Lab 10: Mitigation and Deterrent Techniques – Anti-Forensic

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 analyze Windows Event Logs. Students will change the Audit Policy of the system in order to log more information that is critical to keeping track of the security of the system. Students will also act as an attacker and clear the logs. Students will learn how to determine if the Windows Event Logs have been cleared by examining forensic evidence on the system.

**Materials**

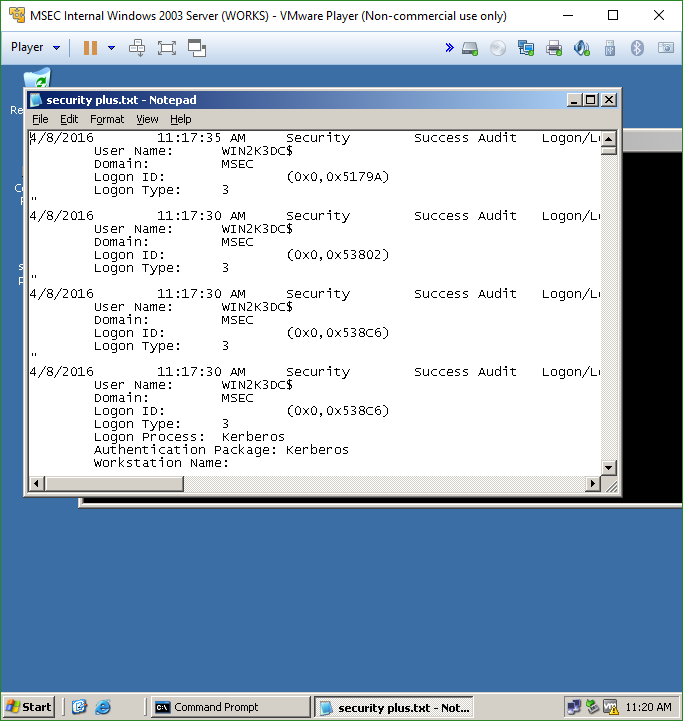
1. Backtrack 5
2. Windows 2003 Internal Victim Machine

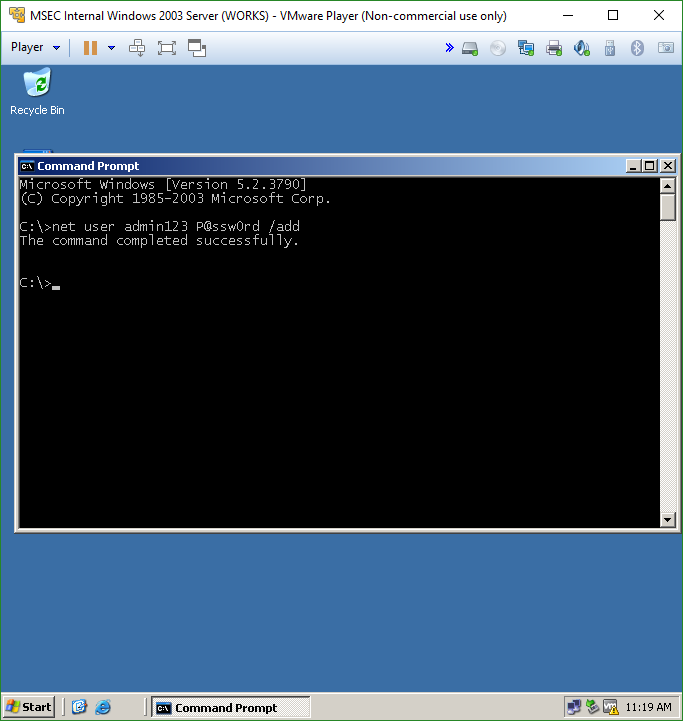
**Methodology**

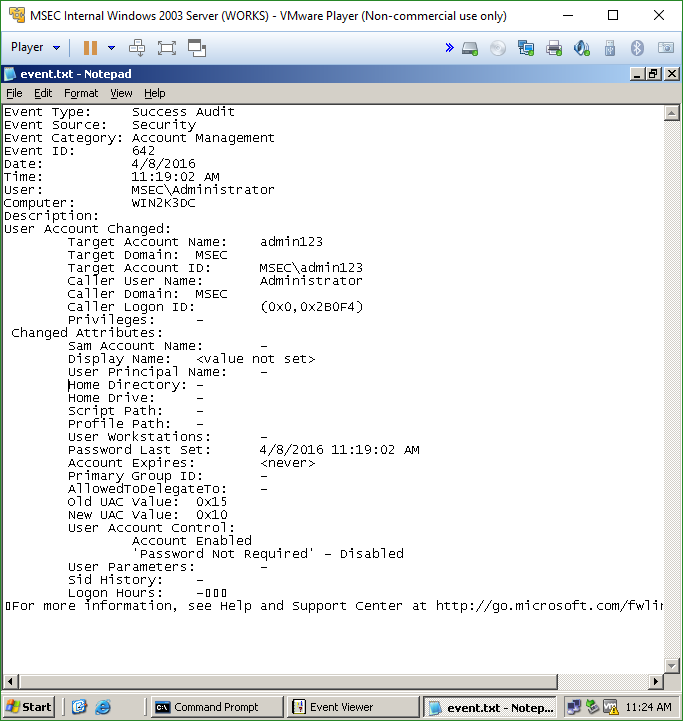
By using various commands such as clearev, gupdate, and several others to clear your logs from an attack and to update a server’s security information

**Lab**

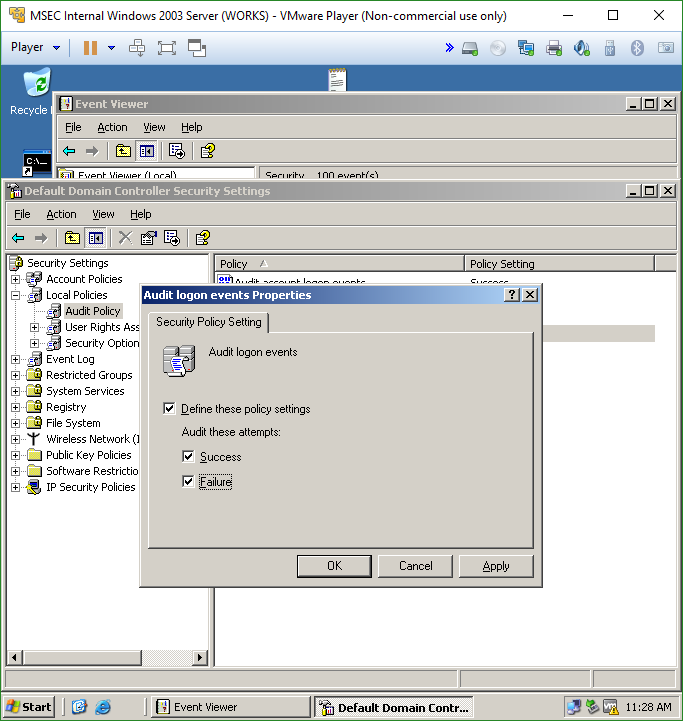
Task 1:

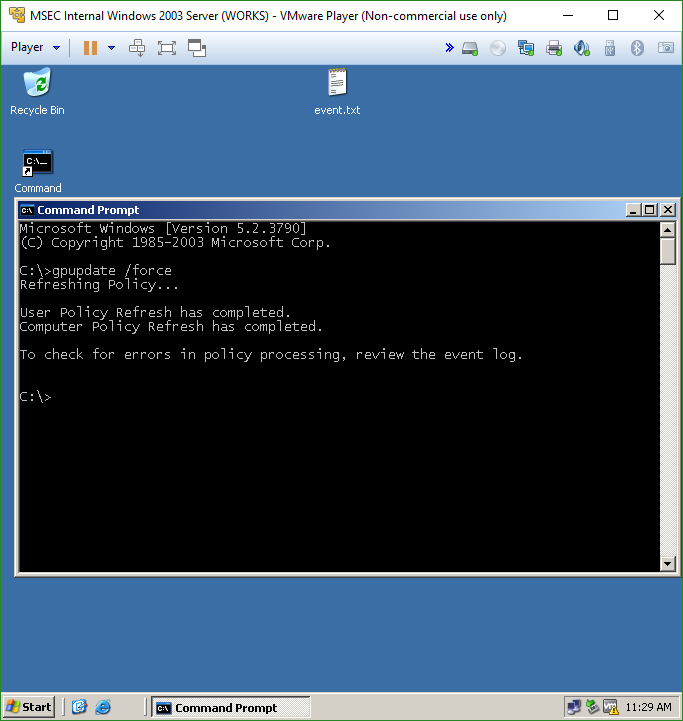
1. 

