EC-Council Licensed Penetration Tester

Methodology: VoIP Penetration Testing

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

PENETRATION

LICENSED

TESTER

Test 1: Test for eavesdropping

Target Organization	
URL	
Technique Used to Decode the Signaling Messages	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Test for flooding and logic attacks

Target Organization	
URL	
Spoofed IP Address Used for Flooding	
Technique Used to Exploit TCP Connection Process	
Flooding Techniques Used to Overload the Devices with VoIP Protocol Packets	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Test for Denial-of-Service (DoS) attack

Target Organization		
URL		
DoS/DDoS Condition Occurred	□ YES	□ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4: Test for call hijacking and redirection attack

Target Organization	
URL	
Victim Session Initiation Protocol (SIP) URI	
3xx Response Codes Classes to Redirect the Victim's Call	
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______

Results Analysis:

______

______

______

______

______

Test 5: Test for ICMP ping sweeps

Target Organization	
URL	
Active Hosts Identified	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Test for ARP pings

Target Organization	
URL	
Live Hosts Identified	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Test for TCP ping scans

Target Organization	
URL	
Active Hosts Identified	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Test for SNMP sweeps

Target Organization		
URL		
Active Hosts Identified		
“Public” Community String Used	□ YES	□ NO
Sensitive Information Gathered		
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____

____

Test 9: Test for port scanning and service discovery

Target Organization	
URL	
Target Host or Devices	
Method Used to Scan Active Services	1. 2. 3.
Vulnerabilities Discovered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9.1: TCP SYN Scan

Target Organization	
URL	
Scanned Ports	
Open Ports Discovered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9.2: UDP Scan

Target Organization	
URL	
Scanned Ports	
Open Ports Discovered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Test for host/device identification

Target Organization	
URL	
Method Used for Identification	
Identified Host or Devices	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Test for banner grabbing

Target Organization	
URL	
Remote Host	
Banner Grabbing Techniques Used	
□ Manual Banner Grabbing	□ Automated Banner Grabbing
Identified Services	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Test for SIP user/extension enumeration

Target Organization	
URL	
Enumeration Techniques Used	
□ REGISTER Username Enumeration	
□ INVITE Username Enumeration	
□ OPTIONS Username Enumeration	
□ Automated OPTIONS Scanning with Sipsak	
□ Automated REGISTER, INVITE and OPTIONS Scanning with SIPSCAN against SIP server	
□ Automated OPTIONS Scanning Using SIPSCAN against SIP Phones	
User Registration Information Recovered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Test for the automated OPTIONS scanning with sipsak

Target Organization	
URL	
SIP Service Issues Identified	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Test for the automated REGISTER, INVITE, and OPTIONS scanning with SIPSCAN against the SIP server

Target Organization	
URL	
Live SIP Extensions/ Users Information	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Test for enumerating the TFTP servers

Target Organization	
URL	
IP Address of the TFTP Server	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16: Test for SNMP enumeration

Target Organization	
URL	
Configuration Information Recovered	
□ Vendor Type Used	□ Mac Address
□ Operating System	□ Ports of UDP Services
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

______

______

______

______

______

______

Test 17: Test for sniffing TFTP configuration file transfers

Target Organization	
URL	
Sniffed TFTP Configuration Files	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18: Test for number harvesting and call pattern tracking

Target Organization	
URL	
Sniffed SIP Traffic	
From: and To: **Header Information**	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: