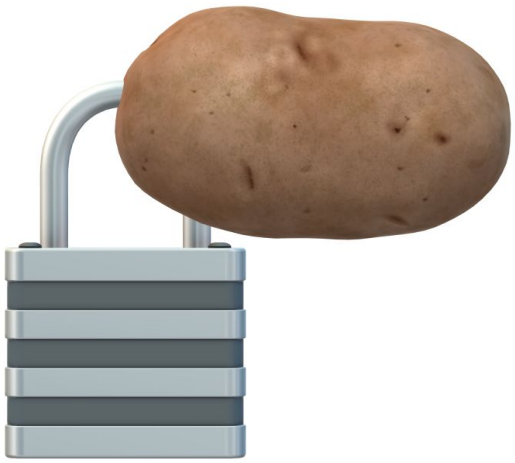
Starch Consulting



Infrastructure Penetration Test

RVAPTHosting

4/22/2020

Prepared by:

Jacob Ruud
Emannual Adewale
Omar Aljaloud
Abdulmalik Banaser

Presented to:

Bob Dino
Joe Bank
Jon Doe

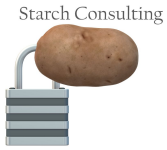


Table of Contents

Table of Contents **2**

Disclaimer **3**

Executive Summary **3**

Managerial Overview **4**

Topology 5

Engagement Timeline (April 6-16, 2020) 6

Risk Level Methodology 6

Recommended Mitigation Plan 7

Technical Risks **8**

High Priority Risks 8

Default Credentials (CVSS 9.0) 8

Compromised Client Information (CVSS 10.0) 9

Medium Priority Risks 10

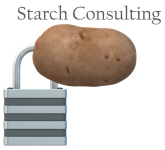
Plaintext Password Storage (CVSS 5.0) 10

Password Reuse (CVSS 4.5) 11

Low Priority Risks 11

Active Legacy Device (CVSS 2.0) 11

Active Retired User Accounts (CVSS 3.0) 12



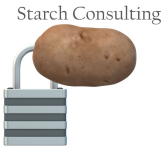
Disclaimer

Starch Consulting does not guarantee that the results of this test will identify absolutely all risks present within The Company's infrastructure and can not be held responsible if a breach occurs even after implementing all suggested mitigation techniques.

Executive Summary

Starch Consulting et. al was contracted by RVAPTHosting, further referred to as "The Company," to perform a comprehensive assessment of its corporate infrastructure. The goal of this assessment was to determine potential risk to the organization as a result of any vulnerabilities that may be present in said infrastructure. This test was designed to be a "black box assessment," meaning Starch Consulting was provided no knowledge of the infrastructure other than VPN access to the hosting DMZ. All tests were performed in a production environment, so steps were taken to ensure The Company experienced as little downtime as possible. RVAPTHosting, and its clients were made aware that testing was taking place during the engagement period. All tests were performed with the end goal of keeping user account information and financial data safe. This goal constitutes identifying, analyzing, and classifying technical risks according to the risk matrix outlined in the Overview section of this report.

Based on our findings, The Company may suffer business impacts through system and network compromise or via disclosure of sensitive client information. The weak password storage and use policies in place on your infrastructure could lead to compromise or downtime of important network endpoints, causing financial impact and customer dissatisfaction. Also, exposure of client financial information is equivalent to multiple compliance violations, including PCI-DSS and GDPR, and could mean potential lawsuits if handled improperly. Starch Consulting suggests remediation of these issues as soon as possible to avoid any significant impact to normal business operations



Managerial Overview

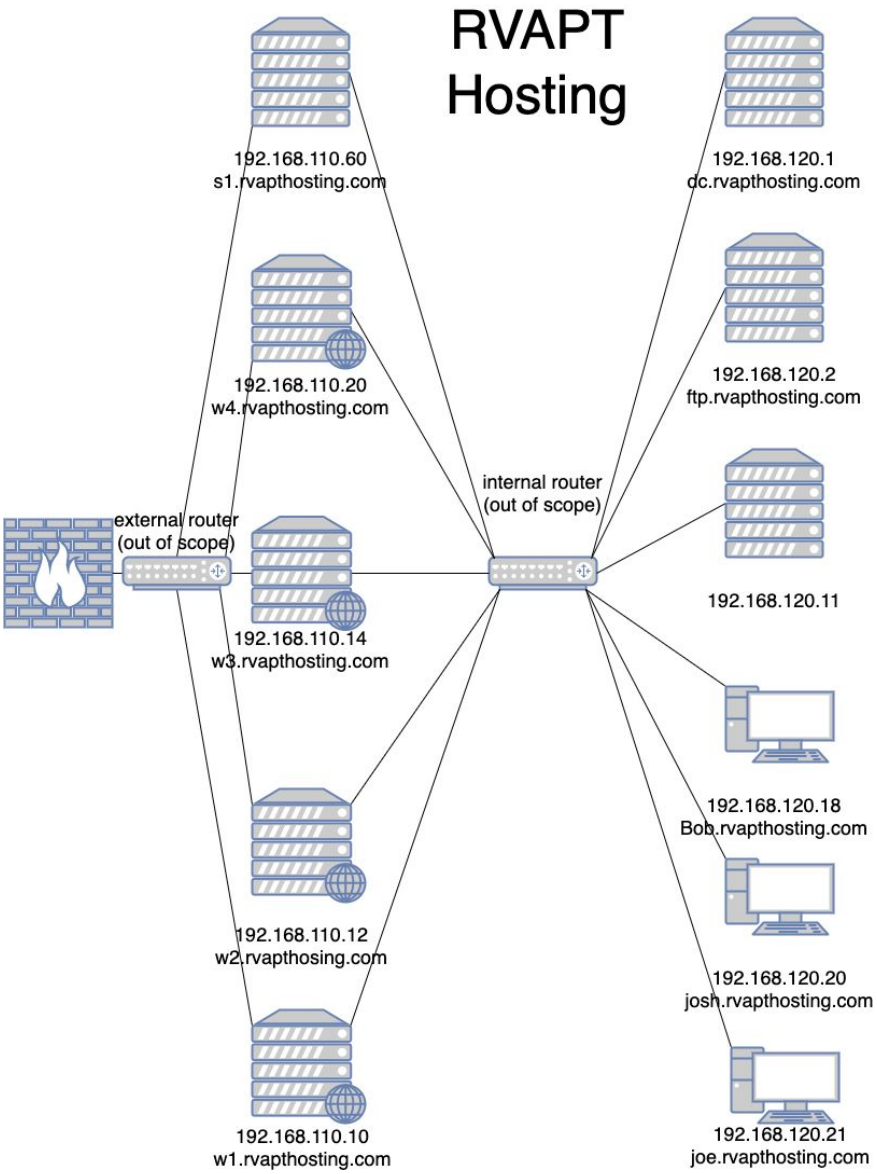
After surveying The Company's corporate infrastructure, Starch Consulting found the **use of default credentials** as well as **compromised sensitive client information** on The Company's network. These two findings are high priority and should be mitigated as soon as possible.

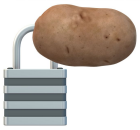
Plaintext password storage and **password reuse** were also found. These findings are medium priority risks. The Company should develop a timeline to remediate or accept the risk on a case by case basis.

Finally, Starch Consulting found **active legacy devices** and **active retired user accounts** available on the infrastructure. These findings are low priority risks. The Company may decide to accept these risks or remediate.

Topology

Starch Consulting was able to generate the following network topology during the Engagement. Any unknown devices should be investigated as soon as possible.



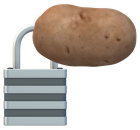


Engagement Timeline (April 6-16, 2020)

- April 7
    - Accessed 192.168.110.60(webmin) using default credentials
    - Discovered the existence of the internal network
    - Found ssh private keys
    - Gained access to all the hosts on the 192.168.110.0/24 subnet
    - Found credentials to VNC running on 192.168.110.14
        - Two Accounts:
            - silkroad
            - 192.168.110.1
- April 8
    - Cracked password for sysadminmike (allowed for ssh access to external network)
    - Enumerated internal network further (not yet accessible)
    - Found more plaintext passwords
- April 10
    - Accessed the internal network
    - Found access credentials to an old ftp server
    - Gained access as another user
        - Access two domain accounts
- April 11
    - Logged in to Joe's computer with Josh’s creds
- April 12
    - Found APT activity (reported to Joe)
- April 16(Last day)
    - Found/accessed the DC
    - Got into the database and found sensitive information
    - Accessed all machines on the internal network with varying levels of privilege.

Risk Level Methodology

Once the technical risks have been identified, they are categorized based on severity based on their Common Vulnerability Scoring System (CVSS) score. This is determined by likelihood and impact to business operations.



The risk value represents the danger that the technical risk poses to The Company's infrastructure and is calculated using the table below.

Risk Level Methodology	Impact			
Likelihood		Low	Medium	High
	Low	Low	Low	Low
	Medium	Low	Medium	Medium
	High	low	Medium	High

Table 1: Risk Level Matrix

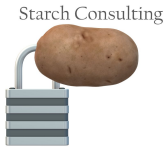
The risk rating helps drive the mitigation planning based on the following guiding principles:

- High: Mitigation should be scheduled as soon as possible. CVSS score of 7.0-10.0
- Medium: The Company should develop a timeline to remediate or accept the risk on a case by case basis. CVSS score of 4.0-6.9
- Low: The Company may decide to accept the risk or remediate. CVSS score of 0.0-3.9

Recommended Mitigation Plan

The company should plan mitigations based on the following parameters

1. **Risk Level** - High risk level vulnerabilities should be addressed first, with Medium, and Low risk items taking a lower priority
2. **Time to mitigate** - Mitigations taking the shortest amount of time should be dealt with first, with longer time items taking a lower priority.



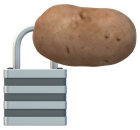
Technical Risks

Risk	Likelihood	Impact	Priority
Default Credentials	High	High	High
Compromised Client Information	High	High	High
Plaintext Password Storage	Medium	High	Medium
Password Reuse	High	Medium	Medium
Active Legacy Device	High	Low	Low
Active Retired User Accounts	High	Low	Low

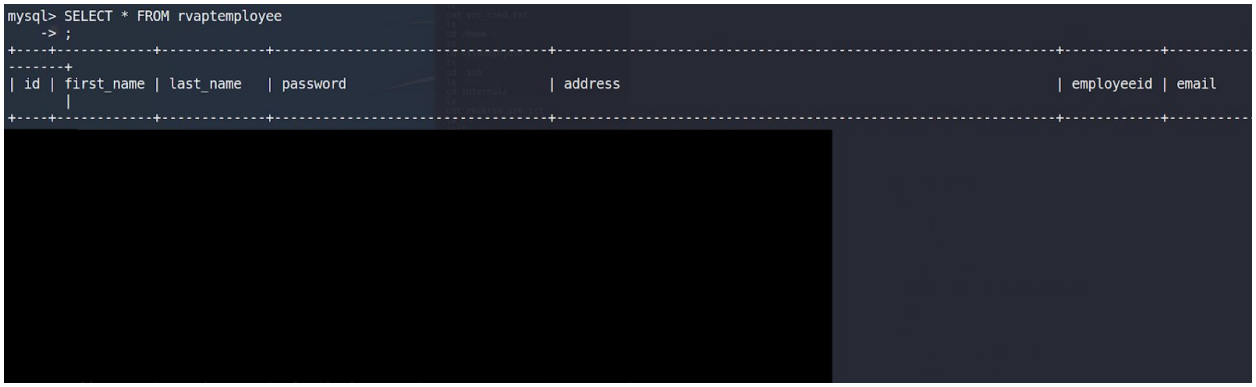
Table 2 - Technical Risks

High Priority Risks

- Default Credentials (CVSS 9.0)
  - **Description**: One of your critical servers(webmin) had default creds. This lead to Starch Consulting initial access to your network
  - **Likelihood** (High) - With default password, an attacker can login and run system commands right from the web server.
  - **Impact** (High): This could be the entry for the attackers when they need to get into your system. They could establish persistence by storing their SSH keys onto the server.
  - **Evidence**: Logging in with webmin's default password will allow anyone to log in to the web server.
  - **Mitigation:** Changing the default cred to a more secure and complex password.



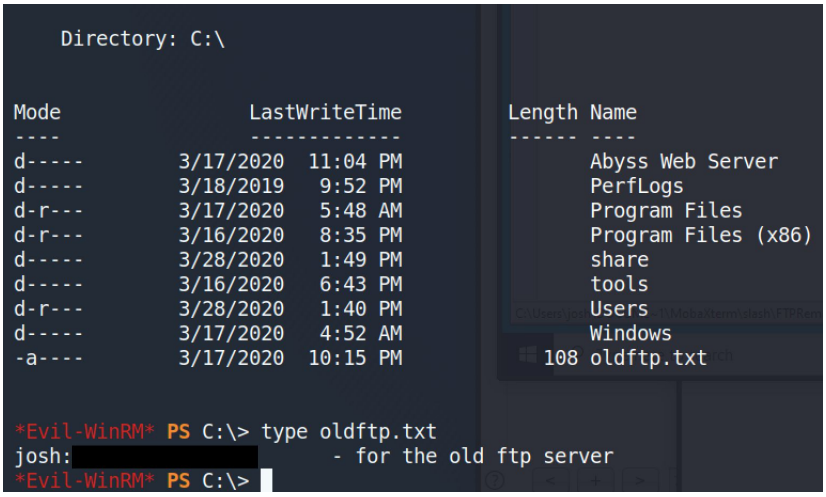
- Compromised Client Information (CVSS 10.0)
    - **Description**: Starch Consulting gained access to the SQL core hosting database through a weak password for the user root. This allows an attacker to login to the core database allowing them to view and modify Rvapthositng employees and clients.
    - **Likelihood** (High) - With reusable password, an attacker can guess which password to use to access the database
    - **Impact** (High): The ability to change the database is very critical to Rvapthosting because an attacker can sell client's data.
    - **Evidence**:

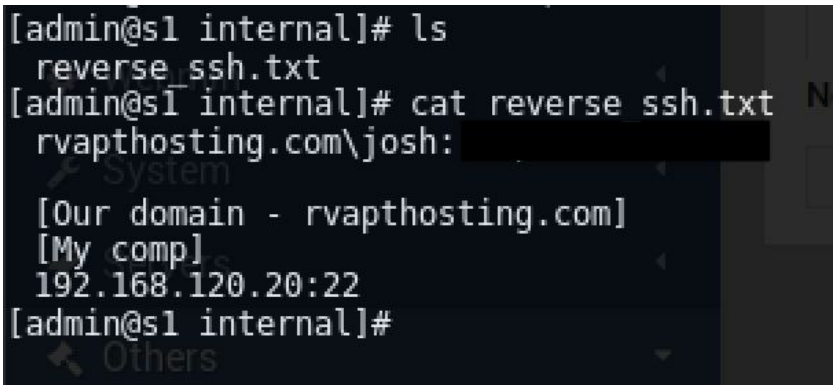


    - **Mitigation**: Use a more complex password for the database and not stored in easy to find location like the Desktop

Medium Priority Risks

- Plaintext Password Storage (CVSS 5.0)
  - **Description** - storage of user accounts and passwords in plaintext were found throughout the network.
  - **Likelihood** (Medium) - basic enumeration and the name of plaintext leads us to find additional credentials.
  - **Impact** (High) - the attacker will be able to expand his insider network and that might lead to additional damage.
  - **Evidence** - going to the C drive we find a plaintext that has credential for oldftp



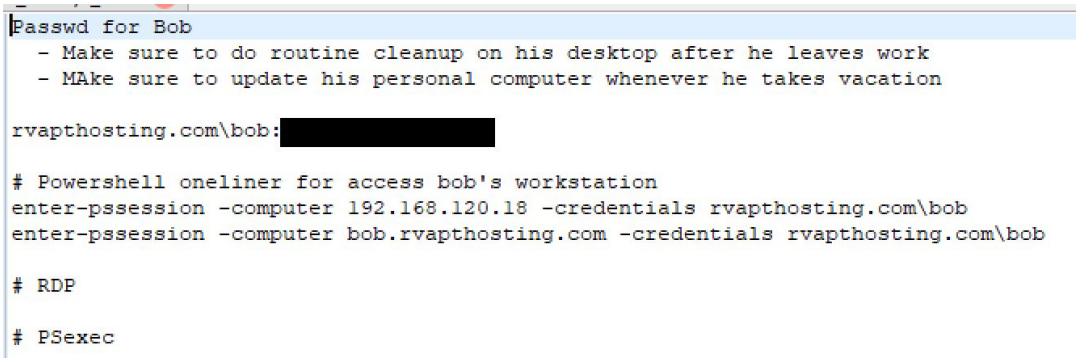


  - **Mitigation** - the ideal solution is to encrypt or delete any plaintext that contains critical information to eliminate the risk associated with plaintext password storage.

- Password Reuse (CVSS 4.5)
    - **Description** - Starch Consulting found out that some of RVAPTHosting employees reuse their passwords either on other machines or with other services.
    - **Likelihood** (Medium) - the attacker will try to use any password that he found on different users/services since password reuse is common practice that people should not do.
    - **Impact** (High) - it makes it very easy for the attacker to gain access to privileged users.
    - **Evidence** - password reuse makes starch consulting to have access to mysql service using josh password as well as getting access to all josh accounts in the internal network.
    - **Mitigation** - force the employees to use a unique password for different machines and different services

Low Priority Risks

- Active Legacy Device (CVSS 2.0)
    - **Description** - A legacy device from was found to still be active on the internal network. Documentation hinting to the requested deletion of this device was also found
    - **Likelihood** (Medium) - A simple scan of the internal network allowed us to pinpoint the location device. Through slightly more enumeration we were able to determine that this device was running legacy software and should have been deleted.
    - **Impact** (Low) - The information found on the FTP server was not up to date with the current configuration of the network, and therefore not applicable for an attacker to use
    - **Evidence** - This file was found on the FTP server containing information about a previous employee



```
Passwd for Bob
  - Make sure to do routine cleanup on his desktop after he leaves work
  - MAke sure to update his personal computer whenever he takes vacation

rvapthosting.com\bob:[redacted]

# Powershell oneliner for access bob's workstation
enter-pssession -computer 192.168.120.18 -credentials rvapthosting.com\bob
enter-pssession -computer bob.rvapthosting.com -credentials rvapthosting.com\bob

# RDP

# PSexec
```

- **Mitigation** - Remove the legacy server from the network if possible. If not, ensure it has the latest security updates released from the manufacturer to ensure the minimum amount of risk associated with that device.

- Active Retired User Accounts (CVSS 3.0)
  - **Description** - Our testing revealed active user accounts that looked to be scheduled for deletion, but were never deleted.
  - **Likelihood** (Medium) - The information about these accounts was available only after compromising the system on which they resided, meaning an attacker would need access to a system in order to determine that there was an old user account active on it.
  - **Impact** (Low) - The old accounts had very low levels of privileges on their respective systems, so even if compromised they would have limited access to resources that could prove fatal for the network.
  - **Evidence** - After closely examining each user account on the Domain Controller (192.168.120.1) a comment was found on an old user account expressing intent to get the old account removed

“Comment FFS this dude has been retired for 8 years. JOSH, GET RID OF HIM. -bob”

  - **Mitigation** - Old user accounts should be, at minimum, deactivated if not deleted. This eliminates any kind of risk associated with disgruntled employees or outdated credentials.