FOSS Enterprise Security Solutions

Free and Open Source Software
Enterprise Security Solutions

Joseph Guarino
Owner/Sr. Consultant
Evolutionary IT
http://www.evolutionaryit.com

Copyright © Evolutionary IT 2008

Who am I?

- Joseph Guarino
- Working in IT for last 15 years systems, network, security admin, technical marketing, project management, IT management, etc.
- Full time IT consultant with my own firm Evolutionary IT
- CISSP, LPIC, MCSE, PMP
- www.evolutionaryit.com

Copyright © Evolutionary IT 2008

?

- How many of you are familiar with or use FOSS in some way?

Copyright © Evolutionary IT 2008

Goals

- What is this FOSS stuff?
- Where did FOSS come from?
- Why FOSS as a model works and just generally rocks!
- Clear up some FUD.
- Overview of tools a system, network, security administrator can use.

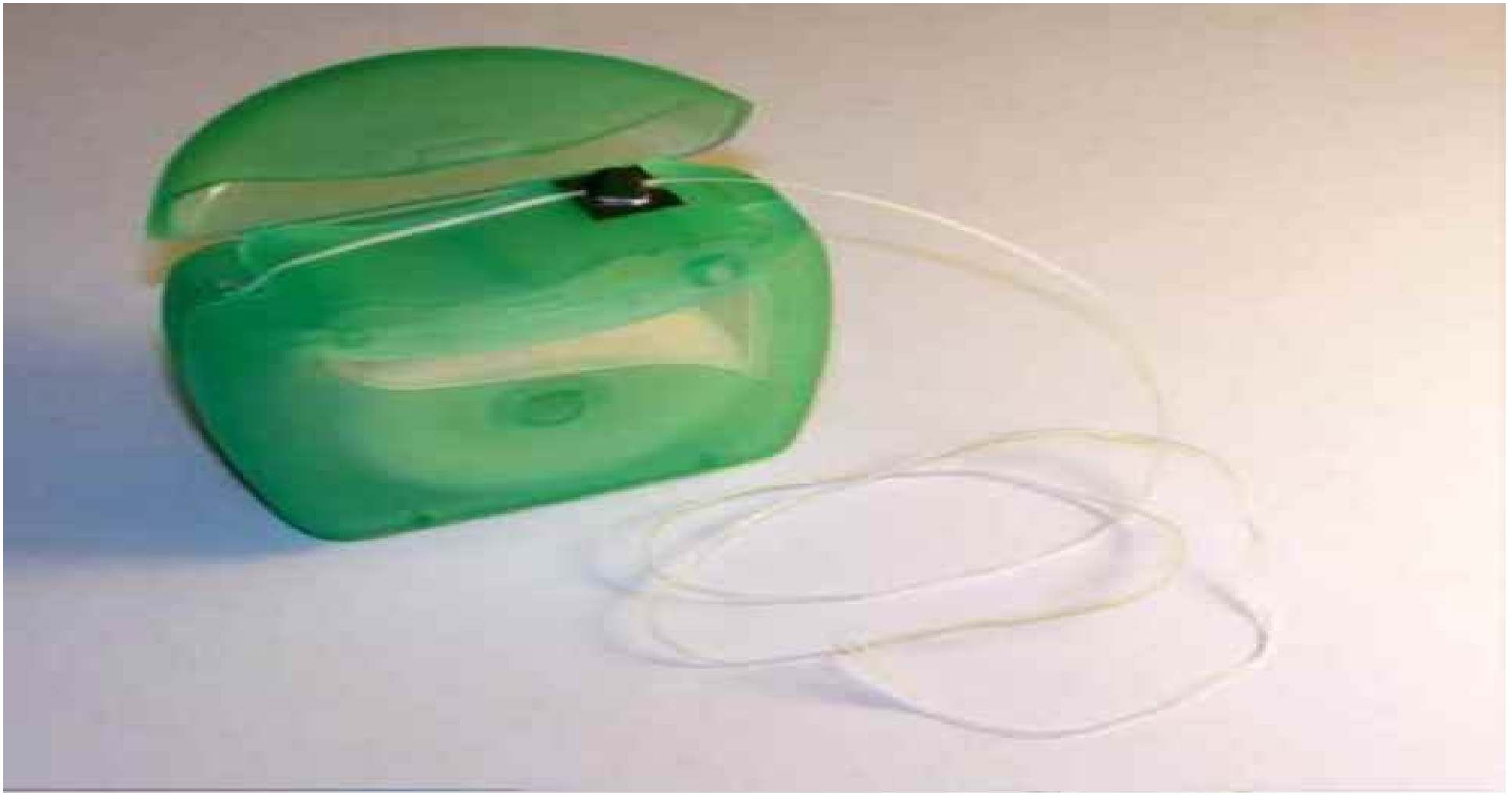
Copyright © Evolutionary IT 2008

What is FOSS/FLOSS?

- Free and Open Source Software
- FLOSS or Free/Libre/Open-Source Software.
- Libre is used to clarify the ambiguity of the word free in English.
- Alternative term to describe software spectrum from free to open.

Copyright © Evolutionary IT 2008

Dental Hygiene?



Copyright © Evolutionary IT 2008

What is FOSS?

- Represents a spectrum of licenses from Free to Open.
- FOSS (Free and Open Source Software) is a software licensing model that allows anyone the liberty to use, extend and distribute the software as they see fit.
- FOSS is unique as well in that it produces innovation quickly by the very concept of open, cooperative, collaborative sharing and development.
- Commercial software is much more restrictive.

Copyright © Evolutionary IT 2008

FOSS vs. Commercial

- Licensed with very specific rights associated with its use, modification, distribution and use that are not commonly available to a user via commercial “closed” software.
- Software licenses of traditional commercial software define specific permission, rights and restrictions.
- Licensee determines the license terms.
- Much more restrictive that FOSS.
- Freedom, sharing, collaboration are not inherit parts of this traditional “closed” model which typifies the traditional software industry.

Copyright © Evolutionary IT 2008

What FOSS is NOT

- ≠ Freeware
- ≠ Shareware
- ≠ Public Domain Software
- ≠ Doesn't contain malware, spyware, etc.
- Community standards.

Copyright © Evolutionary IT 2008

History

How it all started....

Copyright © Evolutionary IT 2008

?

Where did it come from?

Copyright © Evolutionary IT 2008

Was it any of these people?

Copyright © Evolutionary IT 2008

Or perhaps?

Copyright © Evolutionary IT 2008

Maybe...

Copyright © Evolutionary IT 2008

Seriously

It's an amazing story...

Copyright © Evolutionary IT 2008

FSF & RMS

- FSF – Free Software Foundation
- Founded in 1983 by Richard Stallman with the goal of creating a free Unix like OS, GNU Project.
- Consummate computer scientist/hacker who created Emacs, GNU Complier, GNU Debugger.
- Spearhead the efforts of Free Software movement.

Copyright © Evolutionary IT 2008

Free Software Definition

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and adapt it to your needs (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to improve the program, and release your improvements to the public, so that the whole community benefits (freedom 3).
- Access to the source code is a precondition for this.

Copyright © Evolutionary IT 2008

FSF & RMS

- Created several copyright license such as the GNU/GPL which is the most popular FOSS licenses.
- Patent reforms are also critical to RMS and the FSF.
- Free as in Freedom. Price is not the issue. Uncompromising stance on free software and patents.
- Doesn't like the term Open Source.
- http://www.fsf.org/

Copyright © Evolutionary IT 2008

Enter the Linus

- Linus Torvalds in 1991 creates first Linux kernel.
- Released in 1992 under GNU/GPL
- Kernel + GNU Project (systems libs/utils) = GNU/Linux
- Now kernel project coordinator and keeper of Linux trademark.
- Neutral on Free Software and more focused on quality.
- Differs with RMS.
- http://www.kernel.org/

Copyright © Evolutionary IT 2008

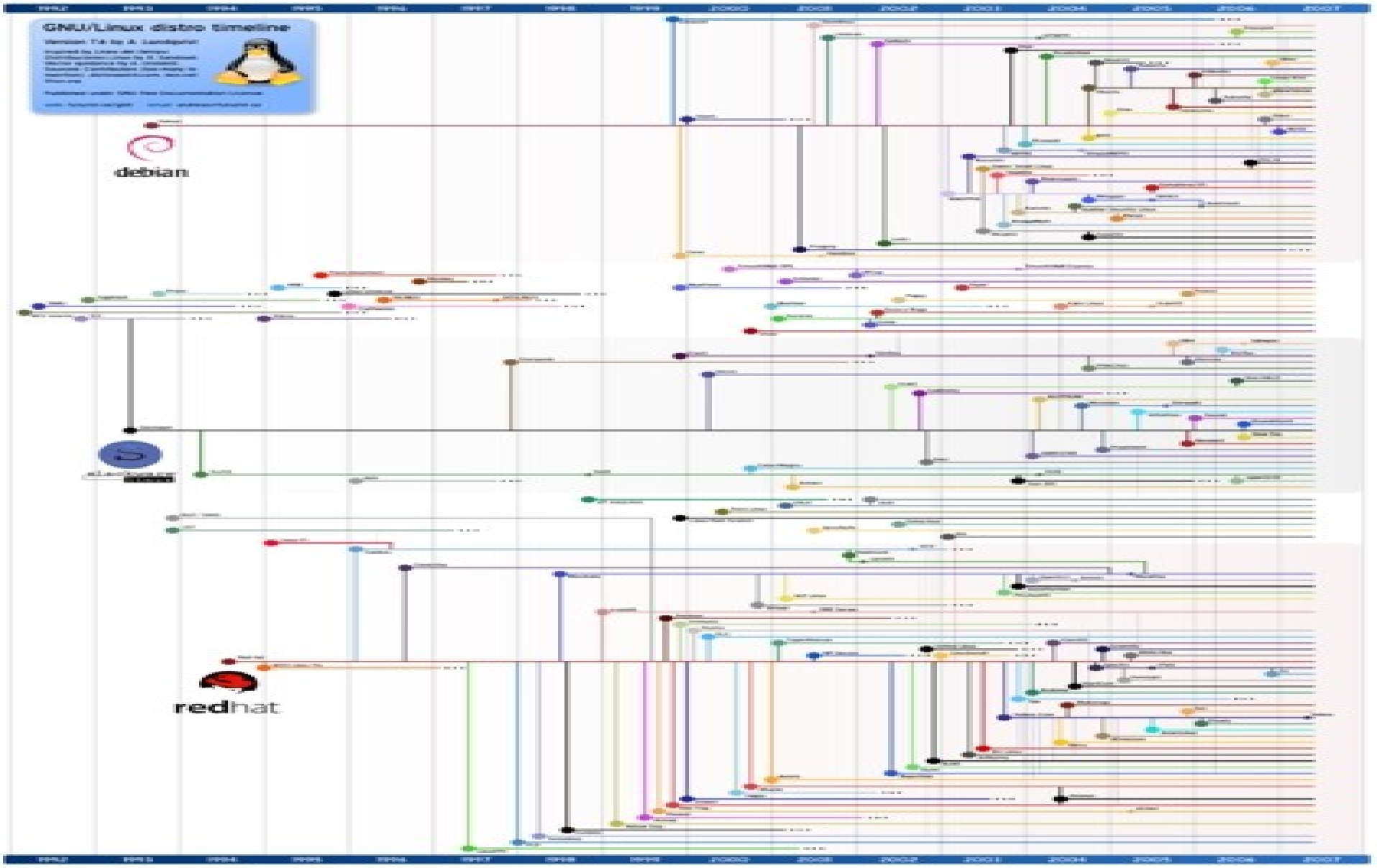
Early Days

- Kernel licensed under GNU/GPL propelled interest, innovation and ingenuity of FOSS community.
- The Linux Kernel plus the systems utilities and libraries from the GNU project yielded Linux in many forms.
- Early distributions such as Debian & Slackware appeared in 93.
- Evolution of GNU/Linux.....

Copyright © Evolutionary IT 2008

evolutionaryIT
BEST PRACTICE IT

Linux Evolutionary Time line



Perception & Ambiguity of Free

- Free software inherently supports capitalism and free enterprise within the context of it supporting free software.
- Problem was the term “free” was not helpful in selling software.
- If its “free” what would you be buying? Ugh!
- Who would champion such a cause?

Copyright © Evolutionary IT 2008

And along came the OSI

- OSI – non-profit created in 1998 by Bruce Perens & Eric Raymond to promote “open source.”
- Open source was a repositioning of free software with a term that was to clear up the ambiguity seen in the term free.
- Attempt was to make free software provide a more business friendly effort.
- Uphold and promotes Open Source Definition.
- http://www.opensource.org/

Copyright © Evolutionary IT 2008

Many Licenses

- There are many FOSS licenses each which allow different rights and responsibilities
- Most popular are GNU General Public License, GNU Lesser General Public License, BSD License, Mozilla Public License, MIT License and the Apache License.
- OSI Licenses – OSI Software Definition http://opensource.org/licenses/
- FSF Licenses – Free Software Definition http://www.gnu.org/licenses/

Copyright © Evolutionary IT 2008

?

- Is FOSS secure?

Copyright © Evolutionary IT 2008

FOSS & Security

- FOSS software's development models often parallel development of commercial except the code is open to audit by any and all project/community/users.
- Openness is a benefit in customization and flexibility of solutions.
- Result is quality, reliable and secure code.
- FOSS Security solutions are among the most cost effective security solutions.
- FOSS software is often the basis for innovations and evolving open and commercial closed source security solutions in the market.
- Appliance marketplace, network devices, UTM, embedded devices,etc...

Copyright © Evolutionary IT 2008

?

- Who actually uses that?

Copyright © Evolutionary IT 2008

No one uses that!?

- Redhat, Oracle, Sun, Dell, IBM, HP, Novell, Oracle, Canonical are big players behind it.
- Business, government, military, educational and scientific community, i.e. NSA, FBI, CIA, NSF, NASA, Wall Street.
- Google, Yahoo, Adobe, Juniper.
- I bet its on your corporate network, at home, in your car or phone right now.

Copyright © Evolutionary IT 2008

Distro/Os Options

- Freedom and choice yours

Copyright © Evolutionary IT 2008

OS's (Linux/Unix - Commercial)

- Linux/Unix Distros -
- Redhat - www.redhat.com
- Novell - www.novell.com
- Canonical – www.canonical.com
- Sun – www.sun.com
- Commercial support
- All of these projects have a community driven effort.

Copyright © Evolutionary IT 2008

OS's (Linux/Unix - Community)

- Debian Linux - www.debian.org
- Slackware - www.slackware.com
- Ubuntu - www.ubuntu.com
- Gentoo - www.gentoo.org
- Fedora - www.fedoraproject.org
- OpenSUSE - www.opensuse.org
- Open Solaris - www.opensolaris.org

Copyright © Evolutionary IT 2008

Operating Systems (BSD)

- FreeBSD - www.freebsd.org
- OpenBSD - www.openbsd.org
- Both are community driven but community support is available.
- No single company drives projects.
- OpenBSD has stellar security history. Project is model of success of security in the Open Source world.
- Only 2 remote holes in the default install in 10 years!
- O'Bsd brought you OpenSSH, OpenBGPD, OpenNTP and OpenCVS. =P

Copyright © Evolutionary IT 2008

Friends forever!?

Copyright © Evolutionary IT 2008

Call for collaboration

- Its my hope that we learn to work cooperatively and find our common ground across projects.
- We actually share many of the same goals.
- Communicate, find common ground and collaborate.
- With maturity & mutual respect.
- We will all be better for it!

Copyright © Evolutionary IT 2008

Now onward....

- FOSS security tools are supernumerary and are available for nearly EVERY function you might need in the enterprise.
- I double dog dare you to check out...
- http://www.sourceforge.net

Copyright © Evolutionary IT 2008

?

- Where do you use FOSS security tools in your enterprise?

Copyright © Evolutionary IT 2008

Strap in people!

Copyright © Evolutionary IT 2008

Anti-malware/virus

- Anti-malware.

Copyright © Evolutionary IT 2008

ClamAV

- GPL AV toolkit for email scanning.
- Project is the basis for many other projects.
- Ported to nearly every OS such as Linux, BSD, UNIX, Windows.
- http://clamav.net/
- Core ClamAV is applied to so many ends such as:
- MTA Scanner - for Sendmail, Qmail, Postfix, etc.
- POP3 Scanner - Any
- Web/FTP Scanner – Proxy, Apache, IPCop
- File system Scanner - NFS
- Desktop Anti-virus – ClamWin, KlamAV (KDE Front-end), ClamXav (OSX)
- Development Libraries for nearly every language
- http://www.clamav.net/download/third-party-tools

Copyright © Evolutionary IT 2008

HAVP & ClamWin

- **HAVP** - HTTP Anti-Virus proxy
- Integrates with Squid& other Proxies
- GNU/GPL
- http://www.server-side.de/
- **ClamWin** – GPL Windows Anti-Virus
- Scanning scheduler
- Automatic updating
- Outlook Add-in
- No on access scanning.
- http://www.clamwin.com/

Copyright © Evolutionary IT 2008

SPAM

Not that deliciously dubious “meat.”

Copyright © Evolutionary IT 2008

Anti-Spam – SpamAssassin

- **SpamAssassin** -
- Perl based standalone (spamc) or daemon (spamd)
- Suports Blackhole and URI Blackhole lists SURBL and URIBL.com
- SPF(Sender Policy Framework)
- Checksum based filters Vipul's Razor, Distributed Checksum Clearing House
- Apache 2.0 License
- Kerio, McAfee and many more build upon this project.
- http://spamassassin.apache.org/

Copyright © Evolutionary IT 2008

Anti-Spam - Dspam

- **Dspam**
- Statistical spam filter
- GNU/GPL
- MTA-Independent with support for Sendmail, Postfix, Qmail, Courier, and Exim to name a few.
- Bayesian filters – which take advantage of Bayes Theorem which takes probabilistic measure of an email is spam by its content (words) to determine if its spam.
- Adaptive filter – it is capable of learning.
- http://dspam.nuclearelephant.com/index.shtml

Copyright © Evolutionary IT 2008

Anti-Spam - ASSP

- **ASSP**
- Transparent SMTP Proxy filtering
- Platform independent runs on Linux, Unix, Windows, etc.
- GNU/GPL
- Works with any mail server
- Bayesian Analysis
- Whitelisting, Greylisting (Delaying)
- DNSBL (DNS Black holes), PB (Penalty Box – trapping of offending IP's)
- SPF
- http://assp.sourceforge.net/

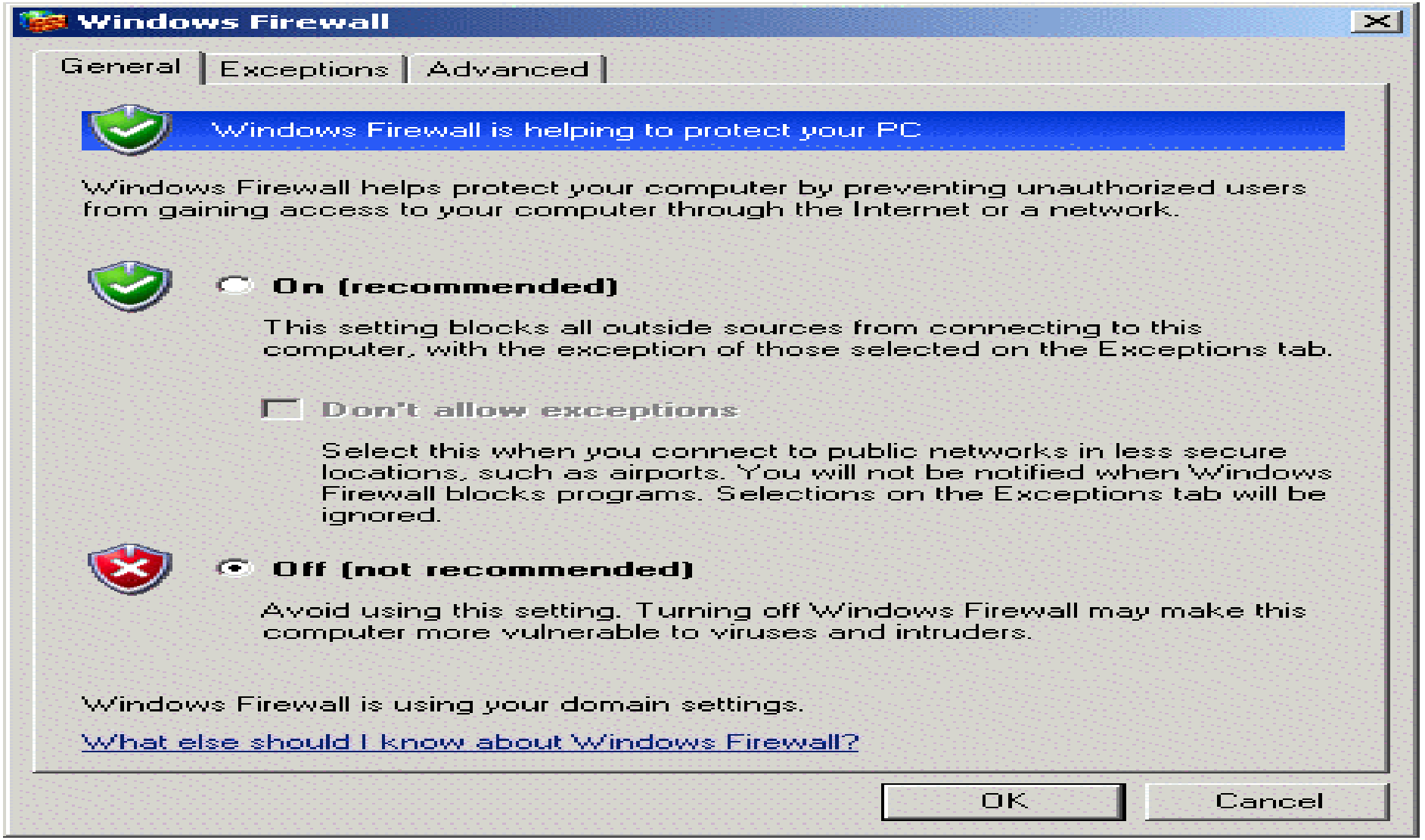
Copyright © Evolutionary IT 2008

Firewalls

- Firewhat?

Copyright © Evolutionary IT 2008

?



Copyright © Evolutionary IT 2008

Firewalls and then some

- Firewall space for FOSS is very vibrant, mature and feature rich space with many options to choose from. Can be used for Firewall, VPN, HTTP Filter, Mail Filter, etc.

- Additionally it commonly serves as the basis for internetworking devices from a variety of vendors.

Copyright © Evolutionary IT 2008

Yes!

- One can build a firewall from scratch with Linux with Netfilter/Iptables or on BSD with PF.
- There are tons of GUI tools to help you build and manage a custom firewall.
- http://www.fwbuilder.org/

Copyright © Evolutionary IT 2008

Firewalls - Monowall

- **Monowall**
- FreeBSD based with BSD License
- Live CD, Embedded, Hard Drive Install
- Simple web management GUI
- Simple single XML configuration file
- Can be built on i386, embedded, WRAP
- Wifi support
- Ipsec/PPTP VPN
- SSH Server
- DNS, DHCP, Dynamic DNS support
- Commercial support available from dozens of vendors
- http://m0n0.ch/wall/

Copyright © Evolutionary IT 2008

Firewall - Pfsense

- **PFSense**
- Based on Monowall
- Built on FreeBSD 6.1 with PF firewall from OpenBSD
- BSD License
- Live CD, Embedded, Hard Drive Install
- Simple web management GUI
- Can be built on i386, embedded, WRAP
- Wifi support a/b/g, WEP, WPA/WPA2
- Ipsec/PPTP VPN

Copyright © Evolutionary IT 2008

Firewall - Pfsense

- DNS, DHCP, Dynamic DNS support
- Traffic Shaping with ALTQ
- Multi WAN
- Load Balancing
- Fail over CARP
- Dozens of plug-ins to expand
- Commercial support available from dozens of vendors
- http://www.pfsense.org

Copyright © Evolutionary IT 2008

Firewall - IPCop

- **IPCop**
- Fork of Smoothwall
- Built from Linux From Scratch
- Embedded, Hard Drive Install
- I386 and embedded.
- GNU/GPL
- Stateful Firewall
- NAT
- Proxy (Squid) HTTP/FTP
- IDS (Snort)

Copyright © Evolutionary IT 2008

Firewall - IPCop

- NTP client/server
- SSH Server
- DNS, DHCP, Dynamic DNS support
- Traffic Shaping
- IPSec/PPTP
- Extensive Logging & Graphing
- Extensive plug-ins to do any and everything under the sun.
- Commercial support available from dozens of vendors
- http://www.ipcop.org

Copyright © Evolutionary IT 2008

VPN

- Virtual private network.

Copyright © Evolutionary IT 2008

VPN - OpenVPN

- SSL/TLS VPN solution
- Flexible authentication options with certificates, smart cards, 2-factor authentication
- Firewall & NAT friendly
- Dynamic address support
- Multiple protocol support
- Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, and Windows 2000/ XP
- Client is required as it is not a proxy solution.
- http://openvpn.net/
- Open VPN Windows GUI
- http://openvpn.se/

Copyright © Evolutionary IT 2008

VPN – SSL Explorer

- SSL/TLS VPN Solution
- GNU/GPL
- Available in commercial enterprise edition – 3SP Ltd.
- Full support web proxy
- Microsoft Windows, Linux, Os X, Sun Solaris supported
- Zero footprint VPN (browser) – no other client needed
- Slick web management GUI
- Internet Explorer 5, IE6, IE7, Mozilla Firefox, Opera and Safari browsers
- Supernumerary strong authentication options such as LDAP, Radius, Public-Key, SSL client cert, one time password via SMS/Cell/PDA, RSA SecureID, VASCO Digipass.
- Full auditing and reporting
- http://www.sshtools.com/showSslExplorerCommunity.do

Copyright © Evolutionary IT 2008

VPN - OpenSwan

- Ipsec VPN Solution
- Fork of defunct FreeS/WAN
- GNU/GPL
- Opportunistic Encryption
- X.509 certificates
- NAT traversal support
- XAUTH
- DNSSEC support
- http://www.openswan.org/

Copyright © Evolutionary IT 2008

VPN - Poptop

- PPTP Server
- Linux, BSD, Solaris
- GNU/GPL
- Microsoft compatible authentication & encryption (MSCHAPv2, MPPE 40-128 bit RC4)
- Supports integration with LDAP/SAMBA
- Windows built-in clients and Linux
- http://www.poptop.org/

Copyright © Evolutionary IT 2008

Proxy solutions

- Advanced content filtering and control

Copyright © Evolutionary IT 2008

Proxy - Squid

- Caching proxy for HTTP, HTTPS, FTP and then some.
- Reverse Proxy
- Basis for many commercial content related devices.
- Many useful add-ons.
- Supports Authentication via proxy_auth for LDAP, NCSA, MSNT, PAM, SMB, SASL, YP(NIS)
- http://www.squid-cache.org/

Copyright © Evolutionary IT 2008

Proxy - DansGuardian

- Web Content Filtering using content of pages, MIME filtering, file extension, phrase matching, POST limiting and URL filtering and URL blacklisting.
- PICS (Platform for Internet Content Selection – metadata labeling of webpages standard developed by W3C) filtering
- Can work with nearly any proxy
- Linux, BSD, OSX, Unix
- GNU/GPL
- http://dansguardian.org/

Copyright © Evolutionary IT 2008

Content Filtering - SquidGuard & HAVP

- **SquidGuard**
- Plug-in for Squid Content Control
- Blacklisting, URL Matching, IP/Network/Domain Blocking, Time based blocking and Authentication Support
- GNU/GPL
- http://www.squidguard.org/
- **HAVP**
- HTTP Anti-Virus proxy
- Proxy with ClamAV
- Integrates with Squid & other Proxies
- GNU/GPL
- http://www.server-side.de

Copyright © Evolutionary IT 2008

Content Filtering - Untangle

- Linux UTM (Unified Threat Management) with simple GUI management.
- Supports Spam prevention, Web Filtering, Antivirus Scanner, Phishing Blocker, IPS, Firewall, Remote Access, VPN (OpenVPN) and basic routing features.
- Advanced Reporting features as well as PDF and HTML export.
- GNU/GPL
- Commercial support and Appliance solutions
- http://www.untangle.com/

Copyright © Evolutionary IT 2008

HID

- Host based Intrusion Detection

Copyright © Evolutionary IT 2008

HID - Osiris

- Centralized client/server systems integrity check program.
- Central server maintains file integrity database
- Monitors kernel and files
- Encryption support
- BSD, Linux, Unix. OSX, Windows
- Email Support
- Syslog
- http://osiris.shmoo.com/

Copyright © Evolutionary IT 2008

HID - Samhain

- File/Systems Integrity and IDS
- Client Server model with centralized monitoring and management
- Supports reports stored in Databases Oracle, MySql, PostgreSQL
- Beltane – web based PHP configuration console
- Linux, BSD, Unix and Windows
- Checksum (Tiger192, SHA-1, MD5), size, mode/permission, owner, group, etc. SELinux, POSIX ACL.
- Kernel Integrity Check (rootkit detection), SUID/SGID, Open Ports, Process Check, Mount Check, Logon Event Check
- Advanced Logging – centralized logging w/ encryption, syslog, built-in email functionality, RDBMS support.
- Inter operates with Prelude & Nagios
- http://www.la-samhna.de/samhain/index.html

Copyright © Evolutionary IT 2008

HID - OSSEC

- Integrates log analysis, file integrity checking, Windows registry monitoring, root kit detection, real time alerting and response.
- Strong and well integrated Log analysis engine.
- Runs on Linux, BSD, OS X, Solaris & Windows.
- GNU/GPL
- http://www.ossec.net/

Copyright © Evolutionary IT 2008

IDS

- Intrusion Detection

Copyright © Evolutionary IT 2008

IDS - Snort

- Real-time traffic analysis & logging via protocol analysis, content searching/matching.
- Signature, protocol and anomaly based detection
- GNU/GPL
- Unix/Linux/BSD/Windows
- Many plug-ins and extensions are available
- Gold standard in the IDS world
- Basis of many commercial intrusion detection products
- Commercial support is available.
- http://www.snort.org/

Copyright © Evolutionary IT 2008

IDS - BASE

- Basic Analysis and Security Engine (BASE)
- Web front-end for analysis of snort IDS data
- Allows for user authentication and role-based system
- Easy web administration
- GNU/GPL
- http://base.secureideas.net/
- Other SNORT add-ons such as ACID, Barnyard, Snortsnarf,etc.
- http://www.snort.org/dl/contrib/

Copyright © Evolutionary IT 2008

Sguil

- Pronounced sgweel
- Intuitive GUI to realtime events, session data and raw packet captures.
- BSD, Linux, Solaris, Windows, Os X
- QT Public License
- http://sguil.sourceforge.net

Copyright © Evolutionary IT 2008

IDS - Prelude-IDS

- Hybrid IDS Framework that supports most open source frameworks such as Snort, Honeyd, Nessus, Samhain, etc.
- IDMEF (Intrusion Detection Message Exchange Format) IETF XML based common format for IDS alerts.
- SSL encrypted communication with sensors
- Text/XML reporting
- Database support for MySQL, PostgreSQL
- Logging from many commercial devices such as Cisco, CheckPoint, Symantec, Syslog
- Linux, BSD, Unix, OSX
- http://prelude-ids.org/

Copyright © Evolutionary IT 2008

Vulnerability assessment

- Scanning & assessment tools.

Copyright © Evolutionary IT 2008

Nmap

- Nmap
- Network Mapper
- Node Discovery
- Port Scanning
- Operating Systems detection
- Linux, Unix, BSD, Windows
- GNU/GPL
- http://insecure.org/

Copyright © Evolutionary IT 2008

Nessus

- All encompassing vulnerability & security scanner
- Vulnerability enumeration, patch & misconfiguration information
- Password testing using brute force/dictionary attacks
- Denial of service test.
- NASL (Nessus Attack Scripting Language) for any vulnerabilities tests.
- Output as Txt, HTML, LaTeX
- Open source until version 2.x now a closed commercial project

Copyright © Evolutionary IT 2008

OpenVAS

- Fork of 2.x Nessus
- All the amazing features of Nessus but focus of Free software licensing.
- Fully GNU/GPL
- Not yet 1.x.
- http://www.openvas.org/

Copyright © Evolutionary IT 2008

NAC

Network Admission Control

Copyright © Evolutionary IT 2008

PacketFence

- Open source NAC solution.
- Based on Fedora, LAMP, Perl and Snort
- Heterogeneous focus and vendor agnostic
- PacketFence Zen (Vmware Virtual Appliance)
- Authentication via Apache (any supported)
- Captive portal and remediation
- Optional ban of unsupported OS's ex. Windows 95/98/ME or NAT devices
- GNU/GPL
- http://www.packetfence.org/

