LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

Cryptography and Security
http://lasecwww.epfl.ch/cs2007/

Cryptography and Security

2006 – 2007

Survey n° 4

5

Name:

Important Note:

Remember that there is only *one* correct answer to each question and that each *incorrect* answer looses you some points. It is preferable not to answer than to answer at random!

1. Which of the following IP addresses is reserved for internal networks?

+

□ 128.178.73.88 □ 192.192.190.15 ☒ 10.178.25.77 □ 216.163.137.3

2. Imagine you want to install a web server on a computer behind a stateful firewall/router doing NAT. Which of these will work?

+

□ Dynamic NAT. ☒ Static NAT. □ Both will work. □ None will work.

3. Which of these attacks can be blocked by a stateful firewall but not by a stateless firewall?

+

□ Trojan Horse invasion. □ SQL injection.
□ Smurf. ☒ syn flooding.

4. When doing dynamic NAT with a single external IP address, the firewall/router might have to handle collisions in its translation table. In which of these cases could such collisions happen?

+

☒ Two internal machines use the same local port to connect to the same web server.
□ Two external machines connect to the same port of the firewall/router.
□ An internal machine opens two connection to a single external FTP server.
□ An external machine connects to the same port of two internal machines.

5. Tick the *false* assertion about (properly configured) demilitarized zones.

—

□ A DMZ is not directly connected to the internet.✓
☒ A machine in a DMZ can be used as a proxy.
☒ Machines in two distinct DMZ cannot exchange packets.
□ A DMZ is not directly connected to the internal network. ✓

6. Tick the *false* assertion about the filtering rules of a stateless firewall.

+

□ The rule order is important.✓
□ The syn and ack flags should be taken into account in the rules.
□ The last rule should always be a deny from all. ✓
☒ A syn packets should always be allowed.

7. Tick the *false* assertion. A HTTPS proxy...

+

☒ ...allows to do content filtering. □ ...can be used as a general proxy.
□ ...is similar to a SOCKS proxy. □ ...cannot decrypt the packets it relays.

8. The main advantage of a transparent HTTP proxy (as compared to a standard HTTP proxy) is that:

+

□ it relays UDP packets. □ it offers better virus protection.
☒ users have nothing to configure. □ it can relay HTTPS requests.

9. You are given the following stateful firewall filtering rules (you are in a situation with three distinct zones: internal, internet and web-dmz). Which rule is *never* used?

+

	src	port	dst	port	protocol	action
rule 1	any	any	web-dmz	80	tcp	permit
rule 2	any	any	internal	any	any	deny
rule 3	web-dmz	any	internal	25	tcp	permit
rule 4	any	any	any	any	any	deny,log

□ rule 1 □ rule 2 ☒ rule 3 □ rule 4

10. By which acronym should one designate a tool which analyzes the traffic around a firewall and applies the necessary coutermeasures when an attack attempt is detected?

+

☒ IPS □ DMZ □ IDS □ DNS