COMPUTER SUBJECT: NETWORK SECURITY

TYPE: GROUP WORK

IDENTIFICATION: MITM-Attacks/MICL&MOFA

COPYRIGHT: *Michael Claudius & Homayoon Fayez*

LEVEL: INTERMEDIATE

DURATION: 4 hours - 1 month

SIZE: 200 lines!!

OBJECTIVE: Various tools for sniffing, spoofing etc.

REQUIREMENTS:

COMMANDS:

IDENTIFICATION: MITM-Attacks/MC

Prolog
You have successfully finalized the IT-Security course. You will like to investigate more!.

The Mission
You are to discuss and apply different techniques to break network security.

Purpose
The purpose is to apply various tools on Windows and to understand how to a spoof, sniff etc. on the net. In order to do this we must install a tool from Cain and Abel.

Useful links

http://www.windowsecurity.com
www.oxid.it

https://www.youtube.com/watch?v=30wh6RhXb30

Assignment 1: Installation of Cain and Abel

a. Cain is using WinPcap, therefore if you have not installed it when installing Wireshark you have to install WinPcap now. You will need WinPcap version 4.1.3 from https://www.winpcap.org/install/

   Warning: *Do NOT install Win10PCap from http://www.win10pcap.org/download/*
   I and my students have tried it, and this Windows 10 version did not work together with Cain and Abel. Reason is that Cain is an old tool not upgraded to the new Win10Pcap.

b. On our local LAN or using your own LAN or hot spot download and install Cain Abel Windows NT version from http://www.oxid.it/cain.html or maybe better Windows 10 version from http://qpdownload.com/cain-and-abel or teachers homepage, which holds two versions cain20.exe (Windows 7 and lower versions) and ca-setup039...exe (Windows 10 version)
   In order to download Cain and Abel –which has features similar to a virus- one must turn-off Windows Defender.
   If there still are some problems when installing on Windows 10 and if you have other problems look at issue 2 in Problems and Hints at the end of this exercise.
   Tip: Before rushing into the tutorial, look at the tool, notice
   - List of icons in Upper symbol list
   - Upper toolbar list with Network, Sniffer etc
   - Lower toolbar with Hosts, ARP

c. Click on Network in Upper Toolbar, hopefully you see your network !

d. Click on Hosts in lower toolbar
   Click on Sniffer, then Network card in Symbol list then click in the middle of window and finally the ”+”
   You should now see a list of IP-addresses of computers/mobiles etc. on your network

e. Click on Configure
   If you Cannot see IP-addresses of your pc; that is you only see 0.0.0.0 then look at Issue 3 in "Problems and hints" at the end of this exercise. Solved it? ☺

Assignment 2: ARP Cache Poisoning

a. First chat with your "friends" soon to become "victims" (former friends) find their IP-addresses so you know who is who.
   Try to ping each other so you are sure you are on the same net.

b. Now act as a man in the middle by following the tutorial on ARP poisoning on:
   http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html
   Before poising start Wireshark
   When poisoning is stopped investigate the ARP's sent/received.

c. See if the victims (A and B) can ping each other's IP-addresses, although as all goes to you the attacker.

d. Start to poising one more time but before that, Start Wireshark and investigated the ARP's sent/received.

e. Start a simple Tcp-socket server communication program.
   Then let one victim (A) run a simple Tcp-socket client communication program using the others victim's (B) IP-address.
   Did you succeed in fooling the victim?

Assignment 3: DNS Spoofing
You are on your own !

Assignment 4: Session Hijacking

Assignment 5: SSL Hijacking Cache Spoofing

Problems and Hints

Issue 1: Missing WinCap
If you don't already have installed Wireshark with WinCap, you might not have WinPcap (WinPcap is the industry-standard tool for link-layer network access in Windows environments**).** Therefore install WinPCap and then make sure to restart your machine after installing WinPcap.

