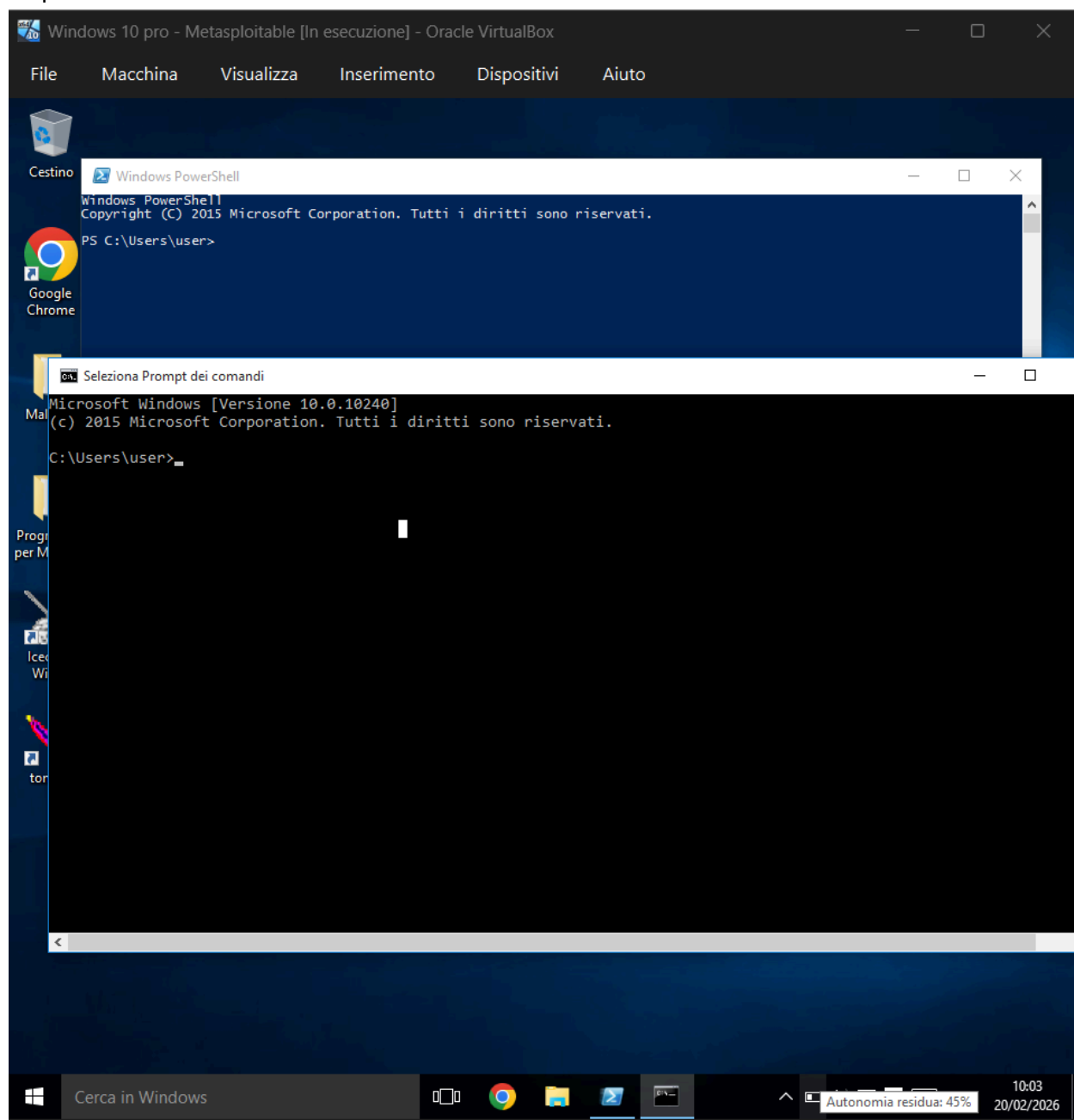


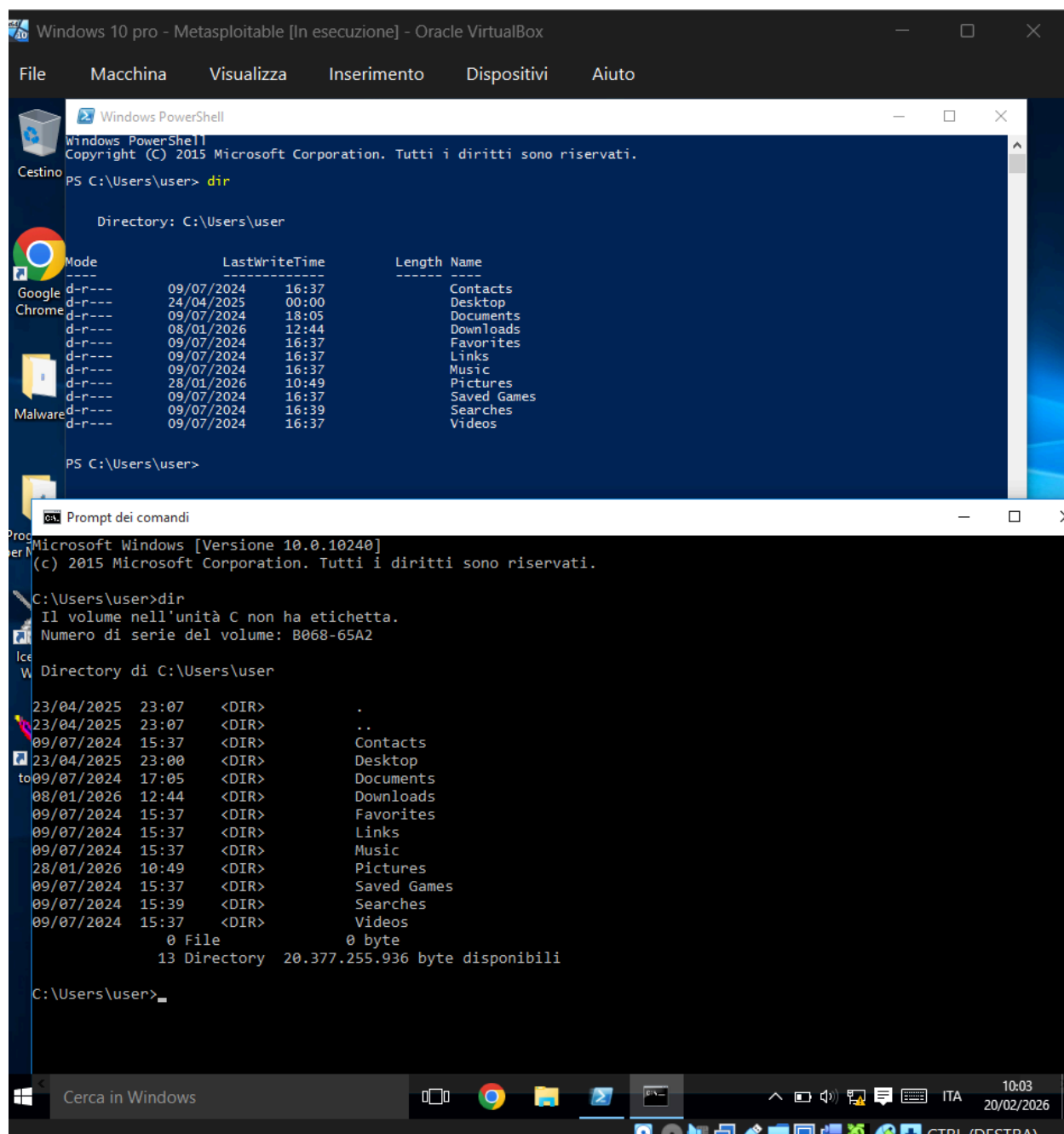
REPORT SU COME USARE WINDOWS POWERSHELL

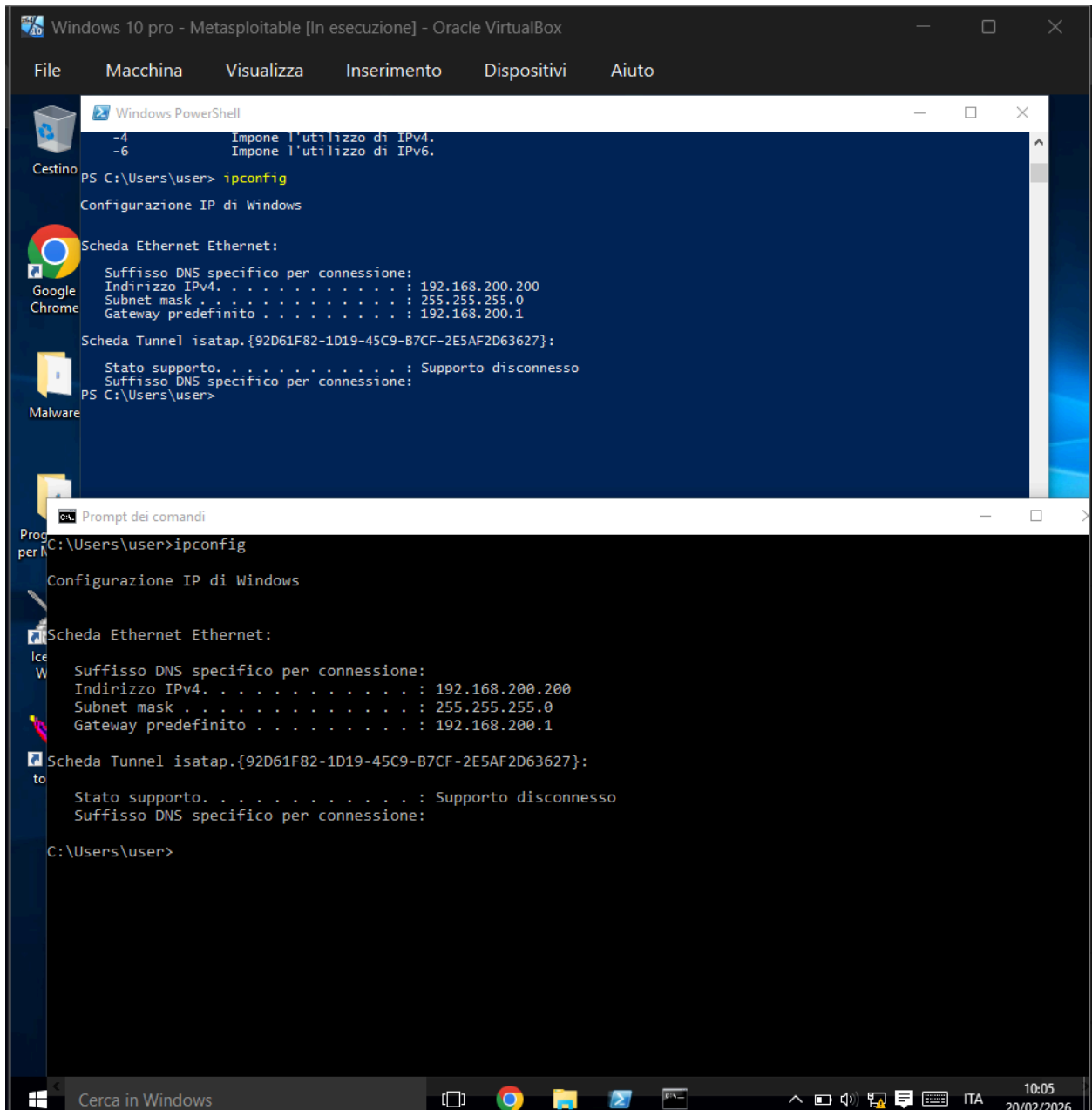
Obiettivi del laboratorio:

- 1) Accedere alla console powershell;
- 2) Esplorare i comandi del prompt dei comandi e della powershell;
- 3) Esplorare i cmdlet;
- 4) Esplorare il comando netstat usando powershell;
- 5) Svuotare il cestino usando powershell.

Risposte alle domande:







Windows PowerShell

```
PS C:\Users\user> netstat -h
```

Visualizza statistiche relative ai protocolli e alle connessioni di rete TCP/IP correnti.

```
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
```

-a	Visualizza tutte le connessioni e le porte di ascolto.
-b	Visualizza il file eseguibile utilizzato per la creazione di ogni connessione o porta di ascolto. Alcuni file eseguibili conosciuti includono più componenti indipendenti. In tali casi viene visualizzata la sequenza dei componenti utilizzati per la creazione della connessione o porta di ascolto e il nome del file eseguibile viene visualizzato in fondo, tra parentesi quadre ([]). Nella parte superiore è indicato il componente chiamato e così via, fino al raggiungimento di TCP/IP. Se si utilizza questa opzione, l'esecuzione del comando può richiedere molto tempo e riuscirà solo se si dispone di autorizzazioni sufficienti. Visualizza le statistiche Ethernet. Può essere utilizzata insieme all'opzione -s.
-e	Visualizza i nomi di dominio completi (FQDN, Fully Qualified Domain Name) per gli indirizzi esterni.
-f	Visualizza indirizzi e numeri di porta in forma numerica.
-n	Visualizza l'ID del processo proprietario associato a ogni connessione.
-o	Visualizza le connessioni relative al protocollo specificato da "proto", che può essere TCP, UDP, TCPv6 o UDPv6. Se utilizzato insieme all'opzione -s per le statistiche per protocollo, "proto" può essere: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-p proto	Visualizza tutte le connessioni, le porte di ascolto e le porte TCP non di ascolto associate. Le porte non di ascolto associate possono essere associate o meno a una connessione attiva.
-q	Visualizza la tabella di routing.
-r	Visualizza le statistiche per protocollo. Per impostazione predefinita, vengono visualizzate le statistiche per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6. Per specificare un sottoinsieme dei valori predefiniti, è possibile utilizzare l'opzione -p.
-s	Visualizza lo stato di offload della connessione corrente.
-t	Visualizza le connessioni, i listener e gli endpoint condivisi.
-x	Visualizza il modello di connessione TCP per tutte le connessioni. Non può essere utilizzata in combinazione con le altre opzioni.
-y	Ripete la visualizzazione delle statistiche selezionate, con una pausa di un numero di secondi pari a "interval"
interval	

