

EXAMINATIONS 2013 / 2014 **AHOLIADAU 2013 / 2014**

Semester 2 re-sit

FACULTY OF: APPLIED DESIGN AND ENGINEERING
SCHOOL OF APPLIED COMPUTING

NAME OF COURSE/PROGRAMME: **MSc. Computer Networks**

YEAR OR LEVEL: **7**

NAME OF MODULE/UNIT/EXAM PAPER: **Network Security**

MODULE NO: **M7X00671**

DATE OF EXAMINATION:

EXAMINATION TIMES:

START TIME:

FINISH TIME:

TIME ALLOWED: 2 hours

INSTRUCTIONS TO CANDIDATES:

Answer three out of four questions. Each question carries equal marks.

Only basic calculators are permitted. Scientific calculators especially with internal memories are not allowed.

Candidates are not permitted to bring dictionaries; text books/case studies or any other reference materials into the exam room.

Assessment weighting: 60%

QUESTION ONE

- a) Imagine you are working on the security team of a small company and you realize that an unauthorized system has successfully connected to the wireless access point. All you know at the outset is the IP address of the wireless system. Figure 1 shows the network diagram.

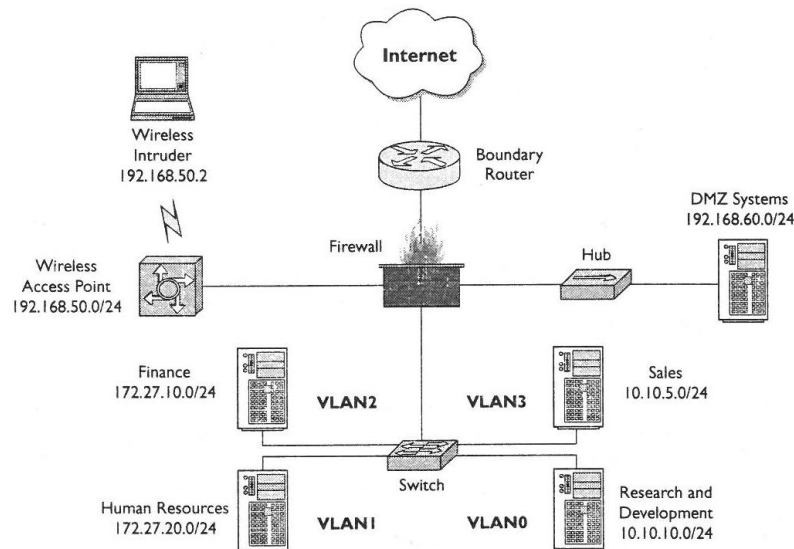


FIGURE 1

You have used the Paros session tool to collect session data on all interface of the firewall/gateway.

The Session Data below is collected from the DMZ segment of figure 1.

Time	Proto	SrcAddr.Sport	Dir	DstAddr.Dport
SrcPkt	Dstpkt	SrcBytes	DstBytes	State
1.	18:23:22	tcp	192.168.50.2.10639	-> 192.168.60.3.22
3039	2719	369110	1047369	EST
2.	18:23:53	icmp	192.168.60.3	<-> 192.168.60.5
1	1	98	98	ECO

9.	18:26:23	tcp	192.168.50.2.10639	->	192.168.60.3.22
	379	576	39966	65308	EST
10.	18:26:43	tcp	192.168.60.3.32786	->	10.10.10.2.22
	332	209	28920	40466	EST
11.	18:27:23	tcp	192.168.50.2.10639	->	192.168.60.3.22
	205	307	21678	22754	EST
12.	18:27:50	tcp	192.168.60.3.32786	->	10.10.10.2.22
	552	828	42672	691864	EST
13.	18:28:26	tcp	192.168.50.2.10639	->	192.168.60.3.22
	8384	3712	825652	3006732	EST
14.	18:28:50	tcp	192.168.60.3.32786	->	10.10.10.2.22
	1003	1581	73382	1986458	FIN
15.	18:29:32	tcp	192.168.50.2.10639	->	192.168.60.3.22
	98	123	10268	9850	FIN
3.	18:23:54	icmp	192.168.60.3	<->	192.168.60.5
	1	1	98	98	ECO
4.	18:24:04	tcp	192.168.60.3.32785	->	192.168.60.5.22
	2351	2675	158372	934469	FIN
5.	18:24:22	tcp	192.168.50.2.10639	->	192.168.60.3.22
	8440	4981	838844	2742726	EST
6.	18:24:43	tcp	192.168.60.3.32786	->	10.10.10.2.22
	3629	19471	250224	4306763	EST
7.	18:25:23	tcp	192.168.50.2.10639	->	192.168.60.3.22
	7494	3656	763472	1948248	EST
8.	18:25:43	tcp	192.168.60.3.32786	->	10.10.10.2.22
	1102	2212	80700	1211560	EST

- i. State the IP address the Attacker used to have access to other systems; this should be evident in the scan result.
- ii. From your understanding about session hijacking explain the scan result of the attacker movements.

(13 Marks)

b) Unmanaged TCP ports can create a number of security threats. Explain what some of these threats are and how they may be mitigated.

(8 marks)

c) Explain Man-in-the-browser attack?

(4 marks)

QUESTION TWO

a) What are the three 'principles' of computer security and what 'mechanisms' can be used in achieving these principles?

(10 marks)

b) Explain the role of a digital signature in information security.

(3 marks)

c) What is the difference between Authentication and Identification?

(2 marks)

d) You are requested by Swansea Security Consulting Company to write a report on '*password only*' security systems for their IT Security Manager (with a view to replacing them with something more secure). Compare and contrast the alternatives to *password only* systems and select what you think is most feasible as a replacement.

(10 marks)

QUESTION THREE

1. Your IT Director from Swansea Security Consulting Company will be attending a security conference within a week time and need to know about the following scans:

- SYN scan
- Connect Scan
- NULL scan
- Xmas scan
- ACK scan

Explain each scan for your IT Director.

(10 marks)

a) Lawful interception is carried out by law enforcement agency (LEA) to perform electronic surveillance on a target as authorized by a judicial or administrative order.

Explain the steps taken by LEA to carry out their investigation and the benefits of lawful intercept.

(12 marks)

b) How does Sniffer works?

(3 marks)

QUESTION FOUR

- a) Compare and contrast symmetric and asymmetric cryptography. (10 marks)
- b) Argue some of the advantages of using DES encryption over asymmetric encryption. (10 marks)
- c) *"Cryptography is 'generally' considered to be the broadest security technique available."* Explain what this statement means with respect to the principles of information security. (5 marks)