Dr. Sorot Panichprecha, Managing Director Epiphany Consulting
CISSP, GSEC, GCIH, GPEN, GCIA, GWAPT, GCFE, GCFA, GREM

Website Security Incident Handling

What to do when you get hacked?

Outline

- Incident Handling Process Overview
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident
- Conclusion

Event vs Incident

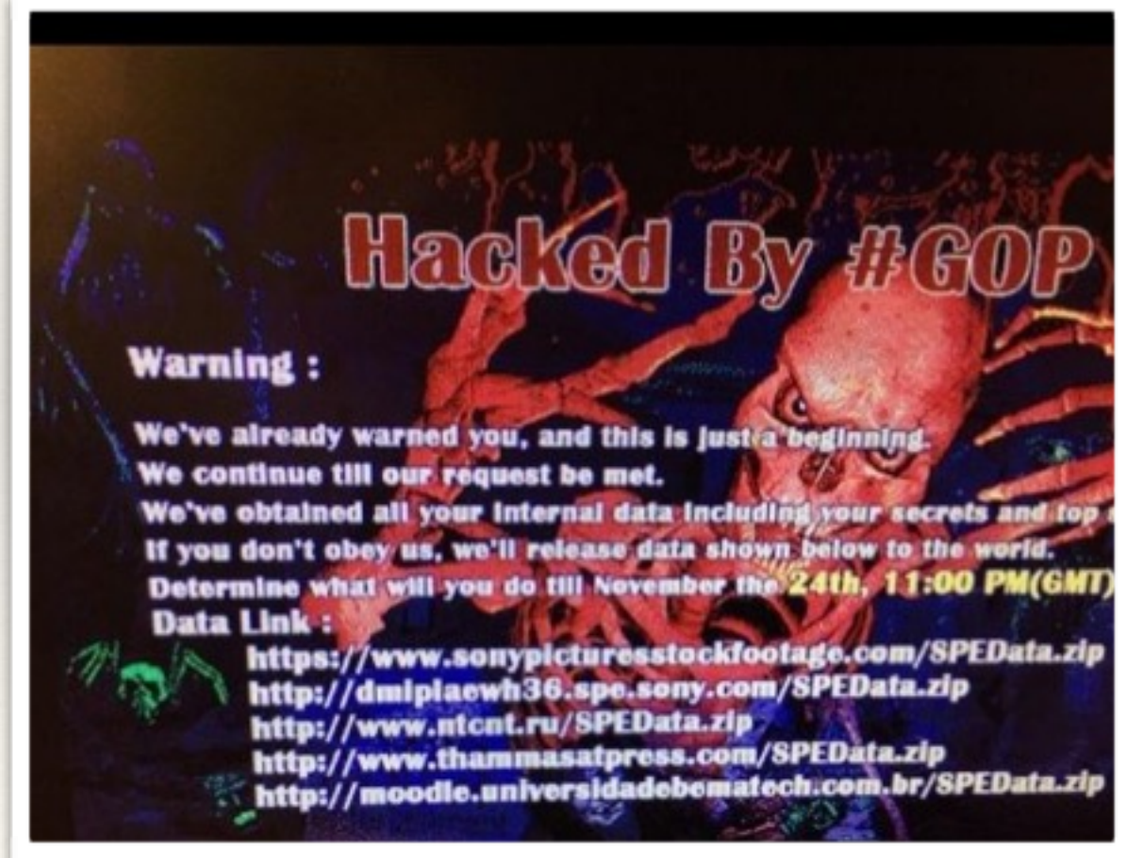
- Event is any observable activity in a system or network.
- Incident is an event that causes harm or has an intent to harm.
  - Depending on the situation and the context.

Event or Incident?

- A user open the organisation web site.
- A user copies files from an intranet file server at 2 AM.
- Someone runs a port scanning on the public web server.
- Someone runs a port scanning on the intranet server.
- A system administrator posts a question about the system configuration on a web board.

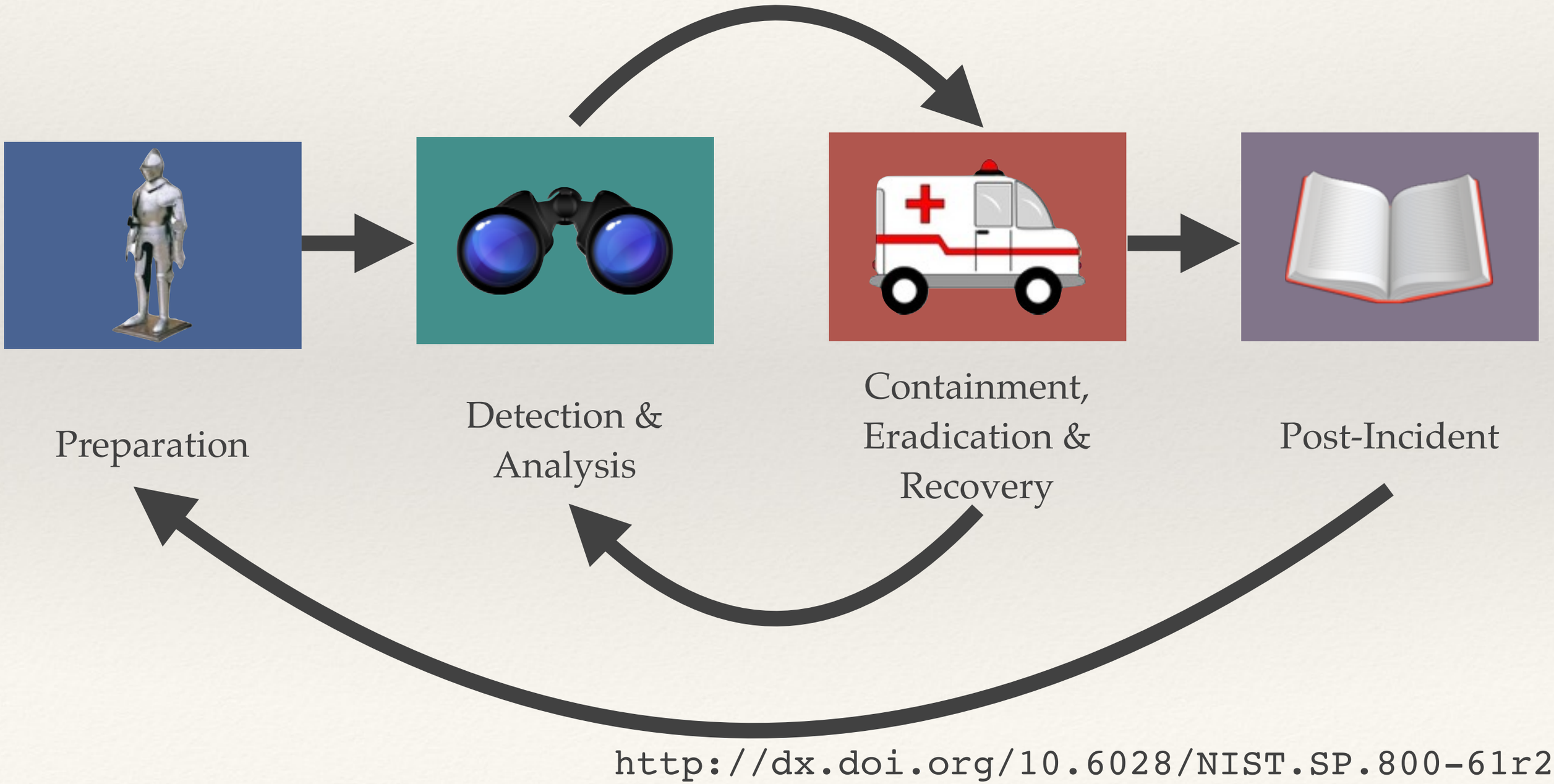
Not “what if” it is “when”

- It is not the matter of “what if” but it is the matter of “when”.
  - Eventually everyone will be hacked!
- Keep that in mind, and start preparing for the worse.



http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

Incident Handling Process



http://dx.doi.org/10.6028/NIST.SP.800-61r2

Outline

- Incident Handling Process Overview
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident
- Conclusion

Preparation

- Contact information
- Incident reporting mechanisms
- Issue tracking system
- Encryption software
- War room
- Secure storage facility

Tools

- Digital forensic workstations and software
- Backup devices
- Laptops
- Spare workstations, servers, networking equipment
- Blank removable media
- Packet sniffers and protocol analysers
- Evidence acquisition accessories

Training

- Incident handler should receive adequate trainings.
- Basic information security.
- Security incident handling.
- Intrusion detection analysis.
- Digital forensic analysis.
- Reverse-engineering malware.

`http://www.sans.org/security-training/roadmap.pdf`

Preventing Incidents

- Risk assessments
- Host and network security
- Malware prevention
- User awareness and training

Outline

- Incident Handling Process Overview
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident
- Conclusion

Attack Vectors

- External/Removable Media: an attack executed from a USB disk.
- Attrition: DoS attack.
- Web: cross-site-scripting attack stealing credentials.
- Email: malware attachment.
- Impersonation: spoofing, man-in-the-middle.
- Improper Usage: user install unauthorised software.

Sign of an Incident

- Automatic detection: IDS/IPS alerts, SIEM alerts.
- Manual detection: problems report by users.
- Precursor: a sign before an actual attack.
- Indicator: alerts.

Analysis (1)

- An intrusion analysis and validation can be a challenging task.
- To make the task easier, you should prepare the following information:
  - Network and system profile: expected activities.
  - Understand normal behaviours.
  - Create a log retention policy: how long the log should be stored.
  - Event correlation: firewall log + application log.

Analysis (2)

- Clock synchronisation: make sure your NTP is working properly.
- Run packet sniffers to collect additional data.
- Filter the data.
- Seek assistance from others.

Documentation

- Issue tracking system should record the following information:
  - Current status of the incident: new, in progress, forwarded for investigation, resolved.
  - Summary of the incident.
  - Indicators related to the incident.
  - Other incident related to this incident.
  - Actions taken by all incident handlers on this incident.
  - Chain of custody.
  - Impact assessments.
  - Contact information.
  - List of gathered evidence.
  - Comments from incident handlers.
  - Next steps.

Prioritisation

- Functional impact of the incident: how the incident impacts the functionality of the affected system.
- Information impact of the incident: may also impact not only the organisation's confidential information, but also other organisation.
- Recoverability from the incident: size and type of resources.

Incident Notification

- Once the incident has been analysed and prioritised, the team needs to notify related people.
- Incident response policy should define whom and when to inform in which case.
  - People who should be informed: CIO, head of information security, system owner, HR (internal case), CERT.

Outline

- Incident Handling Process Overview
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident
- Conclusion

Containment Strategy

- Common strategy: disconnect from the network, shutdown, reinstall, and put the machine back on.
  - This strategy may not always work.
- Criteria for determining an appropriate strategy:
  - Potential damage to resources
  - Need for evidence preservation
  - Service availability
  - Time and resources required to implement the strategy
  - Effectiveness of the strategy
  - Duration of the solution

Evidence Gathering

- Use the digital forensic methodology to acquire the evidence.
- Collect volatile data (RAM) first.
- Collect hard disk, USB disk, CD/DVD.

Identifying the Attacking Hosts

- Validating the attacking hosts's IP address.
- Researching the attacking host through search engines.
- Use incident databases.
- Monitor possibly attacker communication channel.

Eradication and Recovery

- Eradication: deleting the malware, disable the infected accounts, fix the vulnerabilities.
- Recovery: restore systems to normal operation.
  - Beware that if the vulnerability still exists, attackers will attack again.

Outline

- Incident Handling Process Overview
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident
- Conclusion

Lesson Learned

- What happened? When? How?
- How well did everyone perform?
- What information should have been available sooner?
- What can be done differently?
- What corrective actions should be implemented to prevent similar incidents in the future?
- What precursors and indicators should have been monitored?
- What additional tools are needed?

Evidence Retention

- How long should we keep the evidence?
  - Prosecution: may take several years.
- Data retention: 3 - 6 months

Outline

- Incident Handling Process Overview
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident
- Conclusion

Conclusion

- You will be hacked! So be prepared.
- Incident handling process
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery
  - Post-incident

Website Security Standard (ขมธอ.1-2557)

1. ปิดการเชื่อมต่อของเว็บไซต์
2. สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์
3. ตรวจสอบช่องทางการโจมตีและช่องโหว่ของเว็บไซต์ด้วยข้อมูลที่สำเนามา
4. ระหว่างการตรวจสอบจัดสร้างเว็บเพจแบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อชี้แจงสถานการณ์การปิดปรับปรุง
5. กู้คืนโปรแกรมที่เกี่ยวข้อง ข้อมูลเว็บ และฐานข้อมูลที่เกี่ยวข้องกับเว็บไซต์เป็นเวอร์ชั่นก่อนหน้าที่จะถูกโจมตี
6. ตรวจสอบช่องโหว่ของเว็บไซต์ แก้ไขช่องโหว่ของเว็บไซต์
7. บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด

Thank You

Dr. Sorot Panichprecha

sorot@epiphany-consulting.net

@sorotpan

EPIPHANY
CONSULTING