

Lab 7: Metasploit

Operating System Exploitation

Table of Contents

[Lab Outcome 2](#_Toc530928204)

[The Exercise 2](#_Toc530928205)

[Submission – Lab 7: Metasploit 3](#_Toc530928206)

Operating System Exploitation

Lab 7: Metasploit

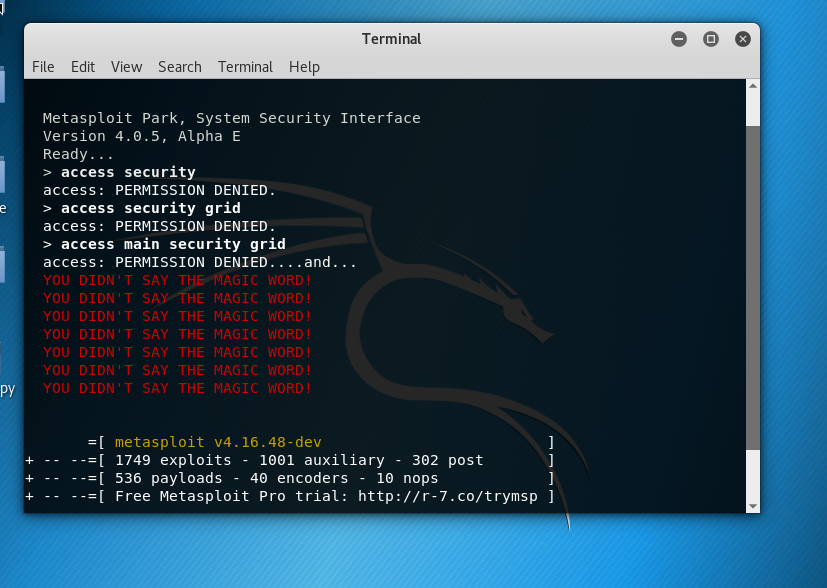
# Lab Outcome

Get familiar with Metasploit, select an exploit, select a payload and run the exploit

# The Exercise

Find and research about a recent Exploit in Metasploit **(2017-2018**):

1. You can run Metasploit from Kali Linux or download the Metasploit framework



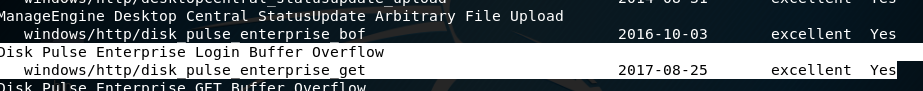
Command:

msfconsole

1. There are four main activities when running Metasploit: Start the console, select an exploit, select a payload and run the exploit
2. Review the existing exploits by running **show exploits**
3. Metasploit exploit quality ratings are **manual, low, average, normal, good, great and excellent**. Most penetration testers will focus on running exploits that are ranked as **normal or higher** and it is preferable to use exploits that are ranked **good, great or excellent.** For this exercise, **search for a recent exploit (2017-2018) with a ranking of good or higher**

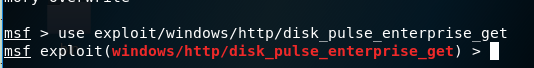
**Command:**

**Show exploits**



**Command:**

**use exploit windows/http/disk\_pulse\_enterprise\_get**



1. There are **three types of exploit modules and eight types of payloads**. Find out about all these types of exploits and payloads and briefly describe each one of them

Types of Exploits:

* Singles are payloads that are self-contained and completely standalone.
* Stagers setup a network connection between the attacker and victim and are designed to be small and reliable.
* Stages are payload components that are downloaded by Stagers modules.

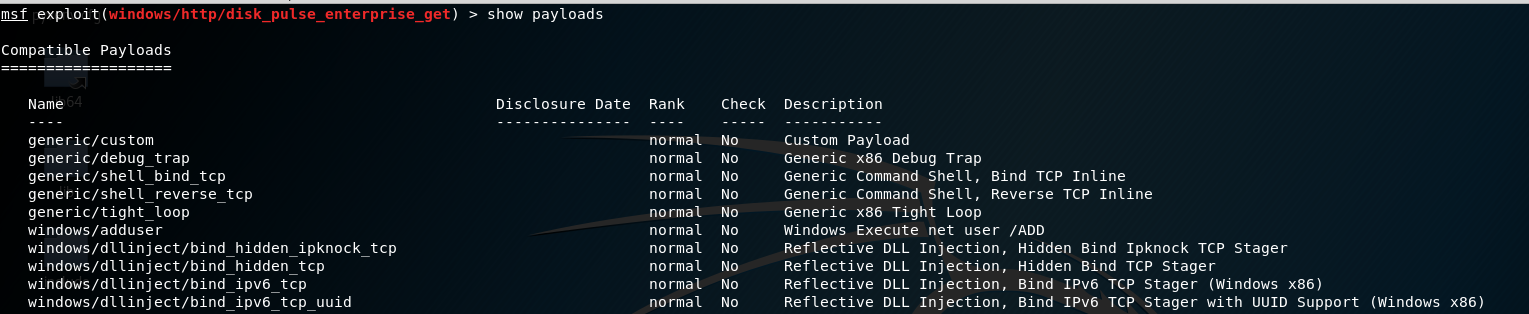
Types of Payloads:

* Inline (Non-Staged) is a single payload containing the exploit and full shell code for the selected task.
* Stager payloads work in conjunction with stage payloads in order to perform a specific task
* Meterpreter (Meta-Interpreter) is an advanced, multi-faceted payload that operates via dll injection..
* PassiveX  is a payload that can help in circumventing restrictive outbound firewalls.
* NoNX (No No eXecute) bit is a feature built into some CPUs to prevent code from executing in certain areas of memory.
* Ordinal payloads are Windows stager based payloads that have distinct advantages and disadvantages.
* IPv6 – looking at the name it tells you that has to do with payloads that are compatible with IPv6 networks
* Reflective DLL Injection is a technique whereby a stage payload is injected into a compromised host process running in memory, never touching the host hard drive

Reference  
<https://www.offensive-security.com/metasploit-unleashed/payload-types/>

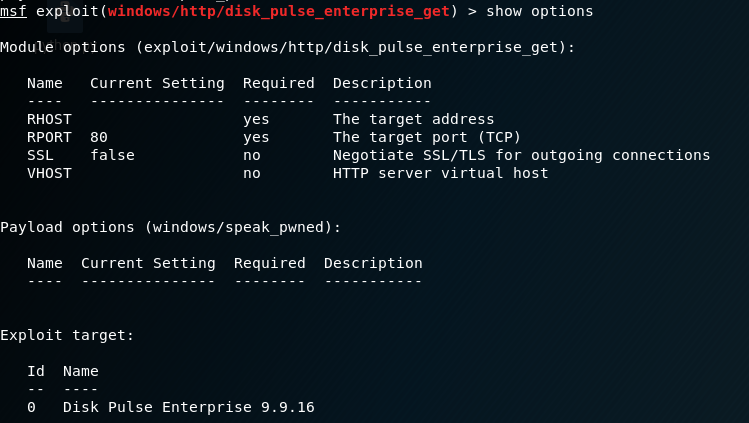
<https://www.offensive-security.com/metasploit-unleashed/payloads/>

1. Once you have identified your exploit, proceed to select a payload



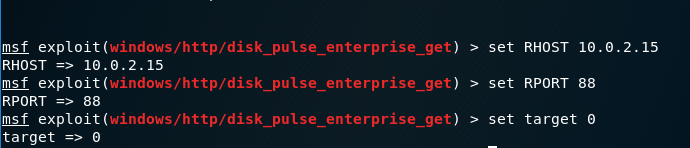


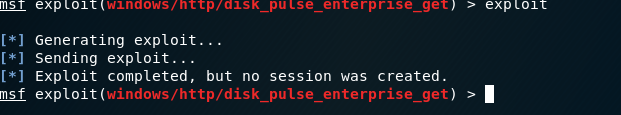
1. Find out if your Metasploit module has options and set them accordingly, what are the exploit targets? Windows, Linux or different targets?



The Exploit targets is Disk Pulse Enterprise 9.9.16.

1. Now that you have selected your exploit and payload, you can attempt to run the exploit. **Test all possible targets**





1. Describe the details of your selected exploit, payload and the steps to complete a successful exploit

A buffer overflow vulnerability lies in the web server component of Disk Pulse Enterprise 9.9.16 where an attacker can craft a malicious GET request and exploit the web server component. Successful exploitation of the software will allow an attacker to gain complete access to the system with NT AUTHORITY / SYSTEM level privileges. The vulnerability lies due to improper handling and sanitization of the incoming request

1. Get all screenshots and commands to complete this lab
2. Submit your work **(Individual Lab)**

**Due date: Dec 10, 18**

# Submission – Lab 7: Metasploit

Submit it to D2L

Weight: 10 %