Penetration Testing Deck

“Organisations should never describe themselves as secure – there are only varying degrees of in-security”

Our Qualifications :

1. **OSCP**
2. **CHFI**
3. **CEH**
4. **NSE 1 | 2**
5. **CNSS**

Services :

Web Application Vulnerability Assessment & Penetration Testing

Types of WebApp Penetration Testing :

1. **Black Box** test is the least time-consuming (and therefore cheapest) option where the tester is given no background information. While Black Box reflects a hacker’s experience, the sanctioned tester is usually under a restricted time frame, while a hacker has unlimited time for trying exploits.

2. **Gray Box** tester receives some background information and is authenticated at a user level.

3. **White Box** test is the most expensive and yields the most accurate and comprehensive results. In addition to receiving extensive background information, the tester has an administrator or root-level access.

No. of unique* Subdomains in scope :

1. Less than or equal to 3
2. Greater than 3 and less than or equal to 7
3. Greater than 7 and less than or equal to 11
4. Greater than 11 and less than or equal to 15
5. Greater than 15

The following sections describe the 10 subcategories of the Web Application Penetration Testing Methodology:

1. **Information Gathering**
    a. Conduct Search Engine Discovery and Reconnaissance for Information Leakage
    b. Fingerprint Web Server
    c. Enumerate Applications on Webserver
    d. Review Webpage Comments and Metadata for Information Leakage
    e. Identify application entry points
    f. Map execution paths through the application

2. **Configuration and Deployment Management Testing**
    a. Test Network/Infrastructure Configuration
    b. Test Application Platform Configuration
    c. Enumerate Infrastructure and Application Admin Interfaces
    d. Test HTTP Methods
    e. Test HTTP Strict Transport Security

3. **Identity Management Testing**
    a. Test User Registration Process
    b. Test Account Provisioning Process
    c. Testing for Account Enumeration and Guessable User Account
    d. Testing for Weak or unenforced username policy

4. **Authentication Testing**
    a. Testing for Credentials Transported over an Encrypted Channel
    b. Testing for default credentials
    c. Testing for Weak lockout mechanism
    d. Testing for bypassing authentication schema
    e. Test remember password functionality
    f. Testing for Browser cache weakness
    g. Testing for Weak password policy
    h. Testing for Weak security question/answer
    i. Testing for weak password change or reset functionalities

5. **Authorization Testing**
    a. Testing Directory traversal/file include
    b. Testing for bypassing authorization
    c. Testing for Privilege Escalation
    d. Testing for Insecure Direct Object References

6. **Session Management Testing**
    a. Testing for Bypassing Session Management Schema
    b. Testing for Cookies attributes
    c. Testing for Cross-Site Request Forgery (CSRF)
    d. Testing for logout functionality
    e. Test Session Timeout

7. **Input Validation Testing**
    a. Testing for Reflected Cross-Site Scripting
    b. Testing for Stored Cross-Site Scripting
    c. Testing for HTTP Parameter pollution
    d. SQL Injection
    e. XML Injection
    f. LDAP Injection
    g. OS Command Injection

8. **Error Handling and Disclosure**

9. **Business Logic Testing**
    a. Test Upload of Malicious Files
    b. Test Upload of Unexpected File Types
    c. Test Defenses Against Application Mis-use
    d. Test Number of Times a Function Can be Used Limits
    e. Test Ability to forge requests

10. **Client-Side Testing**
    a. Testing for DOM-based Cross-Site Scripting
    b. Testing for JavaScript Execution
    c. Testing for HTML Injection
    d. Testing for Client-Side URL Redirect
    e. Testing for CSS Injection
    f. Test Cross-Origin Resource Sharing
    g. Test Web Messaging (SPF & DMARC)

Technical Assistance :

1. Determine business requirements for a penetration test
2. Agree to the testing scope
3. If the system goes down
4. The account gets locked out or expires
5. Answer technical questions
6. Embedded device fails
7. Turn off WAF(web application firewall) incase of internal pentesting

Risk Analysis :

1. Impact of a successful attack

    • How much damage can it cause
    • Taking a business into context

2. Likelihood of a successful attack

    • Vulnerability discovery
    • Payload creation difficulty
    • Any mitigating controls in place

Reporting :

1. Security issue description
2. Evidence/PoC
3. Impact of an attack
4. Severity
5. Recommendations
6. Mitigation

Pricing : As per requirements.