Visual Security Event Analysis
DefCon 13 Las Vegas

Raffael Marty, GCIA, CISSP
Senior Security Engineer @ ArcSight

July 29, 2005
Raffael Marty

► Enterprise Security Management (ESM) specialist
► OVAL Advisory Board
  (Open Vulnerability and Assessment Language)
► ArcSight Research & Development
► IBM Research
  • Thor - http://thor.cryptojail.net
  • Log analysis and event correlation research
  • Tivoli Risk Manager
Table Of Contents

► Introduction
► Related Work
► Basics
► Situational Awareness
► Forensic and Historical Analysis
► AfterGlow
Introduction
Disclaimer

“IP addresses and host names showing up in event graphs and descriptions were obfuscated/changed. The addresses are completely random and any resemblance with well-known addresses or host names are purely coincidental.”
Text or Visuals?

What would you rather look at?
Why Using Event Graphs?

► Visual representation of textual information (logs and events)
► Visual display of most important properties
► Reduce analysis and response times
  • Quickly visualize thousands of events
  • A picture tells more than a thousand log lines
► Situational awareness
  • Visualize status of business posture
► Facilitate communication
  • Use graphs to communicate with other teams
  • Graphs are easier to understand than textual events
When To Use Event Graphs

► Real-time monitoring
  • What is happening in a specific business area (e.g., compliance monitoring)
  • What is happening on a specific network
  • What are certain servers doing
  • Look at specific aspects of events

► Forensics and Investigations
  • Selecting arbitrary set of events for investigation
  • Understanding big picture
  • Analyzing relationships
Related Work
Related Work

► Classics

- Girardin Luc, “A visual Approach for Monitoring Logs”, 12th USENIX System Administration Conference

► Tools

How To Draw An Event Graph?

Device | ... | Normalization | ... | Parser

Event Analyzer / Visualizer

Log File

Event Graph

Jun 17 09:42:30 rmarty ifup: Determining IP information for eth0...
Jun 17 09:42:35 rmarty ifup: failed; no link present. Check cable?
Jun 17 09:42:35 rmarty network: Bringing up interface eth0: failed
Jun 17 09:42:38 rmarty sendmail: sendmail shutdown succeeded
Jun 17 09:42:38 rmarty sendmail: sendmail startup succeeded
Jun 17 09:42:39 rmarty sendmail: sendmail shutdown succeeded
Jun 17 09:42:39 rmarty sendmail: sendmail startup succeeded
Jun 17 09:43:10 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 09:43:42 rmarty last message repeated 2 times
Jun 17 09:45:47 rmarty vmnet-dhcpd: DHCPINFORM from 172.16.48.128
Jun 17 09:54:02 rmarty vmnet-dhcpd: DHCPDISCOVER from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 09:54:03 rmarty vmnet-dhcpd: DHCPOFFER on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8

Raffael Marty

Defcon 2005 Las Vegas
Different Node Configurations

Raw Event:
[**] [1:1923:2] RPC portmap UDP proxy attempt [**]
[Classification: Decode of an RPC Query] [Priority: 2]
06/04-15:56:28.219753 192.168.10.90:32859 ->
192.168.10.255:111
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:148 DF Len: 120

Different node configurations:

- SIP → Name → DIP
  - SIP: 192.168.10.90
  - RPC portmap: 192.168.10.255
  - DPort: 111

- SIP → SPort → DPort
  - SIP: 192.168.10.90
  - SPort: 32859
  - DPort: 111

- SIP → DIP → DPort
  - SIP: 192.168.10.90
  - DIP: 192.168.10.255
  - DPort: 111

- Name → SIP → DIP
  - Name: RPC portmap
  - SIP: 192.168.10.90
  - DIP: 192.168.10.255
AfterGlow – Peak Preview

► AfterGlow is not a SIM - there are no parsers (well, tcpdump and sendmail are there).

► Demo of the tool for use at home and in the Jacuzzi.

```plaintext
cat input.csv | ./afterglow.pl –c color.properties |
| neato –Tgif –o output.gif
```

color.properties:
```
color.source="red"
color.event="green"
color.target="blue"
```

Thanks to Christian @ ArcSight!
Situational Awareness
Real-time Monitoring With A Dashboard
Forensic and Historical Analysis
A 3D Example

► An LGL example:
Monitoring Web Servers

assetCategory(DestIP) = WebServer
Network Scan
Suspicious Activity?
Port Scan

► Port scan or something else?
Next Steps:
1. Visualize “FW Blocks” of outgoing traffic
   -> Why do internal machines trigger blocks?
2. Visualize “FW Blocks” of incoming traffic
   -> Who and what tries to enter my network?
3. Visualize “FW Passes” of outgoing traffic
   -> What is leaving the network?
Firewall Rule-set Analysis

pass

block

Rule #  Dest Port  Action
Load Balancer
Worms
DefCon 2004 Capture The Flag

DstPort < 1024
DstPort > 1024
Source Of Evil
Internal Target
Other Team’s Target
Internal Source
Internet Target

Exposed Services
Our Servers

SIP → DIP → DPort
DefCon 2004 Capture The Flag – TTL Games

TTL
Source Of Evil
Internal Target
Internal Source

192.168.4.1
192.168.4.2
192.168.4.3
192.168.4.152
192.168.4.153
192.168.4.154
192.168.4.157
192.168.4.159
50
30
35
62
63
64
128
126
52

SIP  ---->  DIP  ---->  TTL
DefCon 2004 Capture The Flag – The Solution

Show Node Counts

Only show SYNs
Email Cliques

From: My Domain
From: Other Domain
To: My Domain
To: Other Domain
Email Relays

Do you run an open relay?

Grey out emails to and from "my domain"

Make "my domain" invisible

To: My Domain
From: Other Domain
To: My Domain
From: Other Domain

Open relay?
Email SPAM?

Size > 10,000
Omit threshold = 1

Multiple recipients with same-size messages
Email SPAM?

nrcpt => 2
Omit threshold = 1

From nrcpt
BIG Emails

Size > 100,000
Omit Threshold = 2

Documents leaving the network?

From → To → Size
Email Server Problems?

- 2:00 < Delay < 10:00
- Delay > 10:00
- To

Diagram: Nodes and connections indicating email server status and delay.
AfterGlow
afterglow.sourceforge.net
AfterGlow

► http://afterglow.sourceforge.net

► Supported graphing tools:
  • GraphViz from AT&T (dot and neato)
  • LGL (Large Graph Layout) by Alex Adai
    http://bioinformatics.icmb.utexas.edu/lgl/
Some command line parameters:
- `h` : help
- `t` : two node mode
- `d` : print count on nodes
- `e` : edge length
- `n` : no node labels
- `o` threshold : omit threshold (fan-out for nodes to be displayed)
- `c` configfile : color configuration file
AfterGlow – color.properties

color.[source|event|target|edge]=
   <perl expression returning a color name>

- **Array @fields** contains input-line, split into tokens:

  color.event="red" if ($fields[1] =~ /^192\..*\)

- **Special color “invisible”:**

  color.target="invisible" if ($fields[0] eq "IIS Action")

- **Edge color**

  color.edge="blue"
color.source="olivedrab"
  if ($fields[0]=~/191\141\69\4/);

color.source="olivedrab"
  if ($fields[0]=~/211\254\110\4/);

color.source="orangered1"

color.event="slateblue4"

color.target="olivedrab"
  if ($fields[2]=~/191\141\69\4/);

color.target="olivedrab"
  if ($fields[2]=~/211\254\110\4/);

color.target="orangered1"

color.edge="firebrick"
  if ((($fields[0]=~/191\141\69\4/) or
   ($fields[2]=~/191\141\69\4/)))

color.edge="cyan4"
THANKS!
raffy@cryptojail.net