EC-Council Licensed Penetration Tester

Methodology: Password Cracking Penetration Testing

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

PENETRATION

LICENSED

TESTER

Test 1: Identify the target person's personal profile

Target Organization	
URL	
Person Name	**Personal Information Obtained**
1.	
2.	
3.	
4.	
5.	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Perform non-electronic attacks

Target Organization			
URL			
Techniques Used	□ Shoulder Surfing	□ Dumpster Diving	□ Social Engineering
Person Name	**Personal Information Obtained**		
1.			
2.			
3.			
4.			
5.			
Tools/Services Used	1. ____________ 2. ____________ 3. ____________ 4. ____________		

Results Analysis:

____

____

____

____

____

____

Test 3: Build a dictionary of Word lists

Target Organization	
URL	
Person Name	**Dictionary Built Based on Personal Likings**
1.	
2.	
3.	
4.	
5.	
Equipment	**Dictionary Built Based on Default Passwords Supplied by the Manufacturer**
1.	
2.	
3.	
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______

Results Analysis:

______

______

______

______

______

______

Test 4: Attempt to Guess passwords

Target Organization	
URL	
List of Possible Passwords	1. 2. 3. 4. 5.
Successful guessed passwords	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Perform Brute-force and Dictionary attacks

Target Organization	
URL	
Target System's Username:	**Brute-Force Attack Techniques:**
1.	□ Plain Attack □ Dictionary Attack □ Hybrid Attack □ Complex Attack
2.	□ Plain Attack □ Dictionary Attack □ Hybrid Attack □ Complex Attack
3.	□ Plain Attack □ Dictionary Attack □ Hybrid Attack □ Complex Attack
Passwords Cracked	1. 2. 3.
Tools/Services Used	1. 2. 3. 4.

Results Analysis:

Test 6: Perform wire sniffing to capture passwords

Target Organization	
URL	
Target Network	**Passwords Captured**
	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Perform Man-in-the-Middle attack to collect passwords

Target Organization	
URL	
Target Communication Channels	**Passwords Collected**
1.	1.
2.	2.
3.	3.
Tools/Services Used	1. ________ 2. ________ 3. ________ 4. ________ 5. ________

Results Analysis:

____

____

____

____

____

____

Test 8: Perform Replay Attack to collect passwords

Target Organization	
URL	
Target Communication Channels	**Passwords Collected**
1.	1.
2.	2.
3.	3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Extract SAM file in Windows machines

Target Organization		
URL		
Windows Server IP Address tested	□ Yes	□ No
SAM File Obtained	□ Yes	□ No
Number of Users in the File	**Passwords Successfully Cracked**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
Passwords Obtained	1. 2. 3.	
Tools/Services Used	1. 2. 3. 4.	

Results Analysis:

Test 10: Perform Hash injection (Pass-the-Hash) attack

Target Organization		
URL		
Target Systems	**Hash Injection Attack Technique Successful**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
Passwords Obtained	1. 2. 3.	
Tools/Services Used	4. 5. 6. 7. 8.	

Results Analysis:

Test 11: Perform Rainbow attack (Perform password attack using Pre-Computed hashes)

Target Organization		
URL		
Target Systems	**Rainbow Attack Technique Successful**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
Passwords Obtained	1. 2. 3.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 12: Extract Cleartext passwords from an encrypted LM hash

Target Organization		
URL		
Target Systems	**Cleartext Passwords Extracted**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
Passwords Cracked	1. 2. 3.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 13: Perform password cracking using Distributed Network attack

Target Organization		
URL		
Target Systems	**Distributed Network Attack Successful**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
Passwords Cracked	1. 2. 3.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 14: Extract/etc/passwd and /etc/shadow files in Linux systems

Target Organization		
URL		
Linux Server IP Address tested	□ Yes	□ No
Password File Obtained	□ Yes	□ No
Number of Users in the File	**Passwords Successfully Cracked**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
Passwords Obtained	1. 2. 3.	
Tools/Services Used	1. 2. 3. 4.	

Results Analysis:

Test 15: Use automated passwords crackers to break password-protected files

Target Organization		
URL		
Target Systems	**Cracked Password-Protected Files**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
4.	□ Yes	□ No
5.	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16: Use Trojan/Spyware/Keyloggers to capture passwords

Target Organization		
URL		
Target Systems	**Captured Passwords**	
1.	□ Yes	□ No
2.	□ Yes	□ No
3.	□ Yes	□ No
4.	□ Yes	□ No
5.	□ Yes	□ No
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____