{CLIENT ORGANIZATION}

Security Assessment Report

DATE

Report Prepared by:

{YOUR NAME}, {YOUR CREDENTIALS}

{YOUR EMAIL ADDRESS}

{YOUR PHONE NUMBER}

{YOUR ORGANIZATION}

{MAILING ADDRESS}

The information contained within this report is considered proprietary and confidential to the {CLIENT ORGANIZATION}. Inappropriate and unauthorized disclosure of this report or portions of it could result in significant damage or loss to the {CLIENT ORGANIZATION}. This report should be distributed to individuals on a Need-to-Know basis only. Paper copies should be locked up when not in use. Electronic copies should be stored offline and protected appropriately.

**Executive Summary 4**

**Top-Five List 4**

1. Troll Defensive Perimeter Easily Breached (EXAMPLE) 4

2. {Security Issue #2} 5

3. {Security Issue #3} 5

4. {Security Issue #4} 5

5. {Security Issue #5} 5

**Introduction 5**

**Scope 5**

Project Scope 5

In Scope 5

Out of Scope 6

**Site Activities Schedule 6**

First Day 6

Second Day 6

Third Day 6

Nth Day 6

**Background Information 6**

**{CLIENT ORGANIZATION} 6**

**DEVICES IN SCOPE 7**

**Network and Wireless Security 7**

**Potential Vulnerabilities 8**

The {CLIENT ORGANIZATION} systems are not protected by network elves 8

There is no wireless authentication in use (EXAMPLE) 8

{State the Vulnerability} 9

{State the Vulnerability} 10

**System (PC/Server/Device) Security 10**

**Vulnerabilities 10**

Users can install doughnuts (EXAMPLE) 10

{State the Vulnerability} 11

**AAA (Authorization/Authentication/Accounting) 11**

**Vulnerabilities 12**

{State the Vulnerability} 12

**Backups/Disaster Recovery 12**

**Vulnerabilities 12**

Key computer systems are not being backed up on a regular basis (EXAMPLE) 12

{State the Vulnerability} 13

**Physical Security 13**

**Vulnerabilities 13**

The Rainbow Bridge to the Magical Treehouse is frequently unguarded (EXAMPLE) 14

The backup copies of magical scrolls are not protected from fire, theft, or damage (EXAMPLE) 14

{State the Vulnerability} 15

{State the Vulnerability} 15

**User Education 16**

**Vulnerabilities 16**

{State the Vulnerability} 16

**Network Scan – Internal 16**

**Port Scan – One Internal Device 17**

**Network and Port Scan – External 17**

**Wireless Site Survey 17**

**Action Plan 18**

# Executive Summary

|  |
| --- |
| **\*\*NOTE\*\* These yellow boxes are information for YOU, the author of the document. They should be deleted before the final draft and submission to the customer.**  Briefly describe the activities of the assessment.  Talk about the importance of information security at the client organization.  What are some key findings from the analysis?  What are some things that the organization is doing well?  What are some high level issues that they need to improve upon? |

EXAMPLE – A security assessment was conducted for the Magical Treehouse Corporation between March 1 and April 15, 2014. Major activities conducted included Troll Defensive Perimeter inspection, interviews with key network elves and an analysis of scroll retention procedures. The primary business of the Magical Treehouse is making delicious treats and snacks for magical and non-magical folk. Consequently, their secret recipes are important to their business success now and into the future. Protecting those secret recipes should be a primary goal of their security.

## Top-Five List

|  |
| --- |
| A top-five list is used to highlight the five most urgent issues discovered during an assessment. Clients unfamiliar with security may be overwhelmed by a long list of problems. Putting the major issues together may allow the client to easily focus efforts on these problems first. These are the issues that if you came back in six months that you would want to see all of them addressed. DO NOT JUST COPY AND PASTE FROM THE MAIN BODY OF THE REPORT! These should be brief versions of the more detailed observations in the main body. |

The list below contains the “top five” findings, weaknesses, or vulnerabilities discovered during the site security assessment. Some of the issues listed here are coalesced from more than one section of the assessment report findings. Additional information about each is provided elsewhere in the report.

It is recommended that these be evaluated and addressed as soon as possible. These should be considered significant and may impact the operations of the {CLIENT ORGANIZATION}.

### 1. Troll Defensive Perimeter Easily Breached (EXAMPLE)

The Magical Treehouse has a Troll Defensive Perimeter (TDP) that surrounds the Magical Treehouse in all directions. However, multiple gaps were found in the TDP which could lead to security breaches and possible theft of Magical Treehouse information.

**Recommendation**: Reinforce Troll defensive measures at the points detailed later in this report. Consider hiring additional elves to patrol the TDP. Consider contracting a TDP expert to make further recommendations.

### 2. {Security Issue #2}

{Brief description of Security Issue #2}

**Recommendation**: {Brief list of recommendations for Security Issue #2}

### 3. {Security Issue #3}

{Brief description of Security Issue #3}

**Recommendation**: {Brief list of recommendations for Security Issue #3}

### 4. {Security Issue #4}

{Brief description of Security Issue #4}

**Recommendation**: {Brief list of recommendations for Security Issue #4}

### 5. {Security Issue #5}

{Brief description of Security Issue #5}

**Recommendation**: {Brief list of recommendations for Security Issue #5}

# Introduction

|  |
| --- |
| Provide an overview of the report. This is not the same as the Executive Summary. This is really just a brief introduction into the analysis. |

## Scope

|  |
| --- |
| The scope is the boundaries of the project. It is used to describe the on-site activities. These are good starting points, but feel free to modify them based on what you agreed to with your customer. |

### Project Scope

### In Scope

The following activities are within the scope of this project:

* Interviews with key elves in charge of policy, administration, day-to-day operations, magic enforcement, network management, and dragon management.
* A Visual Walk Through of the Magical Treehouse facilities, offices and Root sectors with administrative and facilities personnel to assess physical security.
* A series of Magical Scans to discover known and potentially unknown devices on the network. (These Scans will be conducted from within the Magical Treehouse perimeter and from the Dark Forest.)
* A configuration and security assessment of at most five key systems at each center.

### Out of Scope

The following activities are NOT part of this security assessment:

* Penetration Testing of systems, networks, buildings, laboratories or facilities.
* Social Engineering to acquire sensitive information from staff members.
* Testing Disaster Recovery Plans, Business Continuity Plans, or Emergency Response Plans.

## Site Activities Schedule

|  |
| --- |
| List the site activities. This section should be the highlights of what you did at the customer site. How many visits and what was accomplished each time. It does not need to be really detailed. It should be closer to calendar entries or agenda items instead of a diary detailing everything you did. |

### Date – xx/xx/xx

### Date – xx/xx/xx

### Date – xx/xx/xx

### Date – xx/xx/xx

# Background Information

|  |
| --- |
| Use this section to talk about any relevant background information. |

## {CLIENT ORGANIZATION}

|  |
| --- |
| Describe the client organization. Who is your customer? Business or residential? What are their high level requirements? How many users on the network? What is their computer knowledge/background? How do they use the network?  Describe the location and the facility. Suburban, urban, rural or commercial? House, apartment, condo, warehouse, strip mall? What is the size of the building? How many floors? How close are other residences/businesses? |

## DEVICES IN SCOPE

|  |
| --- |
| Describe the devices that are in scope for the analysis. For example: user common name (ex: Basement PC, or Steve's Laptop), type of device (Dell Latitude, iPad), and other relevant information (model number or version of software - if needed).  Minimum of 5 devices are to be analyzed (no printers!):  1 wireless router (required)  Four other devices (examples):  1 PC  1 Laptop  1 smartphone  1 tablet |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Type | Device ID | Operating System | User | Description |
| PC | bloom-pc01 | Windows XP | Bob | Dell Inspiron |
| Laptop | raind-lap01 | Mac OS X | Alice | MacBook Pro |
| Tablet |  |  |  |  |
| Smartphone |  |  |  |  |
| Wireless Router | magic-rtr01 | {Firmware of router} |  | Linksys WRT54G |

# Network and Wireless Security

|  |
| --- |
| Describe the state of network security at the client organization. Include a screen capture or photograph to document any particularly bad problems as evidence.  Not every vulnerability that is reviewed needs to be an *actual* problem. However, each vulnerability should be described. If it IS a problem, then recommended steps to remediate the problem that are appropriate for the customer should be addressed.  There should be a minimum of four vulnerabilities analyzed.  Explanation – What vulnerability are you analyzing? Describe it so the customer understands it. What should they be doing  Risk – Why is this a potential problem?  Examples/Observations – Did you find any examples of this problem? If yes, or no, document WHAT you looked for and HOW you looked for it. Did you inspect a setting? Use a scanning tool?  YOU MUST DOCUMENT EACH OBSERVATION! This can be a photograph or a screenshot or some other evidence that you checked this item out. |

## Potential or Actual Vulnerabilities

Listed below are the ***potential or actual*** network security vulnerabilities reviewed during the assessment.

### The {CLIENT ORGANIZATION} should be protected by network elves

**Explanation**

The purpose of network elves is to protect the network using tiny swords and flying around in a defensive manner. Based on instructions from the Elf Lord, they determine which network traffic to permit or deny.

The {CLIENT ORGANIZATION} network is not protected by a network elf-based firewall.

**Risk**

There are several risks in running network services without network elves.

* Incoming network-based scans and attacks are not easily detected or prevented.
* Attackers target vulnerable network services.
* Attacks are not isolated and damage cannot be contained.
* Network probing for vulnerabilities slows system and network performance.

**Observations/Examples Found**

* Network elves were seen lounging around drinking coffee instead of performing their network filtering and monitoring duties. In particular, network elf Snowbloom was engaging in risky behavior allowing network traffic to pass through freely after giving him a bribe.

**Documentation**

* Document this observation with a screenshot, photo or some other means.

**Recommendations**

* Activate network elves where available.
* Install a hardware-based network elf.
* Give network elves instructions to be very restrictive.

### Wireless authentication should be in use (EXAMPLE)

**Explanation**

Explain the purpose of wireless authentication.

**Risk**

Without a guideline for security practices, those responsible for security may not apply adequate controls consistently throughout the {CLIENT ORGANIZATION}.

**Observations/Examples Found**

{Describe observations related to or examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* Recommendation 1
* Recommendation 2

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe observations related to or examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}.

### 

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe observations related to or examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}.

# System (PC/Server/Device) Security

|  |
| --- |
| Describe the state of system security at the client organization. This includes analyses of PCs, servers, laptops, mobile devices and other end-user devices.  Include a screen capture or photograph to document any particularly bad problems as evidence.  There should be a minimum of four vulnerabilities analyzed. |

## Potential or Actual Vulnerabilities

Listed below are the potential or actual system security vulnerabilities reviewed during the assessment. Significant problems are noted and recommendations to remediate them are described.

### Users can install doughnuts (EXAMPLE)

**Explanation**

Since users have privileged access to their workstations, they are free to install doughnuts with sprinkles that can affect the operations of the computers at the Magical Treehouse. Doughnuts are freely available from the Internet. Doughnuts with sprinkles can impede the productivity of the staff, collect information on the users, the Magical Treehouse Company, the network environment, launch attacks or probe internal systems.

**Risk**

There are several risks in allowing users to install unsafe doughnuts.

* The doughnuts may contain a virus, worm, or some other dangerous electronic threat.
* The doughnuts may be a “Trojan Horse” to fool users.
* The doughnuts may capture, disclose, delete, or modify sensitive data.
* The doughnuts may make the network elves fat and lazy and unable to perform their duties effectively.
* Significant time may be wasted discussing which doughnuts to eat first.

**Observations/Examples Found**

Doughnuts were found in the Snowbloom PC, Oakleaf Workstation and Raindrop Laptop.

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

The operations team should

* Remove doughnut credit cards from the network elves.
* Remove unsafe doughnuts that have already been installed from workstations. Reinstall systems as needed.
* Establish a process for the evaluation and installation of new doughnuts.

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}

# AAA (Authorization/Authentication/Accounting)

|  |
| --- |
| Describe the state of AAA security at the client organization.  Include a screen capture or photograph to document any particularly bad problems as evidence.  There should be a minimum of four vulnerabilities analyzed. |

## Potential or Actual Vulnerabilities

Listed below are the AAA potential or actual vulnerabilities discovered during the assessment. These are considered significant and steps should be taken to address them.

### Principle of Least Privilege should be followed (EXAMPLE)

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}

# Backups/Disaster Recovery

|  |
| --- |
| Describe the state of backups/disaster recovery at the client organization.  Include a screen capture or photograph to document any particularly bad problems as evidence.  There should be a minimum of four vulnerabilities analyzed. |

## Potential or Actual Vulnerabilities

Listed below are the potential or actual vulnerabilities related to backups and disaster recovery discovered during the assessment. These are considered significant and steps should be taken to address them.

### Key computer systems should be backed up regularly (EXAMPLE)

**Explanation**

The purpose of backups is to allow the customer to restore data that has been deleted or corrupted. The primary PC used by the customer is not backed up on a regular basis.

**Risk**

If the hard drive crashes or the computer is destroyed in an accident the information will be lost. If the data is lost the customer could lose valuable customer information or even data required for regulatory or tax reasons.

**Observations/Examples Found**

{Describe examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* Recommendation 1
* Recommendation 2
* Recommendation 3

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}

# Physical Security

|  |
| --- |
| Describe the state of physical security at the client organization.  Specifically, list the building, security perimeter, and server room (if applicable) vulnerabilities.  Include a screen capture or photograph to document any particularly bad problems as evidence.  There should be a minimum of four vulnerabilities analyzed. |

## Potential or Actual Vulnerabilities

Listed below are the physical security vulnerabilities discovered during the assessment. These are considered significant and steps should be taken to address them. The list is divided into a list of vulnerabilities that relate to the building, the security perimeter, and the server rooms. The building group contains vulnerabilities within the {CLIENT ORGANIZATION} office. The security perimeter group includes the exterior office windows, doors, alarm system, and the surrounding area. The server room are specific to rooms containing server equipment.

