**Sidejacking Attack**

Completed by Eric Adamian

VirtualBox IP addresses:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Virtual machine: | ClientVM | ServerVM | AttackerVM | localhost |
| IP address: | 10.0.2.15 | 10.0.2.11 | 10.0.2.12 | 127.0.0.1 |

Explanation: Understanding the vulnerabilities of HTTP through a sidejacking attack, and the importance of HTTPS protocol; tested between a client-server interaction

**Step 1:** Open /etc/hosts file through nano; replace localhost with server VM’s IP address for www.SeedLabSQLInjection.com (server VM)

A screenshot of a cell phone

Description automatically generated

**Step 2:** Open link on Firefox browser and access www.SeedLabSQLInjection.com (client VM)

A screenshot of a computer screen

Description automatically generated

**Step 3:** Before logging in, open Wireshark through the same ethernet as the client and server to capture the TCP stream (attacker VM)

**Step 4:** Log into the website (client VM)

A screenshot of a cell phone

Description automatically generated

**Step 5:** Capture the Wireshark packets passed between the client and the server (attacker VM)

A screenshot of a social media post

Description automatically generated

**Step 6:** View the packet capture on the Wireshark; the attacker was able to successfully capture the user’s username and password (attacker VM)

A screenshot of a cell phone

Description automatically generated

**Observation:** Upon the information provided by Wireshark, **the attacker has captured the conversation between the client and server.** This shows the vulnerabilities of HTTP, and how the attacker is able to interfere with the queries that an application makes to its database. As a result, the attacker was able to view data that they could not typically retrieve.