

COMP623 - Digital Security - 14818 - WIN - 202110

Notifications

Announcements

Module Content

Course Handbook

Assessment & Feedback

Academic Integrity Tutorial

Quote Unquote

Turnitin Student Help

Learning Resources

Reading List

MyBeckett Student Help

Library

Skills For Learning

Module Resources

Module Content

Module Handbook

Quizzes

Report Submission

Take Test: Scanning

Test Information

Description

Instructions

Timed Test This test has a time limit of 40 minutes. This test will save and be submitted automatically when the time expires. Warnings appear when **half the time, 5 minutes, 1 minute, and 30 seconds** remain.

Multiple Attempts Not allowed. This Test can only be taken once.

Force Completion Once started, this test must be completed in one sitting. Do not leave the test before clicking **Save and Submit**.

Your answers are saved automatically.

QUESTION 1

1 points  Saved

A SYN scan works by:

- Not answering the SYN with a SYN/ACK
- Not answering the SYN/ACK with an ACK
- Sending a RST packet
- Completing the full three-way handshake



QUESTION 2

1 points  Saved

What will the following command do?

sudo nmap -sS 10.72.35.207

- Perform a scan that connects using a full TCP three-way handshake
- Performs a scan that sets the FIN, PSH, and URG flags
- Perform a scan that uses a connection-less IP protocol
- Perform a scan that does not complete the three-way handshake

QUESTION 3

1 points  Saved

What will the following command do?

sudo nmap -sV 10.72.35.207

- Performs simple banner grabbing
- Perform a scan that connects using a full TCP three-way handshake
- Perform a scan that attempts to identify the software running on the port
- Performs a scan that sets the FIN, PSH, and URG flags

QUESTION 4

1 points  Saved

What will the following command do?

sudo nmap -p 21 10.72.35.207

- None of these services
- Scan for an email server
- Scan for a ftp server
- Scan for an SSH server
- Scan for a web server
- All of these services

QUESTION 5

1 points  Saved

What will the following command do?

sudo nmap -p 20-1000 10.72.35.207

- Scan for a web server
- Scan for an email server
- Scan for a ftp server
- None of these services
- Scan for an SSH server
- All of these services

QUESTION 6

1 points  Saved

What will the following command do?

sudo nmap -sT 10.72.35.207

- Perform a scan that does not complete the three-way handshake
- Performs a scan that sets the FIN, PSH, and URG flags
- Perform a scan that uses a connection-less IP protocol
- Perform a scan that connects using a full TCP three-way handshake

QUESTION 7

1 points  Saved

nmap -sn 192.168.1.1

What does the above command do?

- Attempts a series of actions to detect that the host is live (including an ICMP echo request and ICMP timestamp request)
- A port scan
- A ping sweep (a simple ping echo request)
- Simply resolves the DNS name for the IP address

QUESTION 8

1 points  Saved

nmap -sL 192.168.1.1

What does the above command do?

- Attempts a series of actions to detect that the host is live (including an ICMP echo request and ICMP timestamp request)
- Simply resolves the DNS name for the IP address
- A ping sweep (a simple ping echo request)
- A port scan

QUESTION 9

1 points  Saved

Given the below invocation and output of Nmap, what can you conclude?

```
nmap localhost -p 22
Starting Nmap 5.61TEST2 ( http://nmap.org ) at 2013-10-15 16:09 BST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000028s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
```

- The remote system is listening to port 22
- The local system has a firewall rule that denies access to port 22
- The remote system is not available
- The local system has an ssh server running

QUESTION 10

1 points  Saved

Given the below invocation and output of Nmap, what can you conclude?

```
nmap 10.72.35.110-112 -p 22
Starting Nmap 5.61TEST2 ( http://nmap.org ) at 2013-10-15 16:16 BST
Nmap scan report for 26212pc.dyn.leedsmet.ac.uk (10.72.35.111)
Host is up (0.0016s latency).
PORT      STATE SERVICE
22/tcp    closed  ssh
Nmap done: 3 IP addresses (1 host up) scanned in 1.25 seconds
```

- Of the systems scanned only one is live, and IS accepting connections on port 22
- Of the systems scanned, only one is live and IS NOT accepting connections to port 22
- The system that was detected was a Linux system
- No remote systems were found to be live