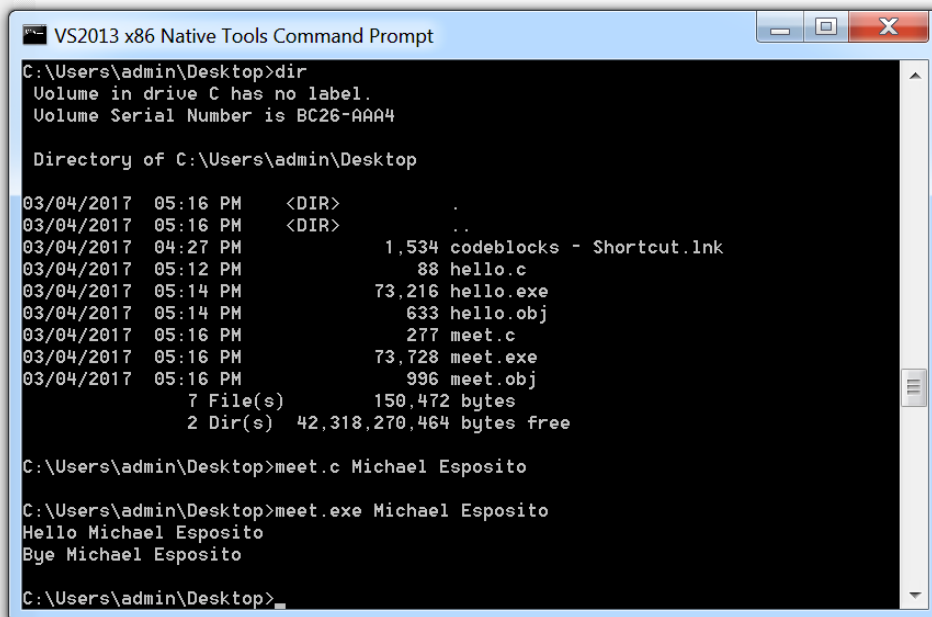


## Lab 12

### 1. Meet.exe successfully compiling

```
1 //meet.c
2 #include <stdio.h>
3 greeting(char *temp1, char *temp2) {
4     char name[400];
5     strcpy(name, temp2);
6     printf("Hello %s %s\n", temp1, name);
7 }
8
9 main(int argc, char *argv[]){
10     greeting(argv[1], argv[2]);
11     printf("Bye %s %s\n", argv[1], argv[2]);
12 }
13
```



```
VS2013 x86 Native Tools Command Prompt
C:\Users\admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is BC26-AAAA

Directory of C:\Users\admin\Desktop

03/04/2017  05:16 PM    <DIR>          .
03/04/2017  05:16 PM    <DIR>          ..
03/04/2017  04:27 PM             1,534 codeblocks - Shortcut.lnk
03/04/2017  05:12 PM              88 hello.c
03/04/2017  05:14 PM          73,216 hello.exe
03/04/2017  05:14 PM           633 hello.obj
03/04/2017  05:16 PM           277 meet.c
03/04/2017  05:16 PM          73,728 meet.exe
03/04/2017  05:16 PM           996 meet.obj
               7 File(s)      150,472 bytes
               2 Dir(s)  42,318,270,464 bytes free

C:\Users\admin\Desktop>meet.c Michael Esposito

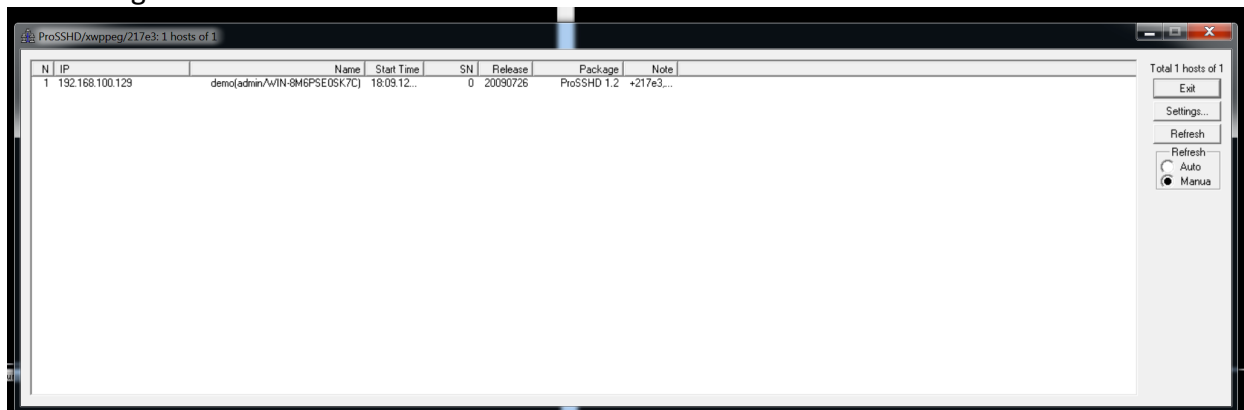
C:\Users\admin\Desktop>meet.exe Michael Esposito
Hello Michael Esposito
Bye Michael Esposito

C:\Users\admin\Desktop>
```

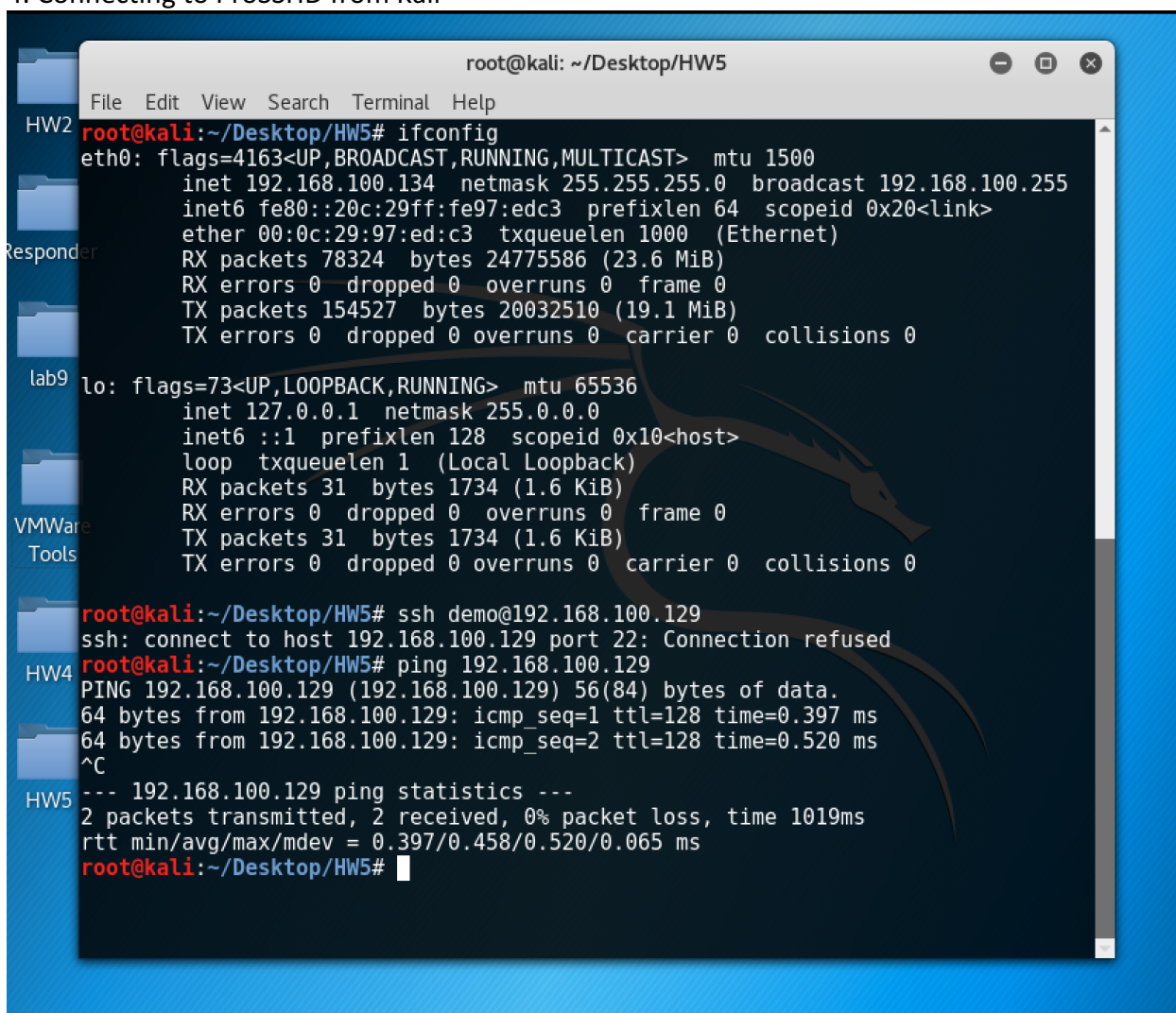
### 2. Command to compile without stack canary

```
c1 meet.c /DEBUG /GS
```

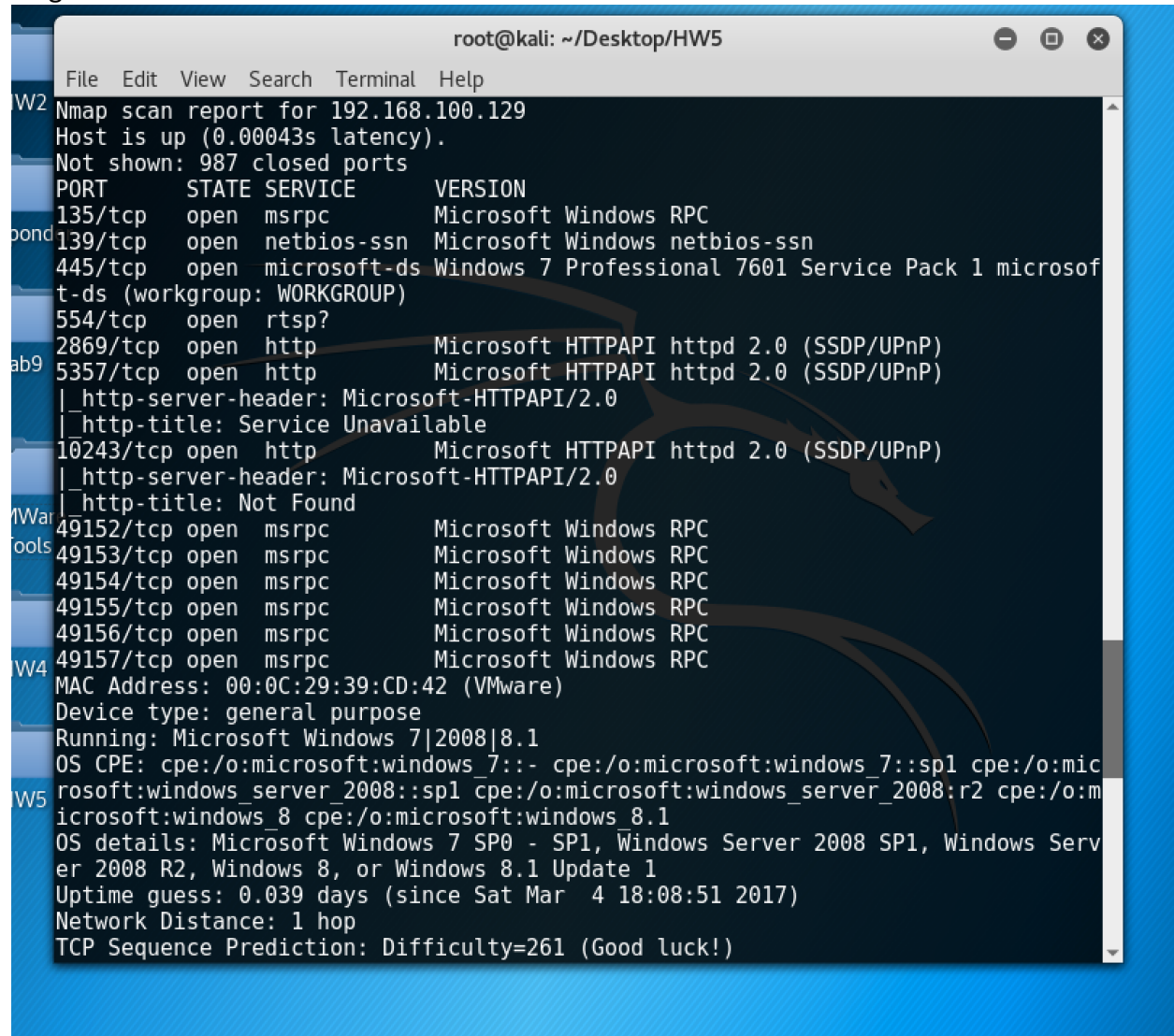
### 3. Running ProSSHD on Windows



### 4. Connecting to ProSSHD from Kali



5. Cannot connect to SSH server on Windows, is anything on port 22 running? Using nmap to diagnose



```
root@kali: ~/Desktop/HW5
File Edit View Search Terminal Help
Nmap scan report for 192.168.100.129
Host is up (0.00043s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Service Unavailable
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 00:0C:29:39:CD:42 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.039 days (since Sat Mar 4 18:08:51 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
```

6. I am unable to connect to ProSSHd server even though it looks like it is running on Windows. Not sure what to do from here.