Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inform. Ralph Holz

Exercises for lecture „Netzsicherheit“
Assignment 5, WS10/11

Hand-out:	Thursday 20th January 2011
Deadline:	Thursday 27th February 2011
Exercise course:	Wednesday 2nd February 2011

This will be the last assignment for this semester. Thus, we will give you a little potpourri of interesting security-related questions. We hope you have enjoyed your exercises and your time with us and profited from both. Good luck for your exams and in your further studies!
PS: If you want to do a graduation thesis with us - just ask or write an e-mail. We often have openings.

Task 1: Firewalls

You are administrating the network of a small company. Your predecessor was not familiar with packet filters and has built a strange set of firewall rules. This is the network topology:

```
+----------------------+                    +----------+
|                      |                    |          |
|    192.168.1.0/24    |-------------->eth0+ firewall +eth2->131.159.1.254 -> (Internet)
|                      |      192.168.1.254|          |
+----------------------+                    +-----+----+
                                               eth1(131.159.2.254)
                                                 |
                                                 |
                                                 v
                                        +-------------------+
                                        |  DMZ: 131.159.2.1 |
                                        |       131.159.2.2 |
                                        +-------------------+
```

The firewall is a Linux PC with three network cards. The Linux packet filter „netfilter“ was configured as follows:

```
iptables -P OUTPUT DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP

iptables -A FORWARD -i eth0 -s 192.168.1.0/24 -j ACCEPT
iptables -t nat -A POSTROUTING -i eth0 -s 192.168.1.0/24 -j MASQUERADE

iptables -A FORWARD -o eth2 -d 131.159.1.1 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -o eth2 -d 131.159.1.2 -p tcp --dport 25 -j ACCEPT
```

Use the documentation for iptables (it’s on the Web) to answer the following questions.

a) Is a PC from the subnetwork 192.168.1.0/24 allowed to send packets to the Internet? Is the PC allowed to access services in the DMZ?

b) The IP addresses of eth1 and eth2 are static, i.e. the network is not connected to the Internet with a dial-up moden. Thus, the IP addresses do not change. What other method than MASQUERADE can then be used to implement the NAT? Why is that other method better in this particular case?

c) Now assume that you want to establish a connection from your PC in the private subnet to a PC on the Internet. Can the reply of the computer you contact travel through the firewall?

d) Is it possible to administrate the firewall via SSH? Does it work from the Internet? From the DMZ? From the private subnet?

Task 2: SSH Weaknesses and TOFU: Trust on First Use

The Secure Shell (SSH) is a tool that can be used to both login to remote computers as well as to secure connections to them. `openssh` is a well-known implementation. Answer the following questions:

a) It is possible to use `openssh` as a SOCKS proxy to establish an SSH tunnel to protect your traffic. Explain how this works. Then give the `openssh` command line for `openssh` to show how you would do it in practice.

b) The tool `tsocks` can be very useful to allow you to direct any kind of traffic through your SSH tunnel. How does this work? A brief explanation is sufficient.

c) SSH uses algorithms for encryption and authentication that can be assumed secure. However, so-called Timing attacks are still possible. One reason is that SSH, just like Telnet, sends one packet for each character that is typed at the console (in Interactive mode).

   1. How can attackers use this to gain security-relevant information when they monitor a SSH session? (Note: feel free to speculate here and produce ideas)
   2. In December 2009, the LRZ found out that a large number of "typing error domains", e.g. `machine.lrz-munchen.de` (!), had been registered by unknown persons. All subdomains of these “typo domains” were running SSH daemons. The daemons accepted the user’s input and then refused the login.
      a. What could the potential goal of such an attack be?
      b. How can a user detect the fraud when the user has **been logged in to an LRZ computer with SSH before**?
      c. Why does this fail when the user **has not yet been logged in on an LRZ machine**?

Task 3: Denial-of-Service Attacks Revisited

Please answer the following questions. Justify your answer.

a) What is the difference between a normal DoS attack and a Reflected DoS attack?
   a. How does the latter work?
   b. Explain: how can you use IP spoofing and ICMP to conduct a Reflected DoS attack?

b) In brief words, what is the principle of a botnet?

c) What role can botnets play in DoS attacks? Give an example. Use `shadowserver.org`, if you want to find up-to-date examples (nice site, have a look).

d) What is a port scan?
   a. Have a look at the `nmap` tool (`man nmap`). What can you do as an attacker to hide a port scan?
   b. If you want to find out which operating system a computer is using, which `nmap` command would you use? (This is called OS fingerprinting)
   c. What is the principle of OS fingerprinting?

Task 4: DNSSEC

In the following, we will discuss the security of the Domain Name System (DNS) and its successor, DNSSEC. Use `www.dnssec.net` and RFC 4033 to answer the questions about DNSSEC.

a) What is the purpose of DNS?

b) How is normal DNS protected?

c) There is an attack called DNS Poisoning. What is the principle?

It is commonly agreed that DNSSEC must be introduced. We are currently seeing a first major roll-out.

d) Explain the key ideas of DNSSEC (the principles only, no need to go into details like Resource Records etc.).

e) What kind of security does DNSSEC provide (which security primitives)? Does it provide confidentiality?

f) Some people propose to add a host’s public key into its DNSSEC entry, too. What is the motivation for this?