EC-Council Licensed Penetration Tester

Methodology: VPN Penetration Testing

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

Test 1: Check the target organization's VPN security policy

Target Organization		
URL		
VPN Security Policy Enforced	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2.1: Scanning - 500 UDP IPsec

Target Organization		
URL		
Target URL		
State of the UDP Port 500	☐ Open	☐ Closed
ISAKMP Service (IPSec VPN Server) is Running on Port 500	☐ Yes	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2.2: Scanning - 1723 TCP PPTP

Target Organization		
URL		
Target URL		
State of the TCP Port 1723	☐ Open	☐ Closed
PPTP Service is Running on Port 1723	☐ Yes	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2.3: Scanning - 443 TCP/SSL

Target Organization		
URL		
Target URL		
State of the TCP Port 443	☐ Open	☐ Closed
Tools/Services Used	6. 7. 8. 9. 10.	

Results Analysis:

Test 2.4: Scanning - Ipsecscan xxx.xxx.xxx.xxx-255

Target Organization	
URL	
Single IP Address Scan	
Range of IP Addresses Scanned	
IPSEC Enabled Systems	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Fingerprinting

Target Organization	
URL	
VPN Vulnerabilities Detected	1. 2. 3.
Information Gathered through Fingerprinting	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.1: Get the IKE handshake

Target Organization	
URL	
Host URL	
Acceptable Transform Attributes from the Security Association (SA) Payload	1. 2. 3.
Combination of Transfer Attributes Tried	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.2: UDP Backoff fingerprinting

Target Organization	
URL	
Host URL	
Implementation Guess	1. 2. 3.
Information Gathered	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.3: Vendor ID fingerprinting

Target Organization	
URL	
Vendor ID Payload	1. 2. 3.
Other Information Gathered	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.4: Check for IKE aggressive mode

Target Organization		
URL		
Host URL		
Aggressive Mode Enabled	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4: Test for default user accounts and passwords

Target Organization		
URL		
IPSEC VPN: Default User Accounts and Passwords		
User Accounts		Passwords
1.		1.
2.		2.
3.		3.
4.		4.
5.		5.
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 5: Check for unencrypted user name in a file or the registry

Target Organization		
URL		
Password File or Registry Entry		
Successfully Recovered Passwords	☐ YES	☐ NO
Recovered Passwords	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Test for plain-text password

Target Organization		
URL		
VPN Client Established to Obtain the Password	☐ YES	☐ NO
Plain-text Password Recovered		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 7: Perform user name enumeration

Target Organization	
URL	
Response Given by the VPN Endpoint to an Authentication Attempt	1. 2. 3.
List of Valid Usernames	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Check account lockout in VPN

Target Organization	
URL	
Connection to VPN Tunnel Using Correct User Name and False Password	
Threshold defined by the authentication system for failed login attempts	
Amount of time required to reset user account credentials	
Impact of the Test	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Audit VPN traffic

Target Organization		
URL		
Sniffing Techniques Used to Intercept VPN Traffic		
Traffic Intercepted Before it Passes the Tunnel		
Traffic Intercepted After it Passes the Tunnel		
Decrypt Traffic Off the Line	☐ Successful	☐ Unsuccessful
Recover Sensitive Information	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 10: Check for proper firewalling in VPN

Target Organization	
URL	
Open Ports in the Firewall	
1.	4.
2.	5.
3.	6.
Packets Passed through TCP and UDP Filtering in the Firewall	1. 2. 3.
Results from examined Firewall Logs	1. 2. 3. 4.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Check denial-of-services in VPN

Target Organization	
URL	
Router Effect on the VPN Under DoS Attack	1. 2. 3.
Effect on the VPN due to Shared Part of the Network under DoS Attack	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: