



An Investigation of Network Security Techniques to Detect Reconnaissance Activity

Simon Rees (0151968)

MSc Cybersecurity and Digital Forensics

Research Methods and Professional
Development (ACFA7004)

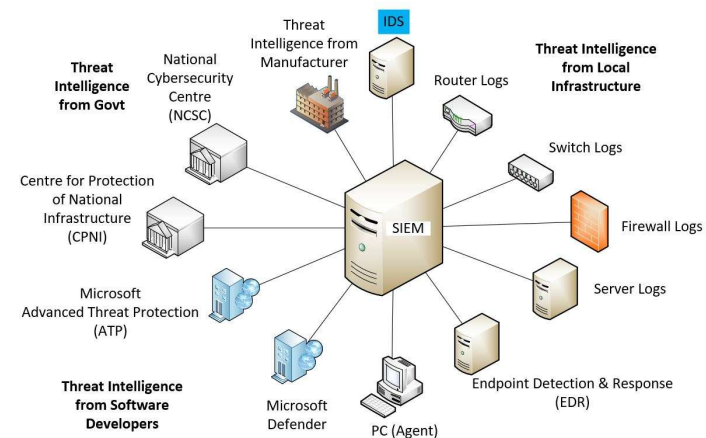
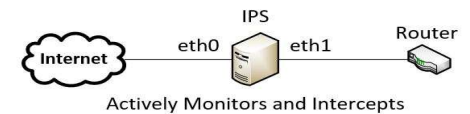
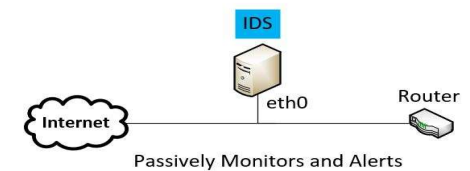
Research Context

Cyber-attack detection tools:

Device	Acronym	Task	End Result
Intrusion Detection System	IDS	Monitor traffic and detects suspicious network activity	Passively sends alert
Intrusion Prevention System	IPS		Actively blocks connection.

Device	Acronym	Description
Network	NIDS	Stand alone server OR built into a Next Generation Firewall.
	NIPS	
Host	HIDS	An agent is installed onto a PC and reports any suspicious activity back to a central server
	HIPS	
Security Information Event Management	SIEM	Central server that collects cybersecurity data from a range of sources including: - IDS/IPS - Firewalls - Logs Server and Network - Threat Intelligence Correlates the data to identify potential threats.

IDS & IPS Implementation



SIEM Deployment

Research Problem

- Cyber-attack frameworks use reconnaissance techniques as their first step [5]
- Hackers conduct reconnaissance to gain information about their target [6]
- The detection of the reconnaissance phase of an attack is an important aspect in network defence
- Consequence of NOT detecting reconnaissance activity

MITRE	Lockheed Martin
ATT&CK	Cyber Kill Chain
Recon	Reconnaissance
Weaponize	Weaponization
Deliver	Delivery
Exploit	Exploitation
	Installation
Control	Command and Control
Execute	Actions on Objectives
Maintain	

Research Aim and Objectives

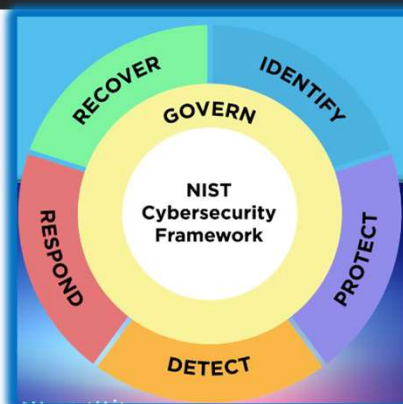
- **Aim:** To develop a system to monitor and detect reconnaissance activity on a network, providing alerting and reporting.
- **Objectives:**
 - 1: To design and build a Virtual Environment (VE) as a testbed based on an enterprise University campus network. Two existing Network Intrusion Detection Systems (NIDS), namely Snort and Suricata will be used.
 - 2: To devise a test plan utilising tools/techniques employed by hackers in order to evaluate detection of reconnaissance activity.
 - 3: To analyse the reconnaissance detection results and conduct a comparison of NIDS effectiveness.

Brief Literature Review

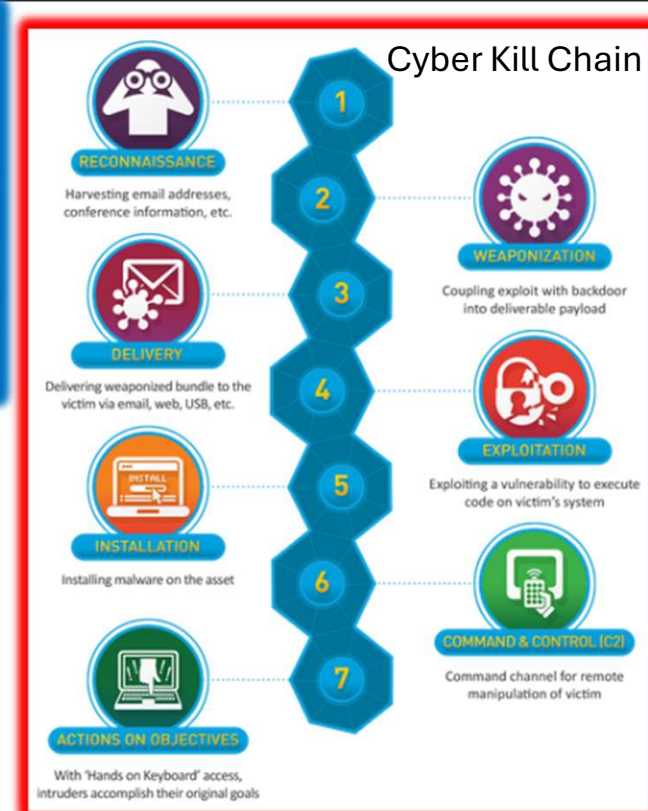
#	Title	Year	Topic / Area of Study	Relevance to my research	Research gaps
1	Detect and Mitigate Cyberattacks Using SIEM [1]	2023	Using Network Intrusion Detections System (NIDS) detect Denial of Service (DoS) and File Integrity Monitoring (FIM).	This paper outlines how to utilise and NIDS and SIEM devices to detect reconnaissance activity.	Does not investigate how to detect reconnaissance techniques.
2	A Comparative Analysis of Snort and Suricata [8]	2024	Reviews the performance of two different NIDS: Snort2, Snort3 and Suricata.	Snort and Suricata NIDS will be used for project.	Does not investigate how to detect reconnaissance techniques.
3	The power of Network Penetration Testing [9]	2024	Provides a review of penetration testing (Pen testing), testing methods used to assess network security.	Provides a very good overview of Pen testing techniques, methods and tools used. Investigates reconnaissance techniques.	Does not investigate how to detect reconnaissance techniques.
4	Modelling Attack, Defence and Threat Trees and the Cyber Kill Chain (CKC), ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks. [5]	2020	Cybersecurity Attack/ Defence Frameworks are examined as well as Threat Modelling.	Reviews cyber attack and defence frameworks such as CKC and MITRE ATT&CK used to test NIDS.	Does not investigate how to detect reconnaissance techniques.
5	A Review of Research Work on Network-Based SCADA Intrusion Detection Systems [10]	2020	A Systematic Literature Review (SLR) of IDS relating to network connected control equipment.	A NIDS will be used to detect active reconnaissance and suspicious activity on the network.	Does not investigate how to detect reconnaissance techniques.

Brief Literature Review (Continued)

Published Peer Reviewed / Conference Papers	
Subject Area	Quantity
IDS / SIEM	11
Reconnaissance Detection	7
Cyber-Attack Framework	4
Reconnaissance / Footprinting	6
Penetration Testing	1
Port Scanning	1
Threat Hunting	12
Kerberos Authentication	5
Cybersecurity	5
Total	52



Literature Type	Subject Area
Books	
Certified Ethical Hacker Study Guide	Pen Testing / Reconnaissance techniques
CompTIA Security+ Study Guide	Cybersecurity
Online Resources	
MITRE ATT&CK Framework	Cyber-Attack Framework
Lockheed Martin Cyber Kill Chain	Cyber-Attack Framework
Online Web Application Security Project (OWASP)	Cyber-Attack Framework
Snort IDS (Cisco)	IDS (Open Source)
Suricata IDS (Open Information Security Foundation) (OISF)	IDS (Open Source)
Wazuh SIEM	SIEM (Open Source)
National Institute of Standards and Technology (NIST)	Cybersecurity Framework (CSF)



[4] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25]

Summary of Literature Gap

Subject Area	Qty	Topics Covered	Literature Gap
IDS / SIEM	11	* Intrusion Detection * Scanning a network is discussed * Focus on DDoS and File Alteration detection * IDS Rules, Detection Methods	Reconnaissance Detection of Scanning, including different types of scans were not researched. Also, other reconnaissance tools were not discussed.
Reconnaissance Detection	7	* Detecting Recon via: * System Performance * AI and Machine Learning (ML) * Specifically on a Web server * Specifically focused on SDN using SDNRecon	Detecting network reconnaissance using a NIDS not researched.
Cyber-Attack Framework	4	MITRE ATT&CK, CKC, Cybersecurity Framework (CSF)	Reconnaissance detection not researched.
Reconnaissance / Footprinting	6	* DNS Footprinting * AI and ML in Reconnaissance Detection	Detecting network reconnaissance using a NIDS not researched.
Penetration Testing	1	* Good overview of Pen Testing	Detecting network reconnaissance using a NIDS not researched.
Port Scanning	1	* If Port Scanning is a precursor to an attack	Detecting network reconnaissance using a NIDS not researched.
Threat Hunting	12	* Log analysis to ID suspicious activity * Attack Frameworks * Indicators of Compromise (IoC) * Phishing Attacks	Detecting network reconnaissance using a NIDS not researched.
Kerberos Authentication	5	* Kerberos Authentication attacks * Kerberoasting	Detecting network reconnaissance using a NIDS not researched.
Cybersecurity	5	CKC, Wireless Security, DNS Security	Detecting network reconnaissance using a NIDS not researched.
Total	52		