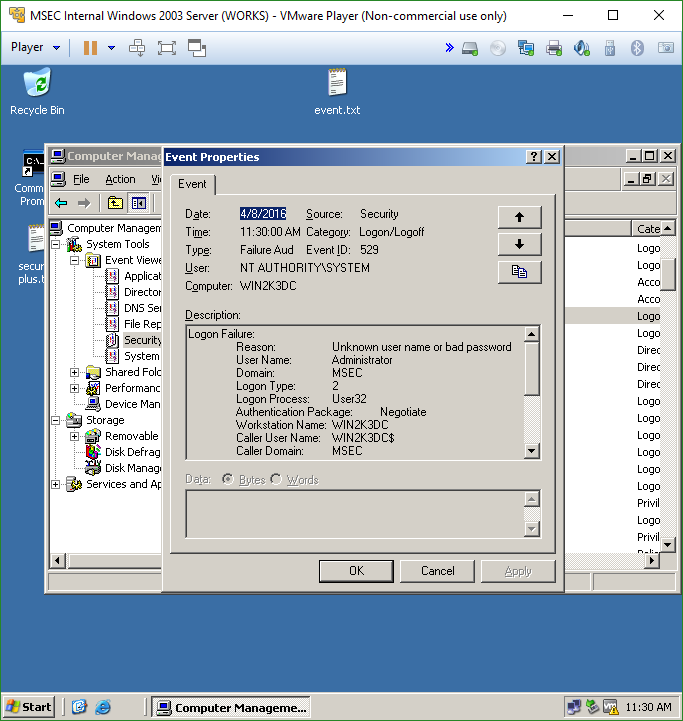
2, 

3. 

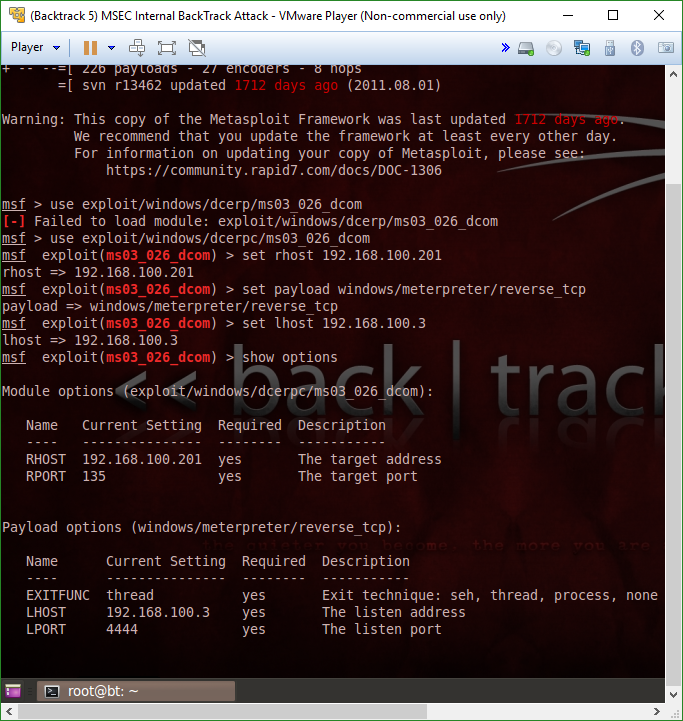
Task 2:

