Lab 8: Analyze and Differentiate Types of Attacks Using Window Commands

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

By the end of this lab, students will be able to view resources on the network, map network drives, and perform administration on remote systems from the command line. Many commands built into the operating system, such as the net command, can be used to access resources. These commands can be used by an insider to attack the network.

**Materials**

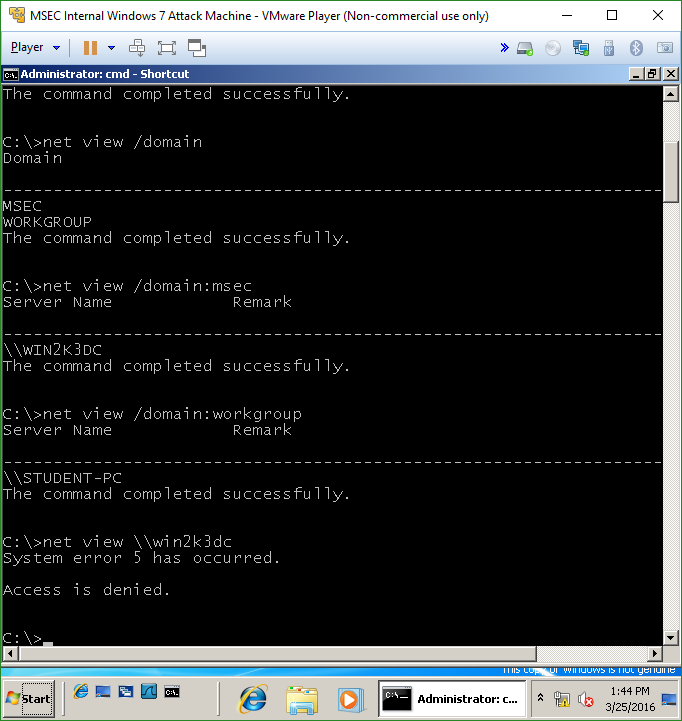
1. Windows 2007 Internal Attack Machine
2. Windows 2003 Internal Victim Machine

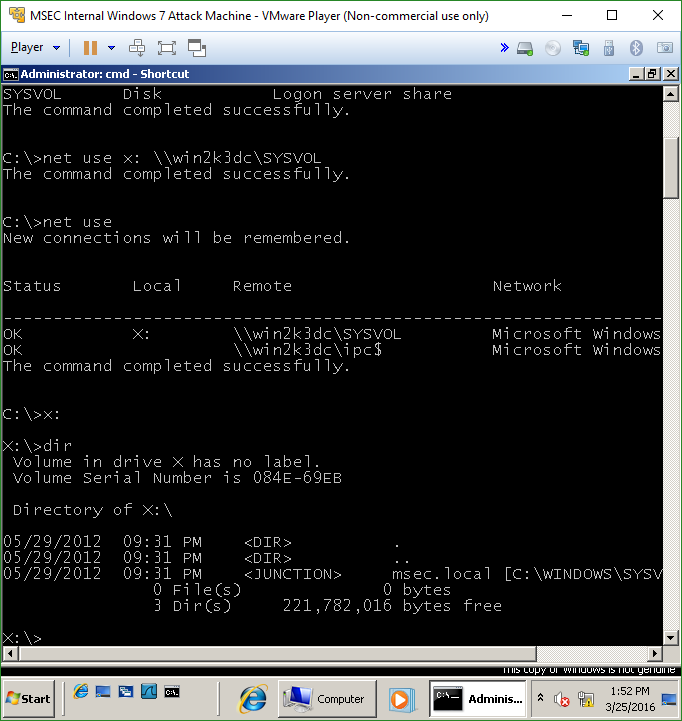
**Methodology**

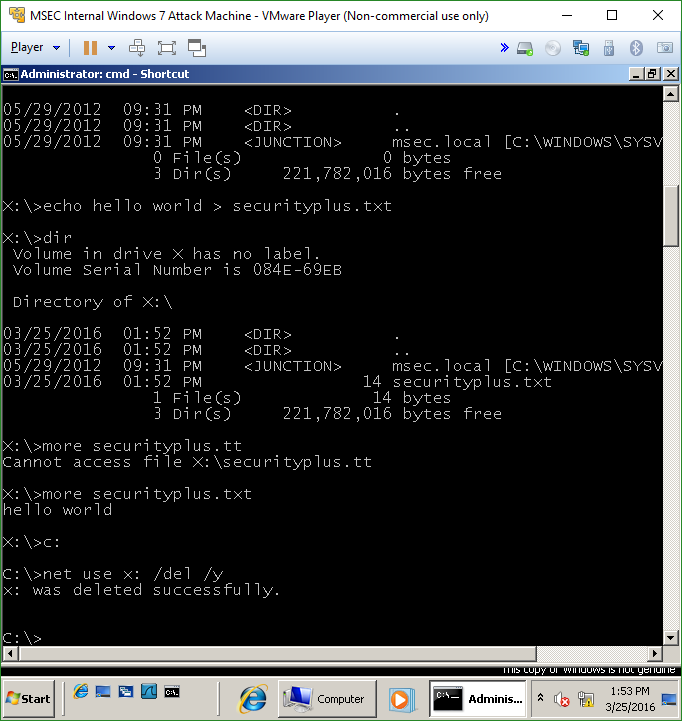
By using various commands such as psexec, net command, sc, and hostname commands as well as others

**Lab**

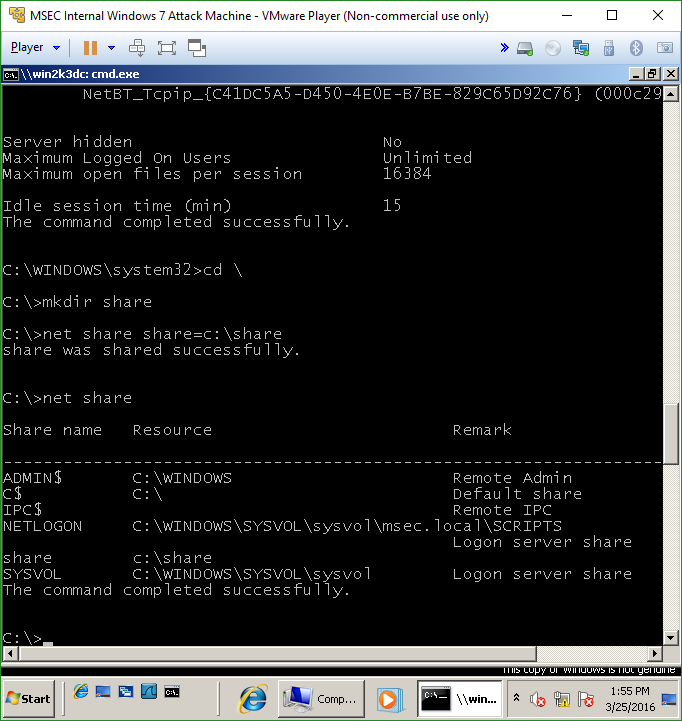
Task 1:

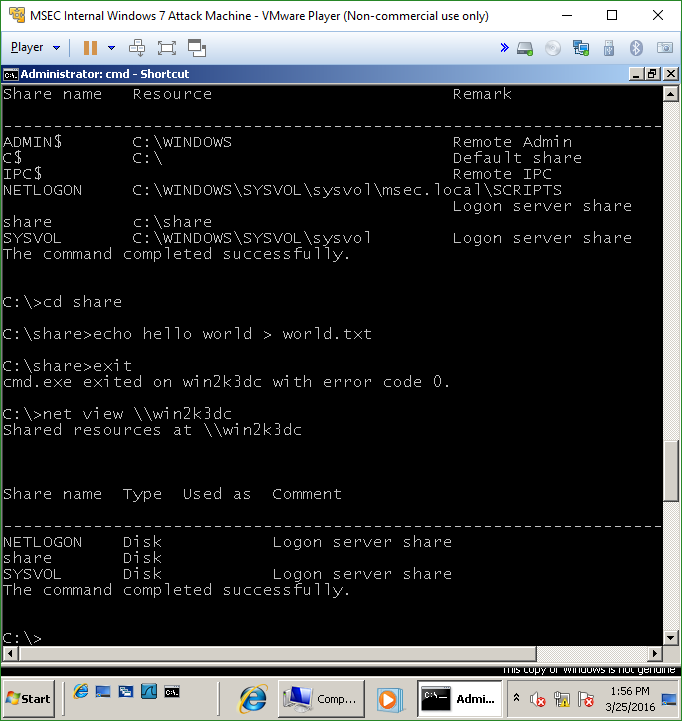
1. 

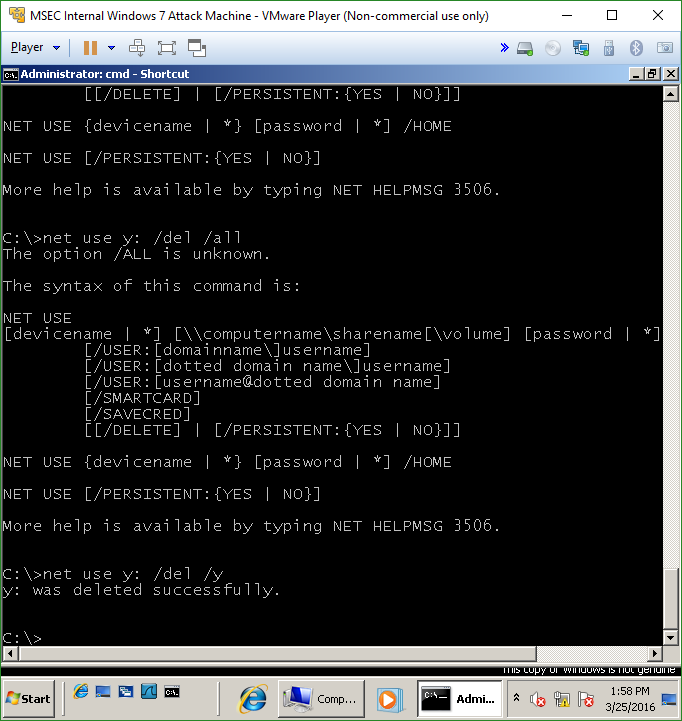
2, 

3. 

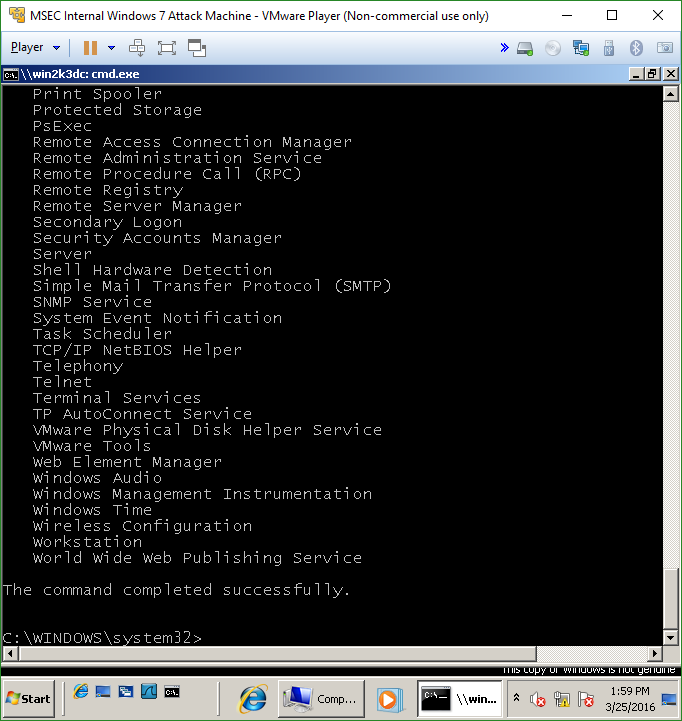
Task 2:

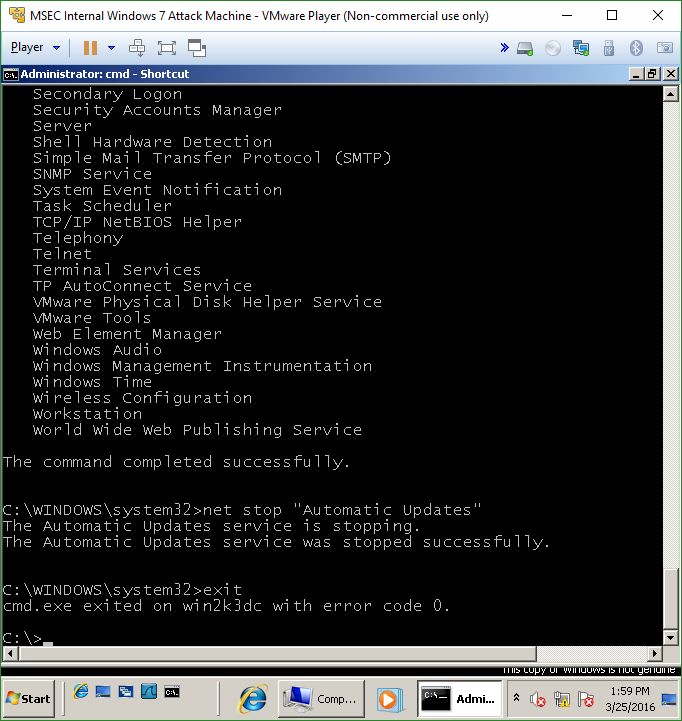
1. 

2.

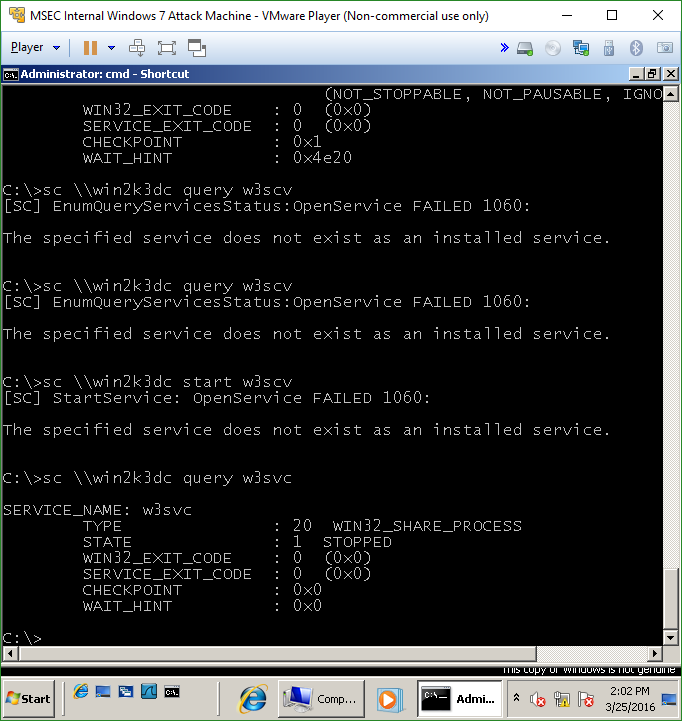
3.

Task 3

1. 

2.

3.



**Questions:**

Task 1

1. What is the command to view your workgroup? **net view /domain**
2. What is the command to enumerate all of the domains on the network? **net view /domain:msec**
3. What is the command to map a drive? **net use x: \\win2k3dc\sysvol**
4. What is the name of the share that will give you access to all resources on the remote machine? **net use \\win2k3dc\ipc$**

Task 2

1. From where do you get the PSEXEC command? **From a Microsoft website download**
2. Do you need to provide credentials when using PSEXEC? **No**
3. What is the command to share a folder on your C: drive called share? **net share share=c:\share**
4. What does an error code of 0 indicate when you are using PSEXEC? **When using PSEXEC it indicates a successful operation even though it’s an error code…**

Task 3

1. What is the net command to stop the Windows Update Service? **net stop “Automatic Updates”**
2. What is the sc command to get the list of services on a remote machine? **sc** [**\\win2k3dc**](file:///\\win2k3dc) **query | more**
3. What is the sc command to stop the W3SVC service on a remote system? **Sc** [**\\win2k3dc**](file:///\\win2k3dc) **stop w3svc**
4. What is the sc command to start the W3SVC service on a remote system? **sc** [**\\win2k3dc**](file:///\\win2k3dc) **start 23svc**

**Conclusion**

This lab felt a bit shorter than the others, I suppose because it was only using new commands on Windows 7, so it was relatively straight forward. However, it provided a decent number of commands that I wasn’t aware of like the sc for service control, psexec to start and stop services without using the task manager, and some other net commands as well. In particular the one that I found useful was the psexec command, because of the lack of control on Windows 10 apparently. From what my dad told me, certain programs won’t show up on the task manager, which is rather annoying, but if you know an alternative like psexec to stop something from running, in my eyes that’s very nifty. Overall the lab was helpful for learning new commands in a windows environment.

**Grading Rubric**

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