EC-Council Licensed Penetration Tester

Methodology: Penetration Testing Planning and Scheduling

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

Listing Project scope

Target Organization	
URL	
Project scope	
☐ Network security	1. 2. 3.
☐ System software security	1. 2. 3.
☐ Client-side application security	1. 2. 3.
☐ Client-side to server-side application communication security	1. 2. 3.
☐ Server-side application security	1. 2. 3.
☐ Social engineering	1. 2. 3.
☐ Dumpster diving	1. 2. 3.

☐ Inside accomplices	1. 2. 3.
☐ Physical security	1. 2. 3.
☐ Sabotage Intruder confusion	1. 2. 3.
☐ Intrusion detection	1. 2. 3.
☐ Intrusion response	1. 2. 3.
List of tests that should not be conducted	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

List the test deliverables	1. 2. 3. 4. 5.
Tools/Services Used	6. 7. 8. 9. 10.

Results Analysis:

List names of your Tiger Team members and their responsibilities

Target Organization		
URL		
Tiger Team		
Job Roles	**Member Name**	**Responsibilities**
☐ Chief Penetration Tester (CPO)		
☐ Database and Application Expert		
☐ Networking Expert		
☐ Ethical Hacker		
☐ Data Analyst		
☐ Project Manager		
☐ Report and Documentation Writer		
Rules of Engagement Signed on	☐ Yes	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

List the skills held by each team member

Target Organization		
URL		
Tiger Team		
S.No.	**Name of Individual**	**Skills Held**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
Internal employees to assist in the project		
S.No.	**Names of employees**	**Job Roles**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
Tools/Services Used	1.	
	2.	

	3. 4. 5.

Results Analysis:

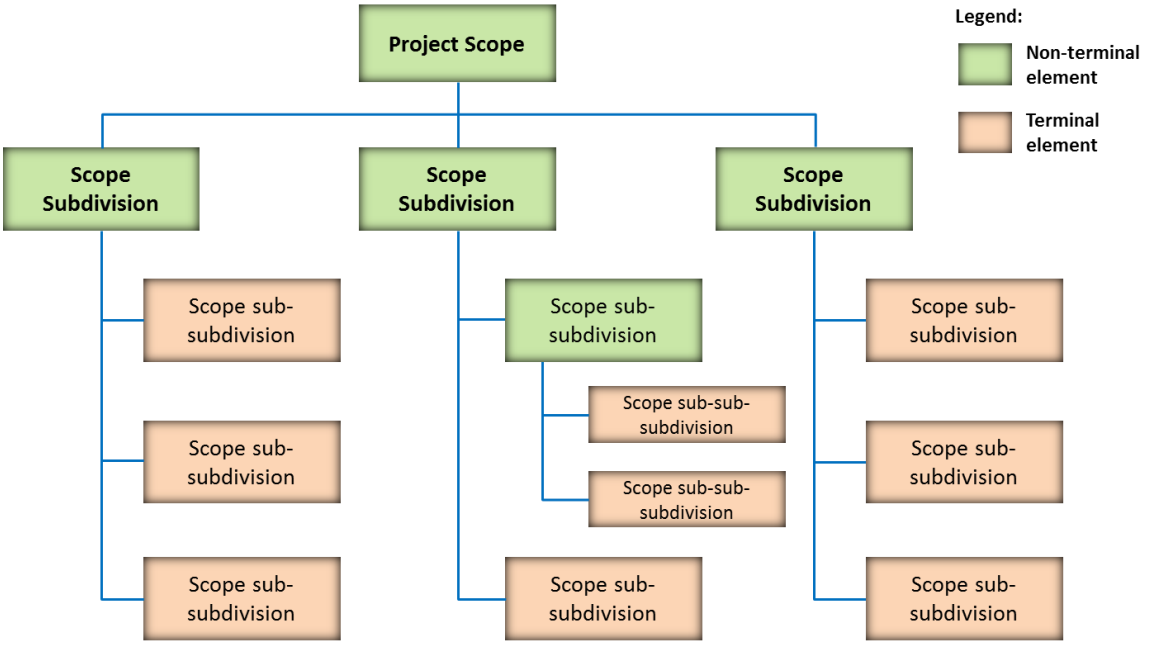
Meeting with the client

Target Organization	
URL	
Minutes of Meeting	
Date	Meeting 1
Date	Meeting 2
Date	Meeting 3
Date	Meeting 4
Date	Meeting 5
List down the project plans (Use commercial project planning software like Microsoft Project)	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13.

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

Results Analysis:

Define WBS using project management software



Target Organization	
URL	
Software/Hardware required for the test: Laptop with the following	
☐ Windows XP virtual server	
☐ Windows 2003 virtual server	
☐ Windows 2000 virtual server	
☐ Red Hat Linux 9	
☐ Wireless Access points	
☐ Wireless cards	
☐ Huge hard disk – preferably 160 GB	
Software/Hardware required for the test: Devices	
☐ Keyloggers	

☐ Jamming devices	
☐ Radio communication interceptors	
☐ Telephone spying devices	
☐ Wireless antennas	
Software/Hardware required for the test: Software	
☐ Hacking Tools CD-ROM (Linux Version)	
☐ Hacking Tools CD-ROM (Windows version)	
☐ Sniffing Devices	
☐ Penetration testing software – Core Impact	
☐ Vulnerability Assessment Tools	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: