



Internal/External Network Penetration Test

IniTech Inc

Bill Lumbergh
Chief Technology Officer
April 18, 2016

Document Information

Assessment Information	
Assessors	Client
Kirit Gupta kirit.gupta@rhinosecuritylabs.com Dwight Hohnstein dwight.hohnstein@rhinosecuritylabs.com	IniTech Inc 1441 Mulberry Lane Seattle WA 98102 (425) 551-6591
Project Manager	Client Contact
Benjamin benjamin.caudill@rhinosecuritylabs.com	Bill Lumbergh blumbergh@initech.com
Assessment Type	Assessment Period
Internal/External Network Penetration Test	04-08-2016 - 04-14-2016
Project Number	Report Date
04-08-16-Ini-177	04-18-16

Revision History		
Date	Author	Notes
04-08-2016	Kirit Gupta	Rough Draft
04-12-2016	Benjamin Caudill	Edits
04-14-2016	Kirit Gupta	Final Copy



1. Executive Summary

Rhino Security Labs conducted a Internal/External Network Penetration Test for IniTech Inc (IniTech). This test was performed to assess IniTech's defensive posture and provide security assistance through proactively identifying vulnerabilities, validating their severity, and providing remediation steps.

Rhino Security Labs reviewed the security of IniTech's infrastructure and has determined a **Critical** risk of compromise from external attackers, as shown by the presence of serious vulnerabilities.

The detailed findings and remediation recommendations for these assessments may be found later in the report.

Summary of Strengths

While Rhino Security Labs was tasked with finding issues and vulnerabilities dealing with the current environment, it is useful to know when positive findings appear. Understanding the strengths of the current environment can reinforce security best practices and provide strategy and direction toward a robust defensive posture. The following traits were identified as strengths in IniTech's environment.

1. Strong firewall rules, closing many common ports and services.
2. Strong security configuration on both Linux servers and workstations.

Summary of Weaknesses

Rhino Security Labs discovered and investigated many vulnerabilities during the course of its assessments for IniTech Inc. We have categorized these vulnerabilities into general weaknesses across the current environment, and provide direction toward remediation for a more secure enterprise

1. Weak password and authentication policies across the enterprise.
2. Poor patching policies, resulting in outdated software packages (and associated vulnerabilities)
3. Sensitive information found across a number of public internet sources.
4. Inadequate log and security monitoring capabilities across network infrastructure.
5. Insufficient security incident response policies / procedures.



Strategic Recommendations

Not all security weaknesses are technical in nature, nor can they all be remediated by security personnel. Companies often have to focus on the root security issues and resolve them at their core. These strategic steps are changes to the operational policy of the organization. Rhino Security Labs recommends the following strategic steps for improving the company's security.

1. Enforce a more secure password policy, and educate users on proper password management.
2. Upgrade all Windows 2003 Servers to Windows Server 2008 R2 or above.
3. Transition company architecture from cleartext protocols to encrypted versions.
4. Enhance security defenses with additional detection and response capabilities, such as a SIEM



2. Summary Vulnerability Overview

Rhino Security Labs performed a Internal/External Network Penetration Test for IniTech Inc (IniTech) on 04-08-2016 - 04-14-2016. This assessment utilized both commercial and proprietary tools for the initial mapping and reconnaissance of the site, as well as custom tools and scripts for unique vulnerabilities. During the manual analysis, assessors attempted to leverage discovered vulnerabilities and test for key security flaws. The following vulnerabilities were determined to be of highest risk, based on several factors including asset criticality, threat likelihood, and vulnerability severity.

Summary

A Internal/External Network Penetration Test was performed on IniTech. The following vulnerabilities were found, indicating the overall risk rating of the networks in scope is **Critical**.

ID	Vulnerability	Risk	Remediation
C1	JBoss Credentials Brute Forced	Critical	Increase password complexity or remove the administrative account if possible.
H1	Linksys Phone Adapter Configuration Openly Accessible	High	Require authentication to access the configuration utility.
H2	Multiple Unpatched Apache Vulnerabilities	High	Update all Apache services and associated modules.
H3	Multiple Unpatched OpenSSH Vulnerabilities	High	Regularly patch and update all OpenSSH servers and associated modules.
H4	Multiple Unpatched PHP Vulnerabilities	High	Update all PHP services and associated modules.
H5	Polycom Administrative Panel Default Credentials	High	Change the default password of the administrative user.
H6	Sensitive Public Information Identified	High	Remove sensitive internal information from public resources.



ID	Vulnerability	Risk	Remediation
H7	Subdomain Takeover	High	Remove the affected CNAME record, which is no longer being used.
M1	Nameserver Processes Recursive Queries	Medium	Restrict the processing of recursive queries.
M2	Telnet Service Externally Available	Medium	For command-line remote access, replace Telnet with SSH, which utilizes end-to-end encryption.
L1	NTP Clock Variables Information Disclosure	Low	Restrict NTP readvar queries from unauthorized clients.
I1	Apache Tomcat default installation/welcome page installed	Informational	Remove the default installation page of Apache Tomcat.
I2	TCP Timestamp Response	Informational	Due to the very mild vulnerability presented, no changes are recommended.



3. Process and Methodology

Rhino Security Labs used a comprehensive methodology to provide a security review of IniTech's network(s). This process begins with detailed scanning and research into the architecture and environment, with the performance of automated testing for known vulnerabilities. Manual exploitation of vulnerabilities follows, for the purpose of detecting security weaknesses in the networks in scope.

Reconnaissance

Prior to the penetration analysis, the first step toward a Internal/External Network Penetration Test is gathering as much information as possible about the systems in scope. The primary goal in this process is to discover crucial data about IniTech's networks, providing the foundation for a tailored penetration test. Reconnaissance is carried out via automated scanners (such as nmap), as well as server fingerprinting and discovery.

Automated Testing

Rhino Security Labs used a vulnerability scanner to conduct an automated analysis on IniTech's network. This scan provides foundation for the full manual assessment, and each finding is manually verified to ensure accuracy and remove false positives.

Exploration and Verification

Rhino Security's consultants use the results of the automated scan, paired with their expert knowledge and experience, to finally conduct a manual security analysis of the client's networks. Our assessors attempt to exploit and gain remote unauthorized access to data and systems. The detailed results of both the vulnerability scan and the manual testing are shown in the tables below.

4. Constraints

The following limitations were placed upon this engagement, as agreed upon with IniTech:

- Vulnerabilities which would cause outages or interrupt the client's environment were noted but not validated.
- Penetration testing was limited to the agreed upon time period, scope, and other additional boundaries set in the contract and service agreement.



5. Assessment Scope

Rhino Security Labs compiled the following notes during the reconnaissance portion of the Internal/External Network Penetration Test penetration test. These notes provide the information needed to accurately assess the networks in scope_notes and test for vulnerabilities.

Enumeration	Description
Assessment Type	External Black-box
Vulnerability Scanner	Rapid7 NeXpose / Proprietary Internal Tools
VPN Utilized	None
Number of IP's in scope	265
IP Addresses	208.10.10.10 - 208.10.10.20 192.168.1.0 - 192.168.1.255



6. Vulnerability Findings

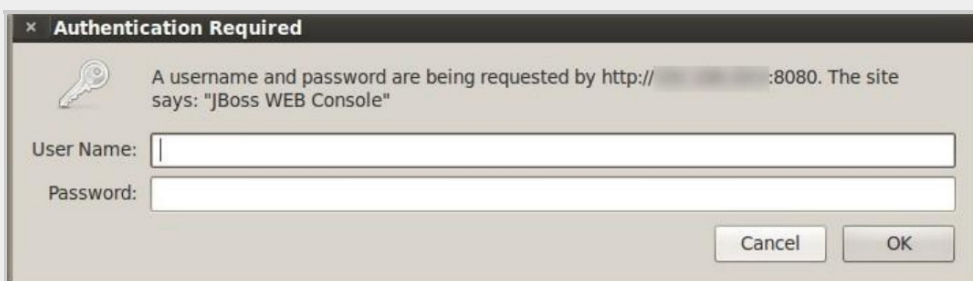
The vulnerabilities below were identified and verified by Rhino Security Labs during the process of this Internal/External Network Penetration Test test for IniTech. Retesting should be planned following the remediation of these vulnerabilities.

JBoss Credentials Brute Forced			
Report ID	C1	Associated CVE	n/a
Affected IP(s)	192.168.1.14 192.168.1.100-101 192.168.1.145 192.168.1.250	Risk	Critical
		Exploitation Likelihood	High
		Potential Impact	Critical
Description	The administrative credentials for a publicly facing JBoss server are easily bruteforced (admin::admin). See the above narrative for more details.		
Remediation	Increase password complexity, remove the administrative account if possible, and remove public access to JMX Console if possible		
Testing Process	During the enumeration phase of the engagement, port 8080 was identified as being open the system and confirmed as an outdated JBoss version (4.0.4) , hosting Java applets for IniTech		



```
Starting Nmap 6.01 ( http://nmap.org ) at
Nmap scan report for [REDACTED]
Host is up (0.00056s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
4445/tcp  open  upnotifyp
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8083/tcp  open  us-srv
8093/tcp  open  unknown
```


After further enumeration of the system, the tester confirmed that the JMX Console (the administrative console to JBoss) required a password.



The image shows a Windows-style dialog box titled "Authentication Required". It contains a key icon and a message: "A username and password are being requested by http://[REDACTED]:8080. The site says: 'JBoss WEB Console'". Below the message are two input fields labeled "User Name:" and "Password:". At the bottom right are "Cancel" and "OK" buttons.



Linksys Phone Adapter Configuration Openly Accessible

Report ID	H1	Associated CVE	CVE-2008-2092
Affected IP(s)	192.168.1.16 1192.168.1.15	Risk	High
		Exploitation Likelihood	Medium
		Potential Impact	High
Description	The Linksys Phone Adapter Configuration utility is publicly accessible. An attacker could route all phone calls through a device to intercept communications, or disrupt the lines entirely.		
Remediation	Require authentication to access the configuration utility.		
Testing Process	<p>This vulnerabilities was found by scanning the local network and accessing the associated web service on that device.</p> <p>See screenshots below:</p> 		



Multiple Unpatched Apache Vulnerabilities

Report ID	H2	Associated CVE	Multiple
Affected IP(s)	192.168.1.152 192.168.1.156 192.168.1.176 192.168.1.201	Risk Exploitation Likelihood Potential Impact	High Medium High
Description	<p>An outdated Apache HTTPD instance - and its multiple associated vulnerabilities - were found on the network. While Apache remote-code execution vulnerabilities are rare, older versions of Apache suffer from a number of other issues which could compromise the organizations confidentiality, integrity, and availability of data.</p> <p>For a list of vulnerabilities affected the version in the screenshot, please visit this URL: https://www.cvedetails.com/version-search.php?vendor=&product=apache&version=[2.2]</p>		
Remediation	Update all Apache services and associated modules to the newest version available, and ensure appropriate patch management policies are in place.		
Testing Process	<p>Using a port scanner, ports 80 and 443 were tested to verify the Apache version and associated vulnerabilities.</p> <p>Screenshots given below:</p> <pre>80/tcp open http Apache httpd 2.2.15 ((CentOS)) _http-server-header: Apache/2.2.15 (CentOS) _http-title: Nagios XI</pre>		



Multiple Unpatched OpenSSH Vulnerabilities

Report ID	H3	Associated CVE	Multiple
Affected IP(s)	192.1.168.210 192.168.1.145 192.168.1.176 192.168.1.188-189	Risk Exploitation Likelihood Potential Impact	High Critical Critical
Description	<p>Multiple OpenSSH vulnerabilities that compromise the confidentiality, integrity, and availability of the OpenSSH service were discovered based on your current version. However under some circumstances where operating systems will back-port patches and explicit version enumeration is not possible, this could yield a false positive.</p> <p>For a list of vulnerabilities affected the version in the screenshot, please visit this URL: https://www.cvedetails.com/version-search.php?vendor=&product=openssh&version=[3.4]</p>		
Remediation	Ensure all OpenSSH servers remain up-to-date by regularly patching OpenSSH and associated modules.		
Testing Process	<p>A port scanner and version-detection tools were used to verify service versions and vulnerabilities. See screenshot below:</p> <pre> 22/tcp open ssh OpenSSH 4.3 (protocol 2.0) ssh-hostkey: 1024 5e:31:2a:47:79:c9:91:13:0b:6c:d7:cc:b7:68:35:89 (DSA) 1024 95:a7:35:c1:2b:d0:4a:ef:99:79:ad:20:a0:5f:65:bf (RSA) 53/tcp open domain ISC BIND 9.6-ESV-R7-P4 </pre>		

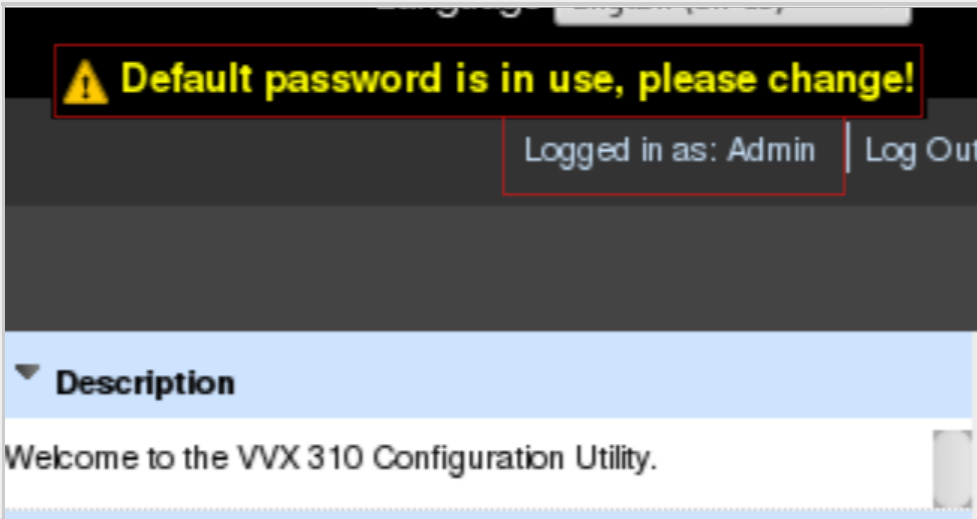


Multiple Unpatched PHP Vulnerabilities

Report ID	H4	Associated CVE	Multiple
Affected IP(s)	192.168.1.15 192.168.1.19 192.168.1.43 192.168.1.101 192.168.1.209 192.168.1.233	Risk Exploitation Likelihood Potential Impact	High Medium High
Description	<p>Multiple Unpatched PHP Vulnerabilities were found on the network.</p> <p>For a list of vulnerabilities affected the version in the screenshot, please visit this URL: https://www.cvedetails.com/version-search.php?vendor=&product=php&version=[2.5] </p>		
Remediation	Update all PHP services and associated modules (such as Apache) to the newest version available, and ensure appropriate patch management policies are in place.		
Testing Process	<p>Using port scanners and version detection tools, the web server was tested for its version of Apache, which was correlated to a corresponding version of PHP.</p> <pre>[200] Apache[2.2.15], Country[UNITED STATES][US] Le[Nagios XI], X-Powered-By PHP/5.3.3</pre>		

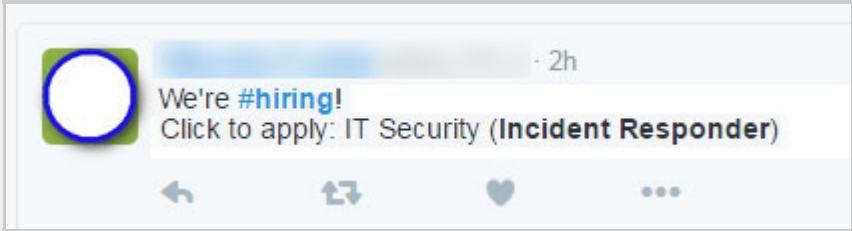


Polycom Administrative Panel Default Credentials

Report ID	H5	Associated CVE	CVE-2002-0626
Affected IP(s)	192.168.1.20	Risk	High
		Exploitation Likelihood	Critical
		Potential Impact	High
Description	The web administrative panel for the Polycom devices use default administrative credentials. This allows for an attacker to control all aspects of the device, including routing, ring tones and more.		
Remediation	Change the default password of the administrative user.		
Testing Process	<p>This Polycom device was found by scanning the local network and accessing the associated web service on that device.</p> <p>Screenshots provided below:</p> 		



Sensitive Public Information Identified

Report ID	H6	Associated CVE	n/a
Affected IP(s)	N/A	Risk	High
		Exploitation Likelihood	High
		Potential Impact	Critical
Description	A number of major sources of sensitive information were publically identified, eventually being leveraged in a targeted brute-force against public resources.		
Remediation	Remove sensitive information on the company from public resources, including social media and the corporate website		
Testing Process	<p>Sources such as Facebook, Twitter, and multiple company websites were spidered and parsed for information, as well as documents mined for metadata. Multiple employee accounts provided information on internal operations, schedules, employee names and emails, and other data that facilitated deeper attacks.</p> <p>See screenshots below: Twitter post indicating a critical IT Security role is unfilled.</p>  <p>Names of critical employees listed in a support page of the company website.</p>		



Need help?

To login please use your [redacted] email address and password.

Don't have a password? [Register for a password today.](#)

Can't find the answer you are looking for? Contact N [redacted] P [redacted], M [redacted] N [redacted] or M [redacted] W [redacted] through the [Contact Us Page](#).

Key employee posting his upcoming vacation on Facebook.



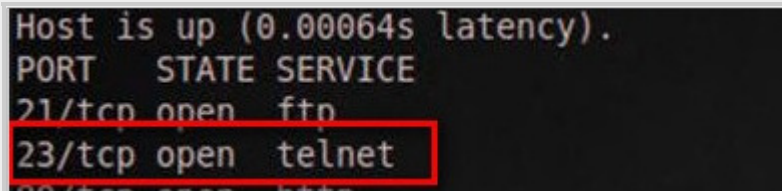
Subdomain Takeover			
Report ID	H7	Associated CVE	n/a
Affected IP(s)	192.168.1.100 192.168.1.135 192.168.1.155 192.168.1.165 192.168.1.205 192.168.1.209	Risk	High
		Exploitation Likelihood	High
		Potential Impact	Critical
Description	During the subdomain enumeration process, a CNAME record was found pointing to a hosted community site (Initech.com) no longer being used. Since the DNS record is still in place, it can be purchased/registered on the community hosting site and seized by an unauthorized user.		
Remediation	Remove the affected CNAME record, which is no longer being used.		
Testing Process	This issue was identified by first enumerating subdomains, which were then tied to specific DNS records and IP addresses. The given CNAME record was identified as pointing to a forum site which is no longer being utilized by the company.		



Nameserver Processes Recursive Queries			
Report ID	M1	Associated CVE	n/a
Affected IP(s)	192.168.1.14 192.168.1.49 192.168.1.147 192.168.1.154 192.168.1.168 192.168.1.189	Risk	Medium
		Exploitation Likelihood	Low
		Potential Impact	Critical
Description	Allowing nameservers to process recursive queries coming from any system may, in certain situations, help attackers conduct denial of service or cache poisoning attacks.		
Remediation	Restrict the processing of recursive queries to only systems that should be allowed to use this nameserver.		
Testing Process	NSE (Nmap Scripting Engine) was used to test for Recursive DNS queries with a given list of domains./r/nScreenshots as given below:/r/n		



Telnet Service Externally Available

Report ID	M2	Associated CVE	n/a
Affected IP(s)	208.10.10.10-11	Risk	Medium
		Exploitation Likelihood	Medium
		Potential Impact	Critical
Description	<p>The Telnet service was found available on the external network and available to the internet. Telnet does not use encryption during the transmission of credentials, making it trivial for attackers to steal credentials if on the same network as the victim client.</p> <p>Since Man-in-the-Middle and snooping-style attacks are one of the largest risks in Telnet, devices where Telnet isn't used (such as printers) are less of a risk than those where Telnet is used as a means of remote access.</p>		
Remediation	For command-line remote access, replace Telnet with SSH, which utilizes end-to-end encryption.		
Testing Process	<p>A port scanner was initially used to identify the open port. From there, a Telnet client and other tools confirmed connectivity and functionality.</p> <p>See screenshots below:</p> 		

