Lab 11: Mitigation and Deterrent Techniques – Password Cracking

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 crack the passwords of user accounts on Linux and Windows systems. Students will use brute force techniques and dictionary attacks to crack the passwords of users on the Linux and Windows operating system.

**Materials**

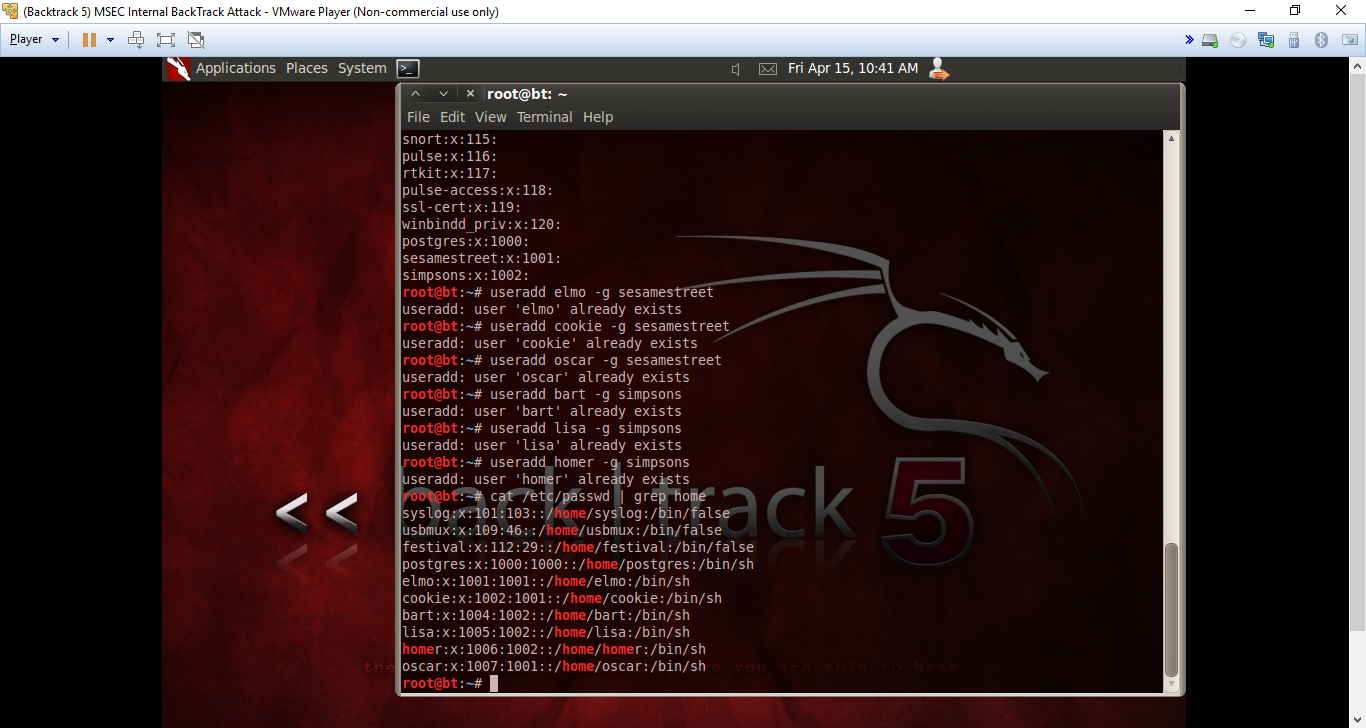
1. Backtrack 5
2. Windows 2003 Internal Victim Machine
3. Windows 7 Attack Machine

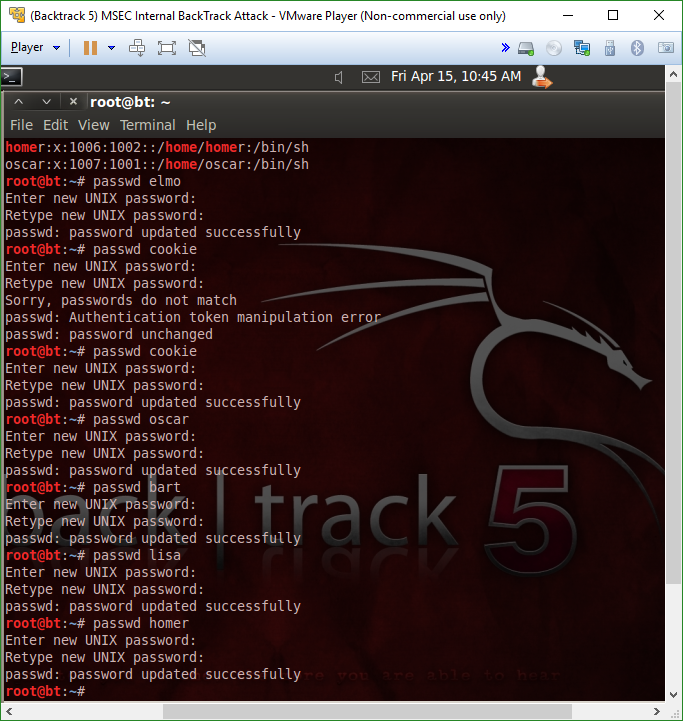
**Methodology**

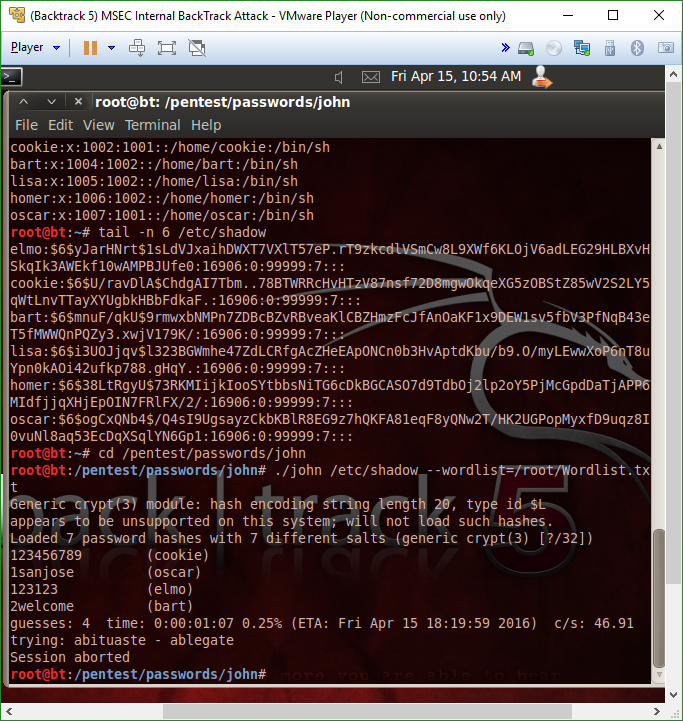
By using both cain and john the ripper

**Lab**

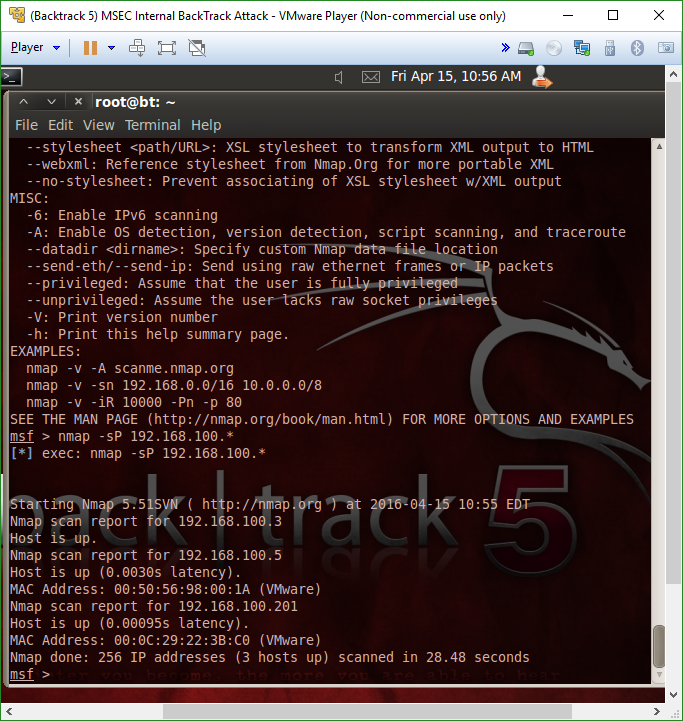
Task 1:

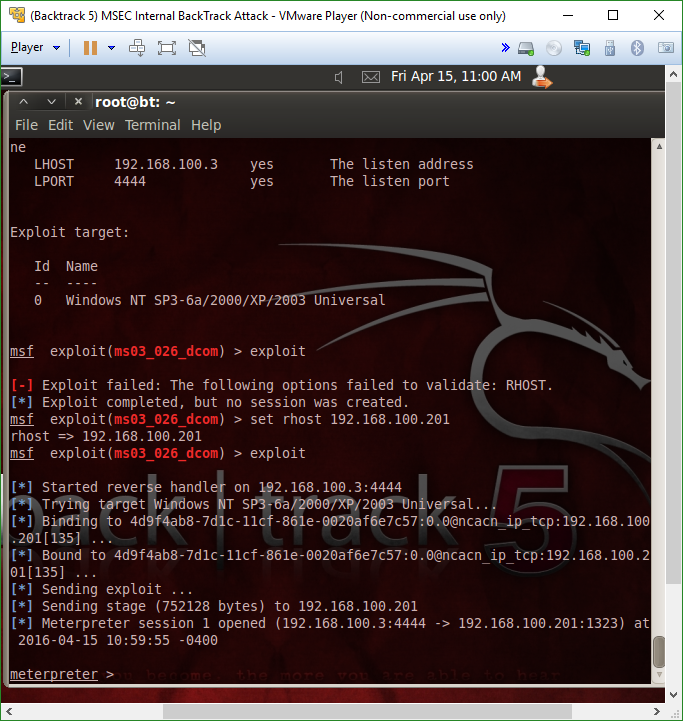
1. 

2, 

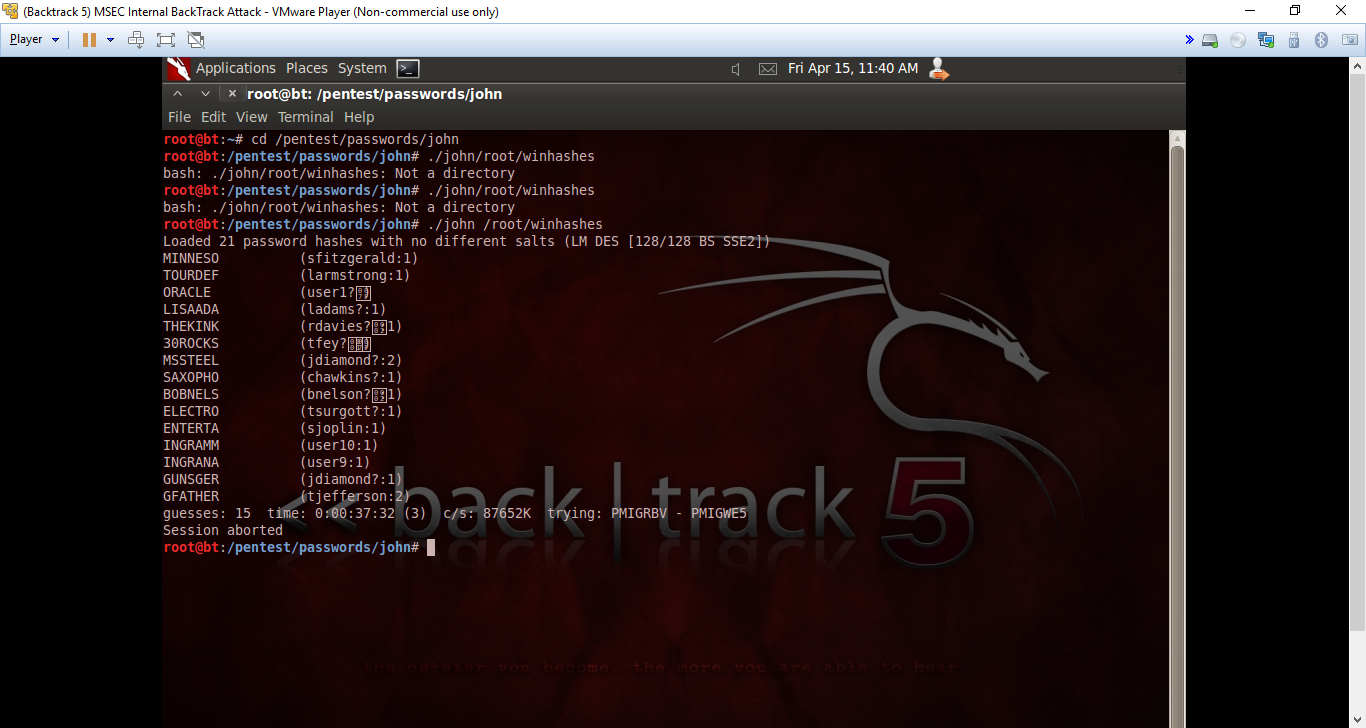
3. 

