# EC-Council Licensed Penetration Tester

## Methodology: External Penetration Testing

| Penetration Tester: | | | |
|---|---|---|---|
| Organization: | | | |
| Date: | | Location: | |

## Test 1: Inventory the company's external infrastructure

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **List of cities the company is located** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| **Company's Website Links** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| **World Map of the Cities where the Company Resides** | |
| **External Resource of the Target's Networks** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

| | |
|---|---|
| **Other Information Recovered** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

## Test 2: Create topological map of the network

| Target Organization | |
|---|---|
| **URL** | |
| **Create Topological Map of the Network** | LAN/WAN Design |
| | Peer-to-Peer (P2P) |
| | Network Topologies |

| | |
|---|---|
| | Network Cabling |
| | Customers and Partners Networked to other Systems |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

                                              

**Test 3: Identify the IP address of the targets**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Mail Server IP Address** | |
| **Web Server IP Address** | |
| **Proxy Server IP Address** | |
| **DNS Server IP Address** | |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 4: Locate the traffic route that goes to the web servers**

| Target Organization | |
|---|---|
| URL | |
| IP Address Traced | |
| **Tracert Results** | |
| **Total Number of Hops** | | **Timeout** | |

| **IP Addresses Hoped** |
|---|
| 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| 6. |
| 7. |
| 8. |
| 9. |
| 10. |
| 11. |
| 12. |
| 13. |
| 14. |
| 15. |
| 16. |
| 17. |
| 18. |
| 19. |
| 20. |
| 21. |

| | |
|---|---|
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 5: Locate TCP traffic path to the destination**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **TCP Traffic Path to the Destination is located Successfully** | ☐  Yes | ☐  No |
| **IP Address Traced** | | |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 6: Locate UDP traffic path to the destination**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **UDP Traffic Path to the Destination is located Successfully** | ☐ Yes | ☐ No |
| **IP Address Traced** | | |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 7: Identify the physical location of the target servers

| Target Organization | | | | |
|---|---|---|---|---|
| URL | | | | |
| Physical location of the target Servers | IP Address | City Located | Country | Hosted by Vendor |
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 8: Examine the use of IPv6 at the remote location

| Target Organization | |
|---|---|
| URL | |
| IP Addresses probed for IPV6 | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| List of IP addresses using IPv6 | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| Tools/Services Used | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

## Test 9: Look Up domain registry for IP information

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **IP Address** | |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

## Test 10: Find IP block information about the target

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **Found IP Block Information about the Target Successfully** | ☐ Yes | ☐ No |
| **List the IP Block Information** | | |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

**Test 11: Locate the ISP servicing the client**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Name of the ISP** | |
| **Pricing Plans** | 1.<br>2.<br>3. |
| **Services Provided** | 1.<br>2.<br>3.<br>4. |
| **Which other companies are assigned IP address from the same block** | 1.<br>2.<br>3.<br>4. |
| **Tools/Services Used** | 1.<br>2.<br>3.<br>4. |

**Results Analysis:**

## Test 12: Port scan every port (65,536) on the target's network

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **IP Address Tested** | | |
| **Performed Complete Port Scan of the Target Network Successfully** | ☐ Yes | ☐ No |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. | |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

**Test 13: List open ports**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **IP Address Tested** | |
| **List Open Ports Identified from Test 12 and their associated Services** | 1. <br> 2. <br> 3. <br> 4. <br> 5. <br> 6. <br> 7. <br> 8. <br> 9. <br> 10. <br> 11. <br> 12. <br> 13. <br> 14. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. |

**Results Analysis:**

**Test 14: List closed ports**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **IP Address Tested** | |
| **List the Ports that are Closed** | 1. <br> 2. <br> 3. <br> 4. <br> 5. <br> 6. <br> 7. <br> 8. <br> 9. <br> 10. <br> 11. <br> 12. <br> 13. <br> 14. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

## Test 15: List suspicious ports that are half open/closed

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **IP Address Tested** | |
| **List the Suspicious Ports that are half open/closed** | 1. <br> 2. <br> 3. <br> 4. <br> 5. <br> 6. <br> 7. <br> 8. <br> 9. <br> 10. <br> 11. <br> 12. <br> 13. <br> 14. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. |

