Information Security, Open Source Software, and Your Future

David Matusiak | NCSU FOSS FAIR | February 18, 2012

image: http://clubmumble.com/wp-content/uploads/2009/03/your_future.jpg
blog: http://clubmumble.com/2009/03/25/your-future-starts-here/
by: Randy Laybourne

Greetings and Thank you for coming to listen to my talk today!

My name is David Matusiak and I work as an Information Security Consultant. I spent most of my early career wrangling mainframes, administering Solaris & Linux systems, and learning about TCP/IP networking. I joined TriLUG in 1999 and was on the Steering Committee in 2004/2005.

Over the past few years, I've begun specializing in auditing systems and networks for sensitive data (such as PCI DSS compliance for handling credit card information), analyzing packets and alerts in Intrusion Detection Systems, and helping large organizations to gain valuable insight from their SIEM (i.e. logging) tools and infrastructure.

Just for reference SIEM stands for Security Information and Event Management, and these are systems designed to gather log information from all devices on your network (firewalls, IDSes, Linux/Windows servers, etc) and provide actionable intelligence around "events of interest." These 'events' are essentially needles in the haystack, which may indicate potential compromises or other anomalies.

So, this talk is titled "Information Security, Open Source Software, and Your Future." To some extent, that title may be an inaccurate depiction of what I plan to talk about. Is it about Information Security? Somewhat. Is it about Open Source? To a certain extent. Is it about Your Future? Absolutely. Some things I cover may wind up being controversial, but I'm just trying to provide the best advice I can.

OK, Who has a social networking account?

image: http://avtecmedia.com/images/blog/social-networking-logos.jpg
blog: http://avtecmedia.com/credit-union-marketing/social-networking/

So, before we start, who here has a social networking account? Okay, this will be important later, as I ask you all to take an online survey I'm running to gauge user behavior and privacy expectation within social networks. So let's get started!

Recent trends in Hacking

U mad, bro?

For the Lulz?

image: http://www.shutterstock.com/pic-86909384/stock-photo-the-hague-october-two-masked-members-of-anonymous-demonstrating-during-the-occupy-protest.html
blog: http://venturebeat.com/2012/02/07/hackers-leak-symantec-source-code/

image: http://venturebeat.files.wordpress.com/2011/06/lulzsec.jpg
blog: http://venturebeat.com/2011/06/23/lulzsec-arizona-police-hack/

Summer 2011 was a golden time for Hacktivism, with groups like Anonymous and LulzSec taking over the media airwaves. Unencrypted databases were dumped and lots of information was uploaded to bittorrent. Security companies were getting owned left and right. SSL certificate providers like Comodo and Diginotar were tricked into issuing fake authentication certificates, allowing hackers to put up HTTPS enabled websites that acted exactly like the real ones.

Email marketing provider Epsilon was mostly unheard of until a breach forced them to inform millions of customers that their email addresses and passwords had been revealed to hackers. These activities were well documented via Twitter, YouTube and other media outlets. And these groups have thrived on the attention they were able to garner.

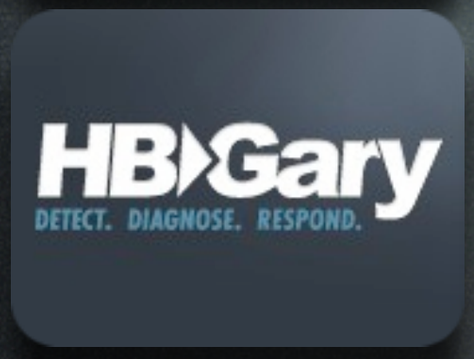
Whereas Anonymous started several years ago as a method to battle the indomitable Church of Scientology, it has now evolved into a full-fledged computer hacking ring, which by its nature is basically impossible to quantify or classify. Anyone can be Anonymous and anyone can take actions in their name. Their efforts came into full swing after the Wikileaks outbreak and the widespread condemnation surrounding that site. Once Visa, Mastercard and PayPal begun preventing payments to the site, the attacks began.

Since then, most of the attacks have been in response to issues that group members perceived as wrong – Anti-piracy laws, anti-immigration laws, anti-war demonstrations, and big corporations spouting how effective their security programs are. Just last week, one of these groups was able to record a phone conference between the FBI and Scotland Yard where the topic of discussion was the Anonymous hacking group itself.

The technical attacks are mostly comprised of SQLi attacks and XSS vulnerabilities against software like Wordpress, but also some PHP and web server vulnerabilities, etc.

But perhaps the most effective hacking tactics these days are not really technical at all. They are social engineering attacks, designed to exploit the trust models between human beings. Spear phishing is sending infected files to victims – such as Word doc or PDF file – which many recipients are happy to open and examine. If these files get a chance to execute and take root, then the sender now has an entry point into their target network. And the payload is usually a rootkit, designed to install backdoor and cleanup tools allowing the attacker to remain on the system indefinitely. This is way easier than jumping a security fence or evading a network-based IDS.

DDoS, D0x, Pwnage



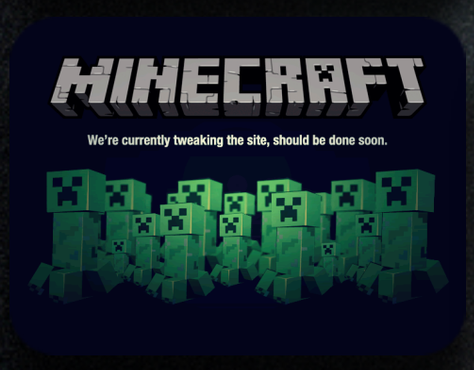


Image credits belong to respective companies and organizations.

The complete list of targets is too long to name, but successful attacks were mounted against sites owned by Fox.com, PBS, Paypal, VISA, Mastercard, RSA, HB Gary Federal, Stratfor, Black & Berg Cybersecurity Consulting, Symantec, Minecraft, EVE Online, Sony Pictures and their PlayStation Network, British NHS, The Sun newspaper, as well as US government targets like the CIA, US Senate, Arizona law enforcement, InfraGard chapters, etc.

These attacks included Distributed Denial of Service (or DDoS) attacks against their networks to prevent their customers from accessing their online services, D0x'ing the organization – which is essentially downloading their sensitive information, be it emails, intellectual property, financials and releasing that info online, or just spats of general pwnage like altering their web page or using email/password combos to jump from site-to-site wreaking havoc for the many victims.

This was all pretty bad, and definitely alarming for most information security professionals. Not to mention the innocent victims who had just been buying shoes online or playing games and then suddenly had their accounts taken over.

Advanced Persistent Threat

image: http://international.loc.gov/intldl/naxihtml/images/china.jpg
blog: http://international.loc.gov/intldl/naxihtml/

Perhaps the most worrisome groups are those we are not hearing about. APT

Jokingly I have a picture of China here, which has become synonymous with the APT nomenclature. But it is true that China (along with Russia, Iran, Ukraine, and others) have become large players in the political hacking scene.

There are still many threats to the average computer user, including Zeus banking Trojans, drive-by downloads within browsers (regardless of platform), and malware links and files shared via social networking (this stuff is based on the hot news of the day, like supposed pictures of Osama bin Laden or Whitney Houston, or cleverly worded come-ons such as “OMG Look at you in this photo!!”).

But the real threats of the future (AKA Cyber War or Cyber Terrorism) are attacks against our utility infrastructures and plans created by our military forces. SCADA (or **supervisory control and data acquisition**) systems in Iran were damaged by the Stuxnet worm and resulted in a setback of the Iranian nuclear program. It is rumored that these tools were developed by the US, probably working with Israel, to defeat the nuclear threat from that region. However, make no mistake that these same attacks could be used against the United States and our allies.

This week news came out that Nortel Networks had been infiltrated by Chinese hackers for the past 10-15 years and that the espionage may have played a large hand in their bankruptcy. Whether business, government, or personal – these folks ain’t playin’. **Basically, the dedicated hackers will spank you.** So you simply have to respect their dark power to do harm and put in concerted effort to protect yourself and your organization from the advancing threat.

Whose fault is it?