Task 2:

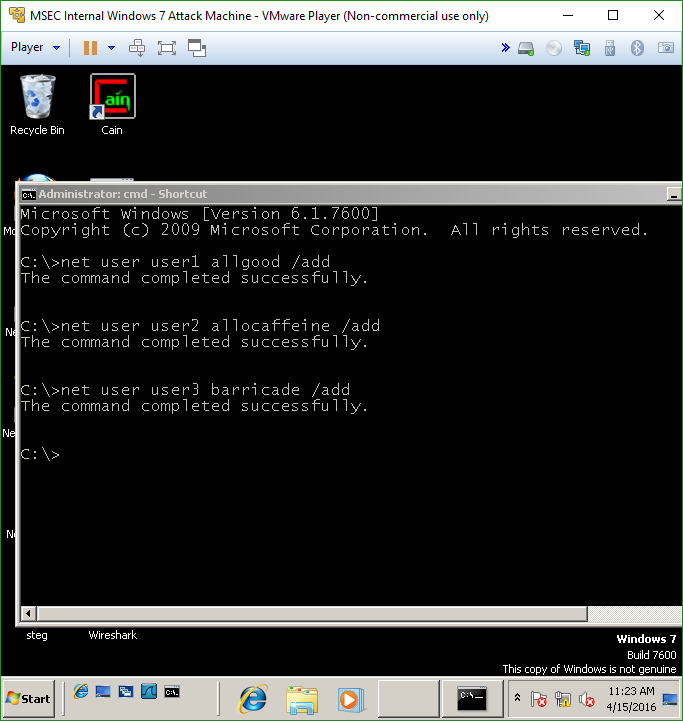
1. 

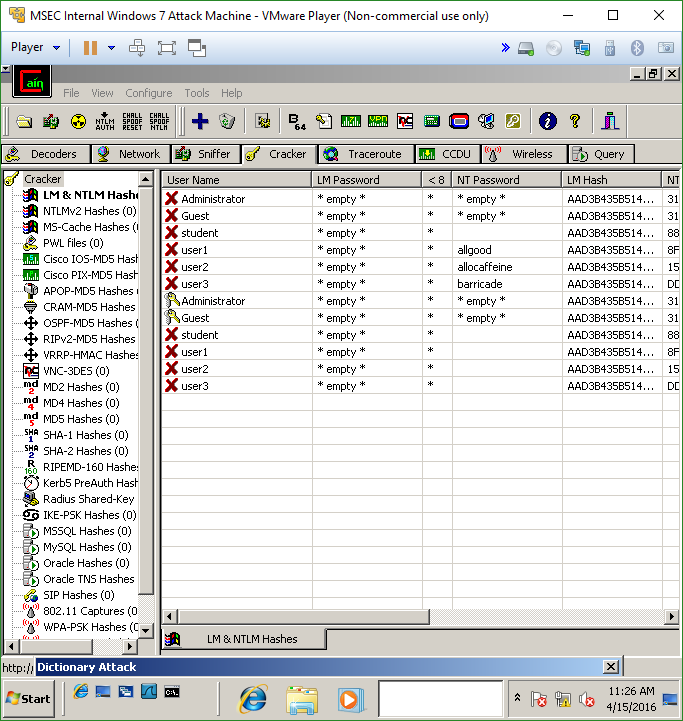
2.

