Windows vs FreeBSD vs Linux

Or: Why Deploying Linux in your Environment is Suicide

DEFCON 13

Don’t Believe Anything I Say

- "Do not believe in anything simply because you have heard it. Do not believe in anything simply because it is spoken and rumored by many. Do not believe in anything simply because it is found written in your religious books. Do not believe in anything merely on the authority of your teachers and elders. Do not believe in traditions because they have been handed down for many generations. But after observation and analysis, when you find that anything agrees with reason and is conducive to the good and benefit of one and all, then accept it and live up to it.” - Buddha
- Daytime - Security consultant
  - “Beltway bandit” in Linthicum MD
- Night - Founder of the Shmoo Group, Capital Area Wireless Network, periodic author

For Your Safety and The Safety of Those Around You

Linux Zealots

Windows / BSD / Others

- This talk **may** be not much more than flamebait
  - You may be reminded of a /. Discussion
- This talk is meant to be interactive

Lets Talk about Security

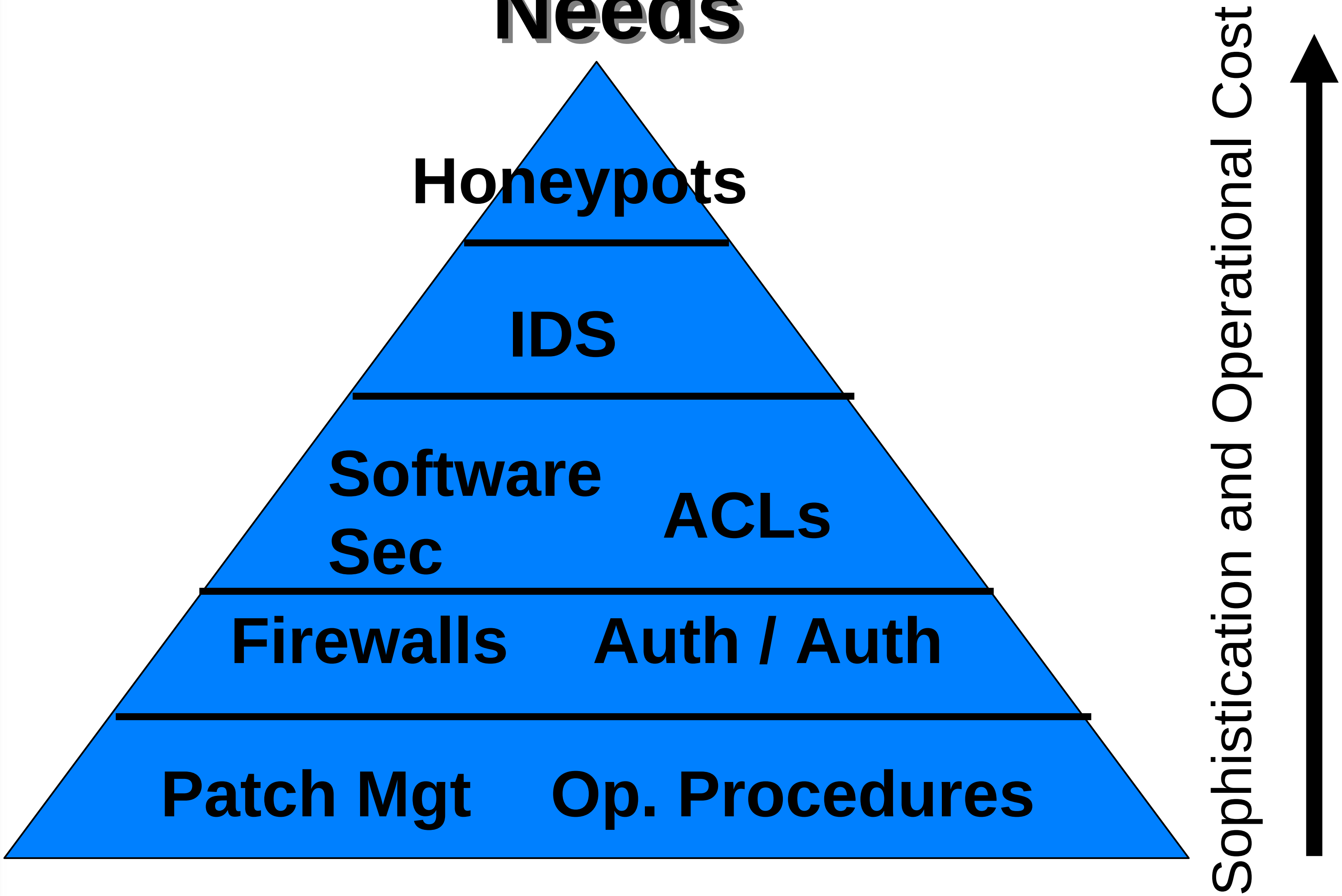
- For the feds, “Information Assurance”
- Tactical Coding Error vs Design Flaw
- Script kiddie vs Dedicated Attacker
- Host Hardening vs Long term operational security

Long term Operational Security

- Often overlooked aspect of "security"
  - We are not an end in and of ourselves.
  - Further, an IDS does not operational security make
- Any idiot can be trained to secure a host
  - Look at all the security books on the shelf
  - Running a long term secure enterprise is the tough thing

Enter Rant Mode

Potter’s Pyramid of IT Security Needs



Honeypots

IDS

Software Sec

ACLs

Firewalls

Auth / Auth

Patch Mgt

Op. Procedures

Sophistication and Operational Cost

Why Does the Development Method Matter?

- You can certainly do belly button contemplation to say why it does or does not matter

Corp View

  - Structured process is the only way to build a secure and scalable system

Or

OSS View

  - Having many eyeballs and lack of clear direction means the best and most useful stuff is what will get integrated, not all the fluff.
  - There is no right answer…
    - Process driven code can suck horribly
    - There are often not “many eyes” looking at security

But really, is there a difference?

- Beyond what the zealots say, and what the media says… Is there a real difference?
- Assessing this difference is a real PIA with lots of red herrings
- Methods of determining difference
  - Examine the development processes
  - Examine the history of security in the architecture
    - Vulnerability statistics?
  - Examine the future directions of security
  - Ideally get statistics from enterprises on how they spend their security budgets and why
    - I’m not Burton or IDG… So I just asked friends…

Let's talk about Vulnerability Statistics

- Vulnerability stats are (generally) an artifact of tactical coding errors, not bigger problems
- "In the last year we cut the number of patches we released from 35 to 12"
  - Well, if you're rolling up many vuln fixes to one patch, it doesn't count
  - Further, the impact from the vulns may vary as well
  - Not just an MS problem… MDKSA-2004-037
- Whose code was the vuln in?
  - Kernel? Integrated Application? Third Party?

But We're ahead of ourselves. First, Windows!

- Developed as a complete system
  - And then some… Applications are tightly integrated with operating system.
  - Obviously, MS works as one organization, and Office upgrades are aware of Windows upgrades and vice versa

Kernel	**Core Sys Utils**	**Applications**
MS Created	MS Created	MS Created

Windows Release Methodologies

- Publicized well in advance
  - Much of it is marketing spam, but there is obviously a HUGE developer network that seeds new technology info well in advance of release
- MS has a habit of once they’ve dominated a market, they stop dealing with the market
  - IE is a prime example
  - This has a negative impact on security
    - MS will only integrate as much security as the market demands.
    - The OSS world will continue to integrate security b/c it’s the right thing to do

Windows Security Roadmap

- Many long term security initiatives
- Internal code security programs
  - Security is woven through their entire development process
  - Tho with the recent announcement of Land II, they may not quite be there yet
- Security functionality roadmap
  - Including a full MLS compliant OS by 09
- Definitely aware of Security Operations

FreeBSD

- FreeBSD is designed and developed as a complete end to end system
  - Kernel to userland system utilities
- Structured development process
  - Core team, and accountability for all parts of the core OS
- Beyond userland system utilities, thirdparty software is packaged by the FBSD team
  - Either in binary or source packaging (or both)

Kernel	**Core Sys Utils**	**Applications**
FBSD Created	FBSD Created	FBSD packaged

FreeBSD Release Methodologies

- For Core system, there is a FreeBSD Release Engineering team.
- For Third party software, there is also a team dedicated to “produce a high quality package set suitable for official FreeBSD release media.”
- More info at http://www.freebsd.org/releng/

FreeBSD Security Roadmap

- FreeBSD provides EOL info WELL in advance of EOL occurring to give operators a heads up.
- Many integrated security features
  - Securelevels are a great feature
  - Expanded ACL control, jails (!chroot)
- While not a Roadmap ala Microsoft, still a great start.

Linux

- It’s Bazaar, right?
- Linus et al control the kernel
- Community creates the rest with some loose coordination
- Distros use Duct Tape as a “value add” to put everything together
  - While they’re all “Linux” they’re basically different OS’s
  - Aren’t they?

Kernel	**Core Sys Utils**	**Applications**
Linus Created	Community Created / Distro Pkg	Community Created / Distro Pkg

A Choice Slashdot Quote

> My point with this is that it's not the kernel that's making GNU/Linux systems crawl on older hardware. It's the newer versions of GNOME and KDE. As long as you aren't running GNOME or KDE, older hardware works just fine. My servers chug along just fine, and my 233 MHz laptop with 64 MBs of RAM running Sawfish also suffices just fine to do virtually all my common tasks (except running any Mozilla product :-P).
>
> So, certainly, GNU/Linux may need more developers from third world nations, as you put it. Linux, however, does not.

- First, why do I care about the bloat of the graphical environment vs the bloat of the kernel? It’s all part of the OS as far as I care
- Second, stop with this GNU/Linux vs Linux argument..

Linux Kernel Release Methodologies

- Whenever they feel like it
  - Whenever they feel like iterating the third digit
- Changes with each major release
  - 2.0 was different than 2.2 than 2.4 than 2.6
- Not necessarily done in conjunction with distros
  - Distros released at the same time will often use different kernels
- Frankly, it’s all at Linus’ and his deputy’s control

Distro Release Methodologies

- Even tho they're all "Linux", they're like their own OS
  - So there…
- Some are very slow evolutions and rely on uber admins
  - Debian is the ultimate example
- Others attempt to have structure and make things easier on the user
  - The Old ReadHet, Ubuntu, etc…
- However, since they're really only responsible for the packaging and glue code, they're at the whim of the community for features, especially security
  - A distro will not, for instance, write their own firewall code

Linux Security Roadmap

- Not much out there for “Linux”
  - There’s barely a kernel roadmap…
- RedHat released a security roadmap 2 years ago that basically amounted to “Integrate SELinux into RH distro”
  - Really, that’s about all I found… Others have insight?
- Lots of add-on things (GRSec, etc…)

Vulnerability Statistics Revisited

- Very interesting study - “Role Comparison Report - Web Server Role” by Ford, Thompson, and Casteran
  - Decomposed the vulns in RH Linux ES 3 and Windows 2k3
  - Focused largely on installation and ops as they relate to the vulns (we’re looking for the root cause)
- Scary statistics (just a sample from the report)…

Severity	MS Server 2k3	RHEL ES 3 (min)
High	33	48
Med	17	60
Days of Risk		
High	1145	2124
Med	426	4003

And now, Patching

- Patching is a core Security function, and releasing patches should be a core vendor function
- MS used to release patches whenever it “made sense”
  - Now they’ve gone to monthly roll-up patches
  - Concerns about losing resolution (aka: making 0day attacks a problem) have not materialized
  - Certainly simplifies ongoing Ops
    - Regression testing / QA can be scheduled in advance and patch deployment times are reduced

Patching on the *NIXs

- FreeBSD Kernel
  - Patches direct from FBSD developers
- Linux Kernel
  - Patches can be applied from kernel.org code
  - Patches can be applied from distro code
  - Which is right?
- Third party patches (network stack, KDE, etc)
  - Patches direct from developer
  - Patches from distro
  - Core system utils in FBSD come from FBSD developers
  - Again, which is right?
- *NIX patches easier to understand, easy to mass deploy
  - More difficult to determine if it’s needed

Before the Debian Users get out of hand

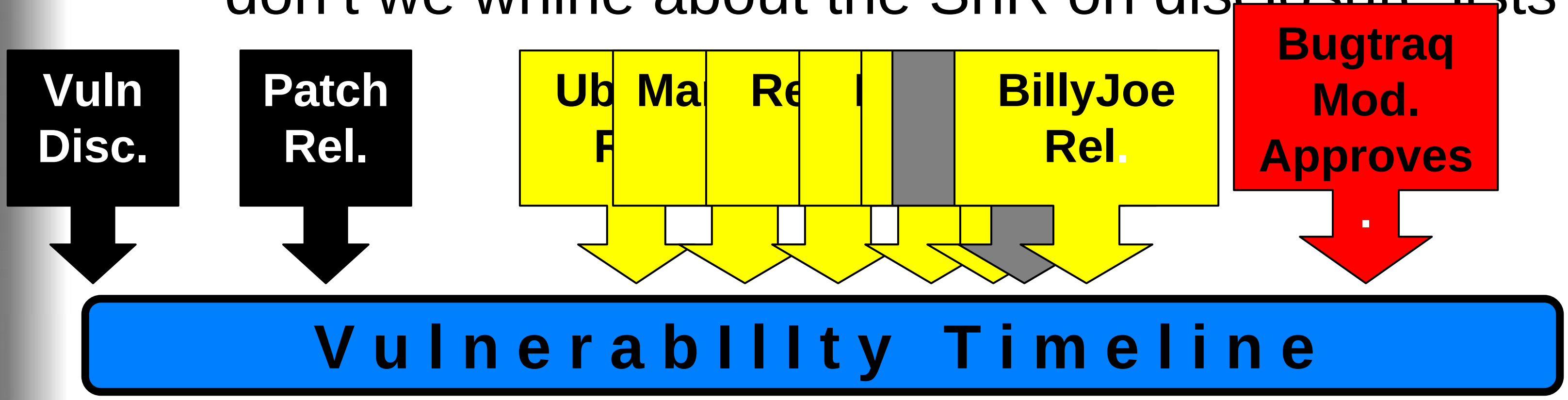
- From the Deb Project Lead Report:

Woody Security Update Challenges and Progress

The ARM problems we've had have also affected the timeliness with which we've been able to get security updates out. A security fix to``xfree86``, for example, has been stalled for weeks because no ARM build daemon has been operational to compile it. (See `Debian bug #298939`_ for details.)

Lets not Forget about SnR

- So, it’s not just about the architecture
- Security admins have to stay up to date
  - I.e. We can justify why see surf the net all day
- The hell that is the Linux Distro security announcements
  - We whine about the bad SnR on an IDS, why don’t we whine about the SnR on disclosure lists



The Future

- Linux continues to survive by brute force and a worldwide network of zealots
  - The Linux zealots make Apple users look tame
- MS will continue to push the bounds of security beyond what the stereotypical OSS operating system can do
  - Especially from an operational security perspective
- The BSD’s will continue to be the leaders in the OSS movement wrt operational security

Questions? Answers?

- Contact Info
  - gdead@shmoo.com
  - potter_bruce@bah.com
- Flames
  - /dev/null
- This talk will be available from www.shmoo.com/~gdead soonish
- Check out “Mastering FreeBSD and OpenBSD Security” from O’Reilly