Lab 10 – Network Scanning and Vulnerability Assessment

By

Lukas Fuller

IAE-201-D02

IA-201: Introduction to Information Assurance

**Abstract**

Conduct research on a network to find a machine and details about it. Use Nessus and Nmap to find out information about a specific machine on the network. Use Armitage to attack a machine using knowledge from Nessus and Nmap.

**Materials**

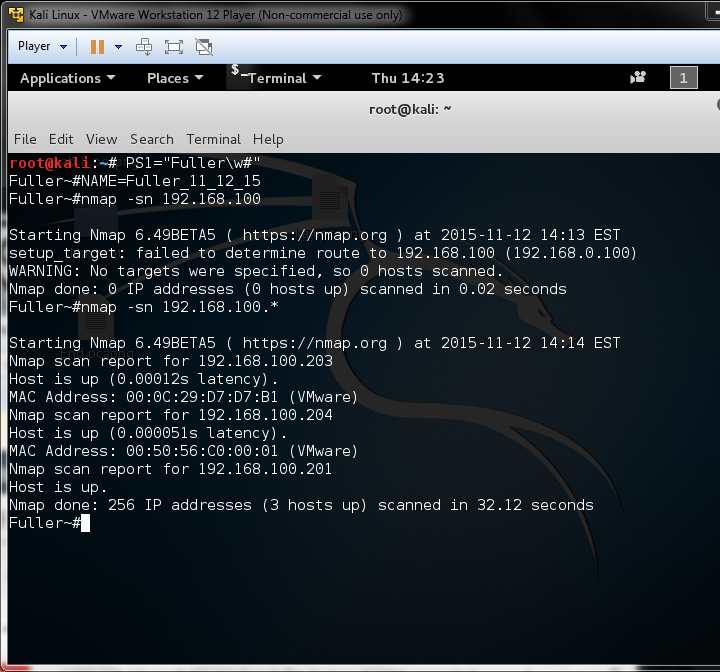
1. Kali Linux Virtual Machine
2. Internal Windows Server 2003 Virtual Machine
3. Nessus installed on your Host Machine

**Conclusion**

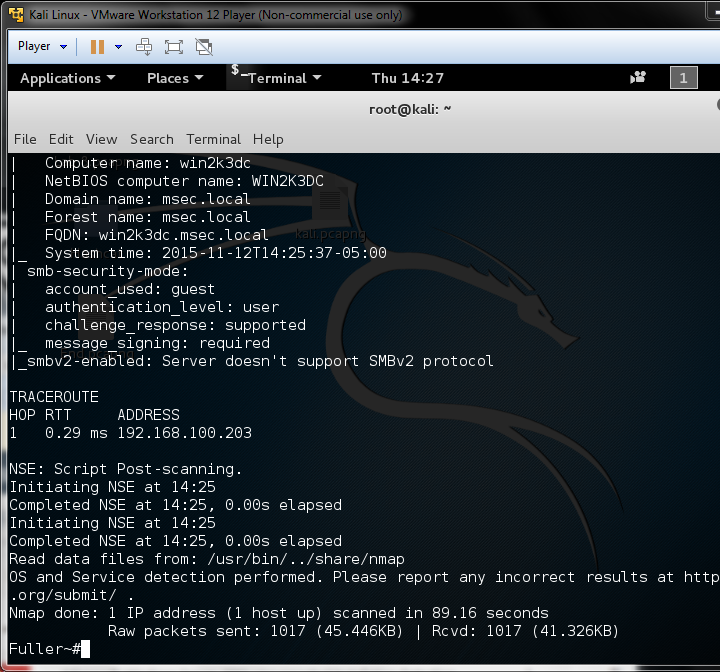
It took longer than expected, but after two class periods I was able to finish hacking into the Windows server VM. It was a bit confusing to me at first, and to be honest it still somewhat is. However, if I were to practice more on finding vulnerabilities, I feel like I could feel much more confident in being able to take control of a system. At this point I do have a basic understanding on how to work Armitage, Nessus, and Nmap, so I suppose that is good for now.

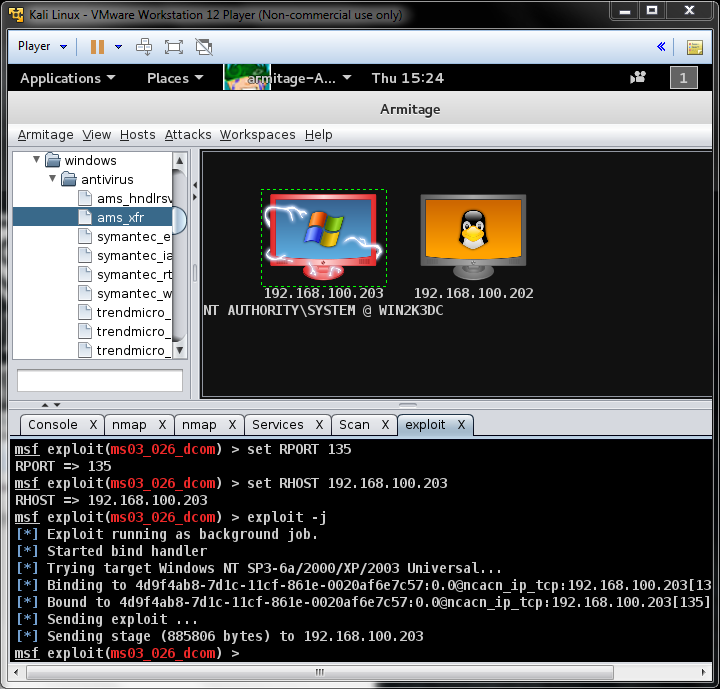
**Screenshots**

1. Step 9



1. Step 12



1. Step 15  
   

**Questions:**

1. Why did we do a ping scan with Nmap? **To make sure the host is up, and finds the desired target**
2. What type of information can be found from an Nmap intense scan? **Which ports are open**
3. What is Armitage? **A Graphic Interface version of Nmap and Zenmap that allows you to visually see the different types of attacks you can do on a system**
4. What exploit did you choose in the final step? **Microsoft RPC DCOM Interface Overflow**
5. Why did you choose that particular exploit? **Because Nessus revealed quite a few vulnerabilities, and one of the major ones was pertaining to the RPC being vulnerable**