EC-Council Licensed Penetration Tester

Methodology: Router and Switches Penetration Testing

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

Router Penetration Testing

Test 1: Identify the router hostname

Target Organization	
URL	
IP address of the router	
Hostname of the router	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Port scan the router

Target Organization	
URL	

Open Ports	
☐ **7** Echo	☐ **113** IDENT
☐ **13** DayTime	☐ **115** Simple File Transfer Protocol (SFTP)
☐ **17** Quote of the Day (QOTD)	☐ **137** NetBIOS
☐ **20** File Transfer Protocol (FTP)	☐ **138** NetBIOS
☐ **21** File Transfer Protocol (FTP)	☐ **139** NetBIOS
☐ **22** Secure Socket Shell (SSH)	☐ **143** Internet Message Access Protocol (IMAP)
☐ **23** Telnet	☐ **161** Simple Network Management Protocol
☐ **25** SMTP	☐ **162** Simple Network Management Protocol
☐ **53** Domain Name System (DNS)	☐ **194** Internet Relay Chat (IRC)
☐ **63** Whois	☐ **443** HTTPS
☐ **66** SQL*net (Oracle)	Other Ports:
☐ **70** Gopher	
☐ **79** Finger	
☐ **80** HTTP	
☐ **88** Kerberos	
☐ **101** Host Name Server	
☐ **109** Post Office Protocol 2 (POP2)	
☐ **110** Post Office Protocol 3 (POP3)	

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

Results Analysis:

Test 3: Identify the router operating system and its version

Target Organization	
URL	
IP address of the router tested	
Operating System and its version	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Identify protocols running

Target Organization	
URL	
IP address of the router tested	
Protocols running	
☐ RIP	☐ OSPF
☐ RIPv2	☐ BGP
☐ IGRP	☐ Others
☐ EIGRP	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Testing for package leakage at the router

Target Organization		
URL		
IP address of the router tested		
Package Leak	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Test for router misconfigurations

Target Organization		
URL		
IP address of the router tested		
Is router misconfigured?	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 7: Test for VTY/TTY connections

Target Organization		
URL		
IP address of the router tested		
Is console access possible?	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 8: Test for router running modes

Target Organization		
URL		
IP address of the router tested		
Modes	☐ USER MODE	☐ PRIVILEGE MODE
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 9: Test for SNMP capabilities

Target Organization	
URL	
IP address of the router tested	
SNMP Strings used	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Perform SNMP bruteforcing

Target Organization	
URL	
IP address of the router tested	
SNMP community strings	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Test for TFTP connections

Target Organization		
URL		
IP address of the router tested		
TFTP Allowed	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 12: Test if finger is running on the router

Target Organization		
URL		
IP address of the router tested		
Finger Service running	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 13: Test for CDP protocol running on the router

Target Organization		
URL		
IP address of the router tested		
CDP Protocol running	☐ YES	☐ NO
CDP Messages		
☐ Device ID (hostname)		☐ IOS software version being used
☐ Port ID (port information about the sender)		☐ Capabilities of the router
☐ Operating system platform		☐ Network IP address
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 14: Test for NTP protocol

Target Organization		
URL		
IP address of the router tested		
NTP Protocol running	☐ YES	☐ NO
Router Synchronized	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 15: Test for access to router console port

Target Organization		
URL		
IP address of the router tested		
Physical console access possible	☐ YES	☐ NO
Console access on router is password protected	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16: Test for loose and strict source routing

Target Organization		
URL		
IP address of the router tested		
Routing	☐ Loose Source Routing	☐ Strict Source Routing
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 17: Test for IP spoofing/IP

Target Organization		
URL		
IP address of the router tested		
IP Spoofing possible	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 18: Test for handling bugs

Target Organization		
URL		
IP address of the router tested		
Test Successful	☐ YES	☐ NO
ACLs used on the router	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 19: Test ARP attacks

Target Organization		
URL		
IP address of the router tested		
ARP spoofing is possible against the router	☐ YES	☐ NO
Victim IP address		
Victim MAC address		
Poisoned IP address		
Poisoned MAC address		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 20: Test for routing protocol assessment

Target Organization		
URL		
IP address of the router tested		
Weak authentication present	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 21: RIP testing

Target Organization	
URL	
IP address of the router tested	
RIP v1	Authentication:
RIP v2	Authentication:
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 22: Test for OSPF protocol

Target Organization	
URL	
IP address of the router tested	
OSPF protocol present	Authentication:
Misconfigured?	Authentication:
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 23: Test BGP protocol

Target Organization		
URL		
IP address of the router tested		
BGP Protocol present	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 24: Test for EIGRP protocol

Target Organization		
URL		
IP address of the router tested		
EIGRP Protocol present	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 25: Test router denial-of-service attacks

Target Organization		
URL		
IP address of the router tested		
Malformed Packet Attack	☐ YES	☐ NO
Packet Flood Attacks	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 26: Test router's HTTP capabilities

Target Organization	
URL	
IP address of the router tested	
Port Used to Connect	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 27: Test through HSRP attack

Target Organization		
URL		
IP address of the router tested		
HSRP group forwarded to IP address	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Switch Penetration Testing

Test 1: Testing address of cache size

Target Organization	
URL	
Frame size relayed	
Address Cache Size	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Data integrity and error checking test

Target Organization	
URL	
Frame Size	
Traffic Rate	
Data Pattern	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Testing for back-to-back frame capacity

Target Organization	
URL	
Number of frames sent at once	
Inter-frame gaps	
Number of frames forwarded by the switch	
Number of test rerun	
Capacity detected	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Testing for frame loss

Target Organization	
URL	
Count the frames that are transmitted	
Frame loss equation	
Measurement	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Testing for latency

Target Organization	
URL	
Method used	
Latency detected	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Testing for throughput

Target Organization	
URL	
Count the frames	
The rate of the offered stream	
Throughput	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Test for frame error filtering

Target Organization	
URL	
Frame Size	
Illegal frame types	
Traffic Rate	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Fully meshed test

Target Organization	
URL	
Frame Size	
Traffic Rate	
Traffic Data Type	
DUT setup	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Stateless QoS functional test

Target Organization	
URL	
Frame size	
Duration	
Traffic Rate	
DUT-QoS	
DUT-Line speed	
DUT-QoS type	
DUT-QoS Policies	
DUT-Queue type	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Spanning tree network convergence performance test

Target Organization	
URL	
Test ports	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: OSPF performance test

Target Organization	
URL	
Frame Size	
Traffic Rate	
OSPF Parameters	
DUT setup	
DUT OSPF Area	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Test for VLAN hopping

Target Organization	
URL	
Dynamic Trunking Protocol	
DTP States	
DTP Negotiation	
VLAN Hopping	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Test for MAC table flooding

Target Organization	
URL	
Content Addressable Memory	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Testing for ARP attack

Target Organization	
URL	
MAC address	
IP address	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Check for VTP attack

Target Organization	
URL	
Command Output	
Cat2950#show vtp status	
VTP Version	
Configuration Revision	
Maximum VLANs supported locally	
Number of existing VLANs	
VTP Operating Mode	
VTP Domain Name	
VTP Pruning Mode	
VTP V2 Mode	
VTP Traps Generation	
MD5 digest	
Configuration last modified by	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16: Automated tool for switch

Target Organization	
URL	
Scanned Status for Network Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: