Lab 12

1. Meet.exe successfully compiling

```
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
                                                                                _ D X
     VS2013 x86 Native Tools Command Prompt
       :\Users\admin\Desktop>dir
      Uolume in drive C has no label.
Uolume Serial Number is BC26-AAA4
      Directory of C:\Users\admin\Desktop
     03/04/2017 05:16 PM
                                <DIR>
     03/04/2017 05:16 PM
03/04/2017 04:27 PM
03/04/2017 05:12 PM
                                          1,534 codeblocks - Shortcut.lnk
                                             88 hello.c
                                         73,216 hello.exe
633 hello.obj
     03/04/2017 05:14 PM
     03/04/2017 05:14 PM
     03/04/2017 05:16 PM
03/04/2017 05:16 PM
                                         277 meet.c
73,728 meet.exe
996 meet.obj
     03/04/2017 05:16 PM
                                                                                                Ξ
                                         150,472 bytes
                      7 File(s)
                      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

cl meet.c /DEBUG /GS

3. Running ProSSHD on Windows



4. Connecting to ProSSHD from Kali

```
root@kali: ~/Desktop/HW5
                                                                                                                                  File Edit View Search Terminal Help
  HW2
         root@kali:~/Desktop/HW5# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.134 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe97:edc3 prefixlen 64 scopeid 0x20<link>
                      ether 00:0c:29:97:ed:c3 txqueuelen 1000 (Ethernet) RX packets 78324 bytes 24775586 (23.6 MiB)
Respond
                      RX errors 0 dropped 0 overruns 0 frame 0
                       TX packets 154527 bytes 20032510 (19.1 MiB)
                      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  lab9 lo: flags=73<UP,L00PBACK,RUNNING> mtu 65536
                       inet 127.0.0.1 netmask 255.0.0.0
                       inet6 ::1 prefixlen 128 scopeid 0x10<host>
                      loop txqueuelen 1 (Local Loopback)
RX packets 31 bytes 1734 (1.6 KiB)
                       RX errors 0 dropped 0 overruns 0 frame 0
 VMWar
                      TX packets 31 bytes 1734 (1.6 KiB)
  Tools
                       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                  kali:~/Desktop/HW5# ssh demo@192.168.100.129
 HW4

HW4

root@kali:~/besktop/HW5# ssh demogl92.168.100.129

ssh: connect to host 192.168.100.129 port 22: Connection refused

root@kali:~/besktop/HW5# ping 192.168.100.129

PING 192.168.100.129 (192.168.100.129) 56(84) bytes of data.
64 bytes from 192.168.100.129: icmp_seq=1 ttl=128 time=0.397 ms
64 bytes from 192.168.100.129: icmp_seq=2 ttl=128 time=0.520 ms
 HW5
--- 192.168.100.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.397/0.458/0.520/0.065 ms
          root@kali:~/Desktop/HW5#
```

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

```
root@kali: ~/Desktop/HW5
                                                                              8
    File Edit View Search Terminal Help
W2 Nmap scan report for 192.168.100.129
   Host is up (0.00043s latency).
   Not shown: 987 closed ports
   P0RT
              STATE SERVICE
                                 VERSION
             open msrpc
   135/tcp
                                 Microsoft Windows RPC
pond 139/tcp
             open netbios-ssn Microsoft Windows netbios-ssn
             open microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsof
   445/tcp
   t-ds (workgroup: WORKGROUP)
             open rtsp?
   554/tcp
                                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
   2869/tcp
             open http
ab9 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
ools 49153/tcp open
                   msrpc
                                 Microsoft Windows RPC
                                 Microsoft Windows RPC
   49154/tcp open
                   msrpc
   49155/tcp open
                                 Microsoft Windows RPC
                   msrpc
                                 Microsoft Windows RPC
   49156/tcp open
                   msrpc
W4 49157/tcp open msrpc Microsoft Mac Address: 00:0C:29:39:CD:42 (VMware)
                                 Microsoft Windows RPC
   Device type: general purpose
   Running: Microsoft Windows 7|2008|8.1
   OS CPE: cpe:/o:microsoft:windows 7::- cpe:/o:microsoft:windows 7::spl cpe:/o:mic
W5 rosoft:windows_server_2008::spl cpe:/o:microsoft:windows server 2008:r2 cpe:/o:m
   icrosoft:windows 8 cpe:/o:microsoft:windows 8.1
   OS details: Microsoft Windows 7 SPO - SP1, Windows Server 2008 SP1, Windows Serv
   er 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.