Copyright © Evolutionary IT 2008

FreeNAC

- FreeNAC
- Open source NAC solution based on Linux, OpenVMPS, FreeRadius, MySQL
- Dynamic VLAN management
- Slick Web and Windows GUI management console
- 802.1x authentication
- Scanning and identification of attached devices
- Live inventory and reporting
- Does not require end devices in VMPS mode.
- GNU/GPL
- http://www.freenac.net/

Copyright © Evolutionary IT 2008

Network Monitoring

- Without availability how can you have security?
- CIA triad. =)

Copyright © Evolutionary IT 2008

Nagios

- Enterprise network monitoring suite originally Netsaint project.
- GNU/GPL
- Linux, Unix, BSD, etc.
- Notification via pager, email, user defined method.
- Monitoring of network services, host resources and any other metrics.
- Impressive array of plugins/addons.
- Simple usable web interface.
- http://www.nagios.org/

Copyright © Evolutionary IT 2008

Zenoss

- Open network monitoring and management suite.
- GNU/GPL
- BSD, Linux, Unix and even Windows.
- Network health, performance, configuration, inventory/change, event management, logging, alerting and reporting.
- Supports a multitude of environmental, network, server, application, service checks.
- CMDB – configuration management database to model IT assets as detailed in ITIL best practice.
- Ease of management/setup with auto-discovery and web GUI.
- Highly evolved and integrated suite beyond mere monitoring.
- Commercial version is available with additional features.
- http://www.zenoss.com/

Copyright © Evolutionary IT 2008

Zabbix

- Open network monitoring, alerting and visualization suite.
- GNU/GPL
- BSD, Linux, Unix
- Supports auto-discovery, distributed monitoring, enhanced web monitoring, enhanced notification and alerting, agents for nearly every OS, etc.
- Great web management console.
- Commercial support is available.
- http://www.zabbix.com/

Copyright © Evolutionary IT 2008

Network Analysis

- What is going on out there?

Copyright © Evolutionary IT 2008

Wireshark

- Open source network protocol analyzer.
- 100's of supported protocols
- GNU/GPL
- Windows, Linux, BSD, Os X
- 3 pane view with color coding.
- Ability to decode nearly all standard capture file formats
- Supports decryption of Ipsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, WPA,WPA2.
- Outputs to XML, Postscript, CSV or plain text.
- http://www.wireshark.org/

Copyright © Evolutionary IT 2008

Ntop

- Network traffic probe that produces rich graphical output on your networks happenings.
- GNU/GPL
- Linux, BSD, Unix
- CLI or web interface, passive OS fingerprinting, graphical charts, protocol decoders, RDD support, Internet Domain, AS (Autonomous System) and VLAN stats.
- Intuitive and feature rich web interface for insight into networks inner workings.
- Can be an NetFlow/sFlow collector.
- Suite of applications such as nProbe, nBox and PF_Ring
- Commercial support is available.
- http://www.ntop.org/

Copyright © Evolutionary IT 2008

Centralized Consoles

- Security Management Console Suites

Copyright © Evolutionary IT 2008

OSSIM

- Open Source Security Information Management.
- BSD License
- BSD, Linux, Unix
- Well integrated collection of FOSS tools for security management tasks.
- Arpwatch, P0f, Pads, Nessus, Snort, Spade, Tcptrack, Ntop, Nagios, Osiris.
- Event correlation, visualization, reporting and incident management.
- Very nice web based security dashboard for comprehensive 360 view of environment.
- Commercially available with support options
- http://www.ossim.net/

Copyright © Evolutionary IT 2008

Live Cd Distro's

- **BackTrack -** Slackware based penetration testing live CD.
- Merger of Auditor and Whax Live CD projects
- >300 security tools
- http://www.remote-exploit.org/backtrac
- **Helix -** Focus on Incident Response and Computer Forensics
- http://www.e-fense.com/helix/
- **Insert -** Based on Knoppix Network analysis, DR, forensics, penetration testing, etc.
- http://www.inside-security.de/insert_en
- **Nubuntu -** Based on Ubuntu but with security tools
- http://www.nubuntu.org/
- **SecureDVD -** Multiple Security Distro's on one handy DVD
- Backtrack, Operator, PHLAX, Auditor, L.A.S., Knoppix-STD, Helix, Fire, nUbuntu, Insert.
- Bit out of date
- http://www.securedvd.org/

Copyright © Evolutionary IT 2008

Thanks to..

- Bradley J. Dinerman & Jack Daniels of NAISG.
- NAISG community.
- The FOSS community (developers, documenters, advocates, users, etc.) everywhere.

Copyright © Evolutionary IT 2008

Contact

Joseph Guarino

888.404.5074

www.evolutionaryit.com

Copyright © Evolutionary IT 2008