EC-Council Licensed Penetration Tester

Methodology: Information Gathering

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

PENETRATION

LICENSED

TESTER

Test 1: Find the Company's URL

Target Organization		
URL Discovered	□ Yes	□ No
URL		
Sources Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2: Locate Internal URLs

Target Organization	
URL	
Internal URLs	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Identify a company’s private and public websites

Target Organization	
URL	
Private Websites	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Public Websites	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools/Services Used	1. 2. 3. 4.

Results Analysis:

Test 4: Search for the company's information

Target Organization	
URL	
Information Recoverd	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: List the company's contact information, email addresses, and telephone numbers

Target Organization	
URL	
Contact Numbers	1. 2. 3. 4. 5.
Email IDs	1. 2. 3. 4. 5.
Addresses	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: List employees of the company and personal email addresses

Target Organization	
URL	
Employee Name	**Email IDs**
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

Test 7: Investigate key persons – searching in Google, look up their resumes and cross link information

Target Organization					
URL					
Employee Name	**Resumes**	**Work experience**	**Completed projects**	**Promotions**	**Accomplish-ments**
1.	□				
2.	□				
3.	□				
4.	□				
5.	□				
6.	□				
7.	□				
8.	□				
9.	□				
10.	□				

Tools/Services Used

1. ______________________
2. ______________________
3. ______________________
4. ______________________
5. ______________________

Results Analysis:

____

____

____

____

____

Test 8: Search the Internet, newsgroups, bulletin boards, and negative websites for information about the company

Target Organization	
URL	
Inormation Collected	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

____

____

____

____

____

____

Test 9: Find the geographical location of a company

Target Organization		
URL		
Location of the Organization		
Recovered Maps	☐ Yes	☐ No
Neighboring company and famous landmarks	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 10: Use people search online services to collect the information

Target Organization	
URL	
Employee Name	**Contact Details**
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

____

____

____

____

____

____

Test 11: Browse social network websites to find the information about the company

Target Organization	
URL	
Information Recovered	
Social Networks Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Use Google/Yahoo! Finance to search for press releases issued by the company

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

Results Analysis:

Test 13: Search for link popularity of the company’s website

Target Organization		
URL		
Services Used	1. 2. 3. 4. 5.	
Result of Comparison wih Competitors Websites	1. 2. 3. 4. 5.	
Traffic graph of the Website Recovered	□ Yes	□ No
Search Engines Checked	1. 2. 3. 4. 5.	

Results Analysis:

Test 14: Search for the company’s job postings through job sites

Target Organization	
URL	
Search Strings Used	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Postings Discovered	1. 2. 3. 4. 5.
Information Recovered	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

Job Posting Sites Searched	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

Results Analysis:

Test 15: Monitor the target using Google Alerts

Target Organization			
URL			
Email Used to Get Alerts			
Search Query	**Result Type**	**Frequency**	**Number of Alerts**
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______		

Results Analysis:

______

______

______

______

______

______

Test 16: Gather competitive intelligence

Target Organization	
URL	
Competitors	**Information About Competitors**
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

____

____

____

____

____

____

Test 17: Search for trade association directories

Target Organization	
URL	
Trade Association Directories Searched	1. 2. 3. 4. 5.
Information Recovered	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

Results Analysis:

Test 18: List the products sold by the company

Target Organization	
URL	
Products Sold by the Company	**Price**
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 19: List the company's partners and distributors

Target Organization	
URL	

Partners and Distributors	**Details**
1. ______________________	
2. ______________________	
3. ______________________	
4. ______________________	
5. ______________________	
6. ______________________	

7.	
8.	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 20: Compare price of product or service with competitor

Target Organization			
URL			
Company’s Product/Services		**Company’s Product/Services**	
Product/Service	**Price**	**Product/Service**	**Price**
Tools/Services Used	1. 2. 3. 4. 5.		

Results Analysis:

Test 21: Search for web pages posting patterns and revision numbers

Target Organization		
URL		
Page URL	**Revision Date**	**Nature of the Revision**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 22: Visit the company as inquirer and extract privileged information

Target Organization	
URL	
Office Address Visited	
Name of the People Met at the Physical Location	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Information Collected	1. 2. 3. 4. 5.

Results Analysis:

Test 23: Visit the company locality

Target Organization	
URL	
Address Visited	
Time of Visit	
Nearby Landmarks	1. 2. 3. 4. 5.
Approach Routes	1. 2. 3. 4. 5.

Results Analysis:

Test 24: Email the employee disguising as a customer and ask for quotations

Target Organization	
URL	
Email IDs to Send Mails	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Email Template Used

To: ____

From: ____

Subject: ____

Message:

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

Results Analysis:

Test 25: Use web investigation tools to extract sensitive data

Target Organization	
URL	
Information Recovered	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 26: Look up registered information in WhoIs database

Target Organization	
URL	
Registrars Searched	□ African Network Information Centre (AfriNIC) □ American Registry for Internet Numbers (ARIN) □ Asia-Pacific Network Information Centre (APNIC) □ Latin America and Caribbean Network Information Centre (LACNIC) □ Réseaux IP Européens Network Coordination Centre (RIPE NCC)
Registrant Address	
Administrative Contact	
Technical Contact	
Record Created On	
Record Expires On	
Database Last Updated On	
Domain Servers In Listed Order	1. 2. 3.
Tools/Services Used	1.

	2. 3. 4. 5.

Results Analysis:

Test 27: Extract DNS information using domain research tools

Target Organization				
URL				
DNS Records				
Name	**Class**	**Type**	**Data**	**TTL**
Tools/Services Used	1. 2. 3. 4. 5.			

Results Analysis:

Test 28: Search similar or parallel domain name listings

Target Organization	
URL	
Country Code	**URL**
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______

Results Analysis:

Test 29: Retrieve the DNS record of the organization from publicly available servers

Target Organization				
URL				
DNS Records				
Name	**Class**	**Type**	**Data**	**TTL**
Tools/Services Used	1. 2. 3. 4. 5.			

Results Analysis:

Test 30: Locate the network range

Target Organization	
URL	
IP Address	
Network Range	
Subnet Mask	
CIDR	
Network Name	
Net Type	
RESTful Link	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 31: Search the Internet archive pages about the company

Target Organization			
URL			
Page URL	**Search Date**	**Page Found**	
1.		□ Yes	□ No
2.		□ Yes	□ No
3.		□ Yes	□ No
4.		□ Yes	□ No
5.		□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.		

Results Analysis:

Test 32: Monitor web updates using website watcher

Target Organization		
URL		
Page URL	**Revision Date**	**Nature of the Revision**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
Tools/Services Used	6. 7. 8. 9. 10.	

Results Analysis:

Test 33: Crawl the website and mirror the pages on your PC

Target Organization		
URL	HTTP://____	
Proxy (if used)		
Ports Used		
Documents Mirrored	□ Html □ Gif □ Jpeg □ Avi □ Zip □ Mpeg □ Mp3 □ cab □ RAR □ Tar □ .tar.gz □ ISO □ NRG □ IMG □ PDF □ XML □ BMP □ PNG	□ 7z □ AAC □ bzip2 □ gzip □ jar □ Dhtml □ Flash □ DMG □ DB □ ORA □ DOC □ DOCX □ CSV □ ODT □ ODM □ Other ___________________ □ Other ___________________ □ Other ___________________
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____	

Results Analysis:

____

____

____

____

____

Test 34: Crawl the FTP site and mirror the pages on your PC

Target Organization	
FTP URL	FTP://____
Proxy (if used)	
Ports Used	
Documents Mirrored	□ Html □ Gif □ Jpeg □ Avi □ Zip □ Mpeg □ Mp3 □ cab □ RAR □ Tar □ .tar.gz □ ISO □ NRG □ IMG □ PDF □ XML □ BMP □ PNG □ 7z □ AAC □ bzip2 □ gzip □ jar □ Dhtml □ Flash □ DMG □ DB □ ORA □ DOC □ DOCX □ CSV □ ODT □ ODM □ Other ___________________ □ Other ___________________ □ Other ___________________
Tools/Services Used	1. ____________________ 2. ____________________ 3. ____________________ 4. ____________________

Results Analysis:

____

____

____

____

____

Test 35: Track email communications

Target Organization					
URL					
Email ID	Origin/ Destination IP	Origin/Destination Country	Time	Mail Read	Email Lookup Map
				□	□
				□	□
				□	□
				□	□
				□	□
				□	□
				□	□
				□	□
Tools/Services Used	1. 2. 3. 4. 5.				

Results Analysis:

Test 36: Use GHDB and search for the company’s internal resources

Target Organization	
URL	

GHDB Seach Query Used	**Information Recovered**

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

Results Analysis:

____

____

____

____

____

____

Additional Tests

Test __:

Target Organization	
URL	
Information Discovered	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test __:

Target Organization	
URL	
Information Discovered	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test __:

Target Organization	
URL	
Information Discovered	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

____

____

____

____

____

____