

# FOSS TOOLS THREAT SURFACES

attacking yourself  
so that you can't sleep at night

Mike Harrison  
Carilec IT/OT Conference  
October 2015



# 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.

I am NOT a security “expert”.

I am NOT a “hacker”  
(in that sense)

I have NOTHING to sell you.

I am an interested bystander,  
occasional target and victim.

I am a paranoid nutcase.





# 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.

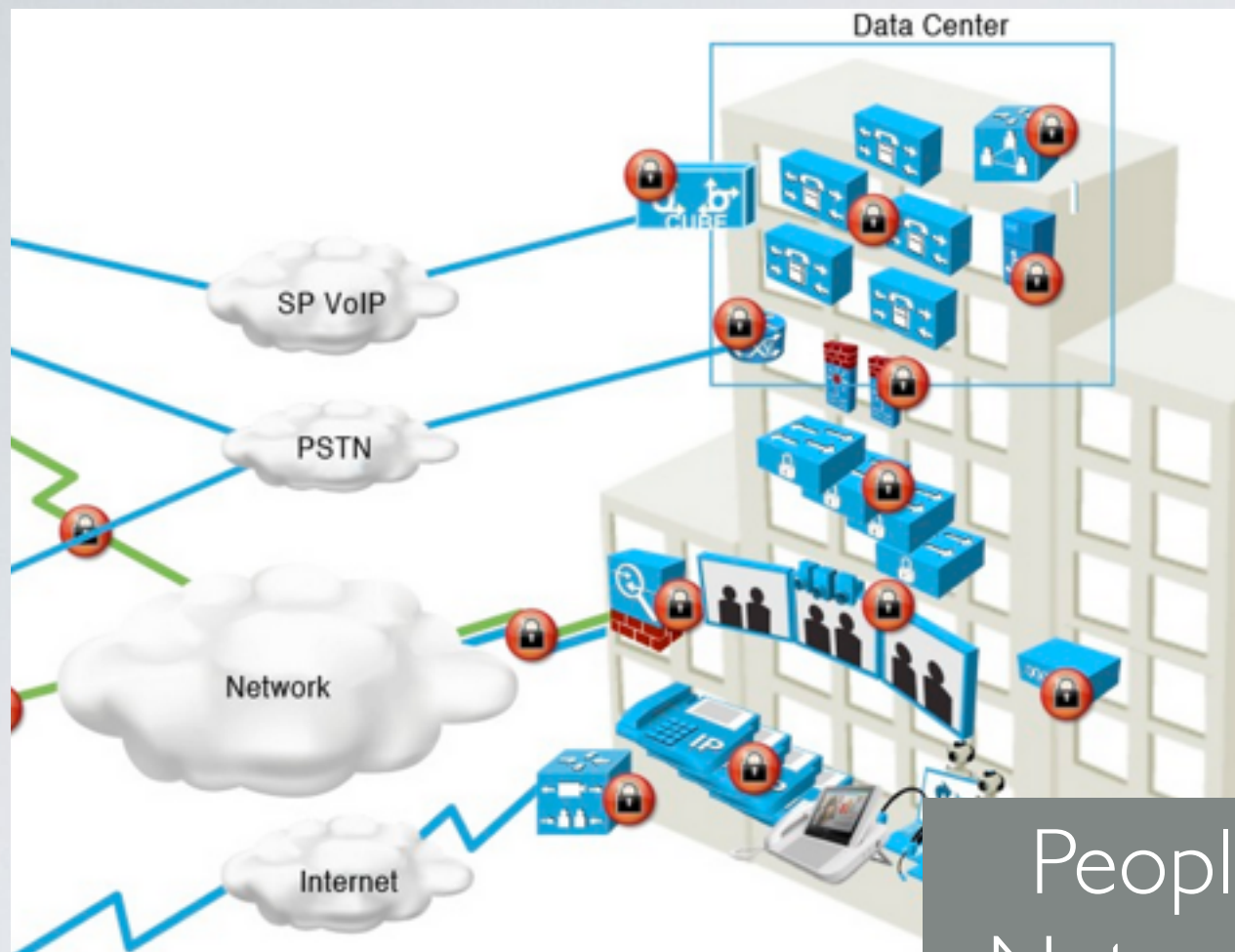
Linux, BSD, \*nix.. Mac,  
Android and Microsoft.

