Scintilla Session 6
Hacked!!!

14-01-20

Abstract

Session 6 was the first session of Scintilla to be held by a guest instructor. It was conducted on 14th of January 2020. The session was held at S8 EC B classroom. Staff-in-charge Vinod sir dictated the conduction of the session. **Sreekanth Sasi** of S8 was the lead instructor. As always team Scintilla and other Elacsta members endeavoured to make the event possible.

1 Objectives of the Session

The session briefly introduces attendees different methods for breaching the security of WiFi networks. It also aims on introducing some tools for the purpose. The final objective of the whole session is to make the pupils aware of the new threats they pose in a digital world and teach them ways to stay secure.

2 Participation

List of Participants

No. of First year attendees: 20
No. of Second year attendees: 12
No. of Third year attendees: 3
No. of Fourth year attendees: 0

Total No. of attendees: 39

3 Technical Details

Different types of attacks on WiFi and it's prevention were demonstrated.

3.1 Capturing handshake and brute forcing password (aircrack-ng)

aircrack-ng can crack pre-shared keys of a router. Handshaking is done when the client connects to the network. The only time you can crack the pre-shared key is if it is a dictionary word or relatively short in length. Conversely, if you want to have an unbreakable wireless network at home, use WPA/WPA2 and a 63 character password composed of random characters including special symbols.
The objective is to capture the WPA/WPA2 authentication handshake and then use aircrack-ng to crack the pre-shared key.

This can be done either actively or passively. "Actively" means you will accelerate the process by deauthenticating an existing wireless client. "Passively" means you simply wait for a wireless client to authenticate to the WPA/WPA2 network. The advantage of passive is that you don't actually need injection capability and thus the Windows version of aircrack-ng can be used.

Here are the basic steps we will be going through:

- Start the wireless interface in monitor mode on the specific AP channel.
- Start airodump-ng on AP channel with filter for bssid to collect authentication handshake.
- Use aireplay-ng to deauthenticate the wireless client.
- Run aircrack-ng to crack the pre-shared key using the authentication handshake.

3.2 Brute forcing the WPA pin

WPS stands for Wi-Fi Protected Setup and was designed to make setting a secure AP simpler for the average homeowner. An attacker within radio range can brute-force the WPS PIN for a vulnerable access point. The attacker can then obtain WEP or WPA passwords and likely gain access to the Wi-Fi network.

3.3 Physical access - unprotected web login

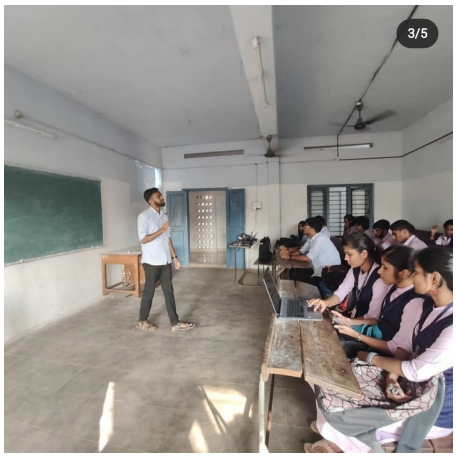
Most WiFi routers will have exposed Ethernet ports. A hacker can utilize this port to get physical connection to the network if the routers web login is unprotected. Router's default page can be accessed by entering 192.168.1.1, 127.1.1.1, 1.1.1.1, or http://localhost in browser address bar. Username and password of most routers will be 'admin', 'admin' or 'admin','12345678' respectively by default. Once successfully logged in the

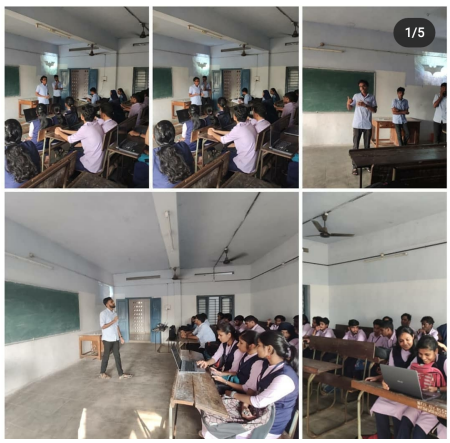
hacker gets full control over the network. So to stay secure one must change the factory password as soon as possible.

4 Prevention methods

- Strong password.
- Disable WPS pin access
- Changing company credentials

5 Gallery





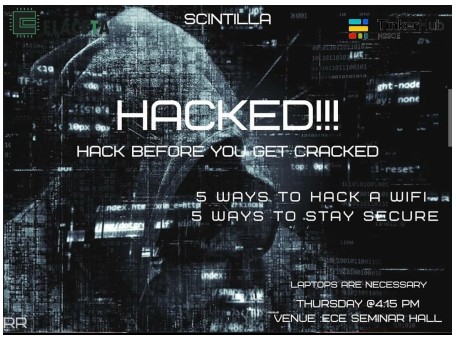


Figure 1: Poster of the session

6 Conclusions and Suggestions

The session was successful in imparting awareness in cyber security. The instructor concluded the session by emphasising the need for playing fair in the digital world. Coming panels should try to incorporate more of such guest/expert sessions into the schedule.