Ex090 - PowerUp

Simon Tobon

2021-07-08

Contents

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

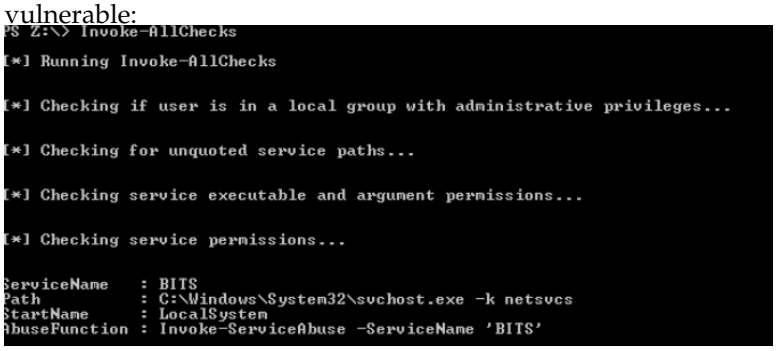
To begin, port forwarding for MS RDP had to be set up. This was done by opening a Web Browser on Kali and navigating to **https://172.30.0.3:443**. This was completed by following the process from the last Exercise, first log in to pfsense with the default credentials admin/pfsense. Then set up a new 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:**

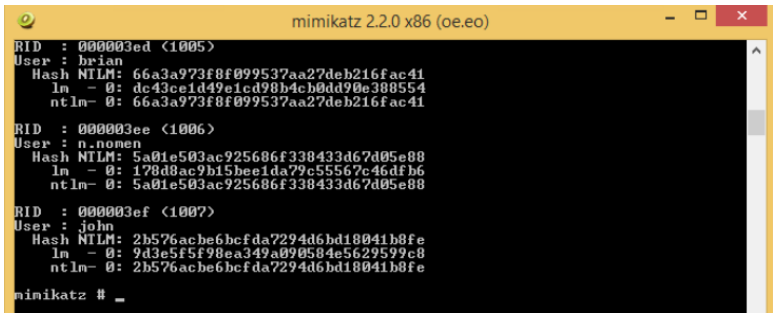
TSCLIENT\win32. This mounts the shared drive to the windows machine.

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:



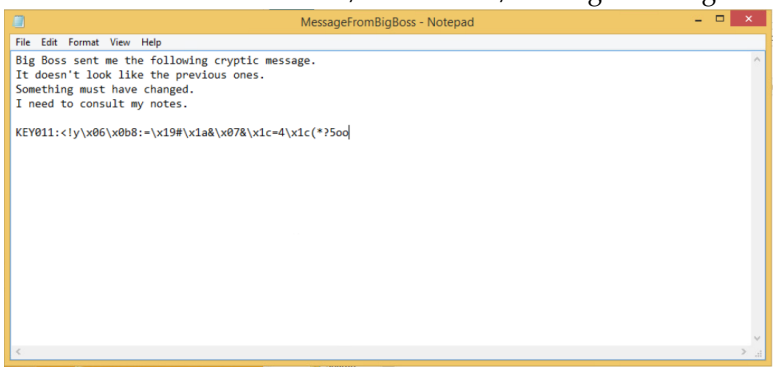
We can then exploit this service by running: **Invoke-ServiceAbuse -ServiceName 'BITS'**. This creates an Administrative User with username **john** and password **Password123!**

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**

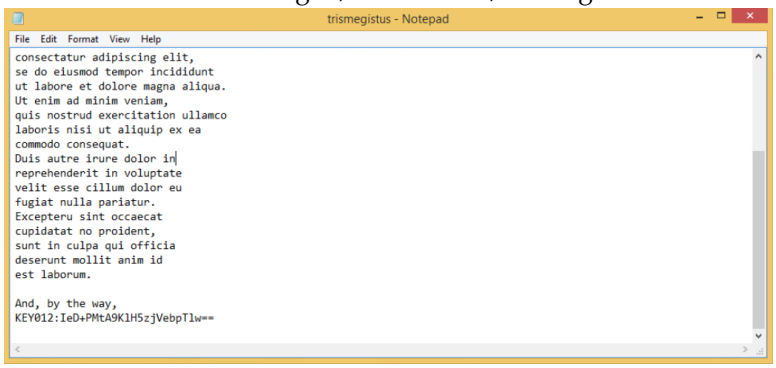


While logged into the HERD with an Administrative user I explored some other user directories and found 3 keys!

- **KEY010:gM12BGOIHNcPVlh1xAiqKA==** was found in brian/Documents/Recipe.txt
- KEY011 was found in Sharon/Documents/MessageFromBigBoss.txt



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



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: