

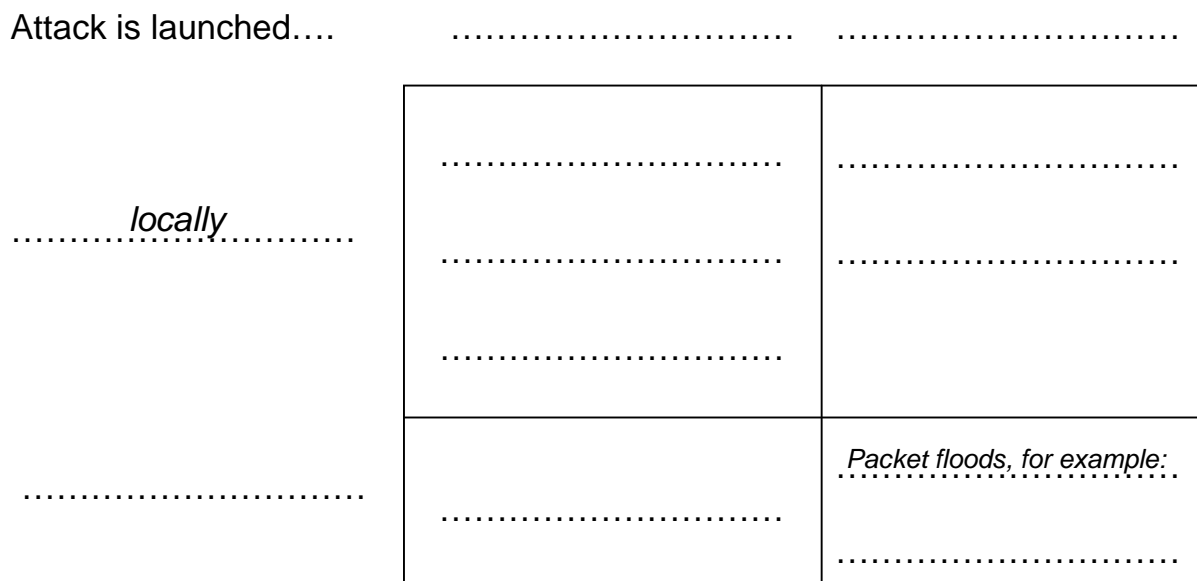
Gruppe A

ISEC (IFS/Weippl) Prüfung Jan 06

(1) Stack-Based Buffer Overflow Attacks: (5pt)

- a) What does a stack “do”? (1pt)
- b) What is the security problem? (1pt)
- c) What could an attacker do? (3pt)

(2) Fill in the missing lines in the drawing about kinds of DOS-attacks! (10pt)



(3) ARP (8pt)

- a) What does ARP mean? What is it for? (1pt)
- b) On which layer does it operate? (1pt)
- c) Which are the two modes of operation? (2pt)
- d) What is insecure about ARP – which attacks are possible? (2pt)
- e) How can you make it harder to launch attacks on ARP? (2pt)

(4) HTTP

- a) What are the two authentication types? Explain them! (4pt)
- b) HTTPS: What is it? What are its characteristics? (2pt)
- c) What is HTTP request smuggling? (2pt)
- d) Explain two possible attack scenarios with HTTP request smuggling! (4pt)

(5) IPSEC (6pt)

- a) Which are the three main parts of IPSEC? (3pt)
- b) Which are the two operation modes? (2pt)
- c) Fill in the word “mandatory” or “optional”: (1pt)
 - IPSEC ispart for IPv6
 - IPSEC is for IPv4

(6) Firewalls (9pt)

- a) What are the two main types of rule sets? Explain them! (2pt)
- b) Explain “stateful inspection” (3pt)

- c) Explain Application Layer Firewalls! (2pt)
- d) Name 4 advantages of personal firewalls over dedicated firewalls! (2pt)