# THREAT/ATTACK SURFACE

- One of the best buzzwords Often shown with scary images in the security industry
- Ways that you are exposed....vulnerable...
- Utilities are accidental and intentional targets
- May include things outside of your control.







People  
Network  
Big Things  
Small Things



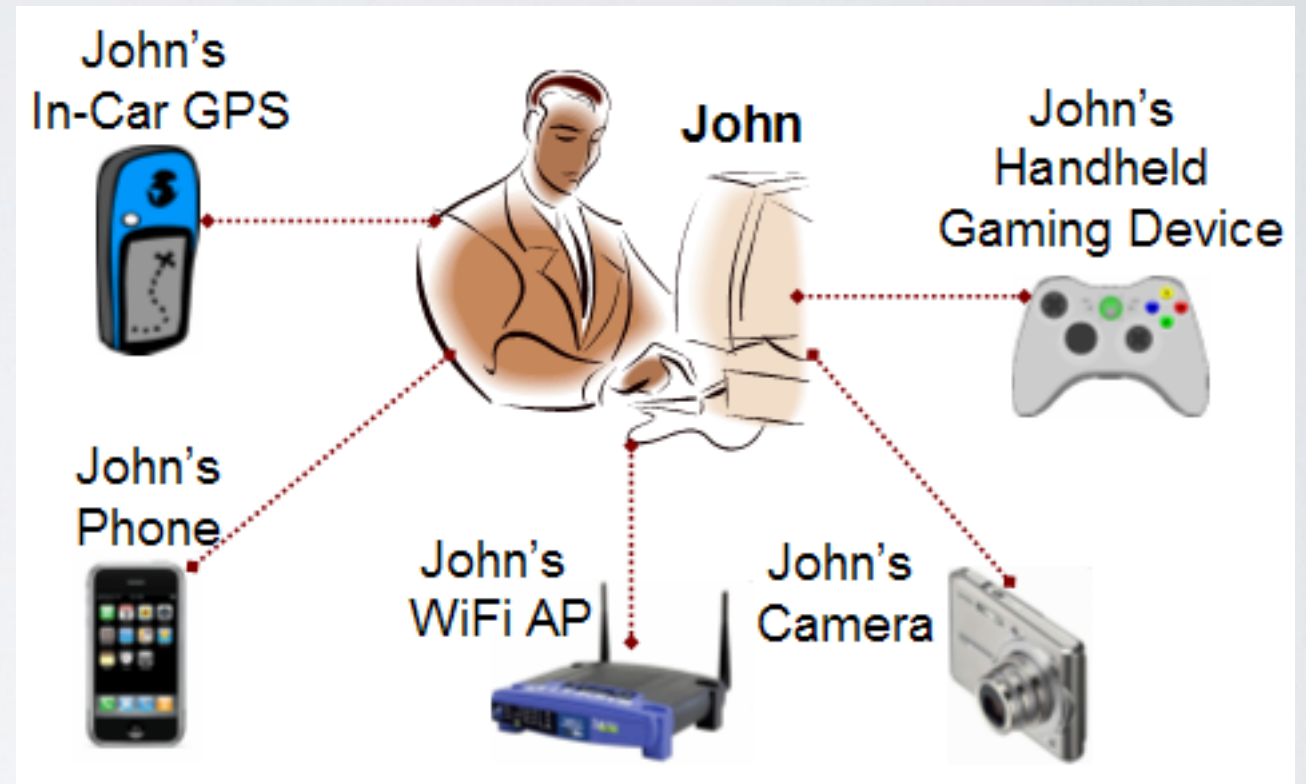
- Order Now
- Docu
  - Produ
  - Produ
  - Evalu

Embedded Linux Networking Server



# PEOPLE

- Share things publicly
- Bring their own devices
- Are smart about doing stupid things. They get better and better at them.



Good news: I'm not even going to touch "social engineering" (con-man)

But you might want to be wary of it as well.

Worst offenders: IT and Administration



# LEARNING RESOURCES

- YouTube Hacker Con Talks: <https://www.irongeek.com>
- Hacker Con's. Attend virtually and in person. Be careful.
- [sans.org](https://sans.org)
- lots of playing around.
- attack yourself



# ATTACK YOURSELF?

- as a learning exercise
- to understand outside audits better
- useful things for internal IT audits

# BASIC

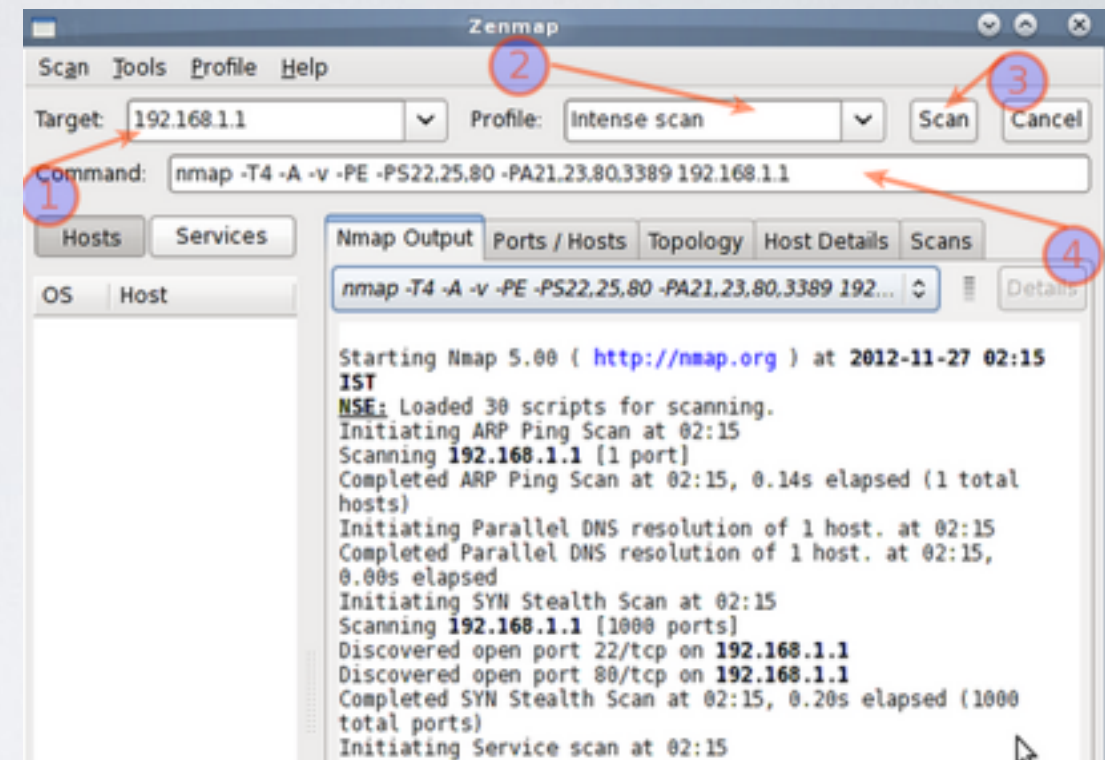
- NMAP “Network exploration tool and security / port scanner”
- It has advanced scripting availability and arcane options that can be useful.



```
bash-3.2#  
bash-3.2# nmap 192.168.15.0/24 >out
```

```
Nmap scan report for 192.168.15.20  
Host is up (0.00082s latency).  
Not shown: 983 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
88/tcp    open  kerberos-sec  
106/tcp   open  pop3pw  
389/tcp   open  ldap  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
548/tcp   open  afp  
625/tcp   open  apple-xsrvr-admin  
636/tcp   open  ldapssl  
749/tcp   open  kerberos-adm  
3659/tcp  open  apple-sasl  
5222/tcp  open  xmpp-client  
5269/tcp  open  xmpp-server  
5900/tcp  open  vnc  
8088/tcp  open  radan-http  
MAC Address: 10:DD:B1:C8:06:26 (Unknown)  
  
Nmap scan report for 192.168.15.42  
Host is up (0.00018s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: BC:AE:C5:6C:3A:D3 (Asustek Computer)
```

ZenMap = GUI



<http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/>

## Other good basic tools

- nc (netcat)
- sniffit (data level sniffer)
- tcpdump (deep sniffer)
- mtr (nice trace route)
- iptraf (good view of your network traffic)

Live demo's on  
Linux Screen



# MOST USEFUL TOOL

- Bare Linux
- pfSense
- OpenWRT
- M0n0wall

.....

