



REDSIEGE

Final Report

EXTERNAL NETWORK PENETRATION TEST

NAKATOMI TRADING CORP

JULY 15, 1988

SIMPLE NAVIGATION

We use links in the document so you can quickly navigate through the document and find the information you want

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
FINDINGS SUMMARY	4
FINDINGS CLASSIFICATIONS	5
FINDINGS	6
CRITICAL RISK FINDINGS	6
RS-NTC-001 Lack of Multi-Factor Authentication	6
RS-NTC-002 Password Reuse	7
HIGH RISK FINDINGS	9
RS-NTC-003 Default Credentials	9
MEDIUM RISK FINDINGS	10
RS-NTC-004 Website Missing HSTS Header	10
LOW RISK FINDINGS	11
RS-NTC-005 Web Server Content-Security-Policy Header Not Present	11
METHODOLOGY	13
APPENDIX	14
FINDING CATEGORIES	14
TABLE OF FIGURES	15

THE SUMMARY FOR THE BUSY EXECUTIVE

Red Siege focuses recommendations to highlight the strategic actions that should be taken by management to have the greatest impact on security.

We also provide a high-level overview of the issues to quickly give the leadership the information they need.

EXECUTIVE SUMMARY

SYNOPSIS

Red Siege experts evaluated the security of Nakatomi Trading Corp's (NTC) perimeter network during the course of a three-week period in July 1988. The goal of the assessment was to identify security vulnerabilities in NTC's internet facing systems and services. All issues identified by Red Siege have been manually verified and exploited (where applicable) to demonstrate the underlying risk to NTC, its employees and clients.

FINDINGS OVERVIEW

Findings grouped by risk severity:

❗ Critical Risk issues	2
🔴 High Risk issues	4
🟡 Medium Risk issues	6
🟢 Low Risk issues	8
ℹ Informational issues	2



KEY FINDINGS

Red Siege found one critical vulnerability related to the authentication to NTC's VPN which allows an attacker to access internal systems. Additionally, Red Siege found two high severity vulnerabilities that have the potential to impact visitors to NTC's website which could impact Nakatomi's brand and reputation.

- NTC's VPN does not use two-factor authentication and multiple users were found using weak passwords. An attacker could easily guess these passwords and access the internal network, compromising the confidentiality of NTC's data and possibly leading to data loss.
- Red Siege found significant shortcomings in defenses and secure coding related to a common web related attack

known as cross-site scripting (XSS). This type of attack allows a malicious actor to use the website to attack visitors, which could expose personally identifying information, authentication credentials, or even compromise the victim's computer.

STRATEGIC RECOMMENDATIONS

To increase the security posture of NTC, Red Siege recommends the follow strategic actions be taken:

- **IMPLEMENT TWO-FACTOR AUTHENTICATION ON PUBLIC FACING SYSTEMS.** Internet facing systems are regularly being probed and attacked. Extra care needs to be taken on these systems to prevent unauthorized access.
- **STRENGTHEN PASSWORD REQUIREMENTS.** NTC should use technical means to ban known bad/weak passwords and train users on safe password practices.
- **REQUIRE DEFENSIVE CODING TRAINING FOR DEVELOPERS.** Developers are the first line of defense when it comes to custom web applications. Developers should be made aware of the common mistakes that lead to vulnerabilities and learn ways to prevent these issues before the code is run on production systems.
- **IMPLEMENT DATA WHITELISTING.** Data sent from a user to the webserver should always be treated as potentially malicious. Developers should identify the data expected by the application and disallow characters that are invalid.

Red Siege would like to thank the Nakatomi Trading Corp for the opportunity to work on this project. Should you have any questions regarding these findings or the contents of this report, please feel free to contact us.

FINDINGS

OVERVIEW AND

QUICK

NAVIGATION

We give you a summary of the findings with links to the in-depth discussion. This allows you to quickly get to the information you need!

FINDINGS SUMMARY

RS-NTC-001 Lack of Multi-Factor Authentication

! Critical Risk Authentication

RS-NTC-002 Password Reuse

! Critical Risk Passwords

RS-NTC-003 Default Credentials

● High Risk Configuration Management

RS-NTC-004 Website Missing HSTS Header

● Medium Risk Configuration Management

RS-NTC-005 Web Server Content-Security-Policy Header Not Present

○ Low Risk Configuration Management

**ICONOGRAPHY
FOR FASTER
READING**

Easy to read icons mean you can quickly get the information you need. Icons are useful when printed in black in white and for those with color vision deficiency.

