FACULTY OF SCIENCE

Academy of Computer Science and Software Engineering

Module	**IT08X57** Information Security in the WWW
Campus	APK
SSA	January 2020

Date	January 2021	**Time**	08:30
Assessor		Dr F F Blauw	
External Moderator		Prof M Olivier (UP)	
Duration	120 minutes	**Marks**	100

MEMO

QUESTION 1

In Information Theoretic Security, it is stated that to achieve perfect secrecy the size of the key must be equal or greater to that of the message, as shown below:

$$|\mathcal{K}| \geq |\mathcal{M}|$$

where $\mathcal{K}$ is the space of all keys and $\mathcal{M}$ is the space of all messages.

However, distributing such a long key would defeat the purpose of secret message exchange. Describe how this drawback is overcome.

[15]

Pseudorandom Generators

Instead of a "random key" use a "pseudorandom" key using a PRG (Pseudorandom Generator)

PRG is a function $\mathbf{G}: \{0,1\}^s \rightarrow \{0,1\}^n$ where $n \gg s$

$$c := \mathbf{E}(k, m) := m \oplus \mathbf{G}(k)$$

$$m := \mathbf{D}(k, c) := c \oplus \mathbf{G}(k)$$

Properties of $\mathbf{G}$:

- Efficient
- **Deterministic**, but **Unpredictable**
  - s is random
  - output should "look random"

QUESTION 2

Due to the ever-growing threat of potential intrusion, companies – great and small – are concerned that the security of their information systems may be the target of data breaches. These companies are hiring security testers to test the security of their information systems. However, does the testing strategy differ depending on the size of the organisation?

Provide a comprehensive strategy in which you describe how you will carry out a security test from start (being appointed) to finish (reporting your findings) all the while referring to the size of the company. Your essay should discuss the various phases of penetration testing, including:

- Information Gathering
- Scanning & Enumeration
- Exploit
- Post-Exploitation

[35]

Student will be required to discuss in detail the various steps they will follow to successfully complete a penetration test while referring to the size differences in companies.

A student must ensure that they put appropriate effort into each of the sections and will thus not be able to obtain 30 marks for writing completely on their information gathering strategy alone.

The student should mention aspects such as coming up with an agreement at the start of the penetration test that defines the parameters of the test (what they may or may not do) – which is important regardless of the size of the organisation. The student may discuss the various penetration testing models (black-box, white-box, or grey-box).

The student may mention tools that are used but should demonstrate insight into why they are using them e.g. they cannot simply say: “I will scan the ports for vulnerabilities”. The student should also take into consideration the scenario presented to them.

QUESTION 3

3.1. Discuss the major differences between (a) Stateful Inspection and (b) Stateless inspection firewalls. (6)

a) Stateful: Firewalls perform protocol conformance checking on filtered network data

- Ensures communication between two peers evolves according to specification

b) Stateless: Firewall decides whether to allow a packet to proceed on a per-packet basis

- Packet header is used for inspection
- Context of packet sequence is not examined
- Filtering rules based on pattern matching

3.2. Of the multiple approaches that an IDS/IPS system can take to perform its function, which is the best? Motivate you answer. (14)

Detection Strategies

Anomaly Based Detection

Statistical Anomaly Based Detection

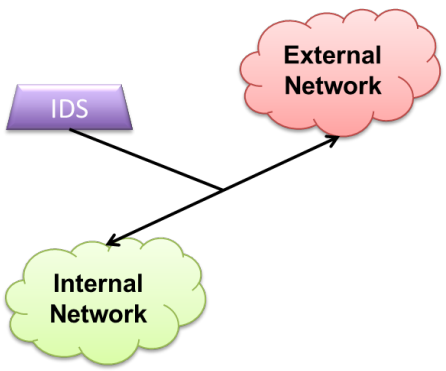
- Threshold detection
- Profile detection

Knowledge/Expert Anomaly Based Detection

Signature Anomaly Based Detection

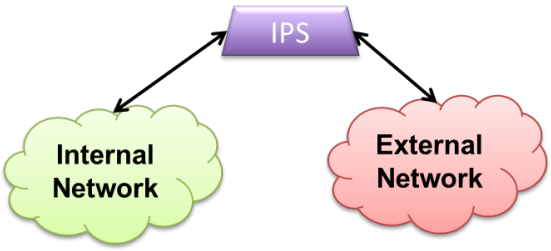
Adaptive Profiles Anomaly Based Detection

