Département Réseaux & Télécommunications
Licence professionnelle / Professional Bachelor 2016/2017

Infrastructure Security (M33)

N.B. : No calculators may be used. No document can be used
Indicative marking: *1 : 5 pts - 2 : 5 pts - 3 : 6 pts - 4 : 4 pts*

FAMILY NAME : _____
FIRST NAME : _____

Ex 1 : Risk analysis

In the field of risk analysis, with a "networks and information systems" view, security can be considered in four main areas:
- Physical security
- Exploitation (Operational) security
- Logical Security
- Application Security

Can you briefly explain what these four areas of security cover and how these four areas impact the "networks and information systems" part?

Ex 2 : <u>IDS, and software used for audits</u>

2.1 What are the differences between a Network IDS and a Host IDS? Explain what are the interests of these two mechanisms?

2.2 During a security audit, some specific software may be used to achieve some analyses ; can you give the examples of two or three of these software and why are they used for?

2.1

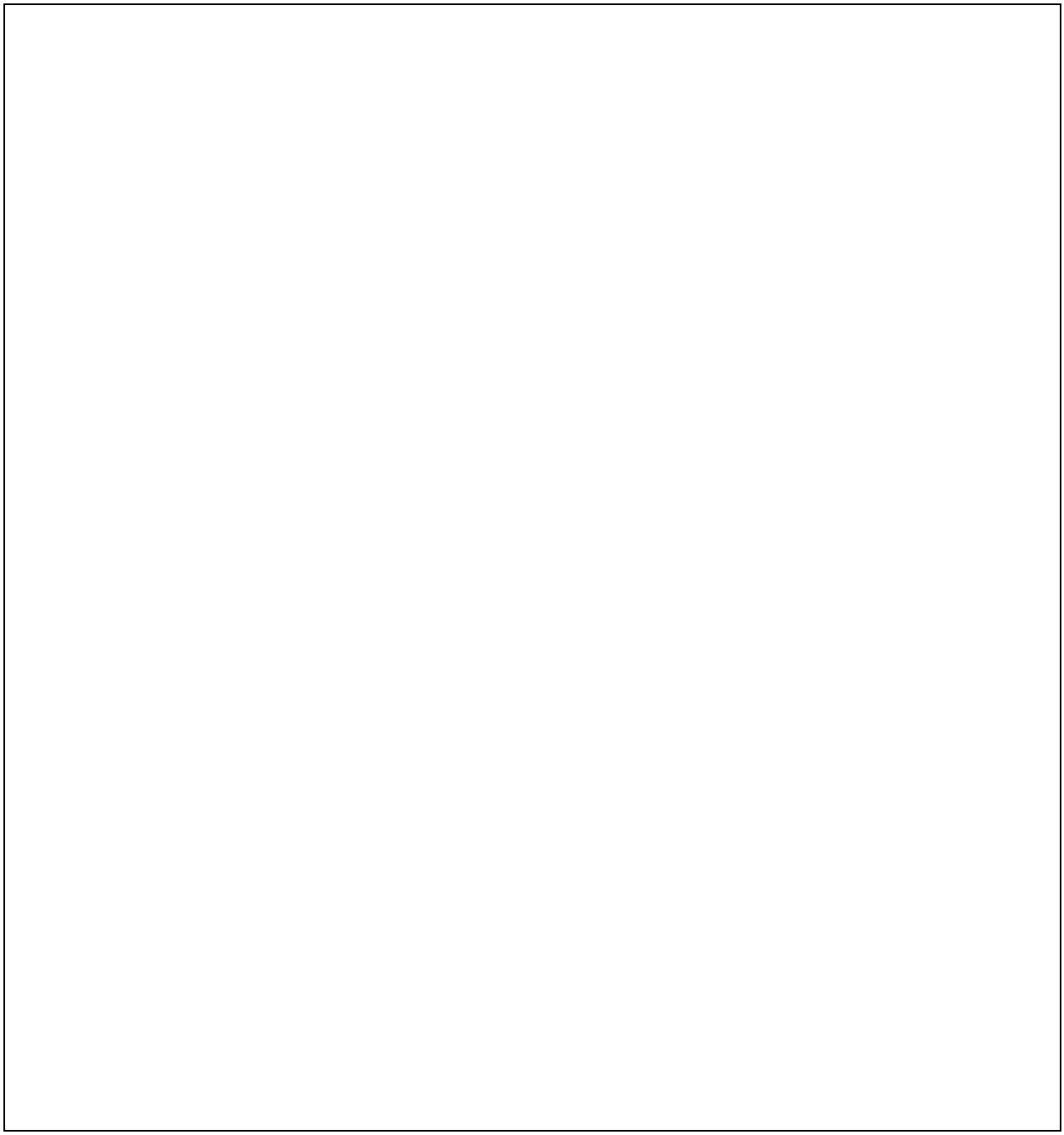
2.2

Ex 3. Attack You are the system and network administrator of a company and are in charge of IT security. Upon arrival, the network consists of a mail server (IMAP and SMTP) and a server hosting the company's website including its organization. These two servers use the Linux Centos operating system and are placed in a DMZ. The network includes client computers (~ 10 under Microsoft Windows) as well as an Active Directory server that also serves as a file server and DHCP. An IP autocom is also present for the IP telephones of the company.

1) For each computer resource (server, autocom, client) specify which vulnerabilities could be exploited?

2) For each server (server, autocom, client) specify to which threats they are potentially exposed?

3) For each server (server, autocom, client) specify to which attacks they could be confronted.



Ex 4: Virus

Below are two malware definitions for which you will need to determine the characteristics by referring to the table at the bottom of the exercise. In both cases it will be necessary to explain your choices.

Name	Logical Bomb	Trojan horse	Virus for executable	Document Virus	Startup Virus	Behavioral Virus	Simple worm	Macro worm
Cryptolocker								
Mydoom.A								

Cryptolocker : Spreads via email and via a pre-existing botnet. When enabled, it encrypts several files on the machine via public and private key encryption. The key to unlock the set is then only stored on the servers hosting the malware. The program then displays a message saying that to decrypt the information, it will be necessary to send a payment. The amount requested is valid until a certain date and then increases if the payment has not been made on time. The encryption system targets certain file extensions in particular, including Microsoft Office, Open Document, AutoCAD files, but also images. It attacks hard disks, shared disks on networks, USB keys, and sometimes files synchronized in the cloud.

Mydoom.A : Is spread by e-mail or Kazaa's P2P service. It affects the Microsoft Windows operating system. Once the computer is infected, it sends itself automatically to the entire address book under false identities, with random objects (Hi, Test, Mailer Daemon failure, etc.) and installs a backdoor in the system folder. This program not only scans the address book, but it also scans the hard drive for email addresses. It will also invent addresses to a domain (<bogus address> @ mondomaine.com) and multiply the infections when all <bogus addresses> @mondomain.com are redirected to a single address by default.