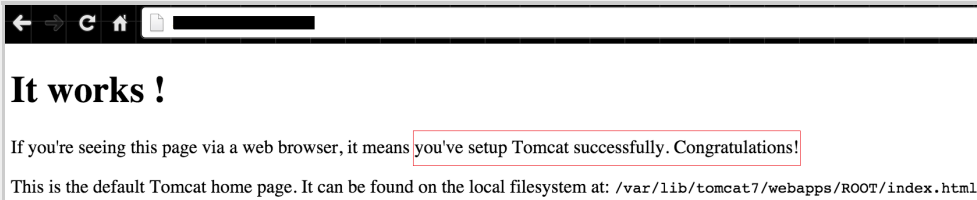


NTP Clock Variables Information Disclosure

Report ID	L1	Associated CVE	n/a
Affected IP(s)	192.168.1.24 192.168.1.69 192.168.1.122 192.168.1.132 192.168.1.222	Risk	Low
		Exploitation Likelihood	Low
		Potential Impact	Low
Description	This system allows the internal NTP variables to be queried. These variables contain potentially sensitive information, such as the NTP software version, operating system version, peers, and more.		
Remediation	Remove NTP from the given systems or apply an ACL that restricts NTP readvar queries from unauthorized clients.		
Testing Process	NTP "readvar" queries are sent to the given NTP server, which then respond with identifying information.		



Apache Tomcat default installation/welcome page installed

Report ID	I1	Associated CVE	CVE-2011-3190
Affected IP(s)	192.168.1.5 192.168.1.10 192.168.1.20-22	Risk	Informational
		Exploitation Likelihood	Informational
		Potential Impact	Informational
Description	A host(s) on the network still contain the default installation page of Apache Tomcat, indicating many of the default configurations of the webserver haven't been changed.		
Remediation	Remove the default installation page of Apache Tomcat.		
Testing Process	<p>By simply browsing to the webserver, the default installation page of Tomcat can be viewed and confirmed.</p> <p>See screenshots below:</p> 		



TCP Timestamp Response			
Report ID	I2	Associated CVE	CVE-1999-0524
Affected IP(s)	192.168.1.1 192.168.1.20-21 192.168.1.25 192.168.1.53	Risk	Informational
		Exploitation Likelihood	Informational
		Potential Impact	Informational
Description	The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.		
Remediation	Due to the very mild vulnerability presented, no changes are recommended.		
Testing Process	This vulnerability was detected by automated scanning.		



Appendix A: Definitions and Criteria

The risk ratings assigned to each vulnerability are determined through averaging several aspects of the exploit and the environment, including reputation, difficulty, and criticality.

Risk Rating Definitions

CRITICAL

Critical vulnerabilities pose very high threat to a company's data, and should be fixed on a top-priority basis. They can allow a hacker to completely compromise the environment or cause other serious impacts to the security of the networks in scope.

HIGH

High severity vulnerabilities should be considered a top priority in terms of mitigation. These are the most severe issues and generally cause an immediate security concern to the enterprise

MEDIUM

Medium severity vulnerabilities are a lower priority, but should still be remediated in a timely manner. These are moderate exploits that have less of an impact on the environment.

LOW

Low severity vulnerabilities are real but trivially impactful to the environment. These should only be remediated after the HIGH and MEDIUM vulnerabilities are resolved.

INFORMATIONAL

Informational vulnerabilities have no impact as such to the environment by themselves. However, they might provide an attacker with information to exploit other vulnerabilities.



Appendix B: Tools and Utilities

Nmap - Nmap is a powerful network security scanning application that uses carefully crafted packets to probe target networks and discover exposed open ports, services, and other host details, such as operating system type.

NeXpose - An enterprise-grade vulnerability assessment tool used to identify many common vulnerabilities in both physical and virtualized systems.

Nessus - Nessus is a proprietary vulnerability scanner that specializes in delivering comprehensive mappings of target system vulnerabilities, including web and network vulnerabilities, misconfigurations, weak passwords and even compliance problems, such as with HIPAA and PCI.

Metasploit - Metasploit is a modular, expandable toolset designed for rapidly discovering and exploiting vulnerabilities in a target system. Though it requires a great deal of skill to utilize effectively, Metasploit allows assessors to quickly and easily enumerate real-world vulnerabilities, as well as discover their potential danger and significance.

FOCA - FOCA is used for extracting hidden information and metadata from various sources. Examples include pulling names and emails from Word document files, application versions from PDF's, and more. This can be used for specific targeting of users and companies in phishing and other social engineering engagements.

Custom Scripts and application - In addition to the above tools, Rhino Security Labs also makes use of its own proprietary tools and scripts to quickly adapt to new and unique environments.



Appendix C: List of Changes Made to IniTech Inc Systems

No changes were made to the environment in scope, such as creating new user accounts or uploading files to the target system. This is provided as the full accounting of modifications by the penetration testing team at Rhino Security Labs.