Windows PowerShell

dopo ogni visualizzazione. Per interrompere la ripetizione della visualizzazione delle statistiche, premere CTRL+C.
Se questa opzione viene omessa, le informazioni di configurazione correnti verranno visualizzate una volta sola.

```
PS C:\Users\user> netstat -r
```

=====

Elenco interfacce

```
4...08 00 27 64 80 4c .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
6...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
```

=====

IPv4 Tabella route

Route attive:

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.200	11
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.200.0	255.255.255.0	On-link	192.168.200.200	266
192.168.200.200	255.255.255.255	On-link	192.168.200.200	266
192.168.200.255	255.255.255.255	On-link	192.168.200.200	266
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.200.200	266
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	192.168.200.200	266

=====

Route permanenti:

Indirizzo rete	Mask	Indir. gateway	Metrica
0.0.0.0	0.0.0.0	192.168.200.1	1

=====

IPv6 Tabella route

Route attive:

Interf	Metrica	Rete	Destinazione	Gateway
1	306	::1/128		On-link
1	306	ff00::/8		On-link

=====

Route permanenti:

Nessuna

```
PS C:\Users\user>
```

Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox

Macchina Visualizza Inserimento Dispositivi Aiuto

Amministratore: Windows PowerShell

Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Windows\system32> netstat -abno

Connessioni attive

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:7	0.0.0.0:0	LISTENING	2220
[tcpvcs.exe]				
TCP	0.0.0.0:9	0.0.0.0:0	LISTENING	2220
[tcpvcs.exe]				
TCP	0.0.0.0:13	0.0.0.0:0	LISTENING	2220
[tcpvcs.exe]				
TCP	0.0.0.0:17	0.0.0.0:0	LISTENING	2220
[tcpvcs.exe]				
TCP	0.0.0.0:19	0.0.0.0:0	LISTENING	2220
[tcpvcs.exe]				
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4

Gestione attività

File Opzioni Visualizza

Processi Prestazioni Cronologia applicazioni Avvio Utenti Dettagli Servizi

Nome	PID	Stato	Nome ute...	CPU	Memoria (...)	Descrizione
Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K	Chiamate di procedura differite e ISR (Interrupt Service Routi...
Processo di inattività...	0	In esecuzione	SYSTEM	91	4 K	Percentuale di tempo di inattività del processore
System	4	In esecuzione	SYSTEM	01	5.712 K	NT Kernel & System
smss.exe	268	In esecuzione	SYSTEM	00	76 K	Gestione sessioni di Windows
svchost.exe	300	In esecuzione	SYSTEM	00	24.084 K	Processo host per servizi di Windows
csrss.exe	352	In esecuzione	SYSTEM	00	428 K	Processo runtime client server
wininit.exe	428	In esecuzione	SYSTEM	00	264 K	Applicazione di avvio di Windows
csrss.exe	444	In esecuzione	SYSTEM	00	452 K	Processo runtime client server
winlogon.exe	504	In esecuzione	SYSTEM	00	476 K	Applicazione Accesso a Windows
services.exe	544	In esecuzione	SYSTEM	00	1.604 K	App Servizi e Controller
lsass.exe	552	In esecuzione	SYSTEM	01	1.712 K	Local Security Authority Process
svchost.exe	608	In esecuzione	user	00	1.028 K	Processo host per servizi di Windows
VBBoxService.exe	616	In esecuzione	SYSTEM	00	656 K	VirtualBox Guest Additions Service
svchost.exe	636	In esecuzione	SYSTEM	00	2.608 K	Processo host per servizi di Windows
svchost.exe	688	In esecuzione	SERVIZIO ...	00	2.068 K	Processo host per servizi di Windows
dwm.exe	796	In esecuzione	DWM-1	00	21.924 K	Gestione finestre desktop
svchost.exe	876	In esecuzione	SERVIZIO ...	00	3.532 K	Processo host per servizi di Windows
svchost.exe	888	In esecuzione	SYSTEM	03	8.784 K	Processo host per servizi di Windows
svchost.exe	904	In esecuzione	SERVIZIO L...	02	6.208 K	Processo host per servizi di Windows
powershell.exe	920	In esecuzione	user	00	43.156 K	Windows PowerShell
svchost.exe	952	In esecuzione	SERVIZIO L...	00	700 K	Processo host per servizi di Windows
svchost.exe	1056	In esecuzione	SERVIZIO L...	00	2.184 K	Processo host per servizi di Windows
WmiPrvSE.exe	1144	In esecuzione	SYSTEM	00	1.524 K	WMI Provider Host

Meno dettagli

Termina attività

Cerca in Windows

ITA 10:12