Linux/BSD router with

all in/out traffic going through it

or available on a sniffer port

Being good with your tools,  
is more important than your tool.

# ADVANCED THE EASY WAY

The starting place for attacking your own network



<https://www.kali.org/>

Live demo on Linux  
using VMware image



# METASPLOT AND FRIENDS

metasploit.. a framework for exploiting things

You know that old application server from the zombie vendor that know one knows the passwords to?

'Spoit It.  
Own It.  
Fix It.

# ANY VOLUNTEERS?

Lets attack our ad-hoc network, right now.

Join WiFi:     **chattmetro**   or   **geeklabsopen**

Live Demo on Linux Screen



# EXTERNAL RESOURCES

## SHODAN.IO



required scary graphic

# SHODAN.IO EXAMPLES

- `net:123.123.0.0/16`
- `port:161 country:US simatic` (Siemens Simatic)

You can use generic search terms like PLC, control system vendor names, etc... If you happen to have banner information for all your assets catalogued, the searches will be more effective.



← → ↻ <https://www.shodan.io/search?query=edesur>


Shodan Scanhub Developers View All...

**SHODAN** edesur 🔍

Explore Contact Us Blog Enterprise Access New to Shodan? [Login](#)

Exploits Maps

TOP COUNTRIES




Showing results 1 - 1 of 1

**200.88.115.221**

221.115.88.200.m.sta.codetel.net.do

**Claro Dominican Republic**

Added on 2015-09-25 04:37:42 GMT

 Dominican Republic, Santo Domingo

[Details](#)

ACP Node **EDESUR** t213 ; Telnet Service  
date: 2015-09-24 time: 23:24:37

Device that control  
something over serial  
that is very helpful.

plain text  
no login

```

bling:~ mike$ telnet 200.88.115.221
Trying 200.88.115.221...
Connected to 221.115.88.200.m.sta.codetel.net.do.
Escape character is '^]'.
ACP Node EDESUR t213 ; Telnet Service
date: 2015-09-29 time: 8:59:03
*help
enter 'h' or 'help' followed by a topic.
possible topics are:
  xtypes
  x28cmds
  x3parms
  mnemonics
  profiles
  rpoa
  help
*help x28cmds
Available commands are:
call : retry previous      clr : clear call      copyclr: clear copy call
copy : copy data call     c : make call        help : help
h : help                  iclr : send inv clear  intd : int & discard
int : send interrupt      logoff : disconnect device menu : dispaly menu
npar : network parity     par : display x3      prof : change profile
reset : reset circuit     rpar : show remote x3 rprof : chg remote prof
rset : set remote x3      send : send data      set : set x3
stat : show status        tactt : channel test  tact : channel test
type : type string        wait : pause          x28type: change x28type
x3type : change x3type    atdt : make call      portstat:
portclr: [c] a.

call request example:
[c] a,r,t4,p128,w(3),d(9600,4800),s-12345*userdata

examples of available facilities are:
g12 = cug      o12 = oacug      r = rev      f = fastsel
fr = fastres   t1234 = rpoa      w3 = wsize   p128 = psze
d9600 = thrupt s = reselction prevention a = accounting

```



“GasPot” answered the question: are they being hacked?

Friend in Chattanooga working for TrendMicro  
faked a common “fuel tank monitoring systems” that were on-net.  
All over the world using a Raspberry Pi Honeypot

Check yours.

“Some evidence suggests links to either the Iranian Dark Coders (IDC) Team, as well as the Syrian Electronic Army.”

<http://blog.trendmicro.com/trendlabs-security-intelligence/the-gaspot-experiment-hackers-target-gas-tanks/>

<http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-gaspot-experiment>

# MITM

the Man In The Middle could/should be IT ?

- Who do you trust and why?
- With power comes responsibility?
- Too many secrets...

# MITMPROXY

- [mitmproxy.org](https://mitmproxy.org) (makes it really easy)
- Proxy HTTP and HTTPS traffic
- Inspect: who, payload and authentication
- Excellent API debugging tool. Seriously.



# LIVE DEMO (MITM)

Live demo of MITM proxy

# GRIPES

- Utility IT Software Vendors
- Auditors (PWC especially)
- MultiSpeak as the poster child for bad XML
- Lack of resources.

# 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>