|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | About how many unified cyber security jobs are expected by the year 2022 ? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | 180,000 |  |
| Option 2 | 180 Million |  |
| Option 3 | 1.8 Million | Y |
| Option 4 | There is expected to a surplus of available skills by 2022. |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Jeff Crime described 5 challenges in security today. Which three (3)  of these are challenges because their numbers are increasing rapidly? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Threats | Y |
| Option 2 | Available analysts |  |
| Option 3 | Available time | Y |
| Option 4 | Needed knowledge | Y |
| Option 5 | Alerts |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which is the National Institute of Standards (NIST) definition of  Cyber security? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | The measures taken to protect governmental and military computer and weapons  systems from unauthorized use, alteration, disruption or destruction. |  |
| Option 2 | The protection of information systems from unauthorized access, use  disclosure, disruption, modification, or destruction in order to provide  confidentiality, integrity, and availability | Y |
| Option 3 | The state of being protected against the criminal or unauthorized use of electronic  data, or the measures taken to achieve this. |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which three (3) are components of the CIA Triad? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Integrity | Y |
| Option 2 | Confidentiality | Y |
| Option 3 | Durability |  |
| Option 4 | Availability | Y |
| Option 5 | Access |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | True or False: Application Gateways are an effective way to control  which individuals can establish telnet connections through the gateway | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | True | Y |
| Option 2 | False |  |
| Option 3 |  |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Why are XML gateways used? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | XML packet headers are different from that of other protocols and often confuse  conventional firewalls. |  |
| Option 2 | XML traffic cannot pass through a conventional firewall. |  |
| Option 3 | XML traffic passes through conventional firewalls without inspection | Y |
| Option 4 | Conventional firewalls attempt to execute  XML code as instructions to the firewall. |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which three (3) things are True about Stateless firewalls? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | They maintain tables that allow them to compare current Packets with Previous  packets. |  |
| Option 2 | They are faster than Stateful firewalls | Y |
| Option 3 | They filter packets based upon Layer3 and 4 information only (IP address  and Port number) | Y |
| Option 4 | They are also known as packet filtering firewall | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which is not included as part of the IT Governance process? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Tactical Plans |  |
| Option 2 | Policies |  |
| Option 3 | Audits | Y |
| Option 4 | Procedures |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Trudy reading Alices message to Bob is a violation of which aspect  of the CIA Triad? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Authentication |  |
| Option 2 | Availability |  |
| Option 3 | Confidentiality | Y |
| Option 4 | Integrity |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | A hash is a mathematical algorithm that helps assure which aspect  of the CIA Triad? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Integrity |  |
| Option 2 | Confidentiality | Y |
| Option 3 | Availability |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | A successful DOS attack against your company's servers is a  violation of which aspect of the CIA Triad? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Availability | Y |
| Option 2 | Integrity |  |
| Option 3 | Confidentiality |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | How would you classify a piece of malicious code designed collect  data about a computer and its users and then report that back to a malicious  actor? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Adware |  |
| Option 2 | Spyware | Y |
| Option 3 | Worms |  |
| Option 4 | Virus |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | A large scale Denial of Service attack usually relies Upon which of  the following? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | A botnet | Y |
| Option 2 | A key logger |  |
| Option 3 | Logic Bombs |  |
| Option 4 | Trojan Horses |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Antivirus software can be classified as which form of threat control? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Passive controls |  |
| Option 2 | Active controls |  |
| Option 3 | Administrative controls |  |
| Option 4 | Technical controls | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Alice sends an encrypted message to Bob but it is intercepted by  Trudy, Trudy cannot read it so, in anger she deletes it without allowing its  delivery to Bob. Which precept of the CIA Triad would have been violated? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Confidentiality |  |
| Option 2 | Availability | Y |
| Option 3 | All of the above |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Alice sends an encrypted message to Bob but it is intercepted by  Trudy. Trudy cannot read it but forwards it on to Bob from an anonymous address she controls. Which precept of the CIA Triad would have been violated? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Integrity | Y |
| Option 2 | Availability |  |
| Option 3 | All of the above |  |
| Option 4 | None |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | **A major metropolitan police department gets a warrant from a**  **judge to hack into the computer of a suspected crime boss. A skilled penetration tester working for the department conducts the hack and retrieves incriminating evidence. What color hat does this officer wear?** | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | A White Hat |  |
