

Wireless Security Lab

(Due on 12/4/08)

Read <http://eupalinos.gtisc.gatech.edu/cs6262> for updates.

Introduction:

The purpose of this lab is to experiment with a wireless network and learn how to exploit its properties. In doing so, you will learn how to use a variety of new tools for surveying and sniffing wireless networks (and networks in general).

Location:

Student study-area between Klaus 3110 and 3124 GTISC labs. There, you will find strong signals for wireless network(s) for this assignment.

Note

You will need a laptop to complete this lab. However, we no longer provide public laptops for students to use since students have mistreated our equipments in the past. Please consult to Manos Antonakakis (manos@cc) if you need wireless cards.

Warning

This lab is **time consuming** depending on the hardware used. Consult first Google and then Manos if you cannot get certain devices/software to work.

Background

You are an elite hacker capable of hacking any computers and networks in the world. Recently, your client “Tech-the-Evil” has contacted you to steal a set of secret files owned by “CS6262 Network Security Inc.”. A deal is quickly made, and you have started the preliminary background research. The investigation reveals that the document(s) and kernel modules is stored in their internal Web Servers located in Klaus Building with no outside access. Using some clever social engineering, you have already bypassed the building security, and you are now in front of the target network. However, the server room is secured with lateral scan, and you unable to physically connect to the target machine....

Part I

Once you get to the site, you quickly find multiple wireless networks, including one labeled “CS6262”. Since your goal is to gain an access to the closed network located in the locked room, wireless networks are essentially the only way to reach your destination. Utilize available tools and explore possible weaknesses that can be exploited. Some networks may belong to neighbor companies while others belong to “CS6262 Network Security Inc.”. Hopefully, after some time you gather enough information to enter the target network.

Hint 1: You may find multiple suspicious networks. In which case, think about the implications for such finding.

Hint 2: You need to crack a WEP key. Find the a network that a lazy employ of the CS6262 company named John Smith have set up and try to penetrate the network.

Hint3: After you obtain the key try to eavesdrop the existing users and not get an IP from the AP.

Hint 4: Do not try to physical tamper the AP devices or change update their configurations. If you can do that you probably can break the key faster and go get a coffee instead.

Part II

Now that you are connected to the network, you will need to collect more information about the target server. (i.e. where it is, how to gain an access to it, etc) You may scan the network, keep sniffing the traffic for further analysis, or start port scanning discovered hosts. Map out the possible network topology and infer the target from gathered information. Keep in mind that you are the elite hacker, and your activities should remain as subtle as possible.

Part III

After doing your reconnaissance, you should have acquired enough information to begin exploiting the WEB traffic in the network. Provide a complete list of files (HTTP traffic) that traverse the network.

What to Turn In

Part I: (30 pts)

1. Describe relevant wireless network(s) you surveyed, then list security features implemented. (10 pts)
2. If you listed more than one wireless network in the previous question, provide possible explanations for the existence of such extra network(s). (10 pts)
3. Briefly explain how you gain the access to the network.

Part II: (35 pts)

1. Illustrate the possible network topology. (10 pts)
2. Describe the Web Server (s) features. (i.e. IP address, service running, etc) (10 pts)
3. Describe how you gain the access to the Web traffic. (15 pts)

Part III: (15 pts)

1. Report all names of the files (documents, modules or any other form of files) found in your network traces (15 pts). You don't have to submit the captured network traffic but you should be able to provided it if requested.

Part IV: (20 pts)

1. Briefly explain why WEP is (or is not) a preferred wireless security mechanism. (10pts)
2. Briefly describe the best practice in creating a secure wireless network. (10pts)

Please email a **PDF file** answering above to manos@cc
Your email should include [6262] in the subject line.

Windows Wireless Security Tools

WireShark – a free network protocol analyzer (sniffer) <http://www.wireshark.org/>
Netstumbler – site surveying utility <http://www.netstumbler.com/>

Linux Wireless Security Tools

WireShark – a free network protocol analyzer (sniffer) <http://www.wireshark.org/>
Kismet – A VERY good tool for surveying wireless networks, puts Netstumbler to shame
<http://www.kismetwireless.net/>
Airsnort – A network sniffing tool + WEP cracking. <http://airsnort.shmoo.com/>
AirDecap – A tool for decrypting WEP and WPA-PSK.
http://www.wirelessdefence.org/Contents/Aircrack_airdecap.htm
Aircrack-ng: <http://www.aircrack-ng.org>
Aircrack-ptw: <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

General Security Links You may find Useful

Security Focus – a decent source for finding vulnerabilities in different systems
<http://www.securityfocus.com>
Linux Security – a very good site for Linux security. Somewhere on that site is a list of known vulnerabilities for each distribution of Linux. <http://www.linuxsecurity.com/>
Packet Storm – a fun place to get new exploits <http://packetstorm.linuxsecurity.com/>
How to change your mac: <http://linuxhelp.blogspot.com/2005/09/how-to-change-mac-address-of-your.html>

NOTE: To break a 40-bit WEP you need as few as 30,000 data packets and 104-bit WEP with 60,000 data packet. As more IV packets you capture as faster the cracking will be. Depending on your capturing method and hardware the WEP breaking process could take from 2-25 minutes.