FOSS TOOLS

for network security,
monitoring, analysis
and operations.

Mike Harrison
Carilec IT/OT Conference
October 2015

Slide 1 of 1,042
in 30 minutes

MIKE HARRISON

- Utiliflex Systems Architect since 2007, Linux based solutions for Prepaid/Postpaid CIS, MDM, AMI… serving utilities worldwide.

- Started using Linux in 1994, built and operated internet service providers, copper, fiber and wireless metro-area networks powered by FOSS technologies. Software solutions using FOSS technologies for small and large companies.

- Zealot, but not a purest. Uses what is best for the job.

FOSS?

Free Open Source Software

Various licenses:

"**The FOSS communities are related, and differ only in extremely judgmental geek lexicon and proclamations.**"

Why? It works.

TCP/IP, EMAIL, WEB, Radius, HTTP..

Acquisition costs:
Low.

Support costs:
Investment in time. Poor or arcane documentation.

Some commercial support available.

Linux, BSD, *nix.. Mac, Android and Microsoft.

LINUX

The poster child of FOSS.
A flexible platform.
Incredible variety.
In most embedded solutions
and core of many many
commercial appliances

DISTRIBUTIONS

Collections of software
with an ethos, ecosystem,
environment and
evangelists.

WHY USE IT?

- Ease of acquisition
- Power
- Flexibility
- Security
- Relevance

FABULOUS CORE TOOLS

- Linux: Redhat and Ubuntu/Debian (use both, be flexible)
- Core Applications: Apache, MySQL/PostgreSQL, SAMBA (Windows Style Networking),

…...and now down the rabbit hole

pfSense

v 2.1

pfsense.org

Commercial Support Available!

- Firewall, VPN Appliance, Security Appliance, Router
- Built on FreeBSD Unix.
- Supports IPV6, OpenVPN and IPSEC
- Flash or "Spinning Disk"
- Supports NTOP / SNORT and more..
- Picky about some hardware…(network cards, etc..)

SNORT.ORG IDS

Intrusion Detection System

- Monitors traffic
- Rules for common problems
- Rule subscriptions available
- Useful for AMI/AMR/SCADA with special rules
- *nix and Microsoft Supported

SECURITY ONION

- http://securityonion.net

- Linux distro for IDS, NSM, and log management

- “based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!”

NTOP.ORG

- network monitoring
- dashboard high level
- drill down
- *nix and Microsoft…. but best on pfSense

OPENVPN

Personal Opinion:

Works better than any commercial VPN product I have seen, supported clients for Microsoft, Android, *nix, Mac.. with config files that can include keys and certs.

Less compromised by nation states, hackers and bad product configs.

NEW & SHINY

Those are some classics…
Here are the new toys.

RACKABLES.ORG

- datacenter asset management system
- crude, but much better than spreadsheets

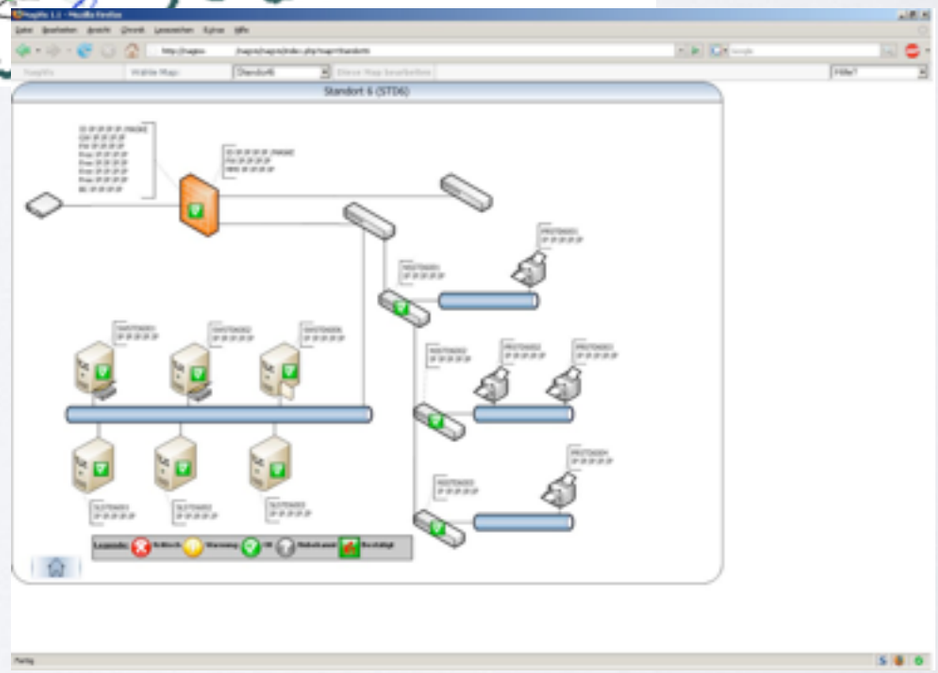
NAGIOS.ORG AND FRIENDS

- Monitor and Alert on just about anything
- SNMP, Agents and More
- Love it, Hate It, Use It.
- Extensible. 50 core plugins, 3000+ community and you can easily add your own.
- Email, SMS, Audio alerts..

