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

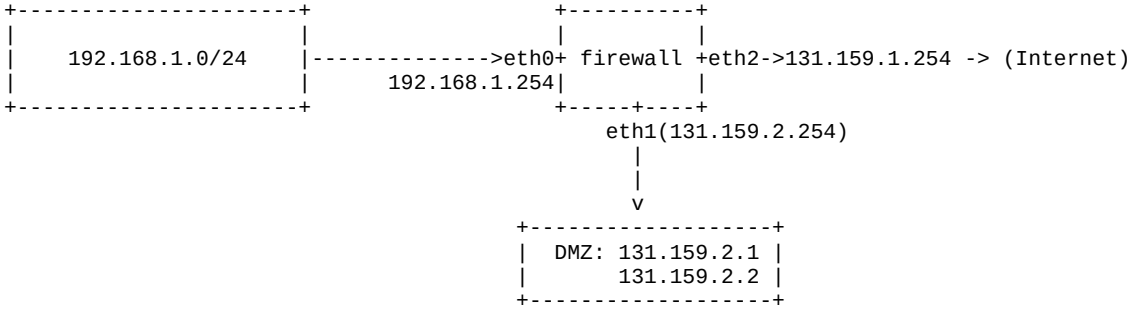
Dipl.-Inform. Heiko Niedermayer
Dipl.-Inform. Ralph Holz
Dipl.-Inform. Lothar Braun

Exercises for lecture „Netzsicherheit“
Assignment 6, WS09/10

Hand-out:	Wednesday 20th January 2010
Deadline:	Thursday 4th February 2010
Exercise course:	Thursday 11th February 2010

Task 1: Firewalls

You are administering the network of a small company. Your predecessor was not very skilled with packet filters and built a strange set of firewall rules. The picture below shows the network topology:



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 FOWARD 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
```

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 the other method better in that case?
c) Now assume that you want to establish a connection from you PC in the private subnet to a PC on the Internet. Can the reply of the computer you contact travel through firewall?
d) Is it possible to administer the firewall via SSH? Does it work from the Internet? The DMZ? The private subnet?

Task 2: Intrusion Detection

The signature-based detection system "Snort" (www.snort.org) operates as network sniffer and analyses the entire traffic that is seen by the network card.

a) Where in the network should an administrator run Snort?

b) What does it mean that a network card is in "promiscuous mode"? Why is this important for Snort?

The configuration data of Snort contains configuration for the various subsystems of Snort, as well as rules for Snort that define how Snort analyzes the traffic.

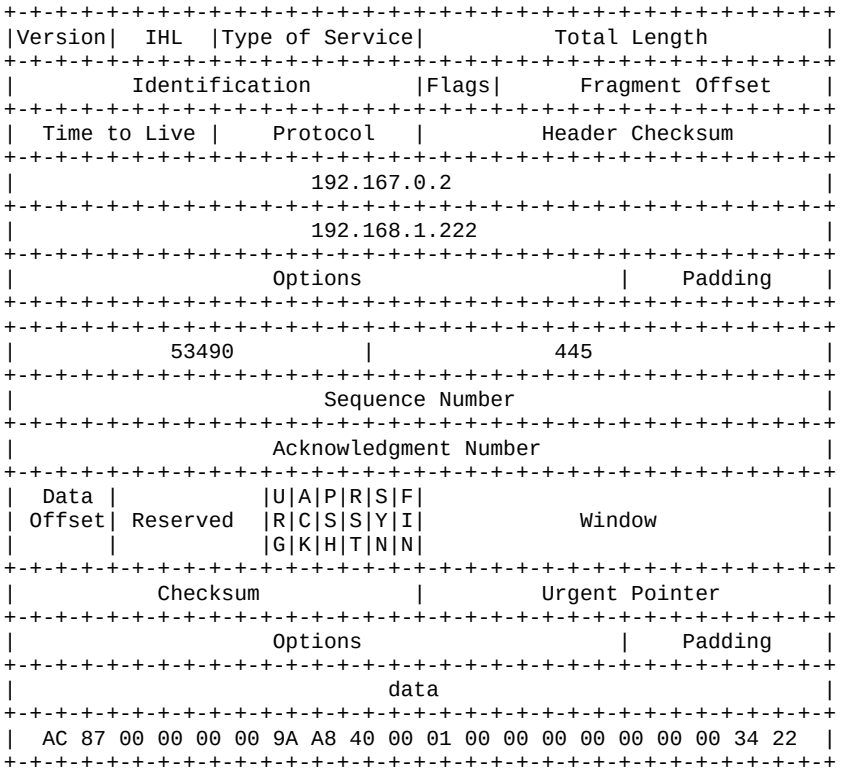
c) Explain the fields of the following rule.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 \
(msg:"ET EXPLOIT MS04011 Lsasrv.dll RPC exploit (Win2k)"; \
content:"|00 00 00 00 9A A8 40 00 01 00 00 00 00 00 00 00|"; classtype: misc-activity; \
reference:url,doc.emergingthreats.net/bin/view/Main/2000046; sid: 2000046; rev:8;)
```

d) Now you try to add a second rather similar rule to the rule database. It follows after the question about. Why is Snort going to ignore this rule?

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 \
(msg:"ET EXPLOIT MS04011 Lsasrv.dll RPC exploit (WinXP)"; \
content:"|95 14 40 00 03 00 00 00 7C 70 40 00 01|"; classtype: misc-activity; \
reference:url,doc.emergingthreats.net/bin/view/Main/2000033; sid: 2000046; rev:8;)
```

The rule database may not consist of only the first of the two rules. The variable $HOME_NET is set to 192.168.1.0/24. The variable $EXTERNAL_NET is set to !$HOME_NET. Now, Snort observes the following network packet (we skip layer 2 here). All fields that are not specified are correctly set:



e) Does Snort show an alert when it sees this packet? What can an attacker do to prevent being detected? Assume that Stream5 or similar Snort preprocessors are turned off.

--- turn page ---

Task 3: Attacks

Please answer the following questions. Justify your answer.

a) Are Flash Crowds a Denial-of-Service attack?
b) What is attacked by a TCP SYN-Flood attack (http://tools.ietf.org/html/rfc4987)?
c) What is a port scan and what could you do to detect such a scan?
d) Now, what could you do as attacker to hide your port scan?

Task 4: Programming with SSL

Use a programming language of your choice, say Java, Python, ... In this task you should try to establish an SSL connection using a library in the programming language. In most cases you can find code for doing this on the Internet that you can use as basis. Document the practical parts by showing suitable fragments of the code and give a short report about your experience.

a) Give a short overview over the classes and methods that you can use in your programming language and its corresponding library to create and use an SSL connection.
b) The first practical step is to create the key and the certificate. Remarks: You may need to create a keystore or resolve this in your code. For keys and keystores Java as example offers the tool “keytool” to create keys and certificates. Please note that the server always needs a way to access its private key, while the client needs access to a truststore with the certificate of the server (or its CA). In Java you could use the same store for this demo purpose.
c) With this prequisit, you can now establish a connection between client and server with the primitives offered by the library. Let client and server send short text messages (e.g. input from the console). Hint: Since socket function calls are often blocking, it may be necessary to consider using multiple threads. This depends on your language and its socket and stream processing libraries.
d) Use Wireshark or a similar network sniffer to check your SSL connection. Does it recognize the SSL?