

EC-Council Licensed Penetration Tester

Methodology: Customers and Legal Agreements

Penetration Tester:			
Organization:			
Date:		Location:	



List the customer penetration testing requirements:

Target Organization	
URL	
Penetration Testing Requirements	<ol style="list-style-type: none">1.2.3.4.5.6.7.8.9.10.
Tools/Services Used	<ol style="list-style-type: none">1.2.3.4.5.

Results Analysis:

List what needs to be tested

Target Organization			
URL			
Items to be Tested			
Items	Inference		
<input type="checkbox"/> Servers			
<input type="checkbox"/> Workstations			
<input type="checkbox"/> Routers			
<input type="checkbox"/> Firewalls			
<input type="checkbox"/> Networking devices			
<input type="checkbox"/> Cabling			
<input type="checkbox"/> Databases			
<input type="checkbox"/> Applications			
<input type="checkbox"/> Physical security			
Rules of Engagement Signed on	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____		

Results Analysis:

Do you have any security-related policies and standards?

Target Organization	
URL	
Security-related Policies and Standards	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Perform a review of the physical security of your servers and network infrastructure

Target Organization	
URL	
Review the physical security of the server	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Review the physical security of the network infrastructure	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Number of Internet Domains	1. _____ 2. _____ 3. _____
Number of Internet Hosts	1. _____ 2. _____ 3. _____
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Results Analysis:

Map your Internet presence

Target Organization	
URL	
Present a detailed diagram of your Internet presence	
IP Addresses	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Host OS types	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Software used on the hosts	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Addresses used on both sides of the hosts if they connect to both the Internet and the internal network	1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Tools/Services Used	1. _____

	2.
	3.
	4.
	5.

Results Analysis:

Review the security of your routers and hubs

Target Organization	
URL	
Number of routers and hubs existing on your network	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Perform a security review of the workstations on the network

Target Organization		
URL		
Operating Systems	1. 2. 3.	
Number of Workstations tested		
Denial-of-service test conducted	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Results inferred from the Denial-of-service test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Perform a modem scan of your analog phone lines

Target Organization	
URL	
RAS server being used	
How many modems are used?	
Assessments performed on systems on other sites	
Tools/Services Used	<div>1. _____</div> <div>2. _____</div> <div>3. _____</div> <div>4. _____</div> <div>5. _____</div>

Results Analysis:

Main clauses in the agreement

Target Organization		
URL		
List the main clauses in the agreement	1. 2. 3. 4. 5.	
List down the risks involved in the testing	1. 2. 3. 4. 5.	
Confidentiality Agreements	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Parties involved		
Pricing (Total Penetration Testing Contract)		
<input type="checkbox"/> Pricing will usually be based on the number of man days required to fulfill the scope of the project		
<input type="checkbox"/> Number of client computers to be tested		
<input type="checkbox"/> Number of server computers to be tested		
<input type="checkbox"/> Different price for tests like social engineering, competitive intelligence, stealing laptops, physical security		
Laws or regulations complied to during the test		
<input type="checkbox"/> Gramm-Leach-Bliley Act		
<input type="checkbox"/> Health Insurance Portability and Accountability Act		
<input type="checkbox"/> Sarbanes-Oxley		

<input type="checkbox"/> FERPA and the TEACH Act	
<input type="checkbox"/> Electronic Communications Privacy Act and Computer Fraud and Abuse Act	
Other Issues	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:
