Lab 6: Incident Response Procedures

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

By the end of this lab, students will learn some of the various methods that can be utilized to determine if an attacker attempted or successfully compromised a system. Some information about the attacker, such as their IP Address, may be lost if the machine is shutdown. For this reason, volatile data is collected before shutting down.

**Materials**

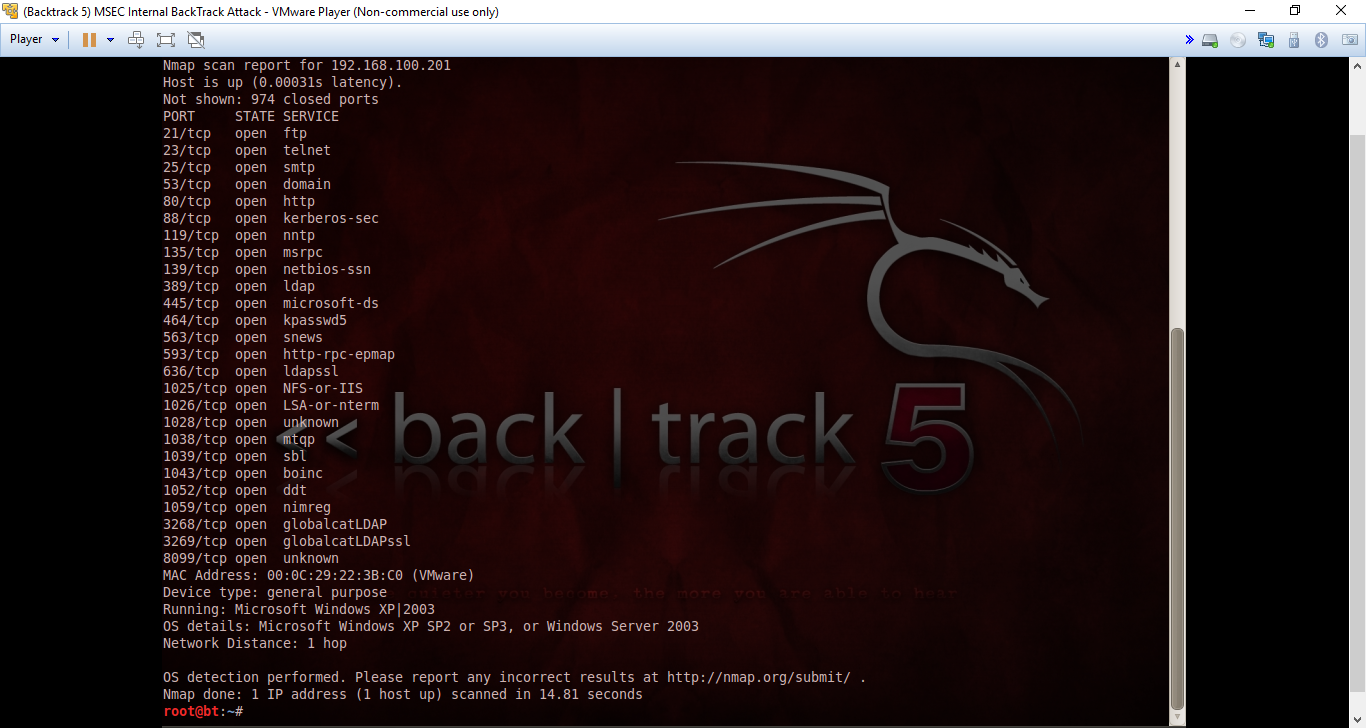
1. Backtrack 5
2. Windows 2003 Internal server

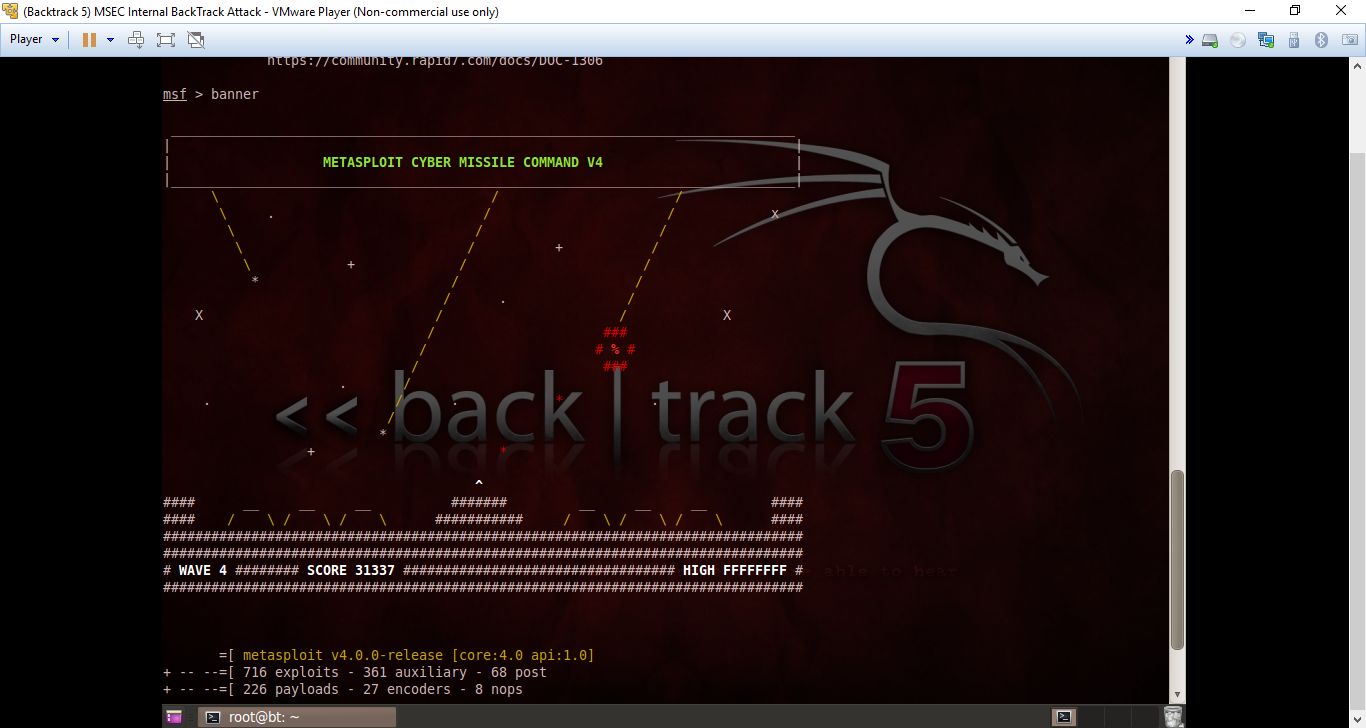
**Methodology**

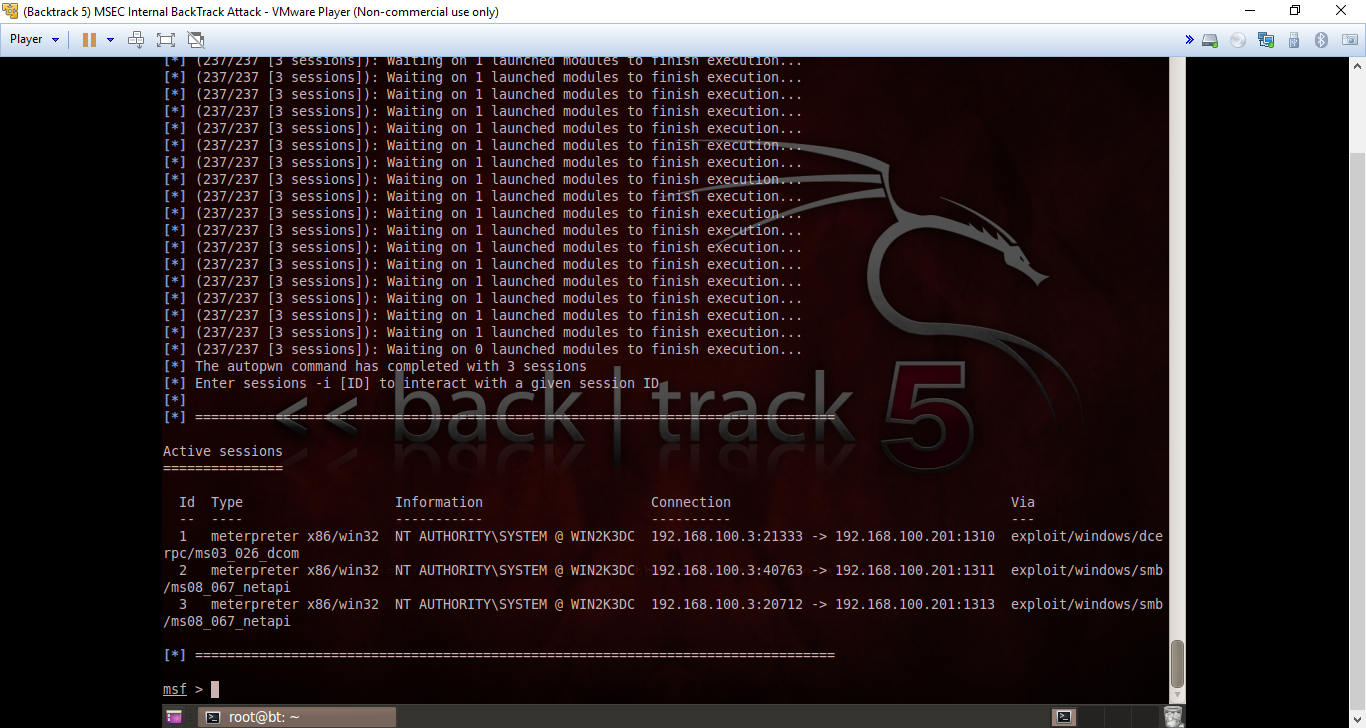
By using various commands such as db\_autopwn and netstat to first attack a system then gather information about the attack

**Lab**

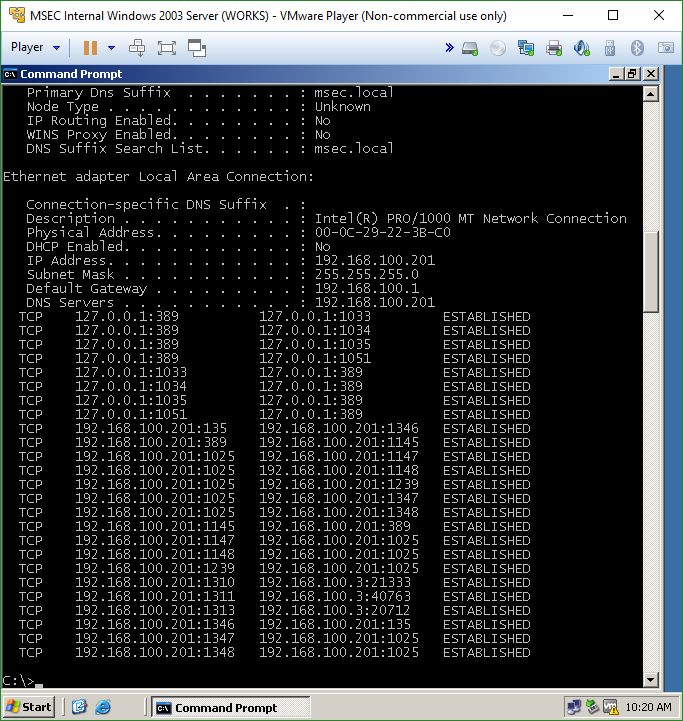
Task 1:

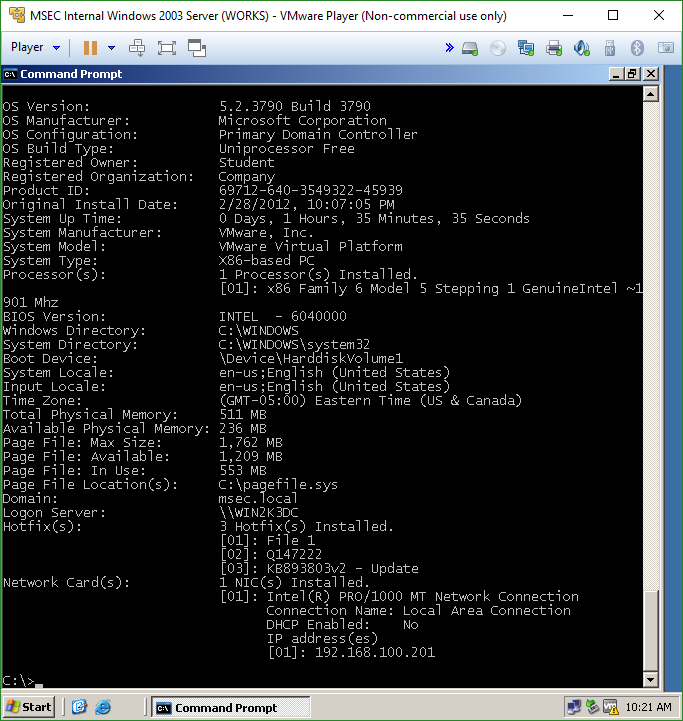
1. 

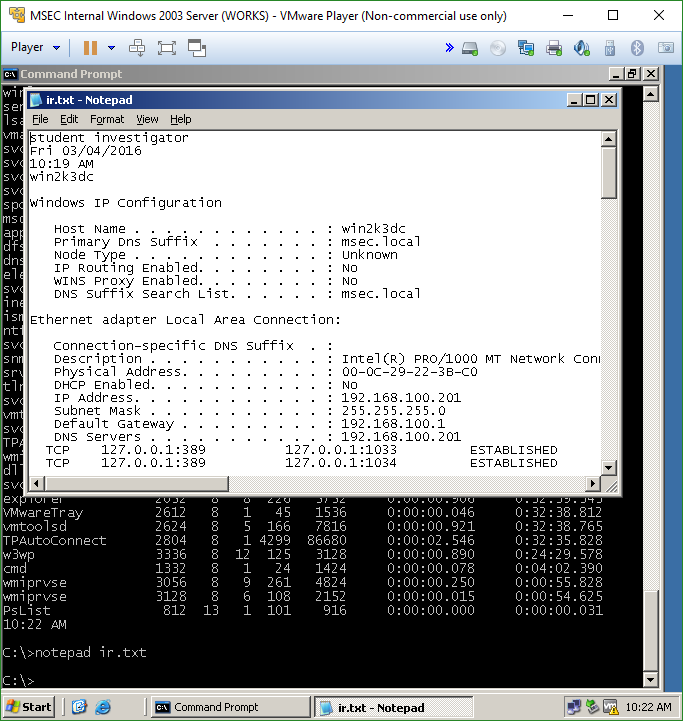
2, 

3. 

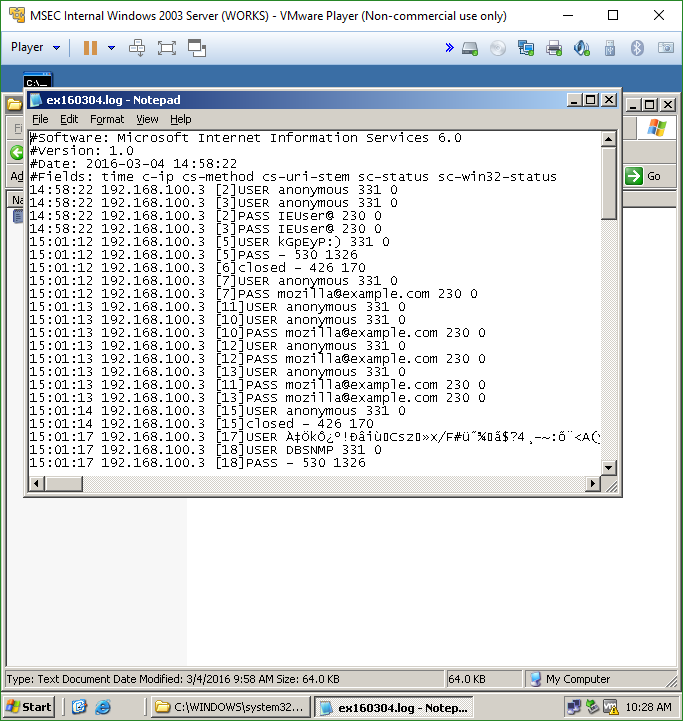
Task 2:

