Armitage

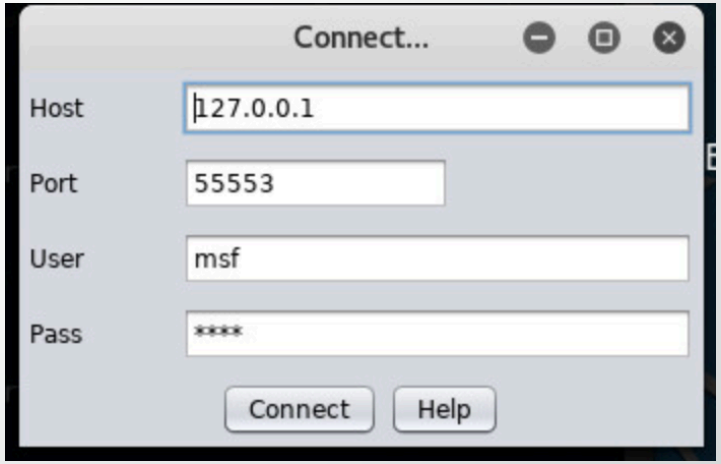
Armitage

- This is very much the easy button to Metasploit
- GUI management tool for Metasploit
  - Visualizes targets
  - Recommends exploits
- Developed by Raphael Mudge

Installing Armitage

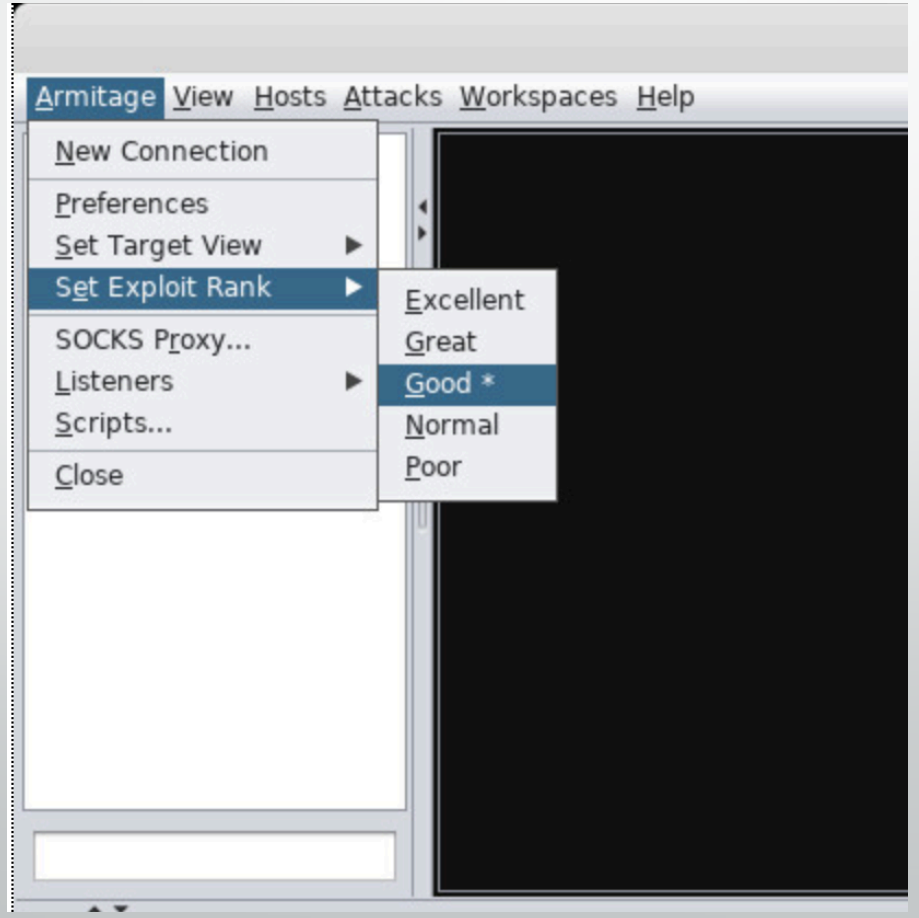
- Already installed on Kali
- apt-get install armitage
- Make sure the postgresql database is running before starting armitage
  - service postgresql start
- armitage

Starting Armitage



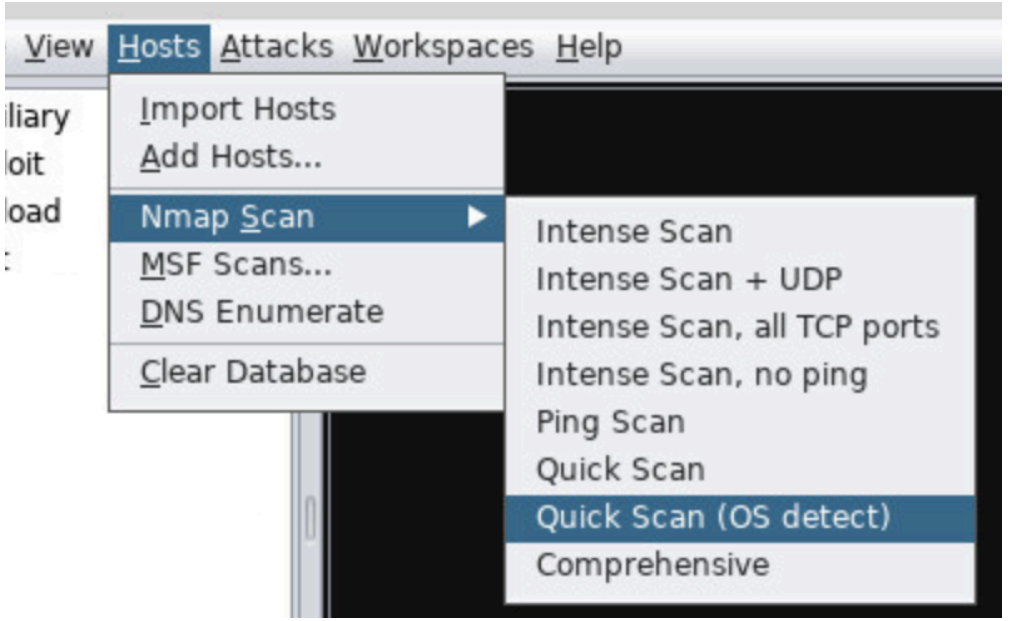
- Choose connect – settings should be correct
- Start the RPC server if prompted

Set Exploit Rank to Good

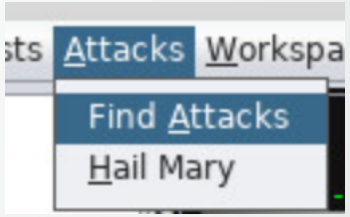


Using Armitage - Scanning

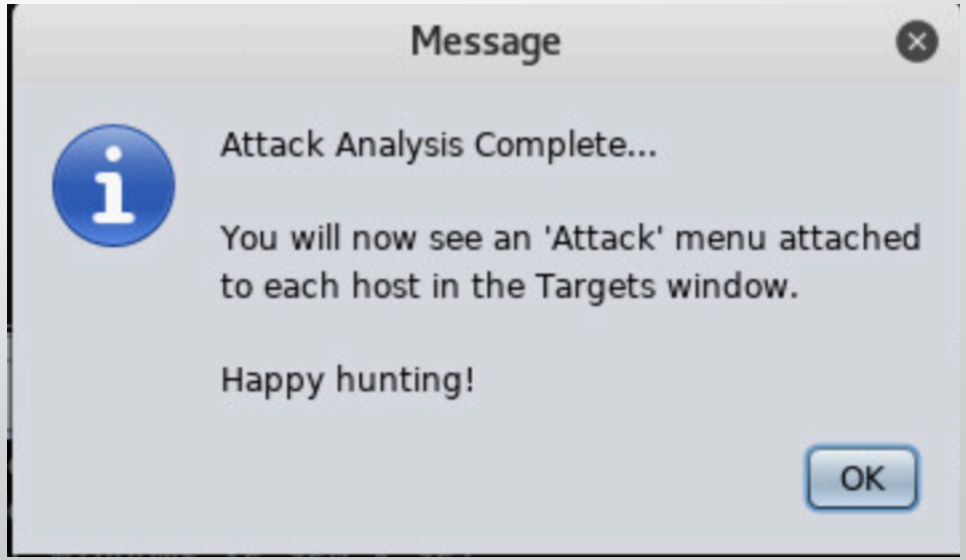
- We need to first scan the network to find the target(s). Armitage can use nmap for that!
  - For now, choose a quick scan. If we had more time, could choose Comprehensive.



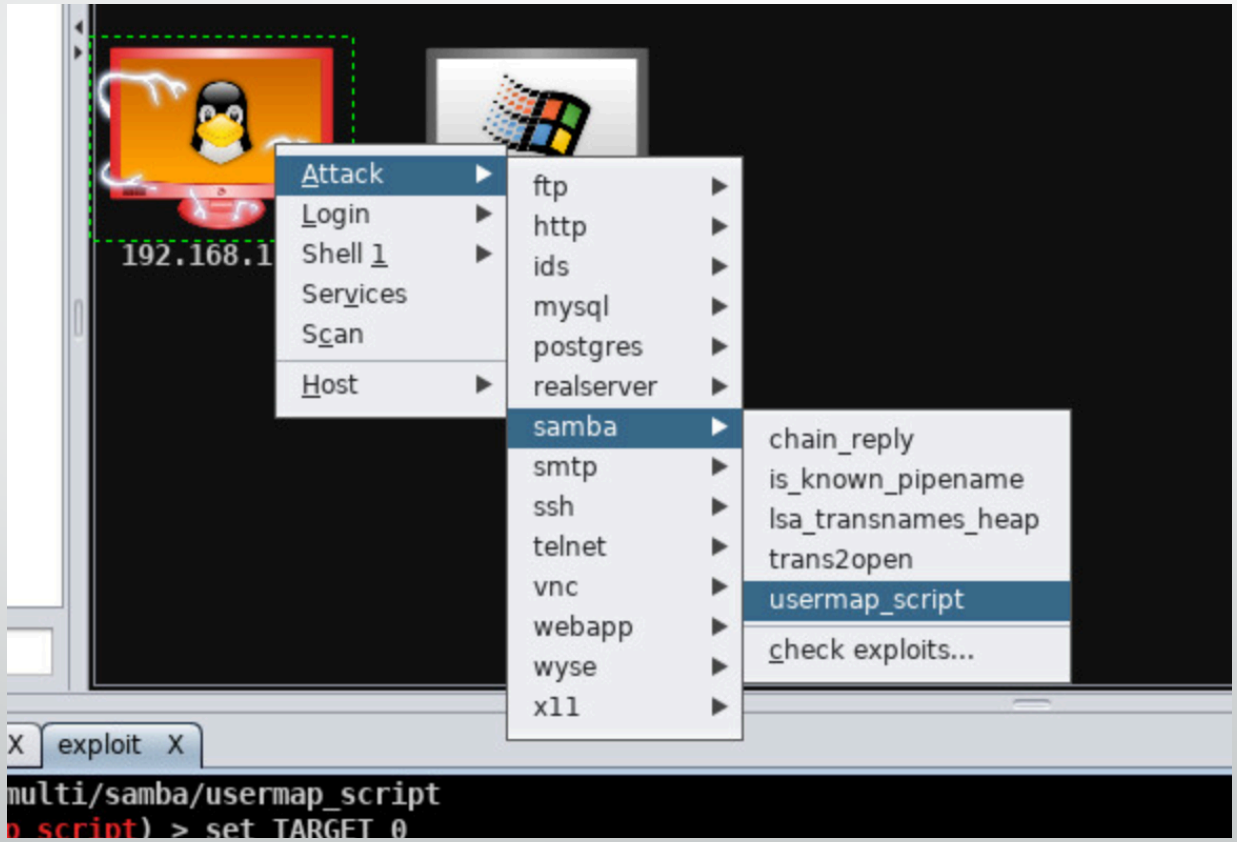
So We Found a Host…

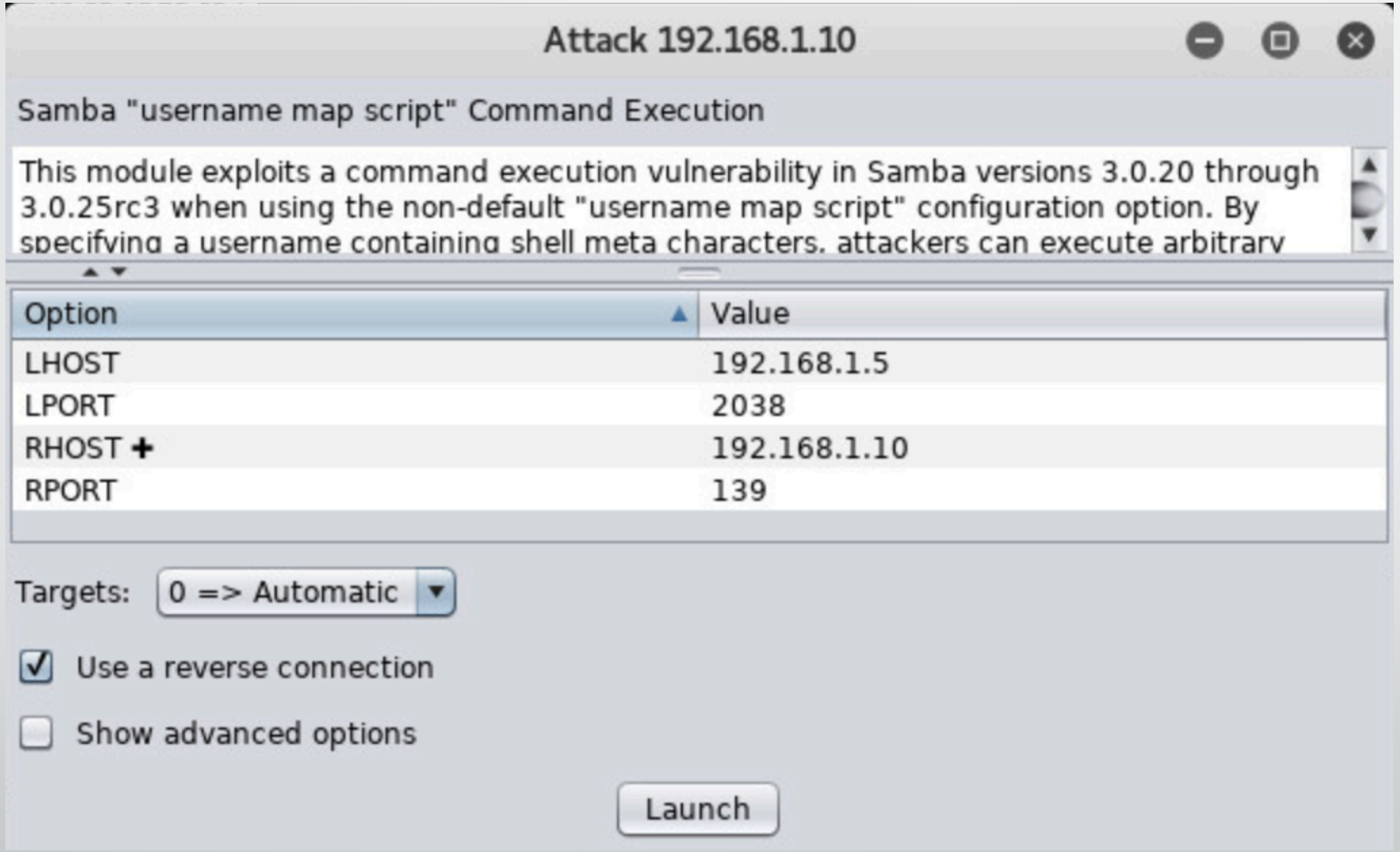


- Find anything you don't want? Remove it.
- Our next step is to find attacks.
  - This is checking for available attacks for that target machine based on the services it is running, and its OS.

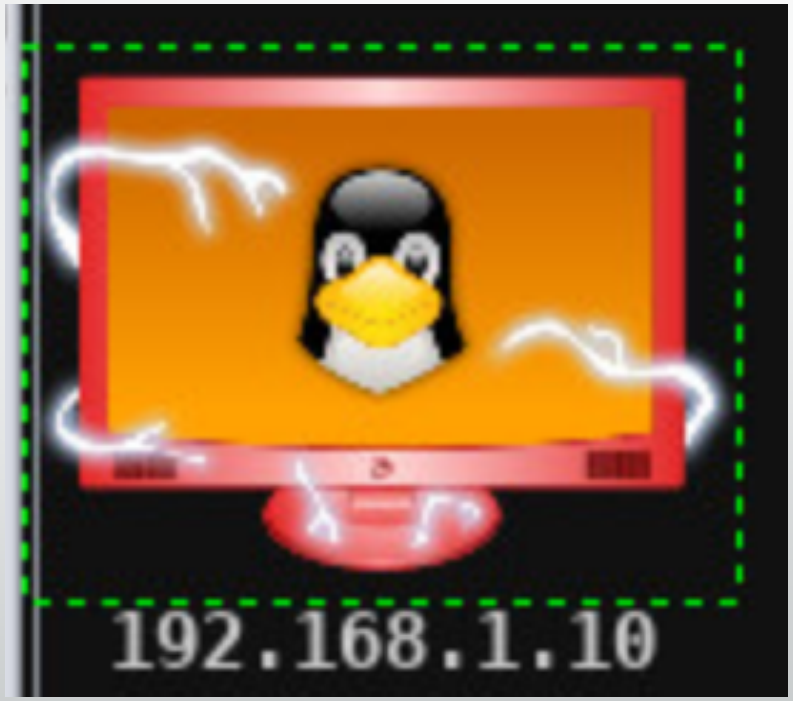


What Did We Find?



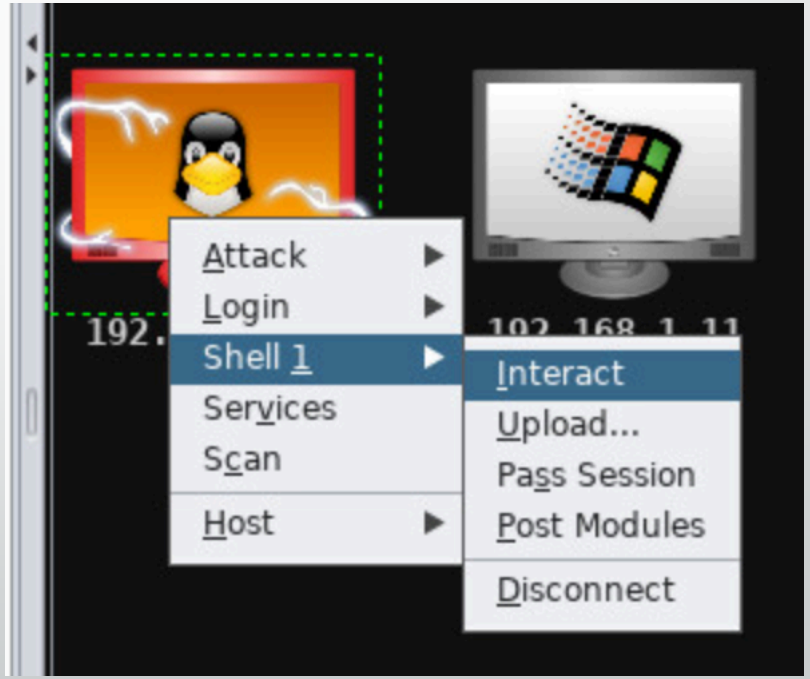

Attack 192.168.1.10
Samba "username map script" Command Execution
This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary
Option
Value
LHOST
192.168.1.5
LPORT
2038
RHOST
192.168.1.10
RPORT
139
Targets:
0 => Automatic
Use a reverse connection
Show advanced options
Launch

Success!



Interacting With the Target

- You could have multiple shells here
- Use the terminal window at the bottom to issue commands and interact with the target



ALL THE ATTACKS