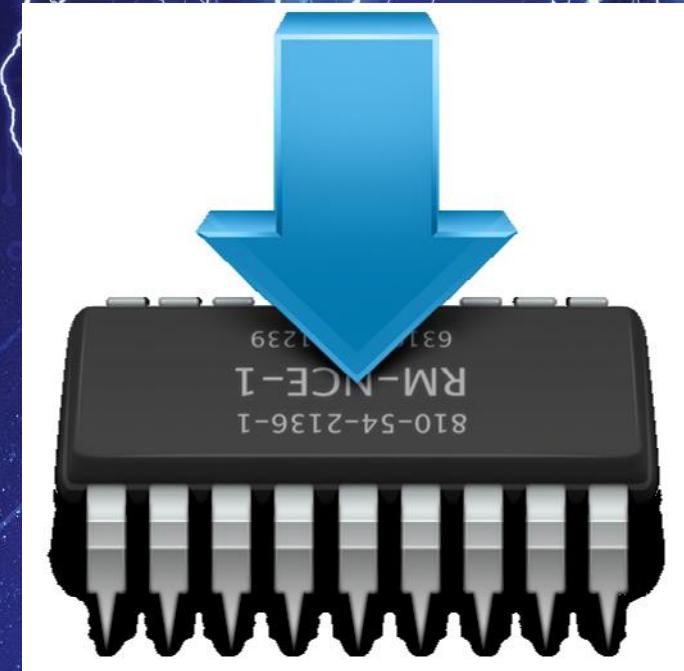


# Staying Persistent in Software Defined Networks





# Hellfire Security

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

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



# Overview

- ➊ White Box Ethernet
- ➋ Stupid Is As Stupid Does!
- ➌ Exploiting it!
- ➍ Moving Forward
- ➎ Wrapping Up



# *What Is Whitebox Ethernet?*

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





# *Why Do It?*

- ⊕ **Reduced Cost**
- ⊕ **Increased Flexibility**
- ⊕ **Gain More Control**
  - ⊕ **Traditional**
  - ⊕ **DevOps**
  - ⊕ **Software Defined Networking**





# ***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*

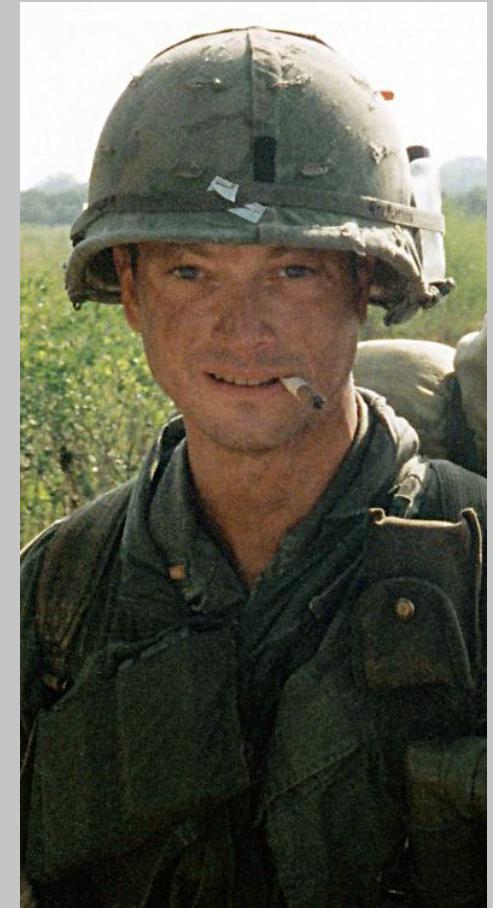


*What Could Go Wrong?*



# *Weaknesses (Operating System)*

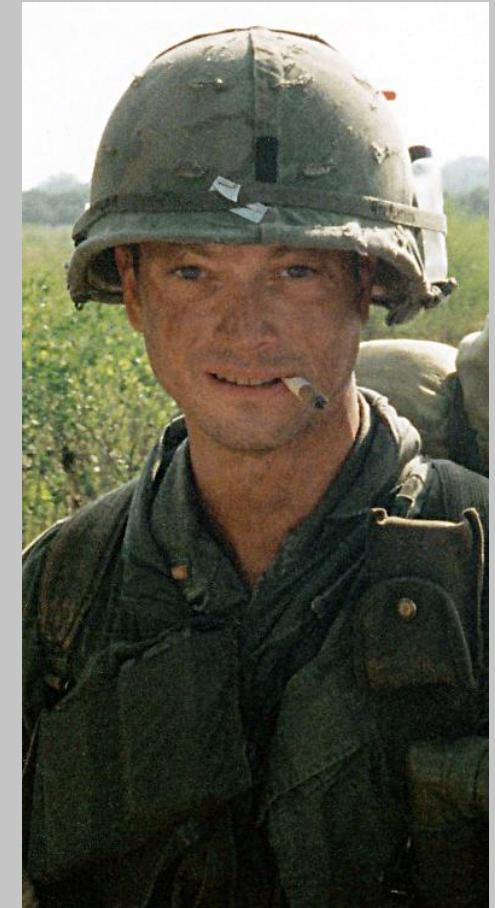
- ➊ **Privileged Account**
  - ➊ No Root Password
  - ➊ Doesn't Force You To Change It!
- ➋ **Management Services**
  - ➊ Uses Telnet
  - ➊ SSH
    - ➊ Installation Mode (18-bits Entropy)
    - ➊ Recovery Mode (26-bits Entropy)





# *Weaknesses (Installer)*

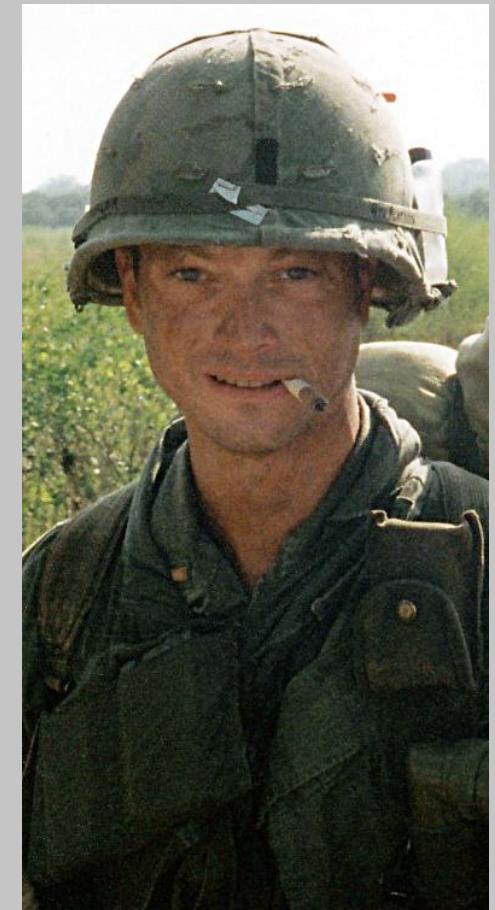
- ⊕ **Predictable URLs**
  - ⊕ Exact URLs from DHCPv4
  - ⊕ Inexact URLs based on DHCP Response
  - ⊕ IPv6 Neighbors
  - ⊕ TFTP Waterfall
- ⊕ **Predictable File Name Search Order**
- ⊕ **No Encryption or Authentication for Installs**





