Hydra FTP Brute Force Attack

Ebrima Jatta

Date: 08/11/2025

contact info ebrimajjjatta@gmail.com

Table of Contents

Introduction

In this project, I simulated a brute-force attack using Hydra on an intentionally vulnerable system.
The project demonstrates how weak passwords can be exploited and the importance of strong authentication policies.

Objective

The goal is to understand password cracking techniques, assess password and explore defensive measures such as strong passwords, account lockout, and multi-factor authentication.

Tools & Environment

-OS: Kali Linux 2025.2 on virtualBox
-Tools: Nmap and Hydra

Methodology

1. Lab setup

configure Kali Linux as the attacker VM and Metasploitable2 as the target VM on an isolated virtual network.

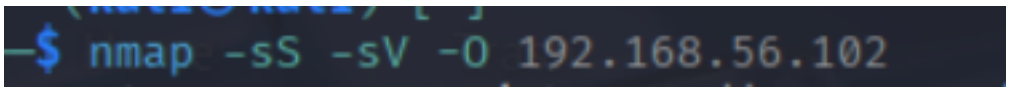
2. Verify connectivity

ping 192.168.56.102

3. Reconnaissance – Nmap scan

Performed a service and os dectection scan:

$ nmap -sS -sV -O 192.168.56.102



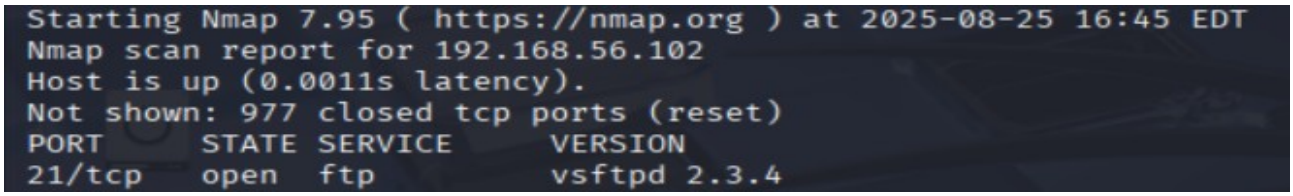
-sS: TCP SYN scan for stealthy approach

-sV: detect service versions

-O: suggests probable os

Observed output:

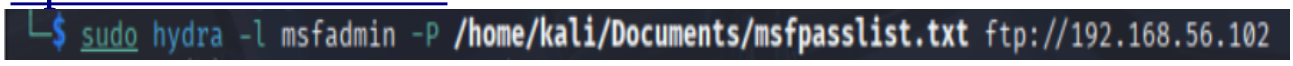
PORT	STATE	SERVICE	VERSION
20/tcp	open	ftp	vsftpd 2.3.4



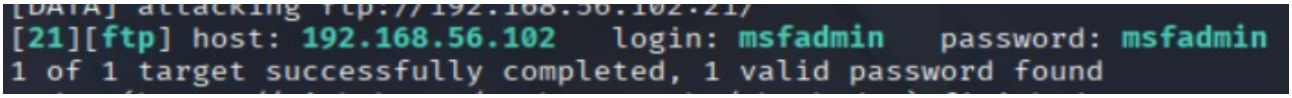
4. Attack – Hydra brute-force (FTP)

Executed Hydra against the discovered FTP service using a password wordlist:

hydra -l msfadmin -P /home/kali/Documents/msfpasslist.txt ftp://192.168.56.102



Observed output:



Results

1. Nmap scan

A network scan was conducted using Nmap to identify open ports and services running on the target machine. The scan revealed multipule open ports and associated services, including the FTP service, which was later targeted with Hydra. This step provided crucial information for planning the brute-force attack.

2. Hydra FTP Brute-Force Attack

Using Hydra, a brute-force attack was performed against the Ftp service o the Metasploitable2 targe machine.

The attack iterated through the provided password list and successfully discovered vaild login credentials for the FTP account. This demonstrates that weak or commonly used passwords can be exploited to gain unauthorized access.

Analysis

1.Nmap Scan

- The Nmap scan provided an overview of the target machine’s open ports and services, which is essential for vulnerability assessment.
- The scan results guided the brute-force attack by identifying the active FTP service and its port.
- Regular network scanning is important in security assessment to detect exposed services and reduce the attack surface.

2.FTP Brute-Force Attack (Hydra)

- The successful brute-force attack shows that the target machine’s FTP service was vulnerable to passwords guessing due to weak credentials.
- Using a common or small password list made it possible to quickly discover the password, demonstrating the importance of strong, unique passwords for system security.
- This emphasizes the need for implementing security measures such as:
  - Enforcing strong password policies
  - Account lockouts after multiple failed login attempts
  - Monitoring login attempts for suspicious activity

Conclusion

- The penetration testing exercise demonstrated that weak passwords on FTP services can be easily exploited using brute-force attacks, highlighting the the critical importance of password policies.
- Nmap scans are an effective reconnaissance tool, providing valuable information about open ports and running services that can guide further testing.
- Overall, the results emphasize the need for continuous security assessment, proper access controls, and reduce vulnerabilities and protect systems from unauthorized access.