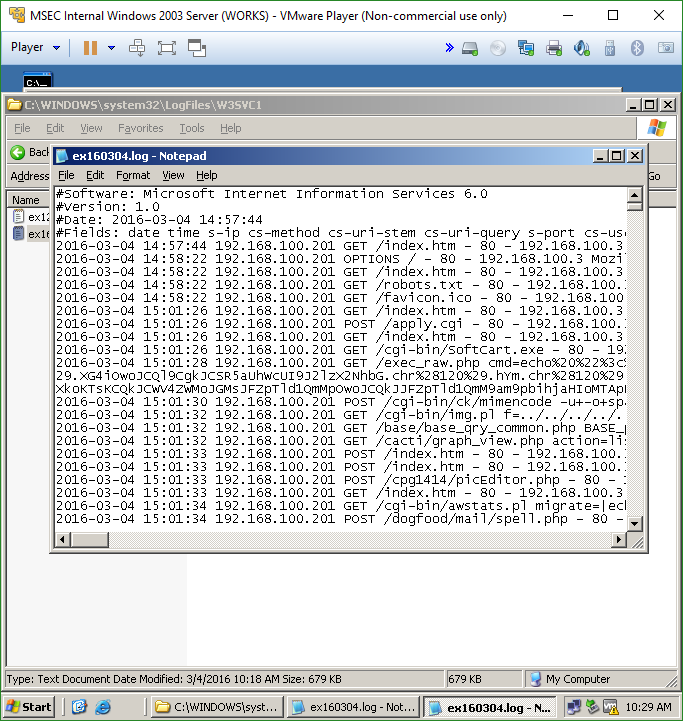
1. 

2.

3.

Task 3

1. 

2.

**Questions:**

Task 1

1. What is the command to scan the 192.168.100.0/24 network for hosts? **Nmap -sP 192.168.100.\***
2. What is the command to scan 192.168.100.147 for open TCP ports? **Nmap -sP 192.168.100.147**
3. How can you determine the operating system that the target system is running? **Nmap -O 192.168.100.201**
4. What command must be run before utilizing the db\_autopwn command? **msfconsole**

Task 2

1. What is the command to get important information about a Windows system? **systeminfo**
2. What is the command to view active connections to a machine? **netstat -an | findstr “ESTABLISED”**
3. What is the command to list all of the processes on a machine? **pslist**
4. What is the command to view the routing table? **netstat -r**

Task 3

1. Where are the log files stored on a Windows system? **Within the c drive, windows, system32 folders**
2. Where are the FTP log files stored on a Windows system? **Within the log files, the MSFTPSVC1 folders**
3. Where are the WWW log files stored on a Windows system? **Within the log files, the W35YC1 folders**
4. Explain the naming format for log files within Windows. **I believing it has to do with the date at which the log file is created, and the area that is accessed as well is indicated next to the time-stamp**

**Conclusion**

This lab was reasonably self-explanatory and it included a few commands that I’m now a bit more familiar with for example the db\_autopwn and netstat commands. I have used the netstat before but never the autopwn, and it was interesting to see it used to gather any open ports information via an nmap scan. Also, it had several instances where I was appending commands into a specific log file, which I’m familiar with doing in a Linux based environment, but it was good practice especially since I haven’t used the Pipe command in a while. Lastly, it was helpful to learn how to gather information on a system before the data is lost due to the nature of the information itself.

**Grading Rubric**

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