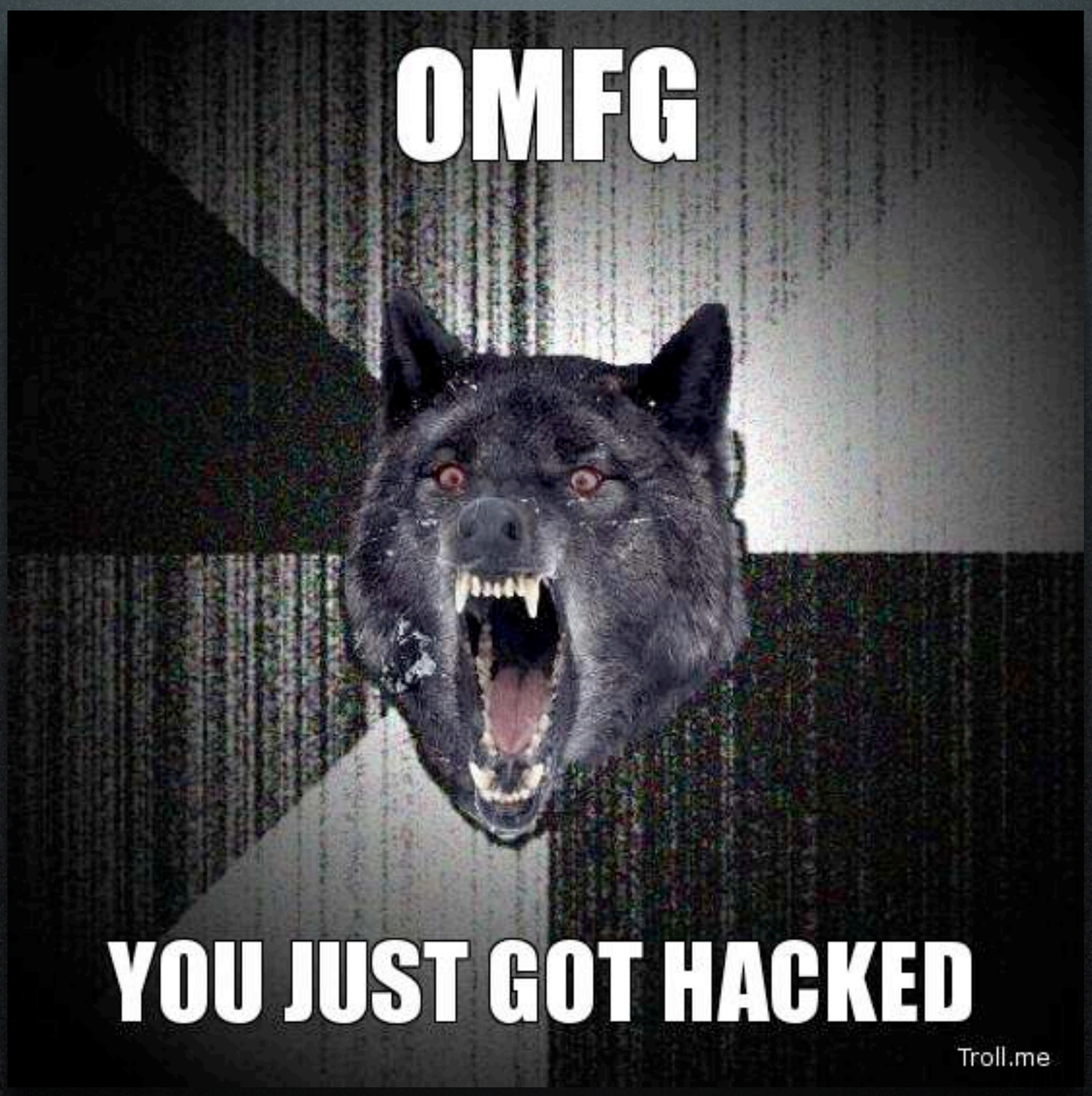


image: http://troll.me/images/insanity-wolf/omfg-you-just-got-hacked.jpg
blog: http://troll.me/

In all of these attacks, is it the fault of the server administrator for not configuring their box right? Or is it the database admin's fault for not encrypting stored data? Perhaps it is the fault of the web programmer for leaving exposed calls in their interface or not sanitizing input? Or how about the folks who wrote all the software in the first place? Well, the person who usually takes the blame is the over-worked security guy who has to keep up with the rapidly evolving info sec world and never gets to take a vacation.

The whole point of my talk today is that it doesn't matter whose fault it is. Everyone is responsible and if you want to lead a successful career in IT, then you should incorporate security into everything you do.

This could be another standard security talk telling you to use complex, unique passwords, and run anti-virus software, while keeping your OS and programs up to date. I could spend time telling you not to click on web links or open emails or ever connect with anyone online. There is lots of advice like this out there – some of it good, some of it less good – but today I thought we should talk about something a little different.

Ten Tips for Success

1. Don’t be a jerk
2. Accept that you don’t know everything
3. Build a good network of smart & trustworthy people
4. Don’t be hard headed about your toolset
5. Realize that Open Source has already changed the software world dramatically
6. Work with OSS tools and virtualization to gain valuable experience
7. Learn a little bit about everything (Be a good troubleshooter)
8. Embrace change
9. Don’t forget those people in your network
10. Incorporate security into everything you do!

I’d like to give you my tips for being successful in IT that I have learned over the past 15 years. Sure, some of it is about being secure and protecting yourself. A little bit is about Open Source Software and finding the best tools. But most of it concerns getting along with others and learning to go with the flow. There is also the caveat to not get too hung up on what technology you get to work with, because in my experience being an obsessive software elitist will only hurt your career.

Top Tips for Success

1. Don’t be a jerk
2. Try to understand that you don’t know everything
3. Build a good network of smart people
4. Don’t be hard headed about your toolset
5. Realize that Open Source has already changed the software world dramatically
6. Work with OSS tools and virtualization to gain valuable experience
7. Learn a little bit about everything (Be a good troubleshooter)
8. Embrace change
9. Don’t forget those people in your network
10. Incorporate security into everything you do!

Don’t Be A Jerk

- Make friends, not enemies
- Reduce your attack surface
- Redefine the target landscape

image: http://www.jennymacbeth.com/wp-content/uploads/2012/02/jerk11.jpg
blog: http://www.jennymacbeth.com/2012/02/the-jerk-all-i-need-is-this-flashlight/

The idea here is simple. You don’t want to attract more attention to yourself by making people mad. It would be hard for me to count the number of times I’ve heard of people getting their email or social network accounts taken over by angry ex-boyfriends or cases of employees trying to frame their arch-rival in the office because of some perceived slight. Human nature is to take revenge on those who thwart us, and in the digital realm this can have extensive costs.

The whole reason many of these organizations are getting hacked is because the righteous hackers think a company or agency is being a big jerk. So they own them in order to give a little payback. It is not worth it to antagonize people online; believe me on this one!

So my advice is to make friends, rather than enemies. In security terms, this will reduce your attack surface and redefine the target landscape so that the bad guys go and focus on someone else. Stay out of the crosshairs.

Admit You Don't Know All

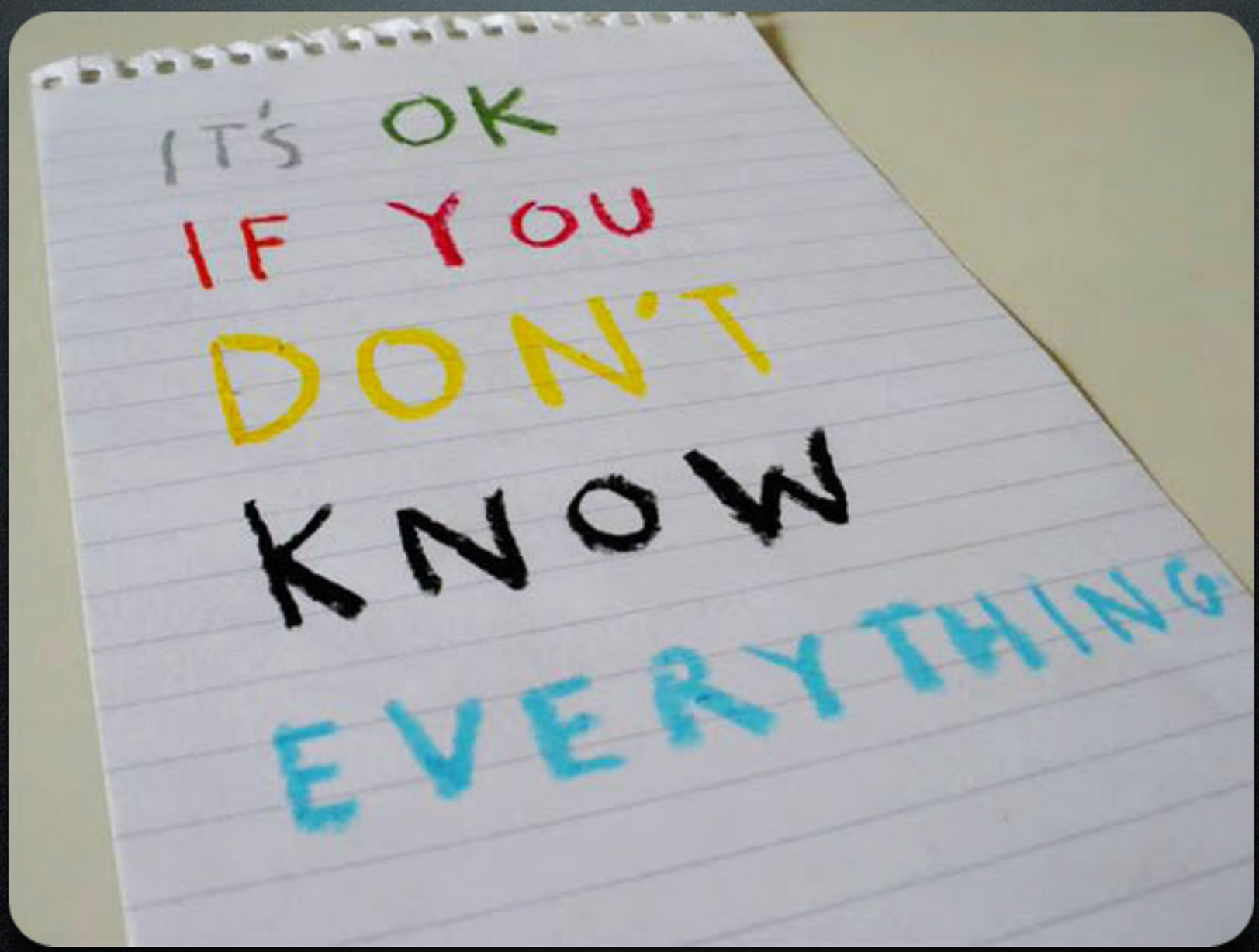


image: http://joshmock.com/wp-content/uploads/2009/05/its-ok-if-you-dont-know-everything.jpg
blog: http://joshmock.com/2009/its-okay-if-you-dont-know-everything/

Hubris is another delicate human condition, and one not well tolerated by the hacker community. No one knows it all and if they say they do, then they're lying. I've had the unfortunate experience of working with a few consultants that could not admit they were ever wrong. Now, confidence is an important trait to have if you want to go into consulting. But to outright lie in front of a client and pass it off as truth is a huge mistake. Even if you don't get caught in the lie, it is still terribly unethical.

There are lots of smart people out there, but none of us has the capacity to know it all. If you act like you do, it is only a matter of time before someone who actually knows better comes along to show you up. Tis better to admit you don't know and turn the conversation into a learning experience. Knowledge is so much better when shared. And no one likes to work with knowledge hoarders, so admit when you don't know something, learn something new, and move on.

Build A Good Network

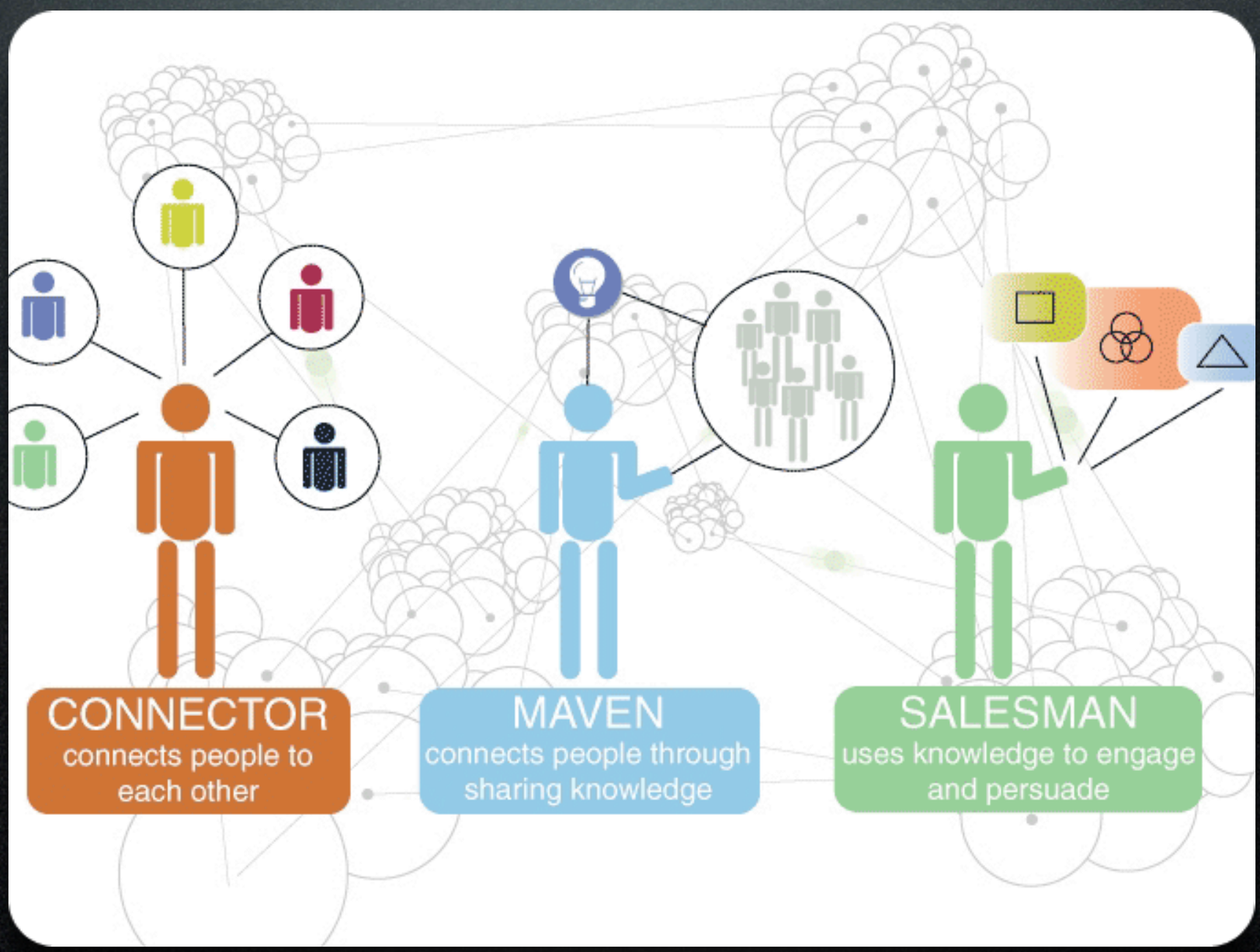


image: http://www.mindmeters.com/upfile/200687211659313.gif
blog: http://www.kstoolkit.org/Social+Network+Analysis

This is so crucial, and yet so many people miss out on the opportunity to network. There are people all around us everyday – at work, in class, out about town – and you should be able to find value in most, if not all of them. There are people who can help you find jobs, people who know answers you seek, and people who know the person who might change your future forever. You don't want to miss these opportunities by being anti-social or caustic. Instead, try to reach out and listen to other folks, and you will see how that favor is returned.

There are people who act as super-hubs to connect many other people. There are some very smart and prolific folks who do research and share knowledge to better our community. There are sociable sales folks who bring us products and services. And believe me, you may think you don't like sales people, but there is so much to be learned from them. You will always have to be good at sales. Always! You will need to sell yourself to get a good job in a competitive market. You will need to sell people on your ideas if you want to get developer funding. And you will need to sell your professors on your thesis if you want to get your degree. Selling is vital!

So get out there and network with others. A good way to connect and maintain these networks is via LinkedIn, but I'm sure there are many other avenues.

Don’t Be Hard Headed

- You are the work you produce, not the tools you use
- Stubbornness can prevent you from getting jobs
- Very rare for a company to provide a Linux desktop

image: http://ministerofblog.files.wordpress.com/2008/11/united-axn-rock.jpg
blog: http://ministerofblog.wordpress.com/which-witch-is-which-testimonies-of-deliverance-from-the-darkest-pit/where-did-our-current-prophetic-systems-come-from-are-they-of-god-or-a-tare-planted-by-the-enemy/

This may be the most important thing I could mention at an Open Source conference. Linux and Open Source people are traditionally very hardcore about their beliefs in the software world and what is “right.” These closely held beliefs may not be shared by the larger segment of the world. In fact, if you push on this issue too hard, you will likely be held in disdain.

You need to realize that your value comes from the work you produce, not necessarily from the tools you use to do it. Sure, there are some fantastic benefits to openness and interoperability, but 99% of businesses and organizations out there are not going to comply with your beliefs. They simply haven’t moved to the enlightened place you’d like them to occupy.

In 15 years, I’ve only seen two companies that would offer employees a Linux desktop. One was at one of my earliest jobs at an ISP, where it was mostly comprised of network engineers who were extremely proficient at Unix and Linux administration. The last was at a large software-as-a-service programming shop where nearly all employees were highly technical. But for all the other companies I’ve consulted for or worked at, it was a Windows desktop. Maybe one or two Mac-friendly companies thrown in there for good measure. You have to be flexible in this realm or you may simply prevent yourself from getting jobs.

Don’t Be This Guy!

image: http://www.coders.me/wp-content/uploads/2009/02/terroristlinux.jpg
blog: http://www.coders.me/reflexiones/la-religion-ultra-linuxista

Whatever you do, you don’t want to be this guy! Because no one will hire you and no one will want to work with you. If you feel this strongly about only using Open Source tools, then you need to open your own company. Even within a great company like Red Hat I’m not sure this sort of affected extremism is welcome.

OSS has changed the world

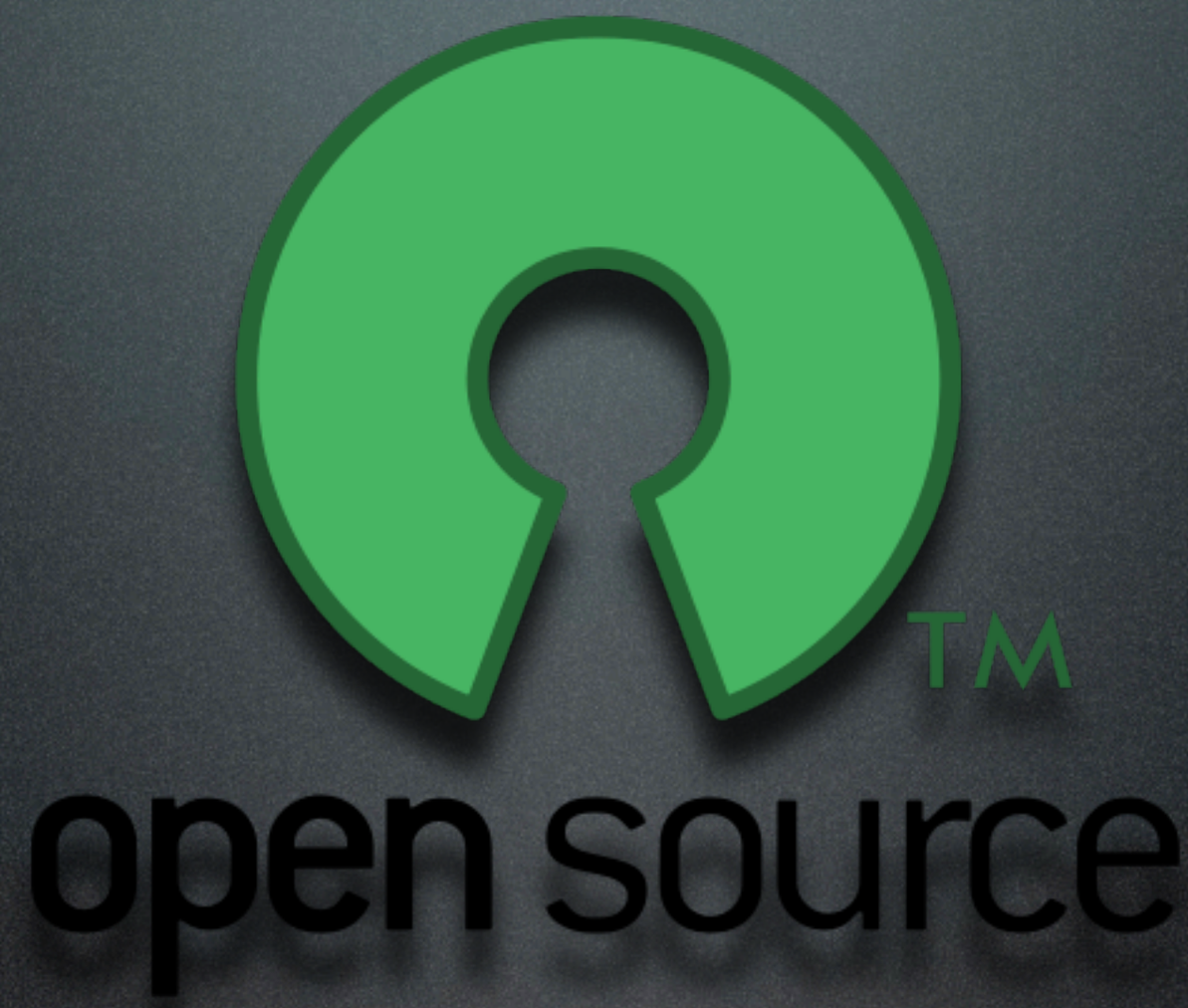


image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

REALIZE THAT OPEN SOURCE HAS ALREADY CHANGED THE SOFTWARE WORLD DRAMATICALLY

This is another very important point that I want you to take to heart. In the past 15 years, the Open Source movement has basically revolutionized the software industry. “Free” products built and maintained by volunteers have essentially challenged or beat down billion dollar software companies. How many of you out there are still running a proprietary web server?

Let’s just examine a few of the massive success stories.

OSS has changed the world

image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

image: http://static.arstechnica.net/opensource/firefox-09-intro.png
blog: http://arstechnica.com/open-source/news/2011/03/mozilla-outlines-16-week-firefox-development-cycle.ars

Firefox web browser by the Mozilla Foundation. This product was able to knock off Internet Explorer as the most popular web browser (user choice terms vs default install terms). It has a near infinite base of plug-ins and extensions that allow it to be customized and do nearly anything, from helping to troubleshoot web applications to security features like NoScript and AdBlockPlus. The rise of Mozilla and Firefox has been nothing short of amazing.

OSS has changed the world

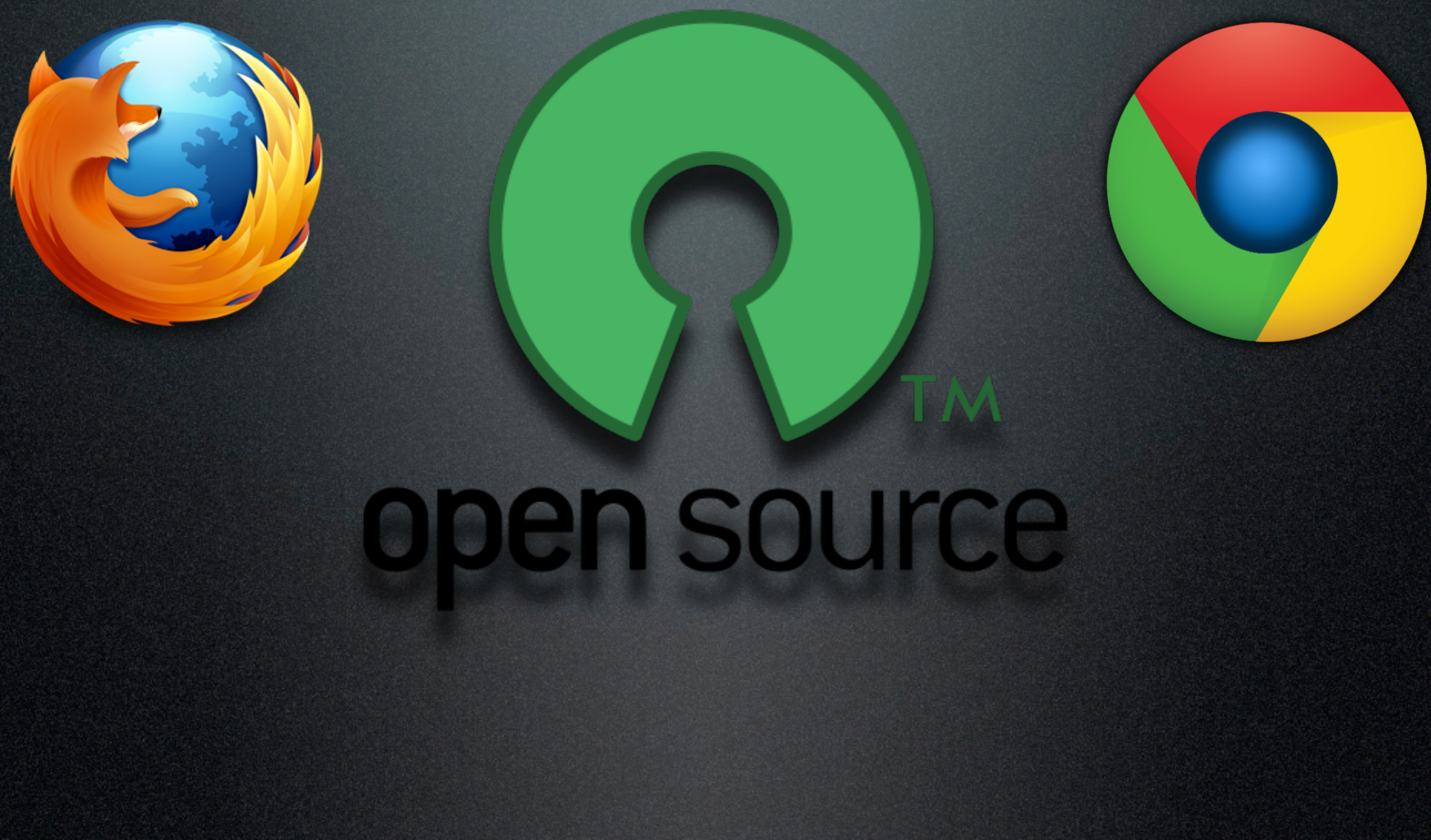


image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

image: http://static.arstechnica.net/opensource/firefox-09-intro.png
blog: http://arstechnica.com/open-source/news/2011/03/mozilla-outlines-16-week-firefox-development-cycle.ars

image: http://www.neowin.net/forum/uploads/monthly_03_2011/post-182672-0-08504800-1300415083.png
blog: http://www.neowin.net/forum/topic/981422-new-chrome-logo-coming/page__st__165

Chrome. A new competitive web browser from a small software shop in California. In it's short life has exploded in growth and caused the other browser manufacturers to up their game. It also has a large cadre of extensions; more than I'll ever be able to know about. And in many ways it may be winning the war for most secure default web browser.

OSS has changed the world

image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

image: http://static.arstechnica.net/opensource/firefox-09-intro.png
blog: http://arstechnica.com/open-source/news/2011/03/mozilla-outlines-16-week-firefox-development-cycle.ars

image: http://www.neowin.net/forum/uploads/monthly_03_2011/post-182672-0-08504800-1300415083.png
blog: http://www.neowin.net/forum/topic/981422-new-chrome-logo-coming/page__st__165

image: http://androinica.com/wp-content/uploads/2008/10/android_logo.png
blog: http://androinica.com/category/androidguide/

Android. Sorry to mention two Google products in a row, but it is unbelievable that this little robot could challenge the iPhone hegemony. I believe that Android now has the most installed handsets in the world. The other is Apple's iOS. No one even talks about RIM Blackberry or other phone operating systems any longer.

OSS has changed the world

image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

image: http://static.arstechnica.net/opensource/firefox-09-intro.png
blog: http://arstechnica.com/open-source/news/2011/03/mozilla-outlines-16-week-firefox-development-cycle.ars

image: http://www.neowin.net/forum/uploads/monthly_03_2011/post-182672-0-08504800-1300415083.png
blog: http://www.neowin.net/forum/topic/981422-new-chrome-logo-coming/page__st__165

image: http://androinica.com/wp-content/uploads/2008/10/android_logo.png
blog: http://androinica.com/category/androidguide/

image: http://linuxtea.org/wp-content/uploads/Linux-server-distros.jpg
blog: http://linuxtea.org/choices-for-linux-server-distros/

Distros. Here are the names we know and love. Ubuntu has pretty much taken over the new user, easy to install, and highly compatible Linux desktop world. I'm not a big fan of the Unity desktop, but I love me some Ubuntu.

OSS has changed the world

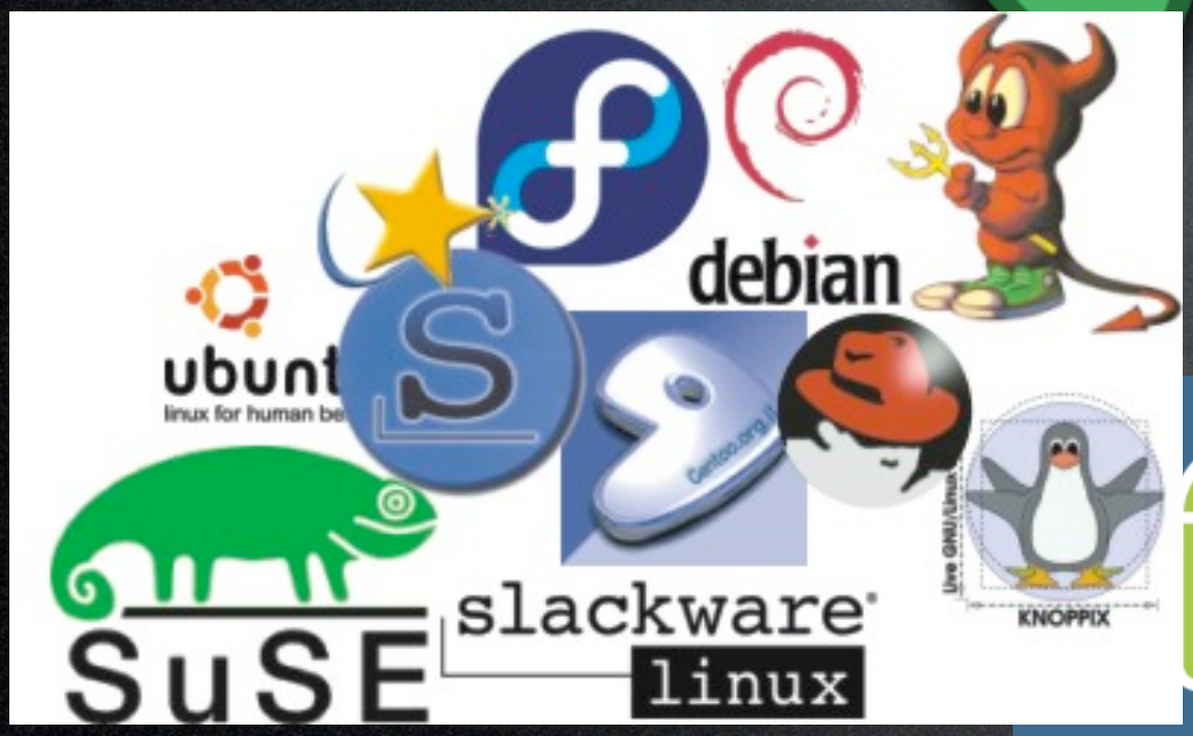


image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

image: http://static.arstechnica.net/opensource/firefox-09-intro.png
blog: http://arstechnica.com/open-source/news/2011/03/mozilla-outlines-16-week-firefox-development-cycle.ars

image: http://www.neowin.net/forum/uploads/monthly_03_2011/post-182672-0-08504800-1300415083.png
blog: http://www.neowin.net/forum/topic/981422-new-chrome-logo-coming/page__st__165

image: http://androinica.com/wp-content/uploads/2008/10/android_logo.png
blog: http://androinica.com/category/androidguide/

image: http://linuxtea.org/wp-content/uploads/Linux-server-distros.jpg
blog: http://linuxtea.org/choices-for-linux-server-distros/

image: http://www.prlog.org/11292437-open-source-cms.jpg
blog: http://www.prlog.org/11292437-open-source-cms-customization-services-at-php-developer.html

Web apps. PHP is perhaps the most common language on the web. It was used to build damn near everything. All of these popular CMSes are built from Open Source tools. Drupal, Wordpress and Joomla have probably created more jobs than anything else I've ever known. So many organizations need someone to come in, set up, customize, and train employees around these tools. This is great progress!

OSS has changed the world

image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

image: http://static.arstechnica.net/opensource/firefox-09-intro.png
blog: http://arstechnica.com/open-source/news/2011/03/mozilla-outlines-16-week-firefox-development-cycle.ars

image: http://www.neowin.net/forum/uploads/monthly_03_2011/post-182672-0-08504800-1300415083.png
blog: http://www.neowin.net/forum/topic/981422-new-chrome-logo-coming/page__st__165

image: http://androinica.com/wp-content/uploads/2008/10/android_logo.png
blog: http://androinica.com/category/androidguide/

image: http://linuxtea.org/wp-content/uploads/Linux-server-distros.jpg
blog: http://linuxtea.org/choices-for-linux-server-distros/

image: http://www.prlog.org/11292437-open-source-cms.jpg
blog: http://www.prlog.org/11292437-open-source-cms-customization-services-at-php-developer.html

image: http://www6.bibl.ulaval.ca:8080/etd2006/pages/papers/Art_Ryhno/pix/icons.jpg
blog: http://www6.bibl.ulaval.ca:8080/etd2006/pages/papers/Art_Ryhno/oss.html

Databases, programming languages, office suites. Open source has ultimate penetration.

OSS has changed the world

image: http://upload.wikimedia.org/wikipedia/commons/thumb/4/42/Opensource.svg/500px-Opensource.svg.png
blog: http://en.wikipedia.org/wiki/File:Opensource.svg

image: http://oss.sgi.com/LDP/linuxfocus/common/images/illustration129.gif
blog: http://oss.sgi.com/LDP/linuxfocus/English/March2000/article147.shtml

And the grand daddy of them all, Apache. All I can say is, “Thank you, Apache Foundation and all you tireless developers” for building the best web server the world has ever seen. Apache basically runs the World Wide Web.

So, all of this combined with embedded Linux, PLCs, and everything else that Open Source has touched means that the battle is already won. You don’t need to fight for Linux adoption. It is already there. (Perhaps just under the covers). Running stable systems all over the globe.

Use Virtualization to Learn

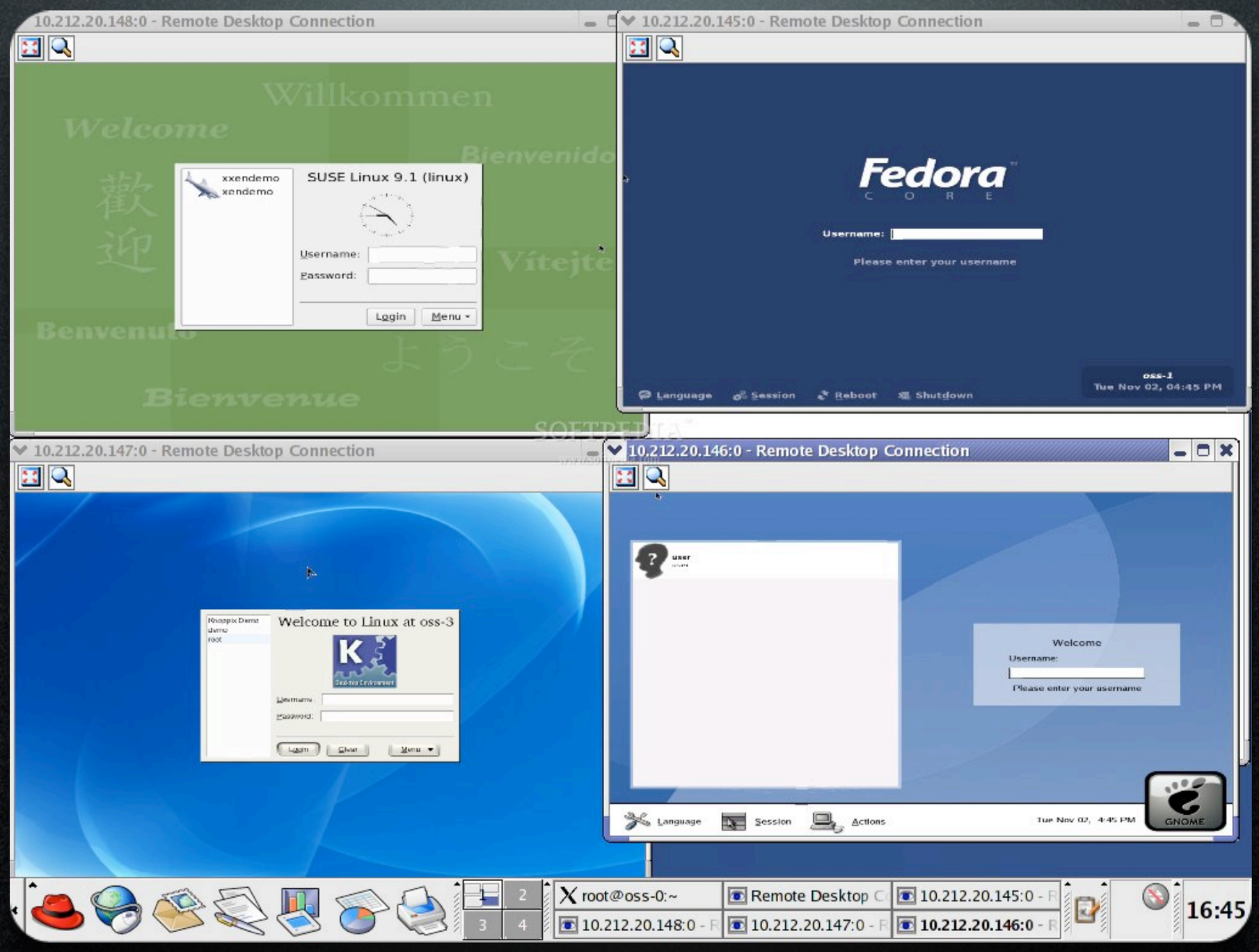


image: http://ostatic.com/files/images/1_5_2.jpg
blog: http://ostatic.com/blog/xen-org-delivers-version-3-3-of-the-xen-hypervisor

WORK WITH OSS TOOLS AND VIRTUALIZATION TO GAIN VALUABLE EXPERIENCE

Virtualization is like an avalanche and if you aren't already caught up in it, then you should be. Companies everywhere are deploying this technology to scale down the amount of hardware they need to run, to save energy, and to consolidate systems. Green computing is a huge initiative right now, especially in the government sector. You need to start learning it in order to use its great power to your advantage.

However, despite all of the advantages, virtualization does pose some potential security risks. One big risk is the idea of multi-tenancy. This is when you have many different customers on your VM server and all of their data resides in different silos. What happens if a bad actor is able to jump silos? It also creates headaches for IT auditors, and groups like the PCI Security Standards Council have had to revisit their assessment techniques in order to address these issues. But anyway, that is a big topic and I'll save it for another day.

