Final Exam

- Due Apr 24, 2024 at 11:59pm
- Points 100
- Questions 18
- Available Apr 24, 2024 at 12am Apr 24, 2024 at 11:59pm 23 hours and 59 minutes
- Time Limit 120 Minutes

Instructions

The final exam is available online at 12:00am Wed April 24th until 11:59pm same day.

You will be given **120 minutes** and **one attempt** to complete it once you start the exam. It will include the topics we have covered after the midterm. There will be three types of questions: true/false, multiple-choice, and fill-in-the-blank.

The exam consists of 18 questions.

Best of luck,

Mesut

This quiz is no longer available as the course has been concluded.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	113 minutes	100 out of 100

Score for this quiz: 100 out of 100 Submitted Apr 24, 2024 at 11:44pm

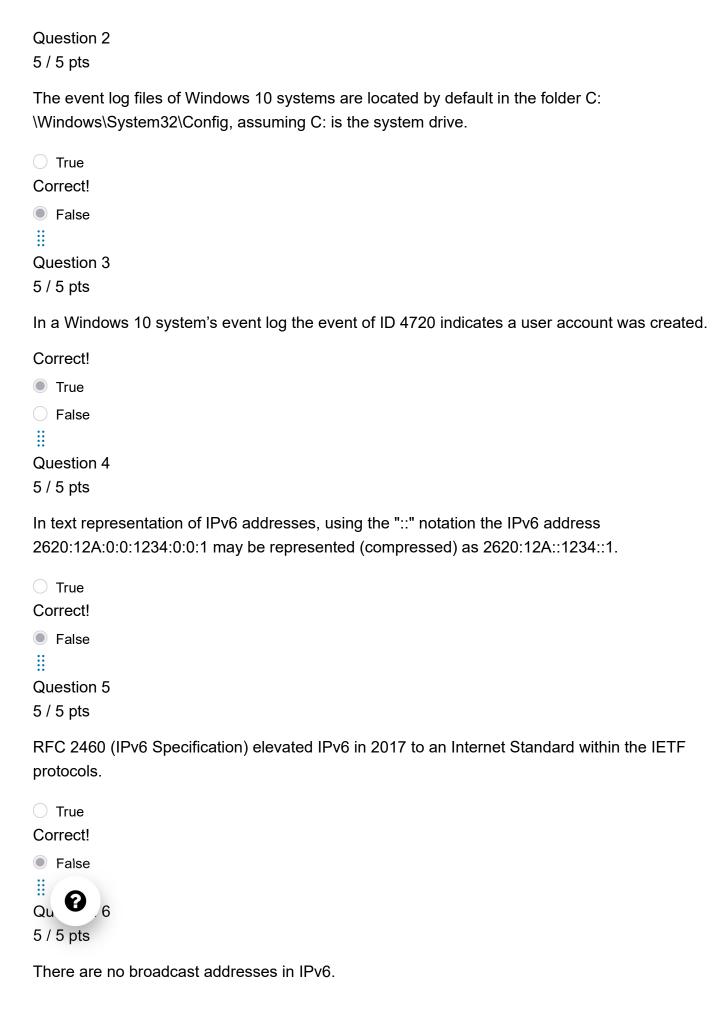
This attempt took 113 minutes.

Question 1

5 / 5 pts

The DLL view of the ProcessExplorer tool (v.17.02 or later) from sysinternals.com can be used to monitor Registry keys being accessed by active processes.





Correct! True False Question 7
5 / 5 pts
The SMTP protocol uses port 25 for transporting emails.
Correct! True False Question 8 5 / 5 pts
The open-source tool Snort can best be described as a network port scanner.
 True Correct! ● False ⋮ Question 9 6 / 6 pts
Which of the following IPv6 address types has been deprecated?
 Link-Local unicast Global Unicast Correct! Site-local unicast ⋮ Question 10 6 / 6 pts
The second frame in the 3-way handshake of a TCP session between two hosts has which of the following flag (or flags) set?
both SYN and ACK SYN only

Question 11

6 / 6 pts

When two hosts are engaged in a TCP connection in which the client makes the initial request to the server in frame 1, this frame's raw sequence number starts at

Correct!