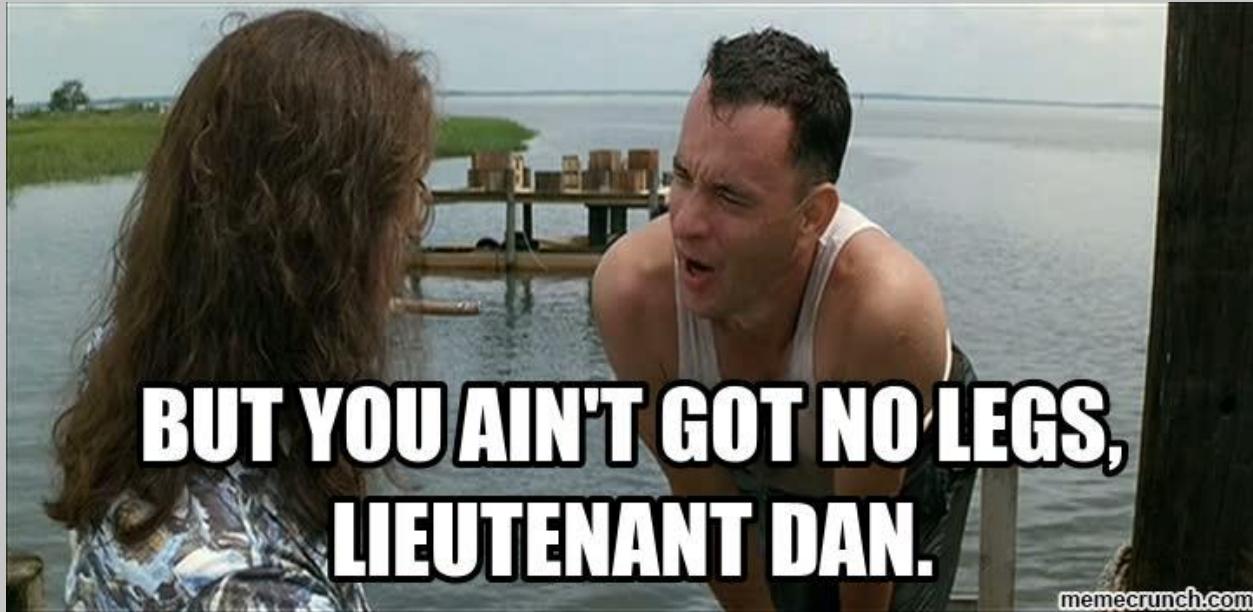
# *Weaknesses (Implementation)*

- ⊕ Exposed Partition
- ⊕ No Secure Boot





## *What Does This Mean?*



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



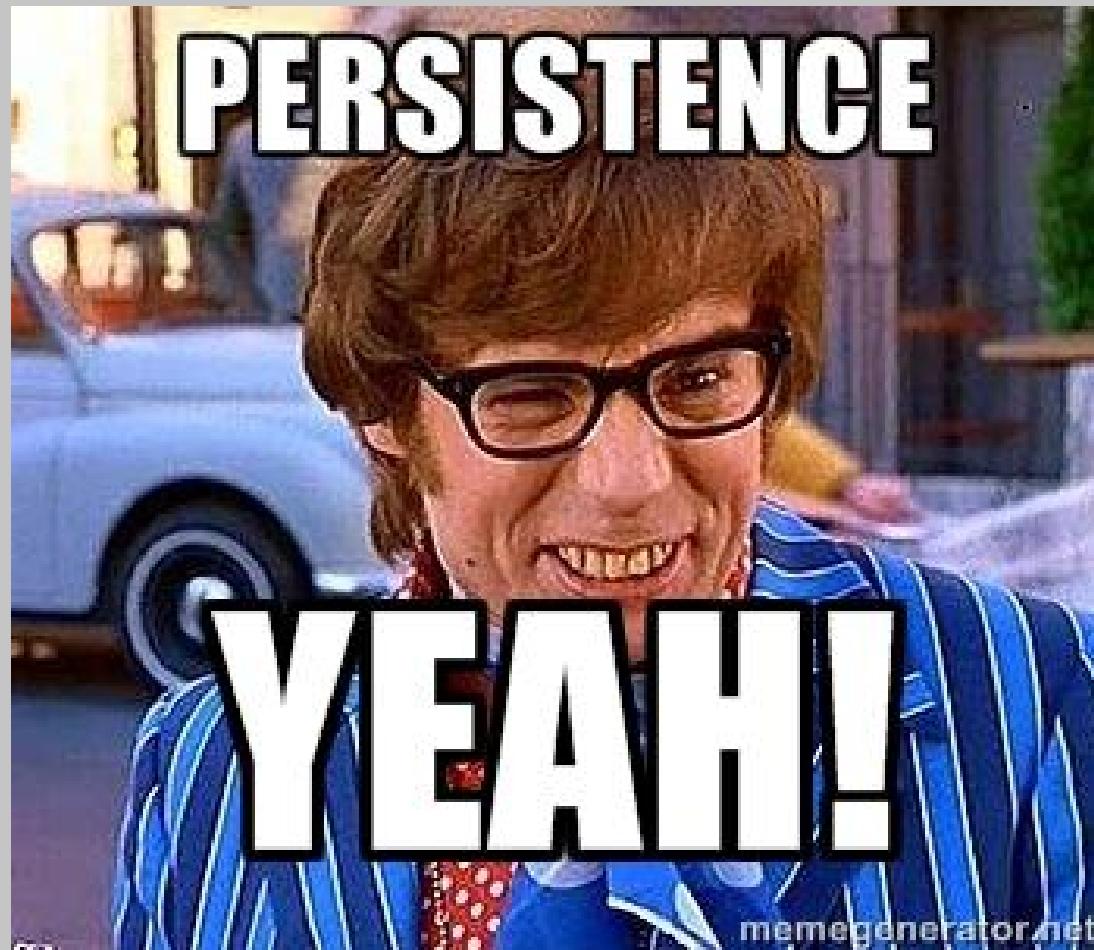
## *Here's How*

- ➊ **Compromise It (Directly)**
  - ➌ **Direct Entry**
  - ➌ **Sniffing/MiTM (Telnet or SSH)**
- ➋ **Compromise It's Installations**
  - ➌ **Via Rogue DHCP Server**
  - ➌ **Via IPv6 Neighbor**
  - ➌ **Via Spoofed TFTP**



# *Even Better*

- ➊ Compromise It (Indirectly)
  - ➊ Get Past Network Operating System
  - ➊ Modify ONIE
    - ➊ Exposed Partition
    - ➊ No Secure Boot
  - ➊ Now You're In the Firmware ...
  - ➊ Now You're There Forever!





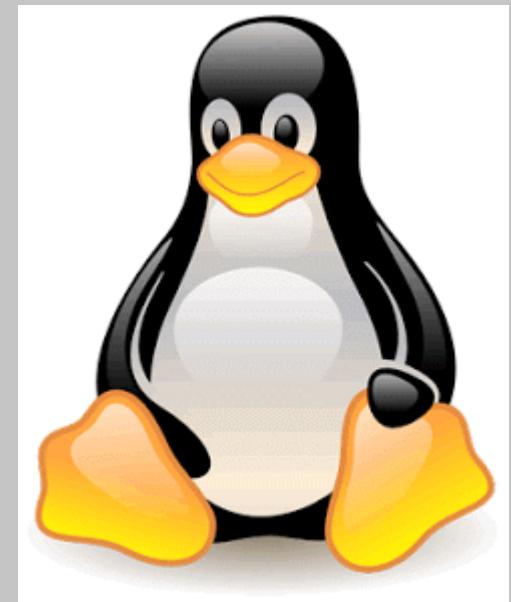
# *Network Operating Systems (NOS)*

- 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 (v2.6.0)***

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





# *Cumulus Linux (v2.5.3)*

- **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 (v3.3.4)**

- 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**

- ➊ Add Access
- ➋ Remove Access
- ➌ Hide Traffic
- ➍ Change Traffic

Switch Light (Indigo)

MLNX-OS (eSwitch)



# *Weaknesses (Operating System)*

- ➊ Default (and Fixed) Accounts
  - ➊ Switch Light
    - ➊ admin
    - ➊ root [hidden/disabled]
  - ➊ Cumulus Linux
    - ➊ cumulus
    - ➊ root [disabled]
  - ➊ MLNX-OS
    - ➊ admin
    - ➊ root [hidden/disabled]



# *Weaknesses (Operating System)*

- ⊕ **Easy Escape to Shell**

- ⊕ **Switch Light [enable, debug bash]**
- ⊕ **Cumulus Linux [N/A]**
- ⊕ **MLNX-OS [puppet]**

- ⊕ **Instant Elevation**

- ⊕ **Switch Light [N/A]**
- ⊕ **Cumulus Linux [sudo]**
- ⊕ **MLNX-OS [N/A]**



## *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



*This Means*

YOUR NETWORK

*Is One Key Logger Away!*



# *Big Cloud Fabric (Controller)*

```
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@54.161.82.18's password:
Last login: Wed Jul 22 22:00:21 2015 from 54.81.138.173
Big Cloud Fabric Appliance 2.6.0 (bcf-2.6.0 #265)
Logged in as admin, 2015-07-23 03:01:10.782000 UTC, auth from 50.165.241.154
10.69.168.196> 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# 
```



# Switch Light



```
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: Sun Jul 26 03:06:42 2015 from 192.168.2.101  
Switch Light OS SWL-BCF-2.6.0 (powerpc.release,bcf,2015.04.30.12.08,1f39188d2648  
7ce948bc2f7439e03ca6136f3026)  
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



# Switch Light (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/mtdblock1
brw-rw---T 1 root disk 31, 1 Jul 26 02:56 /dev/mtdblock1
root@localhost:~#
```



# *Cumulus (sudo)*

```
cumulus@gateway: ~
cumulus@gateway$ sudo cat /etc/shadow | grep root
root:$6$ghngS465$JS4w51C3DCLNcNeMAN24Mc.GwI5xx05IWk4f00zLhumTA6B.jjEV6XJf76ZvCc5mkJiwpXB8Bj8Z
kWuIZai1T.:16637:0:99999:7:::
cumulus@gateway$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
cumulus@gateway$ su
Password:
root@gateway:/home/cumulus# 
```



# MLNX-OS (Backdoor)

```
C:\Windows\system32\cmd.exe - nc 10.9.29.7 2023
C:\Users\lab\Downloads\nc111nt>nc 10.9.29.7 2023
whoami
admin
cat /etc/passwd | grep admin
admin:x:0:0:System Administrator:/var/home/root:/opt/tms/bin/cli
xmladmin:x:0:0:XML Admin User:/var/home/xmladmin:/opt/tms/bin/xg
-
```



