Penetration Test Agreement

Test Conductor: Prob3 Inc.

Client: Art's Tailor Shop

September 2022

Prob3 Penetration Testing Company
Pr0b3 Blvd., Hanksville, FL 33999.

This document serves as a contract between *Prob3*, the penetration testing company (*vendor*), and *Art's Tailor Shoppe*, the client for whom the penetration test will be performed (*client*).

What follows are both the Scope of Work, as well as the Rules of Engagement that will be employed throughout the test.

Scope of Work

Purpose

By way of conducting a penetration test, the vendor seeks to assess and remediate the client's cyber-security posture accordingly to prepare for an expansion of their web presence, especially as it relates to e-commerce.

By identifying and proposing solutions for current weaknesses in security posture, the confidentiality, integrity, and availability of the client's work operations is better ensured, and the sensitive information of customers whom they do online business with in the future is thus protected.

Network Scope

The list of IP addresses of hosts (devices) on the network is as follows:

- 217.70.184.38
  - This is a web Server with domain `www.artstailor.com`
- 217.70.184.3
  - This is an inner-network router with domain `innerrouter.artstailor.com`
- Any IPs that are reachable from 217.70.184.3 are in scope

Separating the network from the incoming connections outside of the network is the outer-network router, with IP 217.70.184.1, which is **not** in scope.

Intrusion Detection/Prevention

Between the outer router and the inner router (see above), there is a *firewall* in place within a *DMZ (demilitarized zone)*. It should be noted that firewall notifications/alerts may be triggered as a result of the pentration test.

System Penetration

Upon penetration of a host on the target network, this penetration test will involve attempts at privilege escalation, which may be done through methods such as local vulnerability assessments or password cracking. Highest privilege (root/Administrator) will be sought out whenver possible.

Type of Test

This penetration test is an **opaque-box** test. That is to say, although testers will have access to the internal network of the company, they will not be provided credentials or special authorization to navigate it.

Login Systems

On the hosts that have Windows as their operating system, Microsoft Active Directory (AD) is used as the cross-network authentication protocol, which forms part of the testing scope.

Linux machines on the network, however, are not integrated into the AD environment yet. As a result, their login systems will be tested only at an individual-machine basis.

Web Systems

Although there will be one in the future, there is not currently a dynamic web application being served on the network – simply a static webpage. As a result, this penetration test will not involve any fuzzing/static/dynamic analysis of code as it relates to its web component.

Wirless Network Testing

A wireless network is present, which uses WPA2-PEAP as its security protocol and covers all the square footage needed within Art's Tailor Shoppe. A RADIUS server is employed to allow users to authenticate using their AD credentials, meaning that authentication with a singular passphrase is not possible. This wireless network, which forms part of the scope, is accessible from the NDG connection in which the test will be conducted.

There are around eight people using the network at once, and they should be notified of potential slowdowns if they make use of the wireless network. However, direct attacks against wireless network users will not be performed.

Social Engineering

Social engineering does not form part of this penetration test.

Rules of Engagement

Timeframe

The timeframe of the penetration test is from September 2022 up to December 7th, 2022. The precise start date is contingent on the date in which the agreement is signed by the client.

Location of Testing

Testing of the network will be done off-site through NDG an connection.

Methods of Disclosure

If upon testing, sensitive information such as account credentials or personally identifiable information are found, it is to remain strictly within the confine of the test, and not to revealed or communicated across the internet. Between the client and the tester, if communication is to happen digitally for the purposes of evidence handling, then encryption will be strictly enforced.

Status meetings

The team will not be requesting status meetings from the client aside from possibly the system administrator, Otto Oppenheimer, during scheduled *Office Hours*.

Contact information

Should communication need to be established for emergencies or otherwise, the following are the points of contact:

- Shop Owner: Art Rosenbaum
  - Phone: 555-555-1414
- Shop System Administrator: Otto Oppenheimer
  - Phone: 555-555-1313
- Lead Penetration Tester: Hank Hacker
  - Phone: 555-555-1212

Time of Day for Testing

Testing can be done at any time throughout the day, aside from times in which *UFSIT* meetings are in session (Thursdays 6:00pm-7:00pm).

Shunning

Shunning should not be an issue within the penetration test, as no intrusion prevention systems are currently set up to do so.

Incident Response Analysis

Throughout the test, the team may assess responses to info-gathering, footprinting, scanning and vulnerability analysis, data aggregation, and data exfiltration not including shunning.

Permission to Test

Permission to test involves the acknowledgement of potential instability and/or temporary downtime of the client's network or certain hosts on their network. This will have no effect on the client's customers, however, as no customer-directed services are currently live on the network.

Legal Considerations

Under Florida Statute 815.06, willfull, knowing, unauthorized access to computer systems is illegal.

By signing this contract, the client hereby grants authorized access to their computer systems in the manner and scope described above:

Client Signature: _____

System Administrator Signature: _____

Vendor Owner Signature: _____

Big Boss
Owner, Prob3 Inc.

Lead Penetration Tester Signature: _____

Hank Hacker
Lead Tester, Prob3 Inc.

Date: _____