UNIX PROJECT TUTORIAL: KALI LINUX - HYDRA AND HASHCAT
GIDEON ELEBODA
DAN LULKIN

Tutorial: Brute-Forcing SSH Credentials Using Hydra

Objective

Demonstrate how to set up a test environment to perform a brute-force attack on an SSH server using Hydra on Kali Linux.

What is a Brute-Force Attack?

- **Definition**: A brute-force attack is a method used to gain unauthorized access to a system or data by systematically guessing every possible combination of passwords or encryption keys.
- **Effectiveness**: It can be effective if the password is weak or the key space is small.
- **Example**:
    1. Suppose a password is a 4-digit numeric code.
    2. The attacker tries combinations: 0000, 0001, 0002... up to 9999.
    3. When the correct combination is found, access is granted.
- **Drawbacks**:
    - It is slow, especially for complex passwords.
    - Systems often have protections like account lockouts or rate-limiting to mitigate brute-force attempts.

What is Hydra?

- **Definition**: Hydra is a versatile tool used for performing brute-force attacks on various protocols and services, such as SSH, FTP, HTTP, and more.
- **Use Case**: It is often used by penetration testers to test the strength of passwords on target systems.
- **Key Features**:
    - Supports a wide range of protocols.

- Can use custom username and password lists.
- Multithreaded, allowing it to test multiple combinations simultaneously for faster results.

Prerequisites

1. Two virtual machines:
    - Kali Linux (attacker)
    - Debian (victim)
2. SSH service installed and running on the Debian VM.
3. Hydra installed on Kali Linux (pre-installed in most distributions).
4. Basic knowledge of terminal commands and Linux system administration.

Steps

1. Set Up the Environment

1. **Create a Test User on Debian VM**:
    - Login to your Debian VM.
    - Create a user with the command: sudo adduser <username>
    - Assign a simple password (e.g., password).
    - Using **sudo usermod -aG sudo <username>** give the user sudo
    - Grab the ip address using **ip address**
2. **Install and Start SSH Services on Both VMs**:
    - Install SSH using: **sudo apt update**
    - **sudo apt install openssh-server**
    - If SSH is already installed, check its status:
      sudo systemctl status ssh

- Start the SSH service:
  sudo systemctl start ssh

---

2. The Attack

1. **Dictionary Files**:
   - Kali Linux includes dictionaries like rockyou.txt and fasttrack.txt. These can be found in /usr/share/wordlists/.
   - Navigate to the wordlists directory (for this tutorial, use fasttrack.txt).
2. **Create a Username List (Optional)**:
   - To test multiple usernames, create a usernames.txt file:
     sudo nano usernames.txt
     Add your desired usernames in the file.
3. **Perform the Brute-Force Attack**:
   - On the Kali machine, run the command:
     hydra -l <username> -P /usr/share/wordlists/fasttrack.txt ssh://<Debian_VM_IP> -V -I -F
   - **Explanation of Flags**:
     - -l: Specifies the username.
     - -P: Specifies the password dictionary.
     - ssh://: Indicates the protocol to attack.
     - -V: Displays login + password attempts.
     - -L: Specifies the file of usernames (use -L usernames.txt if testing multiple usernames).
     - -t <num_of_threads>: Adds threads to improve performance.
4. **The Exploit**:
   - Hydra will display the valid username-password combination, highlighted in the output.

- Use the discovered credentials to log in via SSH:
  ssh <username>@<Debian_VM_IP>
- Once logged in, access or create any files you need.