Helsinki University of Technology
Department of Electrical and Communications Engineering
Networking Laboratory
S-38.133 - Networking Technology, Laboratory Course
Spring 2007

Work number 36: Network Security

Preliminary exercises, laboratory assignment and questions for final report

Jan Tapper
22.11.2004
Revised June 2005 and January 2007 by
Anni Matinlauri

Preliminary Report

Answer the following questions shortly. Finnish students use Finnish, others answer in English. Basic knowledge of network security is recommended and experience using Linux helps. The preliminary report must be returned at least three days before the committed lab time. Make sure that you have read iptables manual pages or any iptables howtos before entering the lab. You should also have read the assignment carefully through before you begin to solve tasks in the laboratory. Assistant can give you some advice but the intention is that you look for answers to the questions yourself.

PQ1: What is a firewall?

PQ2: How do hackers crack into computer systems?

PQ3: Is it legal in Finland to make port scans on computers or in networks owned by others than you? Mention your source of information.

PQ4: What crime does one commit when making a port scan against, say a firewall of a bank? What can be the sentence if found guilty for such a crime?

PQ5: Describe a good password. Give an example.

PQ6: Create an iptables firewall script to prevent connections to any other ports than ssh and ftp. Outgoing traffic is not filtered and the firewall must also pass all related and established connections. Include your firewall script in your report. Explain it. **Also, take this script with you to the lab, you will need it there.**

Laboratory Assignment

In this laboratory work security of IP networking is taken to a closer inspection. It is strictly prohibited to use these tools on any computer outside the lab without permission of the computer owners. The questions marked with * are the ones that you can do at home using the data gathered.

The assistant will show you the equipment which will be used and give you all needed passwords. The instructions do not include all required information so it’s good idea to look for some information about the subject before your lab turn.

In your final report answer to the questions marked with Qx and Fx marks. Answer shortly. You must do some notes in the laboratory and save data to make it possible to answer questions at home.

Network Scanners

First login as *labra* to **bravo**, assistant will provide the password needed. Open a shell window. You can also take a remote ssh connection to bravo if you are not able to take a console session.

Q1: Use nmap to find a Linux host with ftp and ssh services running on 10.38.224.0/24 network. What is the command for this and how does it perform the scan?

Q2: Try a different method of scanning. Perform a TCP SYN scan. Assistant will give you help if needed. What was the command used?

Q3: Then try a Stealth FIN scan with operating system guessing. What was the command used?

***Q4:** What is the difference between these three scans? Why was the result in stealth FIN scan so different from others?

Q5: What is the IP for the Linux box with ftp service running? Its name, *zappa*, has not been added to the name service.

Q6: Use nessus to scan ports on zappa. What services does nessus think that would be better to be invisible to the network? Why?

Nessus server must be started in bravo in order to do scanning. The server can be started by the command *nessusd –D*. Starting takes some time. When the server is running connect to it by a client. If you are on bravo give the command *nessus* and if you are on a Windows PC open nessus client by double clicking its icon.

Q7: What was the most vulnerable service found? What are the vulnerabilities it suffers from?

***Q8:** How would you shorten the security warning / note list?

Firewall

Connect now to zappa. Its root password is eeeeee.

In the preliminary report you created an Iptables firewall script. Input it now to zappa and run nessus against zappa again. Show the assistant that you succeeded creating the iptables rules correctly.

***Q9:** What other functions can firewalls perform besides basic packet filtering?

Root Exploits and Root Kits

Q10: In */home/security-lab/* directory on bravo there is an exploit for the vulnerable service you found on previous questions. Capture all traffic between bravo and zappa with Ethereal and run the exploit to gain remote root access to zappa. What was the command for the exploit?

***Q11**: Analyse your capture. What was the exploit based on?

Password Cracking

Q12: Find the file that keeps passwords for every user on zappa and get it to bravo. Use John the ripper to find out password for *boss* user id of zappa. You can use a ready made wordlist "passwdlist" found from /home/security-lab. What is the password? What was the command? How did the password cracking happen?

Web server security

Q13: In Bravo there is a program by the name Nikto which is used to scan for web server vulnerabilities. Use it to scan Ohmi (10.38.0.5). What does the scan reveal?

***Q14:** If you are maintaining a web server what should you do to keep your server as secure as possible?

Keyloggers

Q15: Currently there are numerous keylogger programs and hardware available. Most of them are for Windows OS and their sophistication level varies greatly from total stealth to regular visibility. One such program is running on PC5. Try to find the log that it keeps. Where was it?

***Q16:** How would you protect yourself from keyloggers?

Intrusion Detection

***Q17:** What is Snort?

Q18: Use the root password to establish a ssh connection to zappa. See any log lines from /var/log and its subdirectories that indicate intrusion attempt has been targeted to zappa. From which files you find evidence of hackers, if any evidence can be found at all? Be sure to include some evidence of your findings to your final report.

Q19: See if you can find tcpdump files created by Snort. Use scp to copy them to your workstation. Use ethereal to see what actually happened during the exploitation. (If you cannot see clearly try to find information about this exploit from the Internet) What did the exploit do? Explain every phase. What was the shell code (in plaintext) it executed?

Q20: How could the service be protected from this exploit?

Q21: Run rkhunter (/usr/local/bin/rkhunter) on zappa. What information do you get from it?

Questions for Final Report

FQ1: Why are passwords stored in shadow, not in passwd?

FQ2: Describe how you can gain access to a company's network using social engineering. (One good scenario is enough.)

FQ3: Describe IDS. What is the difference between IDS and firewall?

FQ4: What is a honey pot? Why are they used?

FQ5: How would you implement a honey pot?