ARMITAGE**

ARMITAGE

Introduction to Armitage

Armitage is a graphical frontend for Metasploit Framework – an extremely popular open source tool for penetration testing.

Armitage provides a slick point-and-click interface to Metasploit, allowing you to harness its full potential without learning complex commands and parameters.

Some killer features of Armitage:

- Intuitive graphical interface – no CLI needed!
- Automatic exploit recommendation based on scans
- Powerful session management and visualization
- Detailed reporting to document your tests
- All the capabilities of Metasploit at your fingertips!

According to surveys, over 60% of penetration testers use Metasploit regularly. And Armitage adoption is growing rapidly as it makes Metasploit much easier to use.

For beginners, Armitage is the perfect tool to get hands-on experience with ethical hacking and vulnerability research. The visual interface and automation remove a lot of complexity.

Even experienced pentesters use Armitage to save time and effort compared to pure command line work. It streamlines many Metasploit workflows.

In summary, Armitage combines the best of both worlds – the flexibility and modularity of Metasploit + an intuitive and automated GUI for faster testing.

Installing Armitage on Kali Linux

Thanks to Kali Linux's penetration testing focus, installing Armitage is a breeze. Metasploit Framework comes pre-installed.

We just need to install the Armitage package from the standard Kali repositories.

Here is the quick step-by-step:

1. Launch a terminal on your Kali system. You can find the Terminal app in the Application Menu.

2. First, let's update the package index to ensure we grab the latest version:

   ```
   sudo apt update
   ```

   This fetches metadata for all packages from the remote repositories. Normally, I run this before installing anything on Kali.
3. Now install the Armitage package:

   ```
   sudo apt install armitage
   ```

   Provide your user password when prompted. Sit back as apt does its thing.
4. After a few seconds, Armitage will be installed on your system!

   You can launch it from the Application Menu under Information Gathering.

See, I told you it was easy peasy! Kali takes care of the dependencies and configurations automatically.

If you ran into any issues, don't fret. Here are some tips:

- Make sure you have an active internet connection on Kali.
- Try running `sudo apt update` first before installing.
- Run `sudo apt install -f` to fix any broken packages.
- Search the Kali forums if you get weird errors. Tons of help there!

Okay, Armitage is now installed. But before we get hacking, some quick configuration is needed.

Connecting Armitage to Metasploit

For Armitage to work its magic, we need to connect it to the Metasploit RPC server. This allows the GUI to talk to the underlying Metasploit Framework.

Here are the steps to set this up:

1. Launch Armitage using the Application Menu.
   You'll see the Welcome screen listing some options.
2. Click Connect to a Metasploit RPC Server.
3. In the Connect window, use the following settings:

   - Host: 127.0.0.1
   - Port: 55553
   - Username: msf

    - Password: msf

4. Click Connect. Armitage will initialize the Metasploit database.

   If you get an error about the RPC server, simply retry the steps above. Triple check the settings.
5. After a few seconds, the main Armitage UI will load.

   The RPC connection is now active and we can start having fun!

The default RPC settings work perfectly for a local connection on Kali.

You only need to tweak them if running the Metasploit RPC server separately or connecting from another system.

Now that Armitage is ready, let‘s explore the awesome features!

Using Armitage: Key Features and Functionality

Armitage empowers us with a shiny graphical interface to Metasploit. Let‘s see what we can do:

Adding Targets

First, you need one or more targets to hack!

Click the Hosts tab > Add Hosts:

Enter the IP address or hostname of your target system and click Add.

The host will appear in the Hosts tab, ready to be scanned and exploited!

Pro Tip: If you have multiple targets, you can import them from a text file. Just click Import Hosts instead.

Scanning Targets

Next, we need to scan our target to find potential vulnerabilities.

Under the Hosts tab, click Nmap Scan:

Select a scanning profile and hit OK. I recommend starting with Fast Scan for quick results.

Armitage will run a port scan using Nmap and enumerate services, OS, open ports, etc. The results will populate under the target.

Troubleshooting: If your network blocks Nmap scans, try connecting through a VPN or enabling IP forwarding on Kali using `sysctl -w net.ipv4.ip_forward=1`

Finding Attacks

My favorite part! Armitage can automatically recommend viable exploits based on the scan findings. Sweet!

Click Attacks > Find Attacks to run the analysis:

Armitage will dig through the Metasploit modules database to identify potential attacks.

The discovered exploits will show up under the Hosts tab. Right click the target and choose Attack for available options.

As you can see, Armitage does all the hard work of matching exploits to vulnerabilities!

Pro Tip: You can tweak the analysis under Armitage > Set Exploit Threshold. Lower threshold = more potential exploits.

Launching Exploits

To launch an attack, double click the exploit you want to run.

Configure any options in the popup and click Launch. Armitage will execute the exploit.

If successful, you‘ll get a shell/meterpreter session on the target!

Interact with sessions under the Sessions tab. Right click a session for further options.

Generating Reports

Once you are done testing, Armitage can generate a detailed report documenting everything performed.

Click Reporting > Generate Report and enter a title, author details etc.

Armitage will compile a PDF with hosts scanned, vulnerabilities found, exploits launched, evidence gathered like files/screens, and more.

These reports are invaluable for record keeping and client deliverables. You get complete visibility into your pen testing engagement.

There are many more features I haven‘t covered like brute forcing, custom scans, payload generators, credential theft and pivoting between hosts.