9

Passpoint security

Penetration Testing as a Service (PTaaS)

FOR

Navarro County- Texoma HIDTA

Project Description

Penetration Testing as a Service ("PTaaS") will help minimize your security risks while meeting compliance guidance, if necessary, by governing bodies. Passpoint Security, LLC. (Company) will conduct an objective review of the technical and operational security weaknesses and vulnerabilities present within external and internal computer systems as well as gaps related to the requirements for Navarro County- Texoma HIDTA. ("Client").

Services Description

PTaaS is performed remotely, unless it is agreed that an onsite visit is required. Company will:

- Perform vulnerability scanning and technical vulnerability testing of your external-facing systems to look for critical security flaws that need immediate attention. As part of this testing, Company will demonstrate how these flaws can impact your firm.
- Perform vulnerability scanning and technical vulnerability testing of your internal network to look for critical security flaws that need immediate attention. As part of this testing, Company will demonstrate how these flaws can impact your firm.
- Company to conduct an o365 Configuration Assessment
- Client will have unlimited access to Passpoint's Remediation Portal
- Company will monitor the Dark Web for threat intelligence about stolen user data associated with Client's domains, Client will be alerted when a compromise is detected, so that you can respond to stop a potential costly and widespread data breach

Penetration Testing/Vulnerability Scans

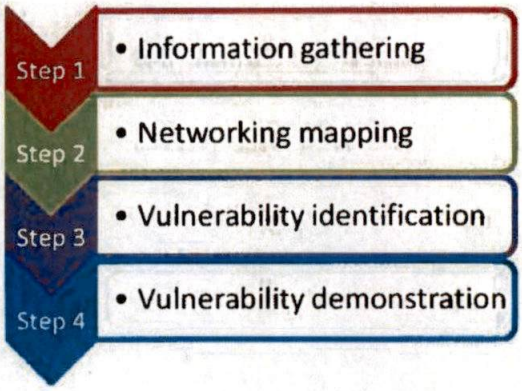
Company will perform technical vulnerability and/or penetration tests on the following:

- Up to **5** Internet-accessible hosts (i.e., routers, firewalls, and servers)
- Up to **300** Internal LAN hosts

Specific technical security checks may include:

- Open Ports
- OS Misconfigurations
- Missing Patches
- Weak Passwords
- Weak Encryption
- Buffer Overflow Weaknesses
- Cross-Site Scripting
- SQL Injection
- Susceptibility to Denial-of-Service Attacks

The following is a graphical representation of the widely accepted ethical hacking methodology we will use when performing our technical testing:



Deliverables

The following will be delivered electronically and discussed in a follow-up phone conversation upon completion:

- A report that includes prioritized findings and recommendations for remediation as follows:
  - Introduction
  - Executive Summary
  - Notes
  - Summary Findings and Recommendations – including any details on how technical vulnerabilities can be exploited
- Security tool test results and/or reports in native tool format (typically in HTML or PDF format)
- Costs required to remediate Client's environment to specified criteria are not included in this Agreement.

Suitability of Existing Environment

- All Servers with Microsoft Windows Operating Systems must be running Windows 2008 Server or later and have all the latest Microsoft Service Packs and Critical Updates installed.
- All Desktop PC's and Notebooks/Laptops with Microsoft Windows Operating Systems must be running Windows 7 Pro or later and have all the latest Microsoft Service Packs and Critical Updates installed.
- All Server and Desktop Software must be Genuine, Licensed and Vendor-Supported.
- The environment must have a currently licensed, up-to-date and Vendor-Supported Server-based Antivirus Solution protecting all Servers, Desktops, Notebooks/Laptops, and Email.
- The environment must have a currently licensed, Vendor-Supported Server-based Backup Solution that can be monitored and send notifications on job failures and successes.
- The environment must have a currently licensed, Vendor-Supported Hardware Firewall between the Internal Network and the Internet.
- All Wireless data traffic in the environment must be securely encrypted.
- There must be an outside static IP address assigned to a network device, allowing RDP or VPN access.
- Any device, system or service that does not present the qualifications as specified in the security and/or compliance standard will be identified as non-compliant until such time that appropriate remedial activities and/or compensating controls may be imposed to ensure environment integrity.

Excluded Services

Service rendered under this Agreement does not include:

- Parts, equipment or software not covered by vendor/manufacturer warranty or support.
- The cost of any parts or equipment. Shipping equipment for testing will be charged to the client at cost, as an additional line-item expense
- The cost of any Software, Licensing, or Software Renewal or Upgrade Fees of any kind.
- The cost of any 3rd Party Vendor or Manufacturer Support or Incident Fees of any kind.
- The cost to bring Client's environment up to minimum standards required for Services.
- Failure due to force majeure, building modifications, power failures or other adverse environmental conditions or factors.
- Service and repair made necessary by the alteration or modification of equipment other than that authorized by Company, including alterations, software installations or modifications of equipment made by Client's employees or anyone other than Company.

O365 Configuration Assessment

An O365 Assessment will facilitate visibility where logical or technical controls might be vulnerable to the latest Internet based threats. The overall purpose of this project is to provide recommendations for a secure baseline which may reduce the impact of these risks.