Inline:



- Sensors connected to a switched port analyser (SPAN)
- Out-of-band detection of intrusions – reports attacks
- Performs a “wiretap”
- Does not interfere with traffic
- False positives possible

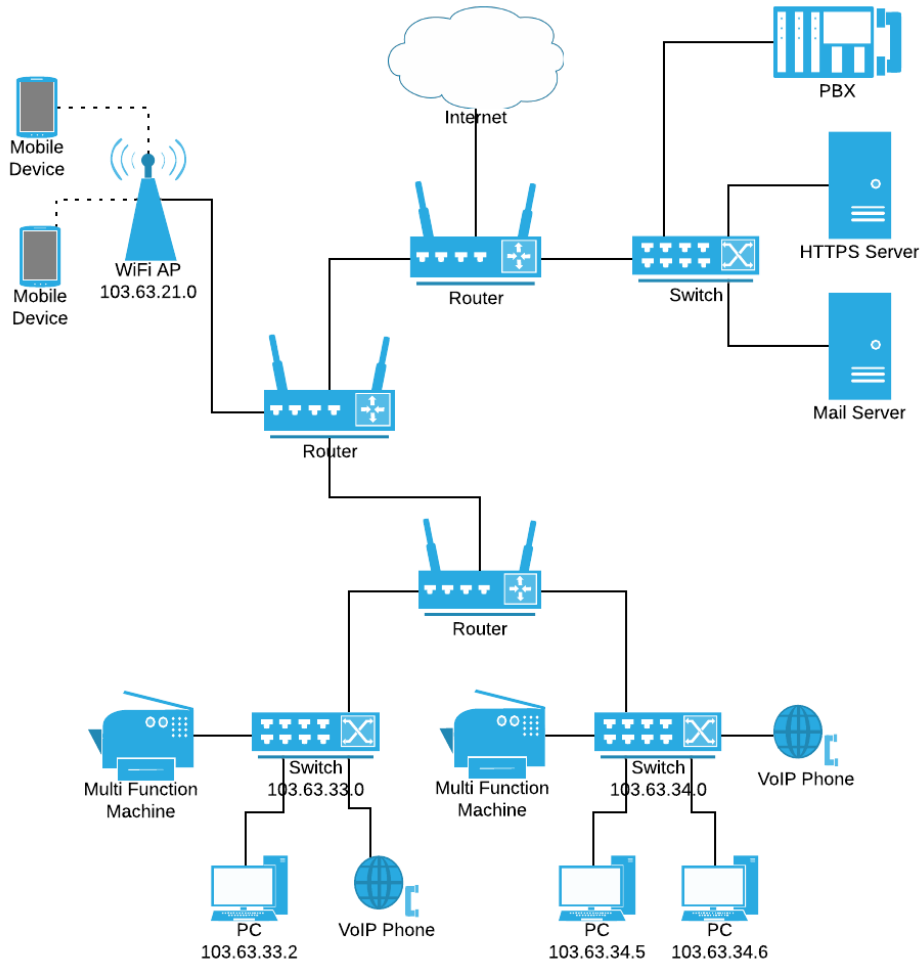
Out-of-Line:



- Provides in-band filtering to block instructions
- Eliminates the need for keeping and reading extension incident logs
- Uses considerable CPU, memory and I/O overhead
- False positives can block legitimate traffic

[20]

QUESTION 4



Consider the network diagram above. Choose any two (2) potential security vulnerabilities. For each chosen vulnerability:

- Briefly discuss the security vulnerability. (3)
- Discuss how an improvement should be implemented. (7)

2×(10) = **[20]**

Lack of Firewall

Lack of WiFi segmentation

Internal firewall for secure areas

QUESTION 5

Considering your research project for this semester, briefly discuss the vulnerability you identified. Refer to:

- Origin of the vulnerability
- Reason for the vulnerability
- Countermeasure / Fix for vulnerability
- Critique of countermeasure

[10]

— END OF EXAM —

Grand Total: [100]