Erich Viebrock

ECPE 178

Lab #5: Sysinternals

What was the count of:

1. **Total events**

   106,185

2. **Filtered events**

   6

3. **Notepad.exe**

   967

4. **Cmd.exe**

   67

5. **Event class: File system**

   9,018

6. **Event class: Process**

   67

7. **Event class: Registry**

   22,533

8. **Result: Buffer Overflow**

   43

9. **Result: Name Not Found**

   1,792

10. What was the Total Kernel CPU time for Notepad

.0673485 seconds