Security checks to show areas where the application is at risk may include the following:

- Account Breach – an attacker breaches an account in the application such that it can be used to interact with either resources in Microsoft 365 or with on premise infrastructure

- Elevation of Privilege - an attacker has managed to compromise one or more accounts in the application and is now working to increase their power

- Data Exfiltration - an attacker has found a way to move data out of the application

Deliverables

A report will be delivered electronically and discussed in a follow-up phone conversation upon completion. The report will include prioritized findings and recommendations for remediation. Report sections are indicated as follows:

- Overview
- Methodology
- Key Observations
- Findings and Recommendations*
- Table of Figures

Security tool test results and/or reports in native tool format (typically HTML or PDF)

Remediation efforts based on findings and recommendations are not included in this Agreement.

Assumptions

The following assumptions accompany this proposal and should be considered to construct the bounds of an operating agreement going forward:

- Full access to all resources, servers, devices, data centers will be provided to Company without reservation or delay.

- User accounts with the necessary administrative level of authority will be granted as required.
- A full and open disclosure of all devices, methods, procedures in support of the activities detailed in this proposal will be provided.
- Access to current planning documentation, any applications necessary to manage the project, report and communicate inside and outside Client will be made available.
- Access to key client personnel for interviews, validation, approvals, etc.
- Appropriate security access (parking, building, internet, etc.)
- No changes to the enterprise environment will be made without common communication between the Client IT organization and Company
- Manufacturer support is available for all devices, software and components and will be maintained by Client during the extent of an operating agreement with Company.
- All hardware, software, tools, assets and any other capital items that are held by Client will be provided and funded by Client.
- Access to any other information that effects these efforts
- Company will perform a security and/or compliance assessment on the basis specified in this SOW.
- Compliance assessments are performed in alignment with industry best practices.
- This assessment does not provide PCI assurance attestation.
- All connectivity to Customer computing systems and all attempts at same will be only through Customer's security gateways/firewalls and only through Customer-approved security procedures.
- Company will not access and will not permit unauthorized persons or entities to access, Customer computing systems and/or networks without Customer's express written authorization, and any such actual or attempted access will be consistent with any such authorization.
- Company will take appropriate measures to ensure that Company's systems connecting to Client's systems, and anything provided to Customer through such systems do not contain any Disabling Device. For purposes of this Agreement, "Disabling Device" means any programs, mechanisms, programming devices, malware or other computer code (i) designed to disrupt, disable, harm, or otherwise impede in any manner the operation of any software program or code, or any computer system or network (commonly referred to as "malware", "spyware", "viruses" or "worms"); (ii) that would disable or impair the operation thereof or of any software,computer system or network in any way based on the elapsing of a period of time or the advancement to a particular date or other numeral (referred to as "time bombs", "time locks", or "drop dead" devices); (iii) is designed to or could reasonably be used to permit a party or any third party to access any computer system or network (referred to as "trojans", "traps", "access codes" or "trap door" devices); or (iv) is designed to or could reasonably be used to permit a party or any third party to track, monitor or otherwise report the operation and use of any software program or any computer system or network by the other party or any of its customers.

Equipment Return

Upon completion by Company of Summary Findings and Recommendations, Client will promptly return laptop to Company utilizing the provided shipping label. Company will invoice Client $500 if laptop is not received within fifteen (15) days of the Summary Findings and Recommendation meeting.

FEES

The fixed price fee for the proposed package is stated in the following table. This contract is a 36-month agreement. Client has the option of canceling the contract at the 36-month renewal date with 30 days written notice to Company. If not canceled, contract will renew for the original term limit.

Program Fees

Cybersecurity Program Support:	List Pricing:
1. Penetration Tests (1 Test)	Included
2. Vulnerability Scans (1 Scan)	Included
3. Project Management	Included
Total Annual Cost	$14,375
Total Bundled Discount (20%)	($2,875)
Total Annual Cost	$11,500

Client has the option to cancel after the initial Penetration Test and Vulnerability Scan at a cost of $11,500. Should Client decide to continue services, Company will invoice the remaining balance of $4,500 for year 1 and $16,000 for years 2 & 3.

Cybersecurity Program Support:	List Pricing:
1. Penetration Tests (1 Test)	Included
2. Vulnerability Scans (4 Scans)	Included
3. O365 Configuration Assessment (one time)	Included
4. Access to Passpoint's Remediation Portal	Included
5. Project Management	Included
Total Annual Cost	$20,000
Total Bundled Discount (20%)	($4,000)
Total Annual Cost	$16,000
Year 1 Remaining Balance	**$4,500**
Year 2&3 Cost	**$16,000**

Example Testing Schedule

Year 1

Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
PT		-	VS	O365	-	VS	-	-	VS	-	-

Year 2

Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
PT	-	-	VS	-	-	VS	-	-	VS	-	-

Year 3

Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
PT	-	-	VS	-	-	VS	-	-	VS	-	-

Travel and Expenses

There is no foreseen travel required for this engagement, but if travel is requested, travel expenses will be invoiced at actual costs as they are not included in the pricing.

APPROVALS

Both parties warrant and represent that they have authority to execute this Statement of Work on behalf of their company and bind them to the obligations.

Navarro County- Texoma HIDTA	Passpoint Security, LLC
By:	**By:** Wade Tucker
Name: H. M. Davenport, Jr.	**Name: Wade Tucker**
Title: Navarro County Judge	**Title: Sales**