



Certified Penetration Testing Professional

Methodology: Network Penetration Testing - External

Penetration Tester:		
Organization:		
Date:		Location:

Test 1: Port Scanning**Test 1.1: Scan the Network to Discover Live Hosts**

Target Organization			
URL			
Commands Used	1.		
	2.		
	3.		
	4.		
	5.		
Discovered live hosts Successfully?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
List of IP addresses scanned	1.		
	2.		
	3.		
	4.		
	5.		
List of the live host discovered	1.		
	2.		
	3.		
	4.		
	5.		
Tools Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

Test 1.2: Checking for Live Systems - ICMP Scanning

Target Organization		
URL		
Commands Used	1.	
	2.	
	3.	
	4.	
	5.	
Performed ICMP Scanning on the Target Successfully?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Response Received		
Range of IP addresses of Live Systems		
Tools/Services Used	1.	
	2.	
	3.	
	4.	
	5.	

Results Analysis:

--

Test 1.3: Identify Default Open Ports

Target Organization			
URL			
Commands Used	1.		
	2.		
	3.		
	4.		
	5.		
IP Addresses Scanned			
Performed Complete Port Scan of the Target Network Successfully?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Identified Open Ports and Services			
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

--

Test 1.4: Use Connect Scan (Full Open Scan) on the Target and See the Response

Target Organization			
URL			
Commands Used	1.		
	2.		
	3.		
	4.		
	5.		
IP Addresses Scanned			
Performed Connect Scan on the Target Successfully?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Response Received			
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

Test 1.5: Use SYN Scan (Half-open Scan) on the Target and See the Response

Target Organization		
URL		
Commands Used	1.	
	2.	
	3.	
	4.	
	5.	
IP Addresses Scanned		
Performed SYN Scan on the Target Successfully?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Response Received		
List of Open Ports	1.	
	2.	
	3.	
	4.	
	5.	
List of Closed Ports	1.	
	2.	
	3.	
	4.	
	5.	
List of Filtered Ports	1.	
	2.	
	3.	
	4.	
	5.	

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

Results Analysis:

Test 1.6: Use Illegal Flag Combinations to Scan the Target

Target Organization			
URL			
Commands Used	1.		
	2.		
	3.		
	4.		
	5.		
IP Addresses Scanned			
Performed NULL Scan on the Target Successfully?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Response Received			
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

--

Test 1.7: Use ACK Flag Probe Scan on the Target and See the Response

Target Organization			
URL			
Commands Used	1.		
	2.		
	3.		
	4.		
	5.		
IP Addresses Scanned			
Performed ACK flag probe Scan on the Target Successfully?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Response Received			
List of Open Ports	1.		
	2.		
	3.		
	4.		
	5.		
List of Closed Ports	1.		
	2.		
	3.		
	4.		
	5.		
List of Filtered Ports	1.		
	2.		
	3.		
	4.		
	5.		

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

Results Analysis:

Test 1.8: Use UDP Scan on the Target and See the Response

Target Organization			
URL			
Commands Used	1.		
	2.		
	3.		
	4.		
	5.		
IP Addresses Scanned			
Performed UDP Scan on the Target Successfully?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Response Received			
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

Test 1.9: Use Fragmentation Scanning and Examine the Response

Target Organization		
URL		
Commands Used	1.	
	2.	
	3.	
	4.	
	5.	
IP Addresses Scanned		
Performed Fragmentation Scan on the Target Successfully?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Response Received		
Tools/Services Used	1.	
	2.	
	3.	
	4.	
	5.	

Results Analysis:

Test 1.10: List Open and Closed Ports

Target Organization	
URL	
IP Address Tested	
List the Open Ports	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
List the Ports that are closed	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
List the Ports that are filtered	1. 2. 3. 4. 5. 6.

	7.
	8.
	9.
	10.
Tools/Services Used	1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.

Results Analysis:

Test 2: OS and Service Fingerprinting**Test 2.1: Fingerprint the OS**

Target Organization			
URL			
Commands Used	1.		
	2.		
	3.		
	4.		
	5.		
OS fingerprinting is Successful?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Information Gathered through Active OS Fingerprinting	1.		
	2.		
	3.		
	4.		
	5.		
Information Gathered through Passive OS Fingerprinting	1.		
	2.		
	3.		
	4.		
	5.		
List of the Web servers and their OSes	1.		
	2.		
	3.		
	4.		
	5.		
Tools/Services Used	1.		
	2.		
	3.		

	4.
	5.

Results Analysis:

Test 2.2: Examine the Patches Applied to the Target OS

Target Organization				
URL				
List of the patches applied to the target OS	OS/Web Server/ Application	Patch Date	Version Number	OS Level
Tools Used	1.			
	2.			
	3.			
	4.			
	5.			

Results Analysis:

Test 2.3: Fingerprint the Services

Target Organization		
URL		
Commands Used	1.	
	2.	
	3.	
	4.	
	5.	
Service fingerprinting is performed successfully?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Successfully grabbed the banner from services?		<input type="checkbox"/> Yes <input type="checkbox"/> No
Protocol	Version of Server	
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
Nmap's Switches Used	1.	
	2.	
	3.	
	4.	
	5.	
Identified Open Services	1.	
	2.	
	3.	
	4.	
	5.	

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

Results Analysis:

Test 3: Vulnerability Research**Test 3.1: Search and Map the Target with the Associated Security Vulnerabilities**

Target Organization			
URL			
Identified vulnerabilities	OS Version	Type of Device	Type of Service
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

Test 3.2: Find Out the Security Vulnerability Exploits

Target Organization			
URL			
Successfully Identified the Security Vulnerability Exploits?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Identified Exploits and their Vulnerabilities	1.		
	2.		
	3.		
	4.		
	5.		
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

Test 4: Exploit Verification**Test 4.1: Run the Exploits against Identified Vulnerabilities**

Target Organization			
URL			
Executed the Exploits against Vulnerabilities Successfully?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Exploited vulnerabilities	Port	State Service	Version
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
Information obtained from Exploitation	1.		
	2.		
	3.		
	4.		
	5.		
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis: