**Batch: B1 Roll No.: 16010121045**

**Experiment No. 3**

|  |
| --- |
| **Title:**  Honeypot with KF sensor. |

**Objective:** Honeypot with KF sensor.

|  |  |
| --- | --- |
| **CO** | **Outcome** |
| **CO5** | Interpret legal and ethical issues in security |

**Books/ Journals/ Websites referred:**

1. <http://www.keyfocus.net/kfsensor/>

2. <http://www.keyfocus.net/kfsensor/help/>

3. <https://www.youtube.com/watch?v=HvuIYE7UMHs>

4. <https://www.youtube.com/watch?v=nBqzBjGgJFw>

5. <https://www.youtube.com/watch?v=O3H1LH-V7nk>

**Abstract:**

A honeypot is a security mechanism designed to deceive attackers, gather information about their tactics, and protect real systems from their malicious activities. This concept involves deploying decoy systems or services that appear legitimate but are actually isolated and monitored, allowing security professionals to study attackers' behavior without risking the integrity of operational networks.

**Related Theory:**

**Types of honeypots:**

Honeypots can be categorized into several types based on their deployment and purpose. High-interaction honeypots fully emulate real systems and interact extensively with attackers, while low-interaction honeypots simulate only specific services or protocols with limited interaction. Additionally, there are research honeypots used for academic or research purposes, and production honeypots deployed within operational networks for security monitoring.

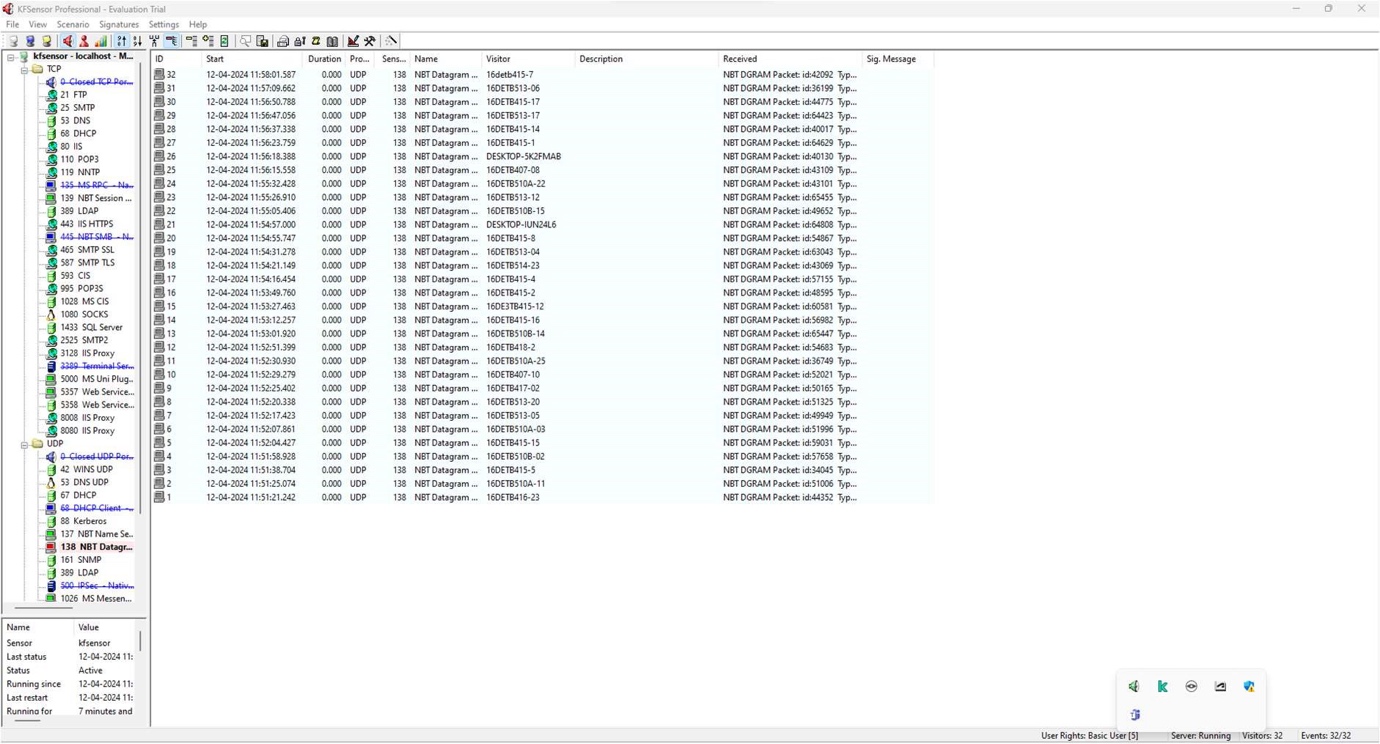
1. **Honeypots and evasion techniques:** Attackers may employ various evasion techniques to identify and avoid honeypots, such as fingerprinting, timing-based analysis, and protocol-specific evasion. Security practitioners must continuously update honeypot configurations and monitoring techniques to mitigate these evasion attempts effectively.
2. **Honeypot applications:** Honeypots serve multiple purposes in cybersecurity, including detecting and analyzing new threats, capturing malware samples, studying attacker tactics and techniques, and diverting attackers' attention away from critical systems. They can also aid in forensic investigations by providing valuable insights into attack methodologies and identifying compromised systems.

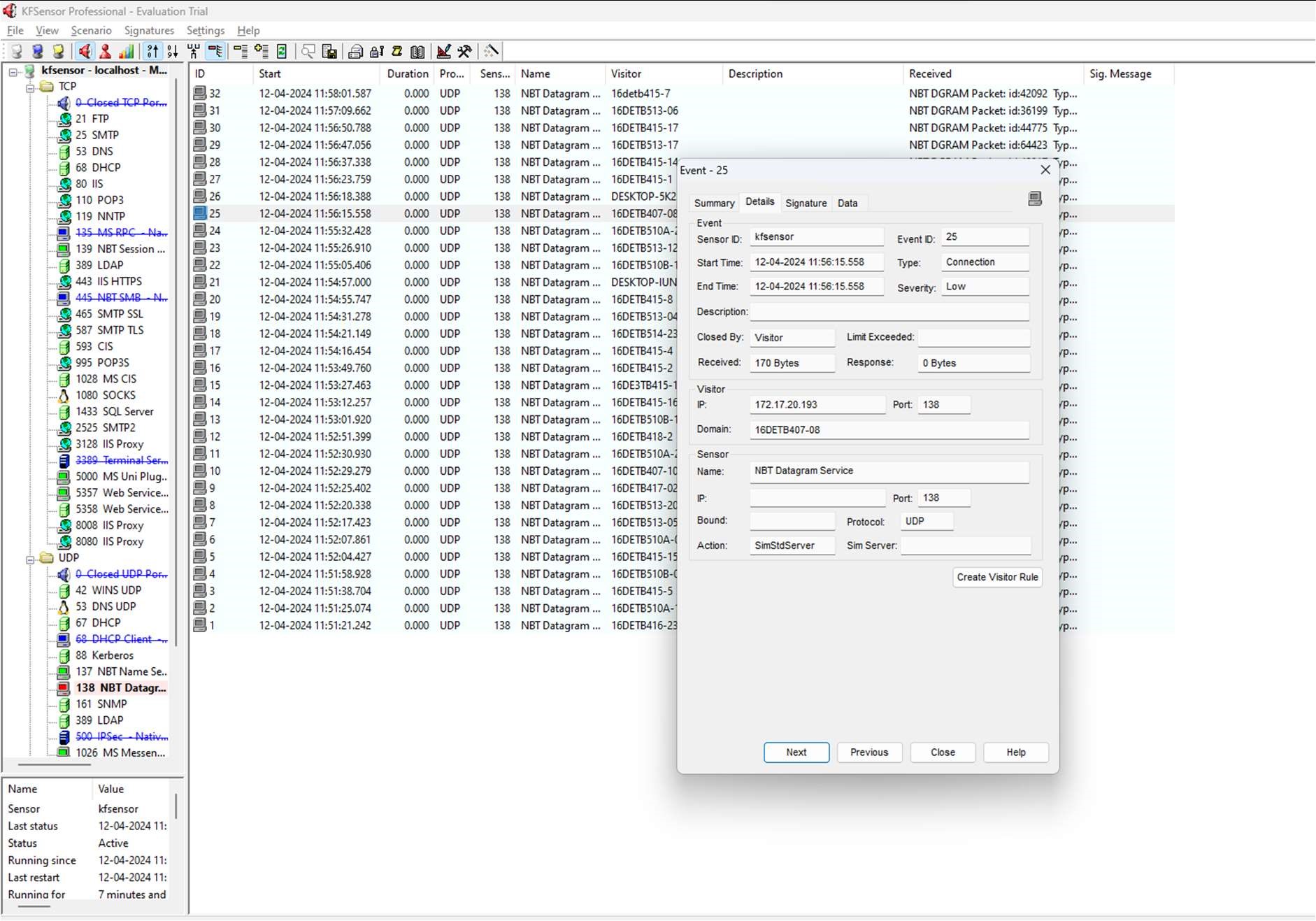
List of tools used as honeypots:

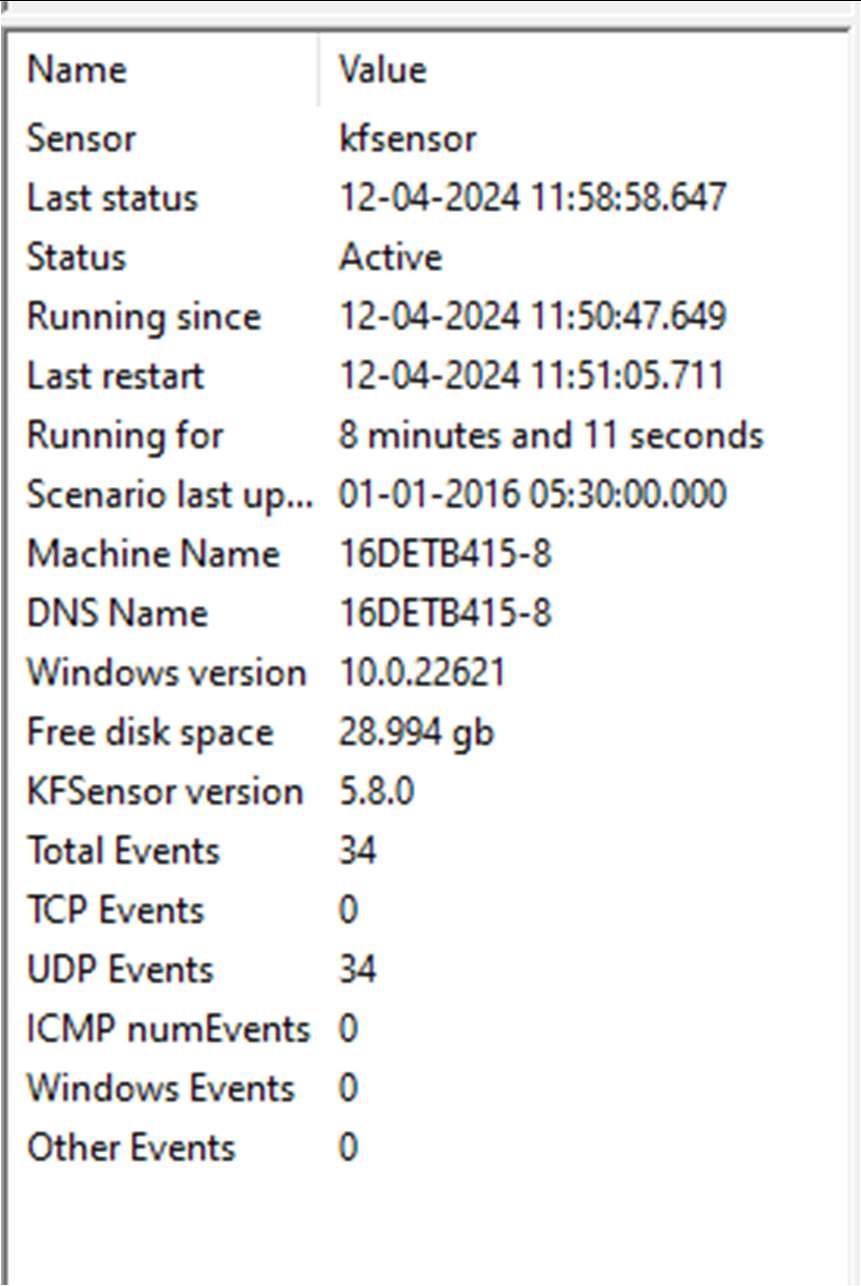
1. **Kippo:** A medium-interaction SSH honeypot designed to capture and log SSH brute force attacks and shell interaction.
2. **Dionaea:** A high-interaction honeypot focused on capturing malware samples and analyzing exploit attempts targeting network services like SMB, FTP, and HTTP.
3. **Cowrie:** A SSH and Telnet honeypot designed to emulate vulnerable Linux systems and capture attacker activity.
4. **Honeyd:** A low-interaction honeypot capable of emulating multiple IP addresses, operating systems, and network services to deceive attackers.
5. **Glastopf:** A web application honeypot that emulates vulnerable web applications to lure and capture attackers attempting to exploit web vulnerabilities.

These tools provide security professionals with versatile options for deploying honeypots tailored to specific environments and objectives, enabling proactive threat detection and intelligence gathering in cybersecurity operations.

**Implementation Details:**

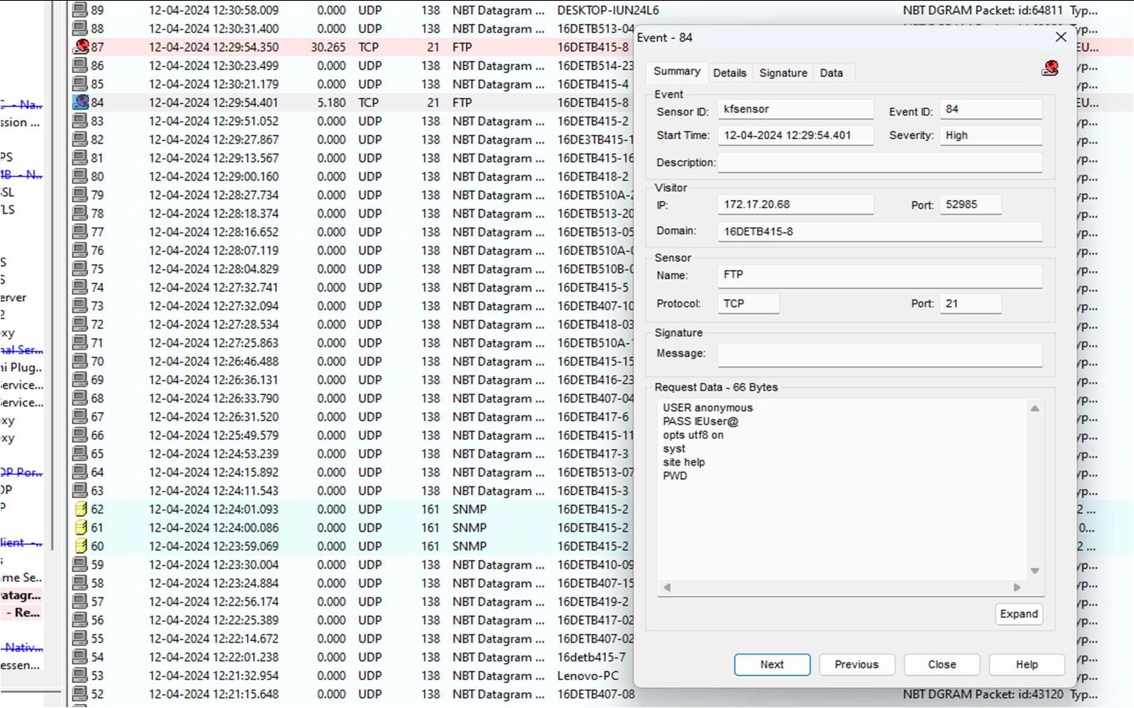






A screenshot of a computer

Description automatically generated



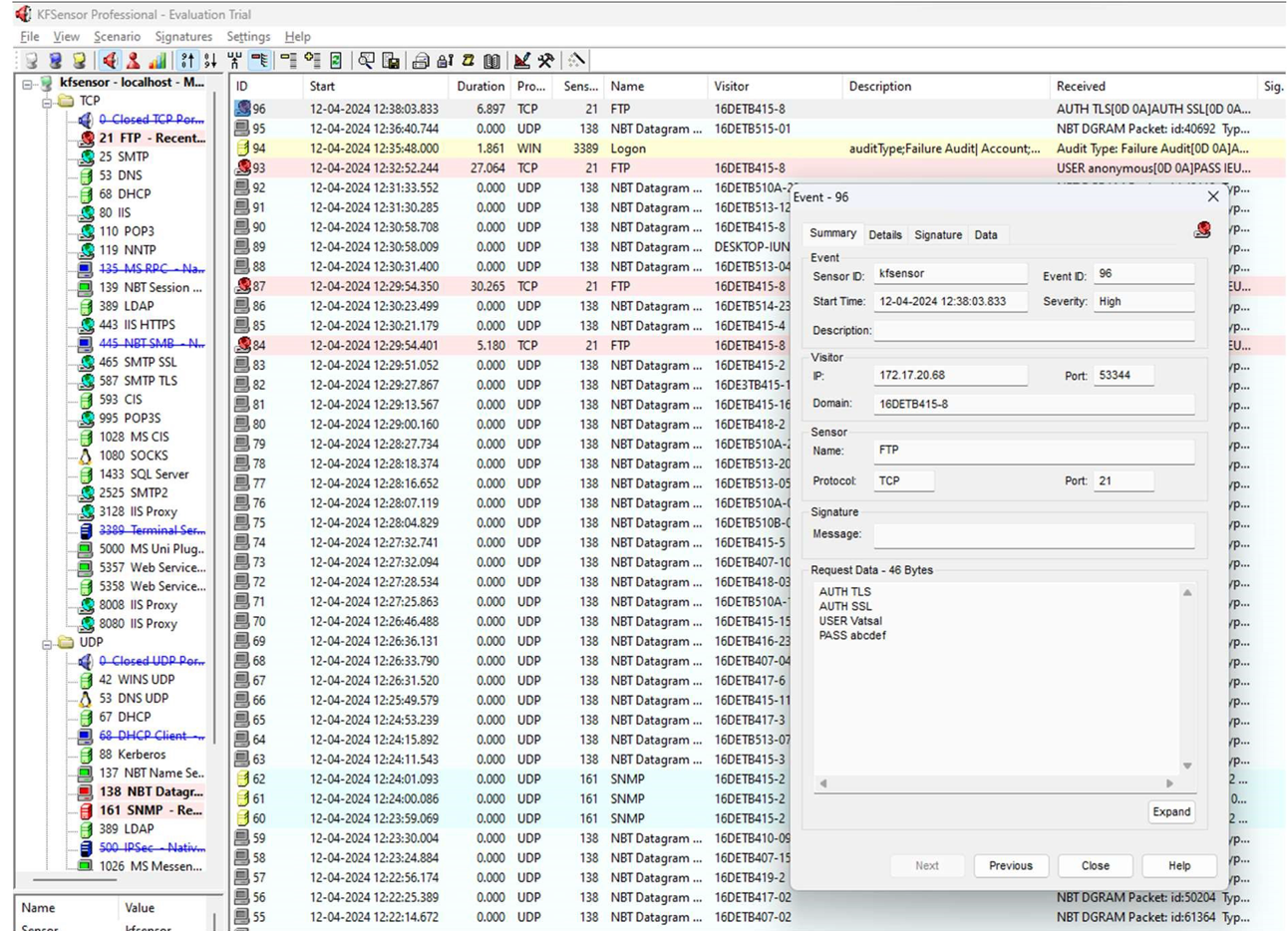
A screenshot of a computer

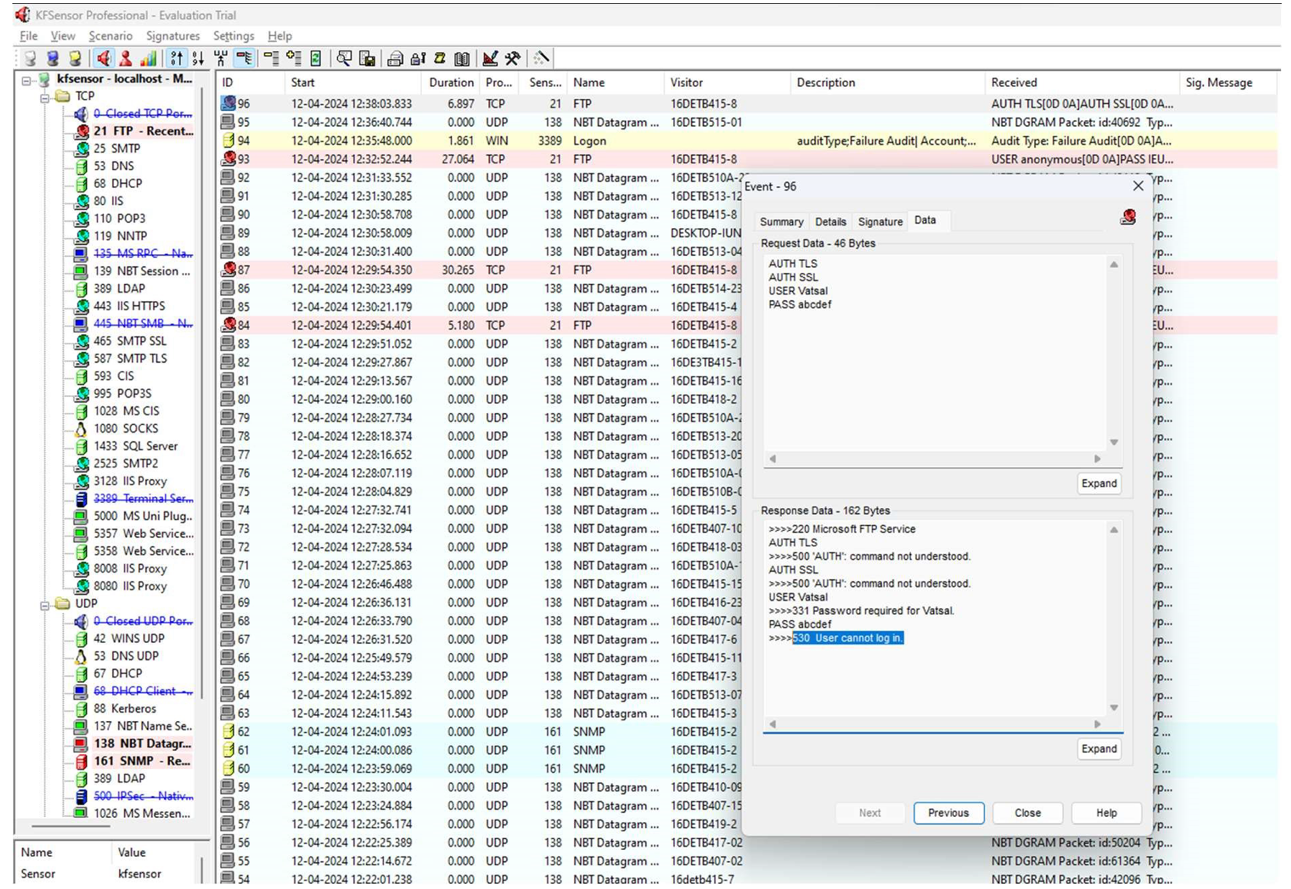
Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

****

****

**Postlab questions:**

**1. Differences and similarities between honeypot and firewall.**

Differences:

* Purpose: A firewall is primarily designed to prevent unauthorized access to or from a private network, whereas a honeypot is designed to lure attackers and gather information about their tactics, techniques, and procedures (TTPs).
* Functionality: Firewalls analyze and control incoming and outgoing network traffic based on predetermined security rules, while honeypots passively monitor and attract malicious activity without actively blocking or allowing traffic.
* Deployment: Firewalls are typically deployed at network perimeters or within the network to regulate traffic flow, while honeypots are deployed within the network or in a DMZ (Demilitarized Zone) to deceive attackers and gather intelligence.

Similarities:

* Both aim to enhance network security by identifying and mitigating threats.
* Both can be part of a comprehensive cybersecurity strategy to protect network resources.

**2. In a network architecture, what are the possible placements of honeypots in the design of the network?**

Honeypots can be placed at various points within a network architecture, including:

* Inside the internal network: Deployed alongside legitimate assets to detect insider threats or lateral movement by attackers who have breached perimeter defenses.
* In a DMZ (Demilitarized Zone): Positioned between the internal network and external-facing services to attract and monitor attacks targeting publicly accessible systems, such as web servers or email servers.
* Outside the network perimeter: Placed in the Internet-facing zone to intercept and analyze incoming threats before they reach the internal network, providing early warning and intelligence gathering capabilities.

**3. Discuss strengths and weaknesses of honeypots.**

Strengths:

* Threat detection: Honeypots can detect previously unknown threats and zero-day attacks by attracting and monitoring malicious activity that might evade traditional security measures.
* Intelligence gathering: They provide valuable insights into attacker tactics, techniques, and procedures (TTPs), which can be used to improve security posture, develop better defenses, and enhance incident response.
* Deception: Honeypots deceive attackers by presenting enticing targets, diverting their attention from critical assets, and wasting their time and resources.

Weaknesses:

* Resource-intensive: Honeypots require dedicated resources for setup, maintenance, and monitoring, which can strain IT infrastructure and personnel resources.
* False positives: They may generate false alerts or attract benign activity that mimics malicious behavior, leading to unnecessary investigations or alarms.
* Increased risk: Honeypots, if not properly configured and isolated, can pose a security risk by becoming compromised and used as launching pads for attacks against the rest of the network.