# Linux Alternative Concepts

## Preview :

- Disclamir
- Inroduction
- Alternative banner grabbing methods (without using security tools)
- Alternative screen capturing methods
- Alternative linux wireless driver installations.
- A few suggestions

## Disclamir :

- This article is tested.
  - Linux Hack-machine 3.8.0-29-generic #42-Ubuntu SMP Tue Aug 13 19:40:39 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux
  - Ubuntu 13.04
  - GNU bash, version 4.2.45(1)-release (x86_64-pc-linux-gnu)
- A few suggestion part is purely personal views of my experience.
- Some information may break your installation/ break your software. Be carefull when following the article.
- Approriate links to in-detail concepts are linked for further studies.

Any notes, complaints, comments, critics are welcome to imporve and add more alternatives concepts available for linux operating systems. Please report the broken links, if you find any.

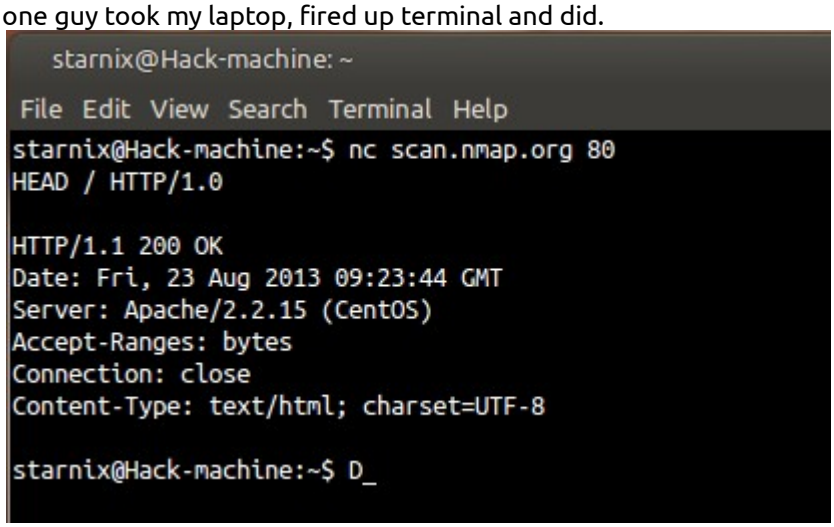
## Introduction :

I usually used to be active on various forums, especially, over **ubuntu forums**, **ask ubuntu**, **fedora forums**, **ask fedora** and a follower of **OMG ubuntu**. I have seen nemourious most common questions floating around, however, they do get solutions, and they do work pretty good as well, but again, there are sometimes either is a over-kill or have a quite obvious solution or alternative than a **regular solution/approach,** which is more easy and powerfull and impressive . When I say alternative concepts it mean, the obvious way to work around the problems/methods. Most of the people who still have very decent knowledge of Linux Operating System, still have never come aound with these approachs, I said “most”, not “all”. However, let start with first alternative “Alternative banner grabbing methods (without using security/tools)”

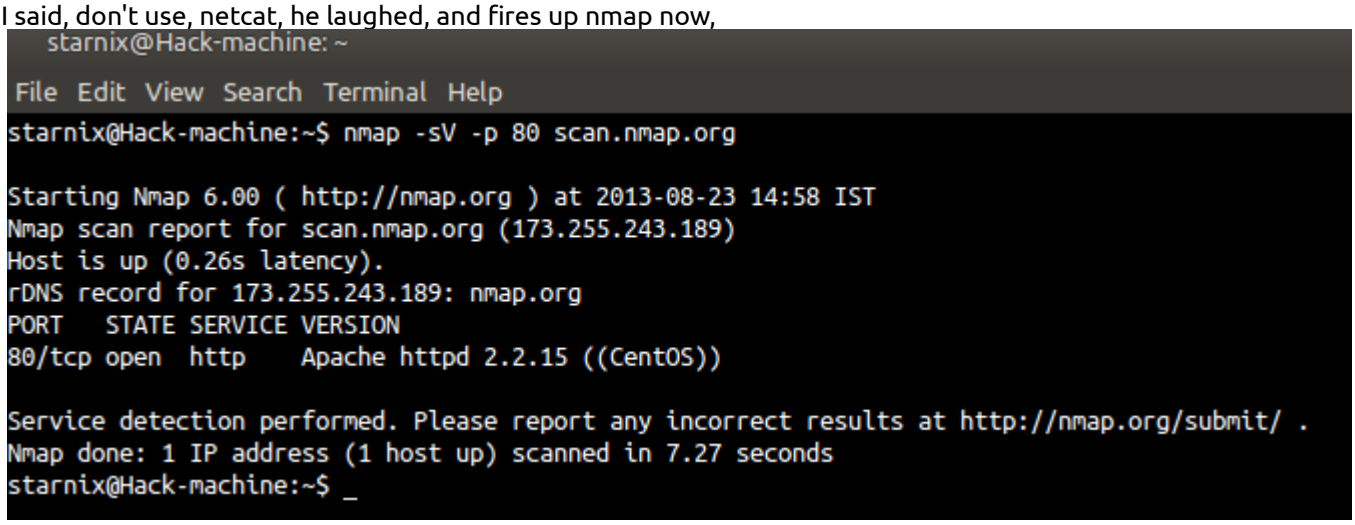
## Alternative banner grabbing methods (without using secuity/tools) :

Enumeration is the process of knowing, how the target server, handles our requests/knowing the basic information about the service running on target machine. Pretty more is there, follow the Reference sections for more standarad definitaions and various other in-details concepts of enumeration. But, we are not intersted in that concept, atleast not here/now, and i consider, you being on this forums, knows, what actually it is, however, let us take one simple example, consider you have a exploit for say apache webserver some-version. And, you have plenty of target machines, the most obvious thing you could do is, finding what is the targets webservers version.

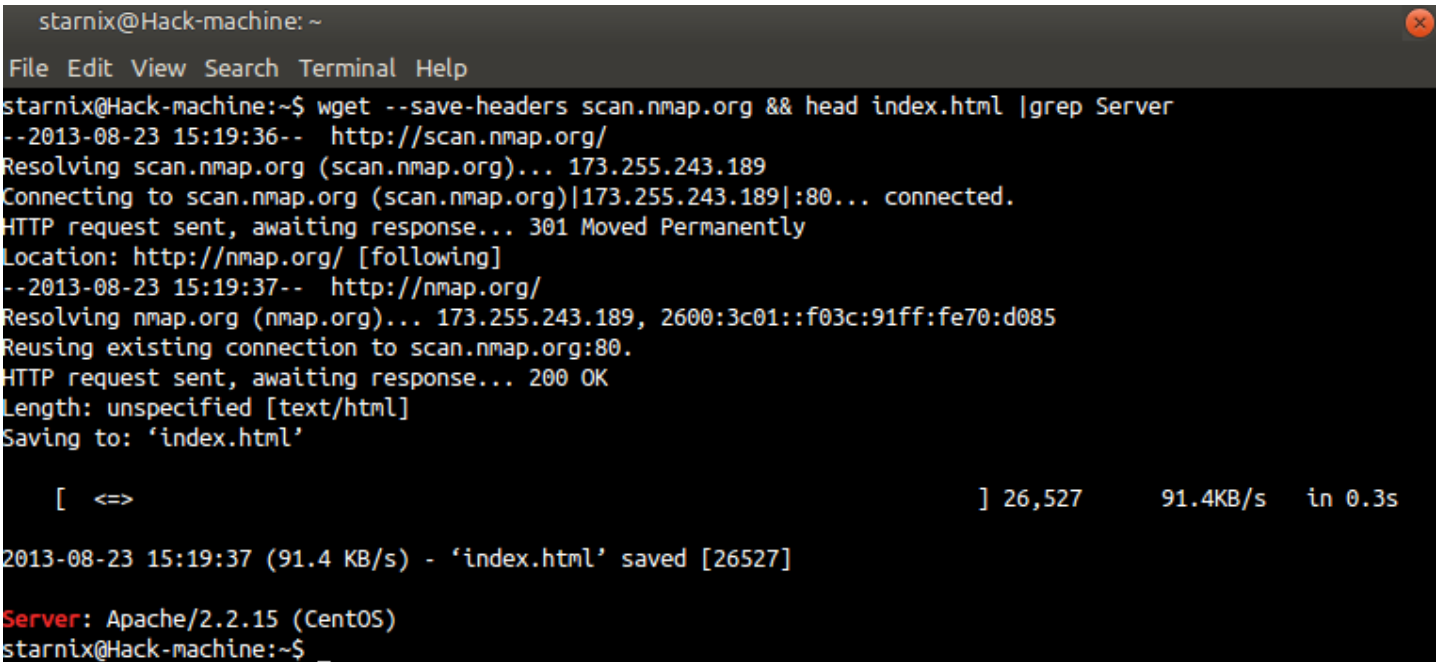
Lets take a real incident, we 4 people having some fun over internet, upgrading and sharing each other knowledge, we do usually. When my turn came up, I threw them a question, “Can you grab a webservers version”, all of them are well versed linux guys (I mean BT fans). They are like you kidding bro?  whats new in that? I said, why don't you do it then, one guy took my laptop, fired up terminal and did.




I said, don't use, netcat, he laughed, and fires up nmap now,




I said, don't use security tools, the he went over-smart now, he did a wget,



I said, okay, thats fine, now don't use any other tool except your terminal and get me the version details. Over smartness gone now. This is what called as Obviousness, we can get that info without using anytools. Let us first analysis, the three methods above, 3rd one wget is absolutely over kill for the task, 2nd one, yep can be used but again starting nmap and time consideration is quite demensive as most of linux distributions have no nmap installed by default. 1St one ya, can be used, but its more interactive, if you have bunch of targes you will be depending on tools like, expect for non interactivity.

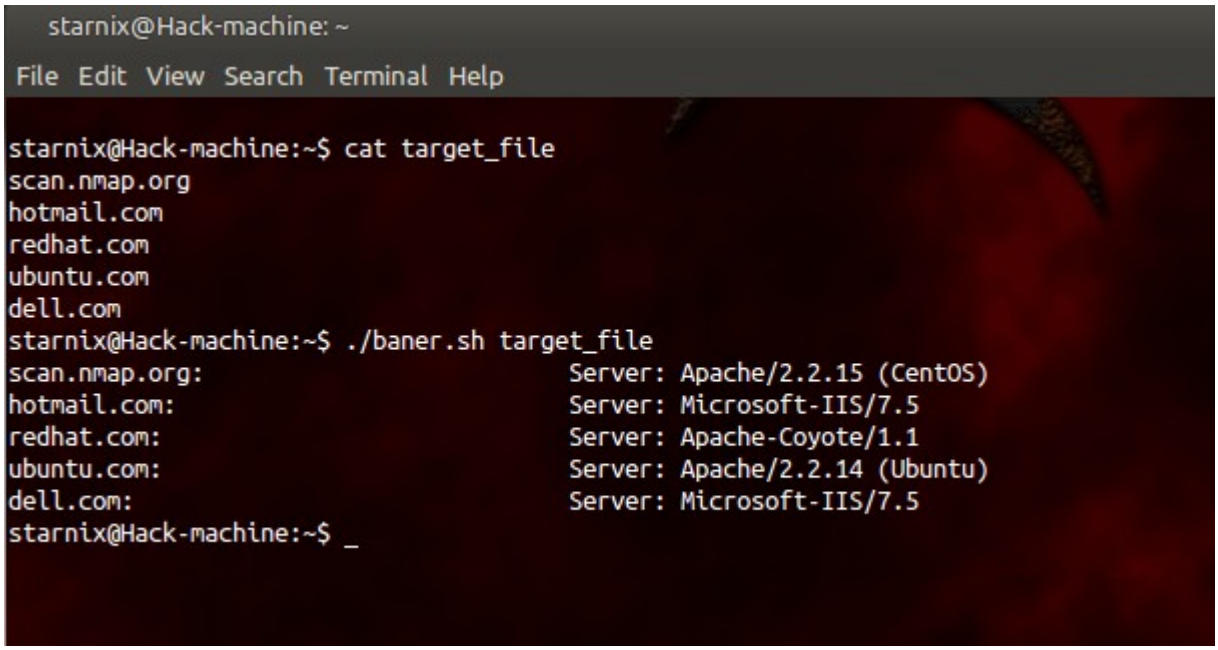
When you alread is in terminal, means you are using bash shell(defualt shell on most of the distributions), and it does have a file decriptor and "**tcp**" device file already availabe for you Linux operating system, you directly get it without using any other security tools or any other tools.
You don't have to installed any non default tools(nmap) or don't have to be in interactive mode(netcat) or you don't have get bunch of un-necessarry data(wget).

```
starnix@Hack-machine: ~
File  Edit  View  Search  Terminal  Help
starnix@Hack-machine:~$ exec 3<> /dev/tcp/scan.nmap.org/80 && echo -e "HEAD / HTTP/1.0\r\n\r\n" >&3 && cat <&3
 |grep Server
Server: Apache/2.2.15 (CentOS)
starnix@Hack-machine:~$ _
```

Another advantage is the fastness, lets us set time on all these methods and check the time consume by one single target (scan.nmap.org).

```
starnix@Hack-machine: ~
File  Edit  View  Search  Terminal  Help
starnix@Hack-machine:~$ time nc scan.nmap.org 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 23 Aug 2013 11:14:11 GMT
Server: Apache/2.2.15 (CentOS)
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=UTF-8


real    0m6.413s
user    0m0.000s
sys     0m0.004s
starnix@Hack-machine:~$ time nmap -sV -p80 scan.nmap.org |grep open
80/tcp open  http    Apache httpd 2.2.15 ((CentOS))

real    0m7.306s
user    0m0.180s
sys     0m0.020s
starnix@Hack-machine:~$ time wget --save-headers scan.nmap.org &>/dev/null && head index.html |grep Server

real    0m1.344s
user    0m0.000s
sys     0m0.016s
Server: Apache/2.2.15 (CentOS)
starnix@Hack-machine:~$ time exec 3<> /dev/tcp/scan.nmap.org/80 && echo -e "HEAD / HTTP/1.0\r\n\r\n" >&3 &&
 cat <&3 |grep Server

real    0m0.257s
user    0m0.000s
sys     0m0.000s
Server: Apache/2.2.15 (CentOS)
starnix@Hack-machine:~$ _
```

I guess, after seeing that image, you could easily guess, what is best, you have a excelent solution with in your shell, you don't need to install any tool, or use any defualt security /tools and get the best result. You could easily implement this on your bash script as a function() for grabing server version fastest way, or just a source a file with targets like,




## Alternative screen capturing methods :

This is actually non OS, related, but, I figured out zillion of times people asking or looking for a screen capturing application for linux, I did see decent answers like, application like “Record my Desktop”, “Xvid-Xcapture” etc., but, when I usually ask these people, what is video player you use, most of them about 70% tells, VLC media player, they have no clude, the VLC itself is a very good desktop recorder. Even that you have more flexability with it.

First let me give you an example:

**http://www.youtube.com/watch?v=pps1W9_B0Z0**

Done that video with vlc. Nothing special.

You just need to open vlc media player, and select stream from you Media menu of vlc and then you have to navigate to capture device tab, and then in capture mode you have select “Desktop”. And for the frame set, you could go with 20.0 f/s and then you have click the select button beside, the stream button on bottom and select convert option, and give the desired file name and click the start button and after finishing you just need to quit the vlc player and there you have the screen capture file ready.

You could find it quit ironic, as if you use record my desktop application, you have select the screen and set various options etc., and after you finish recording you have damn wait like hell to compete the whole recording it does take time, but in our obvious case of vlc, it done simultiously.

## Alternative linux wireless driver installations:

This is the most common issue/question I have encounter over various ubuntu users. When you test or run the ubutnu live CD, with your laptop with proprietary devices. You could easily go to sources/ubuntu software center and select addition drivers and install the proprietary drivers for you device, most commonly with boadcom wireless drivers, you see after installing it and testing ubuntu with live CD/USB, every thing works fine, and you go about installing it, and all of a sudden when you reboot, you have ubuntu without wireless drivers, and do the same thing, either you go to addition drivers and software center and sources and select addition drivers and try to use that proprietary drivers, and it fails no matter what you do. And by know you have no clue what to do.

No, need to panic. When the driver was working perfectly with live CD/USB, it mean there was a package with working drivers on you laptop. You just need to use some common sense here, you just need to insert you live CD/USB and navigate to packages in case of this, you could navigate to, direcotry “pool” , then “restricted” and

select the manufactrues alpabet, like if you have broadcom wireless device, you could navigate to directry “b”, there you will find the wireless driver package, and copy that to your desktop/any other folder and open terminal and do a “dpkg -i filename-here”, it will install the driver, if you run into package dependency problem, remember those all dependiciens are availabe on that live CD/USB. You just need to concentrate on the error more to figure the issue.

## A Few Suggestions:

Linux is not a Rocket Science, you just need to understand, how it works, even I have seen plenty of *nix users who used to use copy paste at terminal with mouse, because, Ctrl + v or Ctrl +c , won't work, just remember you need to use shift button as well, I mean, for copying thing from terminal with keyboard, you have to use Ctrl + Shift + c and same for the paste.

- I would recommend the intermediate *nix users, to work with distro's they like, and experiment with them. Use KVM, as I find for command users, virtual machines, either VMPlayer or Xen to be heavy resource taker, as far as I could for my experience, KVM is too light weighted when compare to other VM's.
- Spend time on terminal with Bash Scripting, code code and more code's will give you the power, you will be amazed off with *nix
- Spend time on *nix support forums or IRC's support servers, where you will find absolutely new methods, absolutely new concepts which you might have not known.

I have not much time, I will come up with four new alternative this last week of month.

**References**:


- Device File in *nix
- Service Scans
- Recommended Books:
    - Ubuntu Kung Fu
    - ABS Guide, Advance Bash Scripting


[ * ] Exploit Code Not People!.
[ * ] Hope you enjoyed the read.
[ * ] Please comment or provide feed back.

-Hackuin