Lab 12: Discovering Security Threats and Vulnerabilities

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

By the end of this lab, students will learn how to scan remote systems for open ports and vulnerabilities. Vulnerability scanners, such as Nessus from Tenable Security, are often used by people working in the field of information assurance to determine what steps can be taken to lock down systems and patch the holes. If vulnerabilities are not addressed, hackers can take advantage of them with tools like Metasploit.

**Materials**

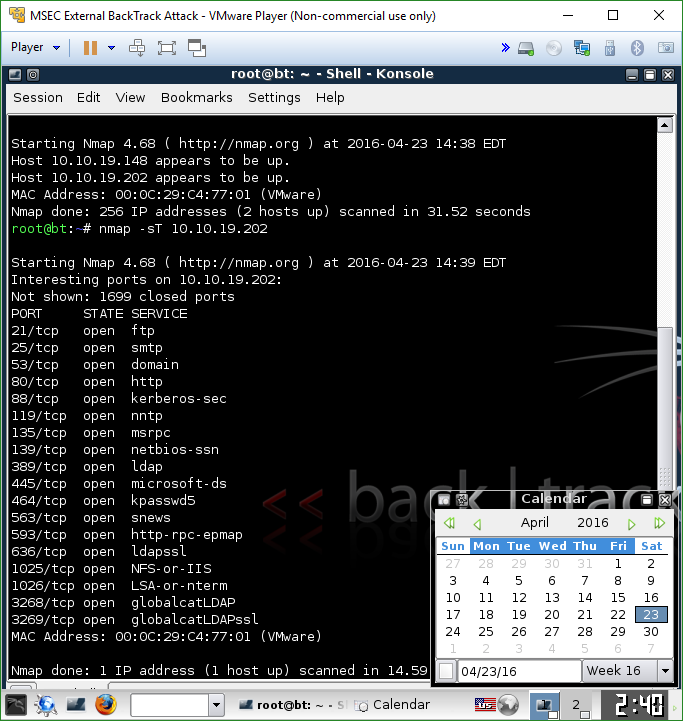
1. Backtrack 4
2. Windows 2003 External Victim Machine

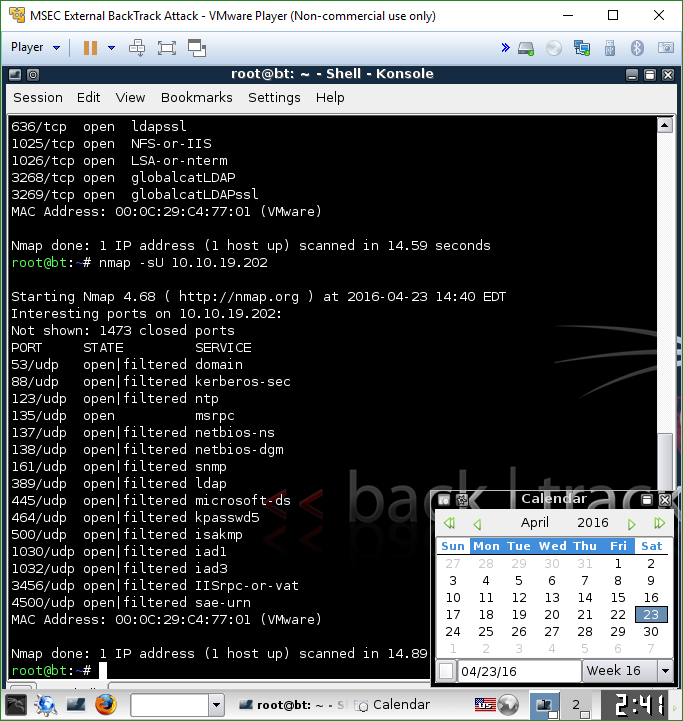
**Methodology**

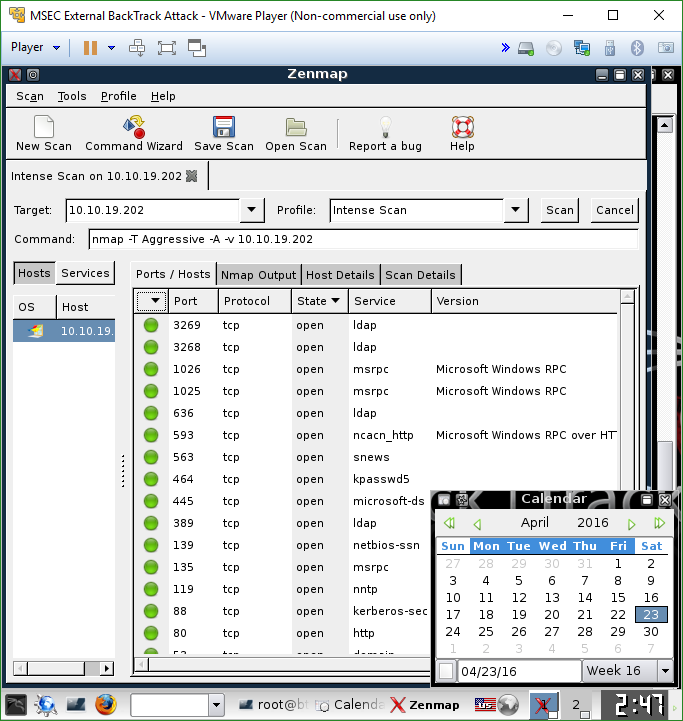
By using nmap, Nessus, and zenmap to find the host and figure out a particular exploit to use

**Lab**

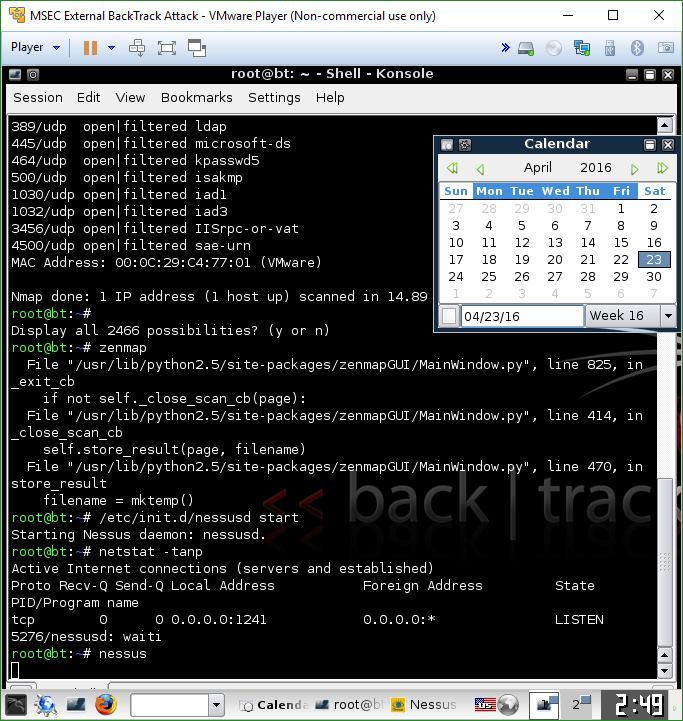
Task 1:

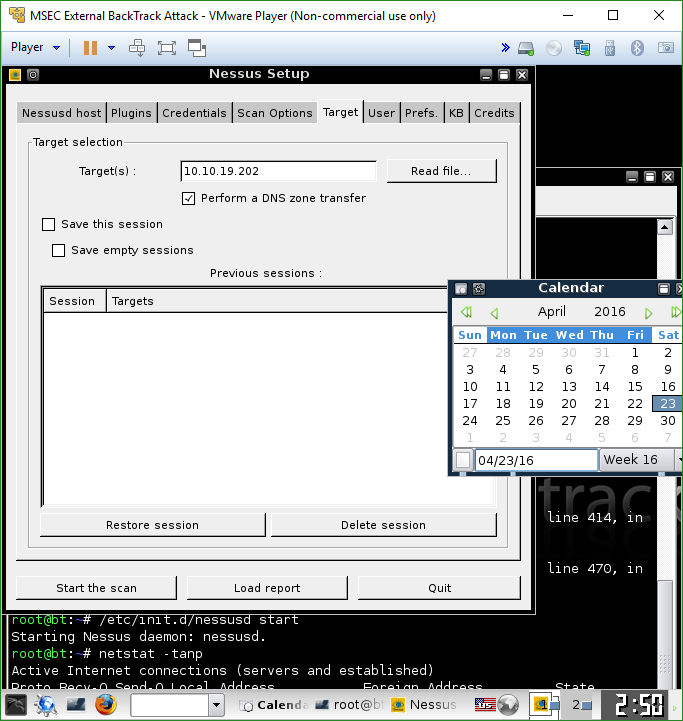
1. 

2, 

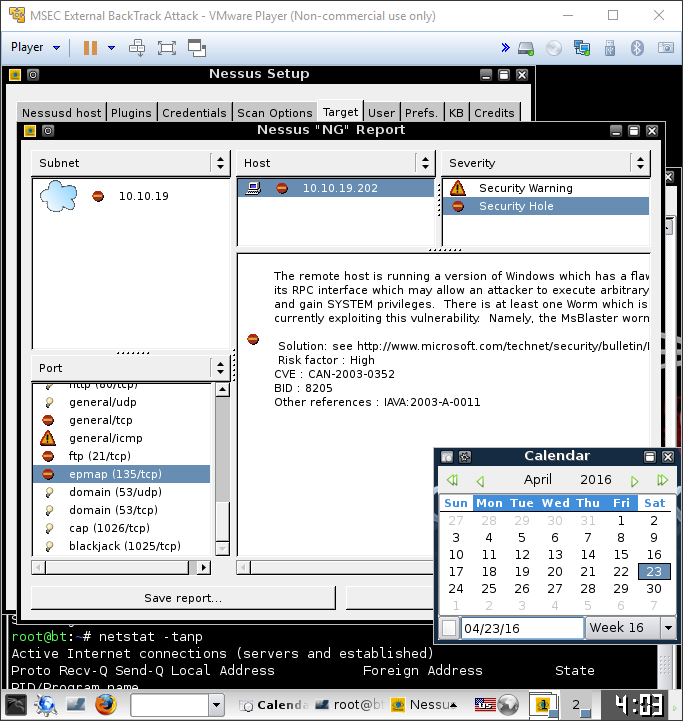
3. 

Task 2:

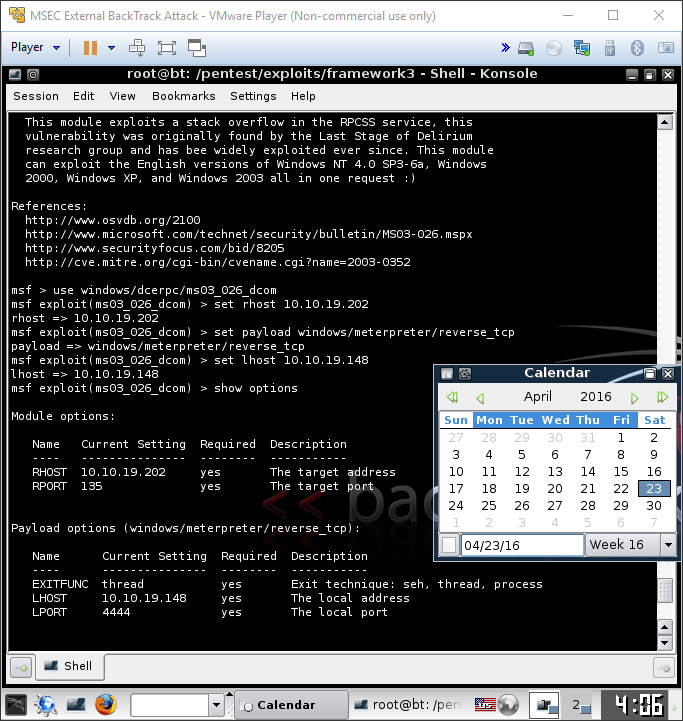
1. 

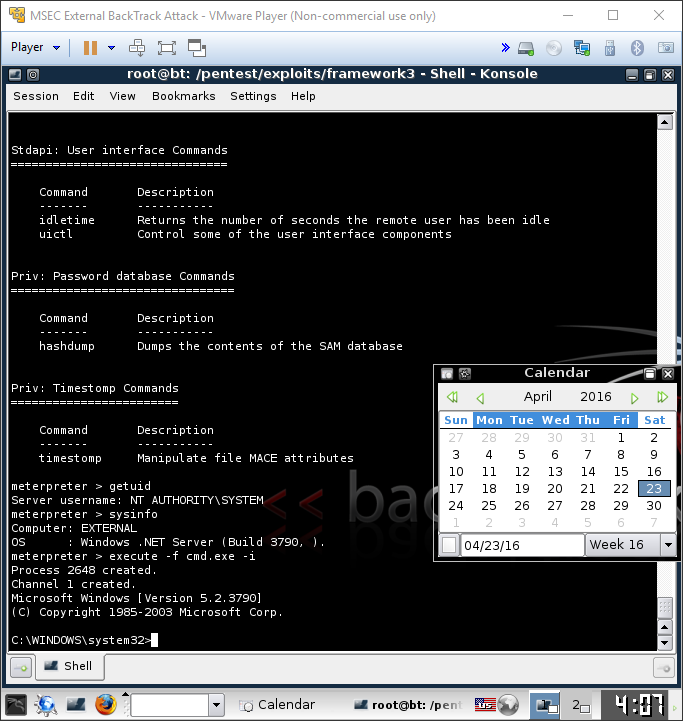
2.

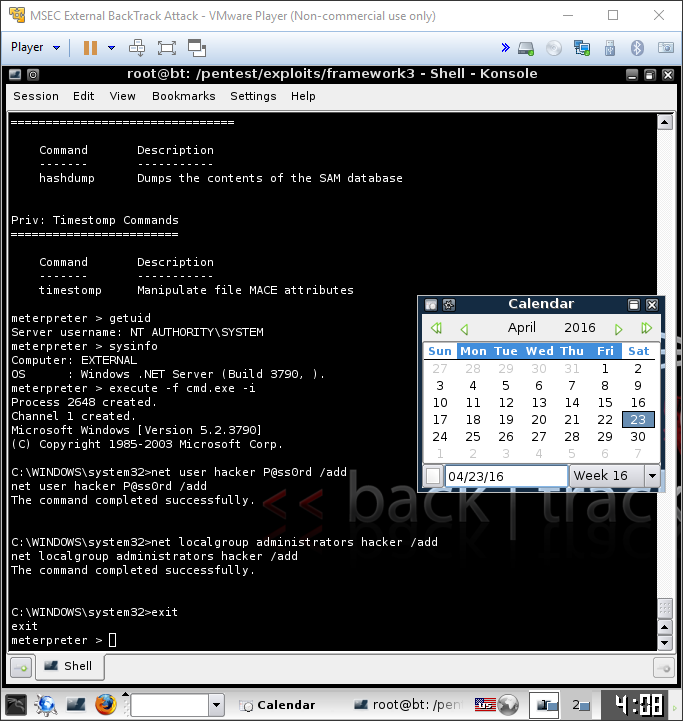
3.



Task 3

1. 

2.

3.

**Questions:**

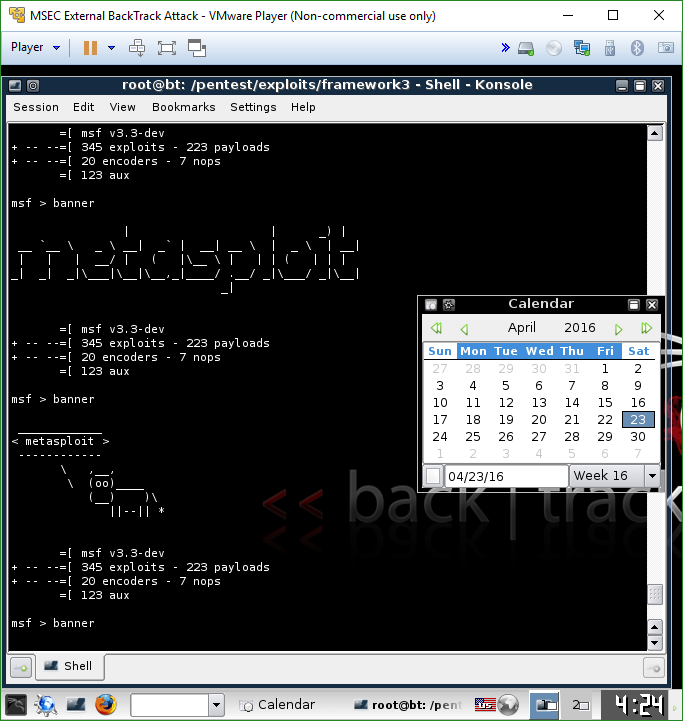
Task 1

1. Why is nmap useful for people working in the field of Information Assurance? **Because it can help find out which hosts are up on a network and then determine which TCP or UDP ports a remote system has running**
2. What is the best way to find out all of the available switches for nmap? **by typing nmap to see its options**
3. How can you perform a ping scan to determine alive hosts using nmap? **nmap -sP 10.10.19.\***
4. What is the syntax to scan a remote machine for open UDP ports? **nmap -sU 10.10.19.202**
5. What is the syntax to scan a remote machine for open TDP ports? **nmap -sT 10.10.19.202**

Task 2

1. Why do you need to be cautious when initiating a Nessus scan? **Because Nessus could possibly take down a system while it is being scanned**
2. What is the command to start the Nessus server? **/etc/init.d/nessusd start**
3. Which command can be used to verify that the Nessus server is running? **netstat -tanp**
4. Is it possible to run the Nessus client and server on the same machine? **Yes, but they don’t have to run on the same system**

Task 3

1. What is the command used to show all Windows exploits in Metasploit? **search exploits windows**
2. What is the command used to show all Macintosh exploits in Metasploit? **search exploits osx**
3. How can you learn more information about a particular exploit? **info exploit/\*\*\*\*(exploit’s address)\*\*\***
4. Launch msfconsole again. Use the banner command until you are able to get the picture of the cow. Type exit to leave the msfconsole environment. 

**Conclusion**

This lab took considerably longer for several reasons, but mainly due to my own fault (since I didn’t realize which VM it wanted me to use for a while). Also, the Nessus scan took a little over 30 minutes it seemed, but besides that the lab was rather self-explanatory. I’m familiar with Nessus because I used to a few times in my previous IAE class, but it was interesting to see it used on Backtrack 4 (since we used Kali). For the most part, the commands altered slightly, but the simple idea of acquiring the host’s address, setting up the rhost, lhost, and such was rather familiar as well. Overall, this lab made me more familiar with Nessus and the commands used in nmap.

**Grading Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | **Points Allowed** | **Points Actual** | **Comments** |
|  |  |  |  |
| **Title page** | **5** |  |  |
| **Screen shots** | **5** |  |  |
| **Questions** | **10** |  |  |
| **Conclusion** | **5** |  |  |
|  |  |  |  |
| **Extra Credit** |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Points** | **25** |  |  |