



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

LOCATION: SWANSEA

LLEOLIAD: ABERTAWE

LEVEL 7

LEFEL 7

EXAMINATION PERIOD
JANUARY 2018

CYFNOD ARHOLIADAU
IONAWR 2018

MODULE CODE: M7X01701
Network Security

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

ANSWER THREE QUESTION OUT OF FOUR

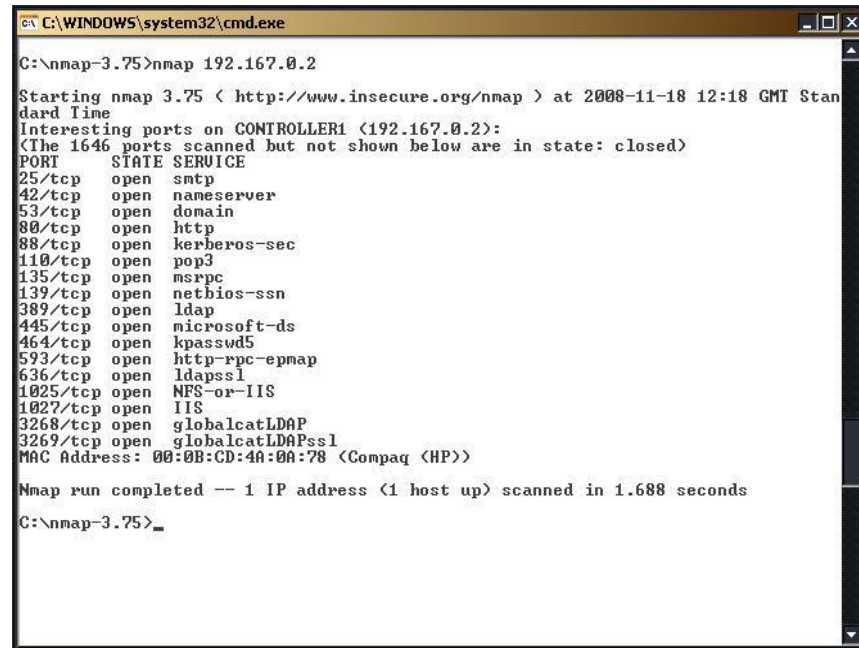
Equipment or materials required – Basic Calculator

Adnoddau neu ddefnyddiau sydd eu hangen – Cyfrifiannell Sylfaenol

ANSWER THREE QUESTIONS

Q1.

- a. Examine the output from the scanning tool shown in Figure 1 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  nethios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd
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 1: Output of Scanning Tool

(10 marks)

- b. As a security tester, one of your daily task is to research 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 do not meet the company's expectation. Your IT Director asks you to research new or improved products on the market.

Inform your IT Director on **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.

(15 marks)

Q2.

- a. As a qualified ethical hacker you have been consulted by Tecomex Forensics Ltd to conduct a real life penetration testing on <http://cupstc.com> or <http://tecomex-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.

- iv. Briefly explain the difference between Penetration Testing and vulnerability Assessment.
- v. Give a brief description of your contingency plan before commencement of penetration testing.

(25 marks)

Q3.

- a. In reference to the types of Penetration Testing, explain the differences between the following:

(20 marks)

- i. External and internal testing
- ii. Black-box and white-box testing
- iii. Announced and unannounced testing
- iv. Automated and manual testing

- b. Explain the purpose of a penetration testing Service Level Agreement (SLA)

(5 marks)

Q4.

- a. The first step in creating a security policy for a company network is to define and acceptable use policy (AUP).

- i. Construct an example of a policy mapping.

(5 marks)

- ii. Outline what is expected to be written in a security policy.

(5 marks)

- iii. What are some of the wrong assumptions you should avoid when writing a security policy?

(5 marks)

- iv. List the ten step approach in writing a policy.

(10 marks)

Diwedd/End