RADICL Lab 1
Network Discovery, Attack and Network Traffic Forensics

Learning Objectives: Differentiate between types of traffic, use a network discovery tool to locate machines, services, and vulnerabilities on a network, and learn how an attacker uses an attack script to access a machine.

Scenario: You are the attacker in this scenario. You've been hired by E-Corp, an ecommerce company, to hack into and deface Big-Corp's (an E-Corp competitor) website. You will use a network discovery tool to find a vulnerable web-server on the network. Then use a web-browser to browse the website and secure e-commerce of the site to make sure that it is the company you are targeting. Finally, execute the attack script to gain access to the machine and use the vi editor to edit the webpage.

Deliverables: Write a 2 page report for E-Corp (your employer) describing your activities and the results of your activities. The report should be written in a way so that E-Corp can do this again in the future. Include in your report: your motivation, the tools you used, a description of your actions, the results of your actions, and a description of the various types of network traffic (e.g. web traffic, SSH traffic, attack traffic, etc.) that you analyzed (with specific traits of each type of traffic). Make sure to include a paragraph on the ethical and legal concerns of these activities in a non-lab environment.
-> You will also be expected to keep notes during the lab regarding interesting IP addresses, command line arguments that were helpful, etc. These will also be included with the report (but do not necessarily have to be formally typed up as opposed to the formal report). OPTIONAL: Look through the exploit source code for where the exploit actually takes place, and some other additional characteristics of this exploit. Include your findings in the report.

Tools To Be Used:

- Gentoo: A Linux distribution
- nmap: A network discovery, service discovery and vulnerability discovery tool
- Firefox: A web browser
- vi or pico: A text editor
- Ethereal: A network traffic sniffer (with graphical interface)
- A buffer-overflow attack script

Directions:

You will not be able to print, email, or otherwise transport data out of the RADICL lab, so it is imperative that you take the notes necessary to compose the report.

You will be using Gentoo, a Linux distribution during this lab that has been installed with a graphical manager called Fluxbox. The distribution has been bundled with a number of security tools that you are free to explore during this lab. Right click on the screen to bring up a menu and select your tool. Some tools, however, will only be available in the command line (xterm selection on the fluxbox interface).

If your workstation has not been logged into, login to your workstation using the username ‘root’ and password ‘password’.

Start by doing some network discovery, see what’s out there and what it is running. Do this by using nmap (on the command line). Use nmap to scan our local RADICL network: 1.1.1.[0-100]. (Use ‘nmap –h’ to find necessary commands) Find the Linux box running Samba and an HTTP and HTTPS service.

Once you have collected some information (IP addresses, interesting services, OSes running, etc.) it is time to get down to business. First you should know something about your box (like your IP address), get this information by using ‘ifconfig eth0’ on the command line.

Then start up Ethereal to start collecting network packet information for future analysis.

- Use fluxbox to select Ethereal
    - Go to Capture->Start in the Ethereal menu
    - Make sure eth0 is selected, and uncheck the promiscuous box
    - Click start
    - Run this window in the background for the next steps

Open up Firefox using fluxbox. Browse (http://<IPADDRESS>) to the IP address that you already know is running an HTTP server. Click on the link that is available. Now download the script that is available on the website.

- Make a directory called ‘exploits’ in the root partition using the command line
    - mkdir /root/exploits
- Right click on the link to the file -> save to /root/exploits

Now go into the exploits directory, ‘cd /root/exploits’ and compile the attack script by running the gcc compiler: ‘gcc sambal.c –o sambal’

Now, go ahead and run the attack script. You can do this on the command line: ‘./sambal’. It will show you the correct usage of the script. You should already have the necessary information compiled from the previous steps to successfully run the script.

For the next stage, your group number will have been assigned to you, and your group name you can make up. Please make sure that your group name contains NO SPACES, and is relatively unique for the class.

The script, when successful will return you a root shell (primitive shell) to the server. When a shell is returned, you should be able to ‘cd /’ and ‘ls’ the root directory. Now, add a user to the system by executing the command **(BE VERY CAREFUL WITH THIS COMMAND)**: echo ‘<GROUP NAME>::0:0::/root:/bin/bash’ >> /etc/passwd
Now type the command ‘passwd <GROUP NAME>’ and give your new user a password.

Type ‘exit’ to get out of the script. Now use ssh to get back into the server by typing ‘ssh <GROUP NAME>@<IP ADDRESS>’. It will ask you for your password, which you provided before. You will now have access to the server and all of the editors for the next step.

Now deface the website (of your group) by going to the WWW directory, ‘cd /var/www/html/group<GROUP NUMBER>’. Use either vi or pico to edit the index.html file and insert the text: “U R HAXORD BY l337 <YOUR FIRST NAMES> <GROUP NUMBER>”. Test that your defacement has been successful by using Firefox, browse to (http://<IP ADDRESS>/group<GROUP NUMBER>/).

Open up the Ethereal window now, and click on the stop button to stop Ethereal from collecting packets. Use the Ethereal windows to examine the network traffic that you have collected. Identify several events in the traffic (e.g. the unencrypted from encrypted HTTP (and SSH) traffic, your execution of the exploits, etc.) Make sure you note what differentiates these events apart in the network traffic and how you were able to tell.

You are now finished with the lab. Close the connection to the hacked server by typing ‘exit’ in the remote shell window and then close all windows and logout of the machine.