EC-Council Licensed Penetration Tester

Methodology: Stolen Laptop, PDAs, and Cell Phones Penetration Testing

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

Test 1: Look for the laptop login password

Target Organization		
URL		
Laptop Login Password		
Removed Login Password	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2: Check if the sensitive data is encrypted or not in the devices

Target Organization		
URL		
Devices		
Sensitive Data Encrypted	☐ YES	☐ NO
Extracted Sensitive Information	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3: Perform penetration testing in Android applications

Target Organization	
URL	
Methods used to Test Android Mobile Applications	1. 2. 3. 4. 5.
Personal Information Extracted from Cell Phones	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Perform PDA penetration testing

Target Organization		
URL		
Technique used to Crack PDA Password		
Encrypted Data can be Decrypted	☐ YES	☐ NO
Private Information Obtained using ActiveSync Attack	1. 2. 3. 4. 5.	
IR Port is Enabled	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 5: Look for sensitive information in the PDA or laptop by cracking MS Outlook

Target Organization		
URL		
Outlook Password Client is Protected	☐ YES	☐ NO
Sensitive Information Gathered from Email Messages	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Identify the sensitive data in the devices

Target Organization	
URL	
List Sensitive Documents	
☐ Company finance documents	☐ E-mail messages
☐ Excel spreadsheets	☐ Operations plan
☐ Word documents	
Extracted Sensitive Information	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Look for personal information in the stolen laptop

Target Organization	
URL	
Personal Information from Stolen Laptop	
☐ Bank Account Number:	
☐ Internet Shopping Account:	
☐ Credit Card Details:	
☐ Tax Return Information:	
☐ Passport Details:	
☐ Resume of the Host:	
☐ Check Digital Signature:	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Look for passwords

Target Organization	
URL	
Device	
List of Passwords	
☐ VNC Password	☐ Passwords stored in the registry
☐ E-mail account passwords	☐ FTP passwords
☐ Active directory passwords	☐ SSH/Telnet passwords
☐ Web site history passwords	☐ Application passwords
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Look for the company's infrastructure or finance documents

Target Organization	
URL	
Device	
List Sensitive Documents	
☐ Building plans:	
☐ Plan of operations:	
☐ Overseas operations and procedures:	
☐ Company handbooks or manuals:	
☐ Contracts and agreements:	
☐ NDA documents:	
☐ Bank statements:	
☐ Auditing information:	
☐ Insurance documents:	
Extracted Sensitive Document	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Extract the address book and phone numbers

Target Organization	
URL	
Device	
Phone Book Entries	
1.	6.
2.	7.
3.	8.
4.	9.
5.	10.
Information Extracted	
1.	6.
2.	7.
3.	8.
4.	9.
5.	10.

Results Analysis:

Test 11: Extract schedules and appointments

Target Organization	
URL	
Device	
Schedules and Appointments	
1.	6.
2.	7.
3.	8.
4.	9.
5.	10.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Extract information from applications installed on these devices

Target Organization	
URL	
Device	
Installed Applications	

Sensitive Data Collected from Installed Applications on the Device	
1.	6.
2.	7.
3.	8.
4.	9.
5.	10.

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

Results Analysis:

Test 13: Extract email messages from these devices

Target Organization	
URL	
Device Name	
Email Messages	1.
	2.
	3.
Extracted Sensitive Information	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Check for the BIOS password

Target Organization		
URL		
Device		
BIOS Password Enabled	☐ YES	☐ NO
Hard Disk set as Bootable Device in BIOS Setting	☐ YES	☐ NO
Different User Name and Password from the Domain's Logon	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 15: Look into the encrypted files

Target Organization		
URL		
Encrypted Files	☐ YES	☐ NO
Information Gathered from Decrypted Files		
1.	4.	
2.	5.	
3.	6.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16: Check cookies in web browsers

Target Organization	
URL	
Information Gathered from Web Browsers	
☐ Cookies:	
☐ History File:	
☐ Cache:	
☐ Temp File:	
☐ Recycle Bin:	
☐ Passwords:	
☐ Frequently Accessed Data:	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17: Attempt to enable wireless

Target Organization		
URL		
Company's LAN Network Located	☐ YES	☐ NO
SSID		
SSID Password Enabled	☐ YES	☐ NO
Technique used to Crack Password		
Connection Successful to the Company's Network	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis: