Lab 7 – Vulnerability Scanning & Patching – Metasploit/Armitage

By

Lukas Fuller

IAE-201-D02

IA-201: Introduction to Information Assurance

**Abstract**

The objective of this lab is to introduce students to Metasploit and Armitage. The students will understand what Metasploit and Armitage are. The students will be able to use Armitage to scan and exploit a host. The student will be able to setup persistence in an exploited host.

**Materials**

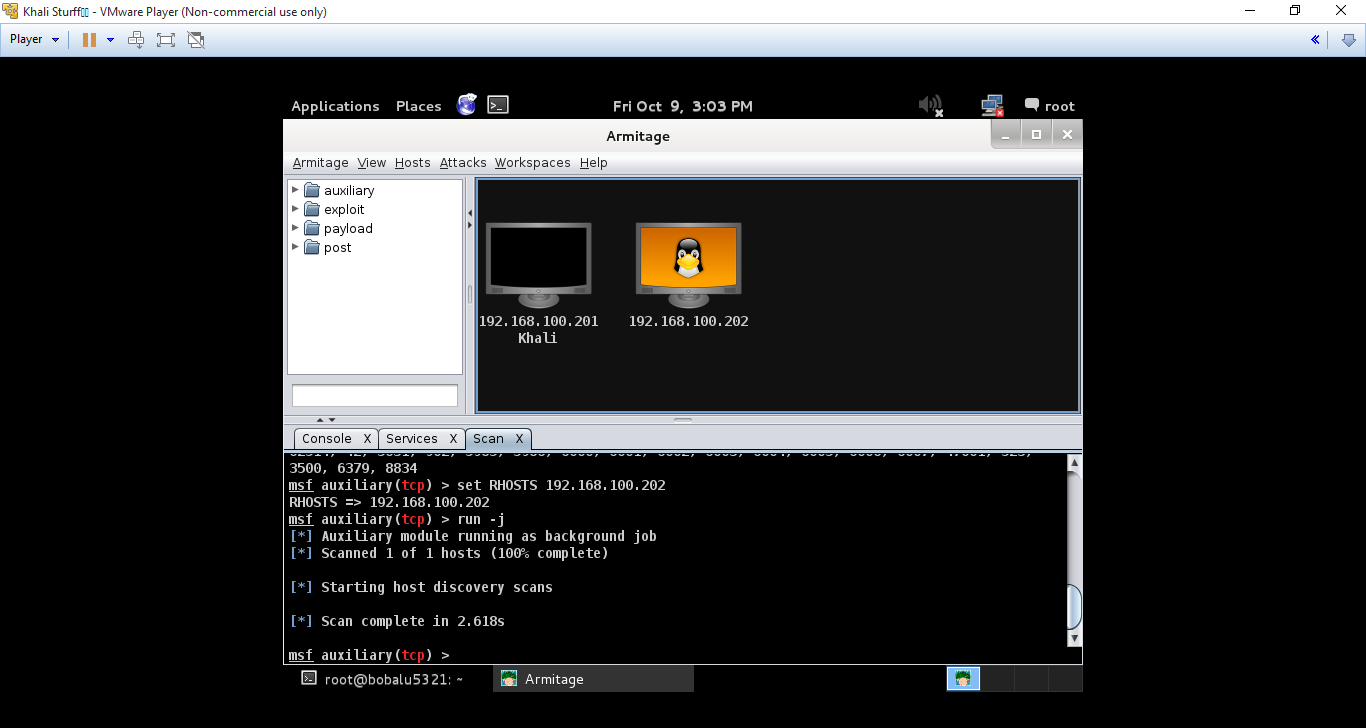
1. Kali Linux Virtual Machine
2. Metasploitable Virtual Machine

**Conclusion**

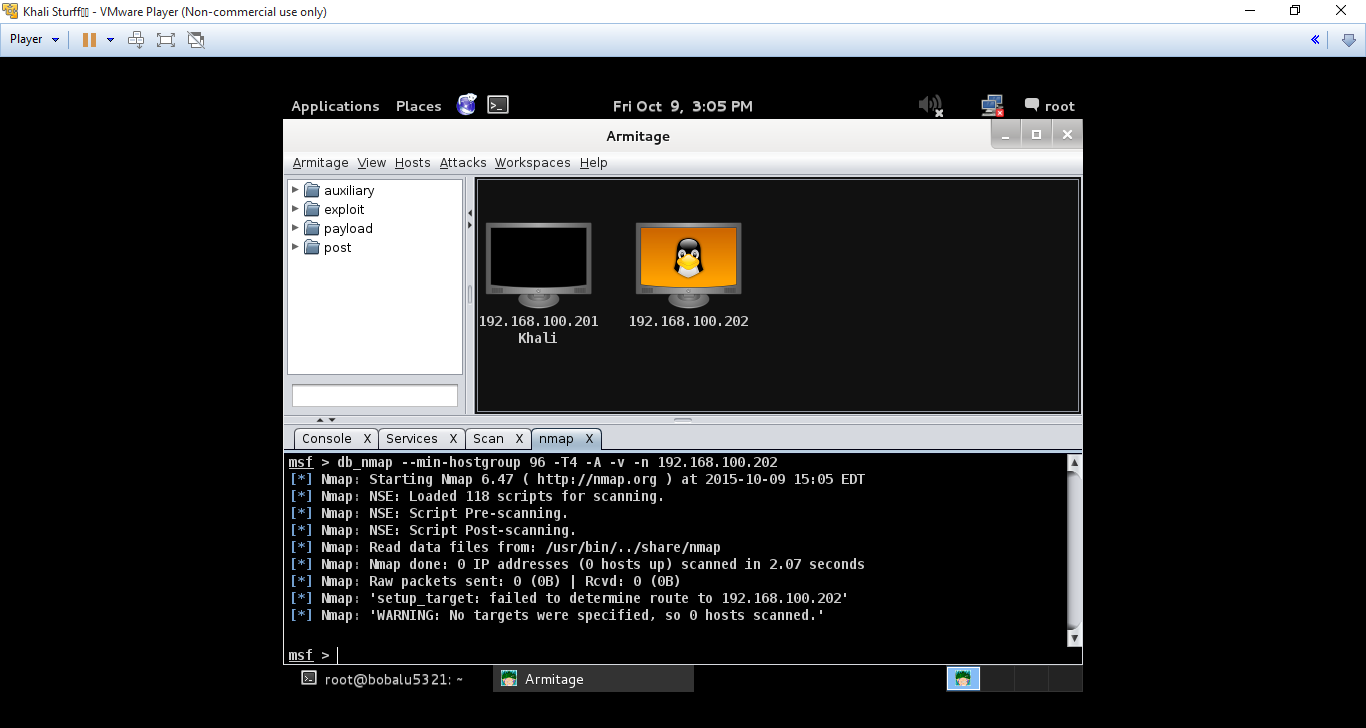
Although I still have a few troubles with my Metasploitable VM being detected (probably since I created a VM with Linux on it and the metasploit program so it isn’t exactly the same) I still am able to understand how Armitage works. It has a very user friendly interface that allows you to visually add and name each host, and it shows a different image for a host that has been compromised. It also allows you to exploit any target host with a number of different exploits after finding which one will work for the box. Essentially, it allows the user to run several different attacks on a system in a user friendly environment instead of just in code.

**Screenshots**

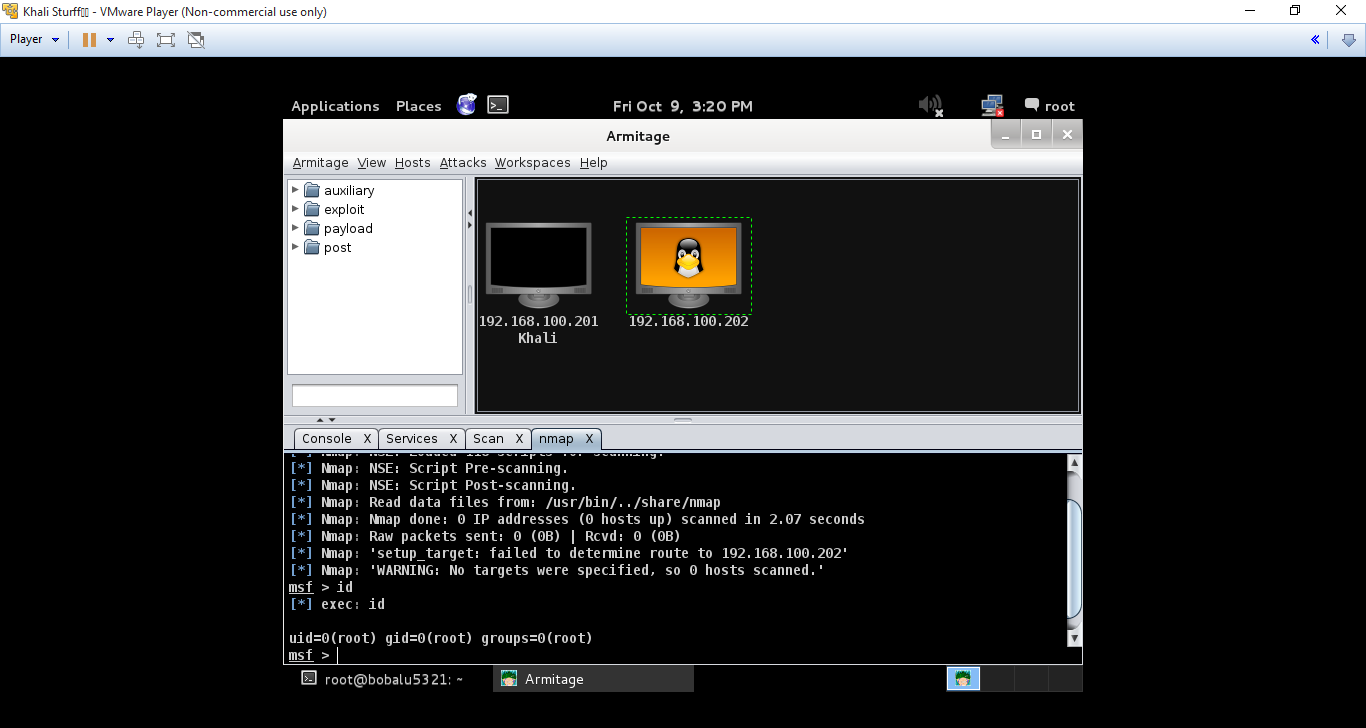
1. Screenshot of Armitage NMAP scan.



2. Screenshot of Armitage with Metasploitable host shown.



3. Screenshot of Armitage with Metasploitable host shown as owned and id command running on the console.



**Questions:**

1. What is Metasploit? **Software that is used for finding security vulnerabilities, and help manage security assessments**
2. What is Armitage? **It adds a GUI to the metasploit environment, making it more user-friendly**
3. Are you allowed to use Metasploit or Armitage to attack a box you do not own? Why or why not? **No, mainly because if it isn’t yours don’t mess with it, and it’s illegal**
4. What does it mean to “own” a box? **I assume it is referring to a virtual machine**
5. What does it mean to setup persistence on an owned box? **To help setup defenses for a system or virtual machine**
6. What does the backdoor we created do? **Allows you to run a terminal on the metasploit box to run commands on the system**
7. Find an exploit that works and cover in detail what you did. I.E. what exploit and the steps you took to find it and launch it. **I’ve been having trouble with finding my metasploit machine for whatever reason, but I researched how it works so from what I should have been able to do: 1) I would have ran an intense scan on the metasploit box and found a vulnerability then 2) used the exploit on the left window that correlated to the vulnerability and ran a successful attack and added a backdoor.**