DarkNOC

Dashboard for Honeypot Management

Bertrand Sobesto(1), Michel Cukier(1), Matti Hiltunen(2), David Kormann(2), Gregory Vesonder(2), Robin Berthier(3)

(1) University of Maryland, (2) AT&T Labs-Research, (3) UIUC.
Outline

• Honeypots overview
• DarkNOC
• Case study

Do you really want to manage your own honeypots? Join us instead.
Honeypots

- Highly monitored systems meant to attract attackers and analyze their behavior.
- Traffic observed on the honeypot network is considered malicious.

- Different characteristics
  - Scale (local vs. distributed)
    - E.g., Leurre.com, Internet Motion Sensor, SGNET
  - Purpose (research vs. production)
  - Level of interaction (high vs. low)
    - Real OS + apps vs. emulated (e.g., Nepenthes, Dionaea, Honeyd)
The Problems

• Distributed Honeypots can generate large volume of data

• Running high interaction Honeypots is risky as they can get compromised

• Network infrastructure can suffer from attackers’ actions and needs to be monitored
DarkNOC

• DarkNOC (Darknet Network Operation Center) is a management and monitoring tool for complex honeynets
  – Support different types of honeypots (low and high interaction)
  – Support different data collection devices
  – Support both research and production

• Currently used to manage a honeypot network consisting of several subnets with hundreds of IP addresses.
System Architecture
## Data sources

### Netflow

<table>
<thead>
<tr>
<th>Date</th>
<th>Flow start</th>
<th>Duration</th>
<th>Port</th>
<th>SrcIP:Port -&gt; DstIP:Port</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-02-09</td>
<td>06:43:...</td>
<td>4294966.937</td>
<td>TCP</td>
<td>218.8.251.187:20347 -&gt; x.x.x.x:80</td>
<td>2</td>
<td>94</td>
<td>1</td>
</tr>
<tr>
<td>2010-02-09</td>
<td>06:43:...</td>
<td>4294966.977</td>
<td>TCP</td>
<td>218.8.251.187:20347 -&gt; x.x.x.x:80</td>
<td>2</td>
<td>94</td>
<td>1</td>
</tr>
</tbody>
</table>

### Snort IDS events

- 04/15-06:49:15.474819 [**] [1:12799:3] SHELLCODE base64 x86 NOOP [**]
  
  ![Classification: Executable Code was Detected](tcp) a.b.c.d:15017 -> W.X.Y.Z.:80

- 04/15-06:49:15.474819 [**] [1:12802:3] SHELLCODE base64 x86 NOOP [**]
  
  ![Classification: Executable Code was Detected](tcp) a.b.c.d:15017 -> W.X.Y.Z.:80

- 04/15-06:49:15.619028 [**] [1:12800:3] SHELLCODE base64 x86 NOOP [**]
  
  ![Classification: Executable Code was Detected](tcp) a.b.c.d:15017 -> W.X.Y.Z.:80

### Malware Collection

- [2011-04-15T06:49:19] a.b.c.d-> W.X.Y.Z. ftp://1:1@a.b.c.d:21/Rewetsr.exe c511c4f9bdd3bb892e582fbc9a00da9c
Software Architecture

• Constraints
  – Easy to use (any web browser), intuitive.
  – Speed: User interface fast despite the volume of data
  – Data validity: Data displayed up to date even under high data volume.

Backend
Process flow data and populate cache tables for the GUI

Graphical User Interface
Web interface to display the information

Alert Module
Execute user’s flow queries and send the result via email

DarkNOC
Graphical User Interface
Flows / subnet

Honeynet Traffic

- LAAS
- ENSA
- UMD External
- ATT
- UIUC
- UMD Internal
GUI: NetFlow Data

• RRD Graphs
  – Number of attackers
    • Number of unique external source IP addresses
  – Number of flows
  – Different scales: Day, week and month
  – Updated every 5 minutes by the backend program
GUI: More on NetFlow Data

- Top and bottom targeted ports
- Top attackers, top targets
- Top origin countries

<table>
<thead>
<tr>
<th>Top 10 Ports (last 24 hours)</th>
<th>Bottom 10 Ports (last 24 hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number</td>
<td>Protocol</td>
</tr>
<tr>
<td>9999</td>
<td>TCP</td>
</tr>
<tr>
<td>6884</td>
<td>TCP</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
</tr>
<tr>
<td>6889</td>
<td>UDP</td>
</tr>
<tr>
<td>8</td>
<td>ICMP</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
</tr>
<tr>
<td>8909</td>
<td>TCP</td>
</tr>
<tr>
<td>9415</td>
<td>TCP</td>
</tr>
</tbody>
</table>
GUI: Snort Events

- Number of Snort events
- Last 50 snort events (source and destination IPs hidden here).
GUI: More on Snort events

- Top 10 and bottom 10 snort signatures within the last 24 hours

<table>
<thead>
<tr>
<th>Top 10 Signatures</th>
<th>Number</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2P BitTorrent transfer</td>
<td>170708</td>
<td>31.96</td>
</tr>
<tr>
<td>NETBIOS SMB-DS repeated logon failure</td>
<td>132791</td>
<td>24.86</td>
</tr>
<tr>
<td>POLICY remote desktop protocol attempted administrator connection request</td>
<td>57418</td>
<td>10.75</td>
</tr>
<tr>
<td>NETBIOS DCRPC NCACN-IP-TCP srvsvc NtpPathCanonicalize overflow attempt</td>
<td>35809</td>
<td>6.7</td>
</tr>
<tr>
<td>POLICY VNC server response</td>
<td>23827</td>
<td>4.46</td>
</tr>
<tr>
<td>ATTACK-RESPONSES Microsoft cmd.exe banner</td>
<td>19671</td>
<td>3.68</td>
</tr>
<tr>
<td>SHELLCODE x86 inc ecx NOOP</td>
<td>10721</td>
<td>2.01</td>
</tr>
<tr>
<td>ATTACK-RESPONSES 403 Forbidden</td>
<td>9585</td>
<td>1.79</td>
</tr>
<tr>
<td>SHELLCODE x86 NOOP</td>
<td>9489</td>
<td>1.78</td>
</tr>
<tr>
<td>SCAN Proxyfire.net anonymous proxy scan</td>
<td>7031</td>
<td>1.32</td>
</tr>
</tbody>
</table>
Case study: UMD Honeynet

• An infrastructure to support honeypot-based experiments
  – Provide data collection infrastructure (Flow, Snort and PCAP)
  – Controlled environment

• Currently about 2,000 IP addresses from 5 different institutions:
  – University of Maryland
  – AT&T
  – University of Illinois at Urbana-Champaign
  – “Laboratoire d’Analyse et d’Architecture des Systèmes” (LAAS) in Toulouse, France
  – “Ecole Nationale des Sciences Appliquées” in Marrakech

• The UMD Honeynet is hosted at the University of Maryland, traffic from other institutions is forwarded through a secured tunnel (Honeymole).
UMD Honeynet Architecture
Case Study: Honeynet management

- Monitoring of the core components of the architecture (tunnels, honeypots)
- Identification of data collection failures
- Identification of network failures

UMD Internet network is not tunneled

Network issue?

Significant variations in the number of flows for the UMD Internal subnet

Network issue?

Tunnel issues
Case Study: Security tool

- Alert module
  - Alert on compromised campus hosts targeting the Honeynet

- Attack profiling
  - Origin countries and services targeted most

- Identify misconfigurations
  - Traffic that is not normally allowed
Alert module

• Report to U. Maryland security folks twice a day:

--------------- Analysis Report ---------------
Flow Time Window: 2011/06/06.06:00:00-2011/06/06.18:00:01
Number of hosts detected: 3
To access the online version of the report:

xxx.xxx.xxx.xxx (X.umd.edu)
- Number of flows: 1
- Number of packets: 1
- Number of bytes: 51
To visualize the flows:

yyy.yyy.yyy.yyy (Y.umd.edu)
- Number of flows: 10
- Number of packets: 10
- Number of bytes: 1915
To visualize the flows:

zzz.zzz.zzz.zzz (Z.umd.edu)
- Number of flows: 10
- Number of packets: 10
- Number of bytes: 1915
To visualize the flows:
Attack profiling

A typical day of traffic on the honeynet

Significant increase of traffic on the UMD internal subnet

No particular increase of the number of attackers

But port TCP/22 moves to the first place in the Top 10 ports...
You can join the adventure!

• Interested joining the UMD Honeynet? All you need is:
  – A Linux machine
    • An “old” box (Honeymole works great on a PII), can even be a VM
    • 2 network interfaces
    • Internet connectivity (Honeymole works with NAT)
  – Unused IP addresses (from 3 to... a lot)
  – We take care of the honeypot deployment at Maryland.

• What you will get:
  – Access to DarkNOC and our data repository (subject to partners’ approval)
  – Possibility to deploy your experiments using IP addresses of other institutions (within reason and subject to other institutions’ approval :-)

The authors would like to thank the Office of Information Technology at the University of Maryland for permitting this work.