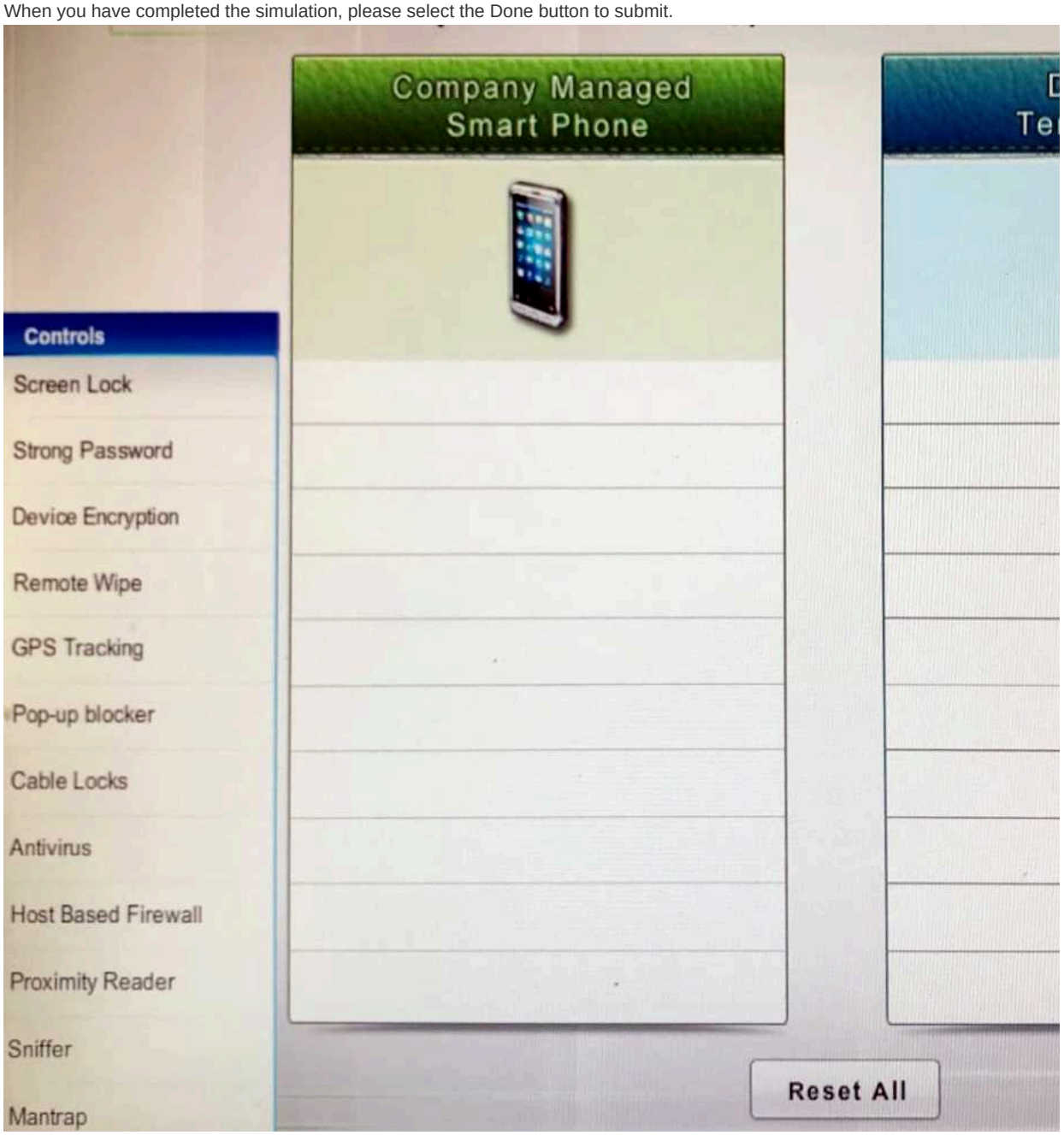
CompTIA Linux+ Exam (2021)

1. DRAG DROP (Drag and Drop is not supported)
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled.
When you have completed the simulation, please select the Done button to submit.



A. See Explanation section for answer.

Answer(s): A

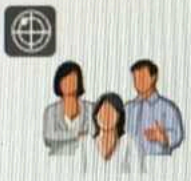
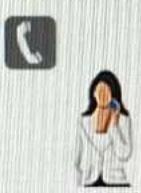
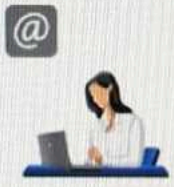
---

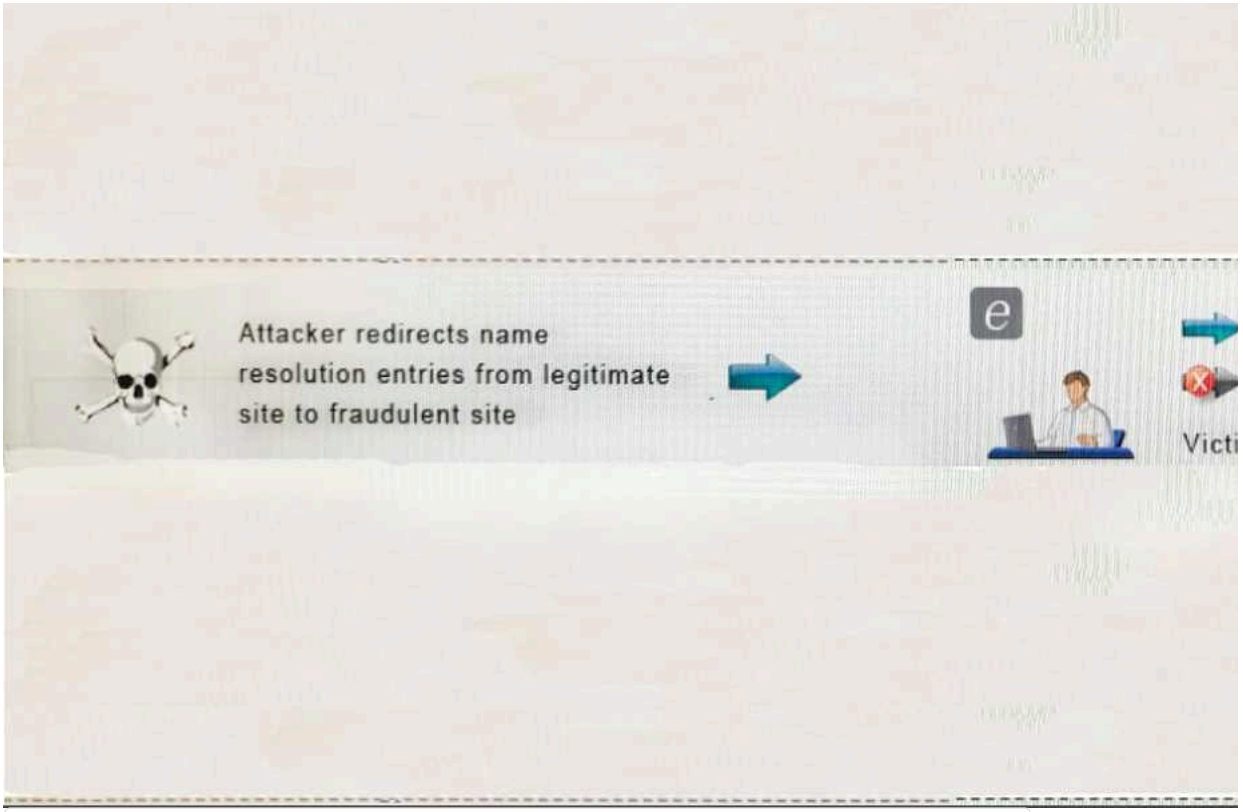
2. HOTSPOT (Drag and Drop is not supported)
Select the appropriate attack from each drop down list to label the corresponding illustrated attack.
Instructions: Attacks may only be used once, and will disappear from drop down list if selected.

When you have completed the simulation, please select the Done button to submit.

Attacks

Instructions: Attacks may only be used once, and will disappear fr
When you have completed the simulation, please sele

Attack Vector	Targ
 Attacker gains confidential company information	 Targ and
 Attacker posts link to fake AV software	 Multiple social networks  Broa
 Attacker collecting credit card details	 Phon
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broa



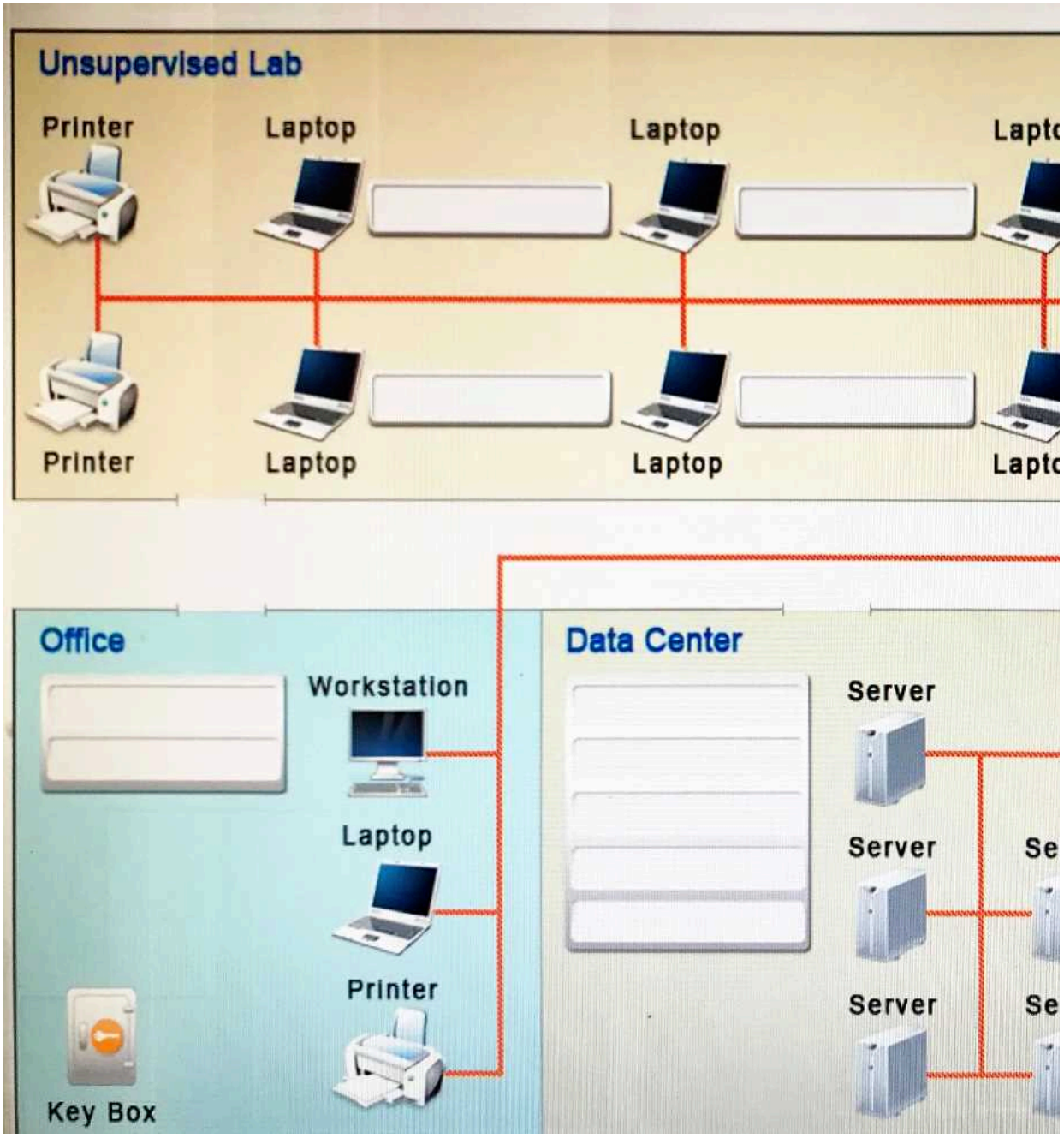
A. See Explanation section for answer.

Answer(s): A

---

3. DRAG DROP (Drag and Drop is not supported)
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter.

When you have completed the simulation, please select the Done button to submit.



A. See Explanation section for answer.

Answer(s): A

---

4. Which of the following would a security specialist be able to determine upon examination of a server's certificate?

A. CA public key

B. Server private key

C. CSR

D. OID

Answer(s): D

---

5. A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666.
Which of the following should the security analyst do to determine if the compromised system still has an active connection?

A. tracert

B. netstat

C. ping

D. nslookup

Answer(s): B

---

6. Multiple organizations operating in the same vertical wants to provide seamless wireless access for their employees as they visit the other organizations.
Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

A. Shibboleth

B. RADIUS federation

C. SAML

D. OAuth

E. OpenID connect

Answer(s): B

---

7. Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

A. Sustainability

B. Homogeneity

C. Resiliency

D. Configurability

Answer(s): C

---

8. In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand.
Which of the following characteristics BEST describes what the CIO has requested?

A. Elasticity

B. Scalability

C. High availability

D. Redundancy

Answer(s): A

---

9. A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system.
Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX

B. PEM

C. DER

D. CER

Answer(s): B

---

10. Which of the following attacks specifically impacts data availability?

A. DDoS

B. Trojan

C. MITM

D. Rootkit

Answer(s): A

---

11. A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients.
Which of the following should the analyst implement to meet these requirements? (Select two.)

- [ ] A. Generate an X.509-compliant certificate that is signed by a trusted C
- [ ] B. Install and configure an SSH tunnel on the LDAP server.
- [ ] C. Ensure port 389 is open between the clients and the servers using the communication.
- [ ] D. Ensure port 636 is open between the clients and the servers using the communication.
- [ ] E. Remote the LDAP directory service role from the server.

Answer(s): A D

---

12. Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?

A. Competitor

B. Hacktivist

C. Insider

D. Organized crime.

Answer(s): A

---

13. A penetration tester is crawling a target website that is available to the public.
Which of the following represents the actions the penetration tester is performing?

A. URL hijacking

B. Reconnaissance

C. White box testing

D. Escalation of privilege

Answer(s): B

---

14. Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select two.)

- [ ] A. Rainbow table attacks greatly reduce compute cycles at attack time.
- [ ] B. Rainbow tables must include precomputed hashes.
- [ ] C. Rainbow table attacks do not require access to hashed passwords.
- [ ] D. Rainbow table attacks must be performed on the network.
- [ ] E. Rainbow table attacks bypass maximum failed login restrictions.

Answer(s): B E

---

15. Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

A. Error handling to protect against program exploitation

B. Exception handling to protect against XSRF attacks.

C. Input validation to protect against SQL injection.

D. Padding to protect against string buffer overflows.

Answer(s): C

---

16. A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.
The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections.
Which of the following would BEST accomplish these goals?

A. Require the SFTP protocol to connect to the file server.

B. Use implicit TLS on the FTP server.

C. Use explicit FTPS for connections.

D. Use SSH tunneling to encrypt the FTP traffic.

Answer(s): C

---

17. Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

A. The recipient can verify integrity of the software patch.

B. The recipient can verify the authenticity of the site used to download the patch.

C. The recipient can request future updates to the software using the published MD5 value.

D. The recipient can successfully activate the new software patch.

Answer(s): A

---

18. Refer to the following code:

```
public class rainbow {
     public static void main (String [] args) {
          object blue = null;
          blue.hashcode (); }
}
```

Which of the following vulnerabilities would occur if this is executed?

A. Page exception

B. Pointer deference

C. NullPointerException

D. Missing null check

Answer(s): D

---

19. Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions:
Shut down all network shares.
Run an email search identifying all employees who received the malicious message. Reimage all devices belonging to users who opened the attachment. Next, the teams want to re-enable the network shares.
Which of the following BEST describes this phase of the incident response process?

A. Eradication

B. Containment

C. Recovery

D. Lessons learned

Answer(s): C

---

20. An organization has determined it can tolerate a maximum of three hours of downtime.
Which of the following has been specified?

A. RTO

B. RPO

C. MTBF

D. MTTR

Answer(s): A