| Option 2 | A Black Hat |  |
| Option 3 | A Gray Hat | Y |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | TCP sequence numbers are protected by which of the following means? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Data leakage prevention |  |
| Option 2 | Randomness |  |
| Option 3 | Complicated selection |  |
| Option 4 | All of the above | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | True or False: The accidental disclosure of confidential data by an employee is considered a legitimate organizational threat | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | True | Y |
| Option 2 | False |  |
| Option 3 |  |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | True or False: The accidental disclosure of confidential information by an employee is considered an attack. | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | False | Y |
| Option 2 | True |  |
| Option 3 |  |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | A replay attack and a denial of service attack are examples of which? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Origin attack |  |
| Option 2 | Passive attack |  |
| Option 3 | Masquerade attack |  |
| Option 4 | Security architecture attack | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | True or False: An application that runs on your computer without your authorization but does no damage to the system is not considered malware. | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | False | Y |
| Option 2 | True |  |
| Option 3 |  |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** | How would you classify a piece of malicious code designed to cause damage and Spreads from one counter to another by attaching itself to files but requires human actions in order to replicate? | |
| **Question** |  | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Virus | Y |
| Option 2 | Worms |  |
| Option 3 | Trojan Horses |  |
| Option 4 | Spyware |  |
| Option 5 | adware |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | How would you classify a piece of malicious code designed collect data about a  computer and its users and then report that back to a malicious actor? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Spyware | Y |
| Option 2 | worms |  |
| Option 3 | Virus |  |
| Option 4 | Adware |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which of the following measures can be used to counter a mapping attack? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Record traffic entering the network |  |
| Option 2 | Look for suspicious activity like IP addresses or ports being scanned sequentially. |  |
| Option 3 | Use a host scanner and keep an inventory of hosts on your network. |  |
| Option 4 | All of the above. | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | In order for a network card (NIC) to engage in packet sniffing, it must be running in which mode? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Promiscuous | Y |
| Option 2 | Sniffer |  |
| Option 3 | Inspection |  |
| Option 4 | Open |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which countermeasure can be helpful in combating an IP Spoofing attack? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Enable IP Packet Authentication filtering |  |
| Option 2 | Ingress filtering y | Y |
| Option 3 | Keep your certificates up to-date |  |
| Option 4 | Enable the IP Spoofing feature available in most commercial antivirus software. |  |
| Option 5 | All of the above. |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which is not one of the phases of the intrusion kill chain? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Delivery |  |
| Option 2 | Command and Control |  |
| Option 3 | Installation |  |
| Option 4 | Activation | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which social engineering attack involves a person instead of fa system such as an  email server? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Vishing | Y |
| Option 2 | Phishing |  |
| Option 3 | Cyberwarfare |  |
| Option 4 | Spectra |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which of the following is an example of a social engineering attack? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Setting up a web site offering free games, but infecting the downloads With  malware. |  |
| Option 2 | Logging in to the Army s missile command computer and launching a nuclear  Weapon. |  |
| Option 3 | Sending someone an email with a Trojan Horse attachment |  |
| Option 4 | observe him logging into his corporate account. | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which hacker organization hacked into the Democratic National Convention and released Hillary Clinton's emails? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Guardians of the Peace |  |
| Option 2 | Anonymous |  |
| Option 3 | Fancy Bears | Y |
| Option 4 | Syrian Electronic Army |  |
| Option 5 | All of the above |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | What challenges are expected in the future? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Enhanced espionage from more countries |  |
| Option 2 | Far more advanced malware |  |
| Option 3 | New consumer technology to exploit |  |
| Option 4 | All of the above | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Why are cyber attacks Using SWIFT So dangerous? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | SWIFT s the protocol used to transmit all diplomatic telegrams between governments around the world |  |
| Option 2 | SWIFT is the protocol used by all banks to transfer money | Y |
| Option 3 | SWIFT is the flight plan and routing system used by all cooperating nations for  international commercial flights |  |
| Option 4 | SWIFT is the protocol used by all US healthcare providers to encrypt medical  records |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which statement best describes Authentication? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Assurance that the communicating entity is the one claimed | Y |
| Option 2 | Prevention of unauthorized use of a resource |  |
| Option 3 | Protection against denial by one of the parties in communication |  |
| Option 4 | Assurance that a resource can be accessed and used |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Trusted functionality, security labels, event detection, security audit trails and security recovery are all examples of which type of security mechanism? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Contingent security mechanism |  |
| Option 2 | Passive security mechanism | Y |
| Option 3 | External security mechanism |  |
| Option 4 | Active security mechanism |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | If an organization responds to an intentional threat, that threat is now classified as what? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | An open case |  |
| Option 2 | An active threat |  |
| Option 3 | An attack | Y |
| Option 4 | A malicious threat |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which type of actor was not one of the four types of actors mentioned in the video  A brief overview of types of 3ctors and their motives? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Black Hats | Y |
| Option 2 | Internal |  |
| Option 3 | Hacktivists |  |
| Option 4 | Hackers |  |
| Option 5 | Governments |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | A political motivation is often attributed to which type of actor? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Security Analysts |  |
| Option 2 | Hacktivist | Y |
| Option 3 | Internal |  |
| Option 4 | Hackers |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | The video Hacking organizations called out several countries with active government sponsored hacking operations in effect Which one or these was among those named? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Israel | Y |
| Option 2 | South Africa |  |
| Option 3 | Egypt |  |
| Option 4 | Canada |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which of these is not a known hacking organization? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Fancy Bears |  |
| Option 2 | Syrian Electronic Army |  |
| Option 3 | The Ponemon Institute | Y |
| Option 4 | Anonymous |  |
| Option 5 | Guardians of the Peace |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Which type of actor hacked the 2016 US Presidential Elections? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Hackers |  |
| Option 2 | Government | Y |
| Option 3 | Internal |  |
| Option 4 | Hacktivists |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | True or False: Passive attacks are easy to detect because the original messages are usually altered or undelivered. | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | False | Y |
| Option 2 | True |  |
| Option 3 |  |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | True or False: Authentication, Access Control and Data Confidentiality are all addressed by the ITU X.800 Standard | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | True |  |
| Option 2 | False | Y |
| Option 3 |  |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Cryptography, digital signatures, access controls and routing controls considered which? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Business Policy |  |
| Option 2 | Pervasive security mechanisms |  |
| Option 3 | Security Policy |  |
| Option 4 | Specific security mechanism | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | True or False: A tornado threatening a data center can be classified as an attack | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | False | Y |
| Option 2 | True |  |
| Option 3 |  |  |
| Option 4 |  |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Traffic flow analysis is Classified as which? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | A passive attack | Y |
| Option 2 | A masquerade attack |  |
| Option 3 | An active attack |  |
| Option 4 | An origin attack |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | How would you classify a piece of malicious code designed to cause damage, can self-replicate and spreads from one computer to another by attaching itself to files? | |
| **Option No** | **Option** | **Correct(Y)** |
| Trojan Horse | Trojan Horse | Y |
| Option 2 | Virus |  |
| Option 3 | Ransomware |  |
| Option 4 | Worm |  |
| Option 5 | Adware |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** | Botnets can be used to orchestrate which form of attack? | |
| **Question** |  | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | DDoS attacks |  |
| Option 2 | Phishing attacks |  |
| Option 3 | As a Malware launchpad |  |
| Option 4 | All of the above | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | Policies and training can be classified as which form of threat control? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | Administrative controls | Y |
| Option 2 | Passive controls |  |
| Option 3 | Technical controls |  |
| Option 4 | Active controls |  |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |

|  |  |  |
| --- | --- | --- |
| **Question Type** | Basic MCQ | |
| **Question number** |  | |
| **Question** | A flood of maliciously generated packets swamp a receivers network interface preventing it from responding legitimate traffic. This is characteristic of which form of attack? | |
| **Option No** | **Option** | **Correct(Y)** |
| Option 1 | A Ransomware attack |  |
| Option 2 | A Masquerade attack |  |
| Option 3 | A Trojan Horse |  |
| Option 4 | A Denial of Service (DOS) attack | Y |
| Option 5 |  |  |
| **Question Metadata** | **Difficulty Level** | **Bloom’s Taxonomy** |
|  | Easy | Apply |
| **Tags** |  | |
| **Subject** |  | |
| **Topic** |  | |
| **Sub Topic** |  | |
| **Code Editor** |  | |
| **Solution No** | **Solution** | **Best(Y)** |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |
| Solution 1 |  |  |
| **Hint No** | **Hint** | |
| Hint 1 |  | |