Lab 9: Analyze and Differentiate Types of Application Attacks

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

By the end of this lab, students will exploit a remote system running Windows Server 2003 using the Microsoft Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Buffer Overflow. This particular vulnerability was issued as Security Bulletin MS03-026 by Microsoft. Students will exploit this vulnerability on a remote system and then run a series of commands on the victim machine. After completing this lab, students will have a more comprehensive understanding of how attackers penetrate systems and importance of locking down machines.

**Materials**

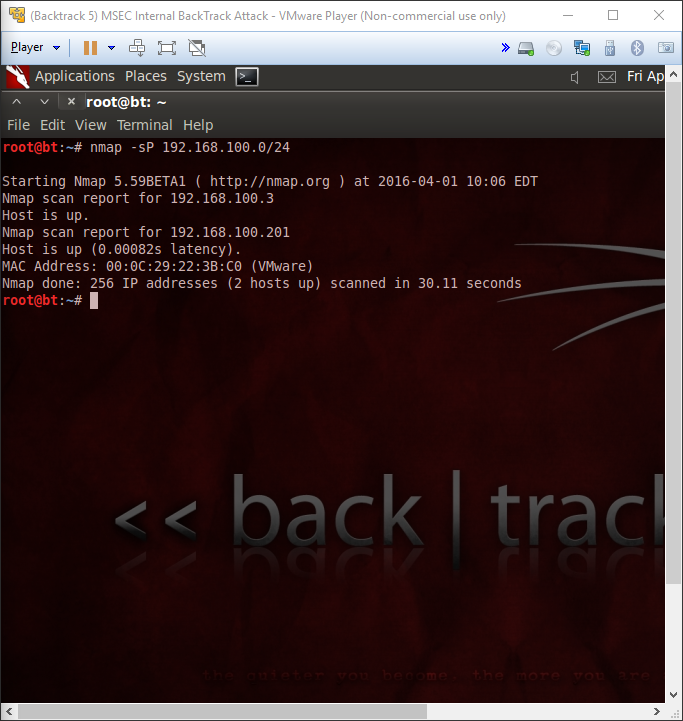
1. Backtrack 5
2. Windows 2003 Internal Victim Machine

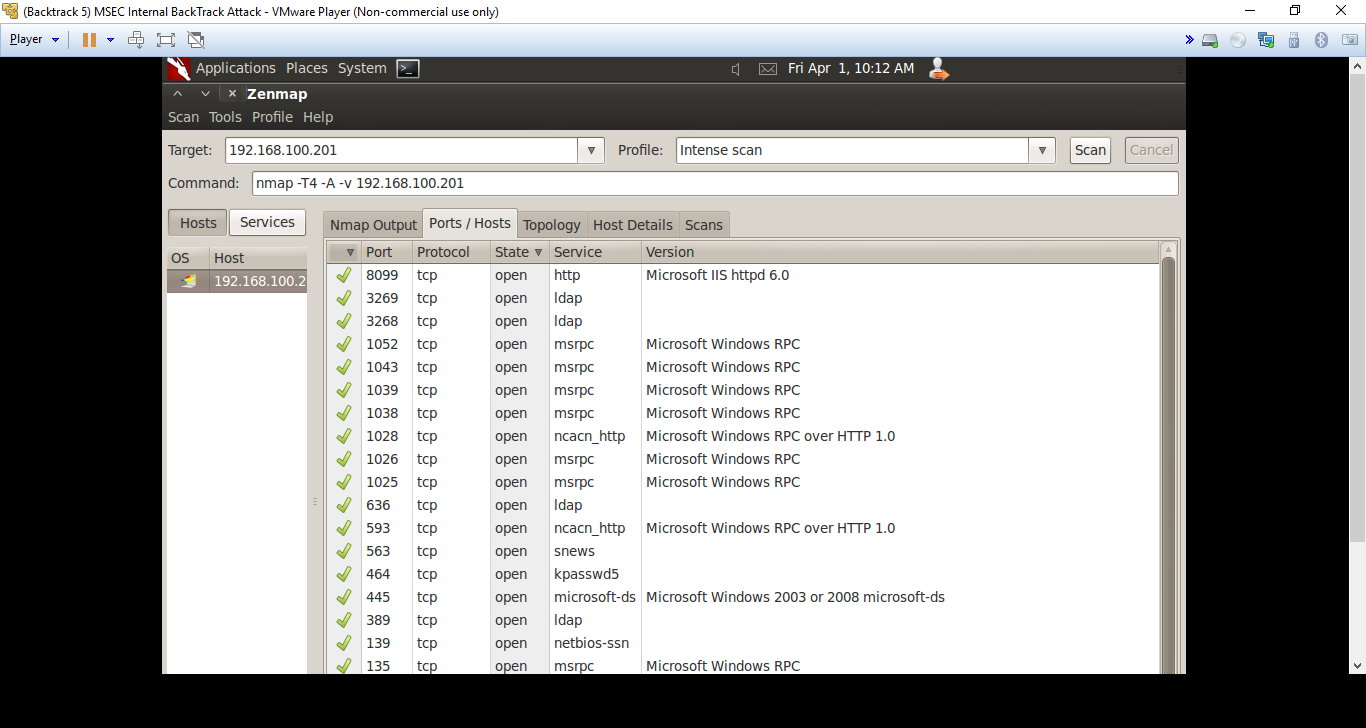
**Methodology**

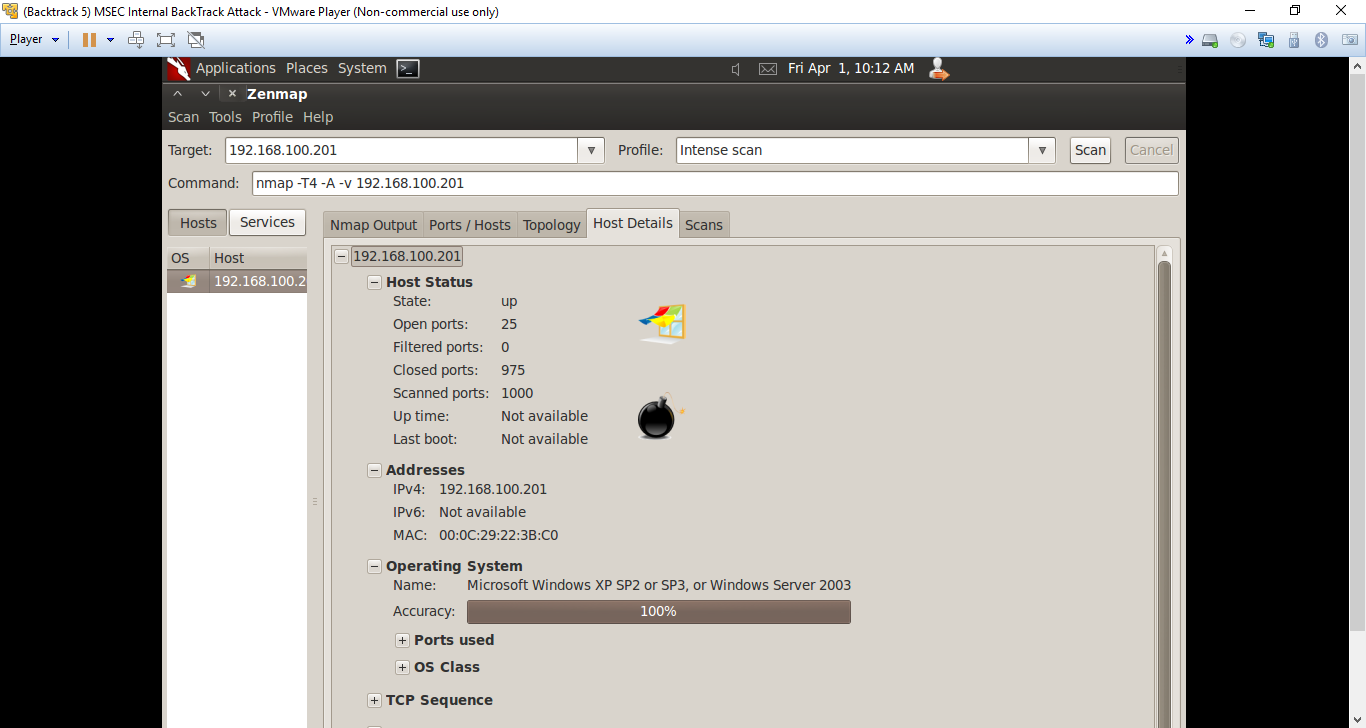
By using various commands such as nmap, zenmap, and Armitage to initialize the attack and gain necessary information for the attack

**Lab**

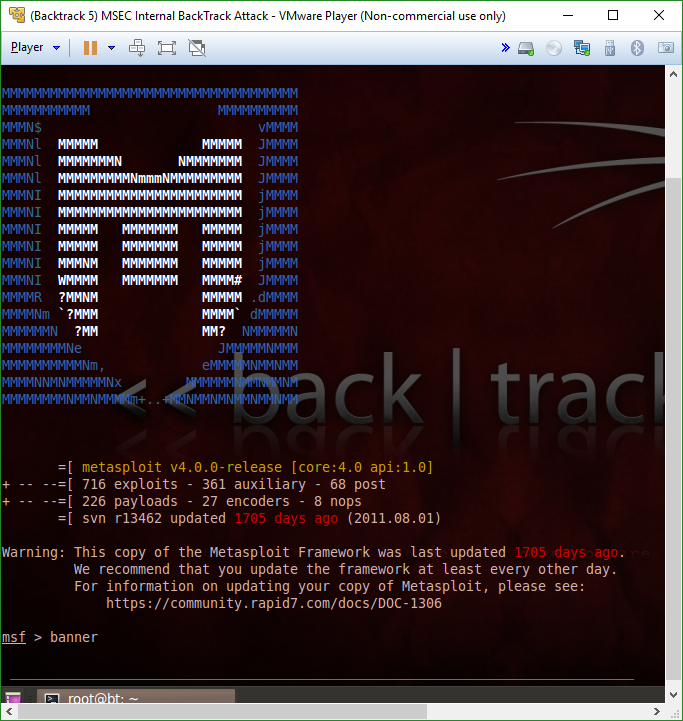
Task 1:

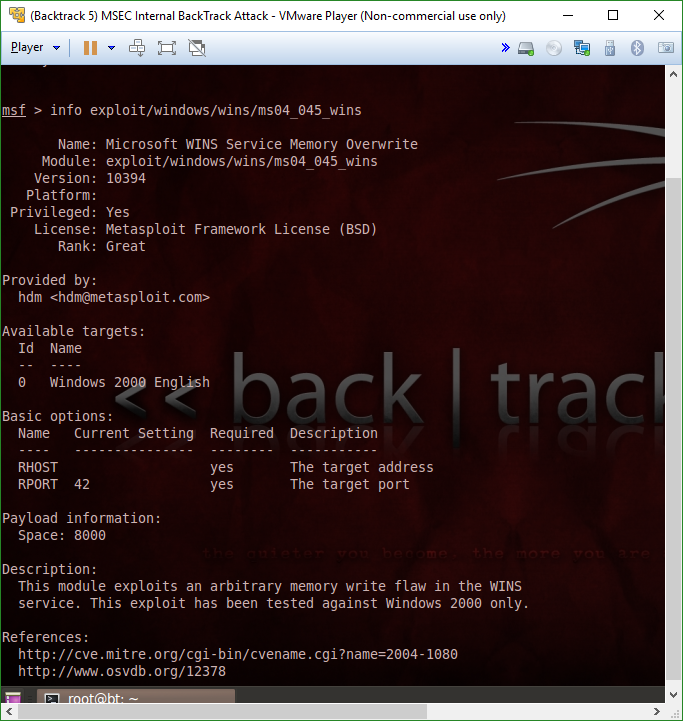
1. 

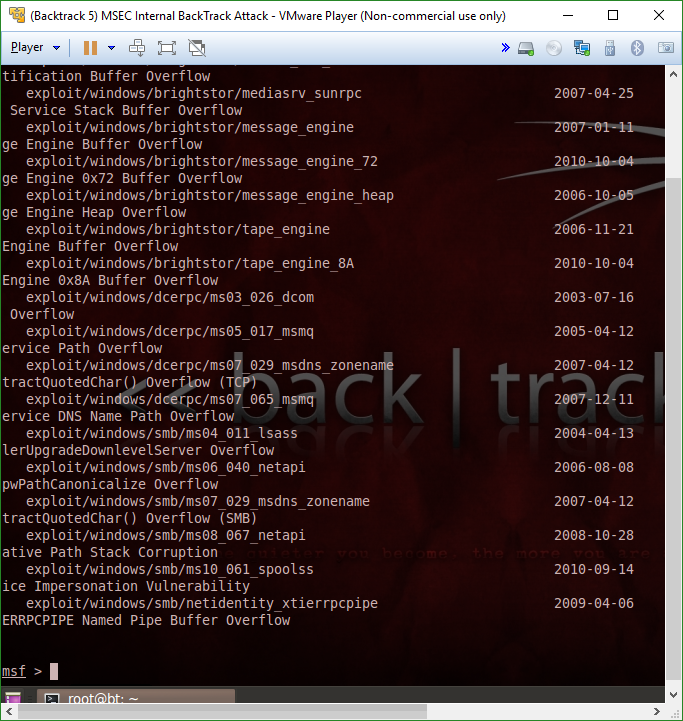
2, 

3. 

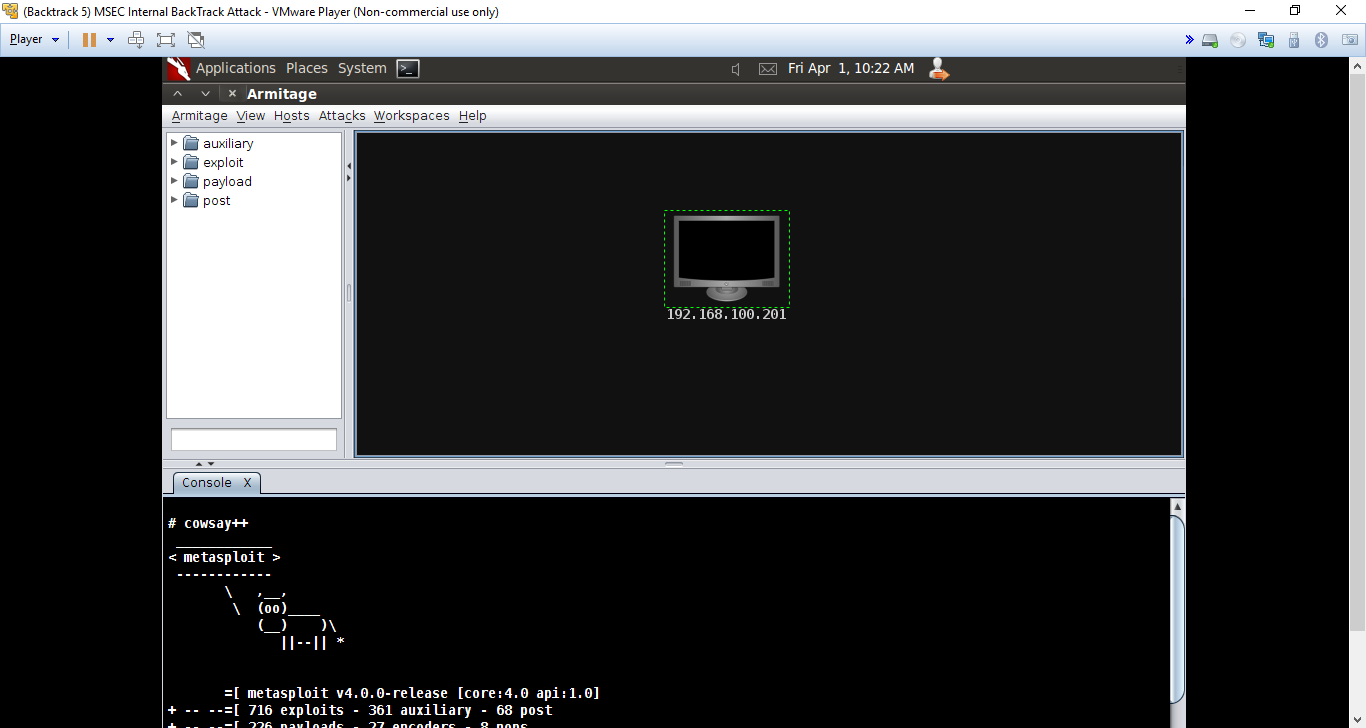
Task 2:

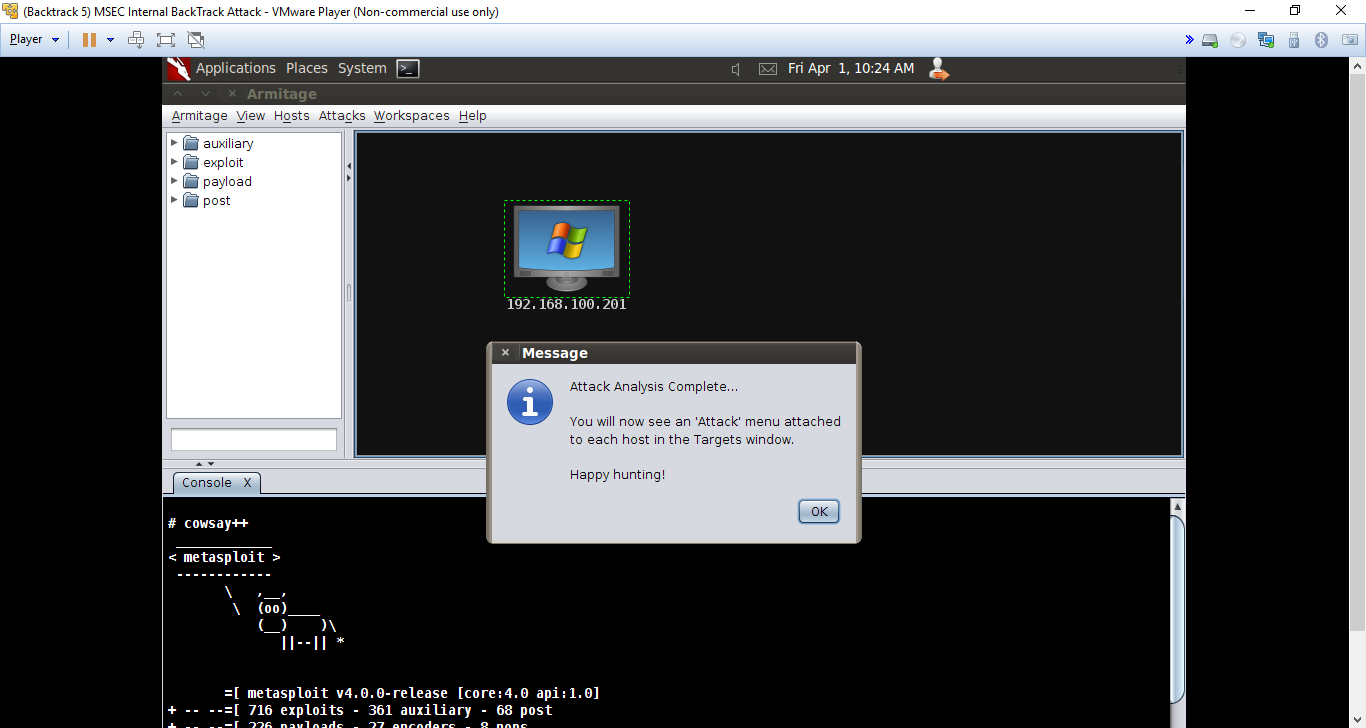
1. 

2.

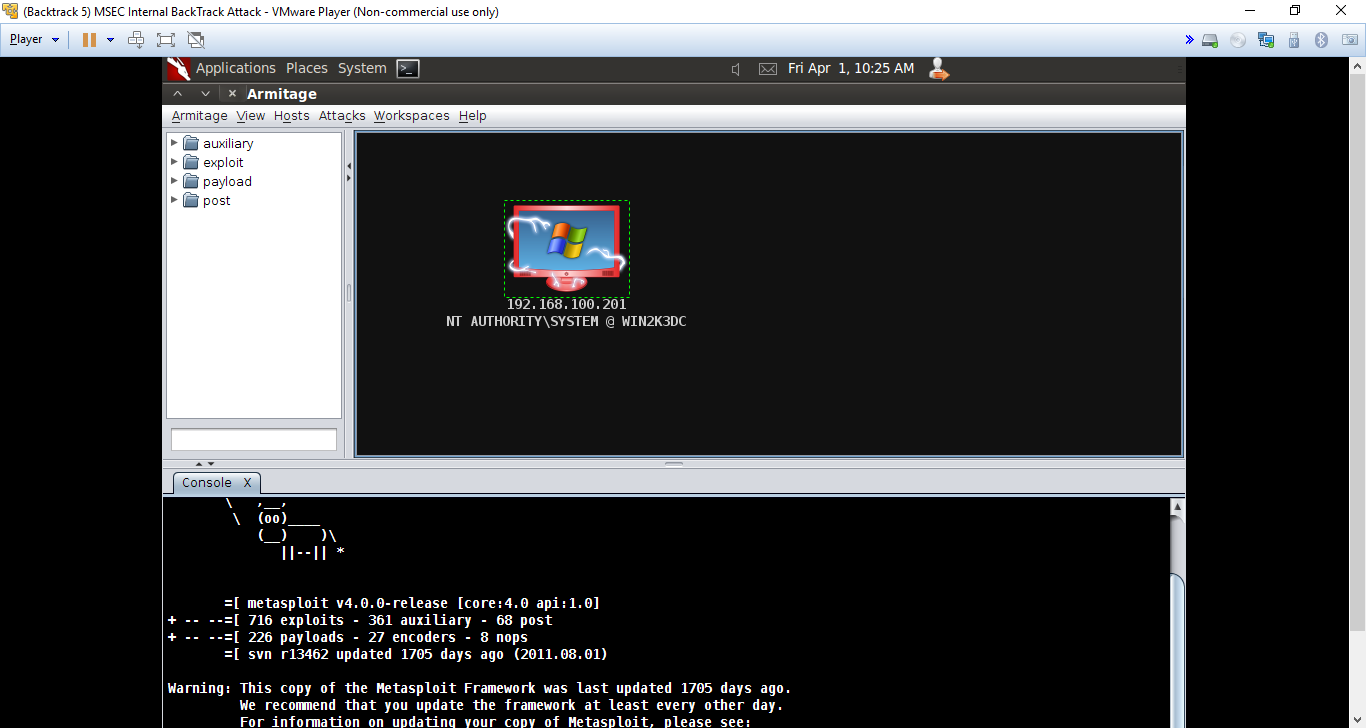
3.

Task 3

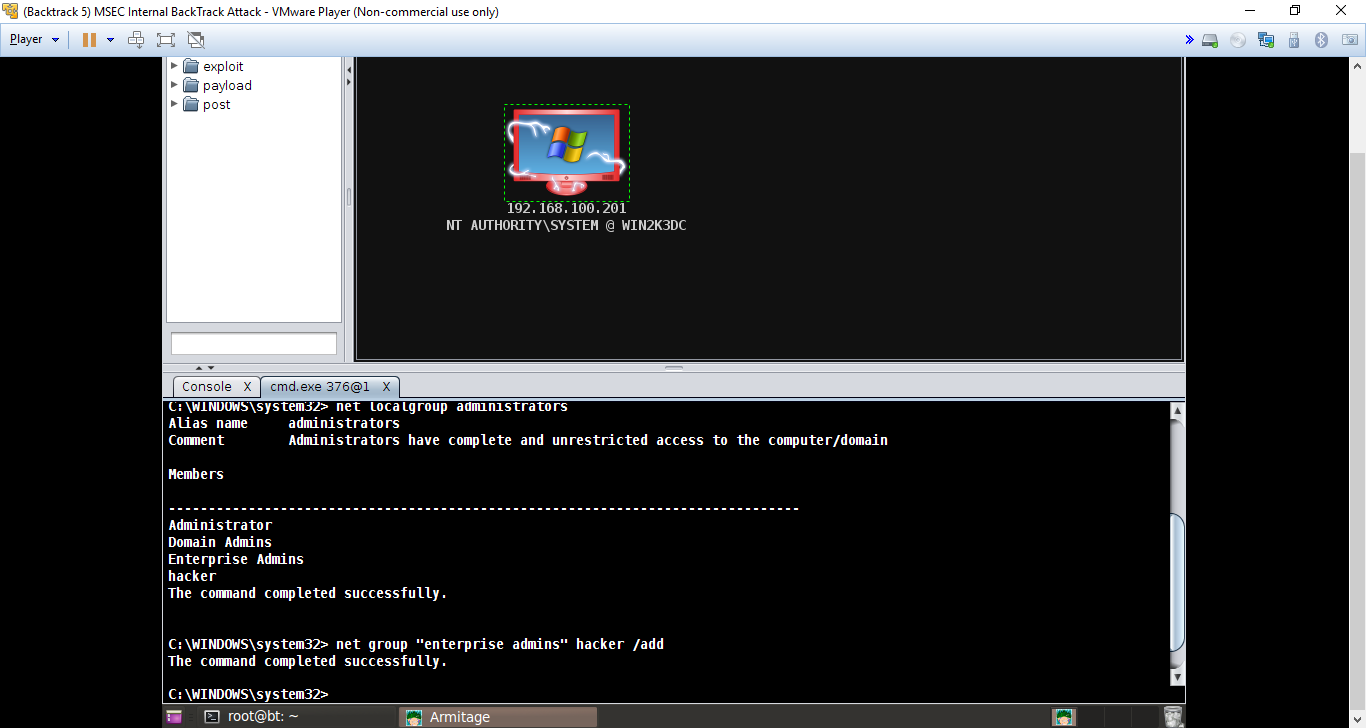
1. 

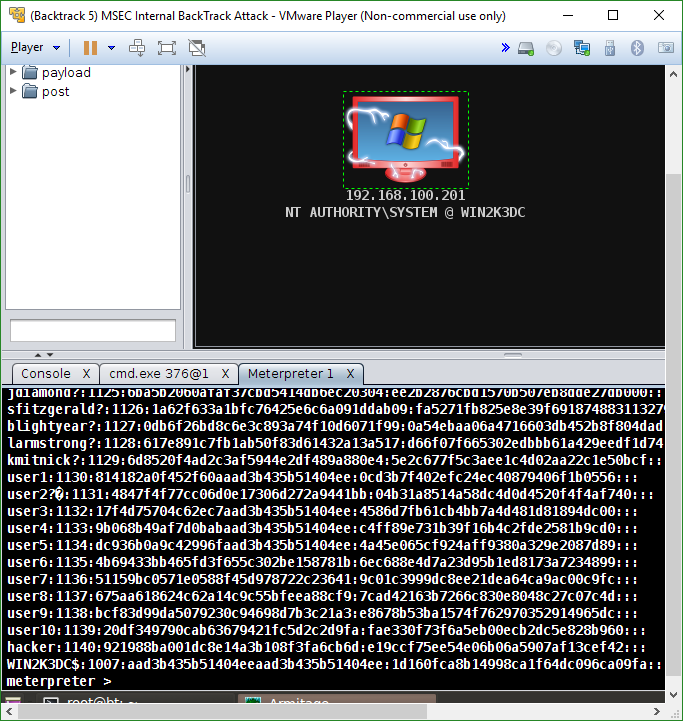
2.

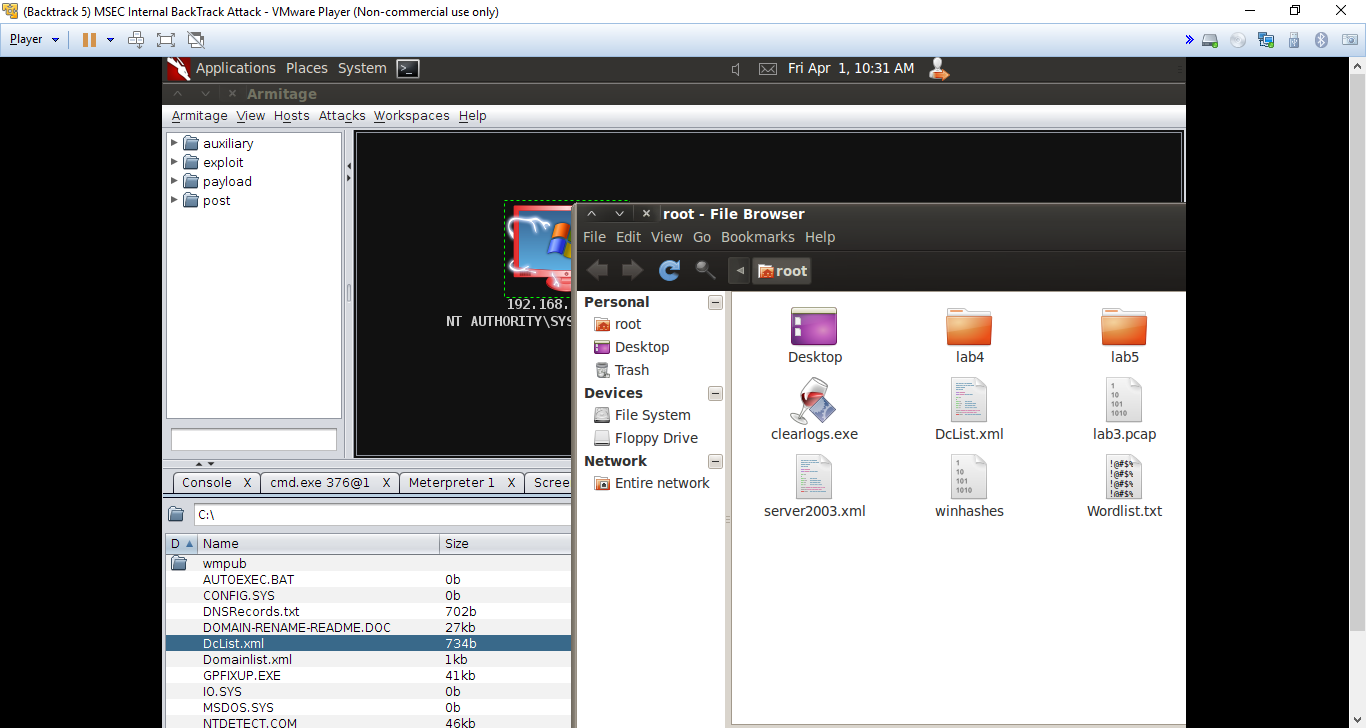
3.



Task 4:

1. 

2. 

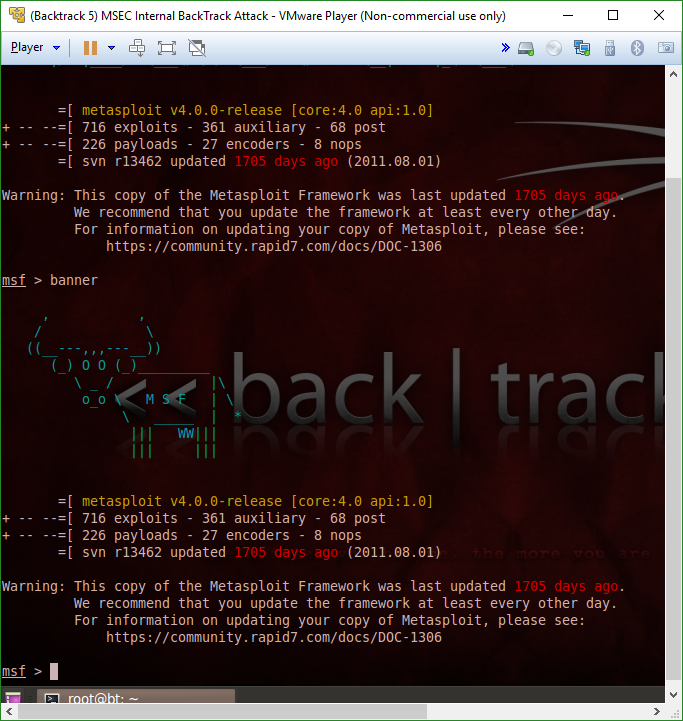
3. 

**Questions:**

Task 1

1. What features of Nmap are useful for people working in the field of information assurance? **The open TCP ports and open UDP ports (as well as the operating system & service pack level and the Banner messages)**
2. What is the purpose of a banner message and how might hackers use these messages to their advantage? **You could include something in the banner message to gather more information from the user, or play a game with them like many hackers have done previously (like wiping their pc’s hard drive if they can’t answer a question)**
3. Type **nmap -sU 192. 168.100.201** from the terminal in BackTrack to perform a UDP scan. Are the UDP ports that are open the same as the TCP ports? **No**
4. Type **nmap -O 192.168.100.201** from the terminal in BackTrack to perform an OS fingerprint scan. Does nmap give you the same OS version that Zenmap did? **It appears so**

Task 2

1. What is the command used to show all Windows exploits in Metasploit? **Search exploit/windows**
2. What is the command to show all Macintosh exploits in Metasploit? **search exploit/all (most likely won’t come up with one though)**
3. How can you learn more information about a particular exploit? **By using them or by reading about them**
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. 

Task 3

1. Armitage is a GUI front end for what exploitation tool? **Metasploit**
2. What message does Armitage display after you try to find attacks by port?  **Happy Hunting**
3. Explore the Armitage menu. What are some other features of the tool? **Different types of exploits for different types of machines or weaknesses, and many other options**
4. At what point is the victim machine considered to be compromised? **When the icon shows red around it and electricity as well as the error underneath it**

Task 4

1. What is the command to add a user to a system through the command line? **Net user name password /add**
2. What are some of the commands that can be used within Meterpreter? **Hashdump and sysinfo**
3. What tools can be used to crack passwords once you obtain the hashes? **Dictionary attack, brute force, and such**

**Conclusion**

This lab was much longer than the previous ones and focused mainly on the features to allow you take control of a user. Some of the commands included nmap, zenmap, and of course Armitage, as well as many others for specific types of processes. I was surprised by how easy some of it was to accomplish when you have the right focus on how to go about doing it. This is mainly because last semester I had a similar lab, but my VM’s never could connect to each other, so I had to do a lot more backtracking then actual attacking… Thankfully this time around it was much simpler and I didn’t have those issues. All around, this lab was very informational and allowed for me to understand different types of things you can do to a computer to first access it, then create a backdoor for later.

**Grading Rubric**

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