Erich Viebrock

ECPE 178

Lab #5: Sysinternals

What was the count of:

1. **Total events**

106,185

1. **Filtered events**

6

1. **Notepad.exe**

967

1. **Cmd.exe**

67

1. **Event class: File system**

9,018

1. **Event class: Process**

67

1. **Event class: Registry**

22,533

1. **Result: Buffer Overflow**

43

1. **Result: Name Not Found**

1,792

1. **What was the Total Kernel CPU time for Notepad**

.0673485 seconds