Use Virtualization to Learn

image: http://www.unitrends.com/blog/wp-content/uploads/2012/02/xen_logo_small.png
blog: http://www.unitrends.com/blog/backup-and-xen/

image: http://www.linux-kvm.org/wiki/skins/kvm/kvmbanner-logo2.png
blog: http://www.linux-kvm.org/page/Main_Page

image: http://www.linux-mag.com/s/i/topics/virtualbox.jpg
blog: http://www.linux-mag.com/id/7949/

image: http://www.linux-kvm.com/sites/default/files/qemu_logo.png
blog: http://www.linux-kvm.com/content/upstream-qemu-0124-released-bug-fixes

image: http://www.hpsoftwareuniverse2009.com/hpswu/images/sponsorLogos/v2/logo_vmware.gif
blog: http://www.hpsoftwareuniverse2009.com/hpswu/controller.cfm?view=sponsor.dspExhibitorsLogos

For now, I just want to get across that there are many ways to play with virtualization and some of the best of these tools are free. One of the earliest and most mature players has been Xen. The latest one I've had a chance to work with was KVM, which I believe is a loadable module in the Linux kernel. Venerable QEMU, which I first heard about at a TriLUG meeting perhaps 10 years ago, is still available.

Sun Microsystems has introduced VirtualBox, which I believe they produced as a challenge to VMware. When this product first came out, I was frustrated by many of its limitations, but in the past few years it has improved substantially. And of course I have to mention VMware, since they are the de facto standard in the virtualization world. You can download and use VMware Player for free and it is an awesome tool.

The big advantage here is that this allows you to spin up environments and play around without damaging your host system. You are freed up to try new things and experiment with new tools which you may have not used before. And if there is a segment of the software world that you'd like to work in or develop for, then using VMs of Open Source systems can give you experience you need to answer questions in interviews or to build the next great technology.

image: http://i44.tinypic.com/9055yu.jpg
blog: http://www.geekpolice.net/t9574-remove-the-warning-your-re-in-danger-wallpaper-removal-guide

Wait. Is this talk about information security or not? Why, sure it is! As you can see from this slide, if you get a screen like this on your computer, then your're in danger! All of your activity is being logged and can be viewed by anyone. Probably best to click on that pop-up and download whatever security program that it recommends!

Diversify & Diagnose

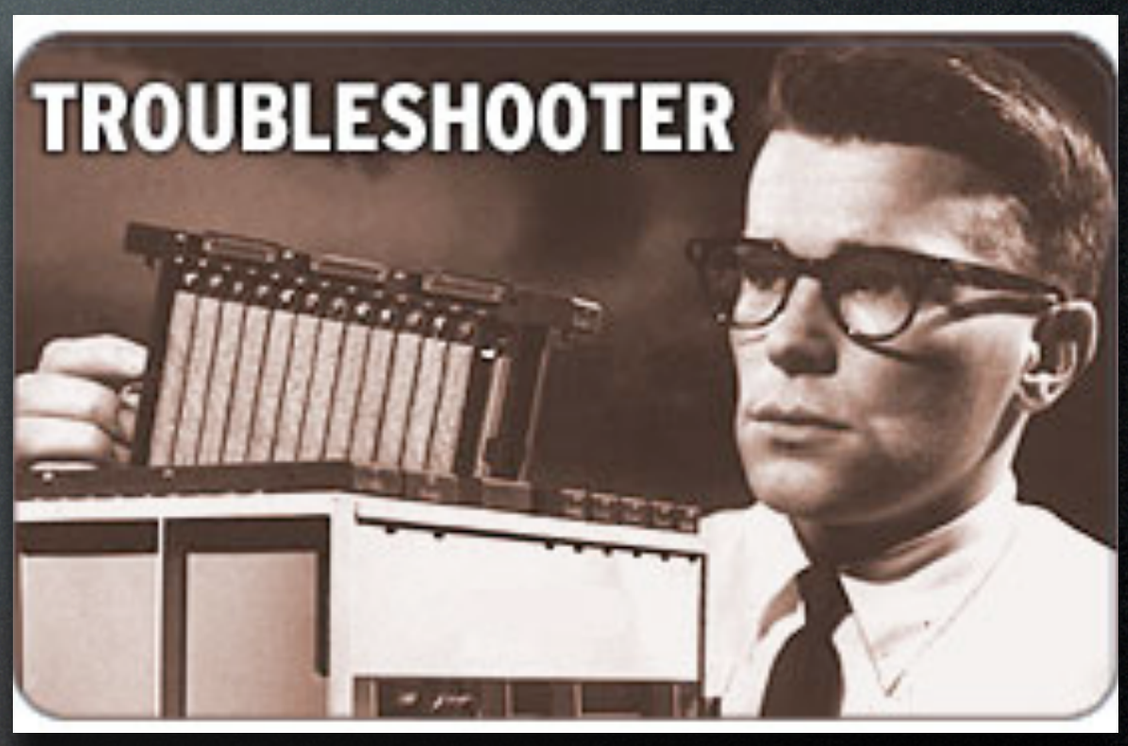


image: http://blogs.smh.com.au/mashup/images/headshot_troubleshooter.jpg
blog: http://blogs.smh.com.au/mashup/archives/troubleshooter/

Moving on to my bullet point number 7. Learn a little bit about everything and be a good troubleshooter. You want to be technically well rounded and able to solve random difficult problems. This is one arena where being a Linux user puts you at an advantage. I have always been thankful for my background in Linux and Unix administration because the practice of installing your own OS and hunting down dependencies and library issues, etc has always been an advantage in the troubleshooting realm. Same thing goes for file permissions. Not many folks in the Windows world understand that stuff, so be proud of your intense geekdom.

The point is, you don't have to become an expert in everything, but you can learn a little bit and broaden your horizons. This will make you a better IT employee and much more valuable to your organization.

Learn about SIEM & Logging

image: http://www.ltidata.com/images/ltimages/security_virus.jpg
blog: http://www.ltidata.com/technologies/optimization/SIEM.html

image: http://www.wiosnek.pl/images/logo3.jpg
blog: http://www.wiosnek.pl/?page_id=38

image: http://labs.alienvault.com/labs/wp-content/uploads/2011/09/av_labs_logo_small2.jpg
blog: http://labs.alienvault.com/labs/

image: http://www.splunk.com/web_assets/v4/diagrams/diagram_wheel.png
blog: http://www.splunk.com/view/change-monitoring/SP-CAAACP2

So my bread and butter these days has been SIEM logging infrastructures that house billions of log records and produce pretty reports for management about what nasty folks are doing on their systems. If you like looking at logs all day, then you can get some experience in the SIEM world via Open Source or low cost programs.

A few years ago there was a project called OSSIM. Or Open Source SIM. It was a bit clunky to set up, but the underlying technology was so good that a company named AlienVault bought them to incorporate into their SIEM product. Thankfully, AlienVault still has a free version of the product available and it is a great way to get some hands-on experience working with an intelligent log solution.

The next one I'll mention is Splunk. Splunk used to be much more free, until they saw the value their product was bringing to customers. Then suddenly their license agreements changed and the cost of the product rose quickly. However, they do still offer a free version, which I believe is limited to around 750MB of logs per day, but this product is fantastic. Splunk is often called the "Google" of log systems because of the easy-to-use search interface. It is very user friendly and the built-in functionality has grown to challenge many larger SIEM vendors. I highly recommend this product to tinkerers, as well as small and medium businesses.

Learn about IDS

SURICATA

image: http://4.bp.blogspot.com/_2IvFH57W8Hc/TPfpzDtwQwI/AAAAAAAAAFk/YFngxr8jLgI/s1600/snort_large.gif
blog: http://insidetrust.blogspot.com/2010/12/how-to-use-snort-on-backtrack-4-basic.html

image: http://www.bro-ids.org/images/bro-eyes.png
blog: http://www.bro-ids.org/

image: http://blog.securitymonks.com/wp-content/uploads/2010/01/suricata.png
blog: http://blog.securitymonks.com/2010/01/05/suricata-a-next-generation-idsips-engine/

image: http://www.ossec.net/img/ossec-hids-1000x350.jpg
blog: http://www.ossec.net/main/ossec-logos

In the world of Intrusion Detection Systems, Snort is king. This little project has grown into a huge, multi-million dollar outfit called SourceFire, but like many of these fantastic security products, they still offer a free Open Source version. Snort was designed to hunt for and alert on anomalies found from a TCPdump session and it is expert at doing so. Essentially, the product is hard to beat.

But that doesn't prevent many vendors from trying to do so! Other new challengers in the IDS arena include Bro IDS and Suricata. They are both trying to develop new engines that will outperform Snort and this competition is good for the IDS ecosystem.

HIDS or Host-based Intrusion Detection Systems are quite powerful ways to lock down a server or workstation. Mostly they work to restrict what applications can be executed on that host, but many also employ heuristics to learn and alarm on abnormal user activity. OSSEC is a program written by Daniel Cid and is one of the most highly recommended HIDS. It is also free and Open Source.

Learn about Vuln Scanning

image: http://blog.tenable.com/.a/6a00d8345495f669e20133f445cc65970b-pi
blog: http://blog.tenable.com/

image: http://www.lotautbrian.fr/wp-content/uploads/2012/01/openvas_logo-e1325892055577.png
blog: http://www.lotautbrian.fr/

image: https://www.rapid7.com/register/nexpose/nexpose-community.png
blog: https://www.rapid7.com/products/nexpose-community-edition.jsp

Vulnerability scanning is pretty cool stuff and I've had the opportunity to do quite a bit of it in my past as a system auditor and assessor. Basically it involves running a very smart tool against your systems which can piece together information to ascertain the operating system type and version, the open ports and running services, and decipher known software vulnerabilities running on a given host. This is what the bad guys use to take you down. That is why it is much better to perform this yourself (or have a qualified third-party do it) prior to someone else finding the holes.