# *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 Low Privilege “admin”
  - ⊕ Commands Processed By “clcdrv\_server.py” On Unix Sockets
- ⊕ Command Injection Issues!
- ⊕ Boom Goes CLCMD\_SERVER
- ⊕ And it runs as “Root”





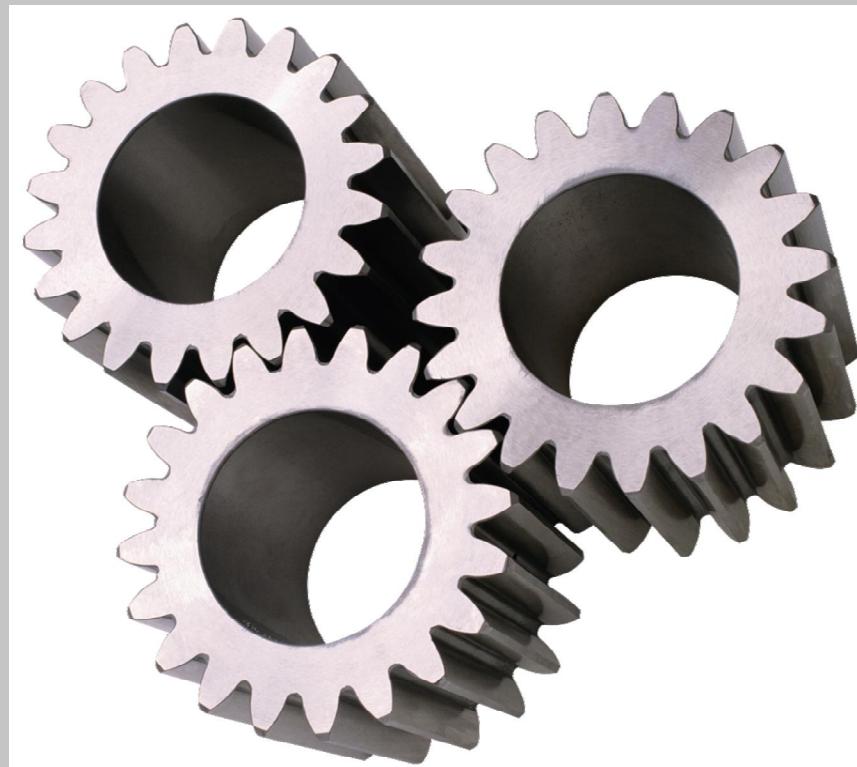
# CLCMD-SERVER Running On A Switch

```
192.168.2.105 - PuTTY

[c]
root      2559  0.0  0.0   3276   620 ?          Ss    13:37  0:00 /usr/sbin/ptmd
-d -l INFO
root      2604  0.0  0.3  11124  6228 ?          S     13:37  0:00 /usr/bin/python
/usr/lib/python2.7/dist-packages/clcmd server.py
root      2703  0.0  0.0   7840   1144 ?          Ss    13:37  0:00 /usr/sbin/sshd
root      2762  0.0  0.2  11684   5036 ?          S     13:37  0:00 /usr/bin/python
/usr/lib/cumulus/ztp-usb
root      2852  0.1  0.0  14544   1692 ?          SNl   13:37  0:05 /usr/bin/monit
-p /var/run/monit.pid -s /var/run/monit/state -c /etc/monit/monitrc
root      2936  0.0  0.0   3116   676 ?          S     13:37  0:00 /bin/bash /usr/
bin/arp_refresh
root      2943  0.0  0.0   3116   676 ?          S     13:37  0:00 /bin/bash /usr/
bin/arp_refresh
root      3128  0.0  0.0   2608    844 ttys0     Ss+   13:40  0:00 /sbin/getty -L
ttys0 115200 vt100
root      3320  0.1  0.4  14716   9288 ?          SN    13:42  0:02 /usr/bin/python
/usr/sbin/ledmgrd
quagga   4322  0.0  0.0   6312   1756 ?          S<s  13:46  0:00 /usr/lib/quagga
/bgpd --daemon -A 127.0.0.1
quagga   4349  0.0  0.0   4580   1260 ?          S<s  13:46  0:00 /usr/lib/quagga
/ospfd --daemon -A 127.0.0.1
root      7652  0.6  0.1  11196   3460 ?          Ss    14:22  0:00 sshd: admin [pr
iv]
```



# Demonstration





# *Exposed ONIE Partition*

```
192.168.2.105 - PuTTY

$ whoami
hacker
$ sudo 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

$ 
```

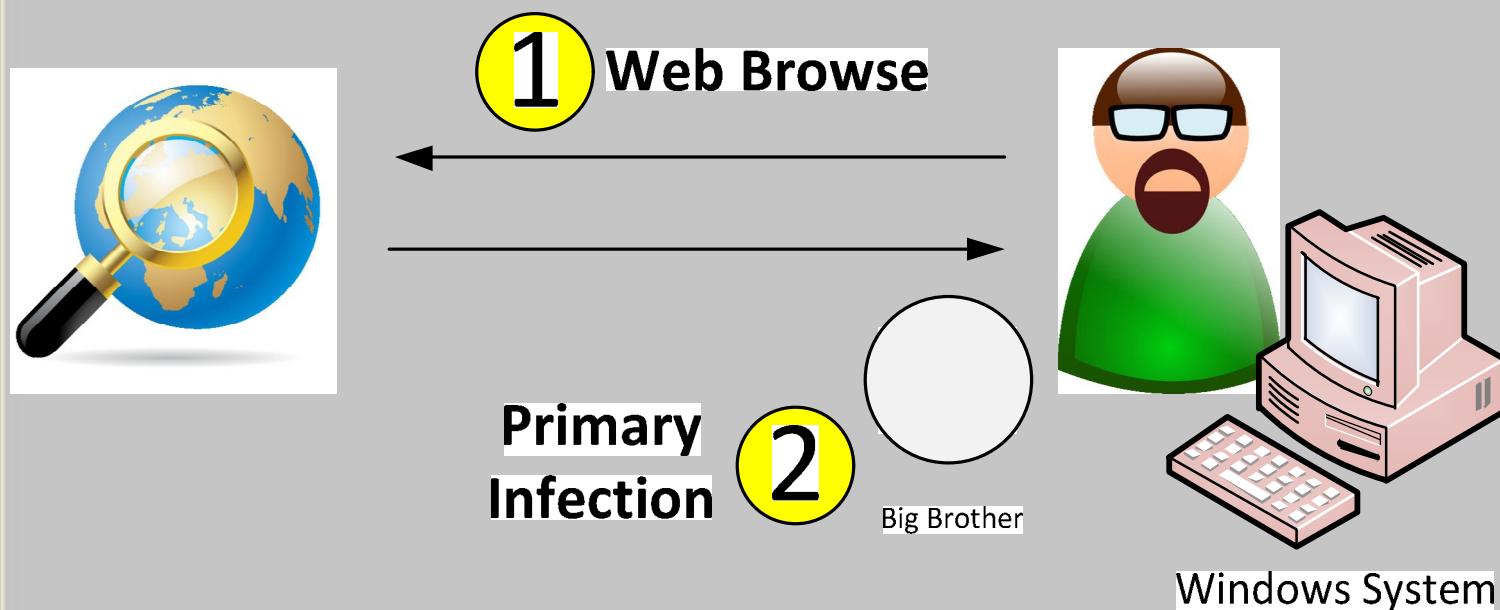


# *Exposed ONIE Partition*

```
$ whoami
hacker
$ sudo dd if=/dev/mtdblock1 of=/tmp/onie_dump
8192+0 records in
8192+0 records out
4194304 bytes (4.2 MB) copied, 2.60318 s, 1.6 MB/s
$ ls -l /tmp
total 4096
-rw-r--r-- 1 root root 4194304 Jul 21 14:31 onie_dump
$ 
```



