JEFFCOMPUTERS
OVERSEEING CYBERSECURITY

Before You Sign

The Essential **Checklist** for Hiring Your Next **Penetration Testing** Service

*** Updated with 2025 proposed requirements. Enforcement expected in early 2026.*

Jeff Computers (941) 759-1120 businessbooster@jeffcomputers.com

Introduction to **Penetration Testing** Standards

Congratulations on prioritizing your cybersecurity!

Hiring a **Penetration Testing (Pentesting) Service** is the most proactive decision you can make to protect your assets. However, poor planning can lead to unexpected costs, delays, or, worse, incomplete results.

This guide focuses on three key areas (Scope, Logistics, and Expertise) that you must define and confirm before starting the hiring process.

Using this **checklist** ensures you get maximum value from your investment and that your security assessment is smooth and successful.

Section 1:

DEFINING THE SCOPE:

What and How is **Tested?**

Defining the scope of the test is the most crucial step. Be as specific as possible about the assets that will be targeted.

Aspect to Confirm	Key Details	Status
1. Test Assets	Which public IPs, subnets, domains, firewalls, or web applications will be included? ***(List all addresses precisely).***	
2. Test Type	Do you need an **External** test (simulating an attack from the internet) or an **Internal** test (simulating an attacker with access to the local network)?	
3. Access Depth	Will it be a **Black Box** test (no prior information), **Gray Box** (with limited user credentials), or **White Box** (with full access to architecture and code)?	
4. Specific Objectives	Is the primary goal compliance with regulations **(HIPAA, PCI, SOC 2)**, or is it discovering "zero-day" vulnerabilities?	
5. Exclusions & Restrictions	Which **systems** or assets are strictly **forbidden** from being touched? (E.g., critical production servers, medical equipment, etc.)	

Section 2

LOGISTICS & INTERNAL PREPARATION

Ensure your IT team is ready for the test's commencement and that legal procedures are established.

Aspect to Confirm	Key Details	Status
1. Rules of Engagement (RoE)	The vendor must provide a **Rules of Engagement (RoE)** document or a Statement of Work (SOW) detailing exactly what they will do and when. **Never start without this.**	
2. Emergency Contact	Designate a 24/7 technical contact from your team to reach the vendor if the test accidentally causes a service disruption.	
3. IT Team Notification	Will your IT team (including SOC or Help Desk) be aware of the test? This is key to distinguish the pentest from a real attack (for Gray/White Box tests) or to assess your detection capability (for Red Team tests).	
4. Testing Window	Define the exact start and end time of the pentest and whether it will occur outside business hours to minimize risk.	

Section 3

VENDOR REQUIREMENTS & REPORTING

Service quality relies on the tester's experience and the clarity of the report.

Aspect to Confirm	Key Details	Status
1. Credentials and Certifications	Ask your vendor to show the credentials of the analysts performing the test (e.g., **OSCP, CEH, CISSP**). Automated tools are not enough.	
2. Insurance Coverage	Confirm that the vendor carries **Liability Insurance** to protect you in case of unintended damage or disruption.	
3. Report Format	The final report must be actionable. It should include: **A)** Executive Summary for Management. **B)** Detailed list of vulnerabilities by risk (Critical, High, Medium). **C)** Clear, technical **Remediation** steps for your IT team.	
4. Testing Methodology	Define the exact start and end time of the pentest and whether it will occur outside business hours to minimize risk.	

NEXT STEP: EXECUTION!

By completing this checklist, you are 100% prepared to begin the assessment.
At Jeff Computers, our goal is to simplify the process and deliver fast, actionable results. If you have any questions about any of these points, we are ready to assist you.

Ready to **secure** your **assets** and meet your compliance **requirements**?

Speak with our certified experts today to get a quote and plan your **Pentesting**.

Contact Us:

JEFFCOMPUTERS
OVERSEEING CYBERSECURITY

510 Old Venice Rd, Osprey, FL 34229
(941) 759-1120
sales@jeffcomputers.com