### The Rainbow Bridge to the Magical Treehouse is frequently unguarded (EXAMPLE)

**Explanation**

There are several important entry points to the Magical Treehouse. The Rainbow Bridge is the primary access to the tree. The Squirrel Defense Force is responsible for guarding the Rainbow Bridge, but they are frequently distracted by acorns and walnuts in the area.

**Risk**

This bridge protects the valuable treasure of the Magical Treehouse. A determined attacker, thief, or disgruntled employee could get across the bridge with minimal effort to steal and/or destroy treasure or magical scrolls.

**Observations/Examples Found**

On the first day of the security analysis, members of the SDF were observed chasing each other and burying acorns instead of guarding the bridge. Analysis of security camera footage shows that this is happens on a regular basis.

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* Replace the rope bridge with a drawbridge.
* Replace the Squirrel Defense Force with a more reliable security team.

### The backup copies of magical scrolls are not protected from fire, theft, or damage (EXAMPLE)

**Explanation**

The backup copies of the magical scrolls are stored in a closet in the roots of the Magical Treehouse. The backup scrolls could be stolen, misplaced, accidentally overwritten, eaten by insects or destroyed in a fire. If a magical spell needed recovery, the scrolls may not be available or functional when needed.

**Risk**

The operation of the Magical Treehouse can be negatively affected if the backup scrolls are not available due to theft, damage, or fire.

**Observations/Examples Found**

Junior Elves were observed playing in the Root sector of the Magical Treehouse near the backup scroll storage area. Some backup scroll copies were not labeled properly and were almost used as scrap paper. The storage area is not secured properly.

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* Store the backup scroll copies in a room protected by a Level 9 defensive perimeter spell
* Periodically validate that the scrolls still work properly.

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe observations related to or examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}.

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

* {Describe observations related to or examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}.

# User Education

|  |
| --- |
| Describe the state of user education in security at the client organization.  There should be a minimum of four issues addressed. |

## Potential or Actual Vulnerabilities

Listed below are some areas where the users should be instructed in the importance of different security issues.

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

{Describe observations related to or examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}.

### {State the Vulnerability}

**Explanation**

{Explain the vulnerability.}

**Risk**

There are several risks in not having {this vulnerability}.

* {Provide a list of risks.}

**Observations/Examples Found**

{Describe observations related to or examples of this vulnerability found at the site}

**Documentation**

Document this observation with a screenshot, photo or some other means.

**Recommendations**

* {Provide a list of recommendations}.

# Network Scan – Internal

|  |
| --- |
| Internal scan - Conduct an IP address scan (like a ping sweep) of the entire internal network using an application like Nmap or Zenmap. Summarize and ANALYZE the results here.  Can you recognize and identify all of the devices? Are there any unknown devices? If so, you should investigate them.  Attach the detailed results of the scans to this document as exhibits. |

EXAMPLE: Performed a scan of the internal network using <state the application here>. The following is a summary and analysis of the key results. The detailed results are attached as Exhibit X.

# Port Scan – One Internal Device

|  |
| --- |
| Port scan – Select ONE internal device (like a PC, laptop, server or wireless router) for more analysis. Perform a PORT SCAN of the device and then summarize and ANALYZE the results here.  What ports are open? Should they be open? Are there any ports that are unusual or unknown to you?  Attach the detailed results of the scans to this document as exhibits. |

EXAMPLE: Conducted a port scan of <DEVICE NAME>scans of the network using <state the application here>. The following analysis describes the results.

# Network and Port Scan – External

|  |
| --- |
| External scan – Conduct an IP address and port scan of the customer network from the internet. Scan their outside IP address and test for vulnerabilities. Look for open ports or other vulnerabilities from the outside. Does the customer have an external facing web server or public FTP server?  Summarize the results in this section. Attach the scan results to this document as an exhibit. |

# Wireless Site Survey

|  |
| --- |
| Wireless leakage scan – Using a laptop or other portable wireless device, conduct a wireless site survey in and around the customer premises. Look for unknown (rogue) wireless devices AND determine the limits of the customer’s wireless network. Provide a map that shows the approximate boundary of the customer’s wireless network.  Summarize the results in this section. Attach the scan results to this document as an exhibit. |

# Action Plan

|  |
| --- |
| Provide an action plan that lists steps to be taken to improve security at the client organization. You have given specific recommendations under each vulnerability, so use this as an opportunity for some high level recommendations covering the analysis. Help the customer prioritize. Which items are cheapest to complete? Which can they do themselves? Which would need a professional? |