single point of contact

Client
Penetration Test Report

Fernando Leon
1 (408) 791 4300
fleon@singlepointoc.com

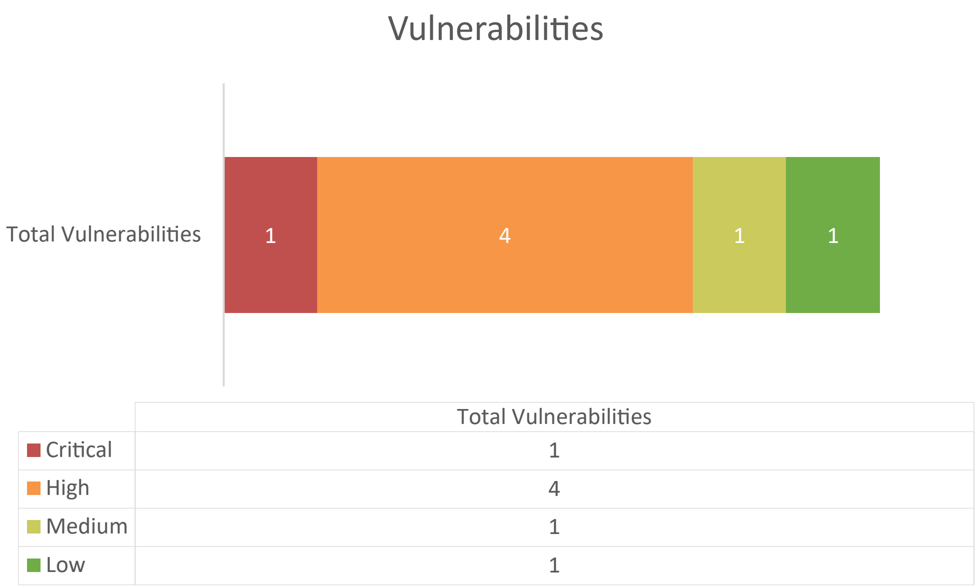
CONTENTS

EXECUTIVE SUMMARY

Single Point of Contact Compliance and Security, Inc conducted a penetration test for CLIENT (“the Company”) from DATE based upon the Authorization to Test document provided by the Company. Single Point of Contact followed a testing methodology that sought to identify vulnerabilities and, through exploitation, determine the impact to the Company’s business operations. Single Point of Contact assigned a risk level based on goals achieved during testing.

Internal Network Testing		**overall risk: HIGH**
Description	Goal	Result
Simulate a malicious insider that has internal network access.	Compromise internal systems, elevate to administrative access and obtain sensitive data.	Single Point of Contact abused a known vulnerability to gain a list of all usernames, guessed a weak password and used that account obtain sensitive data that was on internal network shares.

Over the duration of the goal-based testing, Single Point of Contact attempted to identify and leverage vulnerabilities that put the Company at the greatest risk. The count of vulnerabilities for the entire penetration test is shown below:



	Total Vulnerabilities
🟥 Critical	1
🟧 High	4
🟨 Medium	1
🟩 Low	1

Single Point of Contact prioritized attack paths that maximized the impact to the Company’s business and therefore did not attempt to identify or validate every vulnerability that existed in the environment. The Company should review the results of the engagement, remediate identified weaknesses and continue to perform regular security reviews, including vulnerability scanning and penetration testing.

Findings from penetration testing often indicate systemic underlying problems. The Company should investigate the root cause that allowed vulnerabilities to go undetected (e.g., lack of regular vulnerability scans) or unfixed (e.g., slow patch management).

Penetration testing is also a useful exercise for measuring detection and response capabilities. The Company should review their alerting and logging processes to identify whether systems detected testing actions and whether personnel took the appropriate actions.

FINDINGS

Summarized below are the findings that Single Point of Contact identified during testing:

1. Weak Credentials (Critical)			
Description	Devices and user accounts used weak or default credentials and allowed unprivileged access to the environment.		
Found During	Internal testing		
Instances	**Host**	**Port**	**Notes**
	Sample Report – Intentionally blank	443/tcp, 623/udp	iDRAC root user with default password
	Sample Report – Intentionally blank	443/tcp, 623/udp	iDRAC root user with default password
	Sample Report – Intentionally blank	445/tcp	authentx, warez, wellpoint domain accounts have the same password as the username
	Sample Report – Intentionally blank	443/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer
	Sample Report – Intentionally blank	80/tcp	printer

1. Weak Credentials (Critical)

<table>
<tr><td>Solution</td><td colspan="2">Consider implementing the following recommendations, which are based off NIST Special Publication 800-63B:
• Lock out accounts after 10 invalid logon attempts
• Require passwords to be at least 12 characters in length
• Use passphrases (e.g., “Secure the summit with Single Point of Contact”)
• Avoid imposing other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for passwords
• Avoid requiring memorized secrets to be changed periodically and instead force a change if there is evidence of compromise
• Avoid storing password hints or relying upon secret questions (e.g., “What was the name of your first pet?”)
• Compare prospective passwords against a list of values known to be commonly used, expected or compromised (e.g., passwords obtained from previous breaches)
• Use password managers to generate and store passwords</td></tr>
<tr><td rowspan="2">Remediation</td><td>Date</td><td>Description</td></tr>
<tr><td>N/A</td><td>N/A</td></tr>
<tr><td colspan="3">Testing Notes

Sample Report – Intentionally blank</td></tr>
</table>

2. IPMI v2.0 Password Hash Disclosure (High)

<table>
<tr><td>Description</td><td>The affected host supports the vulnerable protocol Intelligent Platform Management Interface version 2.0 which allows an attacker to gain password hash information. These password hashes can be cracked and used to gain access to valid user accounts via HMAC from a RAKP message 2 response from a BMC.</td></tr>
<tr><td>Found During</td><td>Internal testing</td></tr>
<tr><td>Instances</td><td>
<table>
<tr><th>Host</th><th>Port</th></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>623/udp</td></tr>
</table>
</td></tr>
<tr><td>Solution</td><td>Single Point of Contact recommends disabling IPMI over LAN if not needed or using strong passwords that are difficult to crack as well as using ACLs to limit access.</td></tr>
<tr><td>Remediation</td><td>
<table>
<tr><th>Date</th><th>Description</th></tr>
<tr><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td colspan="2">Testing Notes

<i>Sample Report – Intentionally blank</i></td></tr>
</table>

3. IPMI Cipher Suite Zero Authentication Bypass (High)

Description	The IPMI service listening on the remote system has cipher suite zero enabled, which permits logon as an administrator without requiring a password. Once logged in, a remote attacker may perform a variety of actions, including powering off the remote system.	
Found During	Internal testing	
Instances	**Host**	**Port**
	Sample Report – Intentionally blank	623/udp
Solution	Disable cipher suite zero or limit access to the IPMI service.	
Remediation	**Date**	**Description**
	N/A	N/A

Testing Notes

```
[+]- IPMI - VULNERABLE: Accepted a session open request for cipher zero
```

4. Oracle TNS Listener Remote Poisoning (High)

<table>
<tr><td>Description</td><td>The remote Oracle TNS listeners allows service registration from a remote host, which an attacker can exploit to manipulate database instances. This can lead to man-in-the-middle attacks, session hijacking or denial of service attacks to the affected database servers.</td></tr>
<tr><td>Found During</td><td>Internal testing</td></tr>
<tr><td>Instances</td><td><table><tr><th>Host</th><th>Port</th></tr><tr><td><em>Sample Report – Intentionally blank</em></td><td>1521/tcp</td></tr><tr><td><em>Sample Report – Intentionally blank</em></td><td>1521/tcp</td></tr></table></td></tr>
<tr><td>Solution</td><td>Apply the valid workaround for the version of Oracle running. More information on this can be found here<ul><li>https://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html</li></ul></td></tr>
<tr><td>Remediation</td><td><table><tr><th>Date</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table></td></tr>
<tr><td colspan="2">Testing Notes

<em>Sample Report – Intentionally blank</em></td></tr>
</table>

5. SMB Null Session (High)

<table>
<tr><td>Description</td><td colspan="2">It is possible to log into Microsoft Windows systems using a NULL session (i.e., with no login or password). This allows information to be enumerated without any prior knowledge. An attacker can use this information to footprint the organization’s internal network without authorization.</td></tr>
<tr><td>Found During</td><td colspan="2">Internal testing</td></tr>
<tr><td rowspan="7">Instances</td><td><b>Host</b></td><td><b>Port</b></td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>445/tcp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>445/tcp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>445/tcp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>445/tcp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>445/tcp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>445/tcp</td></tr>
<tr><td>Solution</td><td colspan="2">Configure the service to disallow Null Session.</td></tr>
<tr><td rowspan="2">Remediation</td><td><b>Date</b></td><td><b>Description</b></td></tr>
<tr><td>N/A</td><td>N/A</td></tr>
<tr><td colspan="3">Testing Notes

<i>Sample Report – Intentionally blank</i></td></tr>
</table>

6. SNMP Agent Default Community Name (Medium)

<table>
<tr><td>Description</td><td>It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).</td></tr>
<tr><td>Found During</td><td>Internal testing</td></tr>
<tr><td>Instances</td><td><table><tr><th>Host</th><th>Port</th></tr><tr><td><i>Sample Report – Intentionally blank</i></td><td>161/udp</td></tr></table></td></tr>
<tr><td>Solution</td><td>Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port or change the default community string.</td></tr>
<tr><td>Remediation</td><td><table><tr><th>Date</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table></td></tr>
</table>

Testing Notes

```
[+]- Login Successful: public (Access level: read-only); Proof (sysDescr.0):

[+]Connected.

[*] System information:

Host IP
Hostname
Description                    : -
Contact                        :
Location                       :
Uptime snmp                    : -
Uptime system                  :
System date                    : -

[*] Network information:

IP forwarding enabled          : no
Default TTL                    : 64
TCP segments received          : 285240
TCP segments sent              : 282886
TCP segments retrans           : 1877
Input datagrams                : 354782
Delivered datagrams            : 354757
```

7. FTP Anonymous (Low)

<table>
<tr><td>Description</td><td colspan="2">Single Point of Contact found FTP servers which allow anonymous access via the username and password combination of ‘anonymous’.</td></tr>
<tr><td>Found During</td><td colspan="2">Internal testing</td></tr>
<tr><td rowspan="3">Instances</td><td><b>Host</b></td><td><b>Port</b></td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>21/tcp</td></tr>
<tr><td><i>Sample Report – Intentionally blank</i></td><td>21/tcp</td></tr>
<tr><td>Solution</td><td colspan="2">Disable the use of anonymous accounts and if possible, switch to the secure alternative of FTP, FTPS.</td></tr>
<tr><td rowspan="2">Remediation</td><td><b>Date</b></td><td><b>Description</b></td></tr>
<tr><td>N/A</td><td>N/A</td></tr>
<tr><td colspan="3">Testing Notes

The services appeared to belong to printers and did not appear to contain sensitive data.</td></tr>
</table>

METHODOLOGY

Single Point of Contact's penetration testing methodology is based upon the National Institute of Standards and Technology (NIST) SP 800-115 and Penetration Testing Execution Standard (PTES) frameworks and contains the following phases.

Planning

Single Point of Contact prepares for initial planning sessions with the Company by reviewing the Company's business processes, key personnel, physical locations and Internet-accessible footprint. Single Point of Contact and the Company collaborate to create the rules, attack scenarios, and goals for testing. The Company may provide additional documentation and access to applications, systems and networks to facilitate targeted testing. Single Point of Contact and the Company capture scenarios, rules of engagement, goals and targets within an Authorization to Test (ATT) form, which the Company uses to authorize testing. The Company is responsible for ensuring that the ATT contains all targets for testing and that the Company has the authority to permit Single Point of Contact to perform penetration testing against the identified targets.

Discovery

The discovery phase of testing includes two parts, which are information gathering about targets, including available attack surface, and vulnerability analysis. Single Point of Contact's discovery techniques differ depending on the class of target that is being tested.

Network Targets

Single Point of Contact probes network targets to identify available ports and services. Single Point of Contact reviews accessible services to determine service version and configuration, including the underlying operating system. Single Point of Contact compares enumerated software and configurations against known vulnerabilities to determine targets for the exploitation phase. Single Point of Contact also reviews communication across the network, as devices frequently leak information that contains sensitive data or can otherwise be manipulated. Where applicable to achieve the defined goals of each test, Single Point of Contact discovers vulnerabilities by leveraging the advanced tactics and techniques defined within the MITRE ATT&CK framework:

- **Initial Access** - techniques that adversaries use to gain an initial foothold within a network
- **Execution** - techniques that result in execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with initial access as the means of executing code once access is obtained, and lateral movement to expand access to remote systems on a network
- **Persistence** - any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access
- **Privilege Escalation** - techniques that allows an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. Adversaries can enter a system with unprivileged access and must take advantage of a system weakness to obtain local administrator or SYSTEM/root level privileges. A user account with administrator-like access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege
- **Defense Evasion** - techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation

- **Credential Access** - techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network. This allows the adversary to assume the identity of the account, with all of that account's permissions on the system and network, and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment
- **Discovery** - techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase
- **Lateral Movement** - techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems
- **Collection** - techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration
- **Exfiltration** - techniques and attributes that result or aid in the adversary removing files and information from a target network
- **Command and Control** - techniques that allow adversaries to communicate with systems under their control within a target network. Single Point of Contact may use command and control techniques to, for example, compromise and query multiple systems at a time for sensitive information

Attack

Single Point of Contact verifies previously identified potential vulnerabilities by attempting to exploit them. Vulnerabilities are exploited to gain an initial foothold, escalate privileges, gain widespread administrative access, install malicious tools, pivot into new areas and gain access to sensitive information in accordance with the goals of the test.

Throughout testing, Single Point of Contact uses a combination of commercial, open-source and proprietary tools including, but not limited to:

- Metasploit
- Nmap
- Responder
- Kali Linux
- SQLmap
- Wireshark
- Empire
- Mimikatz
- Impacket
- Nessus
- Burp Suite
- hashcat

Single Point of Contact does not perform denial-of-service attacks unless specifically requested by CLIENT. Single Point of Contact makes best efforts to reduce the likelihood of service interruption.

Reporting

Single Point of Contact regularly communicates on the progress and results of testing during the engagement. Single Point of Contact immediately notifies the Company if a critical-risk finding is discovered so that the Company can quickly remediate the issue.

Single Point of Contact creates a report that contains, at minimum, the following items:

- **Executive Summary** - provides a high-level overview of the testing results and is intended to be read by executives, customers and business partners. This section is designed to stand alone and be removed from the report so that the Company can provide it to other parties
- **Findings** - describes each exploitable vulnerability. The findings results are intended to be distributed to technical teams
  - **Solution** - recommendations on how to resolve each identified issue
  - **Risk Ranking** - each issue identified is assigned a risk ranking that is derived from the Common Vulnerability Scoring System (CVSS). Single Point of Contact adjusts ratings based on the specific instances identified in the the Company environment

        - **Critical** - Findings that are likely to allow an attacker administrative-level access to systems or data that would catastrophically impact the organization
        - **High** - Findings that are likely to allow the attacker administrative access to sensitive data or systems
        - **Medium** - Findings that are likely to allow an attacker with user-level access to systems or data or would otherwise need to be combined with other vulnerabilities to form an effective attack
        - **Low** - Findings that are likely to provide an attacker with useful information that might aid in future attacks or when combined with other vulnerabilities
        - **Informational** - Findings that do not represent a security risk but may contain useful information to review
    - **Testing Notes** - additional details that provide enough information such that the issue can replicated by technical teams
    - **Remediation** - updates about the finding, such as retesting notes or management responses
- **Methodology** - describes Single Point of Contact's testing process
- **Attack Narrative** - describes an account of the testing from the point-of-view of the tester, including the attacks that failed or vulnerabilities that could be chained together as part of a multi-step attack
- **Scope -** lists the targets of the testing
    - **Constraints** - describes any limitations placed on testing that the Company should consider when interpreting the results of the engagement (e.g., bandwidth restrictions)

Penetration testing is performed at a point in time during a defined testing window. Single Point of Contact prioritizes attack paths that will fulfill the goals of testing and therefore does not attempt to identify or validate every vulnerability that exists in the environment. New vulnerabilities and exploits are developed and discovered regularly. The Company should continuously monitor the environment, including by performing periodic vulnerability scans and penetration tests.

SCOPE

The Company authorized testing of the following resources:

Internal Network Testing

Networks	Priority	Notes
Sample Report – Intentionally blank		VLAN 100 | PROD_INTERNALI
Sample Report – Intentionally blank	x	VI-AN 110 | DATABASEI
Sample Report – Intentionally blank		VLAN 115 IWEB_SVCSI
Sample Report – Intentionally blank		VLAN 120 IAPP_SVCSI
Sample Report – Intentionally blank		VLAN 199 ISVR_MGMTI
Sample Report – Intentionally blank		VLAN 20 TEST_DEV
Sample Report – Intentionally blank		VLAN 230 |
Sample Report – Intentionally blank		VLAN 240 | REPLICA|
Sample Report – Intentionally blank		VLAN 100 | PROD_INTERNALI
Sample Report – Intentionally blank	x	VLAN 110 | DATABASE I
Sample Report – Intentionally blank		VI-AN 115 IWEB_SVCSI
Sample Report – Intentionally blank		VLAN 120 IAPP_SVCSI
Sample Report – Intentionally blank		VLAN 199 ISVR_MGMTI
Sample Report – Intentionally blank		VLAN 200 ITEST_DEVI
Sample Report – Intentionally blank		VLAN 230 | BACKUPI
Sample Report – Intentionally blank		VLAN 240 | REPLICAI
Sample Report – Intentionally blank		VLAN 99 J NW_MGMT I
Sample Report – Intentionally blank		VLAN 100 RX_LINC I
Sample Report – Intentionally blank		VLAN 102 | RX_SELECT I
Sample Report – Intentionally blank		VLAN 104 | MAXCARE I
Sample Report – Intentionally blank		VLAN 106 | OPHA
Sample Report – Intentionally blank		VLAN 108 | ACCOUNTING I
Sample Report – Intentionally blank	x	VLAN 110 | SERVERS
Sample Report – Intentionally blank	x	VLAN 112 | IT
Sample Report – Intentionally blank	x	VLAN 113 | NEW_IT I
Sample Report – Intentionally blank		VI-AN 114 | EXECUTIVE
Sample Report – Intentionally blank		VLAN 116 | PERIPHERALS I

<table>
<tr><th>Networks</th><th>Priority</th><th>Notes</th></tr>
<tr><td><em>Sample Report – Intentionally blank</em></td><td></td><td>VLAN 128 | VOICE</td></tr>
<tr><td><em>Sample Report – Intentionally blank</em></td><td>x</td><td>VI-AN 192 | CORP_WIFI I</td></tr>
<tr><td><em>Sample Report – Intentionally blank</em></td><td>x</td><td>VI-AN 193 I PHONES</td></tr>
<tr><td><em>Sample Report – Intentionally blank</em></td><td>x</td><td>VLAN 228 | GUEST_WIFI I</td></tr>
<tr><td><em>Sample Report – Intentionally blank</em></td><td></td><td>VLAN 240 | DATA_REP I</td></tr>
</table>

Internal Testing Starting Points

Network Address	Method
Sample Report – Intentionally blank	Testing device provided by CLIENT

Constraints

Testing occurred under the following constraints:

- Intentional attacks that could cause outages, such as denial of service attacks, were not performed. The Company should investigate any downtime experienced during testing as it may indicate a lack of service or organizational resiliency
- Hosts that are not defined within the scope of the engagement were excluded from testing

Aside from these constraints, the Company provided sufficient bandwidth and access for testing. Real attackers are not limited, which the Company should consider when interpreting the results of this engagement and planning future penetration tests.

ATTACK NARRATIVE

Single Point of Contact began the internal testing by running enumeration scans to determine what ports and services were running and accessible to the hosts. Doing so returned a wealth of information to comb through. Single Point of Contact initially focused on web servers in the internal environment and manually accessed all applications running HTTP or HTTPS. Doing so allowed Single Point of Contact to discover unauthenticated access to internal devices such as printers. Single Point of Contact discovered that the same printers also typically allowed anonymous access over FTP but did not appear to contain any sensitive data. Single Point of Contact performed LLMNR/NBT-NS spoof attacks but did not capture any hashes during the duration of the test.

Single Point of Contact discovered IPMI services and known weaknesses, including password hash disclosure. Single Point of Contact cracked the password hashes, which revealed that the passwords were the default for Dell iDRAC devices.

Sample Report – Intentionally blank

Single Point of Contact connected to the iDRAC interfaces. At this point, Single Point of Contact could power off the device, connect to the console or take over the hosted operating system by changing the bootable media.

Sample Report – Intentionally blank

Single Point of Contact did not take further action because doing so would require rebooting the hosted operating system.

Single Point of Contact tested all hosts with SMB services running for Null access and identified several devices that allowed access. Single Point of Contact used this access to enumerate the CLIENTDOM domain, including user and group membership.

Sample Report – Intentionally blank

Single Point of Contact performed a password guess against each account by guessing the username as the password and discovered three users whose password was the same as the username (authentx, warez, wellpoint). Single Point of Contact used the authentx account, which was a domain user, and enumerated all available shares to discover sensitive information.

Sample Report – Intentionally blank

At this point, Single Point of Contact had access to dozens of shares and thousands of internal files, including files that appeared to be related to the Company's store locations.

Sample Report – Intentionally blank