**Question 1**(1 point)

*Saved*

The concept of defense in depth is not important when deploying endpoint defenses.

Question 1 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 2**(1 point)

*Saved*

Which of the following combines both aggressor and defender teams?

Question 2 options:

|  |  |
| --- | --- |
|  | red team |
|  | blue team |
|  | black team |
|  | purple team |

**Question 3**(1 point)

*Saved*

When traditional security measures have been put in place, a single flaw open to exploit cannot provide the way in for an attacker.

Question 3 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 4**(1 point)

*Saved*

Which of the following U.S. Department of Defense (DoD) initiatives is a broad array of systems that provides situational awareness and can react and respond?

Question 4 options:

|  |  |
| --- | --- |
|  | Unmanned Aircraft System (UAS) |
|  | Research, Development, Test, and Evaluation (RDTE) |
|  | Command, Control, Communications, Computers, and Intelligence (C4I) |
|  | Man Transportable Robotic System (MTRS) |

**Question 5**(1 point)

*Saved*

Targeting endpoint systems is an attractive option for attackers.

Question 5 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 6**(1 point)

*Saved*

The use of anti-malware requires that staff know about threats and attacks.

Question 6 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 7**(1 point)

*Saved*

Vulnerability scanning uses attacks and exploits against an organization to verify the effectiveness of its security controls.

Question 7 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 8**(1 point)

*Saved*

The term military systems describes a range of devices and platforms.

Question 8 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 9**(1 point)

*Saved*

Due to a push by the Food and Drug Administration (FDA), many standards for the security of medical devices have been created and adopted.

Question 9 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 10**(1 point)

*Saved*

A Trusted Platform Module (TPM) chip is a cryptographic processor built in to the motherboard of the device.

Question 10 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 11**(1 point)

*Saved*

Due to their critical role in battlefield control, programmable logic controllers (PLCs) are an important part of current and future combat strategies.

Question 11 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 12**(1 point)

*Saved*

Traditional techniques for detecting malware have become more effective over the past decade.

Question 12 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 13**(1 point)

*Saved*

The U.S. Wounded Warrior design includes individual solider computer systems that provided monitoring of individual soldiers with health sensors.

Question 13 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 14**(1 point)

*Saved*

Cyberhygiene is a term that defines security practices limited to endpoints.

Question 14 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 15**(1 point)

*Saved*

Global positioning system (GPS) attacks against U.S. drones have allegedly caused the drones to attempt landing in the wrong place. This is an example of which type of attack?

Question 15 options:

|  |  |
| --- | --- |
|  | Attacks that require the user or an administrator to take action |
|  | Attacks that use the endpoint's normal function against it |
|  | Attacks that target the hardware or firmware of the device |
|  | Attacks against application software |

**Question 16**(1 point)

*Saved*

Distributed database systems (DDSs) are frequently used to control water and wastewater treatment.

Question 16 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 17**(1 point)

*Saved*

Which of the following best describes policies?

Question 17 options:

|  |  |
| --- | --- |
|  | Policies specify specific technologies that are used for computer network defense activities. |
|  | Policies focus on the direction and management of each individual department. |
|  | Policies are typically authorized by individual department heads in an organization. |
|  | Policies assign responsibility and set the overall tone for computer network defense activities. |

**Question 18**(1 point)

*Saved*

Which of the following incidents demonstrates that the boundaries of cyberwarfare may include direct physical harm?

Question 18 options:

|  |  |
| --- | --- |
|  | The Russia-Georgia War produced simultaneous cyberattacks against numerous government Web sites. |
|  | Tunisia's Jasmine Revolution included the hacking of usernames and passwords for the entire online population. |
|  | The Stuxnet worm infected at least 14 industrial sites in Iran, allowing the attackers to spy on the industrial systems. |
|  | Former U.S. Vice President Dick Cheney revealed that his doctors had disabled the wireless control capabilities of his pacemaker. |

**Question 19**(1 point)

*Saved*

Which of the following is the reason drone software and the systems used to control them are a target of attacks on drone platforms?

Question 19 options:

|  |  |
| --- | --- |
|  | Drone hardware is proprietary and closely guarded by the government. |
|  | Drone software is simplistic, making it easy to attack. |
|  | Drone software is commercially available for anyone to purchase. |
|  | Drone command-and-control system links are encrypted. |

**Question 20**(1 point)

*Saved*

Blacklisting builds a list of prohibited applications, files, sites, or other data or access.

Question 20 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 21**(1 point)

*Saved*

The Aurora malware was specifically designed to attack the Siemens Simatic S7-300 PLC's firmware.

Question 21 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 22**(1 point)

*Saved*

The most common type of endpoint from a cybersecurity perspective is the mobile phone.

Question 22 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 23**(1 point)

*Saved*

Organizations such as the U.S. government's U.S. Computer Emergency Readiness Team (US-CERT) provide which of the following?

Question 23 options:

|  |  |
| --- | --- |
|  | counter intelligence |
|  | internal federal emergency alerts |
|  | information sharing |
|  | cyberwarfare strategies |

**Question 24**(1 point)

*Saved*

When specific accesses must be blocked, or when the list of known files is already established, which of the following is most effective?

Question 24 options:

|  |  |
| --- | --- |
|  | whitelisting |
|  | redlisting |
|  | blacklisting |
|  | greylisting |

**Question 25**(1 point)

*Saved*

Most disk encryption systems that aren't built in to the disk itself are vulnerable to which of the following attacks?

Question 25 options:

|  |  |
| --- | --- |
|  | identity-spoofing |
|  | side-channel |
|  | eavesdropping |
|  | teardrop |

**Question 26**(1 point)

*Saved*

The root of most defensive strategies is a cyberdefense policy.

Question 26 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 27**(1 point)

*Saved*

What percentage of military aircraft functions in recently developed models are handled by software?

Question 27 options:

|  |  |
| --- | --- |
|  | 80 |
|  | 10 |
|  | 45 |
|  | 65 |

**Question 28**(1 point)

*Saved*

Which of the following is a sensor that provides reporting back to the central data collection system in Supervisory Control and Data Acquisition Systems (SCADA) systems?

Question 28 options:

|  |  |
| --- | --- |
|  | Trusted Platform Module |
|  | remote telemetry unit |
|  | human machine interface |
|  | programmable logic controller |

**Question 29**(1 point)

*Saved*

Which of the following is the main reason industrial control systems (ICSs) are often not as well secured as a traditional computing infrastructure?

Question 29 options:

|  |  |
| --- | --- |
|  | ICS systems have high requirements for stability and continuous operations. |
|  | ICS systems are older, legacy systems that cannot be secured or patched. |
|  | ICS systems are installed on proprietary hardware requiring vendor support. |
|  | ICS systems have high requirements for visibility and sporadic operations. |

**Question 30**(1 point)

*Saved*

An industrial control system (ICS) includes the devices and systems that control industrial production and operation.

Question 30 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 31**(1 point)

*Saved*

Which of the following is the primary reason personal computers provide attackers with a multitude of attack options?

Question 31 options:

|  |  |
| --- | --- |
|  | Because hardware for personal computers is relatively specialized. |
|  | Personal computers have far fewer security features than servers. |
|  | Because the software personal computers run is usually commercially available. |
|  | Personal computers are not made to withstand most attacks. |

**Question 32**(1 point)

*Saved*

The typical layers of defense for a computer workstation start at which level?

Question 32 options:

|  |  |
| --- | --- |
|  | firmware level |
|  | operating system level |
|  | network level |
|  | application level |

**Question 33**(1 point)

*Saved*

Which of the following is part of the U.S. Department of Defense's (DoD's) process to provide a defensive endpoint strategy?

Question 33 options:

|  |  |
| --- | --- |
|  | Employ a passive cyberdefense capability. |
|  | Maintain the current state of cyberhygiene techniques. |
|  | Strengthen workforce communications to deter and mitigate insider threats. |
|  | Utilize existing defense operating concepts and computing architectures. |

**Question 34**(1 point)

*Saved*

Embedded systems create unique challenges for defenders because security standards are rare or nonexistent for most embedded systems.

Question 34 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 35**(1 point)

*Saved*

Security standards define the settings and options a system, application, or other part of an endpoint system has in place.

Question 35 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 36**(1 point)

*Saved*

Which of the following is an example of firmware?

Question 36 options:

|  |  |
| --- | --- |
|  | operating system software on a PLC |
|  | an industrial control system |
|  | a program stored in random access memory |
|  | software that operates a pacemaker |

**Question 37**(1 point)

*Saved*

Which of the following includes awareness on the part of individuals in the U.S. Department of Defense (DoD), software and operating system updates, cybersecurity practices for users and administrators, and configuration management? It is critical to the DoD's cyberspace operations endpoint strategy.

Question 37 options:

|  |  |
| --- | --- |
|  | war games |
|  | cyberhygiene |
|  | heuristics |
|  | decisive engagement |

**Question 38**(1 point)

*Saved*

Many of the most successful attacks against endpoints in cyberwar have been \_\_\_\_\_\_\_ based.

Question 38 options:

|  |  |
| --- | --- |
|  | malware |
|  | denial of service (DoS) |
|  | phishing |
|  | man-in-the-middle (MITM) |

**Question 39**(1 point)

*Saved*

The U.S. Future Force Warrior design provided monitoring of individual soldiers with \_\_\_\_\_\_\_.

Question 39 options:

|  |  |
| --- | --- |
|  | e-readers |
|  | pen-based webcams |
|  | advanced cyberwarfare tools |
|  | helmet-mounted displays |

**Question 40**(1 point)

*Saved*

Which of the following best describes the role of central management systems?

Question 40 options:

|  |  |
| --- | --- |
|  | They are used to make changes and updates to systems from a single, central location. |
|  | They are used to define the settings and options a system has in place. |
|  | They are used to apply one or more prebuilt configuration templates to a device. |
|  | They are used to apply patches and updates to a device. |