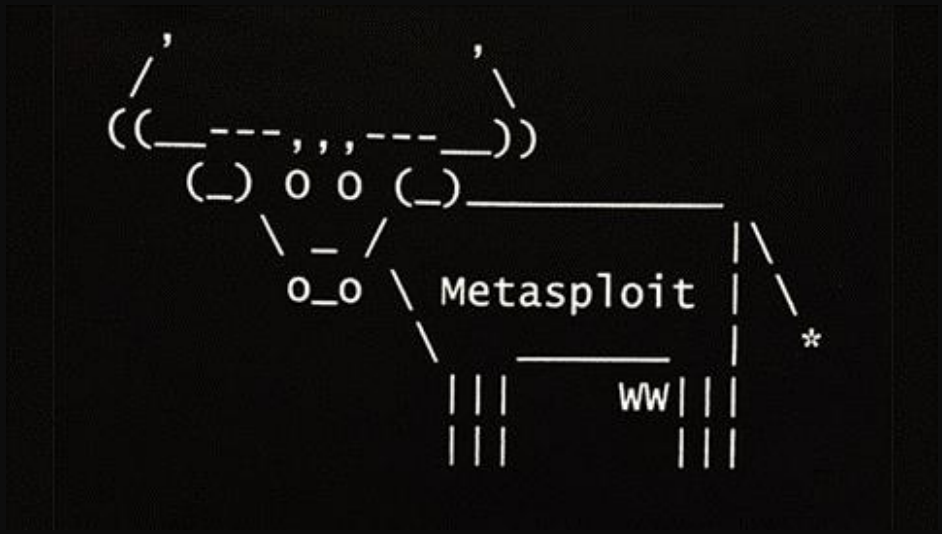
METASPLOIT

The most widely used penetration testing tool on the market

What is Metasploit



- Set of tools used for penetration testing that allow users to run exploits to target vulnerabilities
- Can load a special payload called a meterpreter that allows for a lot of very fun options post exploitation
- Seamlessly integrates with multiple other tools on the market (e.g. Armitage)

Usage of Metasploit

- Widely used by hobbyists, developers and large corporations
- Real world Security tests
- Testing for Vulnerabilities in the network
- Making sure network security is working
- Or hacking

The Metasploit Project

The Before Times

- Started in 2003 to create a solution to solve the problem of disorganized and faulty exploits
- Originally developed by one person
- First version was in Perl and included a whopping 11 exploits when released!

The Metasploit Project Now

- One of the most well known penetration tools in the market with thousands of public WORKING exploits
- Picked up by Rapid7
- Rebuilt in Ruby
- Free and Open-Source (Hosted on GitHub)

A Brief Overview of Rapid7

- Passionate about Metasploit and actively support it in multiple ways
- Encourage a great community around exploit management, creation, and updating
- Excellent customer relations (as opposed to some of their other competitors who are more elitist)

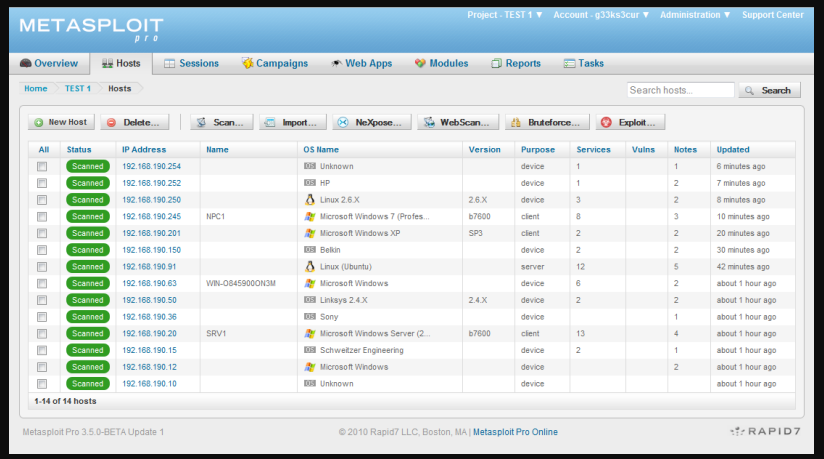
Metasploit Flavors

Metasploit Framework

- Completely free and open-source
- Comes already installed in Kali operating system
- Must use third-party tools to add a GUI, but the command line is user friendly and robust

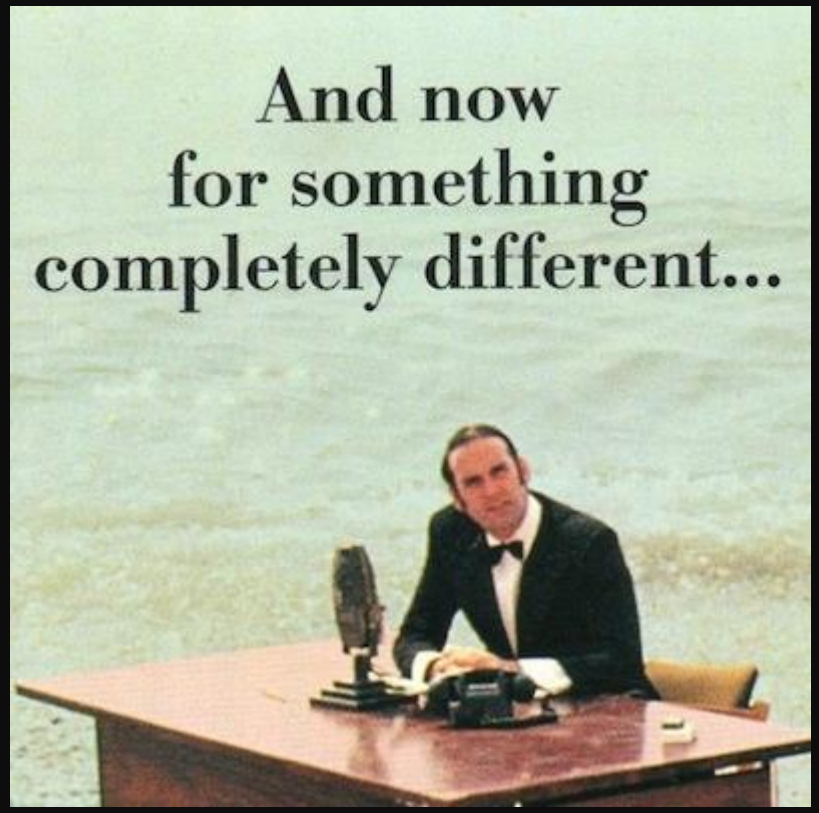
Metasploit Flavors

Metasploit Community, Express, and Pro



- Come with a GUI
- Community is free but limited in features
- Express is an affordable solution for small security companies
- Pro is packed with multiple tools such as automation, phishing attacks and fully unlocked GUI but can cost multiple thousands to use

Metasploitable



- Intentionally vulnerable virtual machine by made by Rapid 7
- Used often by beginners to grasp Metasploit

Question and Answer Time!

- Is it alright to use Metasploit on any computer?

  Totally not! Exploiting different machines can have drastically terrible consequences and can crash or corrupt the target in some cases. Also it may be illegal if you do not have permission to exploit the target.

- Is Metasploit detectable?

  Depending on the types of AV evasion methods used as well as how proficient the hacker is in covering up their tracks, Metasploit can be a very difficult to detect tool. However the flipside is also true where vanilla Metasploit is very easy to detect.

- How do I protect against Metasploit attacks?

  Because Metasploit targets vulnerabilities, none of which (unless using custom made modules) are zero-day; the easiest method of prevention is to keep your system up to date.