Bypassing Web-based Wireless Authentication Systems

Ahmed Hassan, Faculty Mentor Dr. Xiaowen Zhang, Department of Computer Science, CSI

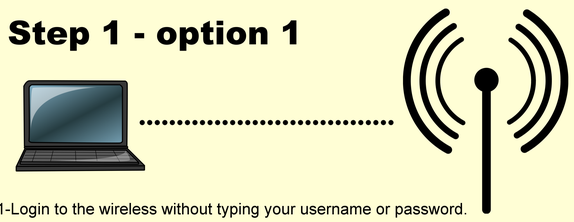
Abstract

Most college wireless networks use software systems and web-based logins to authenticate users.
In this paper we found that it is not hard to bypass such authentication.

Attacker can use DHCP request to collect information about the users on the network. It makes the attacker possible to perform unauthorized access to the network facilities. This can be done by putting the network card on monitor mode, and filter the network frames based on the collected MAC addresses.

Once any client is disconnected from the network, the attacker can spoof the client's MAC address and connect to the network. The authentication system is going to accept the spoofed MAC address and let the attacker to connect to the network.

Step 1 - option 1



1-Login to the wireless without typing your username or password.

2- Turn on your sniffer and filter it to capture all DHCP broadcast.

Step 1 - option 2

1- Put your wireless card in Monitor mode

2-Turn on your sniffer and filter the frames based on DHCP requests or wireless account points MAC addresses.

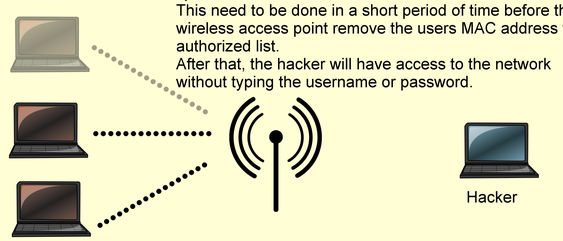
Step 2

1-Put your wireless card in monitor mode if you followed option number 1.

2-Write a script in your favorite language to filter out the MAC addresses from your sniffer captured file.

Step 3

Write another script to monitor the network based on the traffic you captured and compare it to the list you saved before. Once the script find that one of the computer did not send any traffic to the access point, the script should spoof that victim MAC address and connect to the network. This need to be done in a short period of time before the wireless access point remove the users MAC address from authorized list.
After that, the hacker will have access to the network without typing the username or password.



Securing the Wireless Networks

Based on our research, we offer the following two measures to secure campus wireless networks.
1) All users should be authenticated before they enter the network. To do that, network administrator should use strong protocols, such as WPA2 Enterprise. That will prevent non-authorized users from getting into the network. Hackers will not have any chance to do anything. If anyone tried to do similar attacks, he or she will have to authenticate via RADIUS or any similar services. That will make the users identifiable on the network.

2) All users should register their MAC addresses before they enter the network. That can be done by calling the help desk or register it through web portal.

3- Instead of using using logout button to logout from the network, network vendors should use a small browser pop up. If that pop up windows is closed, authenticate system should remove that user MAC address from authorized users list.

Conclusions

Authentication software should not leak any identifiable information. Any leaked information can be used for affecting the services. Switches should forward any network related requests to the right server. For example, DHCP requests to the DHCP server without broadcasting it to all the users on the network.

Authors:

Ahmed Hassan
Email: Ahmed@Linuxism.com
Website: http://Linuxism.com

Professor. Xiaowen Zhang
Email: Xiaowen.Zhang@csi.cuny.edu

Sponsored by

STEAM

CSI CUNY COLLEGE OF STATEN ISLAND
The City University of New York

NSF