EC-Council Licensed Penetration Tester

Methodology: Email Security Penetration Testing

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

Test 1: Perform SMTP service fingerprinting

Target Organization	
URL	
Email System Security Auditing Begins	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Perform directory harvest attacks

Target Organization	
URL	
Directory harvest attack (DHA) is Commonly Used to	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Enumerate enabled SMTP subsystems and features

Target Organization	
URL	
Enabling SMTP Subsystems and Features	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Perform SMTP password brute-forcing

Target Organization	
URL	
Find out for Possible Vulnerabilities in the SMTP Server	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Perform NTLM overflows attack through SMTP authentication

Target Organization	
URL	
What is NTLM (NT LAN Manager) Authentication Mechanism	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Test for SMTP open relay

Target Organization	
URL	
Check with the SMTP Server Configuration	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Perform SMTP user enumeration

Target Organization	
URL	
RCPT TO: and VRFY Commands can be used for	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Perform POP3 password brute-forcing

Target Organization	
URL	
Find out POP3 Services used for Weak Passwords	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Perform IMAP brute-forcing

Target Organization	
URL	
Perform Authentication Process with the Brute-Forcing Method	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Test for IMAP process manipulation attack

Target Organization	
URL	
How to Escalate Authentication and Post Authentication	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Check for known vulnerabilities in mail servers and hosts

Target Organization	
URL	
Find out the Vulnerable Hosts and Mail Servers	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Check the patch status of mail server and host systems

Target Organization	
URL	
Find out all Hosts in the Target Network are Fully Patched	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Try to crack email passwords

Target Organization	
URL	
Note down the Cracked Email Address and Passwords	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Check whether anti-phishing software is enabled

Target Organization		
URL		
Anti-Phishing Software is Enabled	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 15: Check whether anti-spamming tools are enabled

Target Organization		
URL		
Anti-Spamming Tools are Enabled	□ Yes	□ No
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______	

Results Analysis:

______

______

______

______

______

______

Test 16: Try to perform email bombing

Target Organization	
URL	
Perform Email Bombing and List Down the Unwanted emails you have Discovered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17: Perform CLSID extension vulnerability test

Target Organization		
URL		
Check CLSID Extensions are Enabled	☐ Yes	☐ No
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____

____

Test 18: Perform VBS attachment vulnerability test

Target Organization	
URL	
Find the Virtual basic script (VBS) Attachment Vilnerability Test	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 19: Perform double file extension vulnerability test

Target Organization	
URL	
What is .vbs file Extensions	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 20: Perform long file name vulnerability test

Target Organization	
URL	
Check Long File Name Vulnerabilities	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 21: Perform malformed file extension vulnerability test

Target Organization	
URL	
Try to read the .HTA in your mail Attachment	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 22: Perform access exploit vulnerability test

Target Organization	
URL	
VBA (Visual Basic for Applications) Code and Find out the Vulnerabilities	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 23: Perform fragmented message vulnerability test

Target Organization	
URL	
How to Bypass the Anti-Virus Filters	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 24: Perform long subject attachment checking test

Target Organization	
URL	
Find the Vulnerabilities of Long Subject Attachments	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 25: Perform no file attachment vulnerability test

Target Organization	
URL	
Accessing the Mailbox by Sending for Vulnerability Test	
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______

Results Analysis:

______

______

______

______

______

______