Certified Penetration Testing Professional

Methodology: Open-Source Intelligence (OSINT)

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

Test 1: OSINT through the WWW

Test 1.1: Find the Domain and Sub-domains of the Target

Target Organization		
URL		
Search Engine Used		
Found the Domain and Sub-domains of the Target Successfully?	☐ Yes	☐ No
Attack Surfaces of Target Organization		
Command Used		
Domain and Sub-domains Identified	1. 2. 3. 4. 5.	

Results Analysis:

Test 1.2: Find Similar or Parallel Domain Names

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

Results Analysis:

Test 1.3: Refine Web Searches using Advanced Operators

Target Organization		
URL		
Search Engine Used		
Refined Your Web Searches using Google's Advanced Operators?	☐ Yes	☐ No
Google's Advanced Operators Used	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.	
Queries to find, filter, and sort Specific Information		
Information Gathered		
Technique Used		

GHDB Search Query Used	Information Gathered

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

Results Analysis:

Test 1.4: Footprint the Target using Shodan

Target Organization		
URL		
Successfully Blueprinted the Target using Shodan?	☐ Yes	☐ No
Devices Identified using Shodan	☐ Webcam ☐ Router ☐ Switches ☐ Others Specify _____ _____ _____	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

Test 1.5: 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 1.6: List Employees and their Email Addresses

Target Organization	
URL	

Employee Name	Email IDs/Contact Details

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

Results Analysis:

Test 1.7: Identify Key Email Addresses through Email Harvesting

Target Organization		
URL		
Command used		
Domain Name	**Employee Name**	**Email IDs**
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 1.8: Enumerate Key Email Addresses from Pastebin and HaveIBeenPwned

Target Organization				
URL				
Website(s) used	☐ Pastebin ☐ HaveIBeenPwned ☐ Others Specify _____ _____ _____			
Employee Name	**Telephone**	**Date of Birth**	**Email**	**Residential Address**
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____			

Results Analysis:

Test 1.9: List Key Personnel of the Company

Target Organization	
URL	
Search Engine Used	
Job Sites	

Employee Name	Resumes	Work experience	Completed projects	Promotions	Accomplishments
	☐				
	☐				
	☐				
	☐				
	☐				
	☐				
	☐				
	☐				
	☐				
	☐				

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

Results Analysis:

Test 1.10: Using People Search Online Services to Collect Information

Target Organization	
URL	

Employee Name	Contact Number	Date of Birth	Email	Residential Address	Photo	Satellite pictures of private residencies
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No
					☐ Yes ☐ No	☐ Yes ☐ No

Any other information found:	____________________ ____________________

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

Results Analysis:

Test 1.11: Browse Social Network Websites to Find Information on the Company and Employees

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

Results Analysis:

Test 1.12: Use Web Investigation Tools to Extract Sensitive Data about the Company

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

Results Analysis:

Test 1.13: Identify the Type of Network Devices used in the Organization

Target Organization	
URL	
Search Engines Used	
Sources Used to Gather relevant Information	
Company's Infrastructure in the Organization	☐ Oracle database server ☐ Cisco routing devices ☐ Checkpoint firewalls ☐ Any other, specify _____ _____ _____
Network Devices Identified	
Tools/Techniques Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

Test 1.14: Look for the Sensitive Information in Email Headers

Target Organization					
URL					
Email ID	Recipient's IP address	Information on browser and operating system	MIME-Version	Geo-location	Device Type
Any other information found:					
Tools/Techniques Used	1. 2. 3. 4. 5.				

Results Analysis:

Test 1.15: Look for Valuable Information in NNTP Usenet Newsgroups

Target Organization	
Newsgroups Used to gather Information	
Information Gathered	
Tools/Techniques Used	1. 2. 3. 4. 5.

Results Analysis:

Test 1.16: Other Useful Footprinting Activities to Find Information about the Target

- **Search for the company's information in online trade association directories**

Target Organization	
URL	
Information Gathered	
Tools/Techniques Used	1. 2. 3. 4. 5.

Results Analysis:

- **Collect the company's information through groups, forums, and blogs**

Target Organization	
URL	
Groups/Forums/Blogs used for gathering information	

Public network information found	
System information found	
Employee information found	
Tools/Techniques Used	1. 2. 3. 4. 5.

Results Analysis:

- **Search for press releases issued by the company using Google/Yahoo Finance**

Target Organization	
URL	
Tools used	☐ Google Finance ☐ Yahoo Finance ☐ Any other, specify

Information Gathered	
Tools/Techniques Used	1. 2. 3. 4. 5.

Results Analysis:

- **Search for the link popularity of the company's website**

Target Organization	
URL	
Information Gathered	

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

Results Analysis:

- **Monitor the target using alerts such as Google Alerts, Yahoo Alerts, and Twitter Alerts**

Target Organization	
URL	
Alert used	☐ Google Alerts ☐ Yahoo Alerts ☐ Twitter Alerts ☐ Any other, specify
Information Gathered	

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

Results Analysis:

- **Gather competitive intelligence by visiting websites such as EDGAR Database, Business Wire, LexisNexis, and Hoovers**

Target Organization			
URL			
Website used	☐ EDGAR Database ☐ Business Wire ☐ LexisNexis ☐ Hoovers ☐ Any other, specify		
Company's establishment date	**Strategy used**	**Location of the company**	**Branch**

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

Results Analysis:

- **Search and list the products/services sold by the company**

Target Organization		
URL		
Email	**Product**	**Product Price**

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

Results Analysis:

- **Compare the prices of products or services with those of the competitor**

Target Organization	
URL	
Merchant ratings of the company	
Customer reviews	
List of products and services provided by the company	
Tools/Techniques Used	1.

	2. 3. 4. 5.

Results Analysis:

Test 2: OSINT through Website Analysis

Test 2.1: Search Contact Information, Email Addresses, and Telephone Numbers from Company Website

Target Organization	
URL	
Contact Numbers	1. 2. 3. 4. 5.
Email IDs	1. 2. 3. 4. 5.
Addresses	1. 2. 3. 4. 5.
Company's Location and Branches	1. 2. 3. 4.
Partner's Information	1. 2. 3. 4.

	5.
Any other information found	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2.2: 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.			
Any other information found			
Tools/Services Used	1. 2. 3. 4. 5.		

Results Analysis:

Test 2.3: Search Archive.org for Old Information 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
Any other information found				
Tools/Services Used	1. 2. 3. 4. 5.			

Results Analysis:

Test 2.4: 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.			
Any other information found			
Tools/Services Used	1. 2. 3. 4. 5.		

Results Analysis:

Test 2.5: Examine HTML Source of the Web Pages

Target Organization	
URL	
HTML Source	
Information Gathered	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: OSINT through DNS Interrogation

Test 3.1: Perform Whois Lookups

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) ☐ Reseaux IP Europeens Network Coordination Centre (RIPE NCC) ☐ Any other, specify
Registrant Address	
Domain name details	
IP address and Network Range	
Physical Location	
Administrative Contact	

Technical Contact	
Record Created On	
Record Expires On	
Database Last Updated On	
Domain Servers In Listed Order	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.2: Find IP Address Block Allocated to the Organization

Target Organization		
URL		
Found IP Range Successfully?	☐ Yes	☐ No
IP Registries Used		
Whois database Used		
IP Range Identified		
NSLookup Command		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3.3: Find the DNS Records for Domain

Target Organization				
URL				
Command Used				
DNS Records				
Name	Class	Type	Data	TTL
Any other information found				
Tools/Services Used	1. 2. 3. 4. 5.			

Results Analysis:

Test 3.4: Perform Reverse Lookups

Target Organization		
URL		
Performed Reverse DNS Lookup Successfully?	☐ Yes	☐ No
Commands Used		
IP Range for Reverse DNS lookup		
DNS PTR records found		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3.5: Perform DNS Zone Transfer

Target Organization		
URL		
Performed DNS Zone Transfer Successfully?	☐ Yes	☐ No
Gathered DNS Information		
dig Commands Used to perform DNS Zone Transfer		
nslookup Commands Used to perform DNS Zone Transfer		
dnsrecon Commands Used to perform DNS Zone Transfer		
Identified Host Names		
Identified Machine Names		
Identified Usernames		
Identified IP Addresses		
Any other information found		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3.6: Draw a Network Diagram using Traceroute Analysis

Target Organization		
URL		
Conducted Traceroute Successfully?	☐ Yes	☐ No
Extracted Information after conducting Traceroute		
Is Network Diagram drawn successfully using Traceroute Analysis?	☐ Yes	☐ No
Commands Used to perform Traceroute		
Any other information found		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3.7: Create Topological Map of the Network

Target Organization		
URL		
Created Physical and Logical Topological Map of the Network based on Information Gathered through Traceroute?	☐ Yes If Yes, attach a copy of the network topology map	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4: Automating your OSINT Effort using Tools/Frameworks/Scripts

Target Organization		
URL		
Is OSINT Efforts automated by using Tools/Frameworks/Scripts?	☐ Yes	☐ No
Tools/Frameworks/Scripts Used	1. 2. 3. 4. 5.	
Information Gathered		

Results Analysis: