Best Practice for Logging at Internet-facing Servers

Dave O’Reilly, Chief Technologist, FTR Solutions

IETF-101
19th March 2018
RFC6302 (BCP162) - Logging Recommendations for Internet Facing Servers

• As well as logging incoming IP addresses also log:
  – Source port number
  – Timestamp in UTC, accurate to the second, from a traceable time source (e.g. NTP)
  – The transport protocol (e.g. TCP/UDP) and destination port number.
However research has revealed...

• Server software might not support logging source port
• Server software might require enabling of verbose logging to log source port
• Practically no server software enables (or even provides a sample configuration) logging source port by default
• Logging against a fixed time reference (e.g. NTP) is not necessary as long as time is recorded consistently
• Changing log formats could break existing tooling
In Summary...

• Absence of source port information in logs is a big crime attribution/public safety problem (ref. Europol)
• Logging source port doesn’t solve the problem of crime attribution but addresses a significant current challenge.
• Current BCP needs revision to address more of the practical issues with logging source port.
Therefore:

“Approaches to Address the Availability of Information in Criminal Investigations Involving Large-Scape IP Address Sharing Technologies.”

Thank You! Any Questions?

Dave O’Reilly
Chief Technologist
FTR Solutions

+353 (87) 231 3257
dave.oreilly@ftrsolutions.com