

Buy a [domain](#) with 35 % OFF ! Today only ! for JUST 6 \$ [Get it now !](#)

# HackToHell



[Home](#)   [HTH - Toolbar](#)   [Search](#)   [Contact us](#)   [About](#)

## Hack your friend by using BackTrack 5 | Backtrack 5 tutorial

BackTrack 4 is an penetration testing tool that is run as an live CD , it is an modded form of Linx(Ubuntu) that can be used for hacking.In this tutorial I will show you how to generate payloads in it.

**WARNING !!!!!!!!!!!!!!! THIS HAS BEEN DISCUSSED TO TELL YOU ABOUT THE WAYS IN WHICH YOUR [COMPUTER](#) MIGHT BE EXPLIOTED !!!! DO NOT USE THIS TO HACK ANYONE !!!! [READ MORE HERE](#) !!!! DO NOT USE THIS ON ANYONE ELSE OTHER THAN YOURSELF !**

First get backtrack at [and](#) set it up as per my [guide](#) here.

In this tutorial we will be using a useful tool on Backtrack 4 to create a payload which we will then send a slave, the payload created is in exe, once the slave is Social [Engineered](#) into running the payload, A meterpreter session will appear to us. We will set it up with a listener on a port, meaning we will have a shell prompt open, waiting for a connection from the slave, once this occurs we have a session, and entry to the victims machine.

Start by opening Bt 4 etc, then scroll to Backtrack, Penetration, Fast-Track, Fast-Track interactive, this will open a prompt like below.

[Recent](#)   [Tags](#)   [Blog Archives](#)

[Amazon.com](#)



[Kindle Fire, Full Color 7" Multi-touch Display, Wi-Fi Amazon Digital Ser...](#)  
New \$199.00  
Best \$199.00

[Marware C.E.O. Hybrid for Kindle Fire Cover, Black](#)  
Marware (Kindle Ac...  
New \$44.99  
Best \$44.99

[Kindle, Wi-Fi, 6" E Ink Display - includes Special Off...](#)  
Amazon Digital Ser...  
New \$79.00  
Best \$79.00

[Kindle Fire MicroShell Folio Cover by Marware, Grey](#)  
Marware (Kindle Ac...  
New \$39.99  
Best \$39.99

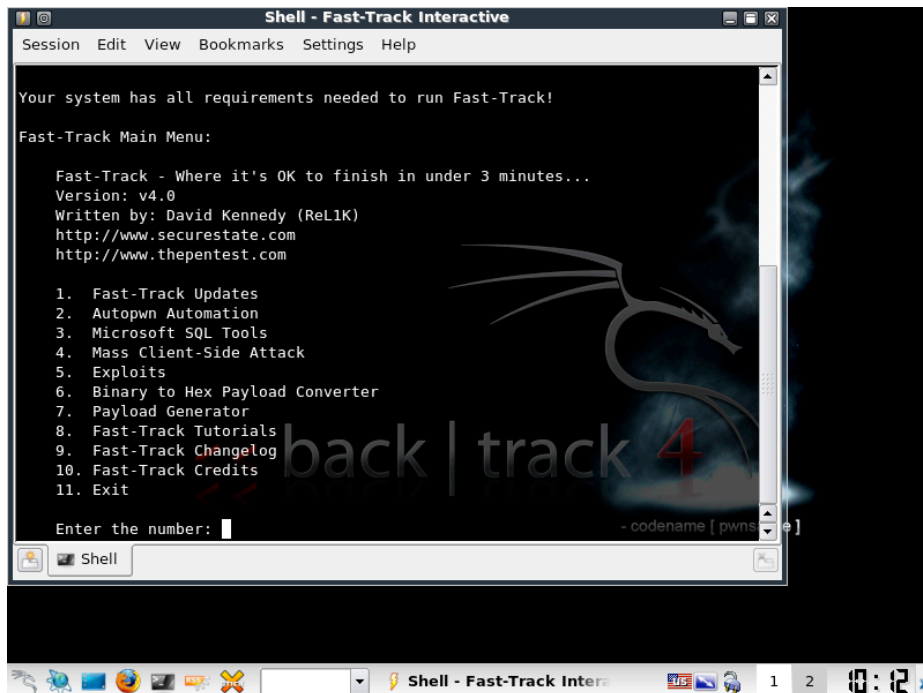
[HDMI Cable 2M](#)  
Ereplacements  
New \$1.69  
Best \$0.01

[Privacy Information](#)

