Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

Cryptography and Network Security
Tutorial 4
FIREWALL, VPN, IDS

Nhat Nam Nguyen
nhatnamcse@gmail.com

11/4/2015

Exercise 1. (3pts) Firewall

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.

a) Describe at least three different firewall functions?

b) What is DMZ?

c) Firewalls work at what layer? Define firewall generations and their roles.

Exercise 2. (3pts) Virtual Private Network

A VPN solutions is, loosely defined, a secure connection between a client machine/network and a server (gateway) in another network designed such that applications in the client do not have to be aware of the presence of the VPN (their code is not affected by it).

a) Explain why TLS cannot directly be used for a VPN?

b) Describe a way to design a system for a secure VPN connection that uses TLS.

c) Explain briefly why IPsec has not the same problem as TLS. Also indicate what is additionally needed in a IPsec based VPN.

Exercise 3. (4pts) Intrusion Detection System

a) What are a network intrusion detection system (NIDS) and host intrusion detection system (HIDS)?

b) How are intrusions detected?

c) What is an advantage of anomaly detection?

d) How does a NIDS match signatures with incoming traffic?

THE END