SYNOPSIS

The project entitled as “LOGGING BRUTE FORCE ATTACKS WITH HONEY POTS”, In the realm of cybersecurity, detecting and mitigating brute force attacks is a critical endeavor to safeguard systems and data integrity. This proposed project aims to deploy honeypots strategically to lure and monitor malicious actors attempting brute force attacks, thereby enhancing threat detection capabilities and fortifying defenses.

The project begins with an overview of brute force attacks, elucidating their mechanisms and potential impact on vulnerable systems. It then delves into the concept of honeypots as deceptive traps designed to attract attackers while concealing actual assets.

Brute force attacks can be identified with the help of System Logs and this work concentrates on building an environment that identifies and records the brute force attacks using a HoneyPot mechanism.

1.INTRODUCTION

1.1 BACKGROUND AND STUDY OF THE PROJECT

Research and study on logging brute force attacks are essential components of cybersecurity efforts aimed at understanding, detecting, and mitigating such threats effectively.

Brute force attacks are a means of determining a combination of username and password or hashed token in order to gain unauthorized access to an account, file, or other protected information. A brute force attack is a trial-and-error–based attack method that works by guessing credentials, file paths, or URLs, either through logic or running all possible keyboard combinations.

Attackers often employ malware and other tools to automate the process of brute force attacks either by distributing the attack across a variety of source locations or leveraging malware to attack protected internal accounts. Common tools such as Hydra, Chaos, CrackMapExec, and PoshC2 all have brute force functions.

1.2 OVERVIEW OF THE PROJECT

Honeypots are sacrificial computer system that's intended to attract cyberattacks, like a decoy. It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets.

Brute force attacks can be identified with the help of System Logs and this work concentrates on building an environment that identifies and records the brute force attacks using a HoneyPot mechanism.

Logging brute force attacks using honeypots involves setting up deceptive systems or services designed to attract attackers and logging their activities.

3.SYSTEM SPECIFICATION

3.1 HARDWARE CONFIGURATION

- PROCESSOR : 12th Gen Intel(R) Core (TM) i5-1235U 1.30 GHz
- HARD DISK CAPACITY : 500 GB
- INTERNAL MEMORY CAPACITY : 8 GB

3.2 SOFTWARE CONFIGURATION

- OPERATING SYSTEM :UBUNTU OS
- ROUTER :JUNIPER ROUTER
- SWITCH :V-SWITCH

3.3 SOFTWARE DESCRIPTION

OPERATING SYSTEM: UBUNTU OS

Ubuntu is a free and open-source operating system based on Debian, another Linux distribution. Ubuntu uses Linux as its kernel. Linux is a free and open-source monolithic kernel. Ubuntu uses an application software called Advanced Package Manager (APT) to help users download, install, and manage packages (software).

Ubuntu is a popular free and open-source Linux-based operating system you can use on a computer or virtual private server. Ubuntu was introduced in 2004 by a British company Canonical. It was based on Debian – a popular distro back then – which was difficult to install.

FEATURES OF UBUNTU OS

- The desktop version of Ubuntu supports all the normal software on Windows such as Firefox, Chrome, VLC, etc.
- It supports the office suite called **LibreOffice**.
- Ubuntu has an in-built email software called Thunderbird, which gives the user access to email such as Exchange, Gmail, Hotmail, etc.
- There are a host of free applications for users to view and edit photos.
- There are also applications to manage videos and it also allows the users to share videos.
- It is easy to find content on Ubuntu with the smart searching facility.

ADVANTAGES OF UBUNTU OS

- Ubuntu is free and an open-source operating system.
- Ubuntu is more secure.
- Ubuntu runs without install.
- Ubuntu supports window tiling.
- Ubuntu is more resource-friendly.
- Ubuntu is completely customizable.
- A well-rounded operating system for desktop computing.

JUNIPER ROUTER

Juniper Networks offers a robust portfolio of software-defined networking routers to help service providers, cloud operators, and enterprises transform their networks to meet today's demands and future growth. We optimize each router family — ACX, MX, PTX, and SSR — to meet the needs of access, edge, and core, as well as cloud and data center networks. Juniper's innovative router portfolio is packed with scale and efficiencies that allow network providers to adapt to unforeseen changes in the market as they build their networks up and out.

ADVANTAGES OF JUNIPER ROUTER

- A router has multiple interfaces and receives data packets through them.
- It evaluates the network addresses of the incoming packets and decides which interface to forward the packet to.
- It uses its local routing table for decision-making.
- This can be statically configured or calculated via dynamic routing protocols such as OSPF or BGP.

V-SWITCH

A vSwitch is a software-based network switch that operates within a hypervisor to facilitate communication between virtual machines (VMs) or between VMs and the physical network.In virtualized environments, multiple virtual machines (VMs) may run on a single physical server.

Each VM requires network connectivity to communicate with other VMs, external networks, or the internet. A vSwitch acts as a virtual networking infrastructure within the hypervisor, enabling VMs to connect to each other and to external networks. It provides similar functionality to a physical network switch by forwarding network traffic between VMs and external networks.

ADVANTAGES OF V-SWITCH

- Separation of networks with VLANs and routers, allowing you to restrict access from one network to another.
- Improved security.
- Flexible network management.
- Fewer hardware network adapters needed for redundant network connection