Issue 2: Cannot install/run Cain&Abel
You can download the ca-setup.exe file but installation if not finished. Observation is like the last window during installation closes and nothing happens!
The reason is that the anti-virus system is blocking for installation. Several solutions are possible:

a. Download the .exe file to an usb-stick and then install from the usb-stick.
   This will work if you are "lucky" and your anti-virus program is weak.

b. Turn off the anti-virus (Avast and McAfee is totally blocking) and especially the Windows-Defender must be turned off and then install.
   This will work and now you can run Cain&Abel.
   If you turn on Windows-Defender again you can still run Cain&Abel, but there can be some actions which will be prohibited. Thus you will have to turn off the Windows Defender again.

c. Use a virtual-bow VT-Box. That's a little hard work.
   Install an old Windows system like Windows XP on a VT-box.
   Download an image iso-file of Windows XP to USB-stick or utilize shared folders.
   Install Cain&Abel on the Windows XP using the image. Notice cain.exe properties might have to be changed to Windows XP compability.
   This actually works fine and also now you as an intruder are very well disguised!!

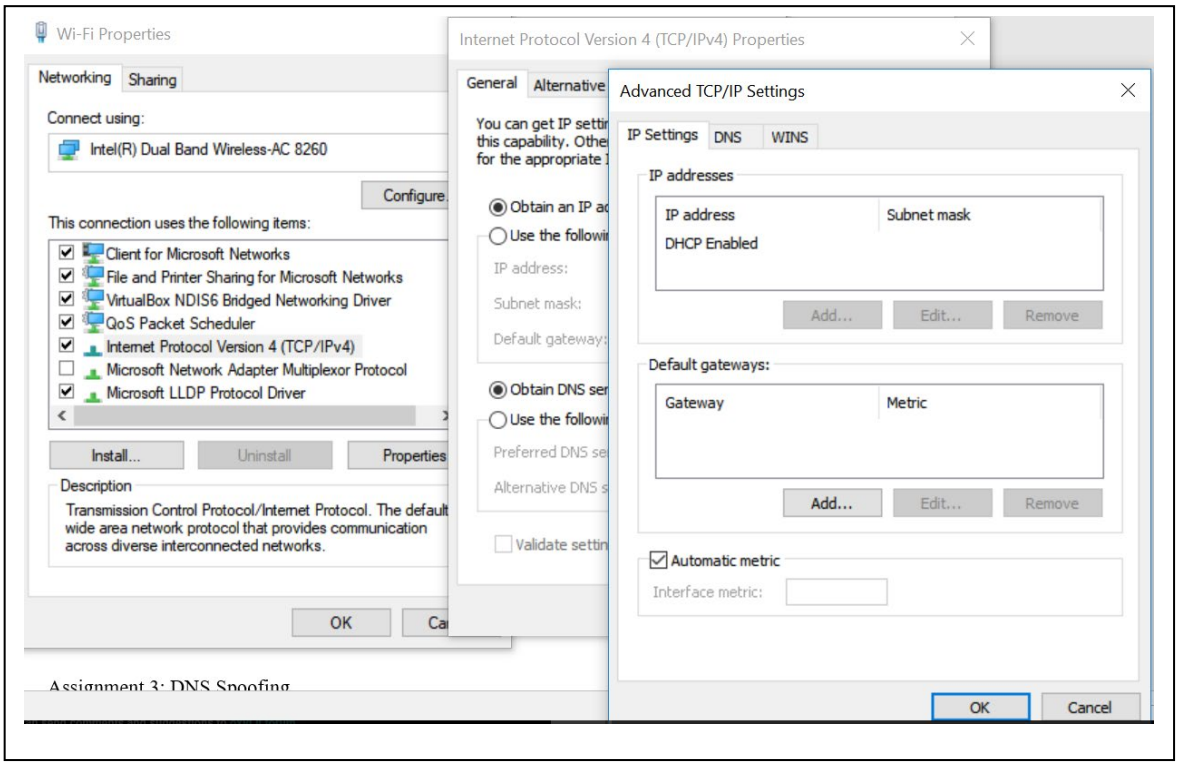
Issue3: Cannot see any IP-addresses in Cain&Abel
Two possibilities:

a. Your anti-virus is too strong.
   Solution: turn it off or remove it (I removed Avast)

b. DNS setup needs to be changed on the adapter.
   Solution: Follow the description below

Start Cain and Abel, if you cannot see an IP address in the Configure window (when you click on Configure menu). Then do the following:

1. Start Control Panel and Choose Network and Internet -> Network and Sharing center
2. Choose “Change adapter settings”
3. Right click on Wi Fi and Choose properties
4. Double click ”internet protocol version 4(TCP/Ipv4).
5. Click on Advanced settings



6. Click on DNS Tab.
7. Tick the ”Use this connection´s DNS suffix in DNS registration” check box