- a random 32-bit value
- 0 (zero)
- a value pre-determined between the two hosts

Question 12

6 / 6 pts

Which of the following IP addresses belong to the subnet 192.168.240.1/20?

192.168.238.101

Correct!

- 9 192.168.250.15
- Neither one of the two choices

Question 13

6 / 6 pts

Consider the following email header (with the email body removed):

4/23/2025, 12:37 PM

```
smtp.helo=strobo.id; dkim=none (message not signed) header.d=none;dmarc=none
 action=none header.from=;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 strobo.id discourages use of 103.168.135.199 as permitted sender)
Received: from strobo.id (103.168.135.199) by
 BN1NAM02FT057.mail.protection.outlook.com (10.13.2.165) with Microsoft SMTP
 Server (version=TLS1 2, cipher=TLS ECDHE RSA WITH AES 256 GCM SHA384) id
 15.20.6254.9 via Frontend Transport; Sun, 26 Mar 2023 01:56:54 +0000
Received: from User (unknown [194.55.224.96])
    by strobo.id (Postfix) with SMTP id BC5092DDAA;
    Sat, 25 Mar 2023 17:22:21 +0700 (WIB)
Reply-To: <andrewtwdie1@aliyun.com>
From: "From Antony J. Blinken" <<>>
Subject: Regarding Your Pending Fund Worth the sum of US$10,000,000.00
Date: Sat, 25 Mar 2023 03:22:31 -0700
MIME-Version: 1.0
Content-Type: text/html;
    charset="Windows-1251"
Content-Transfer-Encoding: 7bit
```

Which of the following would be the non-local IP address closest to the source (sender) of this email?

0 103.168.135.199

Correct!

- 9 194.55.224.96
- 2603:10b6:408:ec::6

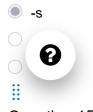
::

Question 14

6 / 6 pts

Which of the following tcpdump option flags is used to specify the maximum length for each of the captured packets?

Correct!



Question 15

6 / 6 pts

Which option in Wireshark under View>Statistics will show connections between hosts; displays the packet time, direction, ports and comments for each captured connection?

Endpoints

Conversations

Correct!

Flow Graph

Question 16

6 / 6 pts

The size/length of an IPv6 fixed header is [] bytes (in decimal value)

Correct!

40

Correct Answers

40

Question 17

6 / 6 pts

The size/length of an ARP (Address Resolution Protocol) packet in a TCP/IP network is [] bytes (in decimal value).

Correct!

28

Correct Answers

28

::

Question 18

6 / 6 pts

Consider a pcap file of 8 frames displayed in Wireshark's packet list pane (with 6 columns showing: frame number, seconds since the first captured packet, source, destination, protocol, and frame len? ___ see below:

Fram Time Source Destination Protocol

Length

1	0.000000	10.10.1.4	10.10.1.1	
DNS	76			
2	0.034025	10.10.1.1	10.10.1.4	
DNS	142			
3	0.036986	10.10.1.4	74.53.140.153	TCP
62				
4	0.383936	74.53.140.153	10.10.1.4	TCP
62				
5	0.383968	10.10.1.4	74.53.140.153	TCP
54				
6	0.727603	74.53.140.153	10.10.1.4	SMTP
235				
7	0.732749	10.10.1.4	74.53.140.153	SMTP
63				
8	1.073326	74.53.140.153	10.10.1.4	TCP
60				

If Wireshark's display filter is set to "ip.addr == 10.10.1.4" (without quotes), then [] frames (in decimal value) will be displayed after filtering.

Correct!

8

Correct Answers

8

Quiz Score: 100 out of 100



7 of 7