OMD = OMDISTRO.ORG

Open Monitoring Distro

- Nagios and Monitoring Plugins (Former known as Nagios-Plugins)
- nsca
- check_nrpe
- Icinga
- Shinken
- NagVis
- pnp4nagios
- rrdtool/rrdcached



GIT

- Version Control for… just about anything
- Useful for config files, documents, source code
- Use internally for private things
- **https://github.com/mikegeeklabs/carilec**

QUICK LIST

- elastic.co ELK Stack: Elasticsearch, Logstash, and Kibana - for logging and more
- kali.org Pen Testing Distro (covered in other talk)
- asterisk.org VOIP/Phone system, IVR stack
- clonezilla Images and Partition Tools
- dban Wipe a disk.
- dnsMasq - small caching DNS server with over-ride

DAVE QUICK LISTS

- Cacti – SNMP poll/graphing of routers/firewalls/switches.
- Rancid – Config backup (if you have telnet/SSH devices)
- Owncloud – Dropbox under your control
- Open-LDAP – Provide OpenID proxy to your Active Directory
- NTP server – Windows sucks at time, and they admit it.
- DHCP server – Win DHCP server requires CAL for every IP assigned (Mike likes DNSMasq)

- SMTP-Proxy – In front of Exchange, sane configuration/ antiSPAM options
- SMTP-Proxy – Outbound, especially if you do mass-mails

- grep – Basic tool. Incredible.

DAVE QUICK LIST 4 WIN

Wireshark – sniff em
Putty – Needs no introduction
Notepad++ – Because Notepad still sucks
VirtualBox – Virtualization on the cheap (free)
FileZilla Server/Client – [s]FTP[s] server/client
WinSCP – [s]FTP[s]/SSH/SCP/WebDAV client
LazPaint – because Paint still sucks (Mike likes GIMP at gimp.org)
TFTPD64 – TFTP/DHCP/SYSLOG server for Windows
VLC – Because your users always find weird media that won't play
Rufus – make bootable and installable VMware USB keys
MySQL/MariaDB/Sqlite – License free databases w/ Win clients/drivers
GPG-WIN – encryption (filesystem/email good luck on Outlook support)
VeraCrypt/Truecrypt – encrypted containers
keepass – password database

OPERATIONS

Things you can install and run in-house that make life better

- RedMine - Project Management (I use and abuse)
- OSTicket - Trouble Ticket
- GIT / GitLab - Source Code / Data / Version Control

- Common for WiFi Access Points
- Extensible: Mesh, Relay, Long Distance
- Useful: SSH access, diagnostics, firewall rules
- Security: Sniffing, Spoofing, Stopping (legal?)
- Ubiquity, Linksys… Lots of supported hardware

#1 GRIPE: PLAIN TEXT EMAIL

- https://www.gnupg.org/
- Windows, Mac, Linux tools for encrypted files and e-mail.
- Marginal:
  - http://www.gpg4win.org/
  - Symantic
  - Java Versions

STOP EMAILING CREDENTIALS IN PLAIN TEXT

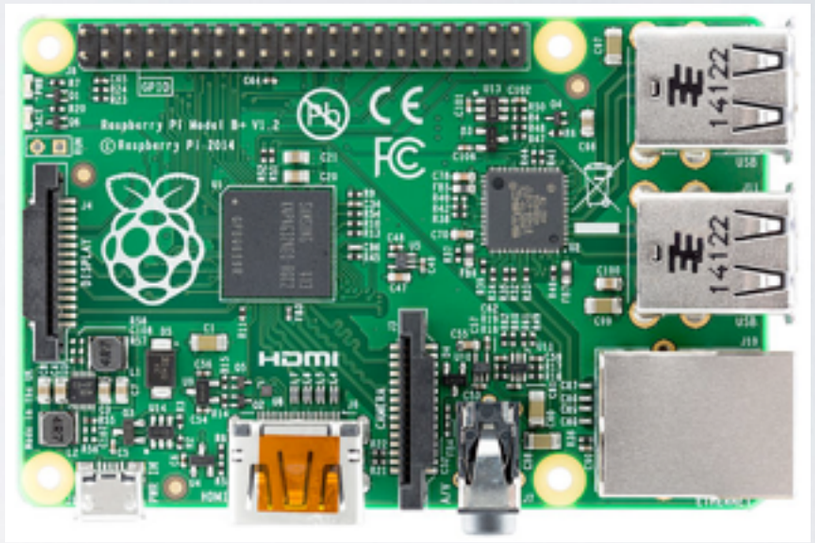
Use PGP/GPG Tools as much as possible.

TINYCA = CERT AUTHORITY

- Makes OpenSSL Easier.
- Create internal SSL Certificates for servers.
- Create Client SSL Certificates
- Use Them.

EMBEDDED PROBLEM SOLVERS

Raspberry Pi (B+ or newer) and friends

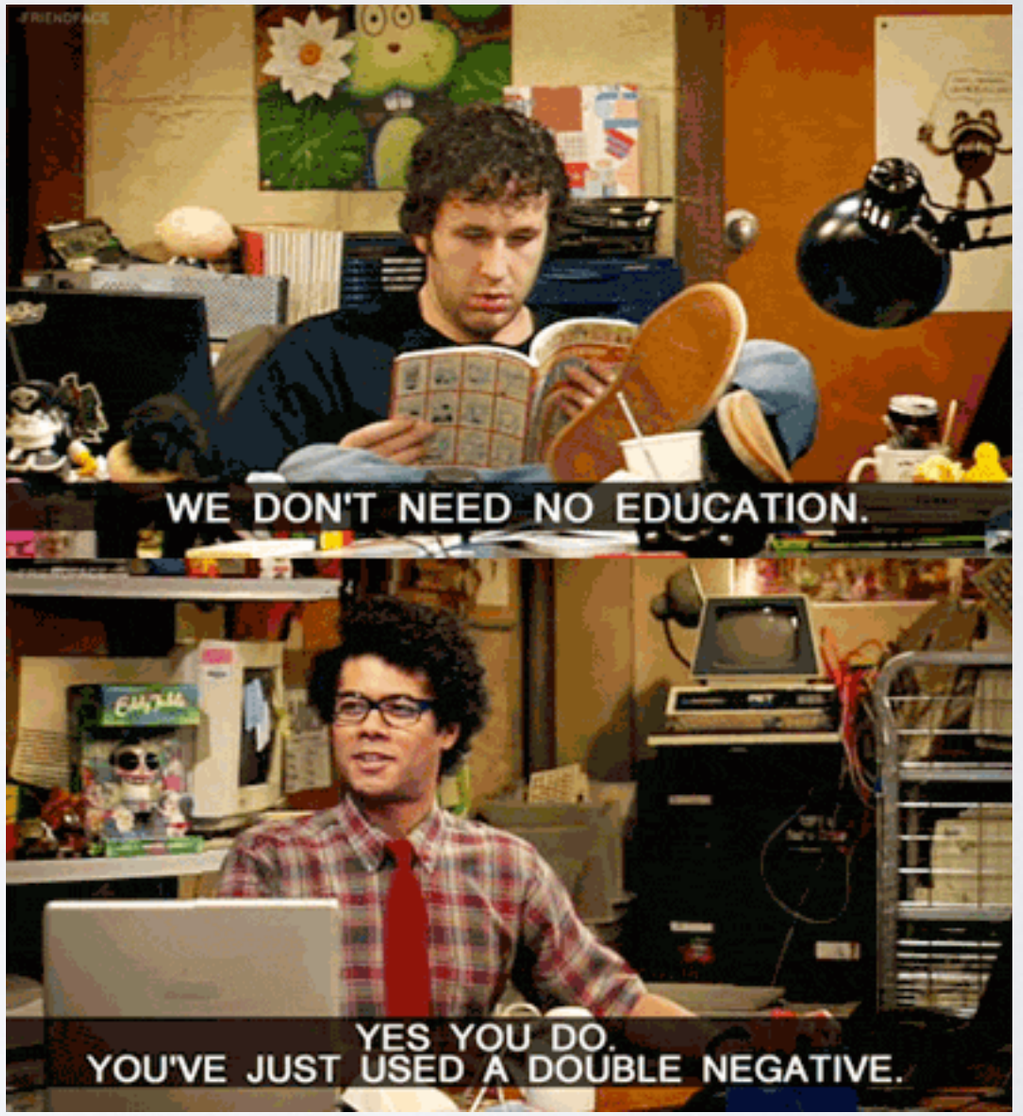


- monitoring
- router
- ethernet to serial, modbus.. (dark ages)
- GPIO (General Purpose In/Out)
- low power, robust, flexible: IoT

CHEAP!

KEY SKILLS

- Reading and Typing
- SSH/Terminal (screen)
- Shell Text Editor
- Willingness to fail
- Self-learning
- Synthesize New Knowledge



MANAGEMENT SUPPORT

- Use your budget for things that require it.
- Report successes and cost savings, increased capabilities.
- Educate that FOSS does not always mean "cheap". You need playgrounds and people time.

QUESTIONS?

Personal:

mike@geeklabs.com

@meuon (twitter)

Skype: meuoned

Professional:

mike.harrison@utiliflex.com

+1 423 605-6943

+1 423 933-3900

This was a personal presentation and not a representation of my employer.

https://github.com/mikegeeklabs/carilec