Ex080 Report

Benjamin Ruddy

2022-10-30

Contents

Technical Report

Introduction

Finding: *Vulnerable permissions on a service for a non-administrator user can allow for the creation of an adminsitrator account*

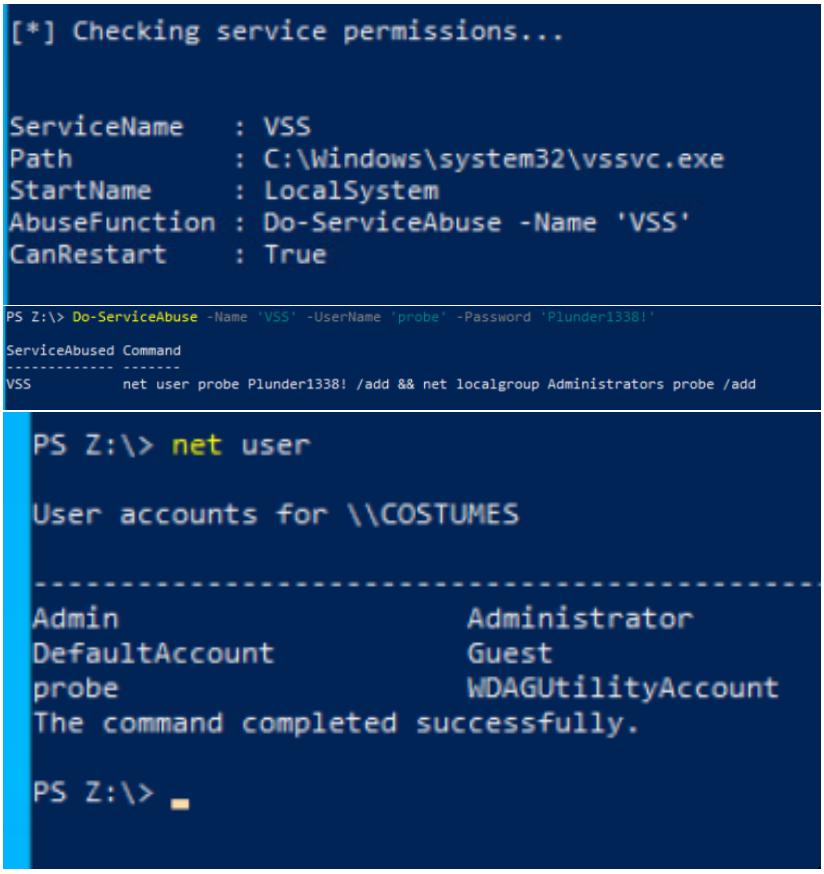
Severity Rating: 8.4

CVSS Base Severity Rating: 7.8 AV:L AC:L PR:L UI:N S:C C:H I:H A:N

Vulnerability Description

On costumes.artstailor.com, non-administrative user 's.wilkins' has permisson to modify the Windows service 'vssvs.exe' such that commands can be executed with SYSTEM-level permissions, meaning an administrator account can be created by a non-administrator user.

Confirmation method



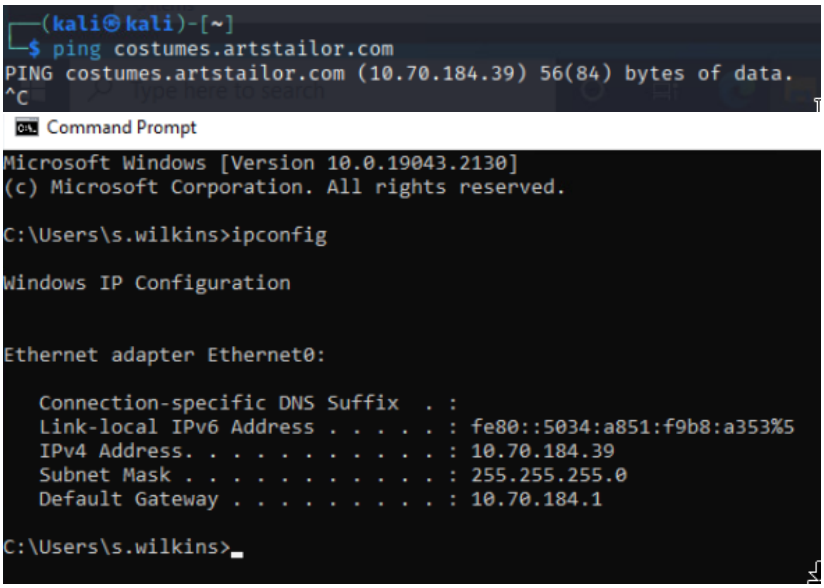
Mitigation or Resolution Strategy

Remove the modification rights that user 's.wilkins' has on this critical Windows program.

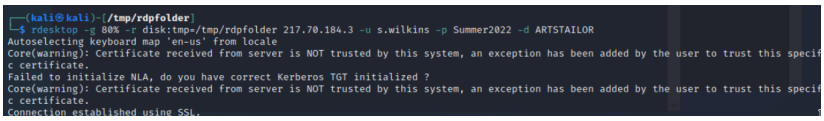
Attack Narrative

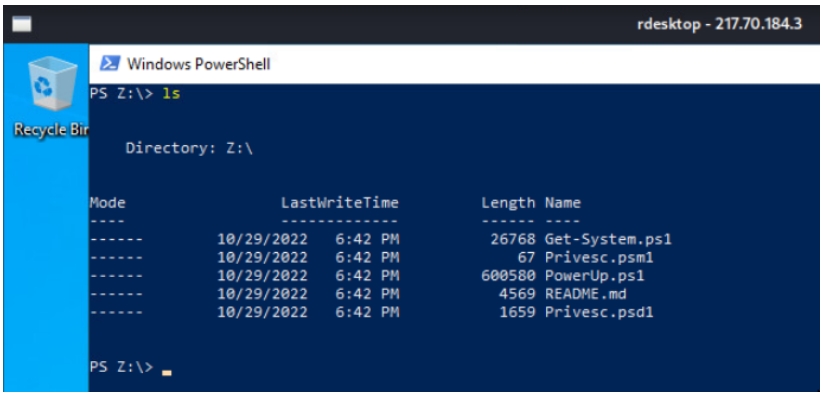
RDPing into costumes.artstailor.com

Using the same port forwarding technique detailed in **Exercise 0x080**, we start by using Windows RDP to gain access to `costumes.artstailor.com`. The following screenshots demonstrate that we have logged in to the correct host:



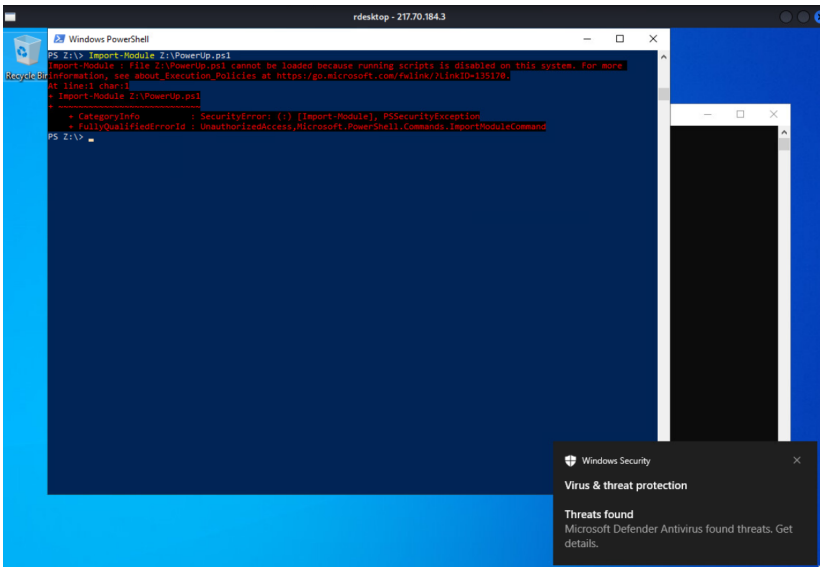
Here, we have imported the PowerUp modules by copying over its respective .ps1 files into a directory in `/tmp`, and then mounted it as a fileshare on the victim host with the following `rdesktop` command, followed by mapping it to the `Z:` drive within Windows:





PowerUp & PowerDown

When trying to run PowerUp, however, we run into a problem related to Windows Defender antivirus detection:

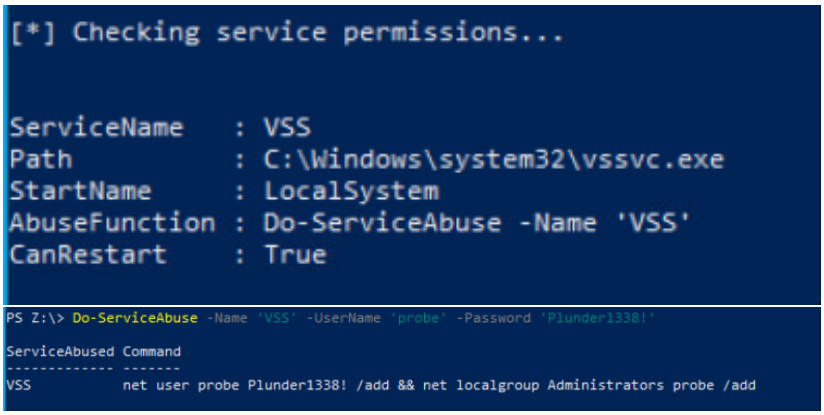


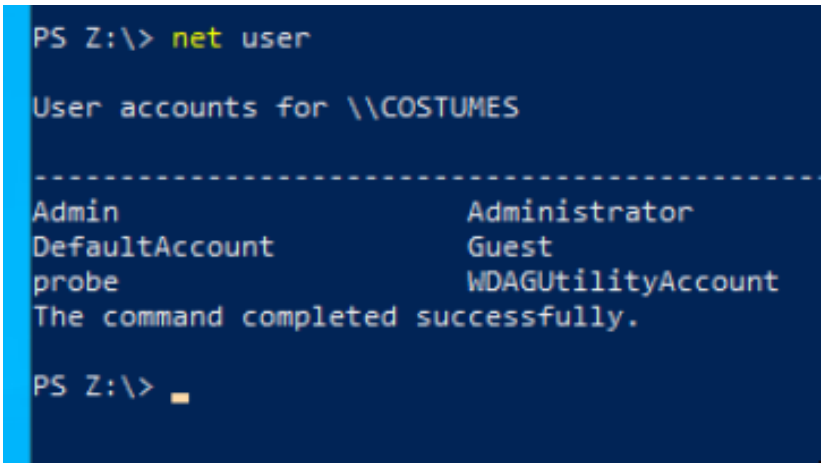
As such, we use a modified version of PowerUp called `PowerDown` which edits the source code of PowerUp and changes various aspects of it, such as removing comments, changing function names, and adding custom string encodings to evade potential forms of signature checking used by the Windows Defender anti-malware.

This indeed ended up bypassing the antimalware checks, subsequently letting us run the `AllChecks` module as seen in the following screen captures:

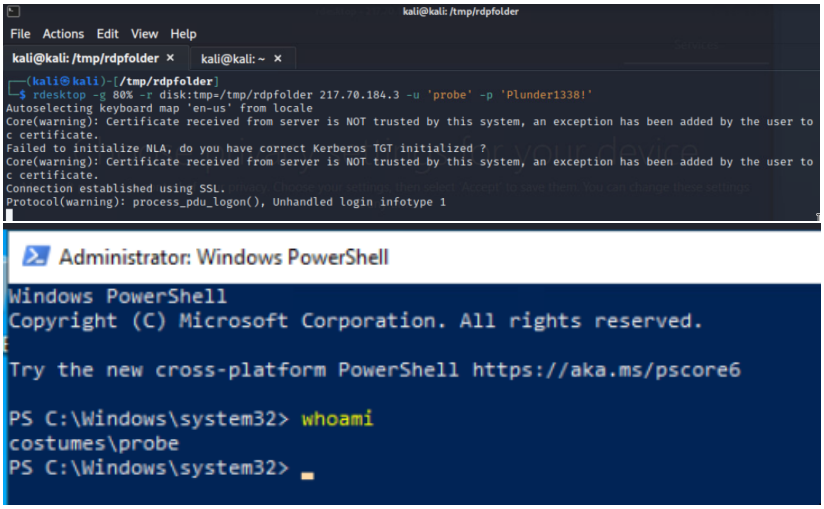
Vulnerable service permissions exploitation

During the PowerDown module execution, vulnerable service permissions for our current user (`s.wilkins`) were found on the Volume Shadow Copy (VSS) service, allowing us to create our own custom Administrator user on the machine. The following screenshots showcase the commands used to add a new administrative user, 'probe', with password 'Plunder1338!':





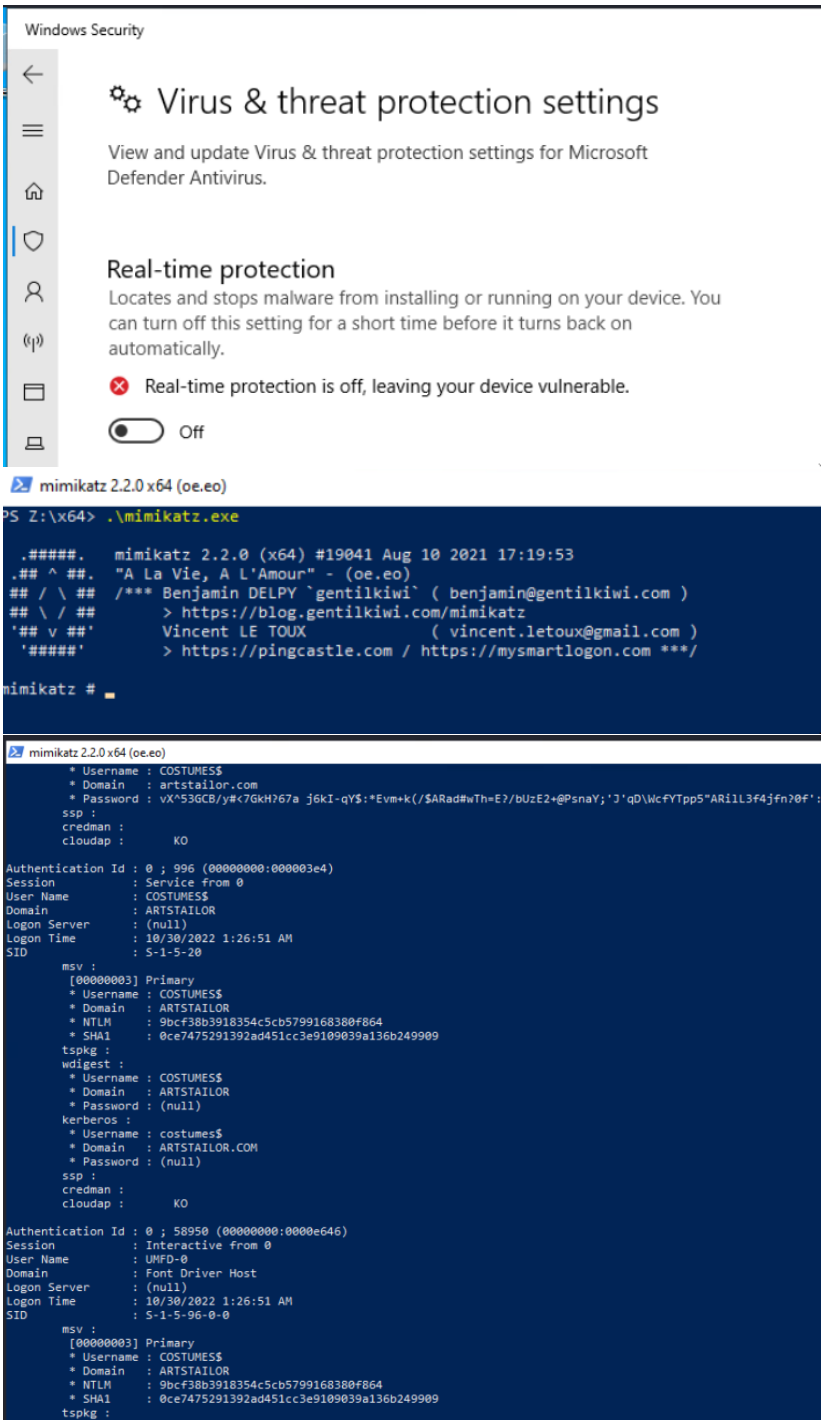
We subsequently logged into our new user with rdesktop, which we also confirmed to have administrator privileges (notice PowerShell is being ran as Administrator):



Mimikatz

Now that we are logged in as an administrator, we can further our post-exploitation by running mimikatz to obtain other possible credentials on the machine for local administrators, which could potentially be reused by other network accounts.

We can take advantage of our administrator privileges to disable Windows Defender entirely as well.

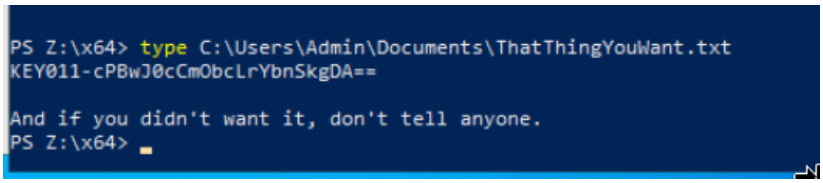


As seen in the above screenshot where we ran the `sekurlsa::logonPasswords`

module, various credentials/hashes were obtained for different users on the machine. This output, along with the output of `lsadump:sam` was stored on the remote plunder.pr0b3 server for future use.

Key found

Taking further advantage of our administrator permissions, we were additionally able to find KEY011 in this machine by looking around in the Admin user's files:



MITRE ATT&CK Framework TTPs

TA0004: Privilege Escalation
- **T1059:** Command and Scripting Interpreter
  - **.001:** PowerShell

TA0006: Credential Access
- **T1555:** Credentials from Password Stores
  - **.004:** Credential ACcess

TA0003: Persistence
- **T1574:** Hijack Execution Flow
  - **.010:** Services File Permission Weakness