**Unit 1**

**1.1**

1. Please mark the correct answer.
What are the two security modes in which code can be executed?
	1. safe and unsafe
	2. teacher and student
	3. *user and kernel*
	4. amateur and professional

**1.2**

1. Please mark the correct answer.
At which ring level are the highest privileges for processes?

1. *Level 0*
2. Level 1
3. Level 2
4. Level 5

**1.3**

1. When analyzing RAM, which artifacts are likely to be found?
	1. the user’s shoe size
	2. the purchase date of the computer
	3. *IP addresses*
	4. when the computer was last powered on

**1.4**

1. Which RAID has a recovery mechanism?
	1. RAID 0
	2. *RAID 5*
	3. RAID 17.5
	4. RAID 100

**1.5**

1. Which of the answers best describes the following issue?
An interrupt-driven I/O or programmed I/O must be implemented to manage the response time to input/output requests.
	1. Memory mapped I/O
	2. Channel I/O
	3. *System response*
	4. Device independence

**Unit 2**

**2.1**

1. The *kernel mode* is where the system’s processes and operations are executed and have full access to the memory space and hardware.

**2.2**

1. The process control block will contain *memory allocation*.

**2.3**

1. The registry is the \_\_\_\_\_of the Windows operating system.
	1. soul
	2. fingers
	3. toes
	4. *heart*

**2.4**

* 1. Which file system that Microsoft Windows, Mac OS, and Linux operating systems can read by default \_\_\_\_\_\_?
		1. NTFS
		2. EXT 3
		3. APFS
		4. *FAT32*

**2.5**

* 1. Please complete the following sentence.
	Return to libc is a \_\_\_\_\_\_ attack.
		1. Mummy
		2. Byte switching
		3. *buffer overflow*
		4. Key logger

**Unit 3**

**3.1**

1. Please mark the correct answer.

Which of the following is a Class A address?

* *45.152.86.9*
* 137.23.1.251
* 192.168.86.5
* 155.55.22.8

**3.2**

1. Please mark the correct answer.

Which of the following records will contain links of alias names to another domain name?

* AName
* BName
* *CName*
* DName

**3.3**

1. Which protocol call is used to protect the user while using a web browser?

* HTTP
* *HTTPS*
* DNS
* Secure IRC

**3.4**

1. Please mark the correct answer.

Which of the following is a hashing algorithm?

* AES
* *MD5*
* TLS
* SSL

**3.5**

1. Please mark the correct answer.

Which encryption key would be used by the sender of an email to protect the confidentiality of the communication?

* *Recipient’s public key*
* Recipient’s private key
* Sender’s public key
* Sender’s private key

**Unit 4**

**4.1**

1. Please mark the correct answer.

A DD forensic image is compressed by default.

* True
* *False*

**4.2**

1. Please mark the correct answer.

Volatility can be used to collect RAM.

* True
* *False*

**4.3**

1. Please mark the correct answer.

Which of the following is a category of information an attacker will look for?

* *Personally Identifying Information (PII)*
* SQL Database
* License keys for the Windows Operating System
* Mail delivery times

**4.4**

1. Please mark the correct answer.

Which of the following methods is used by steganography?

* Data switching
* Data splitting
* *Data insertion*
* Data flipping

**Unit 5**

**5.1**

1. Please mark the correct answer.

In the F3EAD model, the exploit phase is used to \_\_\_\_\_\_\_\_?

* *Collect information*
* Determine Threats
* Locate the attacker
* Share information

**5.2**

1. Please mark the correct answer.

The first step in an anatomy of an attack is?

* Root access
* Data exfiltration
* *Targeting*
* Data infiltration

**5.3**

1. Please mark the correct answer.

How many steps are in the “Intelligence Cycle”?

* 4
* 5
* *6*
* 7

**Unit 6**

**6.1**

1. Please fill in the blank.

Within the MITRE ATT@CK Framework, APT28 is an example of what?

* + *threat group*
	+ policy
	+ requirements
	+ prerequisites

**6.2**

1. Please mark the correct answer.

Which of the following type of IDPS is responsible for monitoring the traffic and events occurring on a specific host?

* Behavioral analysis
* Network-based
* *Host-based*
* User-based

**6.3**

1. Please mark the correct answer.

Which of the following is a technique for an attacker to hide malware?

* Renaming
* *Packing*
* Stuffing
* Clipping