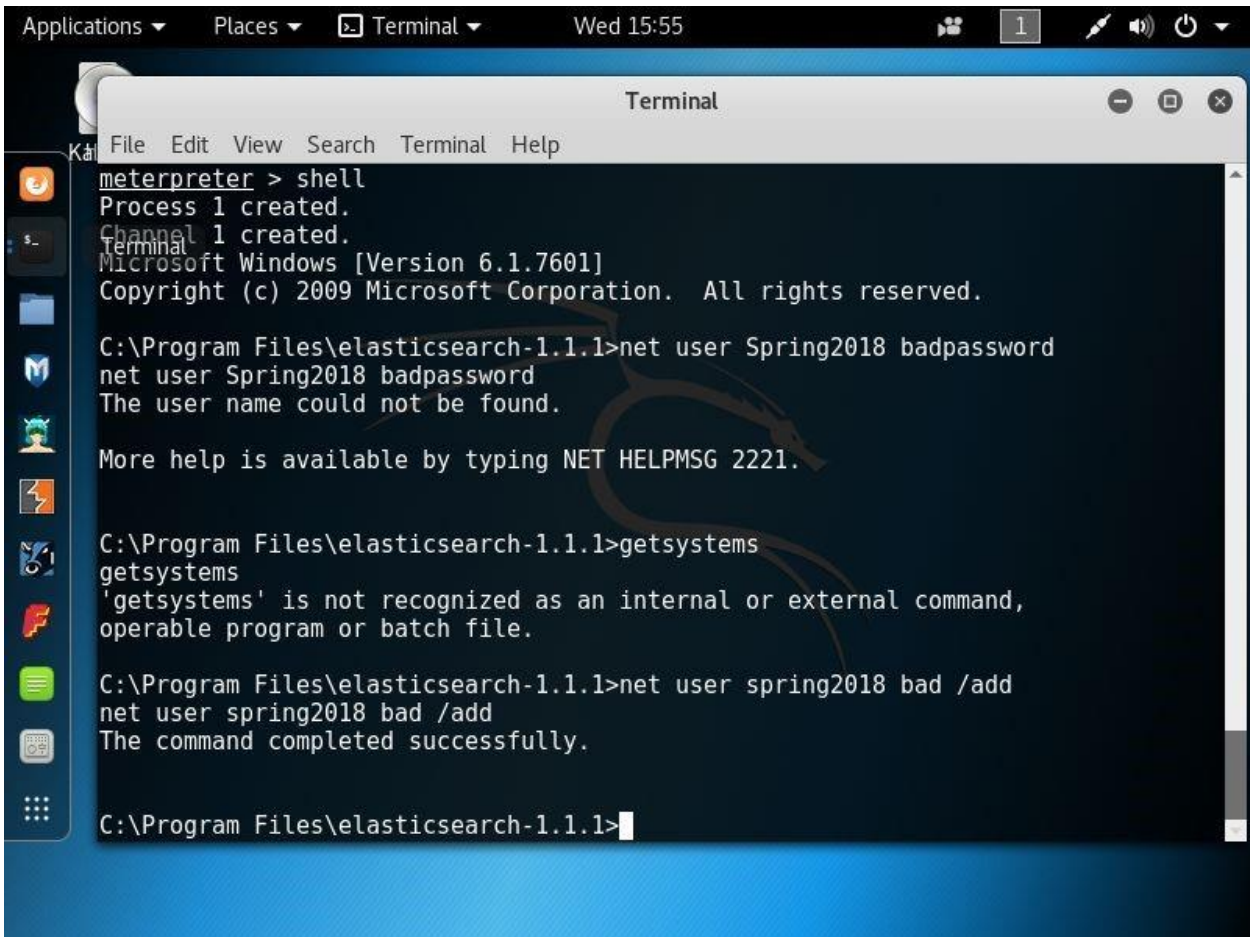


### Assignment #6

- Use Metasploit to get a shell on your Metasploitable3 VM using a different exploit than the MS17-010 exploit like we did in class.
  - (Review your Nessus scan from last week and <https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities> (Links to an external site.) for some ideas.)
- Add a user named 'spring2018' to that system
  - (hint: use incognito)
- Provide me a screen shot of your commands in Metasploit to accomplish this and a screen shot of your Metasploitable3 VM showing the newly added user
  - (hint: Use the Computer Management tool to show a list of users)

#### Deliverables:

1. A screenshot of the commands in Metasploit that you ran
2. A screenshot of the Computer Management tool showing the "spring2018" user that you added via Metasploit on your Metasploitable3 VM.



The screenshot shows a Windows desktop environment. At the top, the taskbar includes 'Applications', 'Places', and 'Terminal' menus, along with a clock showing 'Wed 15:55'. A 'Terminal' window is open, displaying the following text:

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

C:\Program Files\elasticsearch-1.1.1>net user Spring2018 badpassword
net user Spring2018 badpassword
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

C:\Program Files\elasticsearch-1.1.1>getsystems
getsystems
'getsystems' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files\elasticsearch-1.1.1>net user spring2018 bad /add
net user spring2018 bad /add
The command completed successfully.

C:\Program Files\elasticsearch-1.1.1>
```

