EC-Council Licensed Penetration Tester

Methodology: IDS Penetration Testing

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

Test 1: Test for resource exhaustion

Target Organization		
URL		
IDS Network Tested		
Sent Large Amount of Traffic to the IDS System Successfully	☐ Yes	☐ No
IDS Performance		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2: Test the IDS by sending ARP flood

Target Organization		
URL		
IDS Network Tested		
Performed Network Flooding by sending ARP Packets Successfully	☐ Yes	☐ No
IDS Response		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3: Test the IDS by MAC spoofing

Target Organization		
URL		
IDS Network Tested		
Spoofed MAC Address		
Sent spoofed MAC address to the IDS Successfully	☐ Yes	☐ No
IDS Response		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4: Test the IDS by IP spoofing

Target Organization		
URL		
IDS Network Tested		
Spoofed IP Address		
Sent Spoofed IP Address Successfully	☐ Yes	☐ No
Response Received		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 5: Test the insertion on IDS

Target Organization		
URL		
IDS Network Tested		
Character insertion into the IDS is Successful	☐ Yes	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Test by sending a packet to the broadcast address

Target Organization	
URL	
IDS Network Tested	
Broadcast Address	
Sent Packet to the Broadcast Address Successfully	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Test by sending inconsistent packets

Target Organization		
URL		
IDS Network Tested		
Inconsistent Packets		
Sent Inconsistent TCP/IP or UDP/IP Packets with different TCP/UDP and IP Header Sizes Successfully	☐ Yes	☐ No
IDS Response		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 8: Test IP packet fragmentation

Target Organization		
URL		
IDS Network Tested		
Packet Size Sent		
Sent IP Packet Fragments Successfully	☐ Yes	☐ No
IDS Response		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 9: Test for overlapping

Target Organization	
URL	
IDS Network Tested	
Packet Size Sent	
How many Times was it Sent?	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Test for ping of death

Target Organization	
URL	
IDS Network Tested	
Packet Size Sent (along with fragment offset)	
How many Times was it Sent?	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Test for TTL evasion

Target Organization	
URL	
IDS Network Tested	
How was TTL evasion attempted?	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Test by sending a packet to port 0

Target Organization	
URL	
IDS Network Tested	
Packet sent to Port 0	
Response Received	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Test for UDP checksum

Target Organization	
URL	
IDS Network Tested	
UDP Checksum Information	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Test for TCP retransmissions

Target Organization	
URL	
IDS Network Tested	
Retransmitted TCP Packets	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Test the IDS by TCP flag manipulation

Target Organization	
URL	
IDS Network Tested	
Manipulated TCP Flag	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16: Test the IDS by sending SYN floods

Target Organization		
URL		
Tested IDS by Sending SYN Floods	☐ YES	☐ NO
Results from the IDS Test Performed	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 17: Test initial sequence number prediction

Target Organization	
URL	
IDS Network Tested	
Sequence Number Predicted	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18: Test for backscatter

Target Organization	
URL	
SYN Packets Received	
Analyzed SYN/ACK Packets	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 19: Check for false positive generation

Target Organization	
URL	
False Reports Generated Within the IDS	1. 2. 3.
Examined Alert Data that is Logged	1. 2. 3.
Generated False Positives with Specific IDS	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 20: Test the IDS using covert channels

Target Organization		
URL		
Tested IDS Using Covert Channels	☐ YES	☐ NO
Information Gathered Using Covert Channels	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 21: Test using TCPReplay

Target Organization		
URL		
Tested IDS Using TCPReplay	☐ YES	☐ NO
Information Gathered from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 22: Test the IDS using TCPopera

Target Organization	
URL	
IDS Testing Environments Provided by TCPopera	1. 2. 3.
Exhibited TCP Behavior	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 23: Test the IDS using method matching

Target Organization		
URL		
Method Used to Test the IDS		
GET Method	GET Request	GET Signatures
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 24: Test the IDS using URL encoding

Target Organization		
URL		
Tested the IDS Using URL Encoding	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 25: Test the IDS using double slashes

Target Organization		
URL		
Tested the IDS Using Double Slashes	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 26: Test the IDS for reverse traversal

Target Organization		
URL		
Tested the IDS for Reverse Traversal	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 27: Test for self-reference directories

Target Organization		
URL		
Tested the IDS for Self-Referencing Directories	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 28: Test for premature request ending

Target Organization		
URL		
Tested the IDS for Premature Request Ending	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 29: Test for IDS parameter hiding

Target Organization		
URL		
Tested for IDS Parameter Hiding	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 30: Test for HTTP misformatting

Target Organization		
URL		
Tested IDS for HTTP Misformatting	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 31: Test for long URLs

Target Organization		
URL		
Tested IDS for Long URLs	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 32: Test for Win directory syntax

Target Organization		
URL		
Tested IDS for Win Directory Syntax	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 33: Test for null method processing

Target Organization		
URL		
Tested IDS for Null Method Processing	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 34: Test for case sensitivity

Target Organization		
URL		
Tested IDS for Case Sensitivity	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 35: Test session splicing

Target Organization		
URL		
Tested IDS for Session Splicing	☐ YES	☐ NO
Findings from the Test	1. 2. 3. 4. 5.	
Sessions Susceptible to Malicious Data	1. 2. 3.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 36: Try to bypass invalid RST packets through IDS

Target Organization	
URL	
Expected Checksum	
Received Checksum	
Examined Two-way Communication TCP Protocols Using RST Packets	
Results from Verified RST Packets and Checksum	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: