access 4

3.5 House Cleaning 4

4 Target - 10.129.227.195 **5**

4.0.1 Service Enumeration 5

4.0.2 Initial Access - local file inclusion 7

4.0.3 Privilege Escalation 9

1 HackTheBox “Beep” penetration test report

1.1 Introduction

HackTheBox offers vulnerable machines to exploit in a safe and legal manner. In this report, the machine “Beep” 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 “Beep”. 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 "Beep". 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 "Beep". 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 "Beep". When performing the attacks, Michael was able to gain access to the machine, primarily due to outdated patches and poor security configurations.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:

- Beep 10.129.227.195
- Elastix 'graph.php' local file inclusion

2.1 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

10.129.227.195

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 16 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.

4 Target - 10.129.227.195

4.0.1 Service Enumeration

Port Scan Results

Server IP Address	Ports Open
10.129.227.195	**TCP**: 22,25,80,110,111,143,443,941,993,995,3306,4190,4445,4559,5038,10000

TCP Port	Service
22/tcp	OpenSSH 4.3 (protocol 2.0)
25/tcp	smtp?
80/tcp	http Apache httpd 2.2.3
110/tcp	pop3?
111/tcp	rpcbind
143/tcp	imap?
443/tcp	ssl/https?
941/tcp	status
993/tcp	imaps?
995/tcp	pop3s?
3306/tcp	mysql?
4190/tcp	sieve?
4445/tcp	upnotifyp?
4559/tcp	hylafax?

TCP Port	Service
5038/tcp	Asterisk Call Manager 1.1
10000	http

Elastix

Upon manual enumeration of the available http service, Michael noticed it was running an outdated of Elastix 2.2.0 that is prone to a local file inclusion vulnerability.

4.0.2 Initial Access - local file inclusion

Vulnerability Explanation: The Elastix 2.2.0 application plugin vtigercrm is vulnerable to a local file inclusion exploit. Attackers can use this vulnerability to read sensitive data.

Vulnerability Fix: Update to latest Elastix 5.1.0.

Severity: High

Steps to reproduce the attack: Using the following url, Michael was able to gain the root users password and login via ssh.

/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action

Proof Screenshot:

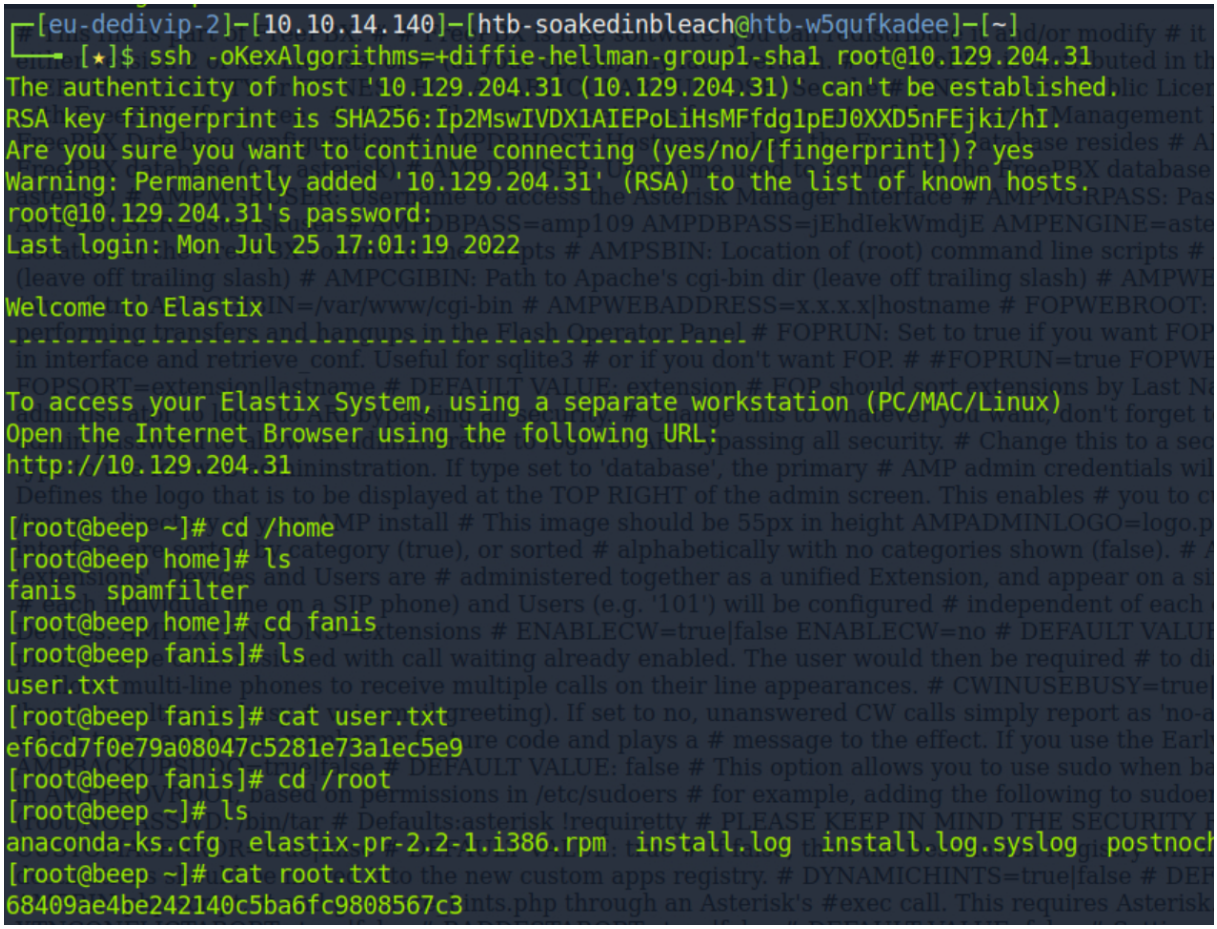

Figure 4.1: user

4.0.3 Privilege Escalation

Upon gaining access to the machine, the vulnerability allowed login as root user via ssh.