FINDINGS CLASSIFICATIONS

Each vulnerability or risk identified has been labeled as a Finding and categorized as a Critical Risk, High Risk, Medium Risk, Low Risk, or Informational, which are defined as:

CRITICAL RISK ISSUES

These vulnerabilities should be addressed promptly as they may pose an immediate danger to the security of the networks, systems, or data.

Exploitation does not require advanced tools or techniques or special knowledge of the target.

HIGH RISK ISSUES

These vulnerabilities should be addressed promptly as they may pose a significant danger to the security of the networks, systems, or data.

The issue is commonly more difficult to exploit but could allow for elevated permissions, loss of data, or a system downtime.

MEDIUM RISK ISSUES

These vulnerabilities should be addressed in a timely manner.

Exploitation is often difficult and requires social engineering, existing access, or special circumstances.

LOW RISK ISSUES

The vulnerabilities should be noted and addressed at a later date.

These issues offer very little opportunity or information to an attacker and may not pose an actual threat.

INFORMATIONAL ISSUES

These issues are for informational purposes only and likely do not represent an actual threat.

ACTIONABLE FINDINGS

Our findings include a "Validation" section will tell you how you can verify an issue is fixed. This let's your people validate fixes by themselves. Always make sure your vendor offers this!

ALWAYS CUSTOM RESULTS. ALWAYS!

YOU'LL NEVER SEE COPY/PASTE FROM A SCANNER... EVER!

FINDINGS

CRITICAL RISK FINDINGS

RS-NTC-001 LACK OF MULTI-FACTOR AUTHENTICATION

! Critical Risk Authentication

Impact

The Web VPN server, allows authentication without use of a second factor. Red Siege was able to guess valid credentials through a *password spray* attack and subsequently access the internal network.

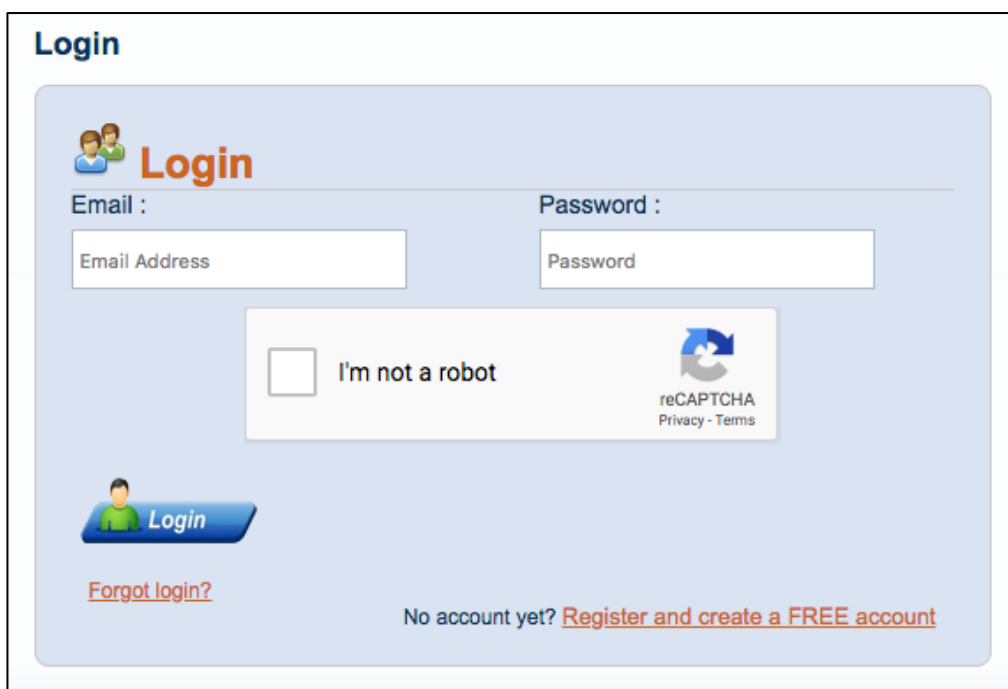


FIGURE 1. VPN LOGIN FORM LACKING 2ND FACTOR

Affected System

10.1.2.3 – <https://vpn.ntc.nope/vpn>

Description

Use of multi-factor authentication, such as a hardware token or mobile application, prevents an attacker from simply guessing passwords, as the attacker needs the token to authentication. Even if the user's password is compromised, an attacker cannot login without the additional factor.

Recommendations

Implement multi-factor authentication on key external facing systems.

References

<https://www.cisecurity.org/newsletter/two-factor-authentication/>

<https://www.cisecurity.org/understanding-cis-control-5/>

Validation

Login in to the VPN server and ensure that it asks for a factor (other than the username and password) before attempting to login. Check all of the VPN profiles to ensure there are no profiles that allow login with simply a username and password.

RS-NTC-002 PASSWORD REUSE



Critical Risk

Passwords

Impact

If users of different access or privilege levels have the same password, an attacker who compromises the password of a lower-privilege user could reuse that password to access other higher privilege accounts with the same password. Red Siege identified users having the same password. It appears the password may be a default password set when provisioning new users.

Password set A: 16 accounts with the same leetspeak¹ version of the word "password"

- apowell
- jnelson
- mfarrell
- arodgers
- karl
- nakatomi-svc-acct
- hgmcclane
- lbarnes
- tgabriel
- hgruber
- marketing
- wstuart
- jmcclane
- mbowman
- ykomarov

Password set B: 3 accounts with the same password based on the word "password" followed by a number.

- bbulaga
- cmatthews
- rcobb

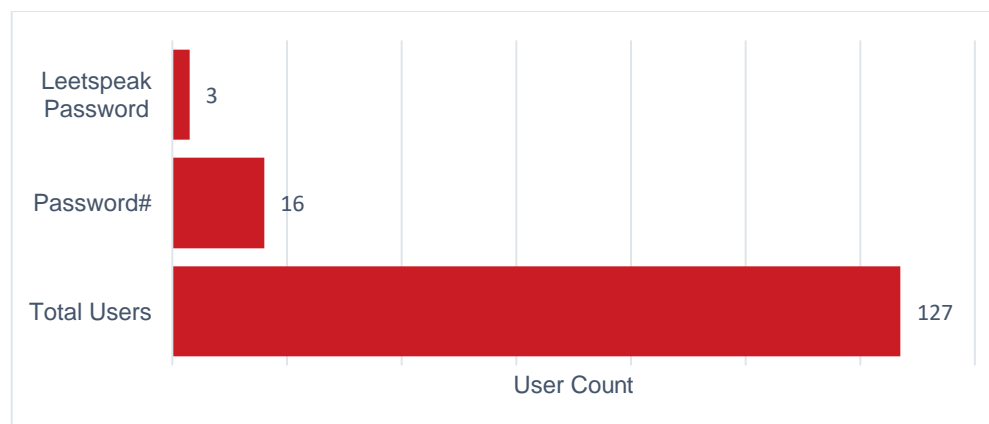


FIGURE 2. NUMBER OF USERS WITH BAD PASSWORDS

Description

Red Siege found multiple users using weak, known bad passwords. Red Siege used Burp Suite Pro² to identify users using common bad passwords.

¹ <https://en.wikipedia.org/wiki/Leet>

² Burp Suite Pro is developed by PortSwigger and is available at <https://portswigger.net/burp>

Recommendations

Review password policies to ensure user password requirements are sufficiently strong (longer) to prevent weak, known-bad passwords.

References

Strong Passphrases

- <https://www.kaspersky.com/blog/remember-strong-passwords/6386/>
- <https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/>

Password Managers

- <https://www.lastpass.com/business-password-manager>
- <https://www.cyberark.com/>
- <https://1password.com/>
- <https://keepass.info/>

Validation

Nakatomi Trading Corporation uses an LDAP directory for user authentication. NTC can extract the password hashes from the directory service using the command below and crack them with a tool like John the Ripper³ or Hashcat⁴.

```
ldapsearch -h 10.29.1.14 -W -o ldif-wrap=no -LLL -b dc=nakatomi,dc=nope -D uid=nakatomi-svc-acct,cn=tech,ou=tech,ou=VPN-access,dc=nakatomi,dc=org uid=* uid userPassword > user-password.txt
```

FIGURE 3. EXTRACT USERNAME AND PASSWORD FROM DIRECTORY SERVICE

Then, convert the hashes to a format crackable by Hashcat or John the Ripper, and use either tool to identify bad/weak passwords.

```
import base64

f = open('user-password.txt', 'r')
s = f.readlines()
f.close()

for l in s:
    if l[:4] == 'uid:':
        out = l[5:-1]
        good = False
```

³ John is an open source password cracking utility available at <http://www.openwall.com/john/>

⁴ Hashcat is an open source password cracking utility available at <https://hashcat.net/hashcat/>


```
elif l[:13] == 'userPassword:':
    out += ':' + str(base64.b64decode(l[15:]).decode('utf-8'))
print(out)
```

FIGURE 4. PYTHON SCRIPT TO CONVERT HASHES TO CRACKABLE FORMAT

HIGH RISK FINDINGS

RS-NTC-003 DEFAULT CREDENTIALS

● **High Risk** Configuration Management

Impact

NTC uses default credentials on APC PDU systems.

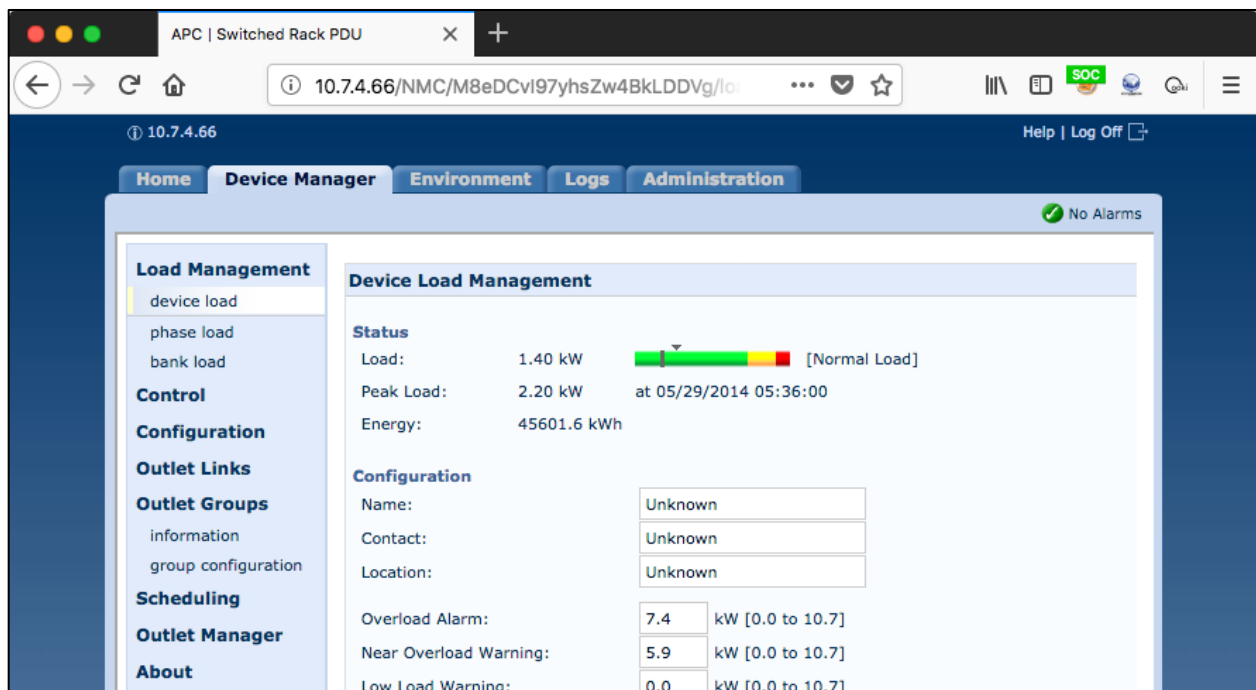


FIGURE 5. ACCESS TO APC PDU VIA DEFAULT CREDENTIALS

Affected System

APC PDU on port 80 with default credentials of `apc/apc`:

10.1.2.50

10.7.4.66

Discussion

Many devices and applications come with default usernames and passwords that provide privileged access to services. These credentials are published and easily discovered. Default credentials provide a common and easy entry point for an attacker.

Recommendations

Change the passwords on the affected systems.

Review or create a system deployment guide that includes 1) checking for default credentials/accounts and 2) changing those accounts to non-guessable passwords or removing the accounts.

References

US-CERT: Risks of Default Passwords on the Internet: <https://www.us-cert.gov/ncas/alerts/TA13-175A>

SANS – Risks of Default Passwords: <https://www.sans.edu/cyber-research/security-laboratory/article/default-psswd>

Validation

N/A

MEDIUM RISK FINDINGS

RS-NTC-004 WEBSITE MISSING HSTS HEADER

 *Medium Risk* *Configuration Management*

Impact

The NTC corporate website does not enforce the HTTP Strict-Transport-Security header.

