Metasploit!?! What is it good for? Absolutely everything!

Presented by

Maurice Cronin

Background

- Left CIT with a BSc in Analytical Chemistry
- Worked in various labs
- Building work
- Tool hire
- Coring and chasing
- Small engine repair
- Back to CIT for the first year of the H. Dip in Cloud Computing
- Software QE at EMC

What is the Metasploit-Framework?

What can you do with it?

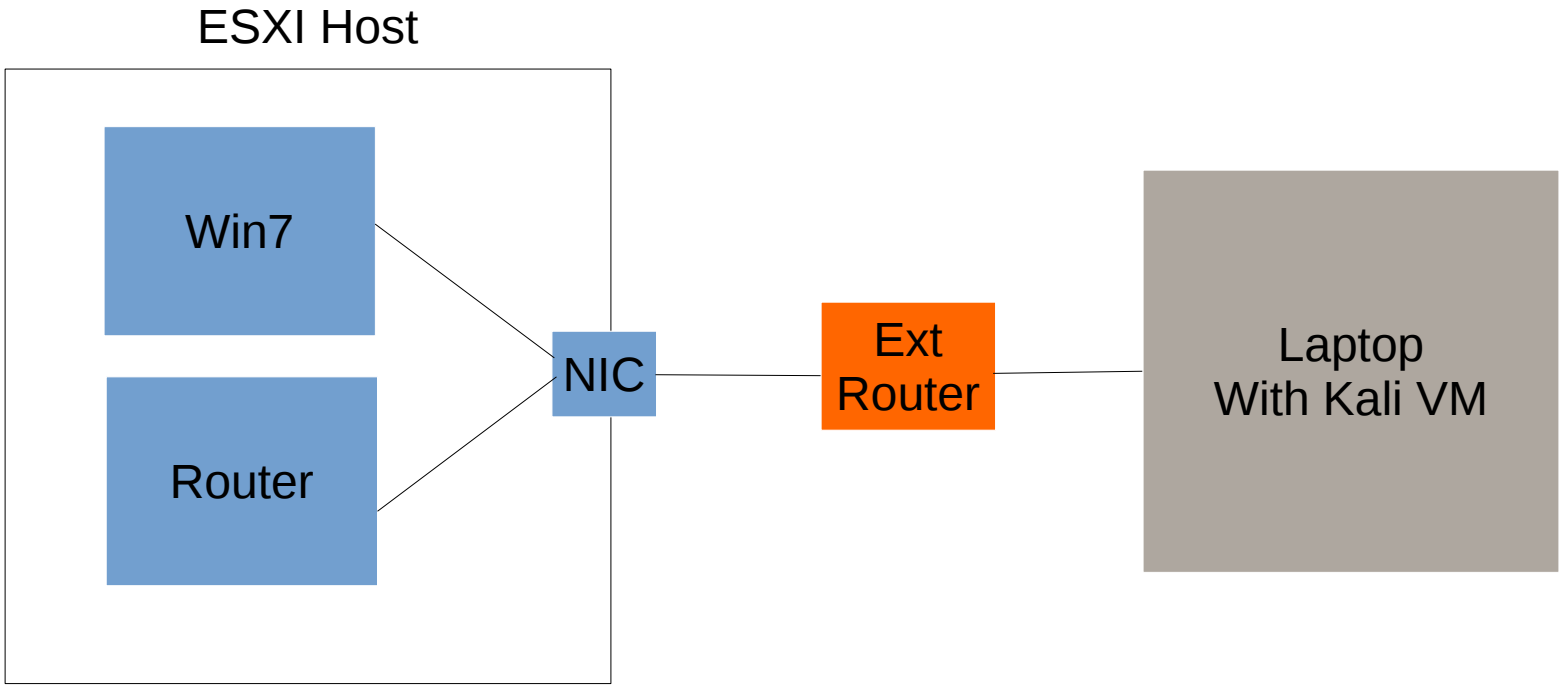
- **Scan networks**
- **Service enumeration**
- **Search and deploy exploits**
- **Create payloads (and deploy them separately)**
- **Gather information and credentials from hosts**
- **Manipuate hosts**
- **Access persistence**
- **Tools for exploit development**
- **Password cracking**
- **NMAP intergration**
- **Meterpreter shell**
- **Store all the data collected in a dedicated DB**
- **And I nearly forgot this one:**

- **SET – The Social Engineering Toolkit**
  - **Create poisoned USBs**
  - **Clone Websites**
  - **Run phishing campaigns**
  - **All with an automatic handler to pick up any successful returns**

The Plan

- Brief description of MSF and what it can do
- Explore some basic MSF functionality
  - Scan for vulnerable services
  - Search for exploits to use on them
  - “Pop a shell” or two
  - Build an executable payload using MSFVenom
- Try answer any questions

Lab Topology



Resources

Rapid7 website:

https://www.rapid7.com/products/metasploit/

Metasploit Unleashed:

https://www.offensive-security.com/metasploit-unleashed/

Metasploit reference book:

Metasploit: The Penetration Tester's Guide

https://www.amazon.co.uk/Metasploit-Penetration-Testers-David-Kennedy/dp/159327288X/ref=sr_1_1?s=books&ie=UTF8&qid=1504438172&sr=1-1&keywords=metasploit

The Plan

- Start/setup of metasploit
- Look at the basic commands/navigation
  - Search/Use/Set
  - Help/set/unset/channel/sessions
- Scan for VMs
- Search for exploits and the configure them
- Pop a shell on the vulnerable machines
- Look at the exploit files
- Look at the running MSFVenom to create an executable payload for the router and use it to get a MP shell on the router.