# Demonstration (Scenario)

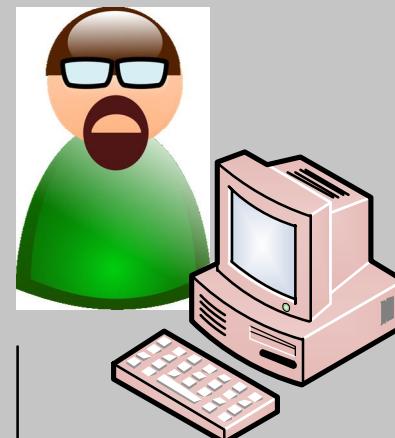


# Demonstration (Scenario)

Key  
Logger

3

Big Brother



Windows System

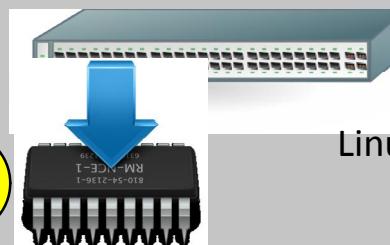
Secondary  
Infection

4

Little Brother

ONIE  
(Firmware)  
Plant

5

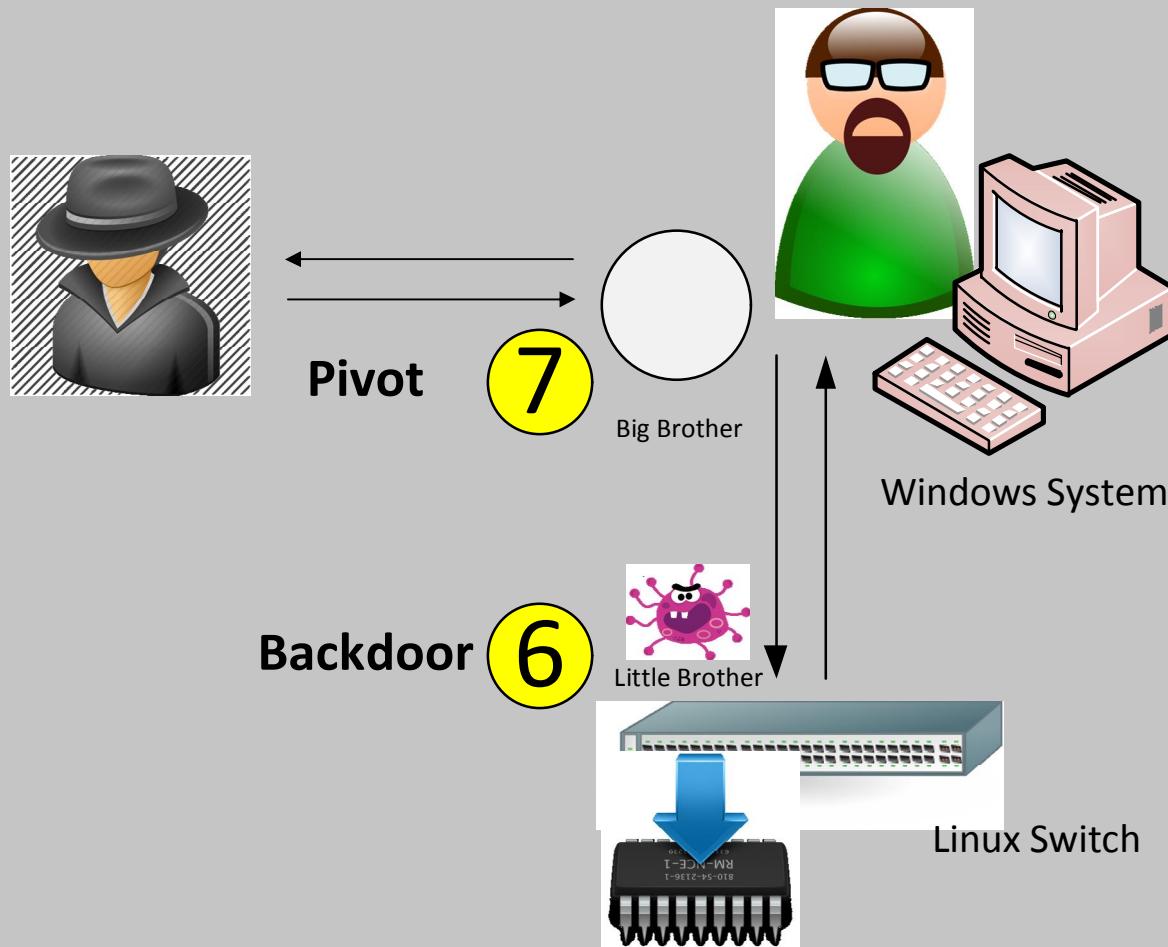


Linux Switch





# Demonstration (Scenario)





# *Demonstration (Execution)*





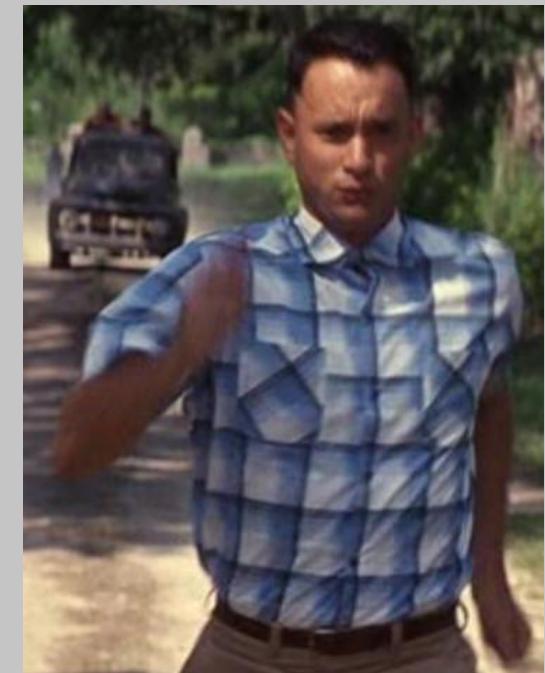
# *Available Solutions*

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



# *Hardware*

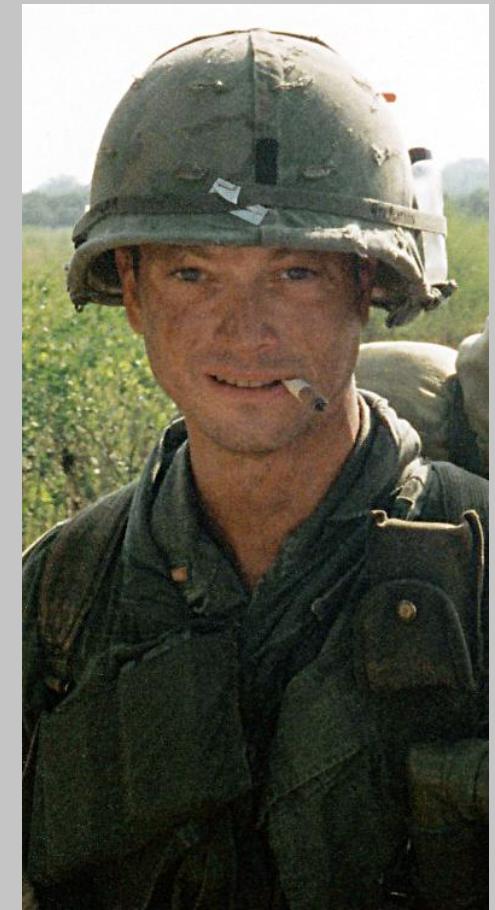
- ➊ Trusted Platform Module (TPM)
- ➋ Rob Sherwood Had These Put In for Most x86-Based Switches
- ➌ Let's Add Them to the PowerPC Switches
- ➍ Then, Let's Use Them!





# *Install Environment*

- ➊ Remove Telnet
- ➋ Increase Key Entropy
- ➌ Force Password Change
- ➍ Remove IPv6 and TFTP Waterfall
- ➎ Sign the Installations





# *Operating Systems*

- ➊ Changeable Names
  - ➊ uid 0 accounts
  - ➊ “reduced” privilege accounts
- ➋ Force Password Change
- ➌ Remove uid 0 from admin
- ➍ Tighten Shell Access
  - ➊ Switch Light (OTP)
  - ➊ Cumulus Linux (Wrapper, OTP)
  - ➊ MLNX (Remove socat)



# *Agents*

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





# *Enterprise Architecture*

- ➊ **Isolate Management Plane**
  - ➊ Rarely Done
  - ➊ What's wrong with Jump Boxes?
- ➋ **Audit Switches**
  - ➊ Password Changes
  - ➊ ONIE Partition Hashes



# *Racing Ahead*

- ➊ Impact On Security
- ➋ Keeping Pressure On Developers (Scaring Them)
- ➌ Making The Difference



# *Impact On Security*

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



# *Scaring Developers!*

- ➊ So Begins The Spinning of the Merry-Go-Round
  - ➊ We Hack It
  - ➊ You Fix It
- ➋ Let The Clean-Up Begin
- ➌ Is It So Hard To Hire Someone for Security
  - ➊ I thought fixing it later was more expensive?
  - ➊ 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*

- **Security of the Network Operating System is critical**
- **However, that security has been neglected**
- **Companies believe that the switches are safe**
- **Single piece of malware could easily make the cross-over from Windows-based systems to these Linux-based switches**
- **Leaving you with a persistent presence on your network**



# 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-fabrictm>
- ⊕ <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/psc/swd/public/detail?swItemID=M\\_TX\\_8adfcbf6e0834d5a82564b4825](http://h20564.www2.hp.com/psc/swd/public/detail?swItemID=M_TX_8adfcbf6e0834d5a82564b4825)
- ⊕ <https://github.com/mellanox-openstack/mellanox-eswitchd>
- ⊕ <http://zeromq.org/intro:read-the-manual>



