Week 7 – Tutorial Exercise

**Answer the following questions:**

1. Why should any network undergo security audits regularly?  
   Regular network security audits help organisations find and fix weaknesses before hackers do. They keep networks protected against new and changing cyber threats, especially as businesses add new devices, software, and support remote work. Audits use expert checks and automated tools to spot risks, making sure the network stays safe and up to date ([Ellis-Barker](https://www.hamilton-barnes.com/about-us/meet-the-team/profile/sarah-ellisbarker/) 2024).
2. How is external audit different from internal audit?  
     
   External audits and internal audits differ on the purpose and the auditors. External audits main purpose is to verify the compliance and provide assurance on the accuracy of the company's IT controls and systems to stakeholders like regulators and investors. This is done by third-party individuals that focus on the compliance framework of the company for regulation. Internal audits on the other hand, focuses on improving the system, updating and identifying any risk that can penetrate the system and breach the data. This audit is performed by the company’s employee.
3. A medium-sized e-commerce company is experiencing increasing attempts at fraud, system scanning, and credential stuffing attacks. The current security setup includes a basic firewall and signature-based IDS. You have been brought in as a security consultant. Your tasks are:
4. Evaluate the limitations of relying solely on a signature-based IDS for this environment.  
   It cannot detect zero-day attacks because those exploits do not yet have a known signature. It also struggles against polymorphic malware, where attackers make small changes to the code to avoid detection. Finally, it is weak at spotting behavioral attacks such as credential stuffing, brute-force logins, or misuse of legitimate accounts, since these often appear to be normal traffic (Toback 2024).
5. Propose a layered IDS approach that includes anomaly detection to improve coverage. Explain where and how you would deploy anomaly detection (e.g., at endpoints, on the network, or in the cloud infrastructure).  
   To improve detection, the company should use a layered IDS that combines both signature-based and anomaly-based systems. At the network level (NIDS), IDS should be placed at important points like the firewall and between servers. The signature-based IDS can catch known exploits, while the anomaly-based IDS can learn normal traffic patterns and detect unusual activity, such as a sudden spike in login attempts or abnormal data transfers. At the host level (HIDS), IDS should be installed on web, application, and database servers. Here, signature-based IDS can detect known malware, while anomaly-based IDS can identify unusual behavior like strange processes, suspicious database queries, or privilege misuse. This way, both known and unknown threats can be detected more effectively.
6. Discuss specific examples of attacks or behaviours that anomaly detection could identify but signature-based systems might miss.  
   Intrusion Detection Systems (IDS) use two main methods which are signature-based and anomaly-based detection. Signature-based IDS works by comparing network traffic to a database of known threats, such as malicious domains, file hashes, or attack patterns, making it effective for detecting familiar attacks with high accuracy. However, it cannot catch new or unknown threats. Anomaly-based IDS, on the other hand, uses machine learning to learn normal system behavior and flags anything unusual, such as logins at odd hours or sudden spikes in connections. This helps detect zero-day attacks, but it can also create many false positives. Because of their strengths and weaknesses, the two methods work best when used together (N‑able, 2021).
7. During a forensic investigation of a suspected compromised system, you are asked to look for subtle indicators that might reveal an intrusion.

Based on the following common clues:

* Unusual dates and times of file creation or modification
* Hidden directories or files (e.g., system or user folders not normally visible)
* Out-of-place files or sockets (files in unusual locations or unexpected network endpoints)
* Abnormal processes (e.g., unknown or suspicious processes running under system or user accounts)

Answer the following:

1. Choose two of the clues above and explain why they may indicate a system compromise.  
   Unusual dates and times of file creation or modification may indicate compromise because attackers often create or alter files at odd hours when normal users are inactive. Abnormal processes can also signal intrusion, since attackers may run unknown or suspicious programs to maintain access or steal data.
2. What general tools or system utilities (not OS-specific) would you use to detect each clue you selected?  
   To detect unusual file dates or changes, tools like file integrity monitoring software or checksum utilities can be used to track modifications. For abnormal processes, process monitoring or system auditing tools can help identify suspicious programs running in the background.
3. Imagine you are setting up a honeypot for a university network that includes student labs, faculty offices, and administrative servers.
4. Where would you place a honeypot in this network to catch unauthorized internal scanning or lateral movement attempts? Justify your choice.  
   I would place the honeypot in the same network segment as the administrative servers, since attackers trying to move laterally or scan internally will likely target high-value systems in that area. This placement increases the chance of detecting unauthorized access attempts before real critical servers are compromised.
5. What kind of fake system or service would you simulate (e.g., file server, SSH login, printer server)? Why would that be a believable target for an attacker?  
   The honeypot could simulate a file server, SSH login service, or an HTTP web server, since all three are believable targets. Attackers often try to access file servers to steal data, use SSH to gain remote control, or exploit web servers to gain entry, making these services effective decoys to attract and detect malicious activity.

Reference:

[Ellis-Barker](https://www.hamilton-barnes.com/about-us/meet-the-team/profile/sarah-ellisbarker/), S., 2024 “What is a network security audit, and why are they important?

” Hamilton-Barnes, viewed on 29 August 2025  
<https://www.hamilton-barnes.com/resources/blog/what-is-a-network-security-audit--and-why-are-they-important-/>

Toback M., 2024, "Signature-based Detection for Enhanced Cybersecurity: What You Need to Know" Smallbiz, viewed on 29 August 2025

https://smallbizepp.com/signature-based-detection/

N‑able, 2021, "Intrusion Detection System (IDS): Signature vs. Anomaly-Based" viewed on 30 August 2025

https://www.n-able.com/blog/intrusion-detection-system