**Results Analysis:**

_____

_____

_____

_____

_____

### Test 16: Use SYN scan on the target and see the response

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **IP Address Scanned** | | |
| **Command Used** | | |
| **Performed SYN Scan on the Target Successfully** | ☐ Yes | ☐ No |
| **Response Received** | | |
| **Tools/Services Used** | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 17: Use connect scan on the target and see the response**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **IP Address Scanned** | | |
| **Command Used** | | |
| **Performed Connect Scan on the Target Successfully** | ☐  Yes | ☐  No |
| **Response Received** | | |
| **Tools/Services Used** | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 18: Use XMAS scan on the target and see the response**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **IP Address Scanned** | | |
| **Command Used** | | |
| **Performed XMAS Scan on the Target Successfully** | ☐  Yes | ☐  No |
| **Response Received** | | |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

## Test 19: Use FIN scan on the target and see the response

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **IP Address Scanned** | | |
| **Command Used** | | |
| **Performed FIN Scan on the Target Successfully** | ☐  Yes | ☐  No |
| **Response Received** | | |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 20: Use NULL scan on the target and see the response**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **IP Address Scanned** | | |
| **Command Used** | | |
| **Performed NULL Scan on the Target Successfully** | ☐  Yes | ☐  No |
| **Response Received** | | |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 21: Use fragmentation scanning and examine the response**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **IP Address Scanned** | | |
| **Command Used** | | |
| **Performed Fragmentation Scan on the Target Successfully** | ☐ Yes | ☐ No |
| **Response Received** | | |
| **Tools/Services Used** | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 22: Firewalk on the router's gateway and guess the access list**

| Target Organization | |
|---|---|
| URL | |
| IP Address Firewalked | |
| Response Received | |
| Tools/Services Used | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 23: Examine TCP sequence number prediction

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **IP Address Tested** | |
| **Command Used** | |
| **Sequence Numbers Predicted** | 1. <br> 2. <br> 3. <br> 4. <br> 5. <br> 6. <br> 7. <br> 8. <br> 9. <br> 10. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 24: Examine the use of standard and non-standard protocols

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **IP Address Tested** | |
| **Standard Protocols Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| **Non-Standard Protocols Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 25: Examine IPID sequence number prediction

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **IP Address Tested** | |
| **IPID number predicted** | 1. <br> 2. <br> 3. <br> 4. <br> 5. <br> 6. <br> 7. <br> 8. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

**Test 26: Examine the system uptime of target**

| Target Organization | | | | | |
|---|---|---|---|---|---|
| URL | | | | | |
| **Server** | **OS** | **Last Seen** | **IP Address** | **Netblock Owner** | **Uptime** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ | | | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 27: Examine the operating system used for different targets

| Target Organization | |
|---|---|
| URL | |

| Server | Operating System Used |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |
| 10. | |
| 11. | |

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

**Results Analysis:**

_____

_____

_____

_____

_____

_____

## Test 28: Examine the patches applied to the operating system

| Target Organization | | | | |
|---|---|---|---|---|
| URL | | | | |
| **OS** | **Server** | **Last Seen** | **IP Address** | **Netblock Owner** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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

**Results Analysis:**

**Test 29: Locate the DNS record of the domain and attempt DNS hijacking**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Domain Name Tested** | |
| **Domain registered at (http location)** | |
| **Authentication used to logon** | |
| **Username** | |
| **Password** | |
| **Original DNS IP Address** | |
| **Fake DNS IP Address Redirected** | |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 30: Download applications from the company's website and reverse engineer the binary code**

| Target Organization | |
|---|---|
| URL | |

| Downloaded Application from URL | Name of the Application | Type of Application |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |

| Information looked at by Reverse Engineering the Binary Code | 1. _____ |
|---|---|
| | 2. _____ |
| | 3. _____ |
| | 4. _____ |
| | 5. _____ |
| | 6. _____ |
| | 7. _____ |

| Tools/Services Used | 1. _____ |
|---|---|
| | 2. _____ |
| | 3. _____ |
| | 4. _____ |
| | 5. _____ |

**Results Analysis:**

**Test 31: List programming languages used and application software to create various programs from the target server**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Type of Application** | ☐ Commercial ᐧ ☐ In-House |
| **Programming Languages Used by Web Application** | ☐ AppleScript<br>☐ C<br>☐ AWK<br>☐ C++<br>☐ JavaScript<br>☐ C#<br>☐ PERL<br>☐ COBOL<br>☐ PHP<br>☐ Java<br>☐ Python<br>☐ J++<br>☐ Ruby<br>☐ J#<br>☐ Tcl<br>☐ PowerBuilder<br>☐ VBScript<br>☐ Visual Basic<br>☐ Others: _____<br><br>_____ |
| **Tools/Services Used** | 1.<br>2.<br>3.<br>4. |

