METASPLOIT FRAMEWORK PRIMER

Null-OWASP Bangalore

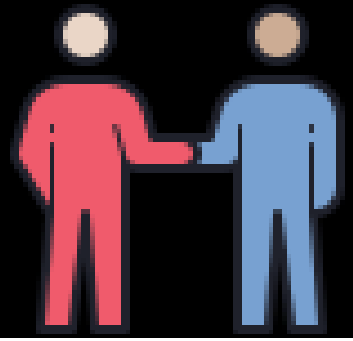
18th January, 2020

AGENDA

- Introduction
- Scenario
- Definitions
- Msfconsole
- Demo
- Sources
- QnA

INTRODUCTION

Created in 2003 by HD Moore
Open Source
Automates assessments
Pentester's Swiss Chainsaw
Vulnerability Research
Modular & customizable
Multiple Attack Vectors
Used by Red & Blue Teamers and alike



metasploit®

DEFINITIONS

- Vulnerability –

  "weakness in a system allowing an attacker to violate the confidentiality, integrity, availability, access control, consistency or audit mechanisms of the system or the data and applications it hosts"

- Exploit –

  “a software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.”

- Payload –

  “an explosive warhead carried by an aircraft or missile.”

  “piece of code to be executed through said exploit”

- Penetration Testing –

  “practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.”

- Modules –

  “piece of software that the Metasploit Framework uses to perform a task, such as exploiting or scanning a target. A module can be an exploit module, auxiliary module, or post-exploitation module.”

- Remote Code/Command Execution –

  "…an attacker is able to run **code/command** of their own, choosing with system level privileges on a server that possesses the appropriate weakness."

- Backdoor –

  "covert method of bypassing normal authentication or encryption"

  "secret portal that hackers and intelligence agencies use to gain illicit access."

Exploit = Vulnerability + Payload

SCENARIO

ag3ntggwp, you're given a task.

You have to test an entire subnet, enumerate the running services, look out for exploits that are public and any of the services that are vulnerable. Once you confirm, you also need to show a Proof of Concept.

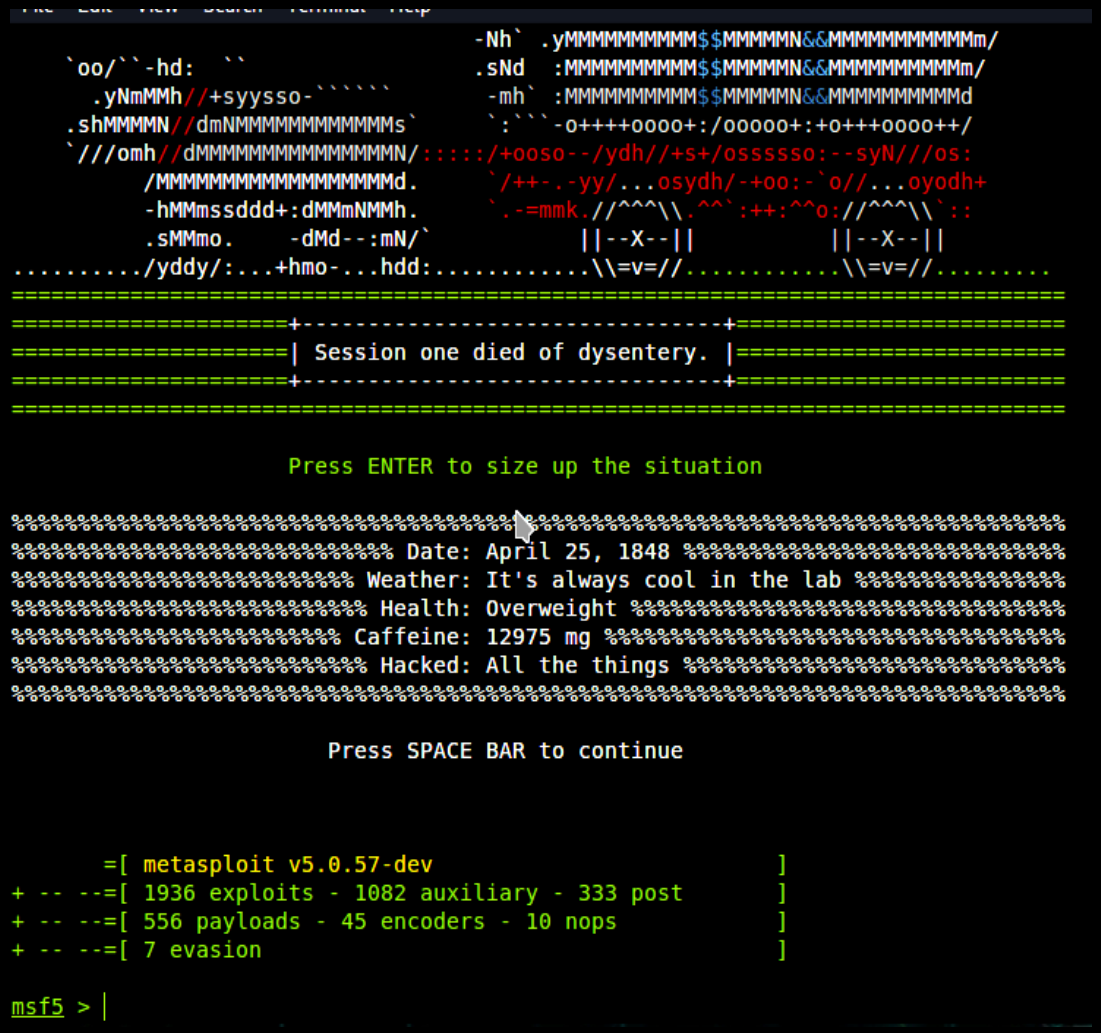
Once done, you're free to go. All your charges will be dropped for life.

Your thoughts?

Enter Metasploit

msfconsole

- Console based interface
- Full read-line support, tabbing, and command completion
- Run system commands from within the console
- In need of help, “help” shall save thou



You have succeeded in life
when all you really want
is only what you really need

search <operator>:<value>

- regular-expression based search functionality
- module name, path, platform, author, CVE ID, BID, OSDVB ID, module type, or application
- Operators: name author platform type app cve
- eg: search cve:CVE-2011-2523

use <module_path>

- changes your context to a specific module
- Global variables set are unchanged
- eg: use auxiliary/scanner/portscan/tcp

show <module_type>

- displays every module contained in Metasploit
- eg:
  show auxiliary
  show exploits
  show payloads
  show options

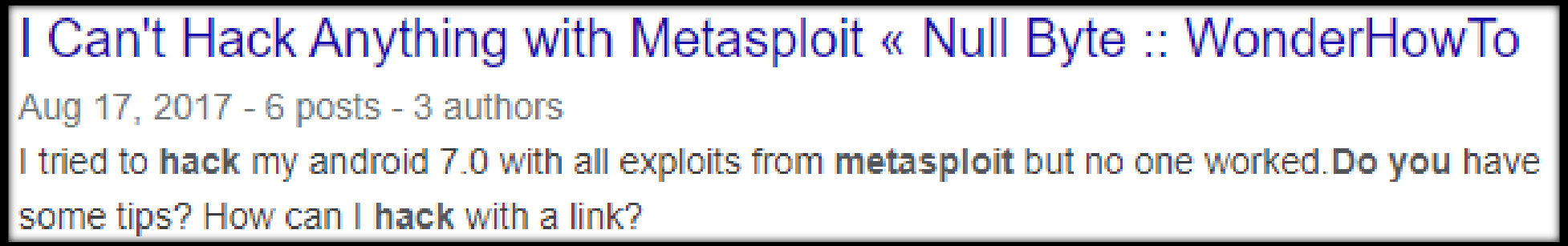
set <param> <value>

- configure Framework options and parameters
- setg sets global parameters
- Payload combinations using set
- eg: set RHOSTS 192.168.56.102

RUN.

IMPORTANT

- Metasploit won’t make you a Hacker.
- Metasploit won’t make you a Hacker.
- Metasploit won’t make you a Hacker.



Demo :)

Sources

- https://www.offensive-security.com/metasploit-unleashed/
- https://medium.com/@hakluke/haklukes-guide-to-hacking-without-metasploit-1bbbe3d14f90
- https://www.sciencedirect.com/topics/computer-science/metasploit-framework
- https://github.com/rapid7/metasploit-framework
- HackerSploit YouTube Tutorials
- Metasploitable 2

QUESTIONS?

ABOUT ME

Hyper-curious
ASE-T - TCS Limited
Musician
IdeaEngine007