Network Forensics: Notions and Challenges

Ahmad Almulhem

ISSPIT’09 – Ajman, UAE
Outline

1. Network Security
2. Network Forensics
3. Related Technologies
4. Challenges
5. Conclusion
Securing computer networks is challenging.
Mixture of Various technologies.
Lack of investigative features.
Firewall logs and IDS alerts are not suitable for investigation.
Network Forensics is proposed to support investigating incidents in computer network.

<table>
<thead>
<tr>
<th>Technologies Used</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus software</td>
<td>97%</td>
</tr>
<tr>
<td>Anti-spyware software</td>
<td>80%</td>
</tr>
<tr>
<td>Application-level firewalls</td>
<td>53%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>23%</td>
</tr>
<tr>
<td>Data loss prevention / content monitoring</td>
<td>38%</td>
</tr>
<tr>
<td>Encryption of data in transit</td>
<td>71%</td>
</tr>
<tr>
<td>Encryption of data at rest (in storage)</td>
<td>53%</td>
</tr>
<tr>
<td>Endpoint security client software / NAC</td>
<td>34%</td>
</tr>
<tr>
<td>Firewalls</td>
<td>94%</td>
</tr>
<tr>
<td>Forensics tools</td>
<td>41%</td>
</tr>
<tr>
<td>Intrusion detection systems</td>
<td>69%</td>
</tr>
<tr>
<td>Intrusion prevention systems</td>
<td>54%</td>
</tr>
<tr>
<td>Log management software</td>
<td>51%</td>
</tr>
<tr>
<td>Public Key Infrastructure systems</td>
<td>36%</td>
</tr>
<tr>
<td>Server-based access control lists</td>
<td>50%</td>
</tr>
<tr>
<td>Smart cards and other one-time tokens</td>
<td>36%</td>
</tr>
<tr>
<td>Specialized wireless security systems</td>
<td>27%</td>
</tr>
<tr>
<td>Static account / login passwords</td>
<td>46%</td>
</tr>
<tr>
<td>Virtualization-specific tools</td>
<td>29%</td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td>85%</td>
</tr>
<tr>
<td>Vulnerability / patch management tools</td>
<td>65%</td>
</tr>
<tr>
<td>Web / URL filtering</td>
<td>61%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

**Definition**

The use of scientifically proved techniques to collect and analyze network packets and events for investigative purposes.

- It is not a **product**. It is a complex **process**.
  - technology (tools), human intelligence, law
- It is not to **replace** firewalls, IDS, etc.
- It **employs** IDS alerts, firewalls logs, packets, etc.
Where does it fit in the forensics family?

- New member of the family of digital forensics.
- Digital forensics in a networked environment.
Current Practice

- Generally means collecting and analyzing logs and captured packets in a networked environment to investigate a hacking incident.
- ad-hoc manual.
- Experienced system admins
- art/science.
Digital Forensics Modeling

- **Readiness phases**: The goal of these phases is to ensure that the personal and infrastructure are able to fully support an investigation when an incident occurs.
- **Deployment phases**: The goal of these phases is to provide a mechanism for an incident to be detected and confirmed.
- **Physical Crime Scene Investigation phases**: The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident.
- **Digital Crime Scene Investigation phases**: The goal of these phases is to analyze digital devices that were obtained from the physical investigation phases.
- **Review phases**: The goal of these phases is to review the whole investigation and identify areas of improvement.
Related Technologies

**Intrusion Detection Systems**

- A system designed to detect computer and network attacks
  - 😊 A sensor to trigger the forensics process
  - 😊 A source of data (Alerts)
  - 😞 Detection Reliability
  - 😞 Data details may not be adequate

**Honeypots**

- A system built to lure and contain intruders
  - 😊 Study attackers and capture their tools (realtime)
  - 😞 Legal issues (damage claim, entrapment)
Computer Forensics

Forensics analysis of standalone computers

- 😊 Investigate the computers as if they were not networked
- 😞 Distributed data sources issues: data correlation, attack propagation.
- ☹️ Volatile data (network traffic)
Network Readiness

Main Tasks
- Data Collection
- Data Analysis
Challenges

- **Data Sources:**
  - Which data sources? All or a subset?
- **Data granularity**
  - How much details? (e.g. complete packets or headers?)
- **Data integrity**
  - Ensure data integrity (deliberately or accidentally)
- **Data as Legal Evidences**
  - Court admissibility
- **Privacy Issues**
  - Handling sensitive information (authorization)
- **Data Analysis**
  - Automation, tools, data mining, visualization (art)
Concluding Remarks

- Network forensics is a dedicated investigation infrastructure for networks.
- It extends the network security model (prevention/detection).
- It is not a product; it is a complex process
- Challenges in term of collecting and analyzing data

Further Readings

Questions?

http://www.ccse.kfupm.edu.sa/~ahmadsms/