

Securing a Wireless LAN

Preparation

The instructor will setup an 802.11b wireless network that contains:

- a wireless-enabled host running Windows XP Professional Service Pack 2 for each student,
- a Linksys BEFW11S4, or similar, router connected to a host running Windows XP Professional Service Pack 2 and a Local Area Network
- Switches (2) are needed to create separate LAN segments or use VLAN's, so the students can demonstrate mastery of the subject.

Using the provided BEFW11S4 document, the class will practice configuring an Access Point for home and small office use.

Activity

Apply the following steps to minimally secure a WLAN.

1. Change the router's Default Service Set Identifier.
The instructor will lead a discussion for changing the wireless router's default SSID/ESSID. The instructor will demonstrate in class the process of changing the SSID/ESSID.
2. Enable WEP Encryption
The students will follow the instructions for enabling WEP encryption:
http://practicallynetworked.com/support/wireless_encrypt.htm.
3. Establish a written policy and procedure for updating WEP keys.
The instructor will lead a discussion on the reasons for periodically changing a WEP key. The students will write the procedure and place it in their notebooks.
4. Establish MAC Address-based Access Control List
The instructor will lead a discussion on the reason for using this feature. The instructor will demonstrate the process of entering each address. The students will write the procedure and place it in their notebooks.
5. Secure the Access Point
The instructor will lead a discussion on the reason for protecting the wireless router with a strong password, and periodically changing it. The instructor will demonstrate in class the process of entering a strong password for the wireless router. The students will write the procedure and place it in their notebooks. The instructor will explain such features as SNMP, and the internal logs the router uses.
6. Disallow remote administration
The instructor will lead a discussion on the reasons for not allowing remote administrative access to the wireless router. The instructor will demonstrate the process of disabling this access. The students will write the procedure and place it in their notebooks.

7. Enable NetBEUI for File and Printer Sharing

The students will follow the instructions for using NetBEUI for file and printer sharing: <http://practicallynetworked.com/sharing/netbeui.htm#HowTo>. Also see the instructions on: <http://www.ezlan.net/netbeui.html>

8. Apply secure-file sharing practices

The instructor will lead a discussion on the risks of sharing files and folders. A good resource is: <http://www.microsoft.com/windowsxp/using/security/learnmore/encryptdata.msp>. The discussion will determine what folders can be shared on each host, and which application data files need to be password protected. Students will test whether they can access designated encrypted shared folders and/or files.

9. Students will repeat this lab on their own, or in teams to demonstrate their mastery of the subject.