Staying Persistent in Software Defined Networks
Gregory Pickett, CISSP, GCIA, GPEN
Chicago, Illinois

gregory.pickett@hellfiresecurity.com
Overview

- White Box Ethernet
- Stupid Is As Stupid Does!
- Exploiting it!
- Moving Forward
- 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)

- Privileged Account
  - 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?

BUT YOU AIN'T GOT NO LEGS, LIEUTENANT DAN.

Lot's Of Opportunities to Blow It Up!
Here’s How

- Compromise It (Directly)
  - Direct Entry
  - Sniffing/MiTM (Telnet or SSH)
- Compromise It’s Installations
  - Via Rogue DHCP Server
  - Via IPv6 Neighbor
  - Via Spoofed TFTP
Even Better

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

YEAH!
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
  - Add Access
  - Remove Access
  - Hide Traffic
  - Change Traffic

Switch Light (Indigo)
MLNX-OS (eSwitch)
Weaknesses (Operating System)

Default (and Fixed) Accounts

Switch Light
- admin
- root (hidden/disabled)

Cumulus Linux
- cumulus
- root (disabled)

MLNX-OS
- admin
- 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
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@54.161.02.10's password:
Last login: Wed Jul 22 22:00:21 2015 from 54.31.130.173
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
10.69.160.196> 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

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, 1f39188d26487ce948bc2f7439e03ca4136f3026)
localhost> enable
localhost# debug base

***** 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)

```
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 5Jul 26 02:56 /dev/mtdblock1
root@localhost:~# execute
```
```
cumulus@gateway$ sudo cat /etc/shadow | grep root
root:$6$ghnq$465$J3w51C3DCLNcN0MAN24Mc.Cw15x05IWK4f00zLhumfA6B.jjEV6XJf76ZvCc5mkJiwpXB8Bj8Z
&WiZealT::16637:0:99999:7::
cumulus@gateway$ sudo passwd root
Enter new UNIX password:
Re-type new UNIX password:
passwd: password updated successfully
cumulus@gateway$ su
Password:
root@gateway:/home/cumulus$  
```
MLNX-OS (Backdoor)

```
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 “clcmd_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

- `root` 2559 0.0 0.0 3276 620 ? Ss 13:37 0:00 /usr/sbin/ptmd
   
- `root` 2620 0.0 0.3 11294 6228 ? S 13:37 0:00 /usr/bin/python
   
- `root` 2703 0.0 0.0 7640 1144 ? Ss 13:37 0:00 /usr/sbin/ssh
   
- `root` 2762 0.0 0.2 11684 5036 ? S 13:37 0:00 /usr/bin/python
   
- `/usr/lib/cumulus/ztp-usb`
- `/usr/lib/python2.7/dist-packages/clcmd_server.py`

- `root` 2852 0.1 0.0 14544 1692 ? SNL 13:37 0:05 /usr/bin/monitor

- `/var/run/monitor.pid` -s /var/run/monitor/state -c /etc/monitor/monitorrc
- `/usr/sbin/ptmd`

- `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` 3129 0.0 0.0 2608 844 ttySO Ss+ 13:40 0:00 /sbin/getty -L

- `root` 3320 0.1 0.4 14716 9280 ? SN 13:42 0:02 /usr/bin/python

- `/usr/sbin/ledmgmd`

- `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 4590 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 [priv]`
```
Demonstration
Exposed ONIE Partition

```bash
$ 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/anie_dump
6192+0 records in
6192+0 records out
4194304 bytes (4.2 MB) copied, 2.60318 s, 1.6 MB/s
$ ls -1 /tmp
total 4096
-rw-r--r-- 1 root root 4194304 Jul 21 14:31 onie_dump
$
Demonstration (Scenario)

1. Web Browse

Primary Infection

2. Big Brother

Windows System
Demonstration (Scenario)

1. Key Logger
2. Secondary Infection
3. ONIE (Firmware)
4. Plant
Demonstration (Scenario)

Pivot

Big Brother

Backdoor

Little Brother

Windows System

Linux Switch
Demonstration (Execution)
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
- Remove uid 0 from admin
- Tighten Shell Access
  - Switch Light (OTP)
  - Cumulus Linux (Wrapper, OTP)
  - MLNX (Remove socat)
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
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!
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

Scaring Developers!
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
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

- https://github.com/opencomputeproject/onie/wiki/CLI-Reference
- http://opennetlinux.org/docs/build
- http://opennetlinux.org/docs/deploy
- 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://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=MTX_8adfcbf6e0834d5a82564b4825
- https://github.com/mellanox-openstack/mellanox-eswitchd