PT – Project

Prerequisites

1. Ensure that all required tools are installed. These tools include:
    a. Nmap
    b. Impacket
    c. Other dependencies required by the script
2. Confirm you have the following:
    a. The script file (e.g., `ptp12.sh`).
    b. Root or sudo privileges on your Kali Linux machine.
    c. A network or IP range to scan.
    d. A password list file if you want to perform password strength checks.

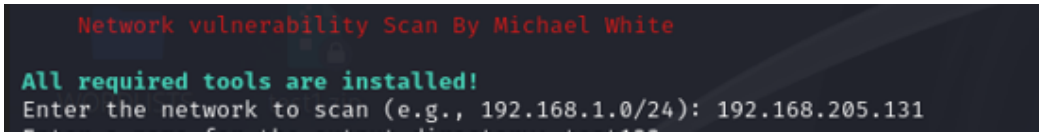
Steps to Use the Script

1. **Run the Script**
    a. Open a terminal and navigate to the directory where the script (`ptp12.sh`) is located.
    b. Use the following command to execute the script with `sudo`:

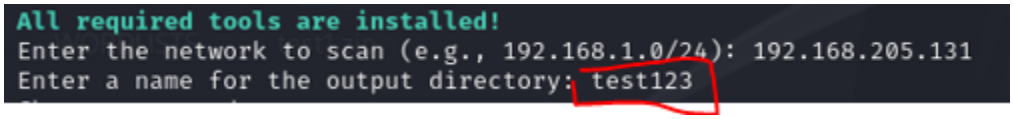
```
sudo ./ptp12.sh
```

2. **Input the Network to Scan**
    a. The script will prompt you to enter the network or IP address to scan.
    b. Examples:

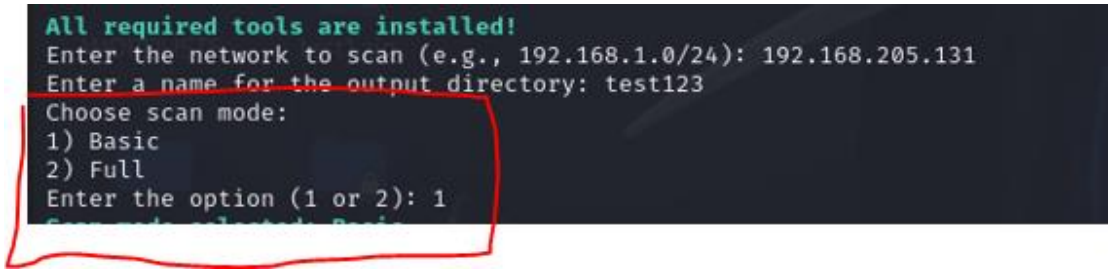
i. For a specific IP: `192.168.1.10`
ii. For a range of IPs: `192.168.1.0/24`



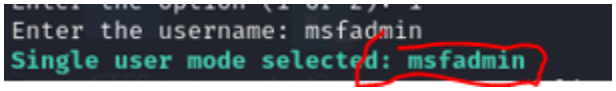
3. **Specify an Output Directory**
   a. Enter a name for the directory where the scan results will be saved.
   b. Example: `test123`



4. **Choose the Scan Mode**
   a. The script provides two scan modes:
      i. `Basic` (Option 1): Focused scan with fewer checks.
      ii. `Full` (Option 2): Comprehensive scan with more checks.
   b. Enter 1 or 2 based on your requirement.

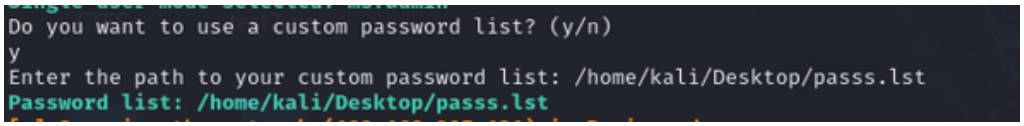


5. **Select the User Mode**
   a. **Single User** (Option 1): Test one specific username for weak passwords.
      i. Input the username when prompted. Example: `msfadmin`
   b. **User List** (Option 2): Use a list of usernames to test for weak passwords.



6. **Use a Custom Password List (Optional)**
   a. The script will ask if you want to use a custom password list. Enter:

i. y (yes): Specify the file path to your password list. Example: `/home/kali/Desktop/passs.lst`
ii. n (no): The script will use its default password list.



7. **Wait for the Scan to Complete**
    a. The script will start scanning the provided network.
    b. Detected services will be checked for weak passwords (e.g., SSH, FTP, Telnet).

Understanding the Output

1. **Log and Results Directory**
    a. The results will be saved in the directory you specified (e.g., `test123`).
    b. Important files include:
        i. `log.txt`: Detailed log of the scan.
        ii. Compressed `.zip` file containing results.
2. **Error Messages**
    a. If the script encounters errors (e.g., `Failed to identify logon prompt` for Telnet), this indicates the service is running but cannot be properly authenticated or identified.
3. **Successful Completion**
    a. Upon completion, the script will display a message indicating that the process is done. You can review the results in the specified output directory.

Tips and Best Practices

1. **Permissions**:
    a. Ensure the script has executable permissions. If not, run:

```
chmod +x ptp12.sh
```

2. **Test Small Networks First**:
    a. When scanning for the first time, try a small range (e.g., one or two IPs) to verify that the script runs as expected.
3. **Password List**:
    a. Use an updated and comprehensive password list for better results.
4. **Analyze Results**:
    a. After scanning, analyze the results to identify weak points and remediate them.

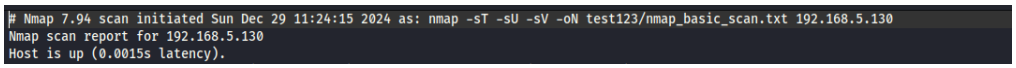
Common Issues and Troubleshooting

1. **Dependencies Missing**:
    a. Ensure required tools (e.g., `nmap`) are installed and accessible.
2. **Permission Denied**:
    a. Run the script with `sudo` privileges.
3. **Errors During Scan**:
    a. Review the `log.txt` file for details about errors.
4. **Scan Too Slow**:
    a. Consider running a `Basic` scan for faster results.

logs guideline:

1. Nmap Scan Log (`nmap_basic_scan.txt`)

- **Purpose**: This file identifies the open ports, services, and service versions on the scanned host.
- **Key Sections**:
  - **Scan Summary**:
    - Example:



    - Indicates when the scan started and the options used (`-sT`, `-sU`, `-sV`).
    - `Host is up (0.0015s latency)`: Confirms the target is reachable and its latency.
  - **Open Ports and Services**:
    - Example:

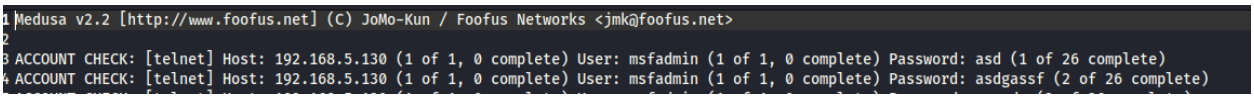
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
2.0)
```

      - **PORT**: Identifies the port number and protocol (e.g., `21/tcp`).
      - **STATE**: Indicates the port's status (`open`, `closed`, `filtered`).
      - **SERVICE**: Name of the service running on the port (e.g., `ftp`, `ssh`).
      - **VERSION**: Version of the detected service (e.g., `vsftpd 2.3.4`).
  - **Additional Information**:
    - Example: `MAC Address: 00:0C:29:51:01:8D (VMware)`
    - Reveals the host's MAC address and potential device type (e.g., VMware).
  - **Filtered and Unresponsive Ports**:
    - Example: `Not shown: 993 closed udp ports, 978 closed tcp ports`.
    - Indicates ports that did not respond or were filtered by firewalls.
  - **OS and Host Details**:
    - Example: `Service Info: Hosts: metasploitable.localdomain; OSs: Unix, Linux`.
    - Provides details about the OS and hostname.

2. Telnet Brute Force Log (`medusa_telnet.txt`)

- **Purpose**: Attempts to brute force Telnet using a list of passwords.
- **Key Sections**:
    - **Password Attempts**:
        - Example:

```
ACCOUNT CHECK: [telnet] Host: 192.168.5.130 User: msfadmin Password: asd
```



            - **User**: The username being tested (e.g., `msfadmin`).
            - **Password**: Password tried in this attempt (e.g., `asd`).
            - This section repeats for all passwords in the list.
    - **Successful Login**:
        - Example:

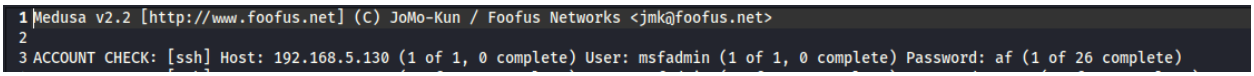
```
ACCOUNT FOUND: [telnet] Host: 192.168.5.130 User: msfadmin Password: msfadmin [SUCCESS]
```

            - Indicates a successful brute force attack using the username-password pair.
    - **Failure Indication**:
        - If no success messages are present, no credentials in the password list worked.

3. SSH Brute Force Log (`medusa_ssh.txt`)

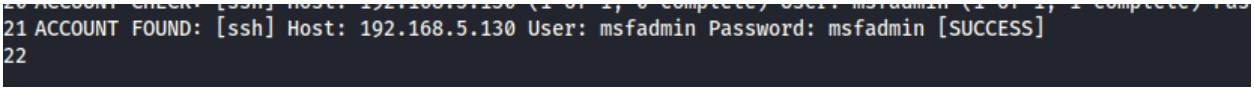
- **Purpose**: Brute forces SSH to test for weak passwords.
- **Key Sections**:
    - **Password Attempts**:
        - Similar to Telnet, logs each username-password pair tried.
        - Example:

ACCOUNT CHECK: [ssh] Host: 192.168.5.130 User: msfadmin Password: admin



- **Successful Login**:
  - Example:

ACCOUNT FOUND: [ssh] Host: 192.168.5.130 User: msfadmin Password: msfadmin [SUCCESS]

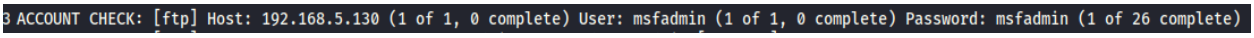


- Highlights the username and password combination that succeeded.

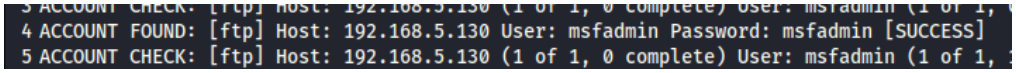
4. FTP Brute Force Log (`medusa_ftp.txt`)

- **Purpose**: Brute forces FTP for weak credentials.
- **Key Sections**:
  - **Password Attempts**:
    - Example:

ACCOUNT CHECK: [ftp] Host: 192.168.5.130 User: msfadmin Password: asdf



  - **Successful Login**:
    - Example:
      ACCOUNT FOUND: [ftp] Host: 192.168.5.130 User: msfadmin Password: msfadmin [SUCCESS]



5. Combined Log (`log.txt`)

- **Purpose**: Combines results from Nmap, Telnet, SSH, and FTP logs.
- **Key Sections**:
  - **Summarized Successful Logins**:
    - Example:

```
test123/medusa_ftp.txt: ACCOUNT FOUND: [ftp] Host: 192.168.5.130 User:
msfadmin Password: msfadmin [SUCCESS]
test123/medusa_ssh.txt: ACCOUNT FOUND: [ssh] Host: 192.168.5.130 User:
msfadmin Password: msfadmin [SUCCESS]
```

- Quickly identifies services where brute force attempts succeeded.

- **Scan Information**:
  - Links to the Nmap file for open ports and service details.