EC-Council Licensed Penetration Tester

Methodology: Internal Network Penetration Testing

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

Test 1: Map the internal network

Target Organization		
URL		
List the Network Devices	**Discovered**	**Make and Model**
Hubs	□	
Switches	□	
Servers	□	
Printers	□	
Workstations	□	
Wireless Access Points	□	
Firewalls	□	
Proxy Servers	□	
No. of Client Computers	□	
Others	□	1. --------------------------------------- 2. --------------------------------------- 3. --------------------------------------
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2: Scan the network for live hosts

Target Organization	
URL	
Subnet scanned	
List the IP Address of live hosts	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25.

	26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Port scan individual machines

Target Organization	
URL	

	IP Address	**Machine Name**	**Ports Open**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			

Tools/Services Used

1. ____________________
2. ____________________
3. ____________________
4. ____________________
5. ____________________

Results Analysis:

Test 4: Try to gain access using known vulnerabilities

Target Organization	
URL	
IP Address Tested	
Machine Name	
Vulnerability Exploited	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24.

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

Results Analysis:

Test 5: Attempt to establish null sessions

Target Organization		
URL		
IP Address Tested		
Machine Name		
Is Null Session Attempted Successful?	☐ Yes	☐ No
If Successful, list the Enumerated Usernames and Other Information here	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22.	

All Rights Reserved. Reproduction is Strictly Prohibited.

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

Results Analysis:

Test 6: Enumerate users

Target Organization		
URL		
IP Address Tested		
Machine Name		
Enumerating Users, Password Policies, and Group Policies based on the Established Null Session is Successful	□ Yes	□ No
If Successful, list the Information Obtained here	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20.	

All Rights Reserved. Reproduction is Strictly Prohibited.

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

Results Analysis:

Test 7: Sniff the network using Wireshark

Target Organization		
URL		
Is Sniffing the Network Successful?	□ Yes	□ No
Interesting Traffic Traversing on the Network	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 8: Sniff POP3/FTP/Telnet passwords

Target Organization			
URL			
List the passwords sniffed	**Protocol**	**Username**	**Password**
	1.		
	2.		
	3.		
	4.		
	5.		
	6.		
	7.		
	8.		
	9.		
	10.		
Tools/Services Used	1.		
	2.		
	3.		
	4.		
	5.		

Results Analysis:

Test 9: Sniff email messages

Target Organization		
URL		
Is Sniffing Email Traffic that goes through the Network Successful?	☐ Yes	☐ No
List the Email Messages Sniffed	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18.	
Tools/Services Used	1. 2. 3. 4. 5.	

All Rights Reserved. Reproduction is Strictly Prohibited.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 10: Attempt replay attacks

Target Organization	
URL	
Victim IP Address Targeted	
Original Message Captured	
Replayed Messages	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Attempt ARP poisoning

Target Organization	
URL	
Victim IP Address	
Poisoned IP Address	
Victim MAC Address	
Poisoned MAC Address	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 12: Attempt MAC flooding

Target Organization		
URL		
Is Flooding the Network with Bogus MAC Addresses Successful?	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 13: Conduct a Man-in-the-Middle attack

Target Organization		
URL		
Victim Machine		
Target Machine		
MITM Machine		
Intercepted the Communication Channel between the Victim and the Target Successfully?	□ Yes	□ No
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____

____

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 14: Attempt DNS poisoning

Target Organization		
URL		
Victim Machine		
List the Hosts added into the Cache of a DNS Server to Corrupt the DNS Tables	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17.	
Is DNS Poisoning Attempt Successful	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 15: Try to log in to a console machine

Target Organization		
URL		
Victim Machine		
Username		
Default Password		
Is Logging into a Console Machine Successful?	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16: Boot the PC using alternate OS and steal the SAM file

Target Organization	
URL	
Victim Machine	
Username Reset	
Password Reset	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 17: Attempt to plant a software keylogger to steal passwords

Target Organization		
URL		
Victim Machine		
Installation of Software Keylogger on the Victim Machine Successful	☐ Yes	☐ No
Captured Keystrokes	1. 2. 3. 4. 5. 6. 7. 8.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 18: Attempt to plant a hardware keylogger to steal passwords

Target Organization		
URL		
Victim Machine		
Installation of Hardware Keylogger on the Victim Machine Successful	□ Yes	□ No
Captured Keystrokes	1. 2. 3. 4. 5. 6. 7. 8.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 19: Attempt to plant spyware on the target machine

Target Organization		
URL		
Victim Machine		
Installed Spyware on the Victim Machine Successfully	□ Yes	□ No
Information Obtained	1. 2. 3. 4. 5. 6. 7. 8.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 20: Attempt to plant a Trojan on the target machine