Affected System

10.1.2.3 – <https://www.ntc.nope>

Description

The HTTP Strict-Transport-Security (HSTS) header prevents browsers from communicating with websites using unencrypted HTTP channels. Without this header, an attacker able to position themselves between a user's web browser and the server can perform HTTPs downgrade attacks. Attackers frequently accomplish this using malicious WiFi hotspots in areas such as coffee shops frequented by employees of the targeted organization.

Recommendations

NTC should configure web servers to enforce the HSTS on all web servers supporting HSTS. Red Siege recommends the following configuration:

Strict-Transport-Security: max-age=63072000; includeSubdomains;

References

Strict-Transport-Security Header:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

Validation

Use curl to review headers being sent by the website as shown below.

```
$ curl -sI https://www.ntc.nope
HTTP/1.1 200 OK
```

```
Date: Fri, 08 Jun 2018 15:39:45 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Last-Modified: Wed, 28 Mar 2018 22:17:10 GMT
Accept-Ranges: bytes
Content-Length: 14968
Vary: Accept-Encoding
Content-Type: text/html
```

FIGURE 6. RETRIEVING WEB SERVER HEADERS VIA CURL

LOW RISK FINDINGS

RS-NTC-005 WEB SERVER CONTENT-SECURITY-POLICY HEADER NOT PRESENT

 Low Risk Configuration Management

Impact

Without a properly set Content-Security-Policy header, an attacker can redress the web page and might be able to trick a user into taking actions on the website they did not intend to take.

Affected Systems

10.1.2.3 - <https://www.ntc.nope>

Description

The website does not implement the Content-Security-Policy header. When properly set, this header prevents the browser from loading the site inside another web page, an attack known as framing. Without this header, an attacker can carefully craft transparent and opaque layers to trick a user into clicking on buttons or links in the victim website and luring the user into taking actions on the targeted website they did not intend to take. The output below shows all the server headers for the affected website.

Recommendations

Configure the web server to set the Content-Security-Policy header for all server responses. Red Siege recommends the following configuration:

```
Content-Security-Policy: frame-ancestors 'self';
```

References

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

Validation

Use curl to review headers being sent by the website as shown below.

```
$ curl -skI https://www.ntc.nope
```

```
HTTP/1.1 200 OK
Date: Fri, 08 Jun 2018 15:39:45 GMT
Server: Apache
Content-Security-Policy: frame-ancestors 'self';
Last-Modified: Wed, 28 Mar 2018 22:17:10 GMT
Accept-Ranges: bytes
Content-Length: 14968
Vary: Accept-Encoding
Content-Type: text/html
```

FIGURE 7. VERIFYING CONTENT-SECURITY-POLICY WITH CURL

METHODOLOGY

This portion intentionally left blank. This section includes examples of the techniques used to assess the target systems.

APPENDIX

FINDING CATEGORIES

Vulnerability categories and the related weaknesses are listed below:

ARCHITECTURE – Related to system or network design

AUTHENTICATION – User authentication and access rights

CONFIGURATION MANAGEMENT – Related to system configuration and hardening

CRYPTOGRAPHY – Implementation and use of encryption and hashing

DATA VALIDATION – Input validation and data handling

DATA EXPOSURE – Unintended or excessive exposure of data

PASSWORD MANAGEMENT – Password storage and complexity requirements

PATCH MANAGEMENT – Patch and vulnerability management of systems

PERMISSIONS AND ACCESS CONTROL – Management of permissions, privileges, and features related to access control

TABLE OF FIGURES

Figure 1. VPN Login Form Lacking 2nd Factor	6
Figure 2. Number of Users with Bad Passwords	7
Figure 3. Extract Username and Password from Directory Service	8
Figure 4. Python Script to Convert Hashes to Crackable Format	9
Figure 5. Access to APC PDU via Default Credentials	9
Figure 6. Retrieving Web Server Headers via Curl	11
Figure 7. Verifying Content-Security-Policy with Curl	12

Prepared by Red Siege, LLC. Portions of this document, and the templates used in its production are the property of Red Siege, LLC. and cannot be used or copied without permission.

While precautions have been taken in the preparation of this document, Red Siege, LLC., the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of Red Siege, LLC and its services does not guarantee the security of any system, or that computer intrusions will not occur.