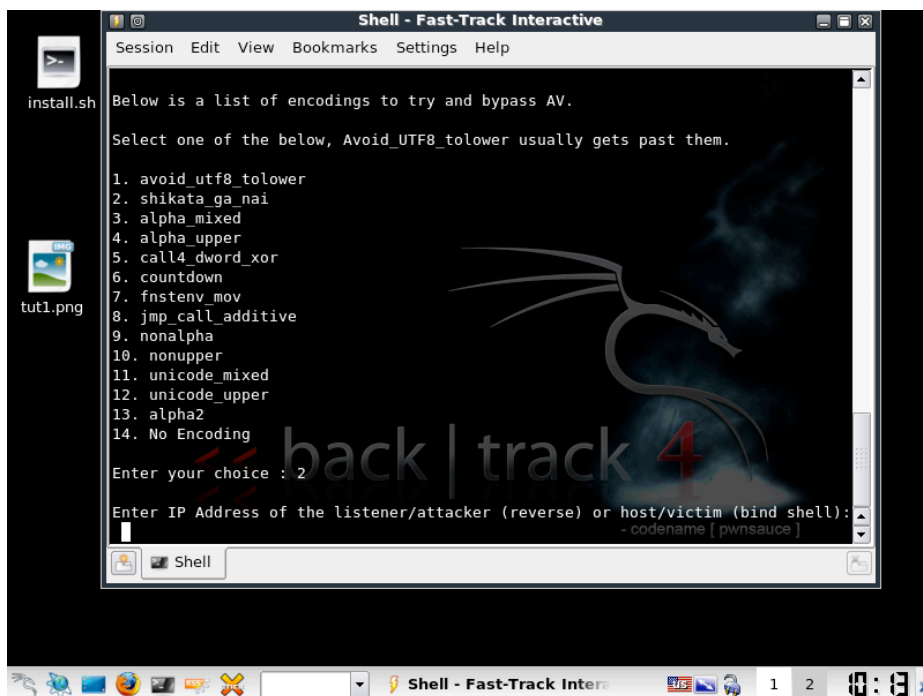
### RECENT POSTS

[HackToHell](#)

[Stuff you must do after moving to a](#)



Choose option 7, it will then ask what exploit you want to use, choose exploit 2.



It will then ask you for an Ip [address](#), you can either enter your own, or the victims, its easier to enter our own (the listener). To obtain your IP on Backtrack 4, open a shall and type ifconfig, your IP appears after inet addr, like below.

### new domain in blogger

You must do a lot of things so that google recognizes your new domain. Step 1: Create a new site...

### I have moved to a custom domain

#### hacktohell.org !

Well i bought anew domain and I have moved to it ! I have bought it from namecheap The name...

### Amazon rocks the Tablet PC world with a new Array of Kindle !

Amazon decided to go ballistic into the Table PC [world](#) with the launch of [Kindle](#) Fire (it's damn hot ).Amazon...

### Control Grooveshark from any tab with Grooveshark Remote | FireFox | Andriod

Grooveshark gets lost in the millions of tab open ? You are not alone fortunately an addon fixes that !...

### Google+ now allows circles to be shared !

Want to share your group of circles to your friends ? Google Plus now allows this too Google+ excels...

Subscribe to this Feed



Powered by Blogger.

Subscribe to our RSS Feed

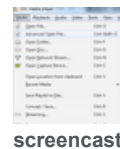
Follow Us on Twitter

Be Our Fan on Facebook

### GET UPDATES VIA EMAIL !

Email address... Submit

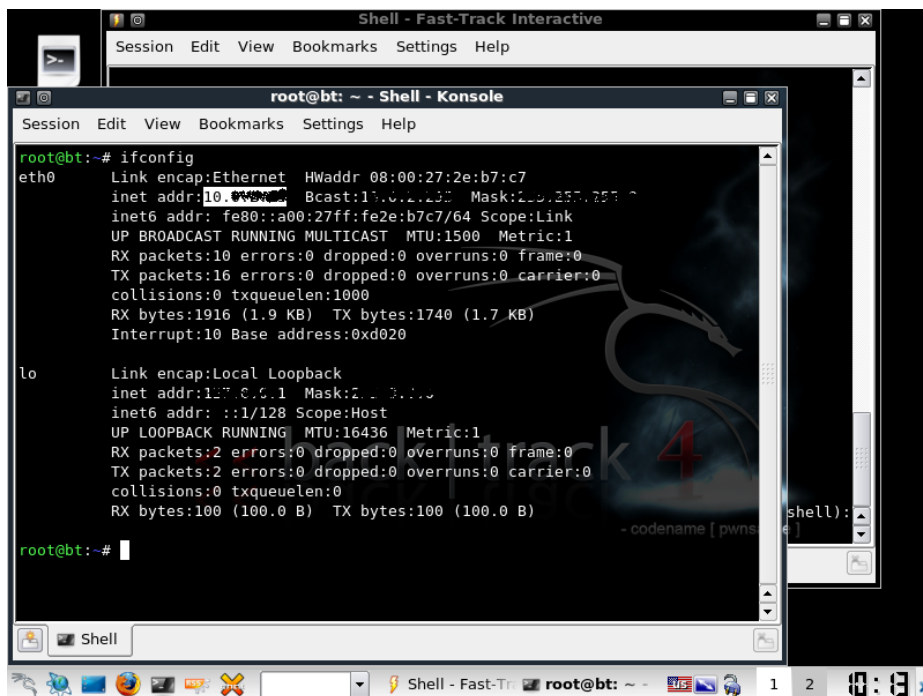
### RELATED POSTS



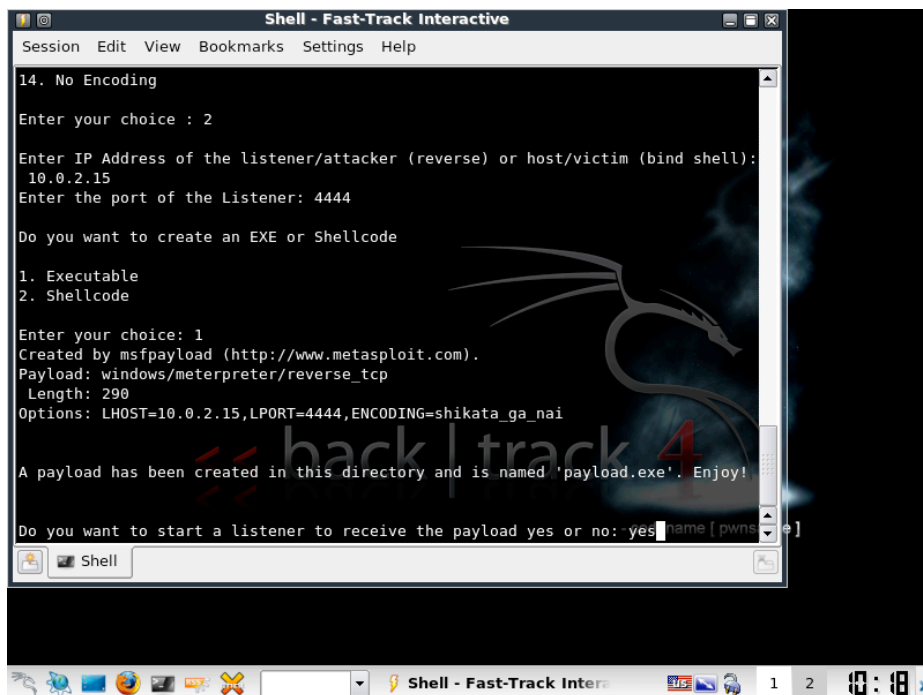
Using VLC Media Player to capture a screencast



Reduce your core temperature instantly on your Asus motherboard using Asus




It will then ask you to choose a port for the listener, choose a random port that isn't in use, for this we will use port 4444, and then choose the payload to be compiled in exe format rather than shell script (text). Also choose yes on starting a listener, this basically means a shell will be opened blank, waiting for the slave to run the exe, once run the connection is made, and the listening shell will then spawn the meterpreter session between your and the victims machine.




At this point, the payload has been created, and the listener has launched, all you have to do now is locate the payload, I would advise you to rename it, Social Engineer the slave into running it, and then check your listening shell for a connection. If successful you will then have a meterpreter session opened and

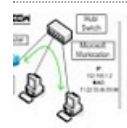
Fan fan xpert !

-  [Using Metasploit to harvest emails of a website](#)

---

-  [How to fix broken images in WMP when automatic update fails](#)

---

-  [Hack A computer over LAN via ARP poisoning using BackTrack | BackTrack 5 Tutorial](#)

@hacktohell · 76 followers

My short bio

FACEBOOK

 **HackToHell** on Facebook

[Like](#)

75 people like HackToHell.

  
Kani

  
Olti

  
Lau

  
Rahul

  
Mohd

  
Jeremy

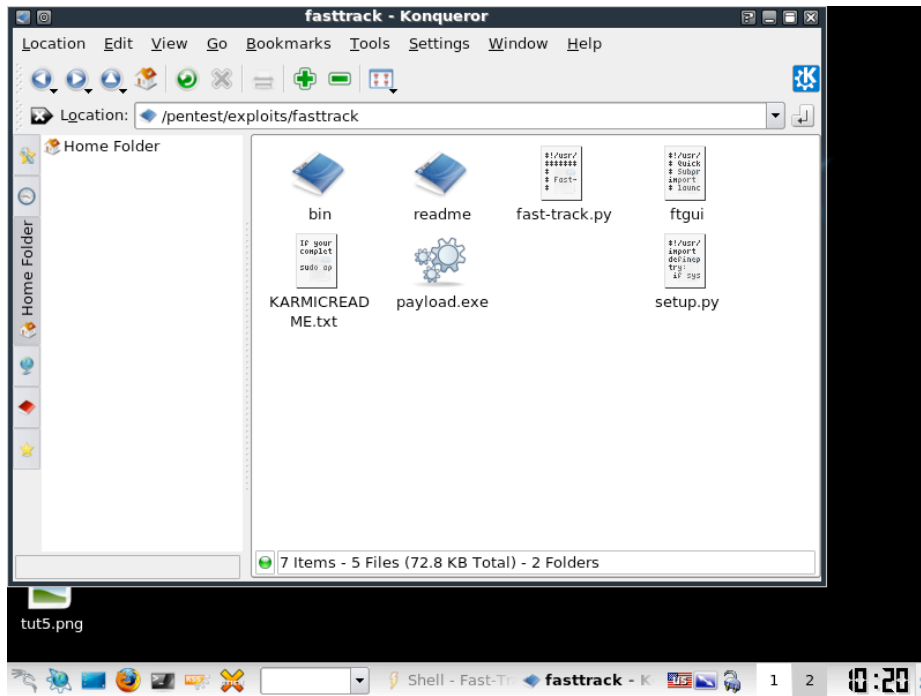
  
Dhanasekar

  
Sidhi

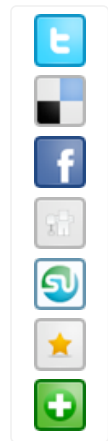
Facebook social plugin

entry to the victims machine.

Below is the [location](#) of the payload you will send.



[The Basics of Hacking and Penetration...](#)  
Patrick Engbreto...  
**Best Price \$17.26**  
or Buy New \$18.23  
[Buy from amazon.com](#)  
Privacy Information



**Related** [A tutorial on hacking your friends over the internet in BackTrack 5](#)

[Hacking WEP Wifi passwords in BT 5](#)

[Hacking webservers using Metasploit](#)

[Posted](#) in: [hack](#)

Like 0

**Ultimate Hacking**

Get hands on Ultimate Hacking at an information security course

[InfoSecInstitute.com](http://InfoSecInstitute.com)

**Vulnerability Scanner**

Integrated vulnerability scanner & penetration testing from SAINT

[www.saintcorporation.com](http://www.saintcorporation.com)

**Track Ip Address**

Download IPAM Whitepaper to Gain Expert Insight on IP Address Mgmt!

[www.BTDiamondIP.com](http://www.BTDiamondIP.com)

**Application Security**

Avoid being hacked! Free White Paper on common attacks

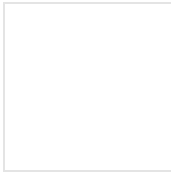
[www.qosoftchoice.com/IBMAppScan](http://www.qosoftchoice.com/IBMAppScan)

You may also like

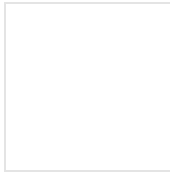
Searching for backtrack 5 tutorials?



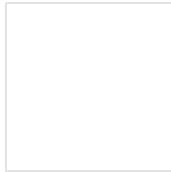
Use Windows Explorer as a ftp client



Use Console2 as THE ultimate command prompt



Using VLC Media Player to capture a screencast



How to backup your blogger blog !

LinkWithin

Posted by hackr at 9:56 PM 3 Comments and 0 Reactions

Tag Cloud

Internet explorer 7 Replacement Window  
Internet Explorer Displaying Tablet Pcs Backups

Like 2 people liked this.

**Add New Comment**

Optional: Login below.

Empty comment input box

Post as ...


**Showing 3 comments**

Sort by Popular now [Subscribe by email](#) [Subscribe by RSS](#)

Comment by **Kennyge** 2 weeks ago


I love you for this

Like Reply

 **Andyrusia** 3 weeks ago

amazingggg111111111

Like Reply

 **gowtham** ★ 2 weeks ago in reply to Andyrusia

Thank You !

Like Reply

Trackback URL

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

---

Copyright © 2011 HackToHell | Powered by Blogger

