EC-Council Licensed Penetration Tester

Methodology: Surveillance Camera Penetration Testing

Penetration Tester:		
Organization:		
Date:	Location:	

Test 1: Check the type of surveillance equipment used

Target Organization	
URL	
Type of Surveillance Camera Used in the Organization	
☐ Bullet Camera	☐ PC-Based Surveillance System
☐ IP Camera	☐ All-in-One Camera Systems
☐ Board Cameras	☐ Others
Depending on the type of surveillance camera, which of the following is used, and is required for an organization	
☐ Hidden Cameras:	
☐ Closed Circuit Television (CCTV) Systems:	
☐ Low-Light Surveillance:	
☐ Long-Range Surveillance:	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

Test 2: Check whether cameras are deployed in critical areas

Target Organization		
URL		
Surveillance Equipment is Mounted in Critical Areas	☐ YES	☐ NO
Provides Required Area Coverage	☐ YES	☐ NO
Audio Recording Enabled	☐ YES	☐ NO
Desired Footage Tone	☐ YES	☐ NO
Tools/Services Used	1. _____	
	2. _____	
	3. _____	
	4. _____	
	5. _____	

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 3: Check the video transmission medium

Target Organization	
URL	
Video Transmission Medium for Various Types of Security Cameras	1. 2. 3. 4. 5.
Components of the Surveillance System used as Effective Means of Video Transmission	1. 2. 3. 4. 5.
Connectivity of the Video Recording Signal in Activated Mode ☐ YES ☐ NO	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 4: Attempt tampering with the wire/wireless connectivity to the cameras

Target Organization	
URL	
Possibility of Tampering the Wire/Wireless Connectivity to the Cameras	☐ YES ☐ NO
Camera Resolution and the Range with Usage of Different Lenses	1. 2. 3.
Weatherproofing Measures Taken to Protect the Wireless Equipment	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

_____

_____

_____

_____

_____

Test 5: Check the bandwidth available for the surveillance cameras

Target Organization	
URL	
Amount of Bandwidth Used by Network Surveillance Cameras	

Factors on which the Bandwidth Requirement of a Surveillance System Depends	1. 2. 3.	
Dedicated Bandwidth Available for the Surveillance System	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Check the settings of the monitoring computer

Target Organization	
URL	
Efficiency of the Security Camera Monitor	

Type of Security Camera Monitor Used		
Set-up Camera	**System or Main Monitor**	**Spot Monitor**

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

Results Analysis:

_____

_____

_____

_____

_____

Test 7: Check video footage clarity

Target Organization	
URL	
Lighting and Resolution of the Footage	

Image Quality Meets Minimum Legal And Policy Requirements	☐ YES	☐ NO
Distance Between the Camera Fixed to the Wall or Ceiling is Proportionate to the Clarity of the Image	☐ YES	☐ NO

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

Results Analysis:

Test 8: Attempt changing video formats

Target Organization	
URL	
Results of Video Formats Testing	
Commonly Used Video Formats	
Used Security Surveillance Cameras are Supported by Certain Commonly Used Video Formats	☐ YES ☐ NO
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

Test 9: Scan for suspicious device drivers in the monitoring computer

Target Organization	
URL	
Scan Results for Devices Used to Monitor Video Surveillance Cameras for Suspicious Drivers	1. 2. 3. 4. 5.
Noticed Driver Interfere with the Working of DVR Systems	1. 2. 3.
Device Drivers being Used are Genuine	☐ YES ☐ NO
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Check the video viewing options

Target Organization	
URL	
Video Viewing Options	
Controls in the Main Screen	1. 2. 3.
Things to be Focused on to Get the Best Images and Video Recordings on the Security Camera	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Identify the possible threats while integrating video with other systems

Target Organization	
URL	
Identified Possible Threats while Integrating Video with Other Systems	
☐ Hardware Threats:	
☐ Electrical Threats:	
☐ Environmental Threats:	
☐ Maintenance Threats:	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

Test 12: Check if the footage storage duration meets the organization's requirements

Target Organization			
URL			
Organization making Valid Usage of Information Obtained from Surveillance Camera Footage	☐ YES		☐ NO
Factors that Determine Whether to Store Bulky Data or Video Footage Straight to the Hard Disks	1. 2. 3. 4. 5.		
Analysis of the Type of Video Storage Used	4. 5. 6. 7. 8.		
Tools/Services Used	1. 2. 3. 4. 5.		

Results Analysis:

Test 13: Check the optimization of DVR/NVR storage

Target Organization	
URL	
Features Included in Video Management System to Store Optimized Data for Security	
1.	6.
2.	7.
3.	8.
4.	9.
5.	10.

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

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 14: Check network settings of the DVR/NVR system

Target Organization	
URL	
Basics Steps to Check the Configuration of the DVR Network and a Computer with Remote Viewer software	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Check if all connections are working properly

Target Organization	
URL	
Devices Checked	1. 2. 3. 4. 5.
List of the Devices Not Working Properly	1. 2. 3. 4. 5.

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 16: Check who has local and remote access to the DVR/NVR

Target Organization	
URL	
Determined Local and Remote Access to DVR/NVR Systems through Surveillance Policy	
Analysis of DVR/NVR Access Logs	
Detected Unauthorized Attempt to Access DVR/NVR Systems	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 17: Scan the organization's network range to detect DVR systems

Target Organization	
URL	
Detected DVR Systems	
Scan Results of the Organization's Network Range	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18: Check if access to the DVR/NVR is protected

Target Organization			
URL			
Access to the DVR System is Protected	☐ YES		☐ NO
Type of Access Control Mechanisms Used			
☐ Physical Security		☐ System Access	
Strong Password Used for Administration	☐ True		☐ False
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____		

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 19: Try cracking DVR/NVR access passwords

Target Organization	
URL	
Target IP Address	
Protocol Used	
Attempt to Crack the DVR/NVR Access Password	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

_____