

9 Advanced Vulnerability and Exploitation Techniques

Lab Scenario

As a member of a Pen Testing team, you will not be compiling the entire final report but you are required to document all of your activities to contribute to the final report. Every detail that is needed for a report must be turned in to the project leader at the end of the job. You are asked to keep that documentation which will be reviewed by your team leader at a later date.

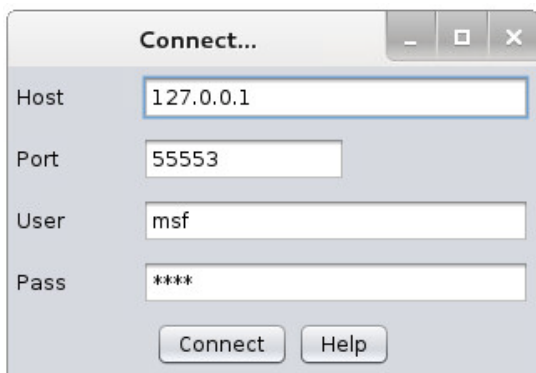
Lab Details - Step-by-Step Instructions

9.1 Armitage

1. Open your Kali Linux and Metasploitable2 VM. Also, run as many other VMs as you can, depending on available RAM. Run ifconfig and take note of the IP address for Kali Linux.

Be Patient... Armitage can take a few minutes to start.

```
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosv.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~# armitage
```

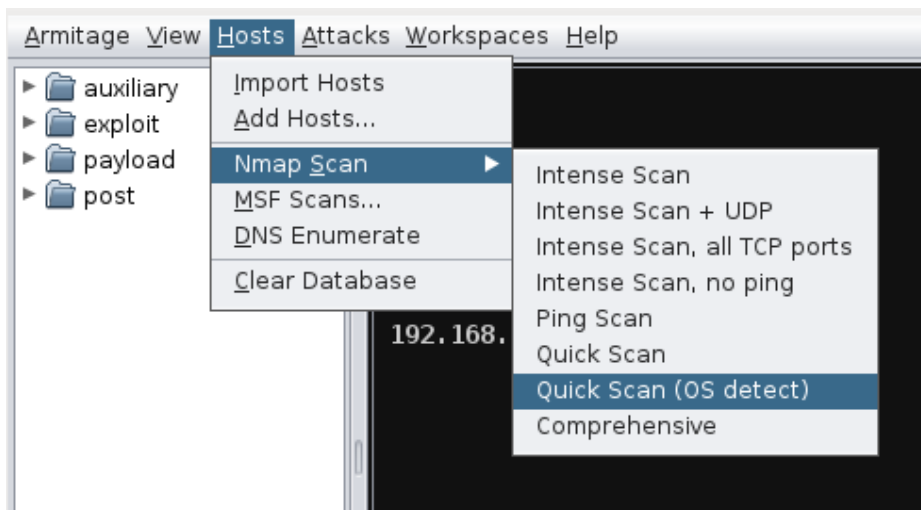


The image shows a screenshot of the 'Connect...' dialog box in the Armitage application. The dialog has a title bar with standard window controls. It contains four input fields: 'Host' with the value '127.0.0.1', 'Port' with the value '55553', 'User' with the value 'msf', and 'Pass' with the value '****'. At the bottom of the dialog are two buttons: 'Connect' and 'Help'.

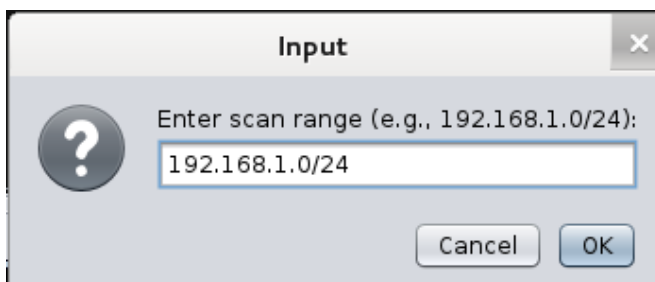
If you receive the Start Metasploit pop-up, click Yes.



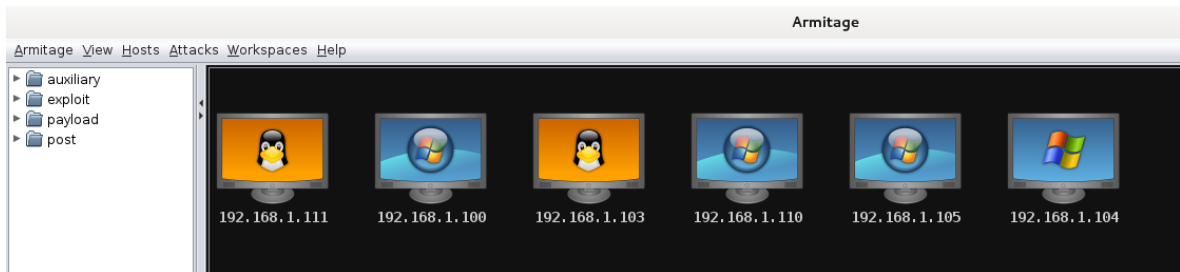
Once Armitage is ready, you'll see a screen similar to the image below. Click on Hosts > Nmap Scan > Quick Scan (OS detect) to start a scan that will find targets in your lab network.



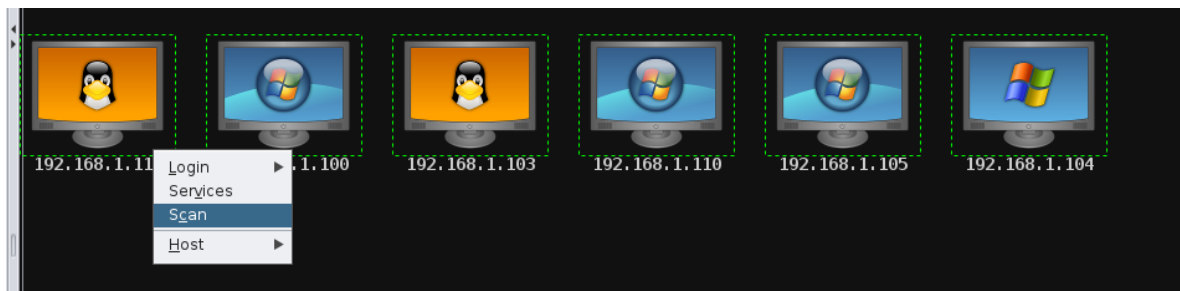
Enter the network/netmask of your lab network. For example: 192.168.1.0/24.



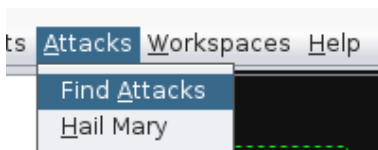
Armitage should detect all of the running hosts in your network. If not, check the network settings on the missing hosts.



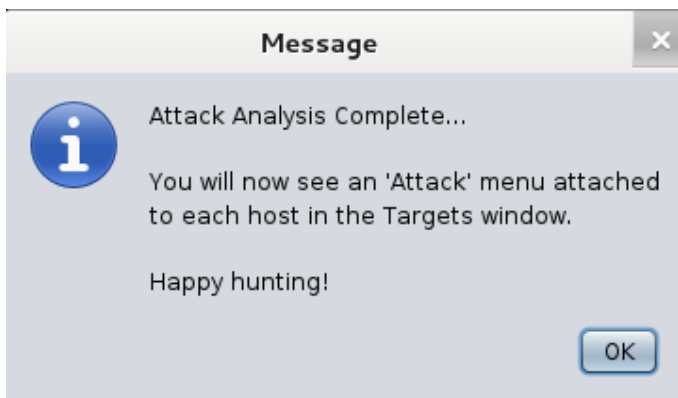
Use your mouse to highlight all hosts. Right-click and select Scan. This will conduct a more thorough scan than the previous one. It will also allow Armitage to find exploits based on the scan results.



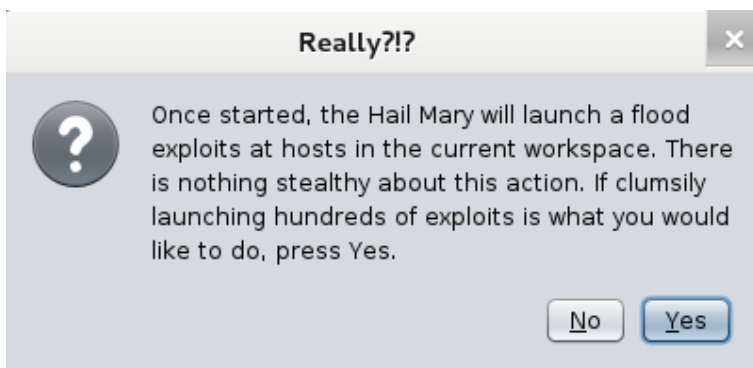
Wait for the scans to finish, then select Attacks > Find Attacks.



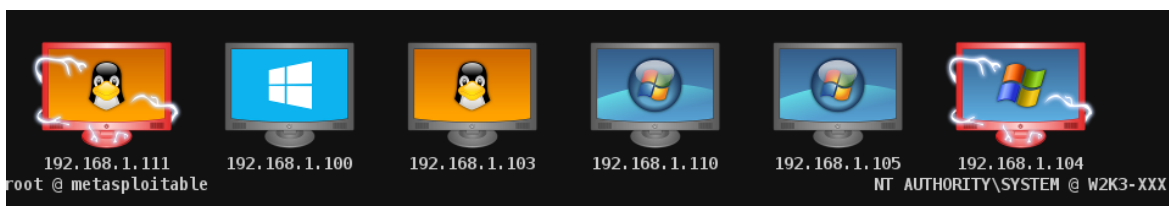
You should receive a pop-up indicating that the attack analysis is complete.



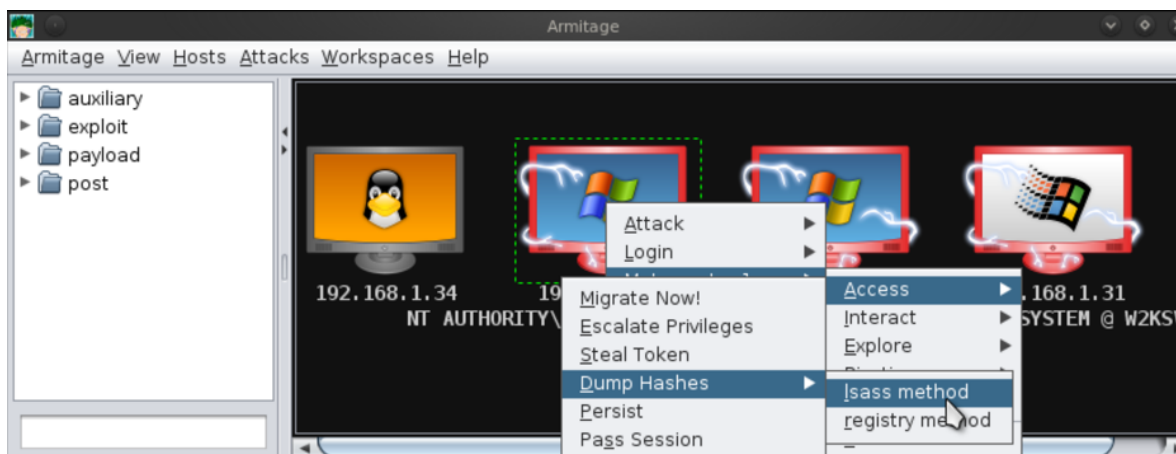
Rarely do you get to launch hundreds of exploits at several different targets. This would not be a stealthy way to verify vulnerabilities during a Pen Test. However, in a lab environment, throwing a Hail Mary is both fun and educational. For added value, Open Wireshark and capture on interface eth0. Click on Attacks > Hail Mary.



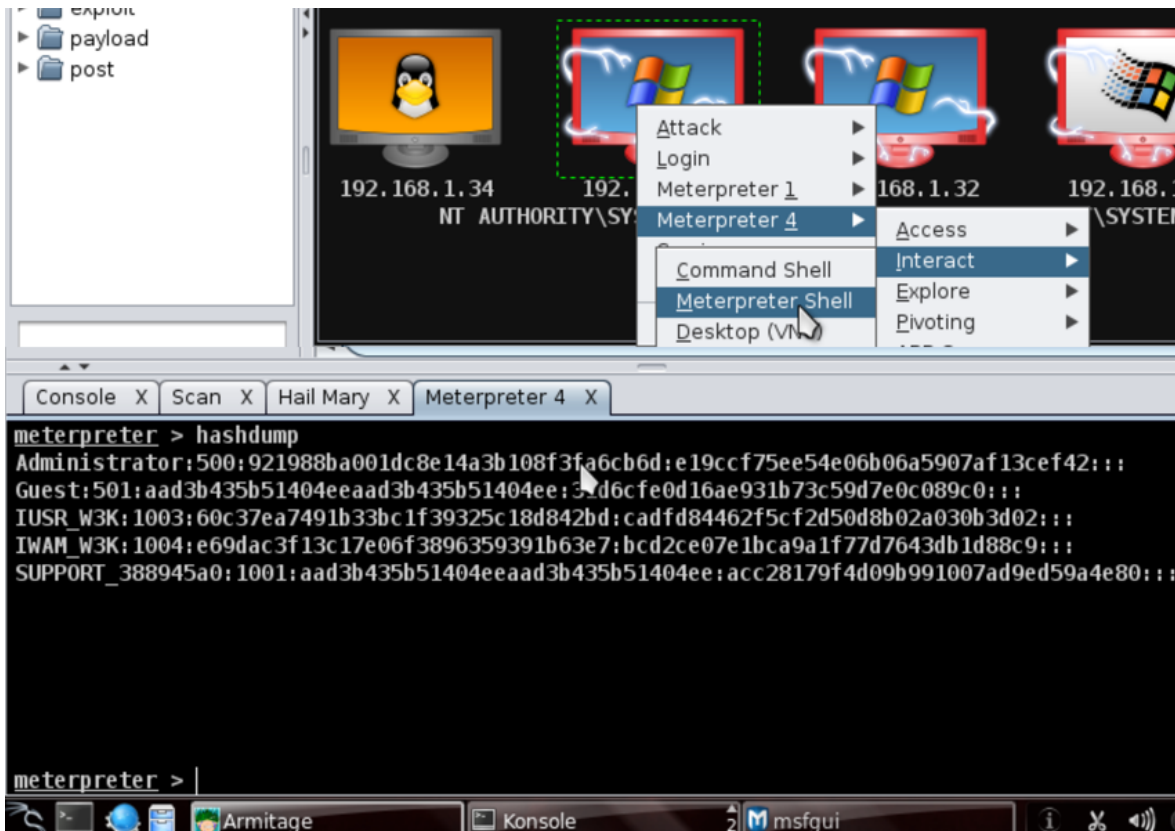
You'll see your targets get electrocuted if an exploit succeeds!



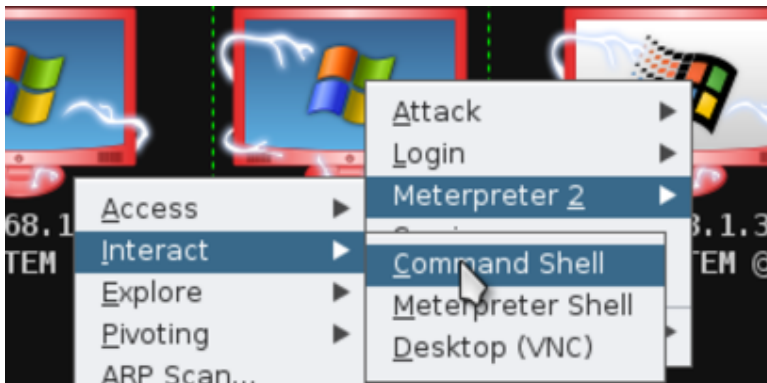
Now that you have a few compromised hosts (your results may vary), let's see what we can do with these victims. Right-click one of your Windows targets and click on Meterpreter > Access > Dump Hashes > Isass method and look at your results.



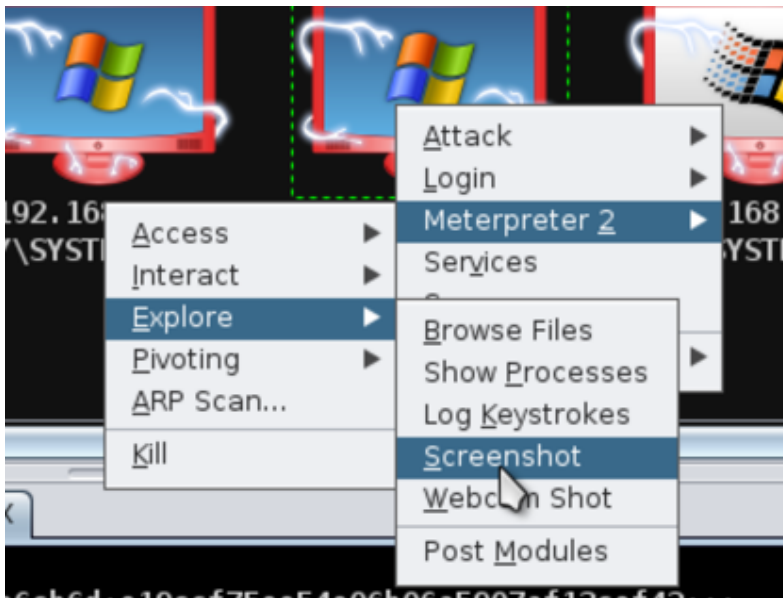
A Meterpreter Shell should open up in the lower section of the Armitage window and display the hashes. If you don't see any results (don't worry, it's a little buggy sometimes), then you can always go to Meterpreter > Interact > Meterpreter Shell, then type in hashdump.



You can also try other items, feel free to take 10 min to explore. You could, for example, get a remote shell from your target.



You could possibly log keystrokes or get a screenshot, etc. Be creative!



NOTE: Take 15 minutes to explore the available options and try out some of the features available in Armitage. Armitage is free, but there is a paid version that has many more features. Check out <http://www.advancedPenTest.com/> and consider downloading a trial, if you have time.