EC-Council Licensed Penetration Tester

Methodology: Wireless Network Penetration Testing

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

Test 1: Discover the wireless networks

Target Organization				
URL				
Rogue Access Points				
	SSID	CHANNEL	FREQUENCY	LOCATION
1.				
2.				
3.				
4.				
5.				
6.				
Tools/Services Used	1. 2. 3. 4. 5.			

Results Analysis:

Test 2: Detect hidden SSIDs

Target Organization	
URL	
SSIDs Discovered on Interface	1. 2. 3. 4. 5.
Hidden SSIDs	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Check physical security of AP

Target Organization		
URL		
Physical Location of Authorized APs		
Physical Access to APs Is Controlled	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4: Detect wireless connections

Target Organization	
URL	
Scanning Methodologies	
Wireless Connections Detected using Active Scanning	**Wireless Connections Detected using Passive Scanning**
1.	1.
2.	2.
3.	3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Sniff the traffic between the AP and linked devices

Target Organization	
URL	
Information from gathered from Sniffed Traffic	
BSSID	STATION
PWR	PWR
Beacons	Packets
#Data	Probes
CH	Others:
HB	
ENC	
ESSID	
BSSID	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Create ad hoc associations with unsecured AP

Target Organization		
URL		
Ad Hoc Mode used	☐ YES	☐ NO
Ad Hoc Association to Unsecured AP	☐ YES	☐ NO
Enterprise Client Operating in Ad Hoc Mode		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 7: Create a rogue access point and try to create a promiscuous client

Target Organization		
URL		
Location of Rogue Access Point		
SSID Broadcast Disabled	☐ YES	☐ NO
AP behind Firewall	☐ YES	☐ NO
Promiscuous Client Creation Successful	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 8: Perform Denial-of-Service attack

Target Organization	
URL	
Deauth Command syntax used	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Attempt rapid traffic generation

Target Organization	
URL	
Source MAC	
Destination MAC	
BSSID	
Hosts on a bridged LAN	
Hosts on a wired LAN	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Jam the signal

Target Organization	
URL	
Device used to jam the signal	
Frequency used to jam the signal	
List of access points discovered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Attempt single packet decryption

Target Organization	
URL	
Source MAC address	
Destination MAC address	
Command syntax used	
First Pass	
Second Pass	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Perform fragmentation attack

Target Organization		
URL		
Packets received from AP	☐ YES	☐ NO
Obtained 1500 bytes of PRGA	☐ YES	☐ NO
Injection Attacks		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 13: Perform ARP poisoning attack

Target Organization		
URL		
IP Address of AP		
MAC Address of AP		
ARP Poisoning Attack Successful	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 14: Try to inject the encrypted packet

Target Organization	
URL	
Auth Frame	
Auth Type	
Share Key	
BSSID	
Source MAC	
Command syntax used	
Data read from prgafile.dat	1. BSSID: 2. Source MAC: 3. IV:
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Crack static WEP keys

Target Organization		
URL		
Information gathered by Cracking Static WEP Keys		
BSSID:		CIPHER:
PWR:		AUTH:
RXQ:		ESSID:
Beacons:		Others:
#Data:		
CH:		
MB:		
ENC:		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16: Crack WPA-PSK keys

Target Organization	
URL	
Command used to Monitor Traffic	
Command used to Collect Traffic Data	

Information gathered by Cracking WPA-PSK Keys	
BSSID:	CIPHER:
PWR:	AUTH:
RXQ:	ESSID:
Beacons:	Others:
#Data:	
CH:	
MB:	
ENC:	

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

Results Analysis:

Test 17: Check for MAC filtering

Target Organization		
URL		
Target Access Point used MAC Filtering	☐ YES	☐ NO
Fake Auth Commands		
Authentication Successful	☐ YES	☐ NO
Association Successful	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 18: Spoof MAC address

Target Organization		
URL		
Name of the SSID tested		
Spoofed MAC Address	1. 2. 3. 4. 5.	
New MAC Address and Vendor Settings		
MAC Filtering Active	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 19: Create direct connection to the wireless access point

Target Organization		
URL		
DHCP Enabled		
Wireless AP	☐ YES	☐ NO
Laptop	☐ YES	☐ NO
IP Address of Wireless AP		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 20: Attempt MITM attack

Target Organization	
URL	
Victim IP Address	
Victim MAC Address	
MITM IP Address	
MITM MAC Address	
Interesting Packets Captured	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: