

LOCATION: SWANSEA

LLEOLIAD: ABERTAWE

LEVEL 7

LEFEL 7

EXAMINATION PERIOD
JANUARY 2017

CYFNOD ARHOLIADAU
IONAWR 2017

MODULE CODE: M7X01701
Network Security

TIME: 2 HOURS (USE 1 ½ NOT 1.5 FOR TIME)

ANSWER THREE QUESTION OUT OF FOUR

Equipment or materials required – Basic Calculator

Adnoddau neu ddefnyddiau sydd eu hangen – Cyfrifiannell Sylfaenol

ANSWER THREE QUESTIONS

Q1.

- a. You have been commissioned to conduct a real life penetration testing on two websites; <http://cupstc.com> and <http://tocomex-forensics.com>. Explain the types of pentests you would carry out on these websites. Diagrams may be used. Your solutions should include the following:
- List of vulnerabilities that you want to targeted at the websites. Defend your choice.
 - At least 5 attack tools that you will be using and briefly tell their purposes.
 - Outline your penetration testing in a few steps, say 1-4.
 - Briefly explain the difference between Penetration Testing and vulnerability Assessment.
 - Give a brief description of your contingency plan before commencement of penetration testing.

(25 marks)

Q2.

- a. Wireless access control aim to penetrate a network by evading WLAN access control. Critically discuss three types of wireless Encryptions that may be used to protect a wireless router. You should explain how they works and the issues associated with them.

(20 marks)

- b. Outline how you would defend a wireless network from attacks?

(5 Marks)

Q3.

- a. Imagine you are working on the National Health Service (NHS), Wales security team 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.

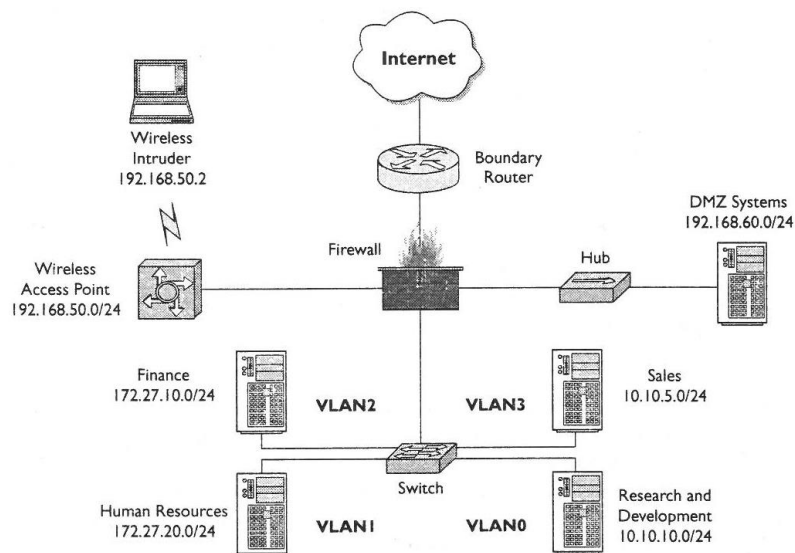


FIGURE 1

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.

(13arks)

- 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. In reference to Security Policy and Management. What is the difference between identification and authentication?
(4 marks)

Q4.

- a. Describe briefly the types of cryptography and any **four** encryption algorithms that security professionals used to protect company's data.
(18 marks)
- b. Active attacks attempt to determine the secret key used to encrypt plaintext. Man-in-the-Middle Attack is one of the common attacks, explain this kind of attack and outline a scenario.
(7 marks)

Diwedd/End