INTRODUCTION

Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphael Hertzog joined them as a Debian expert. Kali Linux was released on the 13th march, 2013 as a complete, top to bottom. Rebuild of Backtrack Linux, adhering completely to Debian development standards.

- More than 600 penetration testing tools included.
- Free (as in beer) and always will be.
- OS Family - Unix like
- Platforms - x86, x86-64, armel, armhf
- Wide-ranging wireless device support.
- Custom kernel, patched for injection.
- Multi-language support.
- Completely customizable.
- Kernel Type - Monolithic kernel (Linux)
- Default UI - GNOME3
- Latest Release – 2017.2 April 25, 2017

Kali Linux is specifically geared to meet the requirements of professional penetration testing and security auditing. To achieve this, several core changes have been implemented in Kali Linux which reflect these needs:

- Single user, root access by design.
- Network services disabled by default
- Custom Linux kernel.
- A minimal and trusted set of repositories

INTRODUCTION TO ARMITAGE

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Armitage is a graphical user interface for the Metasploit Framework. At first glance, it may seem that Armitage is just a pretty front-end on top of Metasploit. Armitage is a scriptable red team collaboration tool. It has a server component to allow a team of hackers to share their accesses to compromised hosts.

Author: Strategic Cyber LLC
License: BSD

Features

- Use the same sessions
- Share hosts, captured data, and downloaded files
- Communicate through a shared event log.
- Run bots to automate red team tasks Use Java 1.7

Use Java 1.7

Kali Linux ships with Java 1.6 and Java 1.7. Java 1.6 is the default though and for some people–this version of Java makes their menus stick or draw slowly. For the best Armitage experience, you should use Java 1.7.

Fortunately, it's one command to change the default. If you have 32-bit Kali Linux, open a terminal and type: **update-java-alternatives --jre -s java-1.7.0-openjdk-i386 .**

If you have 64-bit Kali Linux, open a terminal and type**: update-java-alternatives --jre -s java-1.7.0-openjdk-amd64**

Installing Armitage

Your version of Kali Linux may not include Armitage. To install it, type:

- **apt-get install armitage**

Next, you need to start the Metasploit service. Armitage does not use the Metasploit service, but starting it once will setup a database. yml file for your system. This is a necessary step. You only need to do this once:

- **service metasploit start**
- **service metasploit stop**

Starting Armitage

Before you can use Armitage, you must start the postgresql database. This does not happen on boot, so you must run this command each time you restart Kali:

- **service postgresql start**

To start Armitage in Kali Linux, open a terminal and type:

- **armitage**

Armitage will immediately pop up a dialog and ask where you would like to connect to. These parameters only matter if you want to connect to an Armitage team server. Since we're getting started. Just press Connect.

Then ,Armitage will try to connect to the Metasploit Framework. Armitage Labs

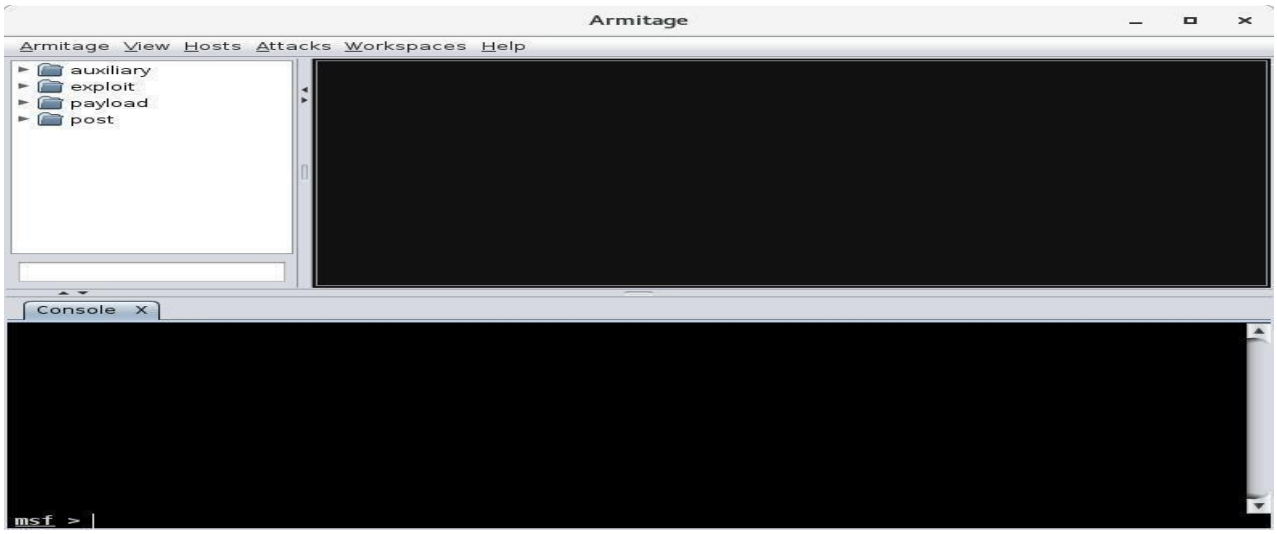


Fig: Armitage Framework

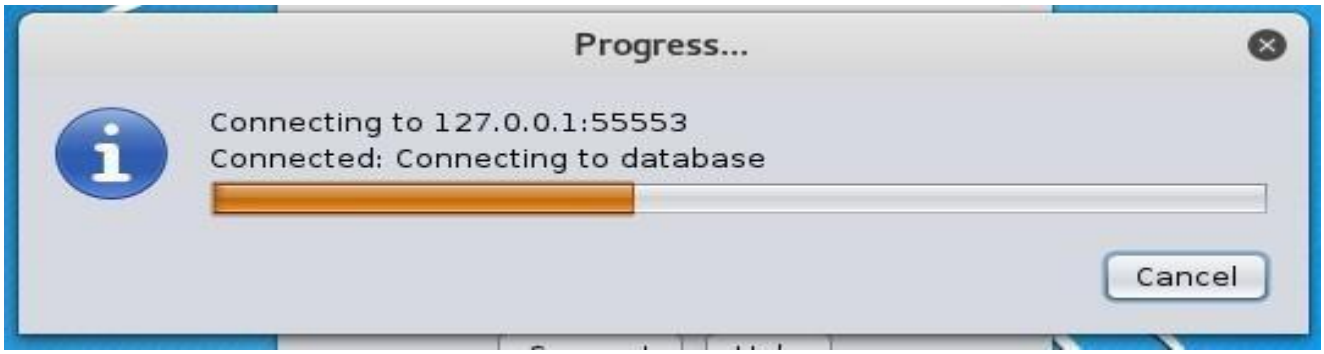
STEPS TO EXPLOIT A LINUX DEVICE

To start Armitage in Kali Linux, open a terminal and type:

- **Armitage**

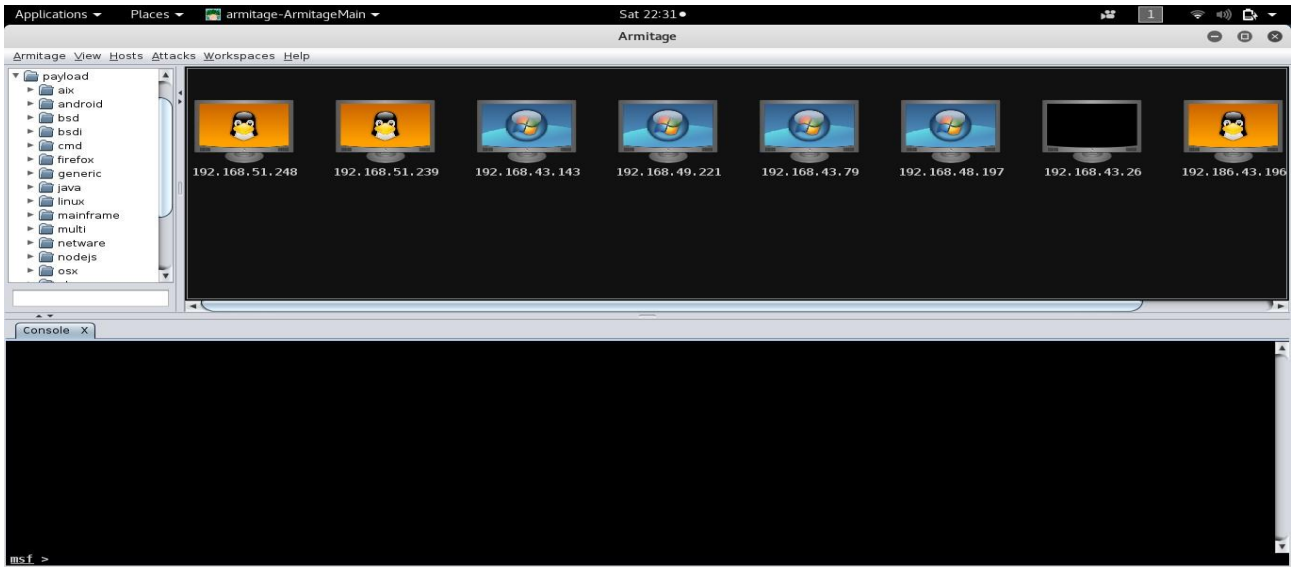
Then accept the default values:

- You will probably get a popup asking to start Metasploit, click **yes**
  you should now see the following:

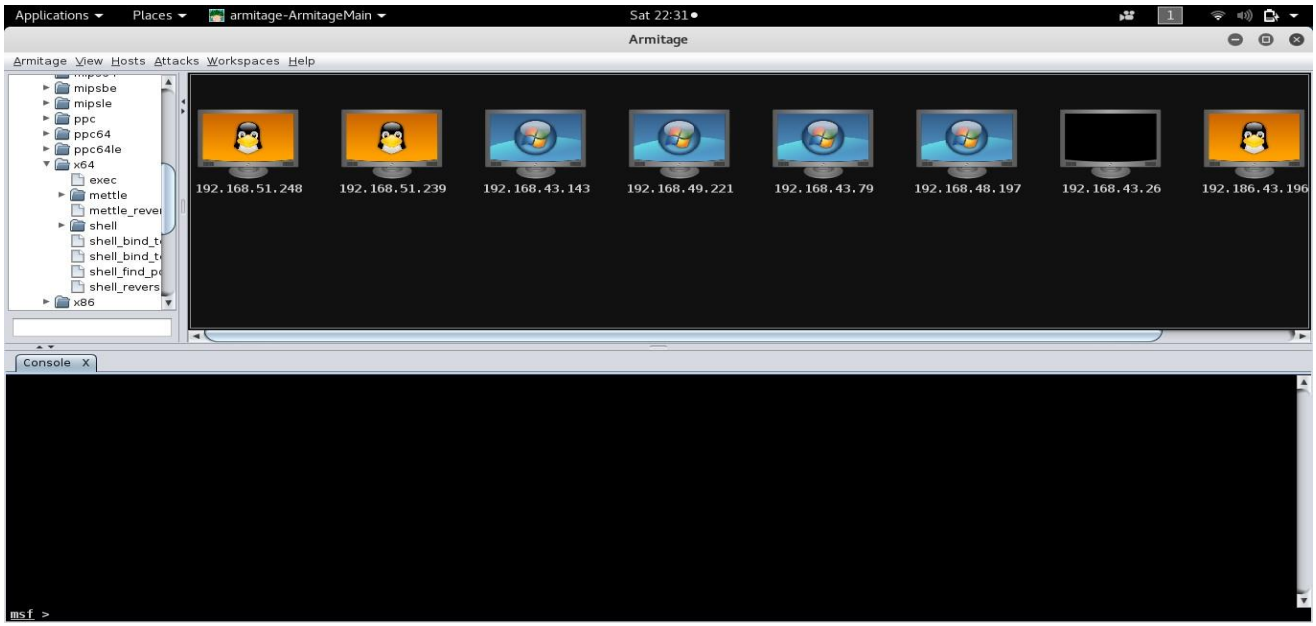


Don't worry about the connection refused it just takes a while to load.

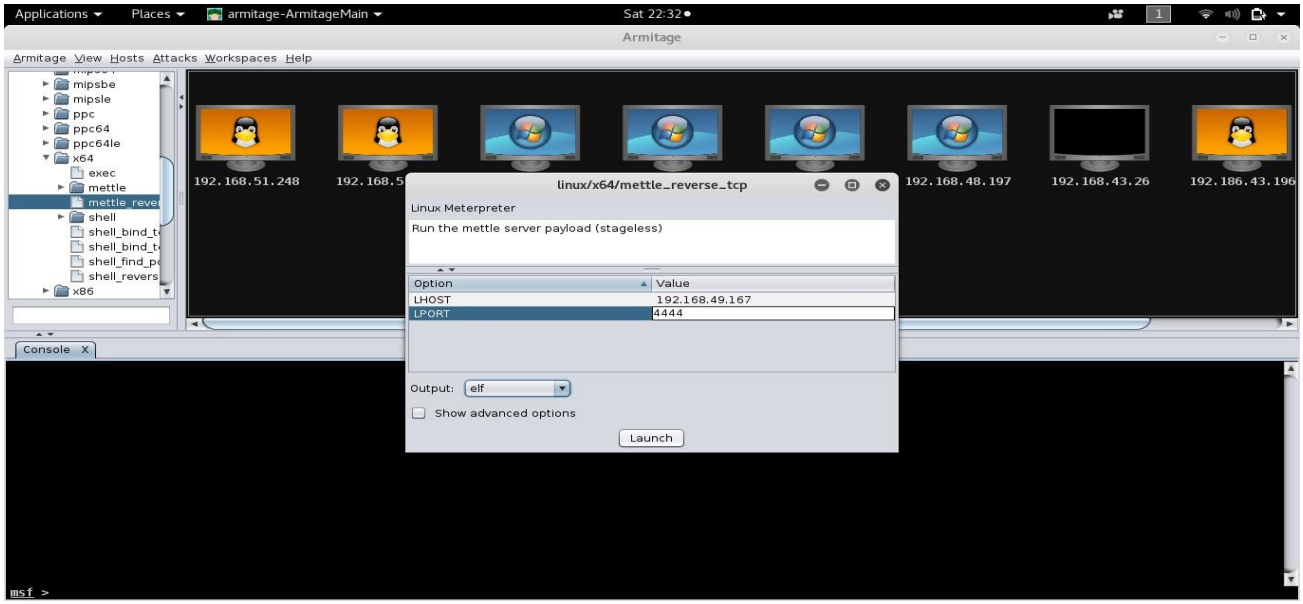
- Now Armitage will boot up if it asks you for the attack computer IP enter your IP Address.
  Navigate to the **Payload>Linux**



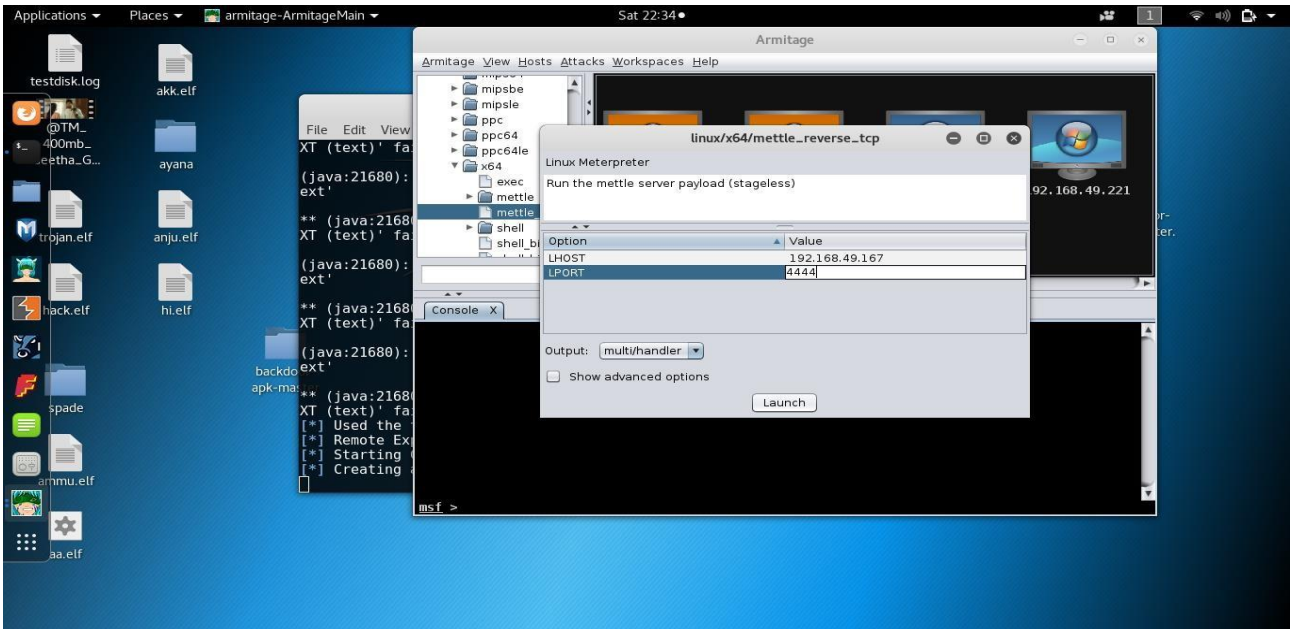
- From here Armitage will have to select which configuration of linux
  Linux>x64>mettle_reverse_tcp



Then **set portnumber>set payload>launch**

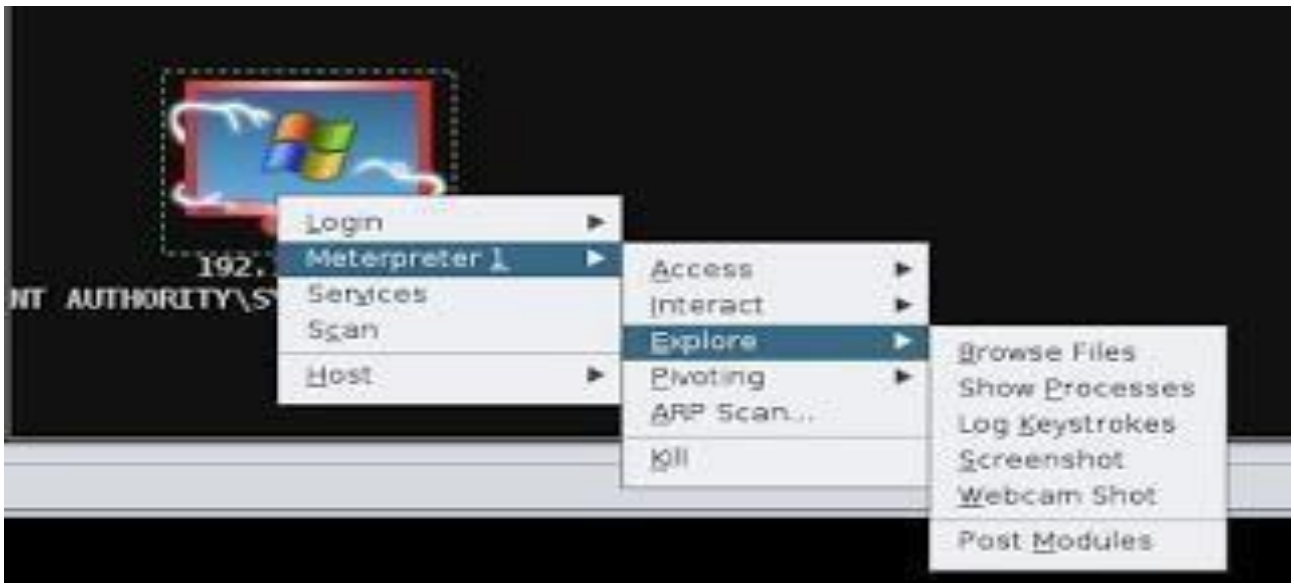


- This will bring up an attack confirmation window check the details and click **launch**

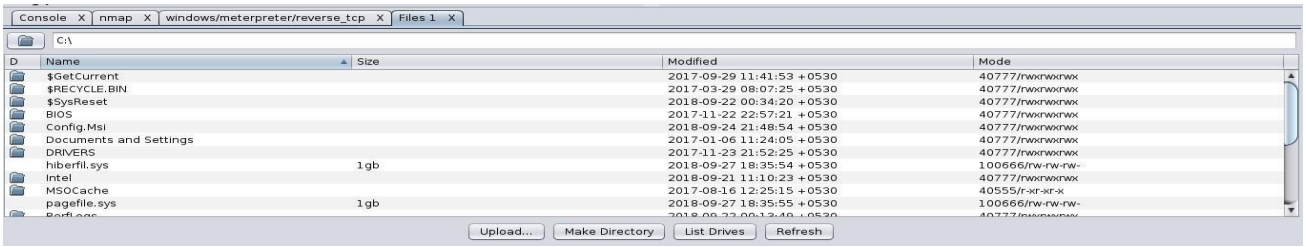


- Confirmation of a successful exploit will look like this:

- You can now right click the target and perform multiple commands



- here is an example of the Browse files of victim system



CONCLUSION

Armitage is one more way to access and use the Metasploit framework. It provides an easy to use GUI interface making it easier for the novice pentester/hacker. It's only real drawback is that it uses significantly more system resources than the msfconsole.

This tool allows penetration testers and security analysts to ensure everything is behaving properly using a combination of manual testing and automation to ensure full visibility.

Not only for accessing remote personal computers, Armitage can be used to access android phones also.

The major advantages of using this tool are that it recommends the exploits, has advanced post exploitation features, and is a very good visualization of the targets. We can scan a particular target or import data from other security scanners, which can then be used in Armitage for further attacks.

REFERENCES

- https://haccoders.blogspot.com/2016/01/how-to-use-armitage-on-kali-linux.html
- http://www.kalilinuxhack.com/2015/11/use-armitage-on-kali-linux-to-hack-windows.html
- https://www.youtube.com/watch?v=H8TGxW_iyaY
- https://www.youtube.com/watch?v=rxOWVYyCods
- https://www.yeahhub.com/armitage-in-depth-windows-exploitation-gui-2017/