

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.

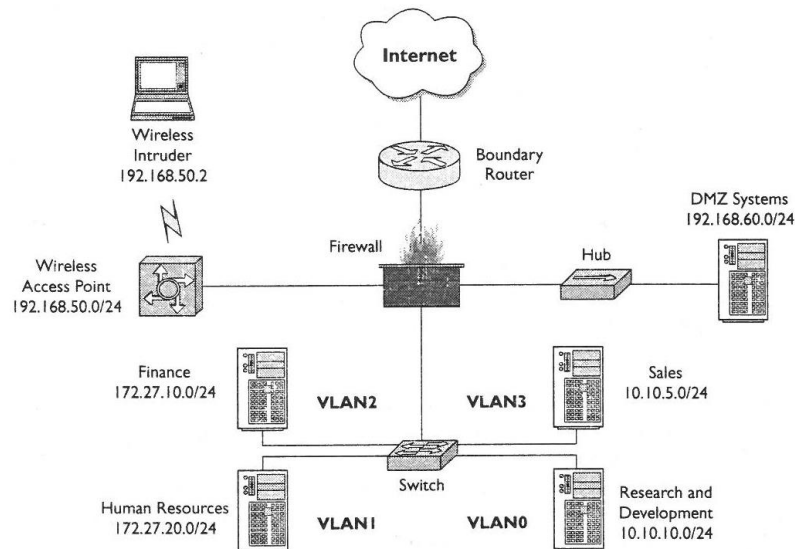


FIGURE 1

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

The session Data from the Wireless Segment is given below. The **new IP address** which appears from the scan result is in **bold**.

Time	Proto	SrcAddr.Sport	Dir	DstAddr.Dport
SrcPkt	Dstpkt	SrcBytes	DstBytes	State
1. 18:22:43	tcp	192.168.50.2.10634	?>	172.27.20.3.22
15	14	1418	1208	FIN
2. 18:22:56	tcp	192.168.50.2.10637	->	172.27.20.3.22
29	22	3842	4064	FIN
3. 18:23:22	tcp	192.168.50.2.10639	->	192.168.60.3.22
3039	2719	369110	1047369	EST
4. 18:24:22	tcp	192.168.50.2.10639	->	192.168.60.3.22
8440	4981	838844	2742726	EST
5. 18:25:23	tcp	192.168.50.2.10639	->	192.168.60.3.22
7494	3656	763472	1948248	EST
6. 18:26:23	tcp	192.168.50.2.10639	->	192.168.60.3.22
379	576	39966	65308	EST
7. 18:27:23	tcp	192.168.50.2.10639	->	192.168.60.3.22
205	307	21678	22754	EST
8. 18:28:26	tcp	192.168.50.2.10639	->	192.168.60.3.22
8384	3712	825652	3006732	EST
9. 18:29:32	tcp	192.168.50.2.10639	->	192.168.60.3.22
98	123	10268	9850	FIN

Session Data from the Wireless Segment

- i. Inspect the Paros data and explain the scan result including the Attackers movement.

(12 Marks)

- b) Examine the output from the scanning tool shown in Figure 2 and describe what services are running and what security implications these may have for this particular network.

```
C:\WINDOWS\system32\cmd.exe
C:\nmap-3.75>nmap 192.167.0.2
Starting nmap 3.75 ( http://www.insecure.org/nmap ) at 2008-11-18 12:18 GMT Stan
dard Time
Interesting ports on CONTROLLER1 (192.167.0.2):
<The 1646 ports scanned but not shown below are in state: closed>
PORT      STATE SERVICE
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp  open  NFS-or-IIS
1027/tcp  open  IIS
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
MAC Address: 00:0B:CD:4A:0A:78 (Compaq (HP))

Nmap run completed -- 1 IP address (1 host up) scanned in 1.688 seconds
C:\nmap-3.75>_
```

Figure 2: Output of Scanning Tool

(10 marks)

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

(3 mark)

QUESTION TWO

a) Explain your understanding of the following network protection systems:

- i. Intrusion Detection System (IDS)
- ii. Firewall
- iii. Honeypot

Include in your answer types of each, how to set up a Honeypot, firewall identification techniques, tools and countermeasures.

(18 marks)

b) Outline the flow of a firewall/IDS penetration testing to evaluate the security by testing for ingress and egress vulnerability.

(7 marks)

QUESTION THREE

a) You are employed by Swansea Security Consulting Company as a security tester, who has to research any new tools that will help you to perform your duties. It has been noted that some open sources tools your company used lack simplicity and

clarity or don't meet the company's expectation. Your IT Director asks you to research new or improved products on the market.

Based on this information, write a report for your IT Director describing **four** port-scanning tools that might be useful to the company. Different port scans might elicit different information; your report should include the port scan types such as SYN, ACK, FIN, etc.

(12 marks)

- a) Explain information security, threats and attacks and describe the elements of Information Security.

(13marks)

QUESTION FOUR

- 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)