Report: Advanced C2 lab

Objective

Set up a C2 infrastructure, manage sessions, customize payloads.

- C2 Setup: Configure a poshC2 HTTPS beacon in a lab. Establish a session with a Windows VM.
- Payload Customization: Generate a stageless PowerShell beacon

Tool Used:

PowerShell, PoshC2

Kali Linux: 192.168.1.58

Windows VM: 192.168.1.46

Methodology

Use Metasploit for initial access and Poshc2 for post-exploitation

Launch Kali Terminal and send payload.exe to Windows using msfvenom and scp.

Fig 1.1 Making and sending payload to windows

Now launch msfconsole and execute the following handler. After the exploit executes, launch the payload on Windows and create a Metasploit session.

Fig1.2 Metasploit getting access of windows vm

Now next Powershell beacon download poshc2 from github and install it.

After that make a new project command

Posh-project -n hello

Now configure the poshc2 config file by adding the Ip and port.

Fig 1.3 Poshc2 configuration

Now run the poshc2 by command

Posh-service

Fig 1.4 PoshC2 server

After open the raw payload file and add the port after the IP. Payload file you find in /var/poshc2/hello/payloads

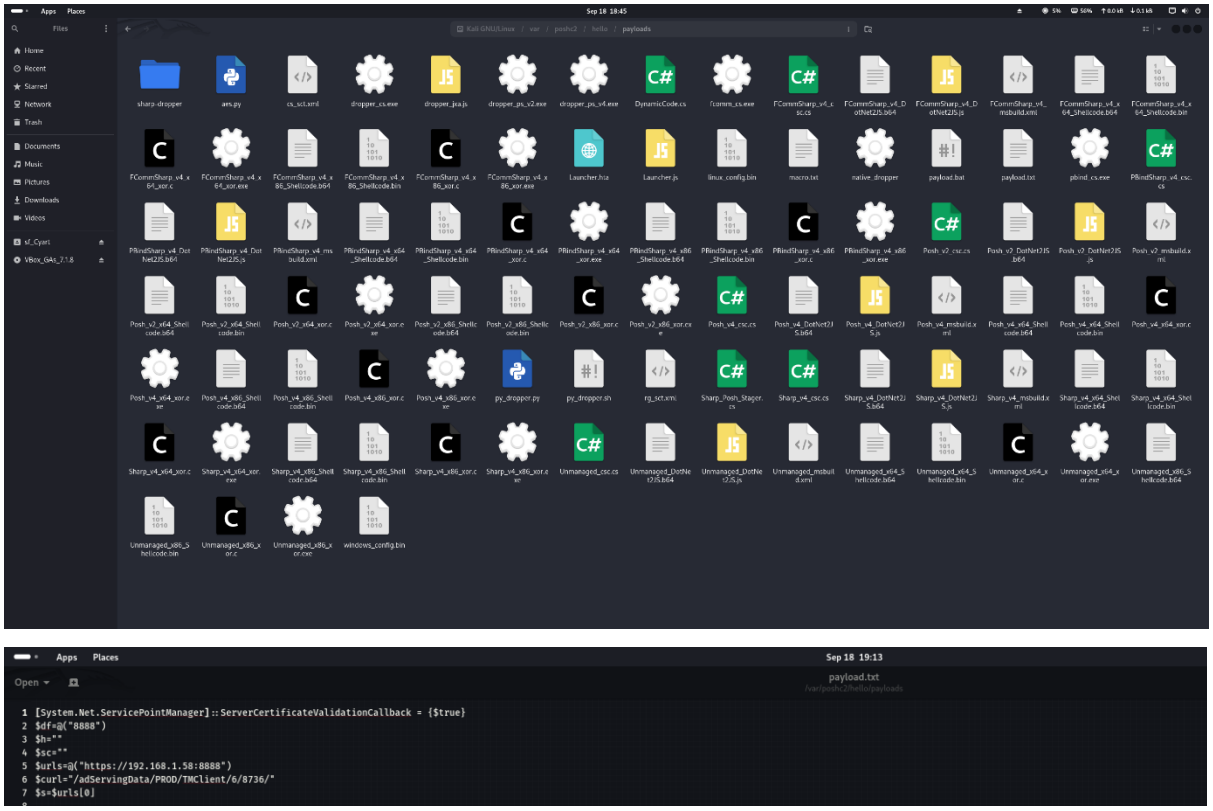

Fig 1.5 Payload.txt file and add port number after IP

Now copy the payload.txt content and paste it on powershell admin.

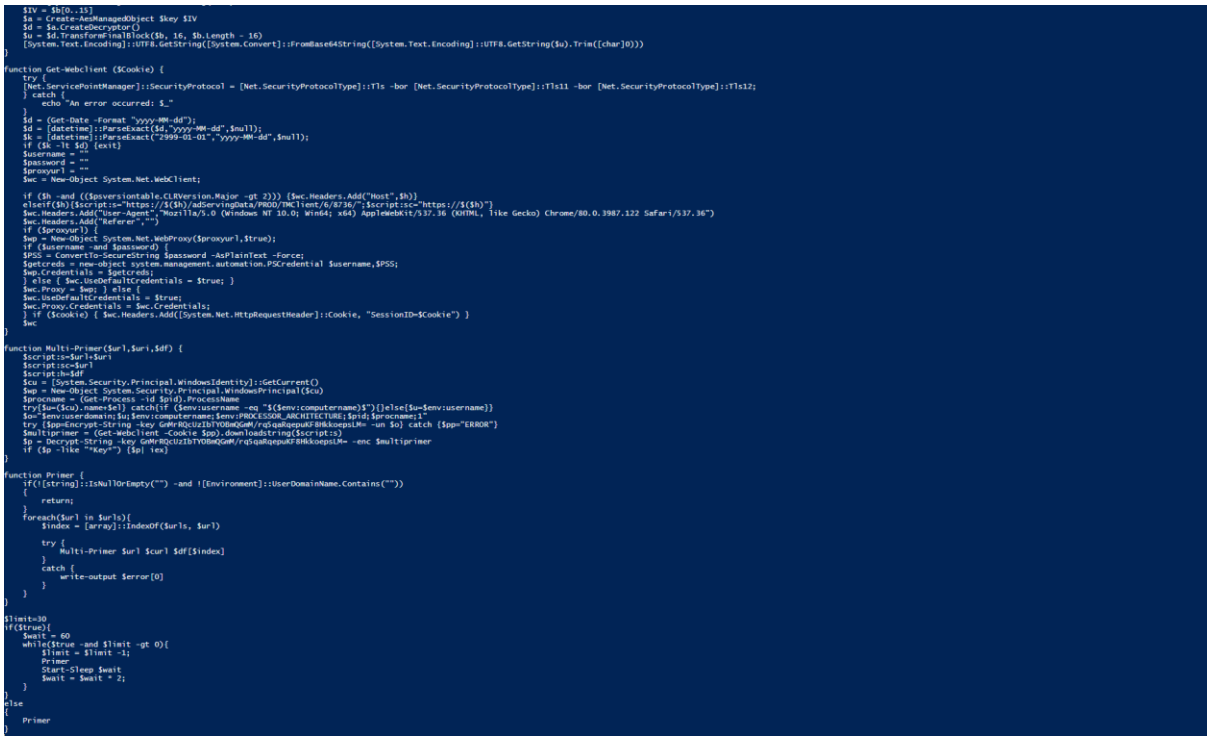

Fig 1.6 Payload content in powershell

A session is established on Poshc2 in Kali.

Fig 1.7 Connection established

Now open implementer by command

posh

And enter the project name and implant ID.

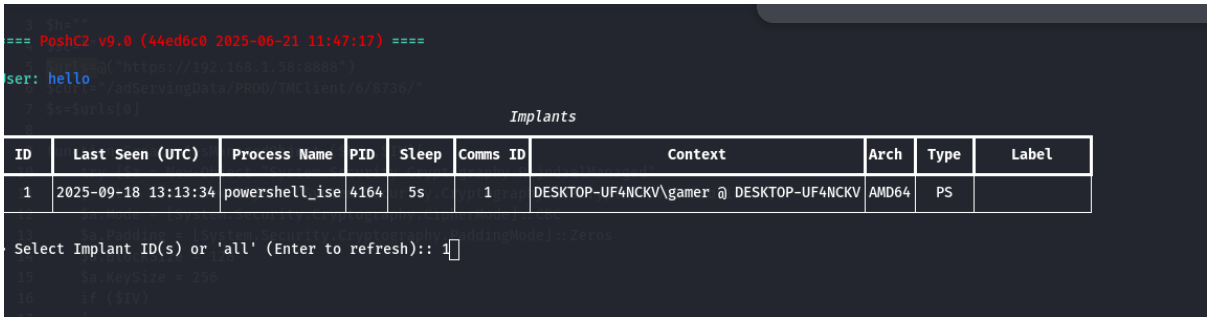

Fig 1.8 Poshc2 implanter

Task ID	PID	Target IP	Payload Type
00001	4164	192.168.1.46	Powershell

A stageless PowerShell beacon was deployed to a Windows virtual machine, and the PoshC2 server was set up on a Kali virtual machine. Payload created a session with the C2. Through HTTP communication, payloads enable module deployment, command execution, and monitoring. The server console is used to manage and log sessions.