Milestone 4: Abstract

Omkar Parkhe, Nida Safia Syed, Sri Sai Bhargav Tiruveedhula

July 3, 2019

Abstract

With the upsurge in open wireless networks at workplaces, hotels, coffee shops, etc., there is a need for a robust method to authenticate users. This is done by means of a captive portal, a web page that the user of a public-access network is obliged to view and interact with, before access is granted. However, implementing a captive portal with its default configuration makes it vulnerable to many attacks. In this paper, we perform a security analysis of a widely used captive portal, pfSense, by carrying out various attacks, proposing countermeasures and formulating the threat model. We show that it is possible for an adversary to bypass the captive portal and gain unauthorized access to the network through DNS Tunneling, MAC spoofing, Dictionary attack, XSS (Cross site scripting) and SQLI (SQL Injection). We also propose many countermeasures to mitigate the vulnerabilities in the captive portal, such as the closing of open ports, input sanitization, enabling encryption and slow hashing. It is through these experiments that we expose the vulnerabilities of the pfSense captive portal and our countermeasures demonstrate techniques that can eliminate or extensively moderate the possibility of the aforementioned attacks.