EC-Council Licensed Penetration Tester

Methodology: Denial-of-Service Penetration Testing

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

Test 1: Test heavy loads on the server

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Check for DoS vulnerable systems

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Run SYN attack on the server

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Run port flooding attacks on the server

Target Organization	
URL	
Server IP Address tested	
Impact of the Test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Run IP fragmentation attack on the server

Target Organization	
URL	
Server IP Address tested	
Impact of the Test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Run ping of death

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Run teardrop attack

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Run smurf (ping flooding or ICMP storm) attack

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Run email bomber on the email servers

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Flood the website forms and guestbook with bogus entries

Target Organization	
URL	
Server IP Address tested	
Impact of the test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Run service request floods

Target Organization	
URL	
Server IP Address Tested	
Service Requests Containing Large Payloads	
Impact of the Test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Run permanent DoS attacks

Target Organization	
URL	
Server IP Address Tested	
Social Engineering Techniques used to Post the Fraudulent Links	
Impact of the Test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Run peer-to-peer attacks

Target Organization	
URL	
Server IP Address Tested	
Unpatched DC++ (direct connect) Hubs	
Non-vulnerable DC++ (direct connect) Hubs	
IP Addresses to Block and Exploit DC++ Hubs	
Impact of the Test	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Test for SQL wildcard injection attacks

Target Organization	
URL	
Server IP Address Tested	
Wildcards used to exhaust CPU resources	
Query Execution Time in the Database Server	
Http Log Files for Response Time of the Query	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Try to log in to customer accounts

Target Organization		
URL		
Logging Mechanism of the Host Applications		
User Account Locked	☐ YES	☐ NO
Number of Failed Login Attempts		
Access User Database using a Brute-Forcing Technique	☐ YES	☐ NO
Logic Behind Machine-Generated User Names		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16: Test for buffer overflow attacks that result in denial of service

Target Organization	
URL	
Server IP Address Tested	
Overwrite Memory Fragments	
Arbitrary Code Executed on the Target Server	
Code Executed to cause Segmentation Fault	
Code Executed to cause Memory Dump	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17: Test for DOS user-specified object allocation

Target Organization	
URL	
Server IP Address Tested	
User-Specified Number of Objects Allocated to the Client's Server	
Automated Script to Exhaust Resources of E-Commerce Sites	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18: Test for user input as a loop counter

Target Organization		
URL		
Applications Loop through a Code Segment that Exhausts Computing Resources	☐ YES	☐ NO
Places Located where Input Values Exhaust Server Resources		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 19: Try to generate large application log files

Target Organization			
URL			
Server IP Address Tested			
Data Validation Method Records the Failed Value			
Upper Limit of Log Dimensions and Maximum Allocated Space for each Log Entry to Perform an Attack on Application Logs			
Application Log Files Record overly large Requests Sent to the Host Server without any Limitation of the Length		☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.		

Results Analysis:

Test 20: Test for memory allocation in applications

Target Organization		
URL		
Server IP Address Tested		
Applications Properly Release Resources after they are used	☐ YES	☐ NO
Special Characters used to Create Errors in Applications and Consume Memory		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 21: Try to store too much data in sessions

Target Organization		
URL		
Server IP Address Tested		
Target Memory Usage		
Automated Scripts sent to Create New Sessions on the Server		
Blocks of Data are Recorded in a Cache	☐ YES	☐ NO
Blocks of Data are Recorded in Database for User Sessions	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis: