4.MODULE DESIGN

In the project entitled as “LOGGING BRUTE FORCE ATTACKS WITH HONEY POTS “, there are three module which was used in this project they are as followed,

- MODULE 1-SYSLOG-NG
- MODULE 2-HYDRA
- MODULE 3-NMAP

MODULE DESCRIPTION

4.1 SYSLOG-NG

A syslog within the setting of a brute constrain assault regularly alludes to the logging of important occasions and exercises related to the assault within the framework log records. Syslog could be a standard logging convention utilized by organize gadgets, servers, and other network-aware gadgets to send framework log or occasion messages to a logging server or collector.
Within the case of a brute constrain assault, syslog passages might incorporate:

IP Addresses: Syslog sections may record the source IP addresses of endeavoured logins, making a difference directors distinguish the root of the assault.

Timestamps: The timestamps of login endeavours can give bits of knowledge into the recurrence and length of the assault.

Client Accounts Focused on: Data almost the client accounts focused on by the assault can be logged, supporting in understanding the scope of the interruption endeavor.

Confirmation Disappointments: Subtle elements approximately verification disappointments, such as off base passwords or usernames, may be logged.

4.2 HYDRA

Hydra is a popular and powerful tool used in cybersecurity for performing brute force attacks against various types of network services and protocols. It's designed to systematically try different combinations of usernames and passwords until it finds the correct credentials, thus gaining unauthorized access to a system or service.

WORKING OF HYDRA

Target Selection: The attacker selects a target system or service that they want to gain access to. This could be an SSH server, FTP server, web application login page, or any other service that requires authentication.

Configuration: The attacker configures Hydra with the target service's protocol (e.g., SSH, FTP, HTTP), specifying the usernames and passwords they want to try. Hydra supports a wide range of protocols and authentication methods.

Execution: The attacker initiates the brute force attack by running Hydra with the specified configuration. Hydra then systematically tries each username/password combination against the target service until it either succeeds in finding the correct credentials or exhausts all possibilities.

Logging and Output: During the attack, Hydra logs its progress, including successful logins and failed attempts. This information can be used by the attacker to identify valid credentials or by defenders to detect and respond to the attack.
Detection and Response: Security teams can monitor network logs and analyze patterns of login attempts to detect brute force attacks early. Upon detection, appropriate response actions can be taken, such as blocking the attacker's IP address, resetting compromised passwords, and strengthening security controls.

4.3 NMAP

Nmap, or Network Mapper, is a widely used open-source tool for network discovery and security auditing. While Nmap itself is not typically used as a brute force attack tool, it can play a crucial role in reconnaissance and preparation phases of such attacks.
Host Discovery: Nmap can discover hosts on a network by sending ICMP echo requests, TCP SYN, ACK, or UDP probe packets to various IP addresses and analyzing responses to determine which hosts are active

Operating System Detection: Nmap can attempt to identify the operating system of a target system by analyzing subtle differences in how it responds to network probes. This information helps in understanding the target environment better

Scripting Engine (NSE): Nmap's scripting engine allows users to write and execute custom scripts to automate various tasks such as service enumeration, vulnerability detection, and exploitation. NSE scripts extend Nmap's functionality and adaptability to specific tasks.

Service Version Detection: Nmap can detect the version of services running on open ports by analyzing the responses received from the target systems. This information is useful for identifying potential vulnerabilities and planning targeted attacks