EC-Council Licensed Penetration Tester

Methodology: Data Leakage Penetration Testing

Penetration Tester:			
Organization:			
Date:		**Location:**	

Test 1: Check the physical availability of USB devices

Target Organization	
URL	
Physical Availability of USB Devices in Device Manager	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Step 2: Check whether the USB drive is enabled

Target Organization		
URL		
USB Drive is Enabled or Disabled	☐ Yes	☐ No
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 3: Try to Enable USB

Target Organization	
URL	
Enabling USB Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 4: Check whether the USB asks for password

Target Organization		
URL		
Check Whether the Device asks for Authentication	☐ Yes	☐ No
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 5: Check whether Bluetooth is enabled

Target Organization		
URL		
Check Bluetooth is Enabled	☐ Yes	☐ No
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 6: Check if FireWire is enabled

Target Organization		
URL		
Check Whether the FireWire Port is Enabled	☐ Yes	☐ No
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 7: Check if the FTP ports 21 and 22 are enabled

Target Organization		
URL		
Check if FTP Ports are Enabled	☐ Yes	☐ No
Tools/Services Used	1. _____	
	2. _____	
	3. _____	
	4. _____	
	5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 8: Check whether any memory slot is available and enabled in systems

Target Organization		
URL		
Check Whether Any Memory Slot is Enabled or not	☐ Yes	☐ No
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 9: Check whether employees are using camera devices within the restricted areas

Target Organization	
URL	
Illegal use of Camera Devices Leads to	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Check whether systems have any camera driver installed

Target Organization		
URL		
Find in Systems that any Camera Driver Installed	☐ Yes	☐ No
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 11: Check whether anti-spyware and anti-trojans are enabled

Target Organization	
URL	
Anti-Spyware and Anti-Trojans Are Enabled	☐ Yes ☐ No
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

Test 12: Check whether the encrypted data can be decrypted

Target Organization	
URL	
Data Encryption Techniques Protect	1.
	2.
	3.
	4.
	5.
Tools/Services Used	1.
	2.
	3.
	4.
	5.

Results Analysis:

Test 13: Check if the internal hardware components are locked

Target Organization		
URL		
Internal Hardware Components are Locked	☐ Yes	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 14: Check whether size of mail and mail attachments is restricted

Target Organization	
URL	
Restrict the Size Limits for mail and mail attachments	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: