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
- 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?

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 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 Switch Fabric (SDN)
- Maintained by Big Switch Networks
Cumulus Linux (v2.5.1)

- 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 \(\rightarrow\) Puppet)
  - MLNX-OS (OpenSSL 0.9.8e-fips-rhel5)

Heartbleed
Could Lead To . . .

- Topology, Flow, and Message Modification through Unauthorized Access
  - Add Access
  - Remove Access
  - Hide Traffic
  - Change Traffic
- Information Disclosure through Exploitation
  - Switch Light (Indigo)
  - MLNX-OS (eSwitch)
  - 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)
Could Lead To . . .

Full Control of Your Switch through Remote Code Execution

Switch Light
Cumulus Linux
MLNX-OS
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)

- Doesn’t Force You To Change Default Passwords for Non-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 (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
Big Cloud Fabric (Controller)

```
login as: admin
Big Cloud Fabric Appliance 2.6.0 (Bcf-2.6.0 #265)
Log in as 'admin' to configure
admin@10.182.69.145's password:
Last login: Thu May 28 02:13:32 2015 from 54.159.92.140
Big Cloud Fabric Appliance 2.6.0 (Bcf-2.6.0 #265)
Logged in as admin, 2015-05-28 20:56:32.565000 UTC, auth from 58.11.74.94
10.182.69.145> 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: Thu Jul 23 20:31:43 2020
Switch Light OS SWC-2 6.0 (powerpo_release, bcf, 2019.04.30.12.08.1f89186d2687ce59c5c74b90e30e6136f2026)

root@localhost:~
root@localhost:~

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

root@localhost:~$
Switch Light (Exposed ONIE Partition)
Cumulus (sudo)

cumulus@gateway$ sudo cat /etc/shadow | grep root
root:$6$ghngs465$J84w51C3DCLNcNoKAN24Mc.CwI3xx05IWK4f00zLhumPA6B.jjiev6XJf762vCc5mkjiwpXB5Bj82
&WuIzalIT.:16637:0:99999:7::
cumulus@gateway$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
password: password updated successfully
cumulus@gateway$ su
Password:
root@gateway:/home/cumulus$
MLNX-OS (Backdoor)
This Means

Your Network

Is One Key Logger Away!
Demonstration (Scenario)

1. Web Browse

Primary Infection

2. Big Brother

Windows System
Demonstration (Scenario)

3. Key Logger

4. Secondary Infection

5. ONIE (Firmware) Plant

Windows System

Little Brother

Linux Switch
Demonstration (Scenario)

Pivot

Backdoor

Big Brother

Little Brother

Windows System

Linux Switch
Demonstration (Execution)
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 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
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/olie_dump
5192+0 records in
5192+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
$ 
```
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
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 greater than what we see now.
- But there is a 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 Starts Here.
Links

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