

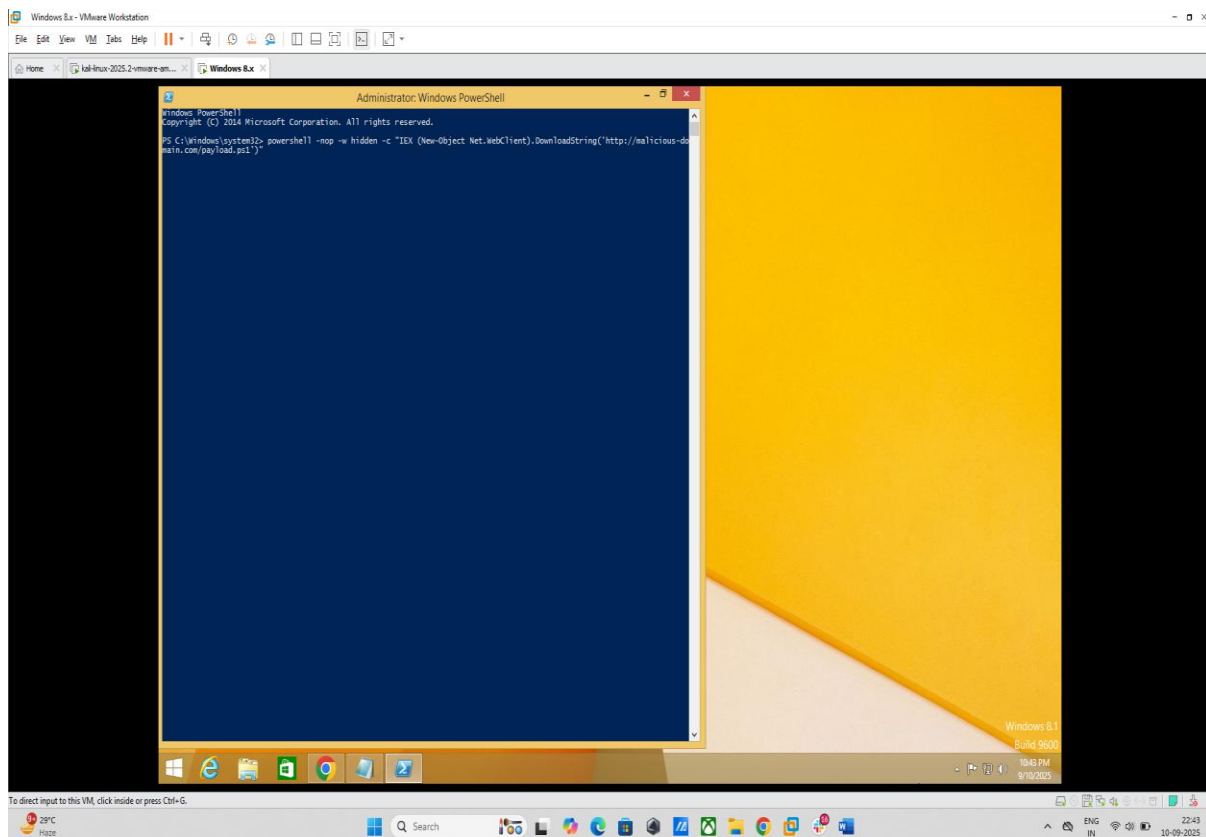


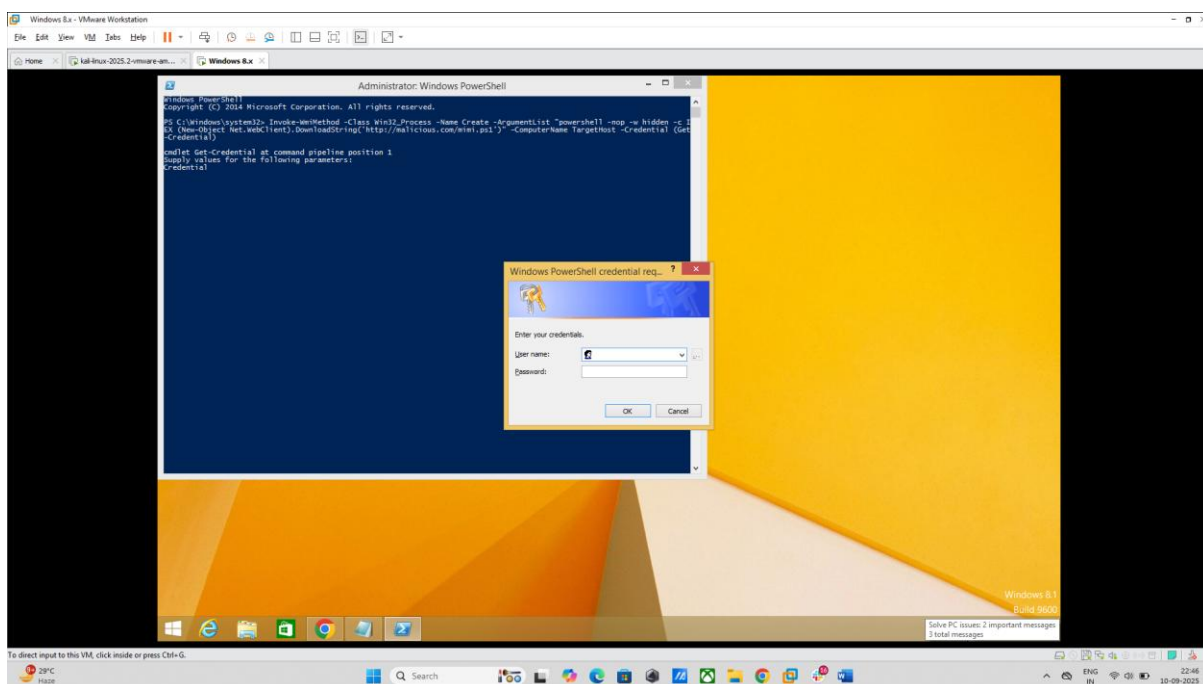
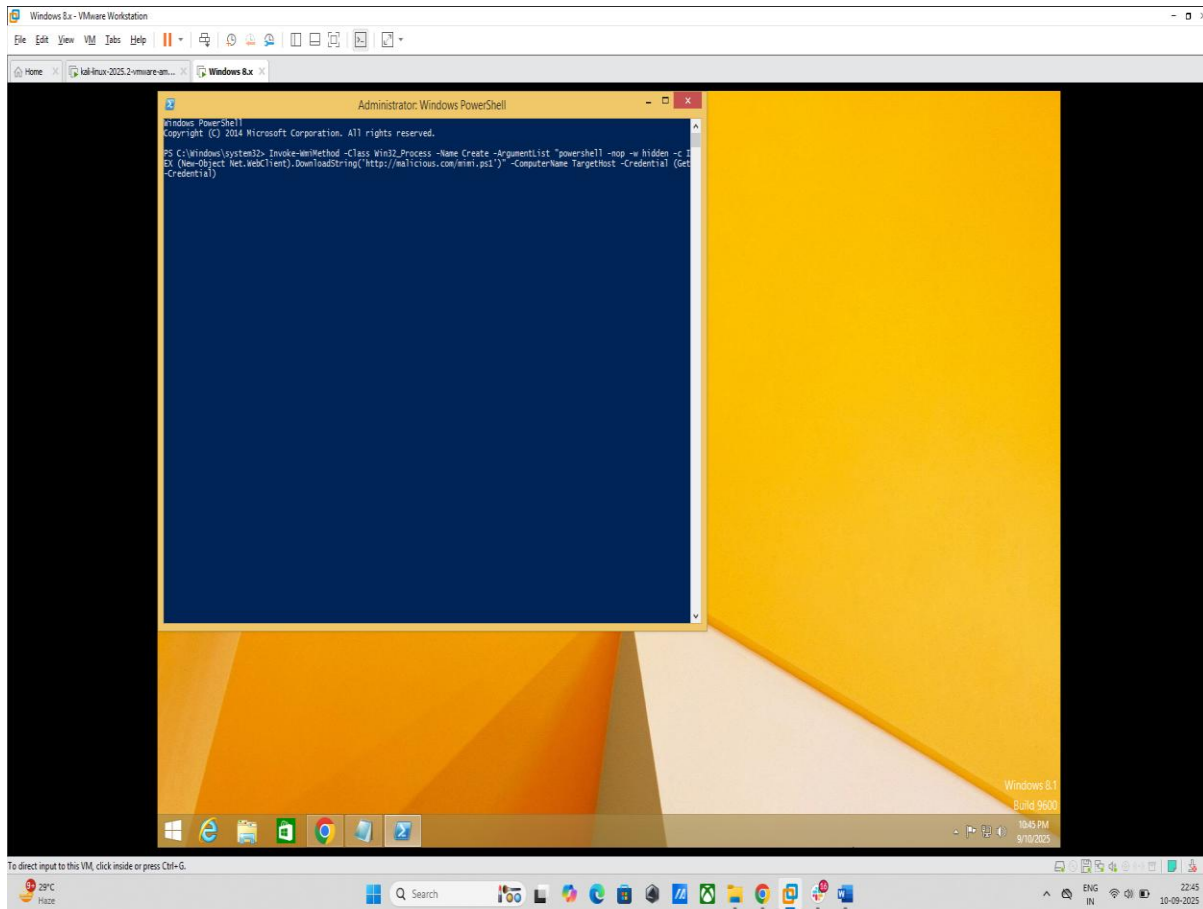
7. Living-Off-the-Land Lab

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







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

The screenshot shows a Windows 8.1 virtual machine running in VMware Workstation. An Administrator PowerShell window is open, displaying the command `Get-WmiObject -Class Win32_Process | Where-Object { $_.Name -eq "lsass.exe" }`. The output lists detailed WMI properties for the `lsass.exe` process, including its parent process (`csrss.exe`), command line, and various system metrics. The background shows the Windows 8.1 desktop with the Start button and taskbar.

```
PS C:\Windows\system32> Get-WmiObject -Class Win32_Process | Where-Object { $_.Name -eq "lsass.exe" }

__GENUS                : 2
__CLASS                 : Win32_Process
__SUPERCLASS            : CIM_Process
__DYNASTY               : CIM_ManagedSystemElement
__PATH                 : Win32_Process.Handle=488
__PROPERTY_COUNT        : 45
__DERIVATION            : CIM_Process, CIM_LogicalElement, CIM_ManagedSystemElement
SERVER                 : WIN-T209VIXDEH1
__NAMESPACE             : root\cimv2
__PATH                 : \\WIN-T209VIXDEH1\root\cimv2:Win32_Process.Handle="488"
Caption                 : lsass.exe
Commandline             : C:\Windows\system32\lsass.exe
CreationClassName       : Win32_Process
CreationDate            : 2020090222245.731194+330
CSCreationClassName     : Win32_ComputerSystem
CSName                  : WIN-T209VIXDEH1
Description              : lsass.exe
ExecutablePath          : C:\Windows\system32\lsass.exe
ExecutionState          :
Handle                  : 488
HandleCount             : 681
InstallDate             :
KernelModeTime          : 1406250
MaximumWorkingSetSize   : 1380
MinimumWorkingSetSize   : 200
Name                    : lsass.exe
OSCreationClassName     : Win32_OperatingSystem
OSName                  : Microsoft Windows 8.1[C:\Windows\Device\Harddisk0\Partition1]
OtherOperationCount      : 1050
OtherTransferCount       : 1009882
PageFaults              : 2720
PageFileUsage           : 5624
ParentProcessId         : 392
PeakPageFileUsage       : 2876
PeakVirtualSize         : 6921648
PeakWorkingSetSize       : 6692
Priority                 : 9
PrivatePageCount        : 2688976
ProcessId               : 488
QuotaNonPagedPoolUsage  : 11
QuotaPagedPoolUsage     : 76
QuotaPeakNonPagedPoolUsage : 11
QuotaPeakPagedPoolUsage : 76
ReadOperationCount       : 40
ReadTransferCount        : 5130
SessionId               : 0
Status                  :
TerminationDate         :
ThreadCount             : 6
UserModeTime            : 2968750
VirtualSize             : 6768868
WorkingSetSize           : 6750008
WriteOperationCount      : 27
WriteTransferCount       : 43890
PSComputerName           : WIN-T209VIXDEH1
ProcessName              : lsass.exe
Handles                 : 631
VM                       : 6768868
AS                       : 6750208
Path                    : C:\Windows\system32\lsass.exe
```

Summary:

The attacker utilized WMI to harvest credentials by remotely executing Mimikatz in memory, bypassing file-based detection.

This approach used inherent Windows functionality to start processes without writing to disk. Using WMI and in-memory execution, the attacker circumvented standard security protections while stealing credentials from the target system.