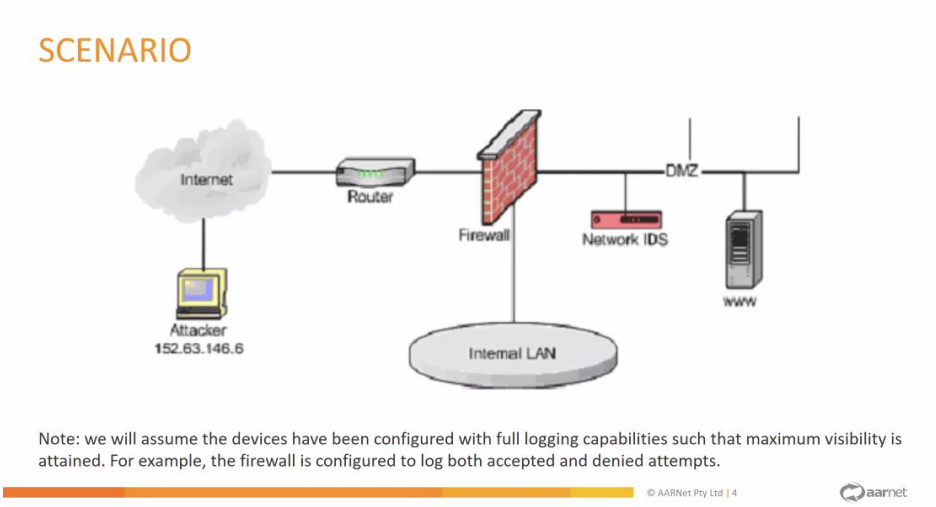
COMP 6448 - Week 4

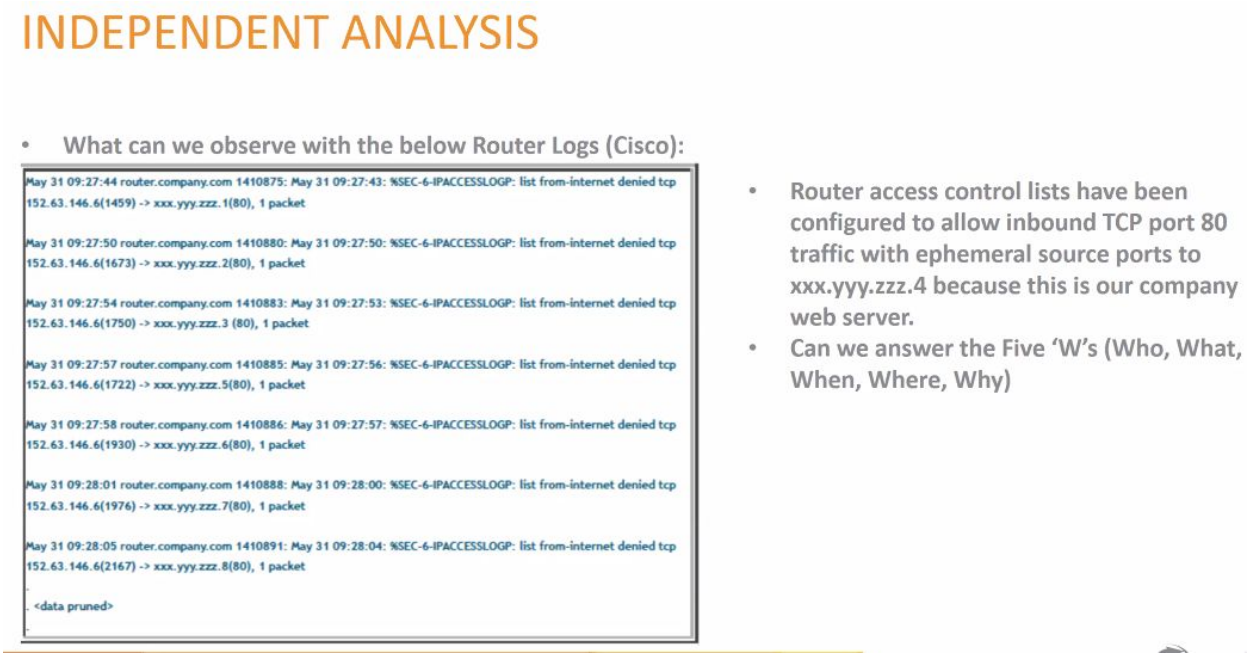
Security Engineering Masterclass

SIEM:

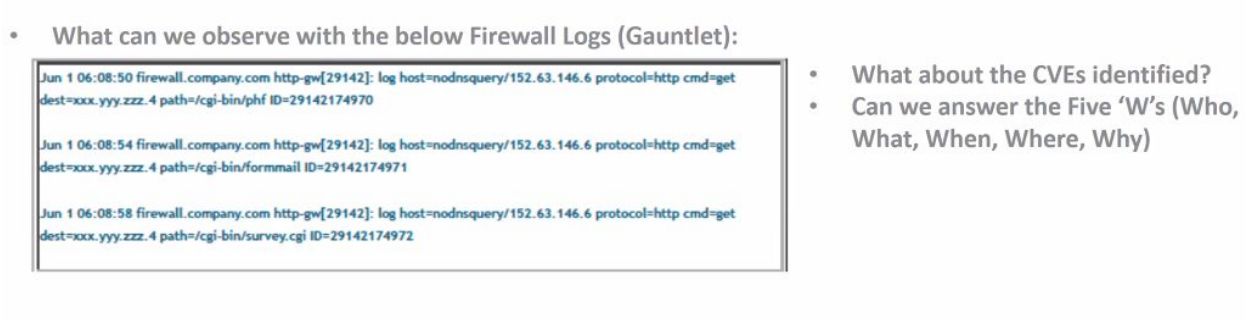
In SIEM systems, we receive thousands of logs, so knowing how to read and interpret information from logs is essential. See in the below image, it shows that possible logs can come from all sorts of places, such as the router, firewall etc.



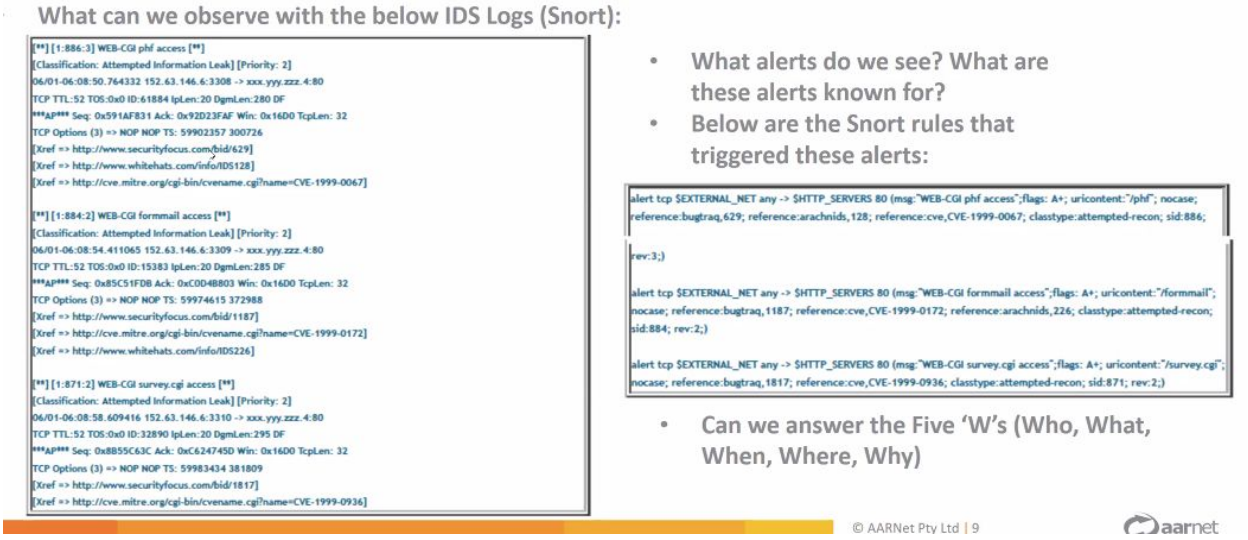
Consider this log from the router, what is it saying?



- Who: 152.63.146.6. But no user attached to IP.
- What: Broad scanning of xxx.yyy.zzz.0/24
- When: May 31 <time>
- Where: DMZ company
- Why: brute forcing ip addr



- Who: 152.63.146.6
- What: Attempt to access the faulty scripts.
- Where: DMZ company trying to gain access still.
- Why: Research shows that phf, formmail and survey.cgi are all exploitable scripts. Attempts malicious activity because if accessed, these scripts would allow remote execution. The access in isolation is a poor move on the red team because it flags it as malicious activity.



- Who: 152.63.146.6
- What: Attempt to leak info about the vulnerable scripts.
- Where: DMZ company trying to gain access still.
- Why: Attempting to leak information from the scripts to exploit them.

Note: Parsing the logs (which are in different format) is required in order to stitch together this information.

Limitations of single device analysis:

- False positives,
- Incomplete info
- Missing the 'why'
- Miss lateral movement or other activities (e.g. exfiltation)

Summary:

- Analysing single devices is the computerised version of tunnel vision.
- Security events should be analysed from as many sources as possible.

- Security Awareness of an environment can be attained by listening to what its devices are saying.