Statement of Work
Penetration Testing Agreement

Purpose of the Assessment

TechWatch Consulting Services will provide a limited ("white box") penetration test service to Fairfax Food Supply (FFS) at the request of Target Corporation, a purchaser of FFS products, due to concerns that FFS's network is vulnerable to basic exploit attempts. This service is an evaluation of the network security from a "hacker's" perspective but will operate within a narrow scope of effort. As part of the penetration testing service, TechWatch will use the Metasploit penetration testing framework to target Windows XP machines and Server 2003 machines on FFS's network in order to open a remote command shell, in an attempt to gain elevated privileges. TechWatch will exploit the MS08-67 vulnerability during this exercise, a flaw in the Windows Server Service that can allow unauthorized remote code executions. This particular vulnerability is especially dangerous because it does not require an attacker to authenticate to the target machine before running an attack. Additionally, exploitation of selected vulnerability is effective in helping technical security professionals obtain a baseline understanding of an organization's network security framework.

Objective

The objective of the assessment is to identify and report on security vulnerabilities to allow the client to address the issues following closure of testing. The test will also provide constructive feedback to Fairfax Food Supply and Target Corporation regarding the vulnerability

of FFS's network to external hacking attempts. Fairfax Food Supply can use the results of this testing to better evaluate the state of their network security framework. If deemed necessary, the results will also aid FFS in taking appropriate measures to bolster network security. Although this is a white box testing scenario, and TechWatch will have knowledge of necessary information regarding target systems. Following the exercise TechWatch will provide a thorough explanation of how attackers can use reconnaissance methods to obtain the information already provided to TechWatch consultant.

It is important to note that this penetration test is simply one method that can be used to evaluate an organization's security, and is by no means a comprehensive assessment. Successful security breaches can also arise from employees or other individuals associated with an organization, and not exclusively from "outsiders" and may not be a function of external access issues.

Scope of Effort

This project will include one TechWatch consultant for a time period of eight hours, at a TechWatch office location, during the week of May 1, to provide external penetration testing services. The time of the testing will remain at the discretion of TechWatch and will not be disclosed to Fairfax Food Supply according to previously negotiated terms. TechWatch will also be responsible for providing the necessary resources including tools, knowledge and expertise to execute the external penetration test on the customer-owned Windows XP machines and Server 2003 machines. A list of TechWatch-provided resources is as follows:

- One TechWatch consultant (CEH, Network +) with three years of pen testing experience
- One TechWatch-owned computer hosting virtual machine software (VMWare)
- Kali Linux operating system within VMWare environment
- Metasploit penetration testing tool

The TechWatch consultant will operate with the knowledge that FFS owns Windows XP machines and Server 2003 machines and will also have knowledge of the IP addresses and server message block (SMB) ports of those machines. The consultant will not be aware of the state of the machines, including any security features on the host machines or on Fairfax Food Supply's network.

TechWatch will attempt to gain remote access to FFS's Windows XP and Server 2003 machines through the implementation of a three-phase process, as is outlined below:

Phase 1 (Set Up): The TechWatch consultant will utilize a specially-designated computer within TechWatch offices to run the Metasploit program from a Kali Linux virtual machine hosted on VMWare. The consultant will have targeted associated IP addresses and SMB ports available for reference)

Phase 2 (Exploit): All Windows XP and Server 2003 machines will be tested for exploitation by utilizing the MS08-067 vulnerability and corresponding payloads found within the Metasploit console. Once the exploit is set up, the TechWatch consultant will attempt to connect to ports hosting the server message block (SMB) throughout the attempt, and will utilize a variety of payloads that open Windows command shells during the exploit. (Steps involved in the exploit process: finding module, setting module options, exploit target, find compatible payloads, test exploit).

Example of phase two detailed action steps to be taken by the TechWatch consultant:

1. Open Metasploit in Kali Linux
2. Find the exploit module (ms08_067_netapi)
3. Enter target address (FFS Windows 2003 servers and XP machines), SMB port used to connect.
4. Select from a variety of compatible payloads that open a command shell to listen in on designated port.
5. If successful, the payloads used will open up listener TCP ports and may even open sessions that report back to the tester's workstation.
6. For each successful exploitation attempt, the TechWatch consultant will verify the exploitation with screenshots taken from the session.

Phase 3 (Documentation): Throughout the penetration attempt, TechWatch will document and record each step of the process. Following the exercise, TechWatch will provide a report of the penetration test which will include data obtained from the network, and any information regarding exploitation of vulnerabilities and the attempt to gain access.

