

Forum:[Hack Forums](#)

Thread: [Why Most Hackers Prefer Linux than Windows? - Q & A's \(Part-2\)](#)

?si?qo? - December 19, 2008, 2:56 am

Part One: <https://hackforums.net/showthread.php?tid=39070>

Q: How frequently do web hosts store backusp for their client websites?

A: When I was taking care of FreeBSD webserver for an ad agency, we did a weekly full backup and a nightly backup of the actual web directories, and the Full went straight to a nas, then the nas backed up to a tape. However the standard is to go directly to a tape.

==*==*==*==*==*==*==*==*==*==*==*==*==*==*==*==

Q: What is FreeBSD?

A: FreeBSD is an advanced operating system. It is derived from BSD, the version of UNIX developed at the University of California, Berkeley. It is developed and maintained by a large team of individuals. FreeBSD is used by companies, Internet Service Providers, researchers, computer professionals, students and home users all over the world in their work, education and recreation.

There is only one real webserver as far as I and any self respecting webmaster is concerned and that is apache *nix only. There are several reasons for this and one is security. The only server I would reccomend is FreeBSD.

==*==*==*==*==*==*==*==*==*==*==*==*==*==*==*==

Q: Where do web hosts store their backups? In other words, What is the standard pathname is used for server backups?

A: Typically backups would be wherever you mounted your backup drive something like /mnt/backups

==*==*==*==*==*==*==*==*==*==*==*==*==*==*==*==

Q: If one of the websites on a server has vulnerability and can easily be attacked, can an attacker gain access to the root server & harm the whole server through one of the vulnerable website? OR The attacker will only be limited and restricted to control the attacked website only?

A: If a website has a mysql vulnerability you will probably only be able to access various parts of the mysql database. A website vulnerability that will allow you to insert perl or php code, may allow you some mobility in the server however your user privileges will probably be for the user www-data not for, root. However you can still do a lot of damage with www-data.

==*==*==*==*==*==*==*==*==*==*==*==*==*==*==*==

Q: Where do web hosts store their backups? In other words, What is the standard pathname is used for server backups?

A: Typically backups would be wherever you mounted your backup drive something like /mnt/backups

==*==

Q: How an attacker can attack my website? Is it only through scripts vulnerabilities? What other alternatives?

A: Your website can be attacked, through script vulnerabilities, mysql injection, any exploits that may affect apache(or iis if you use windows), or exploits to the operating system you are using such as debian or freebsd or windows, or any exploits to any other live services you may run through that server such as dns(bind), email(imap, pop, exchange, or smtp), ftp(proftpd, vsftpd, etc).

==*==

Q: Assume my website is hard coded - static pages - html's only. Can a hacker attack it?

A: If you are running html only, no cgi-bin, no scripts of any kind, no mysql, your webpages themselves are not vulnerable, however if your web server(apache or iis), or your OS(FreeBSD,Windows, etc), or any other services you run(ftp, dns, smtp, etc) are vulnerable then your site can still be taken down or defaced.

==*==

Q: How can a hacker find a vulnerability in one of my web page scripts, while all my scripts are on the server side & not shown on the html source code?!

A: This is usually done through various forms of reverse engineering, by throwing code at your server either through query boxes on your page or by using some software like tamperdata, etc..

==*==

Q: Lets say my webhost is <http://www.xxxxx.com> and my username is randomaccount. When i go to command line & insert

ping <http://www.xxxxx.com>

I get a response back with an ip address ...

After that, i type

ping randomaccount.xxxxx.com

i get a response back with different ip address. Why does this happen?

I think they both should have same ip because my website is in the same host server so both ip's should be the same cause its my web page is located in the same place the server is located! Any idea?

A: A server can have multiple ip's for multiple sites. One reason to do this is for SEO purposes, however these could also be seprate servers, there are a lot of reasons to give domains diffrent ips, they could be very technical, they could be for loadbalancing, and it may be that the tech just doesn't know what he is doing.

==*==

Q: What's the difference between a vulnerability and an exploit?

A: Vulnerabilities are holes in the security of a system caused by software flaws, incorrect configurations and/or insecure user behavior. An exploit is something that takes advantage of that hole to either gain unauthorized access or do damage to a system. Examples include Internet Worms, Trojan Horses, and even Social Engineering.

==*==

Q: People say Linux (Unix Platform) better than Windows Platform - Why? When you hack a computer, you do not need to find a vulnerability in the OS so you can hack it, all you need is to passby the firewall application, such as kaspersky.

A: sure, you might be able to get someone to install a trojan horse from any client system - "install backdoor and hack" is a vulnerability independent to OS type.

==*==

Q: When CS's say Windows has vulnerabilities. Thus, its not secured. In which points these vulnerabilities can harm your system cause a computer hacker can not hack your computer until you except an encrypted malicious file! Some say, they put trojans on other people's PC's from Windows vulnerabilities. How come?

A: A competent hacker can access a vulnerable system without you having to except or install anything. If you OS has a vulnerability that will allow me to tell it to execute a command then I can use this to get it to run something or install something that will allow me to get around your security measures. For example there was many instances of IE vulnerabilities that allowed remote users to execute VB scripts on a system running that version of IE. This would allow a user to embed a trojan within a VB script and have the target system run this script.

==*==

Q: Linux is more Secured than Windows. Why?

A: Windows users run administrator accounts, which do not require a password before a program is executed. If an admin executes a program that has a virus, the virus has complete control over the computer instantly, and without needing to get through anything. On a UNIX system, the user almost never uses the all-powerful "root" account, and if they do, they must put in a password to execute powerful programs.

This is also the reason that UNIX systems won't break because a program does something bad, because that program is perfectly isolated - every program execution requires the password before it can be executed. Therefore, there is no chance for one program to control other programs, only if you are in root mode (account), you can do whatever you want freely.

Windows is not nessasy less secure but it is the domiante OS. If you were a hacker you would want to effect as many people as possibe, and that's why Windows is at a higher risk. More people use Windows, therefore a larger number of people are good at hacking Windows. Windows is a OS based on profit margins, meaning that more sloppy code is let past in order to get the OS out the door. There is also the fact that fewer desktop users use UNIX and Linux etc., so fewer people write viruses for them. Neither Windows nor UNIX are perfect, but the general security design of Windows

is worse.

Q: What kind of firewalls major companies do use?

=*==

Q: What linux got to do with hacking websites and servers? I will be hacking another party, so regardless of what os i have, i will hack the website based on my skills, not based what OS i have! Any suggesstion?

Extra Advise: there's also the idea that if you make a virus for WINDOWS in LINUX then, you can store it and have no worry of auto execection when you put the disc/usbstick back in your PC to edit files.

In summary, *nix is good for hacking/cracking wireless networks, servers, writing exploits, websites, and all things related to cgi scripts.

the majority of people use Windows, so its better to write malicious files for Windows, so you can kick lots of asses.....Write malicious files for linux, only if you are aiming to crash a specific person's pc who uses linux

Q: Can I Write Trojan Under Linux in C++ to Hack Windows Systems?

==*==*==*==*==*==*==*==*==*==*==*==*==*==*==*==

Q: What Does Port Your Code From Linux To Windows Mean?

A: Porting code from linux to windows means making some changes in your code, so that it works on windows. There could be substantial differences between the code that gets successfully on windows and on linux. For the differences, you need to check your coding language manuals.

==*==*==*==*==*==*==*==*==*==*==*==*==*==*==*==

I hope you have learned something from this thread ?

Anyhow, drop a comment if you like it!

Catch ya l8r...

DAMINK - December 19, 2008, 3:01 am

Not a FreeBSD fan actually. I run a server from home but i choose Mandriva as the OS.
I guess it all comes down to personal choice at the end of the day. They all run the same Kernel yes?
If updated etc etc.

?si?qgo? - December 19, 2008, 3:03 am

These are Q's & A's that is been gathered from various sources, so yes i agree with you. At the end, its a personal choice when it comes to having a server...

Chaoz - December 19, 2008, 3:04 am

if i could install linux i would why we prefer it ? simple with a virtual box on linux your basicly 100% secure meaning 80% virus works trojans arnt written to be executed under linux

?si?qgo? - December 19, 2008, 3:10 am

(Dec 19, 2008 04:01 AM)DAMINK Wrote: [CITE](#) Not a FreeBSD fan actually. I run a server from home but i choose Mandriva as the OS.
I guess it all comes down to personal choice at the end of the day. They all run the same Kernel yes?
If updated etc etc.
To learn more about the differences in kernels, visit
http://opensolaris.org/os/article/2005-10-14_a_comparison_of_solaris_linux_and_freebsd_kernels/

It may help.....I do not have enough knowledge regarding differences between kernels, so i can not really talk about.

InCtrl - December 20, 2008, 7:30 am

what i dont like about linux is IT has to have wine to run .exe files,

used LINUX MANDRIVA 2008<- very nice desktop^^ with so cool animations

H3LL - June 4, 2009, 2:03 am

Thank you, i've bumped into an old thread... i came from part 1 =)