EC-Council Licensed Penetration Tester

Methodology: Physical Security Penetration Testing

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

Test 1: Overview from outside

Target Organization	
URL	
Physical Location	
Equipment Used	
Inner View of the Office Premises	
Information Gathered on Security Controls and Work Done Inside the Office through Telephotography from Outside	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Map the physical perimeter

Target Organization	
URL	
Information Gathered about the Target's Physical Location Using Google Maps	1. 2. 3. 4. 5.
Identified	
☐ Ceiling Strength:	
☐ Basement:	
☐ Access Policies:	
☐ Types of Windows Used:	
☐ Doors Used:	
☐ Types of Locks Used:	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Map the possible entrances

Target Organization		
URL		
Physical Location		
Located Different Entrances		
☐ Through Doors	☐ Through Windows	☐ Fire Exits
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4: Check whether the entry points are guarded and monitored

Target Organization	
URL	
Physical Location	
List of Guarded and Unguarded Entry Points	1. 2. 3. 4. 5.
Guard Patrol Routines for Holes in the Coverage	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Try to bypass the security checks

Target Organization		
URL		
Physical Location		
Find Out the Types of Questions Asked by Guards	1. 2. 3. 4. 5.	
High-Security Check to Enter the Premises	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Attempt lock picking techniques to penetrate locks used by the gates, door, and closets

Target Organization	
URL	
Physical Location	
Locking Devices Used	
Keys Accepted by the Locks Used in Organizations	
☐ Mechanical Locks	☐ Electromagnetic Locks
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Intercept and analyze guard communication

Target Organization	
URL	
Guards' Communication - Intercepted and Recorded	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Check physical access controls implemented in the facilities

Target Organization	
URL	
Physical Location	
How Physical Access to Facilities is Controlled for	
☐ Employees:	
☐ Contractors/Stakeholders:	
☐ Trainees:	
☐ Visitors:	
Alternative Access Control Granted to All Individuals	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Test "after office hours" entry methods

Target Organization			
URL			
Record the After Office Hours Entry Made into the Office			
Employees Swiped in Before Entering the Office		☐ YES	☐ NO
Formalities Followed for Visitors Entry	1. 2. 3. 4. 5.		
Tools/Services Used	1. 2. 3. 4. 5.		

Results Analysis:

Test 10: Check if CCTV and motion sensors are implemented

Target Organization		
URL		
Physical Location		
Coverage of CCTV		
Successful in Bypassing Sensors	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 11: Dress as a FedEx/UPS employee and try to gain access to the building

Target Organization		
URL		
Physical Location		
Successful in Getting Access	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 12: Attempt to use fake ID to gain access

Target Organization		
URL		
Physical Location		
Successful in Entering Restricted Areas by Producing Fake ID	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 13: Attempt piggybacking on guarded doors

Target Organization		
URL		
Physical Location		
Successful in Attempting Piggybacking on Guarded Doors	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 14: Check windows/doors for visible alarm sensors

Target Organization		
URL		
Physical Location		
Windows/Doors Do Not Allow Place for an Intruder to Hide	☐ True	☐ False
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 15: Attempt dumpster diving outside the company trash area

Target Organization		
URL		
Physical Location		
Dumpster Diving Possible Outside the Company Trash Area	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16: Create a map of the company's floor plan

Target Organization	
URL	
Plan of Each Floor's Infrastructure	1. 2. 3. 4. 5.
Number of People Working on Each Floor and Kind of Work They Do	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17: Use active high frequency voice sensors to hear private conversation among the company's staff

Target Organization		
URL		
Physical Location		
Private Conversation Distinct	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 18: Find vulnerable fire detection systems

Target Organization	
URL	
Physical Location	
Fire Alarm System Policies and Procedures Within the Company	1. 2. 3. 4. 5.
List vulnerable equipment and confidential information that can be Stolen or Destroyed	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 19: Find breach in air conditioning systems

Target Organization	
URL	
Physical Location	
Possible Penetration Attempts in Air Conditioning Systems	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 20: Electromagnetic interception

Target Organization	
URL	
Sensitive Information Gathered through Electromagnetic Interception	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 21: Check for receptionist/guard leaving lobby

Target Organization	
URL	
Physical Location	
Note the Timings of Receptionist/Guard's Absence	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 22: Check for accessible printers in the lobby – print test page

Target Organization		
URL		
Physical Location		
Test Page Secured as an Evidence	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 23: Obtain phone/personnel listing from the lobby receptionist

Target Organization	
URL	
Physical Location	
Obtained Phone/ Personnel Listing from the Lobby Receptionist	1. 2. 3. 4. 5.
Obtained Phone Extension Numbers of the Employees from the Receptionist Using Your Social Engineering Skills	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 24: Listen to employee conversation in communal areas/cafeteria

Target Organization	
URL	
Physical Location	
Information Gathered from Employee Conversation	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 25: Check areas for sensitive information

Target Organization	
URL	
Physical Location	
Sensitive Information Gathered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 26: Try to shoulder surf users logging on

Target Organization	
URL	
Physical Location	
Extracted Credentials	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 27: Test if the company has a physical security policy

Target Organization	
URL	
Physical Location	
Determined Company's Physical Security Policy	
☐ Visitor Policy:	
☐ Fire Policy:	
☐ Disposal Policy:	
☐ Identification Card Policy:	
☐ Access to Restricted Areas:	
☐ Internal and External Access Controls:	
☐ Security Officers' Responsibilities:	
☐ Ensuring Protection of Personnel and Assets:	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 28: Try to enter into the secure rooms through ceiling space

Target Organization		
URL		
Physical Location		
Ceiling of the Secured Rooms Secure Enough	☐ True	☐ False
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 29: Assess the value of the physical assets

Target Organization	
URL	
Physical Location	
List of Physical Assets which Organization Possesses	
☐ Information Storage Devices:	
☐ Wireless Devices:	
☐ Communication Wires:	
☐ Company Buildings:	
☐ Building Perimeter and Surroundings:	
☐ Air Conditioner and Ducts:	
☐ CCTVs:	
☐ Network Devices:	
☐ Computer Equipment:	
☐ Fire Extinguishers:	
☐ Fax and Photostat Machines:	

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 30: Check access authorization list

Target Organization	
URL	
Physical Location	
Analysis of the Access Authorization List	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 31: Check how these documents are protected

Target Organization		
URL		
Physical Access Measures to Prevent the Unauthorized Access to Paper Documents	1. 2. 3. 4. 5.	
Sensitive Paper Documents Shredded Before they are Thrown Away	☐ True	☐ False
Impact to the Company if Unauthorized Individuals Accessed Sensitive Documents	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 32: Test if any valuable paper documents are kept at the facility

Target Organization		
URL		
Physical Location		
Sensitive Documents Kept in Safes and Lockers	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 33: Test people in the facility

Target Organization		
URL		
Physical Location		
Facility Possess Organization Identification Cards	☐ YES	☐ NO
Identification Policies Coverage	1. 2. 3. 4. 5.	
Devices Used to Test Restricted Areas	1. 2. 3. 4.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 34: Penetrate server rooms, cabling, and wires

Target Organization	
URL	
Physical Location	
Level of Security Given to Server Rooms	
Information that can be Gathered by Gaining Physical Access to the Server Room	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 35: Test for radio frequency ID (RFID)

Target Organization		
URL		
Physical Location		
RFID Tags Identified	☐ YES	☐ NO
RFID is Encrypted	☐ YES	☐ NO
Modified Data Present in the RFID Tag	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 36: Check for the active network jacks in company lobby and meeting rooms

Target Organization		
URL		
Physical Location		
Identify the Active Network Jacks	☐ YES	☐ NO
Connection to the Active Network Jacks in Company Lobby through Access Point Successful	☐ YES	☐ NO
Breached the Physical Security and Entered in the Company's Work Area Successful	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 37: Check for sensitive information lying around meeting rooms

Target Organization	
URL	
Physical Location	
Papers/Electronic Media Left in Conference Rooms	1. 2. 3. 4.
Notes or Other Important Details Lying in the Meeting Rooms	1. 2. 3. 4.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 38: Document everything

Target Organization	
URL	
Physical Location	
Document All Your Findings by Mapping the Physical Perimeter	
☐ Locks Used by the Gates, Doors and Closets:	
☐ Server Rooms, Cabling, and Wires:	
☐ Fire Detection Techniques and Air Conditioning System:	
☐ Electromagnetic Interception and Physical Assets:	
☐ Physical Security Policy and Risk Test:	
☐ Valuable Documents in the Facilities:	
☐ Employee Access and Physical Access to Facilities:	
☐ Documented Process and Authorized People:	

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: