CE0973a - Issues in Network Security
5: Incident Detection & Response

James A Sutherland

Abertay University

Monday, 8th February 2016

Detecting Attacks

- Abnormal traffic (TV sending email)
- Excessive traffic (UoD P2P)
- External reports (spam, probes)
- User reports (files missing or accessed)
- Special purpose IDS rules (see SNORT later)

Detecting Attacks

- Abnormal traffic (TV sending email)
- Excessive traffic (UoD P2P)
- External reports (spam, probes)
- User reports (files missing or accessed)
- Special purpose IDS rules (see SNORT later)

Detecting Attacks

- Abnormal traffic (TV sending email)
- Excessive traffic (UoD P2P)
- External reports (spam, probes)
- User reports (files missing or accessed)
- Special purpose IDS rules (see SNORT later)

Detecting Attacks

- Abnormal traffic (TV sending email)
- Excessive traffic (UoD P2P)
- External reports (spam, probes)
- User reports (files missing or accessed)
- Special purpose IDS rules (see SNORT later)

Detecting Attacks

- Abnormal traffic (TV sending email)
- Excessive traffic (UoD P2P)
- External reports (spam, probes)
- User reports (files missing or accessed)
- Special purpose IDS rules (see SNORT later)

Intruder Detection

Typically network monitoring; similar to anti-virus scanner, matching signatures and heuristic rules to detect ‘hostile’ activity and alert the administrators.

- Port scans
- Bad login attempts
- Sensitive data exfiltration: CC#

Intruder Detection

Typically network monitoring; similar to anti-virus scanner, matching signatures and heuristic rules to detect ‘hostile’ activity and alert the administrators.

- Port scans
- Bad login attempts
- Sensitive data exfiltration: CC#

Intruder Detection

Typically network monitoring; similar to anti-virus scanner, matching signatures and heuristic rules to detect ‘hostile’ activity and alert the administrators.

- Port scans
- Bad login attempts
- Sensitive data exfiltration: CC#

IDS Example

Snort – `http://www.snort.org/` – free, open-source network IDS.
Created 1998, owned by Cisco since 2013.
Key functions: packet logger, protocol analyser, content matching.

Conflict: Protect v Investigate

- Cleanup, restore service
- Preserve information from system
- Gather information about attacker

Conflict: Protect v Investigate

- Cleanup, restore service
- Preserve information from system
- Gather information about attacker

Conflict: Protect v Investigate

- Cleanup, restore service
- Preserve information from system
- Gather information about attacker

Restoring Service Quickly

Roll back to known-good state, patch vulnerability

- How do you know it's really good?
- Advanced Persistent Threats lurk...
- How can you be sure it's patched?
- What about the data since that backup?

Forensics

Having been compromised, you want to investigate:

- Who got in?
- How did they do it?
- What did they do?
- Why did they do it?

Forensics

Having been compromised, you want to investigate:

- Who got in?
- How did they do it?
- What did they do?
- Why did they do it?

Forensics

Having been compromised, you want to investigate:

- Who got in?
- How did they do it?
- What did they do?
- Why did they do it?

Forensics

Having been compromised, you want to investigate:

- Who got in?
- How did they do it?
- What did they do?
- Why did they do it?

Intelligence Gathering

Sometimes keep a system in place knowing it's compromised:

- Honeypot/honeynet[1]
- Spamtrap
- FBI and 'PlayPen' child abuse site[2]

[1] https://www.honeynet.org/

[2] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/12116278/FBI-took-over-worlds-biggest-child-porn-website.html

Intelligence Gathering

Sometimes keep a system in place knowing it's compromised:

- Honeypot/honeynet[1]
- Spamtrap
- FBI and 'PlayPen' child abuse site[2]

[1] https://www.honeynet.org/

[2] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/12116278/FBI-took-over-worlds-biggest-child-porn-website.html

Intelligence Gathering

Sometimes keep a system in place knowing it's compromised:

- Honeypot/honeynet[1]
- Spamtrap
- FBI and 'PlayPen' child abuse site[2]

[1] https://www.honeynet.org/

[2] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/12116278/FBI-took-over-worlds-biggest-child-porn-website.html

Simple Automatic Defences: Fail2Ban

Monitor system logs for brute-force logins, block offending IP.
No panacea:

- User inconvenience
- DoS vulnerability
- Easy to avoid via Tor, IP changing

Brute Force Investigation

Controversial[3] University of California system, capturing *all network traffic from all users* for a rolling 30 day window.
Justification: retrospective investigation of APT (Advanced Persistent Threats).
Problem: includes millions of hospital patients and their data...

[3] https://www.insidehighered.com/news/2016/02/01/u-california-faculty-members-object-new-email-monitoring

Lab Work

Look at your network design from week 4. How would you handle a compromise on each part, and why?

Examine each component. What could compromising, say, a router or printer achieve?