Target Organization		
URL		
Victim Machine		
Installed Trojan on the Victim Machine Successfully	□ Yes	□ No
Information Obtained	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 21: Attempt to create a backdoor account on the target machine

Target Organization		
URL		
Victim Machine		
Backdoor Account on the Target Machine is Created Successfully	□ Yes	□ No
Backdoor Behavior		
Information Obtained	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 22: Attempt to bypass anti-virus software installed on the target machine

Target Organization		
URL		
Victim Machine		
Anti-Virus Installed on the Victim Machine		
Details of the Program Created to bypasses the Anti-Virus rules	1. 2. 3. 4.	
Anti-Virus Evaded	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 23: Attempt to send a virus using the target machine

Target Organization		
URL		
Victim Machine		
Type of Virus		
Successfully sent Virus via Target Machine to Spread throughout the Network	□ Yes	□ No
Viruses Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 24: Attempt to plant rootkits on the target machine

Target Organization		
URL		
Victim Machine		
Type of Rootkit		
Installed Rootkit on the target machine Successfully	□ Yes	□ No
Rootkits Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____

____

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 25: Hide sensitive data on target machines

Target Organization	
URL	
Victim Machine	
Steganography Technique used	
Sensitive Data Hidden	□ IP addresses □ Source code □ Pictures □ Word documents Spreadsheets □ Hacking Tools □ Secret Information □ Pornography images □ Others
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 26: Hide hacking tools and other data on target machines

Target Organization	
URL	
Victim Machine	
Steganography Technique used	
Hacking Tools and other Data Hidden	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 27: Use various steganography techniques to hide files on target machines

Target Organization	
URL	
Victim Machine	
Steganography Techniques used	1. 2. 3. 4. 5.
Hidden Data	1. 2. 3. 4. 5. 6. 7. 8.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 28: Escalate user privileges

Target Organization		
URL		
Victim Machine		
Escalated User Privileges Successfully	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 29: Capture POP3 traffic

Target Organization		
URL		
Filter Used		
Captured POP3 Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 30: Capture SMTP traffic

Target Organization		
URL		
Filter Used		
Captured Incoming and Outgoing SMTP Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 31: Capture IMAP email traffic

Target Organization		
URL		
Filter Used		
Captured IMAP Email traffic Successfully	☐ Yes	☐ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 32: Capture the communications between the FTP client and FTP server

Target Organization		
URL		
Captured the communications between the FTP client and FTP server Successfully	□ Yes	□ No
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____

____

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 33: Capture HTTP traffic

Target Organization		
URL		
Filter Used		
Captured HTTP Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 34: Capture HTTPS traffic

Target Organization		
URL		
Filter Used		
Captured HTTPS Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Offset: Timeline: Duration: Method: Result: Received: Type URL: Redirect URL: Request Headers Info: Response Headers Info: Others:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 35: Capture RDP traffic

Target Organization		
URL		
Filter Used		
Captured RDP Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 36: Capture VoIP traffic

Target Organization		
URL		
Filter Used		
Captured VoIP Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 37: Run Wireshark with this filter ip.src == ip_address

Target Organization		
URL		
Filter Used		
Source ip_address		
Captured Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 38: Run Wireshark with this filter ip.dst == ip_address

Target Organization		
URL		
Filter Used		
Destination ip_address		
Captured Traffic Successfully	☐ Yes	☐ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 39: Run Wireshark with this filter tcp.dstport == port_no

Target Organization		
URL		
Filter Used		
Port Number		
Captured Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 40: Run Wireshark with this filter ip.addr == ip_address

Target Organization		
URL		
Filter Used		
Target IP Address		
Captured Traffic Successfully	□ Yes	□ No
Description of the Packets Captured	Time: Source: Destination: Protocol: Length: Info:	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 41: Spoof the MAC address

Target Organization		
URL		
Victim Machine		
Spoofed the MAC Address Successfully	□ Yes	□ No
Spoofed MAC Address		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 42: Poison the victim's IE proxy server

Target Organization		
URL		
Victim Machine		
Poisoned the Victim's IE Proxy Server Successfully	□ Yes	□ No
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______	

Results Analysis:

______

______

______

______

______

______

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 43: Attempt session hijacking on telnet traffic

Target Organization		
URL		
Implemented Session Hijacking Technique on Telnet Traffic Successfully	□ Yes	□ No
Telnet Commands	1. ______ 2. ______ 3. ______	
Tools/Services Used	1. ______ 2. ______ 3. ______ 4. ______ 5. ______	

Results Analysis:

____

____

____

____

____

____

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 44: Attempt session hijacking on FTP traffic

Target Organization		
URL		
Implemented Session Hijacking Technique on FTP Traffic Successfully	☐ Yes	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 45: Attempt session hijacking on HTTP traffic

Target Organization		
URL		
Implemented Session Hijacking Technique on HTTP Traffic Successfully	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis: