IPTables Exercise Attack/Defend Exercise

This exercise aims to provide students with hands-on experience in configuring firewall rules using IPTables to defend a virtual machine against a series of simulated attacks from another virtual machine. Students will learn how to analyze attack patterns, adjust firewall rules for enhanced security, and ensure the accessibility of legitimate services.

Requirements:

- Two virtual machines (VMs), VM1 Attacker and VM2 Defender (Same network)
- Install necessary tools on the attacker VM: nmap, curl, ssh, and hydra.

IPTables Exercise Attack/Defend Exercise

Conducting Attacks:

- Port Scanning: Use nmap to identify open ports on the defender VM.
- HTTP Request: Attempt to access a web service on the defender VM using curl.
- SSH Connection Attempt: Try to establish an SSH connection with the defender VM.
- SSH Brute-Force Attack: Use hydra to perform a brute-force attack on the SSH service of the defender VM.

IPTables Exercise Attack/Defend Exercise

Hydra

```
hydra -l username -P password_list.txt ssh://IP_address
```

•-l username: Here, you should replace "username" with the username you want to test.

•-P password_list.txt: Here, you should replace "password_list.txt" with the path to a file containing a list of passwords you want to try.

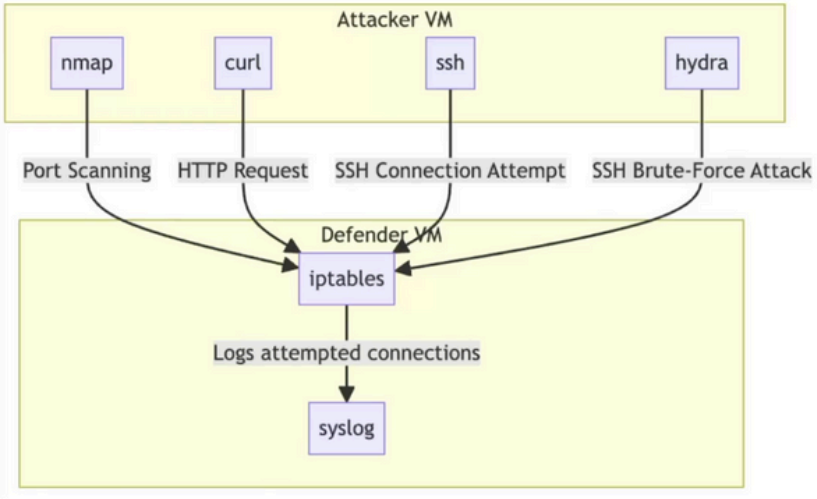
•ssh://IP_address: Here, you should replace "IP_address" with the IP address of the SSH server you want to attempt to access.

IPTables Exercise Attack/Defend Exercise

Defense Strategies:

- Implement rules to detect and block port scanning attempts.
- Block unwanted HTTP requests and limit SSH access to known IPs.
- Use rate limiting to defend against brute-force attacks.
- Log attempted connections for further analysis.

IPTables Exercise Attack/Defend Exercise



Picture source: own creation