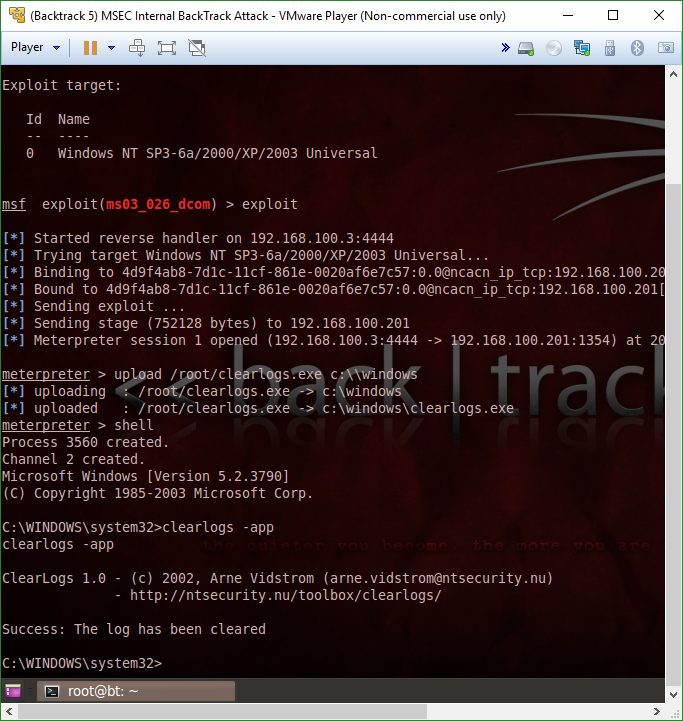
1. 

2.

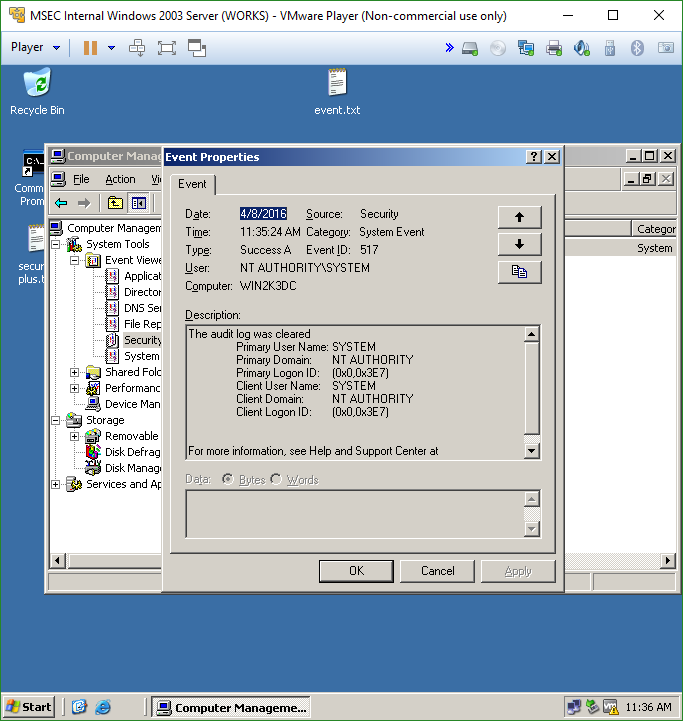
3.

Task 3

1. 

2.

3.



**Questions:**

Task 1

1. Name the three main Windows Event Logs. **Application log, security log, & system log**
2. Explain why saving Event Logs regularly is a good practice. **Just in case they are erased from hackers or an unwanted user**
3. Event Logs can be saved as which three different formats? **Evt, txt, and csv**
4. Adding a user account to the system will trigger an event in which log? **Account management**

Task 2

1. Which is more important, auditing for successes or failures? **Failures**
2. Where do you go in Windows to examine the audit policy? **Local computer policy>Computer Configuration>Windows Settings> Security Settings>Local Policies>Audit Policy**
3. What are two ways that you can get to the Event Viewer in Windows? **start, run, eventvwr.msc or start, administrative tools, event viewer**
4. What is the command line tool that can be used to update security settings? **gupdate /force**

Task 3

1. What happens when the security log is cleared? **No data is in the security log file**
2. What is the difference between the Clear Logs tool and the clearev command? **Clear Logs will let you clear one of the individual logs while the clearev command will clear the application, system, and security logs without any options**
3. Why might a hacker clear the logs? **To cover his tracks**
4. What would be an indicator that a hacker may have cleared one or more logs? **Under the security logs, if a file has a system event category and it says that the logs were cleared**

**Conclusion**

This lab was relatively straightforward compared to the last, with less to figure out in a way. Still very informative though, and knowing where the system logs are located is very helpful. Also knowing the event ID 517 should always be something to look out for incase of a hacker since it is known for the audit log being cleared. Also, remembering the gupdate command is important especially for security audits in case a hacker attempts to break in and fails with several attempts. All in all, the lab was helpful in knowing the basics for clearing log information and how to prevent it from happening from an audit’s perspective.

**Grading Rubric**

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