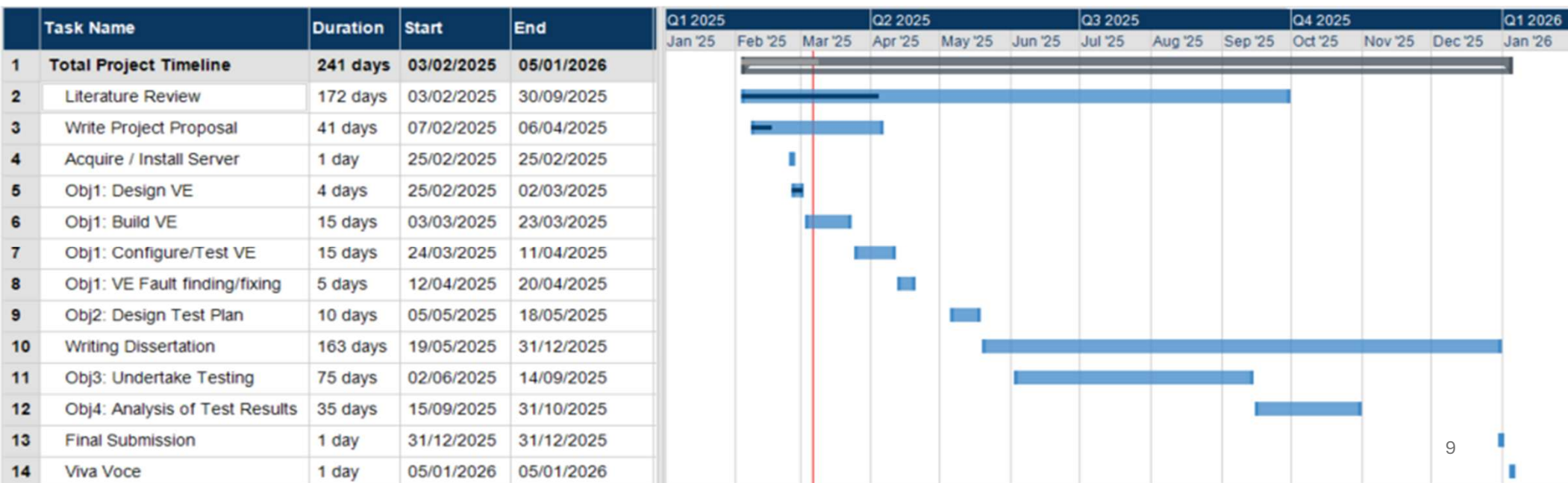
Research Methodology

#	Stage of Onion	Methodology	Reason	Justification in relation to project
1	Philosophy	Positivism	Knowledge based on observable facts, involving testing and measuring. Data will be gathered objectively by experimentation.	NIDS will be used to detect reconnaissance activity. Also, comparison between Snort and Suricata NIDS.
	Underlying Philosophy	Research Focused	Gathering Objective Data	Gathering data of NIDS effectiveness in detecting reconnaissance activity, a theory will be developed from the data gathered.
2	Approach	Inductive	Data will be gathered from experimental testing. Data will be used to develop a theory.	Investigating the effectiveness of NIDS in detecting reconnaissance activity. The data will be analysed leading to developing a theory.
3	Strategy	Experiment	Examining the relationship between two variables Independent Variable (IV) the manipulated variable and Dependent Variable (DV) the observed variable.	IV will be the reconnaissance activity. DV will be the NIDS detection capability.
4	Choices	Mixed Method	Both Qualitative will be used to analyse text data and Quantitative will be used for analysing numeric data.	Qualitative: To analyse the data collected from NIDS in relation to reconnaissance activity. Whether the NIDS was successful or not in detecting reconnaissance activity. Quantitative: To conduct comparative analysis of Snort and Suricata NIDS.
5	Time Horizon	Cross Sectional	A snapshot will be taken during each test of the test plan.	Multiple tests will be carried out, each being a snapshot of how the system reacts at that particular moment in time.
6	Data Collection and Analysis		Data Collection Qualitative Using Qualitative Analysis to detect patterns of detection. Data Collection Quantitative Some Statistical Analysis to compare NIDS devices.	Qualitative Analysis: The goal is to find patterns , to determine which reconnaissance techniques can and cannot be detected. Quantitative - Statistical Analysis: To identify differences in detection between Snort and Suricata.
[26]				

Project Planning and Resources

Resources:

- Server to host VE sufficient Processor, Memory and Diskspace (Acquired)
- Software: Attack & NIDS tools – Open Source and Freely downloadable



Project Impact and Limitations

- System to enable monitoring and alerting of reconnaissance activity
- Reporting of suspicious network activity:
 - Reconnaissance Activity
 - Frequency
 - Trends
- Limitations:
 - Hard Disk space
 - NIDS require substantial disk space to store logs of activity (Dependent on detection method)
 - Cost:
 - Suricata rules are free (Additional Rules are available at a cost)
 - Snort Community rules are free (Subscriber and Snort+ rules between \$500-5000 per annum)
 - Time: Work and other commitments

References

- [1] Z. S. Younus and M. Alanezi, "Detect and Mitigate Cyberattacks Using SIEM," 2023-12-18. doi: 10.1109/dese60595.2023.10469387.
- [2] K. Geetha, A. G. Sreedevi and A. R. Chadha, "Unraveling IoT Network Security with Snort for Robust Intrusion Detection and Prevention," 2024-03-15. doi: 10.1109/inc460750.2024.10649075.
- [3] M. Andronache, A. Vulpe and C. Burileanu, "A_Comparative_Study_of_Intrusion_Events_in_Different_SIEM_Systems," 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), pp.000065, 2025. doi: 10.1109/sami63904.2025.10883178.
- [4] S. Oriyano, *Certified Ethical Hacker (CEH) v9*, 3rd Ed. Indianapolis: Sybex, 2016.
- [5] J. Straub, "Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks," 2020-11. doi: 10.1109/smartcloud49737.2020.00035.
- [6] Roger Kwon, et al., "Cyber_Threat_Dictionary_Using_MITRE_ATT&CK_Matrix_and_NIST_Cybersecurity_Framework_Mapping," *Resilience Week (RWS)*, pp.106–112, 2020. doi: 10.1109/RWS50334.2020.9241271.
- [7] J. Verma, et al., "Ethical Hacking through Foot Printing: A Machine Learning Strategy," 2023-08-18. doi: 10.1109/iccube58933.2023.10392124.
- [8] A. A. E. Boukebous, et al., "A Comparative Analysis of Snort 3 and Suricata," 2023-05-19. doi: 10.1109/globconet56651.2023.10150141.
- [9] H. J. Badarneh, et al., "The power of Network Penetration Testing," 2024 25th International Arab Conference on Information Technology (ACIT), pp.1, December 10 2024. doi: 10.1109/acit62805.2024.1087721.
- [10] S. V. B. Rakas, M. D. Stojanovic and J. D. Markovic-Petrovic, "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems," *IEEE Access*, vol. 8, pp.93083, 2020. doi: 10.1109/access.2020.2994961.
- [11] A. R. Muhammad, P. Sukarno and A. A. Wardana, "Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning," *Procedia Computer Science*, vol. 217, pp.1406, 2023. doi: 10.1016/j.procs.2022.12.339.
- [12] X. Qin, et al., "A hybrid cyber defense framework for reconnaissance attack in industrial control systems," *Computers & Security*, vol. 136, -09-29 2023. doi: 10.1016/j.cose.2023.103506.
- [13] A. Zohourian, et al., "IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks," *Computers & Security*, vol. 146, -11 2024. doi: 10.1016/j.cose.2024.104034.
- [14] A. Waleed, A. F. Jamali and A. Masood, "Which open-source IDS? Snort, Suricata or Zeek," *Computer Networks*, vol. 213, -06-22 2022. doi: 10.1016/j.comnet.2022.109116.
- [15] A. Coscia, et al., "Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks," *Journal of Information Security and Applications*, vol. 82, -03-06 2024. doi: 10.1016/j.jisa.2024.103736.
- [16] J. Zhang, et al., "ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks," *Computer Networks*, vol. 245, -03-27 2024. doi: 10.1016/j.comnet.2024.110376.
- [17] D. Seidl and M. Chapple, *CompTIA Security+ Study Guide*, Eighth Ed. Indianapolis: Sybex, 2021.
- [18] MITRE. "ATT&CK Matrix." <https://attack.mitre.org/> (accessed 20/2).
- [19] Lockheed Martin. "Cyber Kill Chain." <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> (accessed 20/02).
- [20] Open Web Application Security Project (OWASP). "OWASP Top Ten." <https://owasp.org/www-project-top-ten/> (accessed 20/02).
- [21] Cisco. "Snort." <https://www.snort.org/> (accessed 21/02).
- [22] Open Information Security Foundation (OISF). "Suricata." <https://suricata.io/> (accessed 21/02).
- [23] wazuh.com. "Wazuh - Open Source SIEM." <https://wazuh.com/> (accessed 22/02).
- [24] National Institute of Standards and Technology (NIST). "Cybersecurity Framework." <https://www.nist.gov/cyberframework> (accessed 22/02).
- [25] PubGenius.Inc. "Scispace - AI Chat for scientific PDFs." <https://scispace.com/> (accessed 12/02).
- [26] M. N. K. Saunders, A. Thornhill and P. Lewis, *Research methods for business students*, 7th Ed. Harlow, England: Pearson Education Limited, 2016.

Questions?

