CYBERFORTIFY

CyberFortify

Penetration Testing Readiness and Scoping Checklist

2025

www.cyberfortify.co
usamagul@cyberfortify.co

1. INITIAL PLANNING AND OBJECTIVE SETTING

Before choosing your penetration testing vendor, it's vital to define your needs and prepare your environment.

□ Determine the Need for a Pen Test

- □ Fulfill Compliance Requirements:
  - □ Confirm if the test is required for:
    - □ PCI
    - □ HIPAA
    - □ HITRUST
    - □ Other government regulations
- □ Assess Security Improvement Goals:
  - □ Get a penetration test to proactively improve your company's overall security posture.
- □ Verify Breach Fixes:
  - □ Order a penetration test to simulate an attack and double-check that previous security fixes hold up against real-world attempts.
- □ Investigate Root Cause of a Compromise:
  - □ Use a penetration test to gain insight into a system compromise and help determine what may have been exploited.

□ Define the Scope and Objectives

- □ Establish a Clear Objective:
  - □ Articulate your cybersecurity concerns or what compliance standard is driving the test, like:
    - □ Achieve domain admin access
    - □ Secure all services that handle cardholder data
    - □ Ensure remote attackers can't get on the internal network
- □ Define the Starting Place for your Pen Test (Your Scope):
  - □ Have a list of specific targets ready:
    - □ External/Internal Network:
      - □ Specific IP addresses
      - □ IP ranges
      - □ Network services

- □ Web Application:
  - □ The URL
  - □ Domain name
- □ Mobile Application:
  - □ Application code/information

Prepare Your Environment

- □ Run Automated Vulnerability Scans Beforehand:
  - □ Run your own automated vulnerability scans to identify and fix low-hanging issues.
- □ Gather Necessary Access/Credentials (If Applicable):
  - □ Prepare any credentials or access methods required for an authenticated test (especially for web apps, mobile apps, or internal tests).

2. TYPES OF PENETRATION TESTS AND THEIR FOCUS

Select the right test type based on the data you're protecting and the environment you want to assess

External Penetration Testing

- **Target:** Services and systems exposed to the public Internet.
- **Attacker Simulation:** An unauthorized, unauthenticated person on the internet.
- **Objective Focus:** Identify and exploit vulnerabilities that allow an attacker to gain access to the internal environment.

Web Application Penetration Testing

- **Target:** Custom web applications built by your organization
- **Attacker Simulation:** Unauthenticated remote attacker or an authenticated user (with credentials).
- **Objective Focus:** The objective of an application penetration test is to identify security issues resulting from insecure development practices in the design, coding, and deployment of the software

Internal Penetration Testing

- **Target:** Internal network services and systems not exposed to the internet
- **Attacker Simulation:** A threat actor who has already gained a foothold (e.g., a compromised employee account or an external attacker who pivoted in).
- **Objective Focus:** identify security issues with the design, implementation, and maintenance of servers, workstations, and network services

Web Application Penetration Testing

- **Target:** Custom web applications built by your organization
- **Attacker Simulation:** Unauthenticated remote attacker or an authenticated user (with credentials).
- **Objective Focus:** The objective of an application penetration test is to identify security issues resulting from insecure development practices in the design, coding, and deployment of the software

3. PENETRATION TESTING ENGAGEMENT PROCESS

These steps outline the typical process of working with a penetration testing vendor like Cyberfortify.

Scoping and Contract Phase

- □ Request a quote:
  - □ Contact the sales agent to get a personalized price based on the complexity and scope of your environment.
- □ Choose a penetration tester by verifying that:
  - □ They follow industry best practice standards
  - □ They communicate their testing methodologies
- □ Complete the scoping call:
  - □ Have a call with a sales representative and a penetration test team representative to define the scope and objectives.
- □ Sign the contract:
  - □ Formalize the engagement.

