EC-Council Licensed Penetration Tester

Methodology: Firewall Penetration Testing

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

Test 1: Locate the firewall

Target Organization	
URL	
Firewall Location	
Firewall IP Address	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Traceroute to identify the network range

Target Organization			
URL			
IP Address Traced			
Tracert Results			
Total Number of Hops		**Timeout**	

IP Addresses Hoped
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.

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

Results Analysis:

Test 3: Port scan the firewall

Target Organization	
URL	

Open Ports

□ 7 Echo	□ 109 Post Office Protocol 2 (POP2)
□ 13 DayTime	□ 110 Post Office Protocol 3 (POP3)
□ 17 Quote of the Day (QOTD)	□ 113 IDENT
□ 20 and 21 File Transfer Protocol (FTP)	□ 115 Simple File Transfer Protocol (SFTP)
□ 22 Secure Socket Shell (SSH)	□ 137, 138, and 139 NetBIOS
□ 23 Telnet	□ 143 Internet Message Access Protocol (IMAP)
□ 25 SMTP	□ 161 and 162 Simple Network Management Protocol
□ 53 Domain Name System (DNS)	□ 194 Internet Relay Chat (IRC)
□ 63 Whois	□ 443 HTTPS
□ 66 SQL*net (Oracle)	**Other Ports:**
□ 70 Gopher	
□ 79 Finger	
□ 80 HTTP	
□ 88 Kerberos	
□ 101 Host Name Server	

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

Results Analysis:

Test 4: Grab the banner

Target Organization	
URL	
Banner Message	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

______

______

______

______

______

______

Test 5: Create custom packets and look for firewall responses

Target Organization		
URL		
IP of Tested Firewall		
S.No.	**Custom Packet**	**Response**
1.		
2.		
3.		
4.		
5.		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Test access control enumeration

Target Organization	
URL	
IP of Tested Firewall	
Access Controls	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Test to identify the firewall architecture

Target Organization	
URL	
IP of Tested Firewall	
Firewall Architecture Details	
Tools/Services Used	6. 7. 8. 9. 10.

Results Analysis:

Test 8: Testing firewall policy

Target Organization		
URL		
Firewall Configuration Policy is Available	□ Yes	□ No
Firewall is Configured as par Policy	□ Yes	□ No
Firewall Policy Defines All Expected Standard Configuration	□ Yes	□ No
Gap Between Policy and Firewall Implementation		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 9: Test the firewall using a firewalking tool

Target Organization		
URL		
Firewalking Technique used	□ Traceroute	□ Scanning
IP of Tested Firewall		
Internal IPs Discovered	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 10: Test for port redirection

Target Organization	
URL	
IP of Tested Firewall	
Port Redirection Results	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Testing the firewall from both sides

Target Organization		
URL		
IP of Tested Firewall		
Unauthorized connections from the internal network to the Internet can be created	□ Yes	□ No
Vulnerabilities identified by scanners	1. 2. 3. 4. 5.	
Reaction of the firewall to fragmented and spoofed packets		
Identified Firewall Rules	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 12: Overt firewall test from outside

Target Organization		
URL		
IP of Tested Firewall		
Unauthorized Connections from the Internal Network to the Internet can be Created	□ Yes	□ No

Vulnerabilities Identified by Scanners

1.
2.
3.
4.
5.

Reaction of the Firewall to Fragmented and Spoofed Packets

Identified Firewall Rules

1.
2.
3.
4.
5.

Tools/Services Used

1.
2.
3.
4.
5.

Results Analysis:

Test 13: Test covert channels

Target Organization		
URL		
IP of Tested Firewall		
Successfully installed Backdoor on a Victim Machine inside the Network	□ Yes	□ No
Successfully Established Reverse Connection to a Machine Outside the Firewall	□ Yes	□ No
Successfully Bypassed Firewall and Router Security Restrictions	□ Yes	□ No
Tools/Services Used	1. __________ 2. __________ 3. __________ 4. __________ 5. __________	

Results Analysis:

____

____

____

____

____

____

Test 14: Covert firewall test from outside

Target Organization		
URL		
IP of Tested Firewall		
Unauthorized Connections from the Internet to the Internal Network can be Created	☐ **Yes**	☐ **No**
Vulnerabilities Identified by Scanners	1. 2. 3. 4. 5.	
Reaction of the Firewall to Fragmented and Spoofed packets		
Identified Firewall Rules	1. 2. 3. 4. 5.	
Tools/Services Used	6. 7. 8. 9. 10.	

Results Analysis:

Test 15: Test HTTP tunneling

Target Organization	
URL	
IP of Tested Firewall	
HTTP Tunneling Technique Results	
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______

Results Analysis:

Test 16: Test firewall-specific vulnerabilities

Target Organization	
URL	
IP of Tested Firewall	
List Product Specific Exploits against Firewall Vulnerabilities	1. 2. 3. 4. 5.
Response Received from Implementation of Product Specific Exploits against Firewall Vulnerabilities	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: