

# COMMAND PROMPT

## OBJECTIVE

The objective of this report is to demonstrate the importance of command prompt in cyber security. Command Prompt, also known as cmd.exe or cmd, is the default command-line interpreter for the OS/2, eComStation, ArcaOS, Microsoft Windows (Windows NT family and Windows CE family), and ReactOS[2] operating systems.

## TOOLS

The tool we require is command prompt. Command Prompt is a command line interpreter application available in most Windows operating systems. It is used to execute entered commands. Most of those commands automate tasks via scripts and batch files, perform advanced administrative functions, and troubleshoot or solve certain kinds of Windows issues.

On Windows CE .NET 4.2, Windows CE 5.0 and Windows Embedded CE 6.0 it is referred to as the Command Processor Shell.

Its implementations differ between operating systems, but the behavior and basic set of commands are consistent. cmd.exe is the counterpart of COMMAND.COM in DOS and Windows 9x systems, and analogous to the Unix shells used on Unix-like systems.

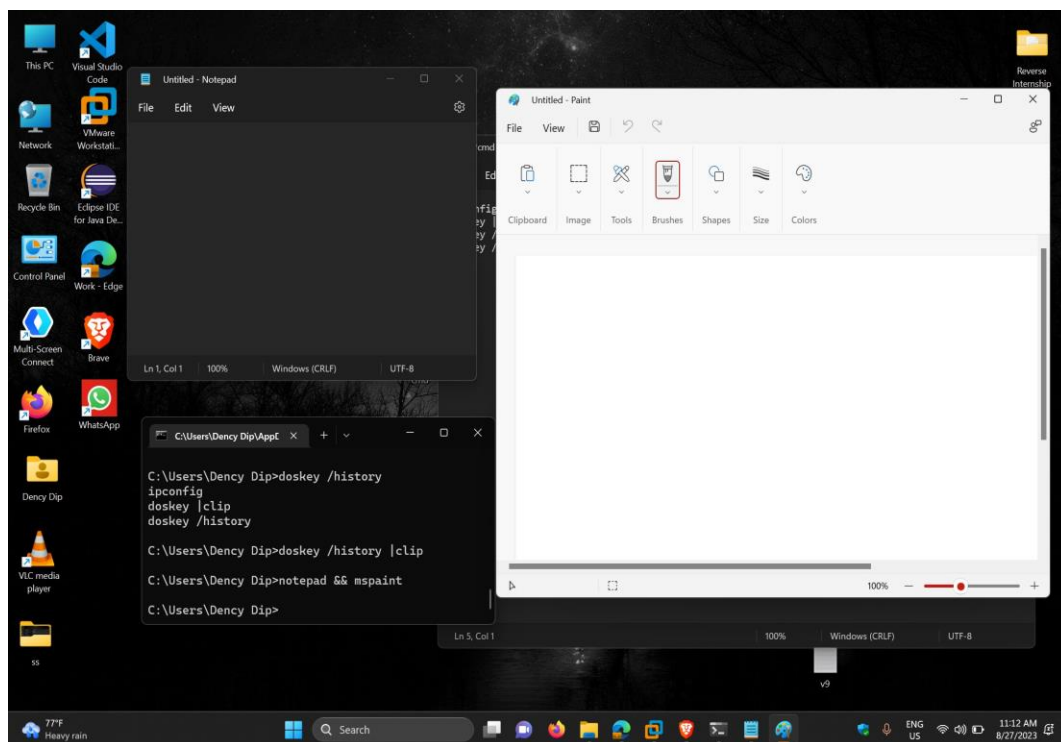
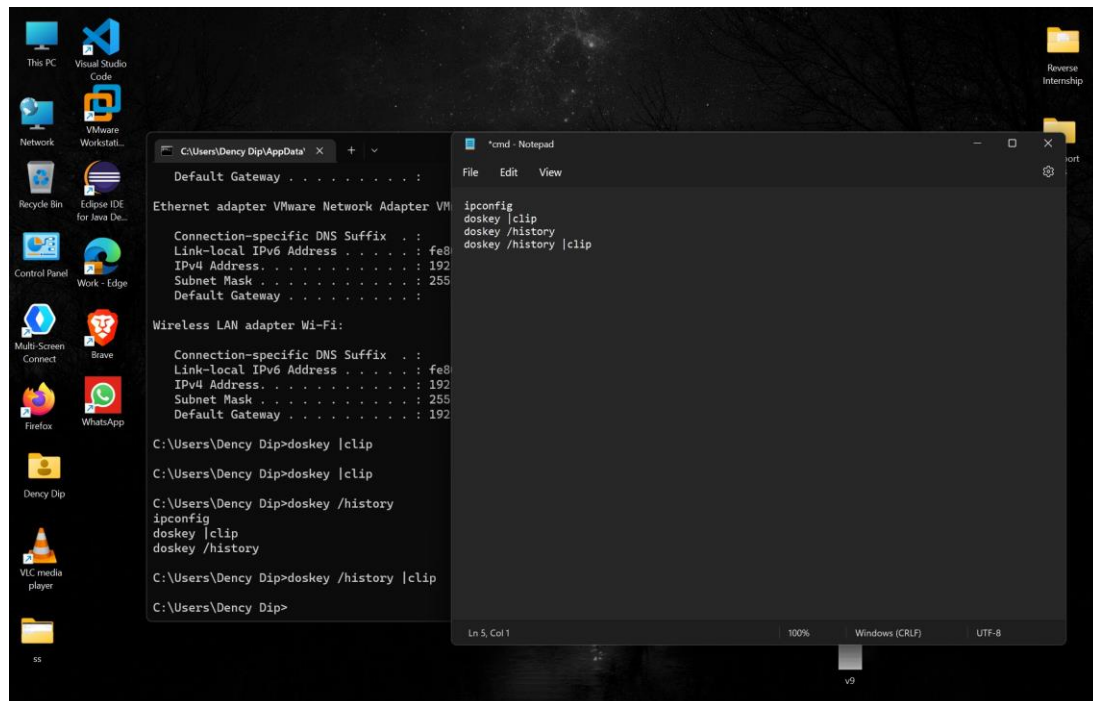
## METHODOLOGY

The steps are to type in or run various commands that will help us in hacking in a targeted system.

The various commands we used for demonstration purposes are **doskey /history**, **doskey /history |clip**, **dir /?**, **netsh wlan show profile**, **netstat**, **ipconfig**, and **tracert**. We can also use many more commands using the command prompt window.

The steps are demonstrated in the screen shots given below.

# PROOF OF CONCEPT



```
C:\Users\Dency Dip\AppData\> + v
C:\Users\Dency Dip>doskey |clip
C:\Users\Dency Dip>doskey |clip
C:\Users\Dency Dip>doskey /history
ipconfig
doskey |clip
doskey /history
C:\Users\Dency Dip>doskey /history |clip
C:\Users\Dency Dip>notepad && mspaint
C:\Users\Dency Dip>dir /?
Displays a list of files and subdirectories in a directory.

] [/B] [/C] [/D] [/L] [/N]
 [/O[[:sortorder]]] [/P] [/Q] [/R] [/S] [/T[[:timefield]]] [/W] [/X] [/4]

[drive:][path][filename]
Specifies drive, directory, and/or files to list.

/A Displays files with specified attributes.
Press any key to continue . . . |
```

```
C:\Users\Dency Dip\AppData\> + v
Profile Smile on interface Wi-Fi:
=====

Applied: All User Profile

Profile information
-----
Version      : 1
Type         : Wireless LAN
Name         : Smile
Control options
:
Connection mode : Connect automatically
Network broadcast : Connect only if this network is broadcasting
AutoSwitch      : Do not switch to other networks
MAC Randomization : Enabled

Connectivity settings
-----
Number of SSIDs : 1
SSID name       : "Smile"
Network type    : Infrastructure
Radio type      : [ Any Radio Type ]
Vendor extension : Not present

Security settings
-----
Authentication : WPA2-Personal
Cipher         : CCMP
Authentication : WPA2-Personal
Cipher         : GCMP
Security key    : Present
Key Content     : DencyDip@147

Cost settings
-----
Cost           : Unrestricted
Congested      : No
Approaching Data Limit : No
Over Data Limit : No
Roaming        : No
Cost Source     : Default

C:\Users\Dency Dip>|
```

77°F Heavy rain

Search

ENG US 11:16 AM 8/27/2023

```
C:\Users\Dency Dip\AppData\Local\Microsoft\Windows\Terminal>
-----
Cost                : Unrestricted
Congested           : No
Approaching Data Limit : No
Over Data Limit     : No
Roaming             : No
Cost Source         : Default

C:\Users\Dency Dip>tracert www.google.com

Tracing route to www.google.com [142.251.42.36]
over a maximum of 30 hops:
  0  1 ms    1 ms    2 ms  192.168.0.1
  1  4 ms    2 ms    1 ms  192.168.1.1
  2  6 ms    4 ms    6 ms  103.57.86.9
  3  *      84 ms   4 ms  103.57.86.1
  4  17 ms   31 ms   57 ms  103.57.86.50
  5  15 ms   15 ms   15 ms  142.250.166.160
  6  17 ms   17 ms   16 ms  72.14.239.103
  7  29 ms   15 ms   15 ms  142.251.69.45
  8  *      19 ms   16 ms  bom12s20-in-f4.1e100.net [142.251.42.36]

Trace complete.

C:\Users\Dency Dip>netstat

Active Connections
Proto Local Address           Foreign Address         State
TCP    127.0.0.1:5354           DencyDip:49669         ESTABLISHED
TCP    127.0.0.1:5354           DencyDip:49671         ESTABLISHED
TCP    127.0.0.1:49669         DencyDip:5354          ESTABLISHED
TCP    127.0.0.1:49671         DencyDip:5354          ESTABLISHED
TCP    127.0.0.1:49798         DencyDip:49799         ESTABLISHED
TCP    127.0.0.1:49799         DencyDip:49798         ESTABLISHED
TCP    127.0.0.1:49803         DencyDip:49804         ESTABLISHED
TCP    127.0.0.1:49804         DencyDip:49803         ESTABLISHED
TCP    127.0.0.1:49805         DencyDip:49806         ESTABLISHED
TCP    127.0.0.1:49806         DencyDip:49805         ESTABLISHED
TCP    127.0.0.1:49820         DencyDip:49821         ESTABLISHED
TCP    127.0.0.1:49821         DencyDip:49820         ESTABLISHED
```

## CONCLUSION

In conclusion, it can be said that command prompt is an essential and powerful tool that can be used for hacking devices.