Information Gathering and Scheduling

- □ Complete the questionnaire:
  - □ Respond to the project manager’s questionnaire to provide all necessary specifics:
    - □ URLs
    - □ IP addresses
    - □ Application details
    - □ Code
    - □ Other required information
- □ Determine your penetration test date by answering these questions:
  - □ Is the penetration test starting early enough to leave time for remediation later?
  - □ Is this during a busy time of the year?
  - □ Will office operations be interrupted?
  - □ How much notice should we give everyone?
- □ Schedule your penetration test:
  - □ The kickoff call is typically scheduled 7-10 days after contract signing.
  - □ The actual test is usually performed 5 to 8 weeks out to allow for preparation time.

- □ Coordinate internally:
  - □ Inform and coordinate with relevant internal teams:
    - □ Product Owners/Developers:
      - □ For web or mobile application tests.
- □ SOC/NOC Teams:
  - □ To ensure that they are aware of the testing efforts, are not “red team” focused, and can react appropriately to alerts.
- □ End Users:
  - □ If an internal application is being tested, inform users that unusual activities may appear.

Execution and Post-Test

- □ Maintain responsiveness:
  - □ Ensure internal contacts are responsive to questions from the penetration testing team during the actual testing phase.
- □ Expect manual testing:
  - □ Define the test, including outlining an initial automated scan followed by a manual penetration testing to exploit vulnerabilities.
- □ Be aware of test impact:
  - □ Be prepared for potential, though unlikely, service degradation; the tester will try to act safely and avoid exploiting denial-of-service conditions.
- □ Report delivery:
  - □ Receive the final report, which should include:
    - □ An executive summary of the penetration test story
    - □ Evidence (including screenshots) of identified and exploited vulnerabilities
    - □ High-level steps to reproduce the findings
    - □ High-level steps to remediate the issues

4.POST-TEST REMEDIATION

Use the report to fix issues and enhance your overall security.

Report Review and Action

- □ Review findings:
  - □ Closely examine the report, paying attention to the executive summary, findings, and remediation steps.

- □ Prioritize remediation:
  - □ Focus on critical findings first, especially those that were successfully exploited to show high impact.
- □ Fix issues:
  - □ Use the provided steps and evidence to recreate and patch the vulnerabilities in your environment.
- □ Utilize retesting:
  - □ Schedule retests within the 90-day window to confirm exploited vulnerabilities are fully mitigated.

5.ONGOING IMPROVEMENT

Now that remediation and retesting is over, you should make process and policy changes to avoid future vulnerabilities.

- □ Develop an improvement plan:
  - □ Create your plan by answering these questions:
    - □ How can we make our environment a little more secure every time?
    - □ Do we need additional training for our developers and network engineers?
    - □ Do we have the resources we need to be successful?
- □ Assess your experience:
  - □ Did you have enough time to get everything done?
  - □ Re-evaluate your timeline
- □ Plan a date for next year’s penetration test:
  - □ Determine your date by answering these questions:
    - □ Did we have enough time to get everything done?
    - □ Do we need to adjust anything based on office operations?
- □ Ensure continued maintenance:
  - □ Regular updates
  - □ Port scans
  - □ App scans
  - □ Incorporate new security practices

Need a Pentest?

Request Qoute

CREST
PATHWAY

ABOUT CYBERFORTIFY

Your proactive cybersecurity partner, enabling businesses with defense against constant digital threats.

CyberFortify is a top-rated cybersecurity service company that delivers industry-leading security testing services and compliance consulting services. We offer innovative and in-depth expertise to assist organizations in protecting data, applications, and networks while gaining regulatory compliance with certainty.

CYBERFORTIFY JOINS THE CREST ACCREDITATION PATHWAY

The CREST community is made up of a diverse spectrum of organizations, each operating across different geographical areas and at various stages of maturity and scale. This includes cyber service providers that offer established services, as well as those that are newer to both the field and the accreditation process.

The Accreditation Pathway is a supportive process that takes an eligible organization through its natural growth stages from early stage (Pathway) through to Accreditation, recognizing their ability to meet predefined standards of quality and maturity using varying types of checks and assurance. It also provides an opportunity for organizations to progress on to CREST Membership.

2025

www.cyberfortify.co
usamagul@cyberfortify.co