Nessus was an Open Source project and it challenged the best of breed in the vuln scanning world. The product was so good, that it was bought by Tenable a few years ago and they started charging $1200 per year to license and use it. However, you can still download and use Nessus for personal use. They just released Version 5 this week and I cannot wait to test it out!

When Nessus went corporate, a fork called OpenVAS sprung from its fan base. So if the Nessus licensing bothers you that much, you can find and use a more free version.

Some of you may be familiar with a company called Rapid7. They have an enterprise grade vuln scanner called Nexpose. If you'd like to download it to compare to other tools, they offer a free version called Nexpose Community. I highly recommend this product, as well.

Learn about Pen Testing

image: http://www.h-online.com/imgs/43/6/7/7/0/2/6/Metasploit_Logo_200-8d609940eb489a73.png
blog: http://www.h-online.com/open/news/item/Metasploit-offers-bounty-for-exploits-1261263.html

image: http://portswigger.net/images/PS_logo.png
blog: http://yossi-yakubov.blogspot.com/p/tools-for-penetration-testing.html

image: http://w3af.sourceforge.net/images/v1.png
blog: http://w3af.sourceforge.net/

image: http://cdn.linuxforu.com/wp-content/uploads/2011/06/samurai.jpg?d9c344
blog: http://www.linuxforu.com/2011/06/web-app-penetration-testing-with-samurai/

Pen testing. This is everyone's new baby. Everyone wants to be a Pen Tester because they are the elite bad ass hackers of the universe. It's true. Penetration Testing is a very difficult to acquire and completely cool set of skills to possess. Some folks think that running a vulnerability scan and pointing a DOS attack at a web server is pen testing. It is not. These guys (and gals) are Python wrangling, exploit breathing, ph33r inducing maniacs. I do not want to anger any pen testers! Cuz they will school you.

HD Moore is a world famous amazing hacker who wrote and fostered a program called Metasploit. It is now the most widely used and extensible attack framework on the planet. The program is designed to target a host, and use your knowledge of its vulnerabilities to find a way in, then provide you a root shell to do whatever you'd like. This is how you win in Capture the Flag. You pop a root shell on the box and you own. It is a very satisfying feeling.

Metasploit is so awesome-tastic that Rapid7 bought them and gave HD a huge budget and tons of hackers to further improve the product. Again, although you can spend lots of dough on Metasploit Express and Metasploit Pro, you can still download and use the basic program for free. I'm not a programmer, but in my estimation, it is one of the best-developed tools around.

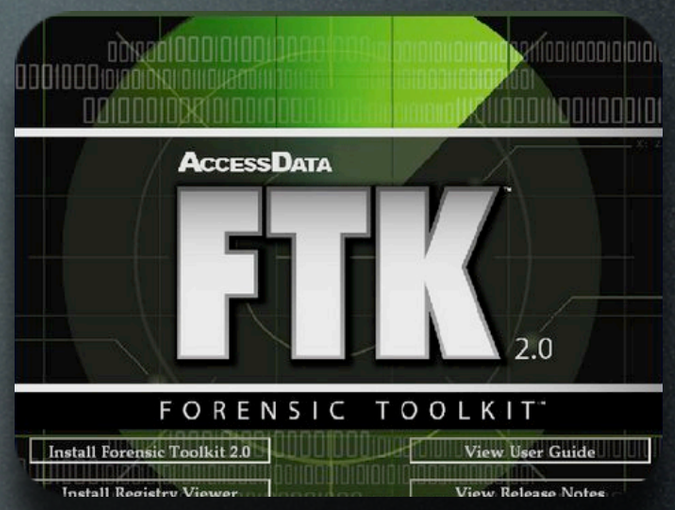
Another competitor in this space is the Burp Suite set of tools released by PortSwigger. Burp Suite is a for-pay toolset, but some of their modules are still free, like Burp Proxy. These are often listed amongst the favorites of pen testers.

There are tools designed to throw a huge number of attacks against a web application and see what causes it to break. Cenzic is a big player in this market with their Hailstorm product. However, you can get a quite good product for free to do this from the w3af project. Takes a little time to set up and configure, but would provide you great experience in testing web apps.

Finally, Samurai from InGuardians is another pen testing tool making strides. It is fairly new and I haven't had a chance to play with it yet, but I promise to know more about it by the next time you see me. The people who wrote it are great and are my personal idols in the information security industry.

Learn about Forensics

vs



SUMURI
Forensics Simplified

HELIX 3 ENTERPRISE

SANS SIFT Toolkit

EnCase logo belongs to Guidance Software. FTK logo belongs to AccessData.

image: http://www.cellebrite.com/images/stories/partners/sumuri.JPG
blog: http://www.cellebrite.com/mobile-forensics-products/ufed-training/173-us-training-partners.html

image: http://www.sumuri.com/cart/img/p/20-109-thickbox.jpg
blog: http://www.sumuri.com/cart/product.php?id_product=20

image: http://www.macforensicslab.com/ProductsAndServices/images/icon_sleuthkit.jpg
blog: http://www.macforensicslab.com/ProductsAndServices/index.php?main_page=document_general_info&cPath=10_15&products_id=67

image: https://www.e-fense.com/images/logo_h3enterprise.gif
blog: https://www.e-fense.com/products.php

blog: https://computer-forensics.sans.org/community/downloads

Another hot topic in the security world right now is Forensics. This is essentially picking through the millions of files on a host to find the one or two indicators of compromise. These are “after-the-fact” tools, meaning you’ve already been owned, incident handlers have taken your system offline, and now we’re running forensic tools against it to find out what happened. EnCase from Guidance Software and FTK from AccessData are the gold standards in this competitive industry.

That doesn’t mean you can’t get world-class forensics experience for cheap, however! There is a great software company out there called Sumuri and they’ve been working on Paladin Forensics OS for years. It is a live boot Linux CD and it works incredibly well. They just released Paladin 2.0 and offer it for a low cost on a USB drive, so you can swoop in with your USB key and get your forensics on!

The Sleuth Kit has been around for quite a while and is actively developed. Their Autopsy Browser is a graphical interface to many forensic tools, which makes them a bit easier to learn.

Back in the day, HELIX was a live boot Linux CD that was a leader in forensics. So much so that it became a for-pay product and no longer offers a free version. I’ve heard rumors that somewhere on the Internet a link to the old free version exists, but I don’t know about it. Still, it has been a historically excellent forensics program and is still quite affordable.

The last one I’ll mention is the SIFT toolkit from the SANS Institute. SANS does security training and Rob Lee is one of their instructors (also a Principle at Mandiant). He along with others have developed this fantastic forensic platform. However, SANS is very touchy about their intellectual property so I decided to not include any official logo for them. That shouldn’t discourage you from checking out this tool if you can!

Learn about Encryption

image: http://u.jimdo.com/www14/o/s9adb9cff63ef4173/img/i8b899a8894467e04/1279288698/std/image.jpg
blog: http://www.truecrypt.org/

You're all encrypting your data, right? Both in transit and at rest? I understand if you haven't, but a completely free way to encrypt volume container or entire disks is with TrueCrypt. It is a great tool and you should check it out ASAP. There are lots of corporate disk encryption tools, ranging from stuff built into anti-virus suites like BitDefender to RSA grade encryption, but they cost real money. TrueCrypt is free and cross platform. It is so good I didn't even put other products on the slide.

Learn about Everything

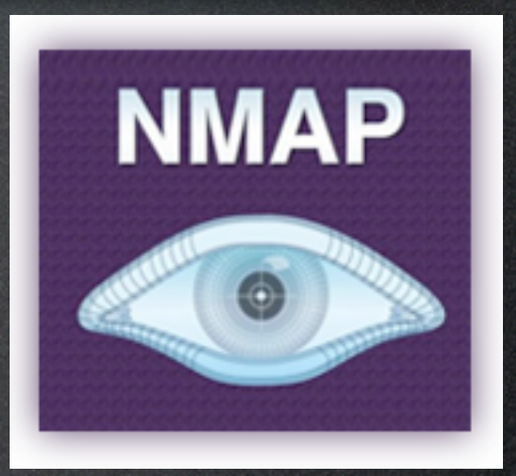


image: http://www.hoggnet.com/NWWPics/Security-Onion.png
blog: https://www.networkworld.com/community/blog/peeling-security-onion

image: http://technopolis.ir/uploads/backtrack-logo-164x164.png
blog: http://www.backtrack-linux.org/

image: http://www.techbabu.com/wp-content/uploads/2010/01/nmap_diff_logo.png
blog: http://www.techbabu.com/2010/01/scan-your-network-with-nmap-and-ndiff/

Some tools are so good, so vast, that they literally afford you the opportunity to learn everything. I stand in awe of the folks who put these things together and am constantly thankful for their brilliance and generosity. These are essentially Super Tools – they either incorporate many of the best tools, or are so multi-faceted that even experts have to spend considerable time learning them.

The new one on the block is called Security Onion and was created by Doug Burks, a respected leader in the security world. Security Onion is a Linux distro which has Intrusion Detection and Network Security Monitoring wrapped into one. It's based on Xubuntu and contains many tools I've already mentioned like Snort and Suricata. It incorporates a variety of other tools to make packet crafting and intrusion analysis better, such as Sguil, Squert, Xplico, tcpreplay, scapy, and hping. Security Onion is the darling of the hacker community right now.

The next weaponized suite of tools I'd like to mention is BackTrack Linux. This distro has been around for a long time and back in the day it was called Auditor. It was scary back then and is downright evil these days. Want to hack wireless? Check this out. Want to hack databases? It's in there. Want to have every top notch hacker tool at your disposal? Look no further than BackTrack. I always have a fresh ISO of this in my toolkit.

Finally, the "simple" network mapping tool that started this whole hacking craze. Nmap. All it does is scan networks and report open ports, right? Not hardly. Nmap can be used for stealthy network scanning, open port detection, OS guesstimation, and a bunch of other things. I've been using Nmap for over ten years and still haven't scratched the surface. Fyodor, Nmap's developer released a book two years ago called Nmap Network Scanning and it is now a reference standard for learning about network security. Another free and Open Source tool that is completely amazing.

Moar Security Tools?

Visit Fyodor's site http://sectools.org/

image: http://sectools.org/images/sitelogo.png
blog: http://sectools.org/

You need more security tools, you say? Well, Fyodor has been kind enough to create a site called sectools.org where he keeps track of the best and ranks them on a regular basis. Check it out if you exhaust the list of tools I just gave you.

What to test on?

image: http://img208.imageshack.us/img208/600/vmwarev.jpg
blog: http://www.dragonjar.org/metasploit-presenta-metasploitable.xhtml

image: http://www.red-blue.it/wp-content/uploads/dvl.jpg
blog: http://www.red-blue.it/linux/damn-vulnerable-linux-ovvero-tutto-cio-che-un-os-non-dovrebbe-essere.html

image: http://blog.hazrulnz.net/wp-content/uploads/2009/03/webgoat_logo-294x300.jpg
blog: http://blog.hazrulnz.net/1455/webgoat-exploit-and-learn.html

It should be mentioned that you are not to use these tools on systems you do not own or manage. Doing so is dangerous and likely in violation of the law. I am in no way endorsing that you use any of these tools for “cracking” or system intrusion purposes.

Besides running a scanner against your own home system, you can set up a variety of target hosts to test out your skills on. There is a VM called Metasploitable that is made for people to attack with the Metasploit tool. Besides this, you could also set up a new host (virtual or physical) running Damn Vulnerable Linux or Web Goat. All of these are free and provided by the community for you to learn on.

I hope that was a good overview of available tools for you to learn a little more about the security world. Playing with software such as this can broaden your horizons and help you troubleshoot networks and applications. You could also become a world famous elite hacker overnight!

Embrace Change

image: http://www.organize-utah.com/wp-content/uploads/2009/07/change-is-the-only-constant.jpg
blog: http://ayagebeely.blogspot.com/2009/09/embrace-change.html

The key here is to understand that nothing is constant, especially in the security world. What we think of as secure one day is completely hackable within 24 hours. The complexity of today's computer systems is so high that few humans can understand them, and all who work on them are prone to error. We all make mistakes. We all get hacked from time to time. You have to learn to deal with this.

A broader application of the 'embrace change' idea is to not get too pigeon-holed in your career goals. If you want to focus on a given programming language or technology, that is great! It is nice to be expert at something and be able to make a living and teach those around you. However, always keep your eye on the future of your industry and what new challengers are coming along. The computing landscape does not remain constant and you cannot just stand in one place.

Always keep learning and improving. Always keep asking questions. Always have your friends and coworkers challenge your work and find ways to improve. This playful and spirited take on change will be to your benefit. Keep moving!

Don’t You Forget About Me

image: http://cdn.stereogum.com/files/2009/08/john-hughes-breakfast-club.jpg
blog: http://stereogum.com/83411/dont_you_forget_about_me_remembering_john_hughes_m/video/

Remember those people you networked with way back when? Your roommates in college? The people who got you your first jobs or helped you along the way? The folks who answered your n00b questions or walked you through your early programming challenges? You owe them a phone call or an email from time to time. Maybe you should set up a lunch meeting and treat them, if you can afford the tab. At the very least, you should ask them how you can return the favor and offer them help to improve their careers. To improve their lives. Build those lasting connections and foster them for the long run. Don’t just add them as “Friends” on Facebook and forget they exist.

This is a difficult thing to accomplish. We all get busy with our day-to-day work lives, with our families and obligations. But it is essential, both for our careers and for our well-being, that we maintain these personal links. It may sound crazy to you now, but believe me – it will be to your advantage. Be a good friend. People will remember a good friend and want to help you out when you need it. I am thankful every day to have had so many wonderful mentors and confidantes in my life.

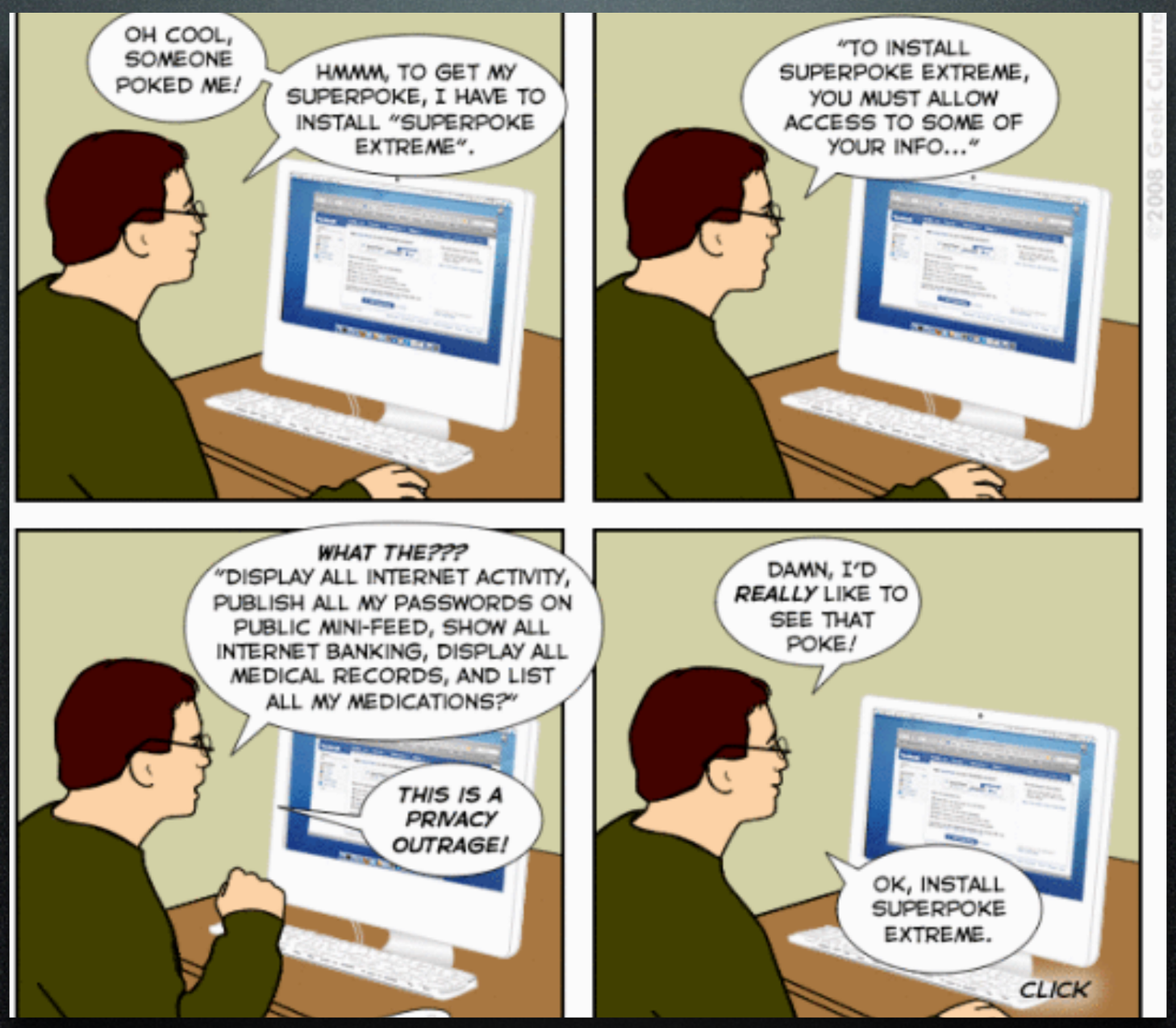
Holistic Security

image: http://www.lavazzaarticle.net/wp-content/uploads/2011/08/Computer-Security-Posters-4.jpg
blog: http://www.lavazzaarticle.net/tag/computer-security-posters/

My final point is to encourage you to incorporate security into everything you do. This includes your work at your IT job, your interactions with people in the real world, and extends to your online networking. Be careful of social network oversharing that could upset people or anger your boss. Learn how to negotiate with others so that you are both winning and satisfied with the outcome. Work with others in a positive manner which makes trust bonds deeper. And don't use the same password across all the sites you log into on the Web!

This idea of holisitic security will benefit you, make you a valuable employee, and hopefully keep you out of trouble. Learn about the world around you… And think before you act.

Social Networking Survey



"Social Networking Privacy and Security Survey 2012"

https://www.surveymonkey.com/s/XDRY6FK

image: http://cultureandcommunication.org/tdm/nmrs/sp2/files/2011/04/Facebook-Privacy-300x2871.gif
blog: http://cultureandcommunication.org/tdm/nmrs/sp2/2011/04/10/privacy-and-social-networking-why-we-trust-facebook/
orig: http://www.joyoftech.com/

As I mentioned at the beginning, I'm currently running an online survey of social network users to gauge how they feel about privacy and what behaviors they exhibit regarding these feelings. In the past, I've spoken to many companies and organizations about risks and rewards of social networking and have provided them with guidance. When I do this work for a company, the intellectual product belongs to them and I cannot share it with another group. So I'm doing this as a way to gather my own independent data set and write an analysis of the results. I do plan to share this write up on my blog and with groups I speak to in the future. Your participation would greatly help me out.

Thank you!

David Matusiak

http://matusiak.org

http://twitter.com/matusiak

"Social Networking Privacy and Security Survey 2012"

https://www.surveymonkey.com/s/XDRY6FK

image created via: memecreator.net

I really appreciate the opportunity to be here today and present to y'all at the 2012 NCSU Free and Open Source Software Fair. Please let me know if you have any questions.