Hanshuo Geng, Dom Spiotta, Joel Meyer, Alex Schieltz

Dr. Noureddine

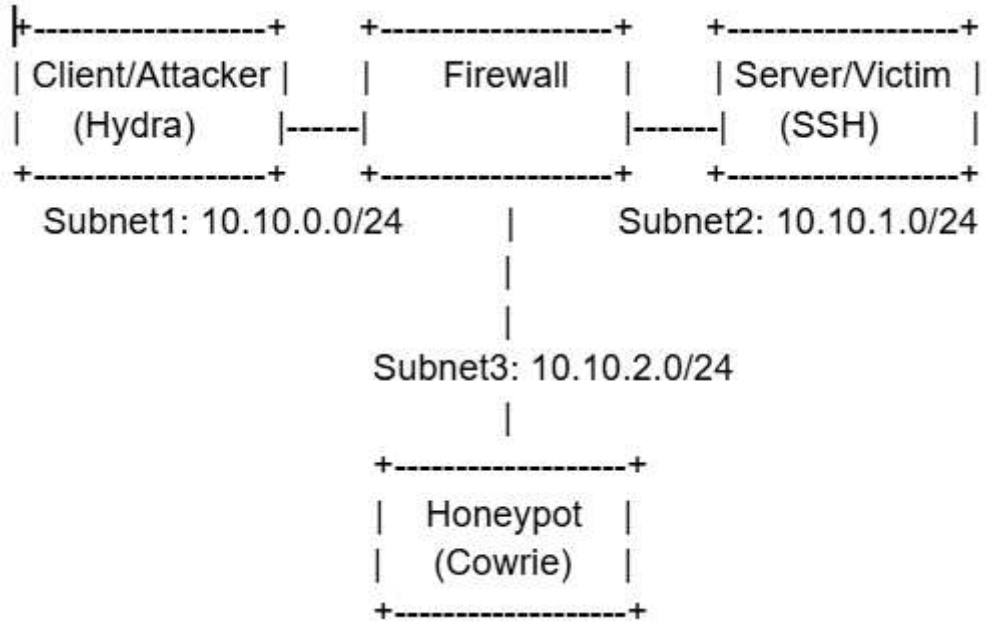
Network Security

Milestone#1 Report

Introduction/Scope

The purpose of this lab is to introduce students to brute-force ssh attacks on a server and potential blocks against it. The lab will start with students analyzing the network and rules on the firewall. Then attempting a brute-force hydra attack. Afterwards students will experiment with firewall rules to detect the brute force attacks and a system for redirecting to an outside machine. (Optional: students can analyze logs in the honeypot the firewall redirects to and see what the attacker tried to do).

Network Topology



Special Attributes

- Firewall (10.10.0.10, 10.10.1.10, 10.10.2.10):
    - only forwards ssh attempts
        - can be tested with ping to server from client and ssh from client to server to show one works and one doesn't
    - Doesn't accept any packets destined for the firewall
- Server (10.10.1.5):
    - configured for ssh (root:netsec)
    - also running services like telnet - not important for this lab since firewall only forwards ssh
- Client/Attacker (10.10.0.4):
    - no special attributes other than hydra, which is installed on startup
        - tested by running hydra command to check that it is installed
- Honeypot (10.10.2.20):
    - running cowrie - to later be setup as a full honeypot

Test Cases:

- Ping server and ping firewall to make sure no response comes back
- Test ssh root@server to ensure ssh connection over firewall is working
- Run "hydra" on client to make sure hydra is installed