Assumptions and Restrictions

Due to the nature of this penetration testing as a white box exercise, TechWatch and Fairfax Food Supply agree that the exercise cannot examine the overall security architecture of FFS systems. The test is designed to target a specific focus area to measure a baseline for FFS network security. Furthermore, the penetration test is unlikely to provide information about new

vulnerabilities, especially those discovered after the test is carried out A list of additional assumptions and restrictions is provided below:

- TechWatch has legal and organizational approval to conduct penetration testing against FFS's network and systems.
- TechWatch assumes that FFS will not disclose the penetration attempt to FFS employees until after testing is complete, in order to facilitate a more effective penetration testing environment.
- Both parties agree that the TechWatch consultant has eight hours to complete the testing. This is considered an ample amount of time for the TechWatch consultant to adequately preform testing, based on past testing performed by our company.
- FFS understands that TechWatch is not testing for all potential vulnerabilities within FFS's network, only the specific MS08-067 vulnerability on FFS's systems that are specified as "at risk" by Target Corporation and FFS.
- The TechWatch consultant is not authorized to use other means to attempt to gain access. Methods that test other vulnerabilities or utilize other exploits are out of the scope of testing according to the terms of this agreement.
- FFS systems that are not Windows XP or Server 2003 are out of scope for testing according to the terms of this agreement. The TechWatch consultant is also not authorized to access any other systems connected to FFS's network.
- TechWatch and FFS understand and agree that the performance of these services, as provided in accordance with this Proposal, may improve your security posture. These Services cannot identify all risks that affect FFS's network.

- If TechWatch successfully accesses FFS systems, both parties agree that TechWatch is not liable for system issues or failures following the exploit and is not responsible for remediation or clean-up measures.
- FFS agrees to forgo awareness of the IP address belonging to the TechWatch computer and the virtual machine used.
- TechWatch will conduct the assessment in our offices. We will bring all required materials and supply all labor required to gather required data to produce the report output. We will require minimal assistance to establish communications on your local network.
- Results of the test will be considered confidential to both parties.
- The time and date that the assessment is conduct is at the discretion of TechWatch and will be carried out within a specific time frame as specified by Fairfax Food Supply.

Preliminary Schedule

The testing process and follow up procedures will take place over a time period of two and a half weeks in April and May, 2015. The external penetration test will take approximately eight hours to complete on one business day during the week of May 1 (May 1-8). A final report will be provided within one week after the work is completed. A kickoff meeting and briefing will take place prior to the testing. Report compilation will take approximately four days to complete, and the subsequent presentation of findings will be held during the week on May 13.

Schedule

April 25	Kickoff meeting and briefing
May 1-8	TechWatch will perform the assessment
May 8-12	Report compilation
May 13	Report delivery and presentation of findings

Pricing

The total cost for one TechWatch consultant to perform penetration testing services for eight hours, in addition to report generation and subsequent presentation of findings is equal to: **$1219.00.** The cost also includes the use of TechWatch tools and resources needed to perform the assessment. Travel to client site is included in the report compilation charge. Please see a breakdown of associated testing costs in the table below.

Hourly rate for one TechWatch consultant (x8 hours)	$100.00 (800.00)
Report compilation & presentation charge:	$200.00
TechWatch provision of tools	$150.00
Sales tax	6%
Total	$1219.00

Communication Strategy

Per the terms of this agreement, the TechWatch point of contact will notify FFS's CTO at the onset of testing via e-mail notification. The TechWatch consultant performing testing will not be in contact with any FFS employee during the time of testing, unless a security incident arises that requires immediate notification. In this instance, the TechWatch consultant will immediately notify an FFS emergency contact. At the end of testing, a TechWatch point of contact will follow up with an end-of-testing notification, again via e-mail to the FFS CTO. No other FFS employees will be contacted or aware of the testing per the terms of this agreement.

Deliverable

Following the completion of testing, the analyst will compile a report that will detail the methods used in the testing, as well as prioritized findings and potential impact on FFS and Target Corporation. The deliverable will also include an Executive Summary that includes high-level operational details such as which components of FFS's network were targeted, which were found to be vulnerable, and which need to be immediately addressed. The technical summary of the report will include more detailed information regarding the attack vector and how the vulnerability can be potentially exploited to further impact FFS's network. This section will explain how the system was accessed (if successful) and will include screenshots to document the targeting and exploitation process. Lastly, during TechWatch's presentation to FFS, our analysts will describe how an attacker can find the information that FFS will provide to TechWatch in order to begin testing through reconnaissance procedures. Additionally, TechWatch representatives will offer some recommendations for improvements and how to

remediate a threat from vector utilized during the testing, as well as the vulnerabilities and past attacks associated with Windows 2003 and XP machines.

Format of the Final Deliverable:

- Vulnerabilities exploited
- Impact (potential impact on FFS's organization)
- Likelihood (Probability that the vulnerability will be exploited)
- Risk Evaluation
- Recommendations

Customer Assistance

In order to optimize the effectiveness of the TechWatch analyst conducting testing, the FFS needs to provide access to systems, services, and employees. To perform the work specified in this statement of work, TechWatch will require the following from the customer:

- Access to relevant personnel
- A point of contact
- A list of IP addresses for the Windows XP and Windows 2003 machines
- A list of SMB ports

Incident Response and Handling Procedures

TechWatch consultants will take reasonable steps to preserve the functional and operational status of systems, but this is not guaranteed. To mitigate liability on behalf of TechWatch, TechWatch requests that FFS executives sign a document agreeing to testing of

their network security and as well as a document waiving the liability of the TechWatch consultant if a system is broken during access.

Additionally, In the event of a security incident that takes place during penetration testing, the TechWatch consultant will notify the FFS Chief Technology Officer (CTO) within fifteen minutes of discovering the incident. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

Penetration Success Criteria

Achievement of anyone of the following scenario would meet the criteria for successful penetration:

- Using the MS08-067 vulnerability with any compatible Windows payload to successfully open a command shell, create an administrator, or start a remote VNC session on the target machine(s).