Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch:_____C3___	**Roll No.:16010121110**
Experiment No.	

Title:	Implementation/configuration of Honeypot

Objective: Understand honey pots using KF sensor

Expected Outcome of Experiment:

Outcome
CO3 Identify and analyze web attacks
CO4 Illustrate and Compare network security mechanisms

Books/ Journals/ Websites referred:

Abstract:-

Honeypots are used to deceive attackers into interacting with a system that appears to be part of a network but is actually isolated and monitored. They serve several purposes, including:

Gathering information about attack techniques and methods.

Diverting attackers away from real systems.

Acting as early warning systems by alerting security teams to potential threats.

Studying attacker behavior to improve cybersecurity defenses.

Related Theory: -

Understanding of Honeypots:

Honeypots are decoy systems or resources intentionally deployed to lure attackers and gather information about their tactics, techniques, and procedures (TTPs). They are typically isolated, monitored, and have no legitimate use, which makes any activity on them highly suspicious.

Types of Honeypots:

Research Honeypots: Used by security researchers to study attackers' behaviors and methods.

Production Honeypots: Deployed within a production network to detect and deflect attacks.

Low-Interaction Honeypots: Simulate only the services required to interact with potential attackers, minimizing resource usage and complexity.

High-Interaction Honeypots: Emulate complete systems or services, allowing deeper interaction with attackers but requiring more resources and maintenance.

Honeypots and Evasion Techniques:

Attackers often use evasion techniques to avoid detection or analysis on honeypots, such as scanning for common honeypot characteristics, fingerprinting the environment, or using encryption to obfuscate their activities.

Honeypot operators must continuously update their systems, employ deception techniques, and monitor for suspicious behavior to counter evasion attempts effectively.

Exploration of Tools for Honeypot Setup:

There are numerous tools available for setting up honeypots, ranging from open-source to commercial solutions. Some popular tools include:

Honeyd: A low-interaction honeypot that can emulate a wide range of services and operating systems.

Kippo: A medium-interaction SSH honeypot designed to log brute force attacks and shell interactions.

Cowrie: An SSH and Telnet honeypot with extensive logging capabilities and support for interaction with attackers.

Modern Honey Network (MHN): A framework for deploying and managing multiple honeypots across distributed environments.

Dionaea: A high-interaction honeypot designed to capture and analyze attacks targeting various network services like SMB, HTTP, and FTP.

KF Sensor and its Features:

KF Sensor is a commercial honeypot solution developed by KeyFocus Ltd.

It is known for its robustness and comprehensive features for detecting and mitigating cyber threats.

Some key features of KF Sensor include:

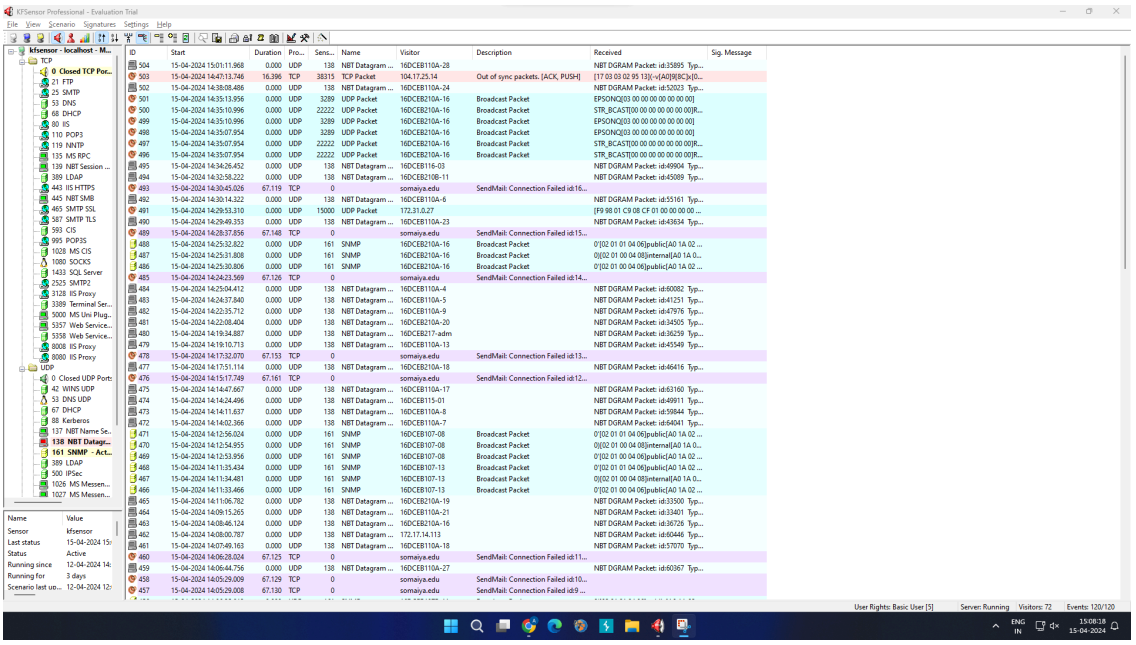
Multiple Protocol Support: It can emulate various network services and protocols, including HTTP, FTP, SMTP, and more.

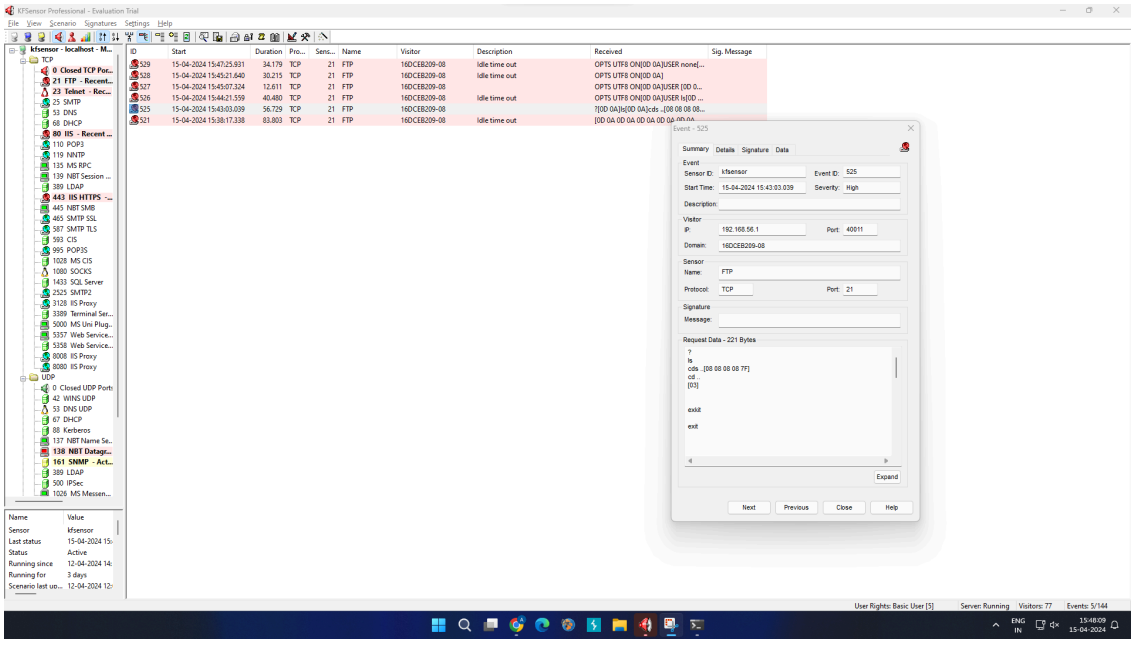
Real-Time Alerting: It provides real-time alerts on suspicious activities, enabling rapid response to potential threats.

Forensic Capabilities: KF Sensor captures detailed information about attackers' activities, facilitating forensic analysis and investigation.

Integration with Security Operations: It integrates with existing security operations workflows and tools, enhancing overall security posture.

Implementation Details:





Conclusion:- We have made a honeypot in the windows software. KF sensor made a honeypot for us. Whatever we typed was visible in the honeypot. KFSensor detects unknown threats and improves security, whilst also providing a low maintenance and cost effective solution. In this experiment, we have understood how honeypots work.

Post-Lab Questions:

1) **Differences and Similarities between Honeypot and Firewall:**

Differences:

Purpose:

Honeypots are designed to be breached, allowing organizations to gather intelligence on attackers' methods and motivations.

Firewalls, on the other hand, are designed to prevent unauthorized access to or from a private network, acting as a barrier between trusted and untrusted networks.

Handling of Traffic:

Honeypots attract and interact with malicious traffic, logging and analyzing it for security purposes.

Firewalls filter and block or allow traffic based on predefined rules and policies, often without direct interaction.

Visibility:

Honeypots provide a high level of visibility into attackers' behavior and tactics, allowing organizations to better understand and mitigate threats.

Firewalls primarily provide network-level visibility and control, focusing on managing traffic flow and enforcing security policies.

Similarities:

Security Enhancement: Both honeypots and firewalls contribute to enhancing network security, albeit in different ways. Honeypots provide insight into potential threats, while firewalls enforce access control policies.

Network Components: Both are components of a comprehensive network security strategy, with each serving a distinct role in protecting the network from unauthorized access and malicious activity.

Deployment: Both honeypots and firewalls can be deployed at various points within a network architecture to provide security benefits.

2) Possible Placements of Honeypots in Network Architecture:

Honeypots can be strategically placed within a network architecture to maximize their effectiveness. Possible placements include:

Internal Network: Inside the internal network to detect insider threats or lateral movement by attackers who have already breached perimeter defenses.

DMZ (Demilitarized Zone): In the DMZ to lure and monitor external attackers attempting to breach the network perimeter.

Behind Firewall: Behind the firewall to capture and analyze traffic that has already passed through perimeter defenses.

Internet-Facing: Exposed directly to the internet to attract and study a wide range of attackers and attack techniques.

3) Strengths and Weaknesses of Honeypots:

Strengths:

1. Early Detection: Honeypots can detect attacks at an early stage, often before they can cause significant damage to production systems.
2. Attack Intelligence: They provide valuable insight into attackers' tactics, techniques, and procedures (TTPs), aiding in the development of more effective security measures.
3. Deception: Honeypots deceive attackers into wasting time and resources targeting fake systems, potentially deterring them from attacking real assets.
4. Flexibility: Honeypots can be customized and deployed in various configurations to meet specific security objectives.

Weaknesses:

1. Resource Intensive: High-interaction honeypots, in particular, can be resource-intensive to deploy and maintain.
2. False Positives: Honeypots may generate false positives if legitimate users inadvertently interact with them or if benign scanning activity is mistaken for malicious behavior.
3. Limited Production Value: While honeypots provide valuable threat intelligence, they do not directly protect production systems and may not detect all types of attacks.
4. Evasion: Sophisticated attackers may recognize and avoid honeypots, limiting their effectiveness against determined adversaries.