EC-Council Licensed Penetration Tester

Methodology: Social Engineering Penetration Testing

Penetration Tester:		
Organization:		
Date:	Location:	

Test 1: Attempt Social Engineering Using the Phone

Target Organization	
URL	
Person to Call	
Phone number to Dial	
Social Engineering Message	
Response from the Team	

Social Engineering Attempt Successful	☐ Yes	☐ No

Extracted Privilege Information (if successful)	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____

Results Analysis:

_____

_____

_____

_____

Test 2: Attempt social engineering by vishing

Target Organization		
URL		
Person to Interact		
Caller ID Used		
Social Engineering Message		
Response from the Victim		
Social Engineering Attempt Successful	☐ Yes	☐ No
Extracted Privilege Information (if successful)	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 3: Attempt social engineering using Email

Target Organization		
URL		
Victim Name		
E-mail Sent to the Victim	To:	
	From:	
	Subject:	
	Message:	
E-mail Response from the Victim	To:	
	From:	
	Subject:	
	Message:	
Extracted Privilege Information (if successful)	1.	
	2.	
	3.	
Tools/Services Used	1.	
	2.	
	3.	

Results Analysis:

Test 4: Attempt social engineering by using traditional mail

Target Organization	
URL	
Victim Name	
Mailing Address	
Letter to the Victim	
Response from the Victim	
Extracted Privilege Information (if successful)	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

_____

_____

_____

_____

_____

Test 5: Attempt social engineering in person

Target Organization	
URL	
Victim Name you will be Visiting	
Position	
Location and Address	
List for Questioning the Victim	1. 2. 3. 4.
Conversation you had with the Victim	
Extracted Privilege Information (if successful)	1. 2. 3. 4.
Tools/Services Used	1. 2. 3. 4.

Results Analysis:

Test 6: Attempt social engineering by Dumpster Diving

Target Organization	
URL	
Trash location	
List of Items Examined	1. 2. 3. 4. 5. 6. 7.
Extracted Privilege Information (if successful)	1. 2. 3. 4.
Tools/Services Used	1. 2. 3. 4.

Results Analysis:

Test 7: Attempt social engineering through Insider Accomplice

Target Organization	
URL	
Make an Accomplice by	☐ Bribing ☐ Date the person (if you look like Britney Spears or Eric Bana) ☐ Helping the person by understanding his needs ☐ Exchange for movie tickets, football games etc. ☐ Handing out gifts such as handphone
Name of the Accomplice	
Position	
Information Extracted from Accomplice	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

_____

Test 8: Attempt social engineering by Shoulder Surfing

Target Organization		
URL		
Name of the Victims	Shoulder Surfing Successful	
1.	☐ Yes	☐ No
2.	☐ Yes	☐ No
3.	☐ Yes	☐ No
Extracted Privilege Information	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 9: Attempt social engineering by Desktop Information

Target Organization		
URL		
Name of the Victims	**Desktop Social Engineering Successful**	
1.	☐ Yes	☐ No
2.	☐ Yes	☐ No
3.	☐ Yes	☐ No
Extracted Privilege Information	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 10: Attempt social engineering by Extortion and Blackmail

Target Organization	
URL	
List the Victims you will be Blackmailing	1. 2. 3. 4.
Position	
Location and Address	
Conversation you had with the Victim	
Extracted Privilege Information (if successful)	1. 2. 3. 4.
Tools/Services Used	1. 2. 3. 4.

Results Analysis:

Test 11: Attempt social engineering using Phishing Attacks

Target Organization		
URL		
Victim Name		
Information used for Phishing Attack		
Social Engineering using Phishing Attack Successful	☐ Yes	☐ No
Sensitive Information Obtained	1. _____ 2. _____ 3. _____ 4. _____	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____	

Results Analysis:

_____

_____

_____

_____

_____

Test 12: Attempt Identity Theft

Target Organization	
URL	
Victim Name	
Victim's Information Obtained to Perform Identity Theft	1. 2. 3. 4. 5.
Identity Theft Successful	☐ Yes ☐ No
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Try to obtain satellite imagery and building blueprints

Target Organization	
URL	
Address of the Target Organization	
List of the Extracted Information	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

_____

_____

_____

_____

_____

Test 14: Try to obtain the details of an employee from social networking sites

Target Organization	
URL	
Name of the Employee	
List of Social Networking Sites to Which an Employee is Associated	1. 2. 3. 4. 5.
Extracted Privileged Information (if successful)	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Use a telephone monitoring device to capture conversation

Target Organization	
URL	
Phone Numbers Tapped	1. 2. 3. 4. 5.
Extracted Privilege Information	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16: Use video recording tools to capture images

Target Organization		
URL		
Capturing Images using Video Recording Tools Successful	☐ Yes	☐ No
Extracted Privileged Information	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

_____

_____

_____

_____

_____

Test 17: Use a vehicle/asset tracking system to monitor motor vehicles

Target Organization		
URL		
Monitoring Motor Vehicles Successful	☐ Yes	☐ No
Details of Tracked Vehicle	1. 2. 3. 4. 5.	
Extracted Privilege Information	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

_____

_____

_____

_____

_____

Test 18: Identify "Disgruntled Employees" and engage in conversation to extract sensitive information

Target Organization	
URL	
Names of Disgruntled Employees	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Conversation you had with Disgruntled Employees	
Extracted Privilege Information	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____

Results Analysis:

_____

_____

_____

_____

Test 19: Document Everything

Target Organization	
URL	
Overall Results and Findings	
Tools/Services Used	1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.
	11.
	12.
	13.
	14.
	15.
	16.

Results Analysis: