Title	Log Files and Event Analysis
Long Title	Log Files and Event Analysis
Credits	5
NFQ Level	Advanced
Module Author	Dr.George. D O'Mahony

Module Description:

Log files contain valuable information for infrastructure management as most malicious exploits and intrusions leave their fingerprints all over log files and system performance issues can be identified from analyzing specific log data. In this module, the learner will evaluate log files and learn tools to extract associated valuable data for detecting cyber threats and system performance issues. In particular, the module will provide the learner with skills to apply and use log file management tools, access log files, efficiently search log data using best practices. The learner will apply this knowledge to evaluate and implement YARA and Sigma rules for Indicators of Compromise (IoCs) and system information and event management tools. At the end of the module the learner should have developed a mindset for using log files for cyber security and incident investigation including system performance issues. This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Evaluate log files, the associated data and accessing and search mechanism

LO2 Interpret valuable data from log files for cybersecurity and system performance purposes by applying best practices and tools.

LO3 Implement a log management system using security information and event management (SIEM) tools for use in infrastructure management.

LO4 Analyse log files from multiple devices and applications utilising log aggregation techniques and SIEM tools to identify indicators of compromise in ill-defined contexts.

LO5 Apply a log file analysis mindset for cyber security and system performance to the effective communication of incident reports.

Indicative Content

Log Files

What are log files and what data do they contain? Types of log files. What type of information regarding the wellbeing and efficiency of the system do they contain? Log data transmission and collection. What collects log data (OS, applications, etc.) Extracting diagnostic data and capabilities from log data. Linux Log files and diagnostic data (grep), Application log files, Windows log files (event viewer), MAC log files (Console), Android log files (Android Studio), firewall logs (e.g. Windows Defender Firewall with Advanced Security). Reading log files using text editors and advanced read log software. Log formats. Log Security (access, data recording, configuration, etc.)

Log File Access and Analysis

Log file analysis – why is it important? Log file analysis use cases. Log file analysis best practices and tools- prioritization, filtering, criticality determination, the need for context and unclear messages. How do log files specify changes that have occurred. How are incident causes extracted from log files? How log data points out red flags in systems: unusual behaviour, unauthorized access, extreme traffic, suspicious changes, etc. How to extract useful information and how to search log data by implementing regex and grep tools.

Log Management Systems

What is a log management system and how does it fit into the overall security architecture (Defense in Depth). Parameters of a complete log management system: Collection, Storage, Search, Correlation and Output. Why is log management important? Why does it make log file analysis more feasible?

SIEM

What are system information and event management (SIEM) tools? How SIEM software operates to collect log and event data generated by different applications, security devices and host systems and collates it together into a single centralized platform. How SIEMs are used with YARA and Sigma rules to identify indicators of compromise to manage security for a large or diverse IT infrastructure. SIEM real-time threat analysis that provides real-time visibility across an organization's information security systems.

Investigating an Incident – Developing the correct Mindset

Analyzing how log management and analysis plays a crucial role during a security incident and identifying system performance issues. Determine normal behaviour (daily basis, by the hour, monthly, longer) and triggers. How Log files (and associated data) are leveraged for fighting cybercrime. Identify the logs where malicious exploits and intrusions have left their fingerprints. How to develop a log file analysis mindset for cybersecurity and system performance.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	In this project, the student will be asked to access, evaluate and discuss log files and extract the associated valuable data for identifying indicators of compromise. The learner may be required to utilize tools introduced in the laboratories.	1,2,5	40.0	Week 6
Project	This project will require students to implement a log management system and appropriate YARA and Sigma rules for use in a SIEM. The learner may be required to utilize tools introduced in the laboratories.	3,4,5	60.0	Sem End

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning learning outcomes	2.0	Every Week	2.00
Lab	Lab supporting content delivered in class	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning learning outcomes	2.0	Every Week	2.00
Lab	Lab supporting content delivered in class	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Recommended Book Resources

- **Anton Chuvakin, Kevin Schmidt, and Chris Phillips 2012, *Logging and Log Management : The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management* [ISBN: 9781597496360]**