

# Proactive Digital Forensics Using Splunk and Attack Graphs

Christopher I. G. Lanclos

Mississippi Valley State University

Research Alliance in Math and Science

Computational Sciences and Engineering, Oak Ridge National Laboratory

Mentor: Louis P. Wilder

[http://info.ornl.gov/sites/rams09/c\\_lanclos/](http://info.ornl.gov/sites/rams09/c_lanclos/)

## Background

### Digital forensic

- Process of extracting information and data
- Guarantee its accuracy and reliability

### Anti-forensics

- Process of deleting or removing information and data
- Make it nearly impossible to use data to prosecute hacker

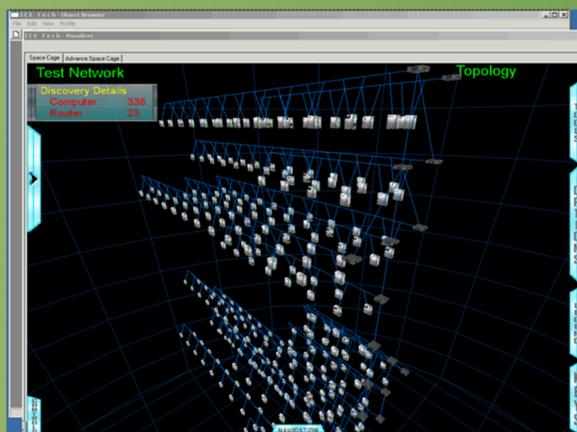


Fig.1: Example of a topology.

## Research Objectives

### Research

- Intrusion detection
- Digital forensics
- Anti-forensics
- Proactive digital forensics
- USB (Universal Serial Bus)
- Splunk
- Attack graphs

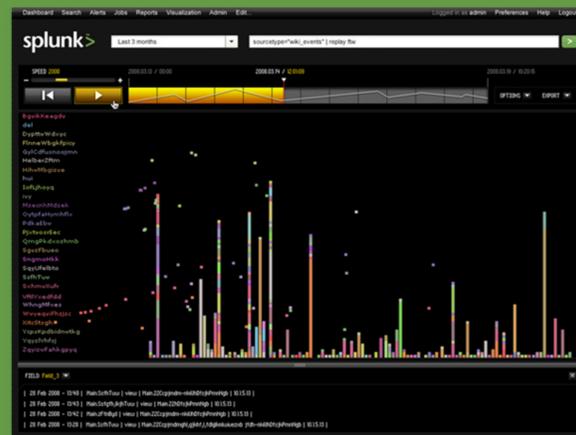
### Implement Splunk

Create an attack graph for an one node user in defense of an USB exploit

## Methods

### Implement Splunk

- Software application
- Search engine for information technology infrastructure
- Real-time capability
- Analysis
- Alert
- Report



<http://www.splunk.com/base/images/777f/Replay1.jpg>

### Create Attack Graph

- Representation of paths through a system
- Analysis of networks
- Based on a single computer or node

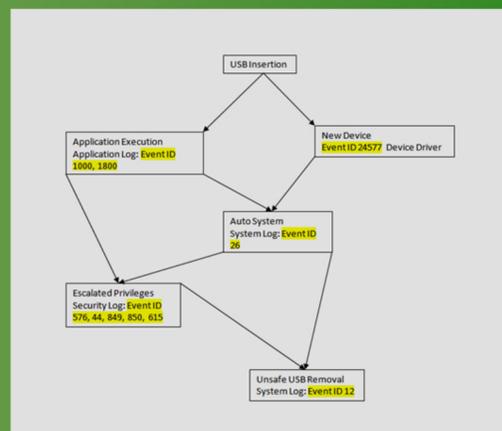


Fig.2. Attack graph based on event ID.

## Theoretical Use of Splunk

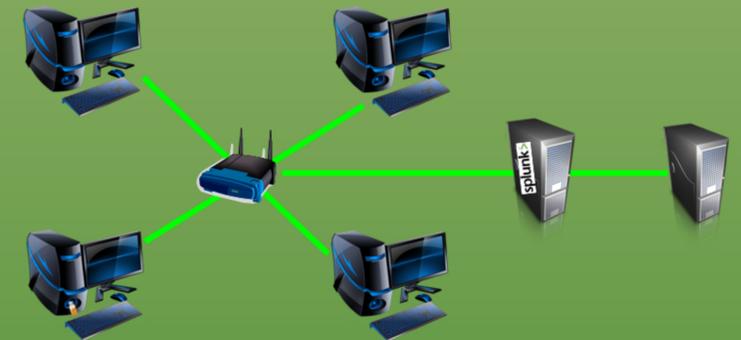


Fig.3: Theoretical Implementation on a network

## Conclusion

- Proactive forensics capable with Splunk and attack graphs
- Splunk and attack graphs have capability to gather information to seize and prosecute hackers

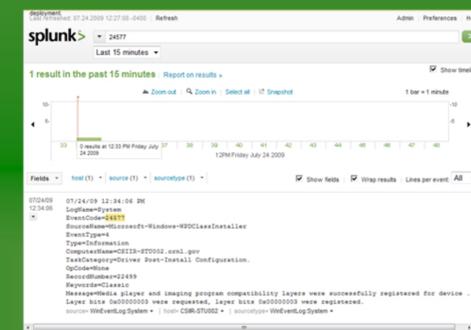


Fig.4: Event code 24577 found in Splunk.

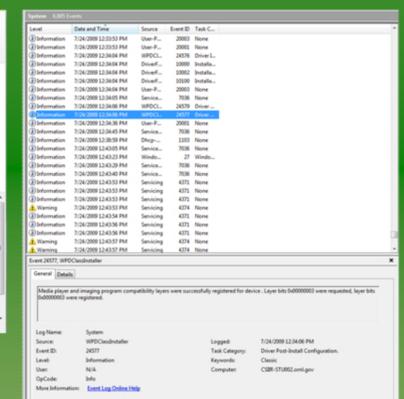


Fig.5: System log with event code

## Future Research

- Create attack graph algorithm to implement within Splunk
- Test design on USB exploits
- Expand Splunk and attack graphs to monitor other exploits