CWL
CyberWarFare Labs

Getting Started with Havoc C2: Installation & Payload Creation

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has these primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform
3. Infinity Learning Platform

CWL provides customized on-site training for organizations and accepts bulk orders for corporate upskilling. For inquiries or more details, feel free to reach out at **support@cyberwarfare.live.**

About Speaker

SUBASHINI BALAJI

(Security Consultant)

Subashini Balaji is a Security Consultant at CyberWarFare Labs, specializing in Red Teaming and APT simulations in enterprise environments. She also writes technical blogs and articles focused on real-world cyber attack techniques and defenses.

Agenta

- What is Command & Control (C2)
- Introduction to Havoc C2
- Havoc Architecture
- Teamserver & client in havoc
- Lab setup for this demo
- Installing Havoc
- Demo in real time & generate a payload
- Conclusion

What is Command & Control (C2)?

Command & Control (C2) is a communication channel used by attackers or red teams to control compromised machines remotely.

Key purposes:

- Execute commands remotely
- Maintain access to systems
- Transfer data
- Run post-exploitation actions

Examples of C2 Frameworks: Cobalt Strike, Sliver, Metasploit, Havoc

Introduction to Havoc C2

Havoc is a modern open-source Command & Control framework designed for red team operations.

Key Features:

- Modern UI
- Modular architecture
- Payload generation
- Multiple listeners
- Post-exploitation capabilities
- Active development community

Link: Havoc Framework, Havoc Github

Havoc Architecture

Havoc works using two main components:

1. Teamserver

- Central server
- Handles payload connections
- Manages communication with agents

2. Client

- Operator interface
- Used by red teamers
- Sends commands to compromised hosts

Workflow:

- Client → Teamserver → Agent (Victim Machine)

Teamserver & Client in Havoc

Teamserver

- The main server of Havoc
- Manages connections from agents (compromised machines)
- Sends commands and controls operations
- Handles listeners and sessions

Client

- The interface used by the operator (red teamer)
- Connects to the Teamserver
- Used to create listeners and generate payloads
- Allows sending commands to agents

Lab Setup for This Demo

Environment used in this webinar:

1. Attacker Machine: Kali Linux
2. Target Machine: Windows VM
3. Network: Internal lab network

Tools Required:

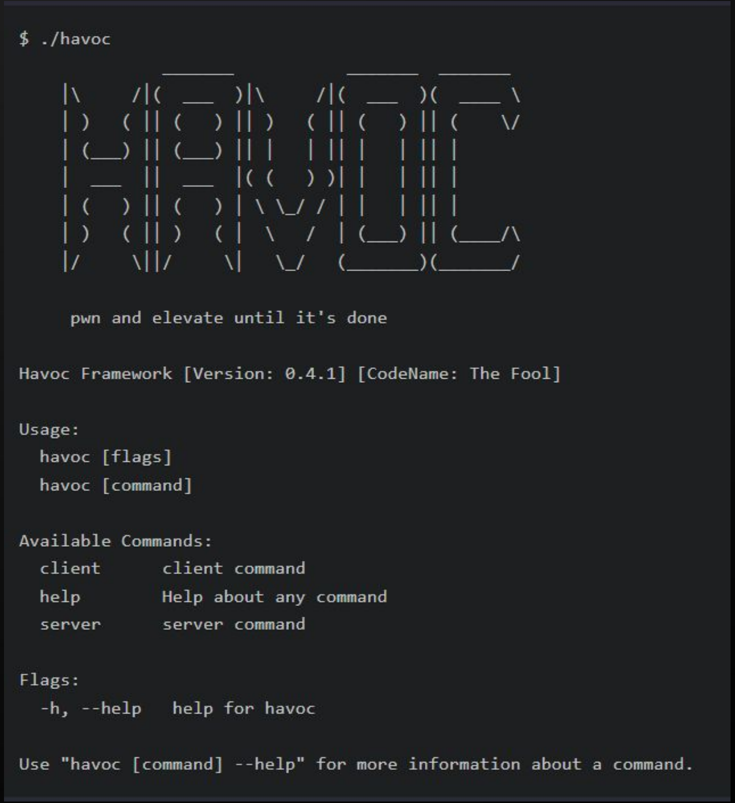
- Git
- Golang
- Havoc Framework

Installing Havoc

Basic installation steps:

- Clone the Havoc repository
- Install required dependencies
- Build the teamserver
- Build the client interface

Link: [Installation of Havoc]



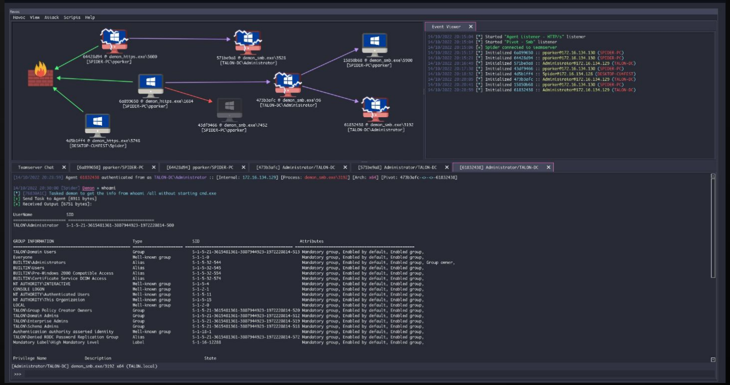
```
$ ./havoc

              _______           _______  _______
    |\     /|(  ___  )|\     /|(  ___  )(  ____ \
    | )   ( || (   ) || )   ( || (   ) || (    \/
    | (___) || (___) || |   | || |   | || |
    |  ___  ||  ___  |( (   ) )| |   | || |
    | (   ) || (   ) | \ \_/ / | |   | || |
    | )   ( || )   ( |  \   /  | (___) || (____/\
    |/     \||/     \|   \_/   (_______)(_______/

     pwn and elevate until it's done

Havoc Framework [Version: 0.4.1] [CodeName: The Fool]

Usage:
  havoc [flags]
  havoc [command]

Available Commands:
  client      client command
  help        Help about any command
  server      server command

Flags:
  -h, --help   help for havoc

Use "havoc [command] --help" for more information about a command.
```

Demo in real time & generate a payload

In this section, we will perform a live demonstration of Havoc C2 in a controlled lab environment.

Steps in the demo:

- Start the Havoc Teamserver
- Connect using the Havoc Client
- Configure a listener
- Generate a payload
- Execute the payload on the target machine
- Observe the agent connection in real time



Havoc
Havoc View Attack Scripts Help
64428d94 @ demon_https.exe\5600
[SPIDER-PC\pparker]
571be9a8 @ demon_smb.exe\3528
[TALON-DC\Administrator]
15850b68 @ demon_smb.exe\5900
[SPIDER-PC\pparker]
6a899650 @ demon_https.exe\1684
[SPIDER-PC\pparker]
473b3afc @ demon_smb.exe\96
[TALON-DC\Administrator]
43df9466 @ demon_smb.exe\7452
[SPIDER-PC\pparker]
61832438 @ demon_smb.exe\3192
[TALON-DC\Administrator]
4d5b1ff4 @ demon_https.exe\5748
[DESKTOP-CU4FEST\Spider]
Event Viewer
Teamserver Chat
[6a899650] pparker/SPIDER-PC
[64428d94] pparker/SPIDER-PC
[473b3afc] Administrator/TALON-DC
[571be9a8] Administrator/TALON-DC
[61832438] Administrator/TALON-DC

```
14/10/2022 20:15:04 [*] Started "Agent Listener - HTTP/s" listener
14/10/2022 20:15:04 [*] Started "Pivot - Smb" listener
14/10/2022 20:15:06 [+] Spider connected to teamserver
14/10/2022 20:15:17 [*] Initialized 6a899650 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:15:21 [*] Initialized 64428d94 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:16:49 [*] Initialized 571be9a8 :: Administrator@172.16.134.129 (TALON-DC)
14/10/2022 20:17:38 [*] Initialized 43df9466 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:18:32 [*] Initialized 4d5b1ff4 :: Spider@172.16.134.128 (DESKTOP-CU4FEST)
14/10/2022 20:20:05 [*] Initialized 473b3afc :: Administrator@172.16.134.129 (TALON-DC)
14/10/2022 20:20:41 [*] Initialized 15850b68 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:28:59 [*] Initialized 61832438 :: Administrator@172.16.134.129 (TALON-DC)
```

```
[14/10/2022 20:28:59] Agent 61832438 authenticated from as TALON-DC\Administrator :: [Internal: 172.16.134.129] [Process: demon_smb.exe\3192] [Arch: x64] [Pivot: 473b3afc-<>-<>-61832438]

14/10/2022 20:30:00 [Spider] Demon » whoami
[*] [76830A1C] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [6911 bytes]
[+] Received Output [6751 bytes]:

UserName              SID
===================== ===============================================
TALON\Administrator   S-1-5-21-3615481361-3807944923-1972220814-500


GROUP INFORMATION                               Type                SID                                            Attributes
=============================================== =================== ============================================== ===============================================
TALON\Domain Users                              Group               S-1-5-21-3615481361-3807944923-1972220814-513 Mandatory group, Enabled by default, Enabled group,
Everyone                                        Well-known group    S-1-1-0                                        Mandatory group, Enabled by default, Enabled group,
BUILTIN\Administrators                          Alias               S-1-5-32-544                                   Mandatory group, Enabled by default, Enabled group, Group owner,
BUILTIN\Users                                   Alias               S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group,
BUILTIN\Pre-Windows 2000 Compatible Access      Alias               S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group,
BUILTIN\Certificate Service DCOM Access         Alias               S-1-5-32-574                                   Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\INTERACTIVE                        Well-known group    S-1-5-4                                        Mandatory group, Enabled by default, Enabled group,
CONSOLE LOGON                                   Well-known group    S-1-2-1                                        Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\Authenticated Users                Well-known group    S-1-5-11                                       Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\This Organization                  Well-known group    S-1-5-15                                       Mandatory group, Enabled by default, Enabled group,
LOCAL                                           Well-known group    S-1-2-0                                        Mandatory group, Enabled by default, Enabled group,
TALON\Group Policy Creator Owners               Group               S-1-5-21-3615481361-3807944923-1972220814-520 Mandatory group, Enabled by default, Enabled group,
TALON\Domain Admins                             Group               S-1-5-21-3615481361-3807944923-1972220814-512 Mandatory group, Enabled by default, Enabled group,
TALON\Enterprise Admins                         Group               S-1-5-21-3615481361-3807944923-1972220814-519 Mandatory group, Enabled by default, Enabled group,
TALON\Schema Admins                             Group               S-1-5-21-3615481361-3807944923-1972220814-518 Mandatory group, Enabled by default, Enabled group,
Authentication authority asserted identity      Well-known group    S-1-18-1                                       Mandatory group, Enabled by default, Enabled group,
TALON\Denied RODC Password Replication Group    Alias               S-1-5-21-3615481361-3807944923-1972220814-572 Mandatory group, Enabled by default, Enabled group,
Mandatory Label\High Mandatory Level            Label               S-1-16-12288                                   Mandatory group, Enabled by default, Enabled group,


Privilege Name            Description                              State
[Administrator/TALON-DC] demon_smb.exe/3192 x64 (TALON.local)
>>>
```

This demonstrates how a Command & Control framework establishes communication with a compromised system.

Conclusion

In this session, we learned the basics of Havoc C2 and how it is used in red team operations.

Key takeaways:

- Understanding the Teamserver and Client
- Installing and setting up Havoc
- Configuring a listener
- Generating and testing a payload

This hands-on approach helps security professionals understand how attackers operate and how such activities can be detected and defended against.

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **cyberwarfare.live**