**Results Analysis:**

## Test 32: Look for error and custom web pages

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **List of Tested URL Strings** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____<br>6. _____<br>7. _____<br>8. _____ |
| **Error Message Location URL's** | 1. _____<br>2. _____<br>3. _____<br>4. _____ |
| **Content of the Message** | |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____ |

**Results Analysis:**

_____

_____

_____

_____

## Test 33: Guess different subdomain names and analyze different responses

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Main Domain** | |
| **List of Sub Domain Names and their Responses** | 1. <br> 2. <br> 3. <br> 4. <br> 5. <br> 6. <br> 7. <br> 8. <br> 9. <br> 10. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

**Test 34: Examine the session variables**

| Target Organization | |
|---|---|
| URL | |
| Website URL tested | |

| Session variable | Value |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |
| 10. | |
| 11. | |

| Tools/Services Used | 1. _____ |
|---|---|
| | 2. _____ |
| | 3. _____ |
| | 4. _____ |
| | 5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

**Test 35: Examine cookies generated by the server**

| Target Organization | |
|---|---|
| URL | |
| Website URL tested | |

| Cookie Name | Value | Cookie is Encrypted | | Content Stored in Cookie | Expiry Date of Cookie |
|---|---|---|---|---|---|
| 1. | | ☐ Yes | ☐ No | | |
| 2. | | ☐ Yes | ☐ No | | |
| 3. | | ☐ Yes | ☐ No | | |
| 4. | | ☐ Yes | ☐ No | | |
| 5. | | ☐ Yes | ☐ No | | |
| 6. | | ☐ Yes | ☐ No | | |
| 7. | | ☐ Yes | ☐ No | | |
| 8. | | ☐ Yes | ☐ No | | |
| 9. | | ☐ Yes | ☐ No | | |
| 10. | | ☐ Yes | ☐ No | | |
| 11. | | ☐ Yes | ☐ No | | |
| 12. | | ☐ Yes | ☐ No | | |
| **Tools/Services Used** | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | | | |

**Results Analysis:**

_____

_____

_____

_____

## Test 36: Examine the access controls used in the web applications

| Target Organization | |
|---|---|
| URL | |

| Website Login Pages Tested | Authentication Used |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |
| 10. | |
| 11. | |
| 12. | |

| Tools/Services Used | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ |
|---|---|

**Results Analysis:**

_____

_____

_____

_____

_____

_____

## Test 37: Brute force URL injections and session tokens

| Target Organization | | |
|---|---|---|
| URL | | |
| Website URL Tested | | |
| **URL Location** | **Injected Value** | **Response** |
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |
| 11. | | |
| **Tools/Services Used** | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

**Test 38: Check for directory consistency and page naming syntax of the web pages**

| Target Organization | |
|---|---|
| URL | |

| Web Page URL | Directory Consistency and Page Naming Syntax |
|---|---|
| 1. | ☐ Logical directory<br>☐ Files named based on naming conventions<br>☐ Repository for images, pdf, and other documents<br>☐ Repository for sensitive information<br>☐ Structured links and pages<br>☐ Site outline |
| 2. | ☐ Logical directory<br>☐ Files named based on naming conventions<br>☐ Repository for images, pdf, and other documents<br>☐ Repository for sensitive information<br>☐ Structured links and pages<br>☐ Site outline |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ |

**Results Analysis:**

_____

_____

_____

_____

## Test 39: Look for sensitive information in web page source code

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Website URL Tested** | |
| **Source Code Leakage** | 1. |
| | 2. |
| | 3. |
| | 4. |
| | 5. |
| | 6. |
| | 7. |
| | 8. |
| | 9. |
| | 10. |
| **Tools/Services Used** | 1. |
| | 2. |
| | 3. |
| | 4. |
| | 5. |

**Results Analysis:**

## Test 40: Attempt URL encodings on the web pages

| Target Organization | |
|---|---|
| URL | |

| Web Page | URL Encodings | Response Received |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |
| 11. | | |
| 12. | | |

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

**Results Analysis:**

_____

_____

_____

_____

_____

_____

## Test 41: Try buffer overflow attempts at input fields

| Target Organization | |
|---|---|
| URL | |

| Web Page | Buffer Overflow Text Attempted | Response Received |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |
| 11. | | |
| 12. | | |

| Tools/Services Used | |
|---|---|
| | 1. |
| | 2. |
| | 3. |
| | 4. |

**Results Analysis:**

**Test 42: Try Cross Site Scripting (XSS) techniques**

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| **Web Page Tested** | **Vulnerabilities in Script** | **Cross Site Scripting Attempted** | **Response Received** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |
| 11. | | | |
| 12. | | | |
| **Tools/Services Used** | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 43: Record and replay the traffic to the target web server and note the response**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Website URL** | |
| **Recorded Browser Sessions** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| **Replay Packet Size** | |
| **Response Received** | |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

## Test 44: Try various SQL injection techniques

| Target Organization | |
|---|---|
| URL | |
| Website URL Tested | |
| Tested Strings | ☐ ' or 1=1-- <br> ☐ " or 1=1-- <br> ☐ or 1=1-- <br> ☐ ' or 'a'='a <br> ☐ " or "a"="a <br> ☐ ') or ('a'='a <br> ☐ ") or ("a"="a |
| Attempted Locations | ☐ Form field's <br> ☐ Directly in URL <br> ☐ Login screens <br> ☐ Feedback forms <br> ☐ Guestbook |
| Tools/Services Used | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 45: Examine hidden fields**

| Target Organization | |
|---|---|
| URL | |

| Web Page | Hidden fields | Information Revealed |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |

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

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 46: Examine e-commerce and payment gateways handled by the web server**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **In-house built e-commerce gateway** | |
| **Outsourced e-commerce gateway** | |
| **Program Logic** | |
| **How Payments are Handled** | |
| **Confirmation Emails** | |
| **Minimum Order Amount** | |
| **Account and Merchant ID** | |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 47: Examine welcome messages, error messages, and debug messages

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Web Application Welcome Message** | |
| **Web Application Error Messages** | 1. <br> 2. <br> 3. <br> 4. |
| **Web Application Intrusion Warning Messages** | 1. <br> 2. <br> 3. <br> 4. |
| **Web Application Debugging Messages** | 1. <br> 2. <br> 3. <br> 4. |
| **Web Application Site Maintenance Messages** | 1. <br> 2. <br> 3. <br> 4. |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

**Test 48: Probe the service by SMTP mail bouncing**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **Mail Sent to** | | |
| **SMTP Bounced Back the Mail** | ☐ Yes | ☐ No |
| **Search in the Bounce Mail** | Server Name: <br><br> Version: <br><br> Services Running on Server: | |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. | |

**Results Analysis:**

**Test 49: Grab the banner of HTTP servers**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **Captured the Banner of HTTP Server Successfully** | ☐  Yes | ☐  No |
| **Identified HTTP Web Server** | | |
| **Tools/Services Used** | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 50: Grab the banner of SMTP servers

| Target Organization | | |
|---|---|---|
| URL | | |
| Captured the Banner of SMTP Server Successfully | ☐ Yes | ☐ No |
| Tools/Services Used | 1. _____ | |
| | 2. _____ | |
| | 3. _____ | |
| | 4. _____ | |
| | 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 51: Grab the banner of POP3 servers**

| Target Organization | |
|---|---|
| URL | |
| Captured the Banner of POP3 Server Successfully | ☐ Yes       ☐ No |
| Tools/Services Used | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

_____

**Test 52: Grab the banner of FTP servers**

| Target Organization | | |
|---|---|---|
| URL | | |
| Captured the Banner of FTP Server Successfully | ☐ Yes | ☐ No |
| Tools/Services Used | 1. | |
| | 2. | |
| | 3. | |
| | 4. | |
| | 5. | |

**Results Analysis:**

**Test 53: Identify the web extensions used at the server**

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Web Extensions Discovered** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |
| **Web Server Type and Version** | |
| **Tools/Services Used** | 1. <br> 2. <br> 3. <br> 4. <br> 5. |

**Results Analysis:**

## Test 54: Try to use an HTTPS tunnel to encapsulate traffic

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **Encapsulated Traffic using HTTPS Tunnel Successfully** | ☐  Yes | ☐  No |
| **Tools/Services Used** | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 55: OS fingerprint target servers**

| Target Organization | |
|---|---|
| URL | |

| Target Server's IP Address | Operating System Used |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |

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

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 56: Check for ICMP responses**

| | | |
|---|---|---|
| **Target Organization** | | |
| **URL** | | |
| **Target System IP Address** | | |
| **Performed ICMP Scan Successfully** | ☐ Yes | ☐ No |
| **Response Received** | | |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 57: Check for ICMP responses from broadcast address

| | |
|---|---|
| **Target Organization** | |
| **URL** | |
| **Broadcast Address Used on the Client's Subnet** | |
| **Tools/Services Used** | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ |

**Results Analysis:**

**Test 58: Port scan DNS servers (TCP/UDP 53)**

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| Target System IP Address | Port | State | Service |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ | | |
| | 2. _____ | | |
| | 3. _____ | | |
| | 4. _____ | | |
| | 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 59: Port scan TFTP servers (Port 69)

| Target Organization | |
|---|---|
| URL | |
| Command Used | |

| Target System IP Address | Port | State |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |

| Tools/Services Used | |
|---|---|
| | 1. _____ |
| | 2. _____ |
| | 3. _____ |
| | 4. _____ |
| | 5. _____ |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 60: Test for NTP ports (Port 123)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 61: Test for SNMP ports (Port 161)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. ___ <br> 2. ___ <br> 3. ___ <br> 4. ___ <br> 5. ___ | | |

**Results Analysis:**

_____
_____
_____
_____
_____

## Test 62: Test for Telnet ports (Port 23)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 63: Test for LDAP ports ( Port 389)**

| Target Organization | | |
|---|---|---|
| URL | | |
| Command Used | | |
| **Target System IP Address** | **Port** | **LDAP Query Response** |
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| **Tools/Services Used** | 1. | |
| | 2. | |
| | 3. | |
| | 4. | |
| | 5. | |

**Results Analysis:**

## Test 64: Test for NetBIOS ports ( Ports 135-139, 445)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| Target System IP Address | Port | State | Service |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

**Test 65: Test for SQL server ports (Port 1433, 1434)**

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ <br> 2. _____ <br> 3. _____ <br> 4. _____ <br> 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 66: Test for Citrix ports (Port 1495)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. | | |
| | 2. | | |
| | 3. | | |
| | 4. | | |
| | 5. | | |

**Results Analysis:**

**Test 67: Test for Oracle ports (Port 1521)**

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 68: Test for NFS ports (Port 2049)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| Target System IP Address | Port | State | Service |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____
_____
_____
_____
_____

## Test 69: Test for Compaq, HP Inside Manager ports (Port 2301, 2381)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| Target System IP Address | Port | State | Service |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 70: Test for Remote Desktop ports (Port 3389)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

**Test 71: Test for Sybase ports (Port 5000)**

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| **Tools/Services Used** | 1. | | |
| | 2. | | |
| | 3. | | |
| | 4. | | |
| | 5. | | |

**Results Analysis:**

## Test 72: Test for SIP ports (Port 5060)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 73: Test for VNC ports (Port 5900/5800)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. | | |
| | 2. | | |
| | 3. | | |
| | 4. | | |
| | 5. | | |

**Results Analysis:**

## Test 74: Test for X11 ports (Port 6000)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. <br> 2. <br> 3. <br> 4. <br> 5. | | |

**Results Analysis:**

## Test 75: Test for Jet Direct ports (Port 9100)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. | | |
| | 2. | | |
| | 3. | | |
| | 4. | | |
| | 5. | | |

**Results Analysis:**

### Test 76: Port scan FTP data (Port 20)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. <br> 2. <br> 3. <br> 4. <br> 5. | | |

**Results Analysis:**

**Test 77: Port scan web servers (Port 80)**

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 78: Port scan SSL servers (Port 443)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 79: Port scan Kerberos-Active Directory (Port TCP/UDP 88)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____<br>2. _____<br>3. _____<br>4. _____<br>5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____

## Test 80: Port scan SSH servers (Port 22)

| Target Organization | | | |
|---|---|---|---|
| URL | | | |
| Command Used | | | |
| **Target System IP Address** | **Port** | **State** | **Service** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| Tools/Services Used | 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ | | |

**Results Analysis:**

_____

_____

_____

_____

_____