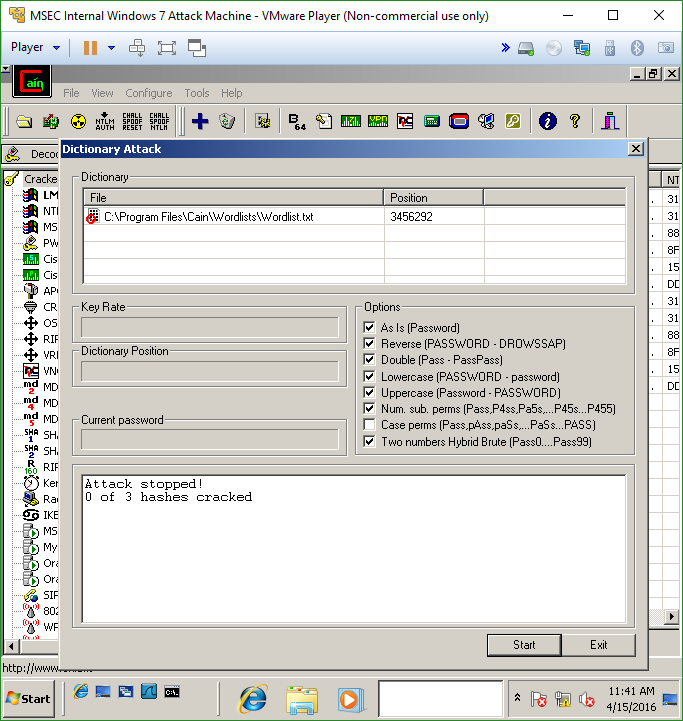
3.



Task 3

1. 

2.

3.

**Questions:**

Task 1

1. What is the command to add a group to the system in Linux? **groupadd**
2. What is the command to give a user a password in Linux? **passwd**
3. What is the command to add a user to the system in Linux? **useradd**
4. Where is the user’s encrypted password hash stored on a Linux system? **Wordlist.txt in the /etc/shadow directory**

Task 2

1. How can you learn more information about a particular exploit? **by typing the ‘info’ command while in msf**
2. What is the command to dump the password hashes in meterpreter? **hashdump**
3. What port needs to be open in order to use the DCOM RPC exploit? **135**
4. What directory is John the Ripper located in on BackTrack? **/pentest/passwords/john**

Task 3

1. What Windows operating systems exclusively use the NTLM hash? **Windows Vista and higher**
2. What Windows operating systems use the LM hash? **Prior to Windows Vista**
3. Where can someone obtain Cain? **www.oxid.it**
4. What is a disadvantage of using Cain? **It is classified as a virus by most AV vendors**

**Conclusion**

This lab took a bit longer than others, partially due to the length of time some of the attacks took for my machine to accomplish. However, this was an informative lab nonetheless and I haven’t seen Cain or John the Ripper in use until now. They both again took a while to finish, but it’s understandable after all the data they have to process to retrieve the passwords. Also, knowing the location of the files like the shadow file that stores user accounts info, and the SAM files that contain password hashes for users was also helpful to know. In conclusion, this lab helped me understand how brute force attacks like Cain and John the Ripper perform and where the information is contained.

**Grading Rubric**

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