Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Dr. Heiko Niedermayer
Dipl.-Inform. Ralph Holz
Cornelius Diekmann, M.Sc.

Network Security WS13/14
Assignment 4 – v1.0

Submission by **Wed, 22 January 2014, 23:00 UTC (24:00 CET)**.

Important directions:

- **Attention:** For questions regarding Tasks 1 and 2, contact diekmann@net.in.tum.de. For questions regarding Tasks 3 and 4, contact holz@net.in.tum.de.
- Submit by SVN. **Always** indicate your team: place a file `team.exercise04.txt` in **both** user directories under `exercise04/`. E.g. in `s_gu27jaf/exercise04/` **and** in `s_guab38/exercise04/`.
- **Always** show how you arrived at your answer to get full credits. I.e. show the computation, refer to the output, the man page, the RFC, etc. – whatever it takes to make your answer understandable.
- Be sure you do not violate our plagiarism guidelines
- Submit solutions for T-credits and P-credits in a **PDF**.

Task 1 Terminology (2 T-Credits)

a) **(1 T-Credit)** What are the three security components as defined in the lecture 'Security Policies and Firewalls'?

b) **(1 T-Credit)** Consider the following statement by the Pointy-Haired Boss: "We need to protect our corporate secrets. Therefore, all outgoing connections to Facebook are blocked by our firewall!" Match the previous statement to the security components.

Task 2 Generic Firewall Configuration Mistakes (4 T-Credits)

Below, in Table 1, you see a firewall configuration for the network topology of Figure 1. Independently of the security policy, the firewall configuration is flawed. Find four mistakes that lead to behaviour that is probably undesired.
(Note that this task is not related in any way to the security policy you are going to apply in the next task)

Rule	Direction	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	Zone 1 → *	*	*	TCP	*	*	New	Permit
B	* → *	Zone 2	Zone 1	*	*	*	New	Permit
C	Zone 1 → *	*	*	TCP	*	22	New	Drop
D	* → *	*	*	*	*	*	Est	Permit

Table 1: Flawed firewall rules.

Task 3 Firewalls (6 T-Credits)

We will practice firewall configuration in this task. You want to configure a firewall for your home network because you have learned how to do that at university. Figure 1 shows the configuration you want to achieve. In Zone 2, you've got one Web server (`131.159.20.1`) on TCP ports 80 and 443, and one mail server (`131.159.20.2`) on TCP port 25. Your home users reside in Zone 1.
Your security policy is as follows:

1. Your home users may freely access any Web service, anywhere, on ports 80 and 443, but only if they initiate the connection themselves (i.e. they are allowed to browse the Web). Noone outside Zone 1 can initiate connections to Zone 1, on any port.

2. Everyone, including the Evil Internet, can access Web (both ports) and mail in Zone 2. However, no host in Zone 2 can initiate connections anywhere else.

3. Home users can access the Web servers and mail servers in Zone 2 via SSH, too. They can also use SSH to hosts on the Evil Internet. However, hosts in Zone 2 can only be contacted on port 22 by hosts in Zone 1.

You can use zone names instead of IP ranges. Use 'Ext' if you want to refer to the Evil Internet, 'Zone 1' if you want to refer to Zone 1 etc. Use `*` to indicate 'all'. If you want to indicate directions, note it in the style of 'Zone 1 → Zone2'

a) **(3 T-Credits)** Draw and complete a table to define a statefull firewall configuration for the given scenario (as we did in the lecture). 1 T-Credit for each of the above policies.

b) **(3 T-Credits)** Based on the above, do the same again to define a stateless firewall configuration. 1 T-Credit for each of the above policies.

Rule	Direction	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action

Table 2: Template for stateful filtering.

Rule	Direction	Src IP	Dst IP	Protocol	Src Port	Dst Port	ACK	Action

Table 3: Template for stateless filtering.

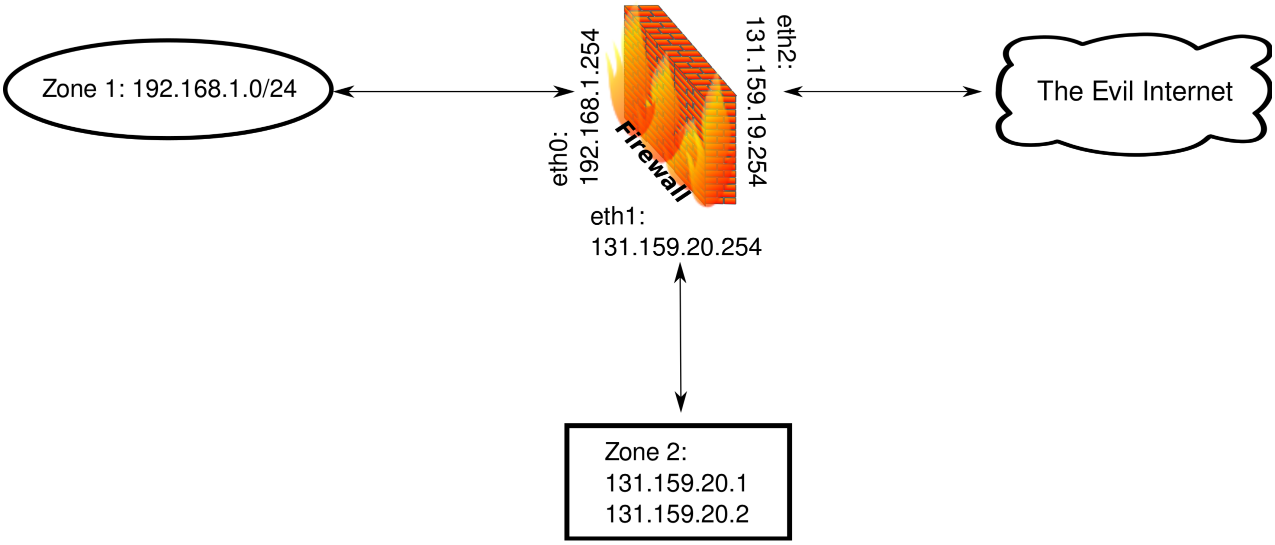

Figure 1: The network topology, with a firewall in the middle.

Task 4 Port scanning (6 P-Credits)

The goal of this Task is to acquaint you with port scanning techniques. First, install nmap using *sudo apt-get install nmap*. Second, read the man page for nmap and refer to http://nmap.org. Then answer the following questions.

a) **(1 P-Credit)** What do the following nmap results with respect to port status indicate, i.e. what results does nmap get on *packet level*? You don't need to write much, but be precise and complete.

- 'open'
- 'closed'
- 'filtered'

b) **(1 P-Credit)** What is the difference between a TCP SYN scan and a TCP Connect scan? Explain by indicating which packets are sent, with which TCP flags set. You can use header diagrams, if you find it convenient.

c) **(2 P-Credits)** What is the basic idea of the so-called idle scan? Draw a diagram for the case of a filtered port on the destination host. Be sure to make your explanation complete. State one advantage and one disadvantage of this scan type.

d) **(1 P-Credit)** Carry out an idle scan with idle host `svm060.i1.as.net.in.tum.de` on TCP port 23. The host to be scanned is `olbia.net.in.tum.de` on TCP port 113. Use the `nmap` options `-v` and `--packet-trace`, too. Give the command line. Why does the scan not work?

e) **(1 P-Credit)** Finally, carry out a TCP SYN scan. The machine to be scanned is olbia.net.in.tum.de on TCP port ranges 42000-43000. Give the command line you used. Find out what service is running on the open port. Explain how you found out (there is more than one way).