Security Assessment Report

This document outlines the various attempts and methodologies employed during our security assessment of multiple machines within the target network. Despite several efforts, these attempts did not yield successful exploitation or unauthorized access.

Machine 10.10.10.10
OpenSSH 7.2p2 on Port 22: Attempted enumeration of users using a Python script. This approach did not lead to any actionable intelligence or vulnerabilities.

Dnsmasq 2.76 on Port 53: Conducted a Denial of Service (DoS) attack attempt based on the exploit detailed at Exploit Database - EDB-ID:42941. The attack did not disrupt the service as anticipated.

Machine 10.10.10.11
OpenSSH 7.2p2 on Port 22: Similar to machine 10.10.10.10, user enumeration attempts using a Python script on the OpenSSH service were unsuccessful.

Dnsmasq 2.76 on Port 53: Repeated the DoS attack attempt using the methodology from Exploit Database - EDB-ID:42941 with no success.

Machine 10.10.10.216
FTP Services on Port 21: Utilized Hydra to attempt connections using common usernames and passwords. These efforts did not result in a successful login.

SMTP Services on Port 25: Faced an issue where the connection attempts failed with the error: "Auxiliary failed: Rex::BindFailed The address is already in use or unavailable: (10.10.10.216:25)."

Machine 10.10.10.222
Apache HTTPd 2.4.38 on Port 80: Attempted to brute-force the web server using Hydra with usernames "frazer" and "warren". These brute-force attacks did not lead to any compromise.

Machine 10.10.10.223
MySQL Service on Port 3306: Tried to bypass authentication using the msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) module. The attempt to exploit the service was unsuccessful.