DLMCSECSNF01\_E\_Unit01\_Question01

RAM is managed by the …

* …operating system. (1 Pts)
* …file system. (0 Pts)
* …user. (0 Pts)
* …administrator. (0 Pts)

DLMCSECSNF01\_E\_Unit01\_Question02

Which form of memory needs electric current to retain data?

* RAM (1 Pts)
* ROM (0 Pts)
* SSD (0 Pts)
* EPROM (0 Pts)

DLMCSECSNF01\_E\_Unit01\_Question03

Which of the following is not a source of memory similar to RAM?

* System32.dll (1 Pts)
* hiberfill.sys (0 Pts)
* pagefile.sys (0 Pts)
* swapfile.sys (0 Pts)

DLMCSECSNF01\_E\_Unit01\_Question04

Which of the following is not a state in the three-state process management model?

* Not Running (1 Pts)
* Running (0 Pts)
* Ready (0 Pts)
* Blocked (0 Pts)

DLMCSECSNF01\_E\_Unit01\_Question05

What is the smallest structural unit on a hard drive?

* sector (1 Pts)
* cluster (0 Pts)
* track (0 Pts)
* ring (0 Pts)

DLMCSECSNF01\_E\_Unit02\_Question01

Which of the following has full access to the memory space?

* kernel mode (1 Pts)
* user mode (0 Pts)
* admin mode (0 Pts)
* root mode (0 Pts)

DLMCSECSNF01\_E\_Unit02\_Question02

Which of the following is not a function of the process table?

* resource management (1 Pts)
* process management (0 Pts)
* memory management (0 Pts)
* file management (0 Pts)

DLMCSECSNF01\_E\_Unit02\_Question03

What is the name for a logical group of keys, sub-keys, and values in the registry?

* hive (1 Pts)
* colony (0 Pts)
* swarm (0 Pts)
* settings (0 Pts)

DLMCSECSNF01\_E\_Unit02\_Question04

Which file system can be read by Windows, macOS, and Linux?

* FAT32 (1 Pts)
* EXT3 (0 Pts)
* APFS (0 Pts)
* ZFS (0 Pts)

DLMCSECSNF01\_E\_Unit02\_Question05

The “stack canaries” technique is used to mitigate which type of attack?

* buffer overflow (1 Pts)
* side channel (0 Pts)
* social engineering (0 Pts)
* phishing (0 Pts)

DLMCSECSNF01\_E\_Unit03\_Question01

How many layers are in the OSI model?

* seven (1 Pts)
* six (0 Pts)
* nine (0 Pts)
* eight (0 Pts)

DLMCSECSNF01\_E\_Unit03\_Question02

Which DNS record identifies the server of the domain’s email accounts?

* MX (1 Pts)
* TXT (0 Pts)
* CName (0 Pts)
* A Record (0 Pts)

DLMCSECSNF01\_E\_Unit03\_Question03

What is the default port for HTTP?

* 80 (1 Pts)
* 110 (0 Pts)
* 25 (0 Pts)
* 21 (0 Pts)

DLMCSECSNF01\_E\_Unit03\_Question04

What type of attack occurs when a third party places themselves in the middle of the communication channel between two other parties?

* man-in-the-middle (1 Pts)
* phishing (0 Pts)
* social engineering (0 Pts)
* Trojan horse (0 Pts)

DLMCSECSNF01\_E\_Unit03\_Question05

What type of attack occurs when the attacker inserts fraudulent DNS information into a DNS server’s cache?

* DNS spoofing (1 Pts)
* DNS altering (0 Pts)
* DNS faking (0 Pts)
* DNS hijacking (0 Pts)

DLMCSECSNF01\_E\_Unit04\_Question01

The chain of custody is critical for…

* …evidence authentication. (1 Pts)
* …forensic examination. (0 Pts)
* …keyword searches. (0 Pts)
* …certification. (0 Pts)

DLMCSECSNF01\_E\_Unit04\_Question02

Which of the following is not an option when making a working copy of a storage device?

* forensic backup (1 Pts)
* forensic copy (0 Pts)
* forensic image (0 Pts)
* logical forensic image (0 Pts)

DLMCSECSNF01\_E\_Unit04\_Question03

Which of the following is code that encrypts the contents of the user system, with the attacker then demanding payment to decrypt the contents?

* ransomware (1 Pts)
* kidnapware (0 Pts)
* hostageware (0 Pts)
* worm (0 Pts)

DLMCSECSNF01\_E\_Unit04\_Question04

What occurs when the confidentiality of data has been violated and the attacker completes an unauthorized data transfer?

* data exfiltration (1 Pts)
* data capture (0 Pts)
* data expiration (0 Pts)
* data piracy (0 Pts)

DLMCSECSNF01\_E\_Unit04\_Question05

What is the technique used to hide a file within a file?

* steganography (1 Pts)
* encryption (0 Pts)
* encoding (0 Pts)
* compressing (0 Pts)

DLMCSECSNF01\_E\_Unit05\_Question01

Network forensics is a function of digital forensics and…

* …incident response. (1 Pts)
* …computer forensics. (0 Pts)
* …digital investigations. (0 Pts)
* …network investigations. (0 Pts)

DLMCSECSNF01\_E\_Unit05\_Question02

Which of the following is not helpful without context?

* information (1 Pts)
* intelligence (0 Pts)
* analysis (0 Pts)
* examination (0 Pts)

DLMCSECSNF01\_E\_Unit05\_Question03

Which of the following uses compression to hide malware?

* packer (1 Pts)
* code Insertion (0 Pts)
* encryption (0 Pts)
* encoding (0 Pts)

DLMCSECSNF01\_E\_Unit05\_Question04

ROT-13 corresponds to a type or method of…

* …encryption. (1 Pts)
* …compression. (0 Pts)
* …steganography. (0 Pts)
* …cipher text. (0 Pts)

DLMCSECSNF01\_E\_Unit05\_Question05

Which of the following is an example of obfuscation?

* deleting log files (1 Pts)
* deleting image files (0 Pts)
* deleting applications (0 Pts)
* deleting user accounts (0 Pts)

DLMCSECSNF01\_E\_Unit06\_Question01

Which of the following is used by signature-based intrusion detection?

* hash values (1 Pts)
* algorithms (0 Pts)
* analysis (0 Pts)
* artificial intelligence (0 Pts)

DLMCSECSNF01\_E\_Unit06\_Question02

Which of the following is not an element needed to deploy TTP?

* offensive analysis (1 Pts)
* threat intelligence (0 Pts)
* defensive engagement (0 Pts)
* information sharing (0 Pts)

DLMCSECSNF01\_E\_Unit06\_Question03

Which of the following is done to analyze threat intelligence?

* reviewing data points of past attacks (1 Pts)
* reviewing emails (0 Pts)
* reviewing policies (0 Pts)
* reviewing attendance rosters (0 Pts)

DLMCSECSNF01\_E\_Unit06\_Question04

Which of the following is a label used by the ATT&CK framework?

* Tactics (1 Pts)
* Teams (0 Pts)
* Polices (0 Pts)
* Methods (0 Pts)

DLMCSECSNF01\_E\_Unit06\_Question05

Which protocol ensures that devices on a network are synced to the same time?

* NTP (1 Pts)
* ARP (0 Pts)
* IP (0 Pts)
* FTP (0 Pts)