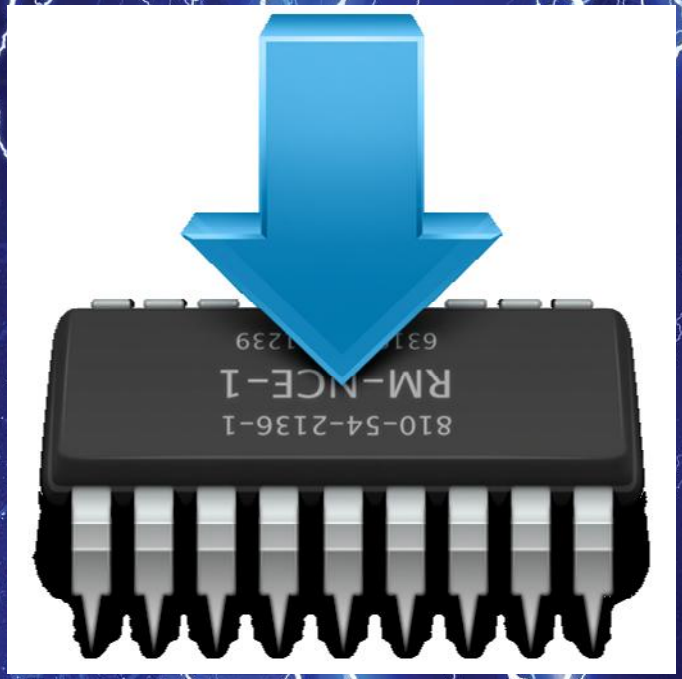
Staying Persistent in Software Defined Networks

black hat USA 2015



UBM Tech

Hellfire Security

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?

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!

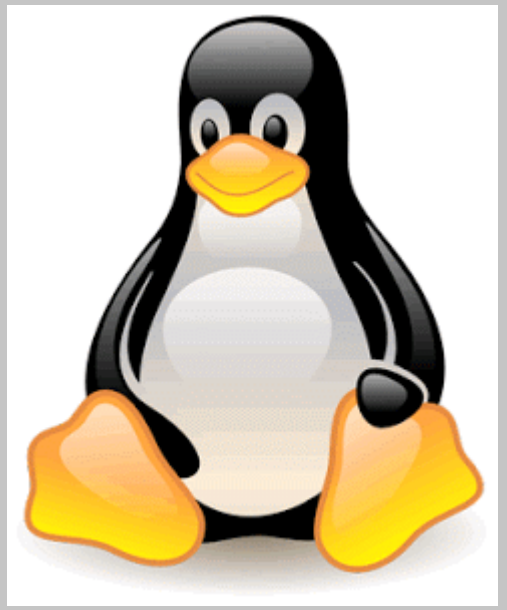

PERSISTENCE
YEAH!
memegenerator.net

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**

Switch Light

Cumulus Linux

MLNX-OS

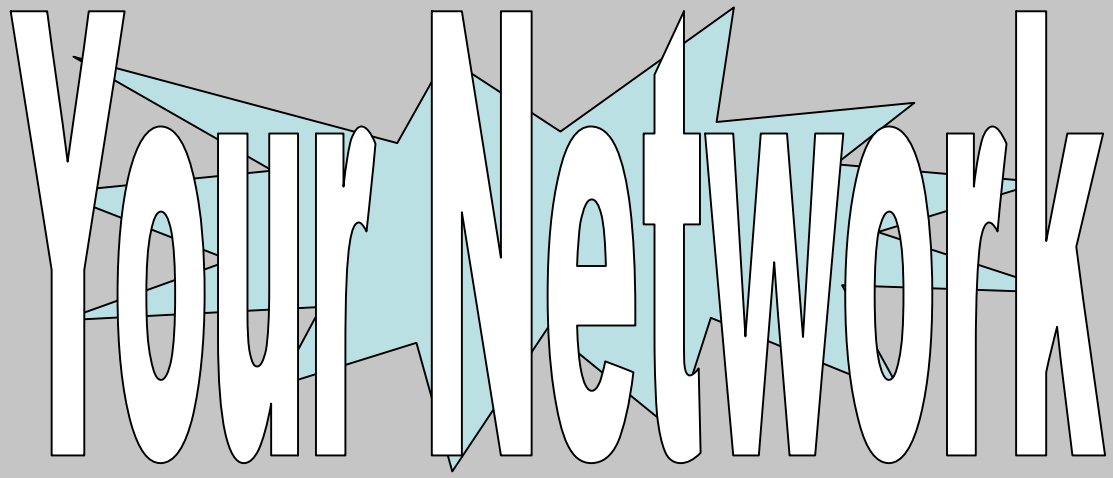
- **Compromise of Firmware through Unauthorized Access**

Switch Light

Cumulus Linux

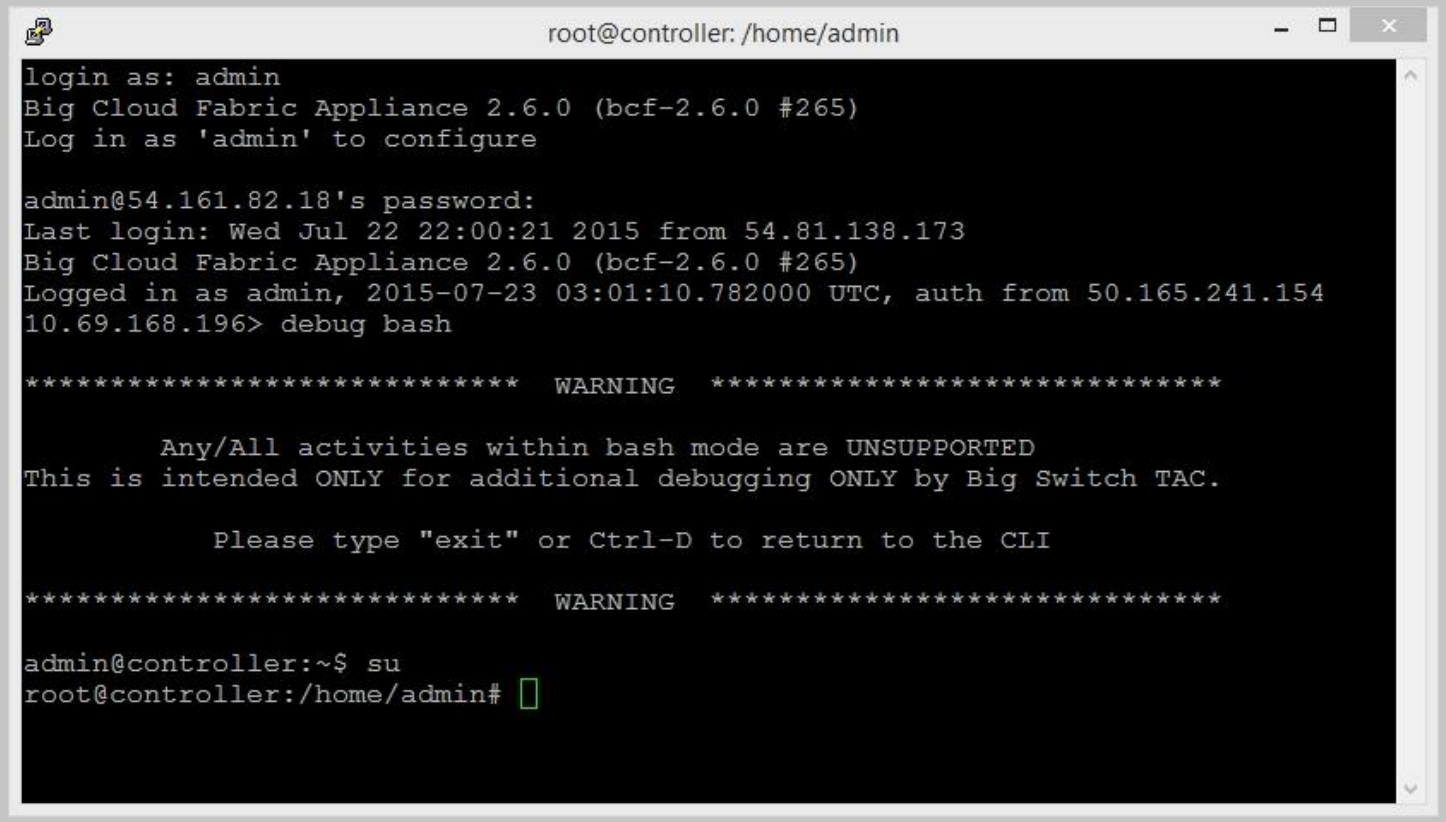
MLNX-OS

This Means

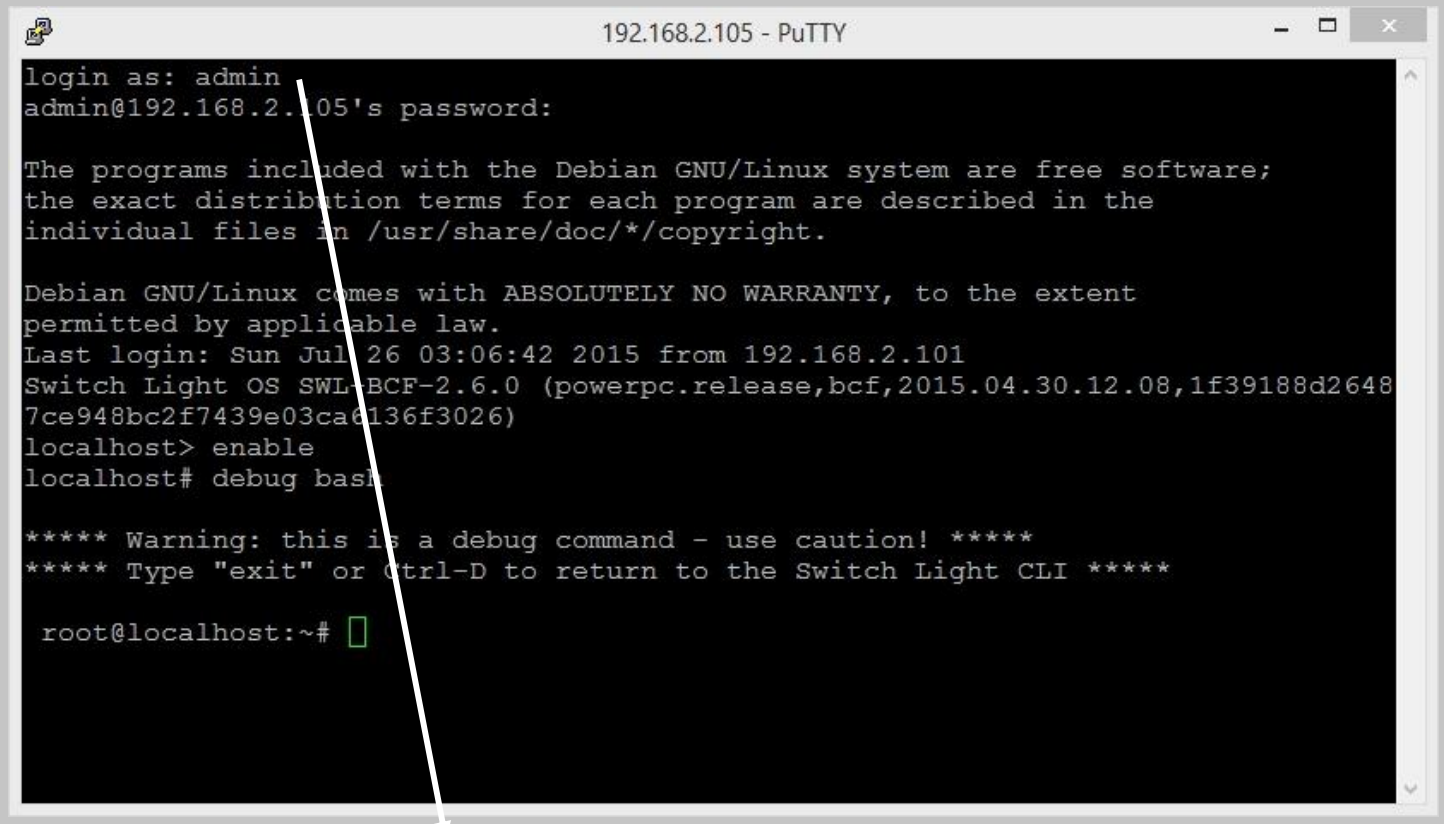


Is One Key Logger Away!

Big Cloud Fabric (Controller)

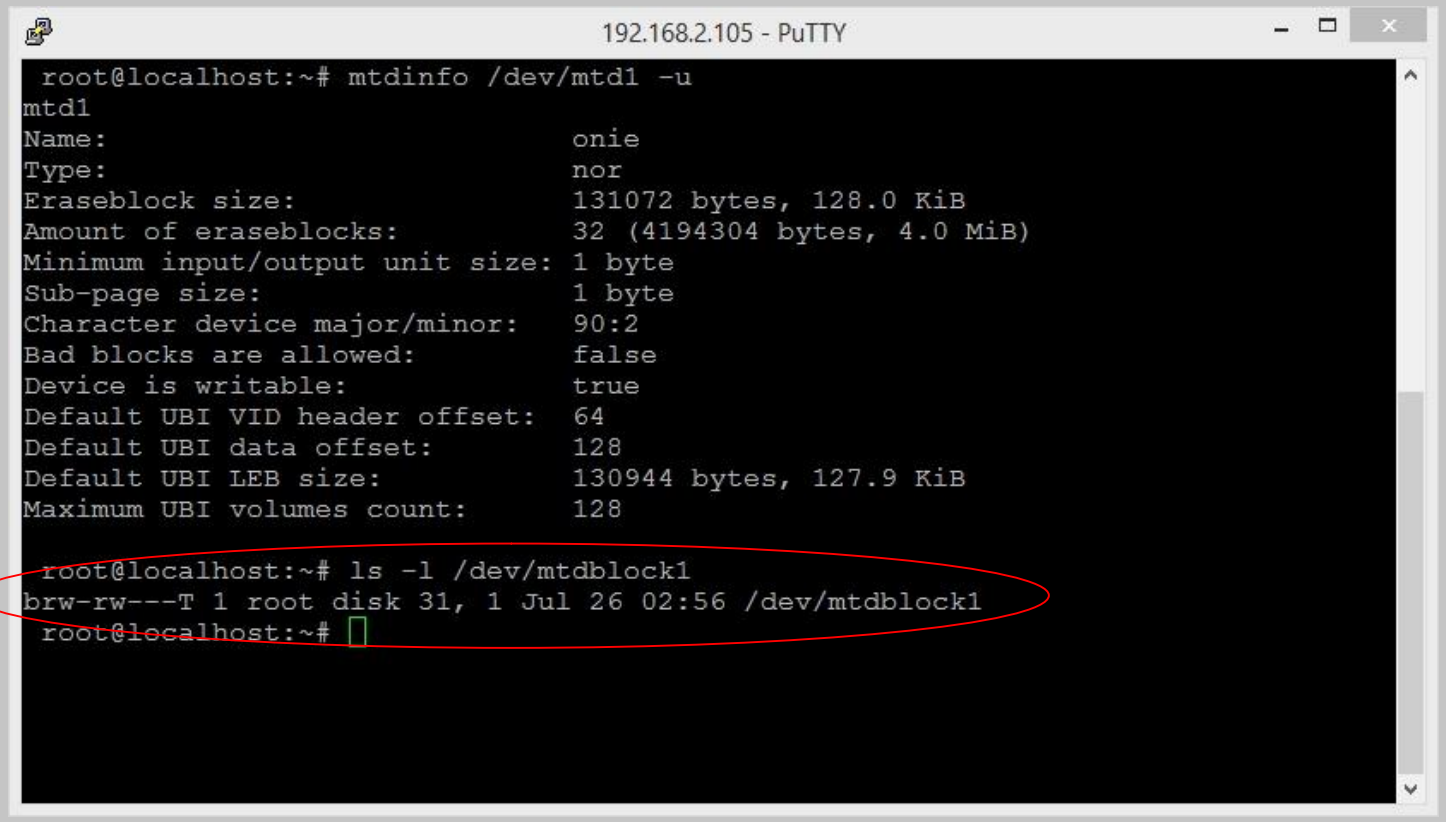


Switch Light

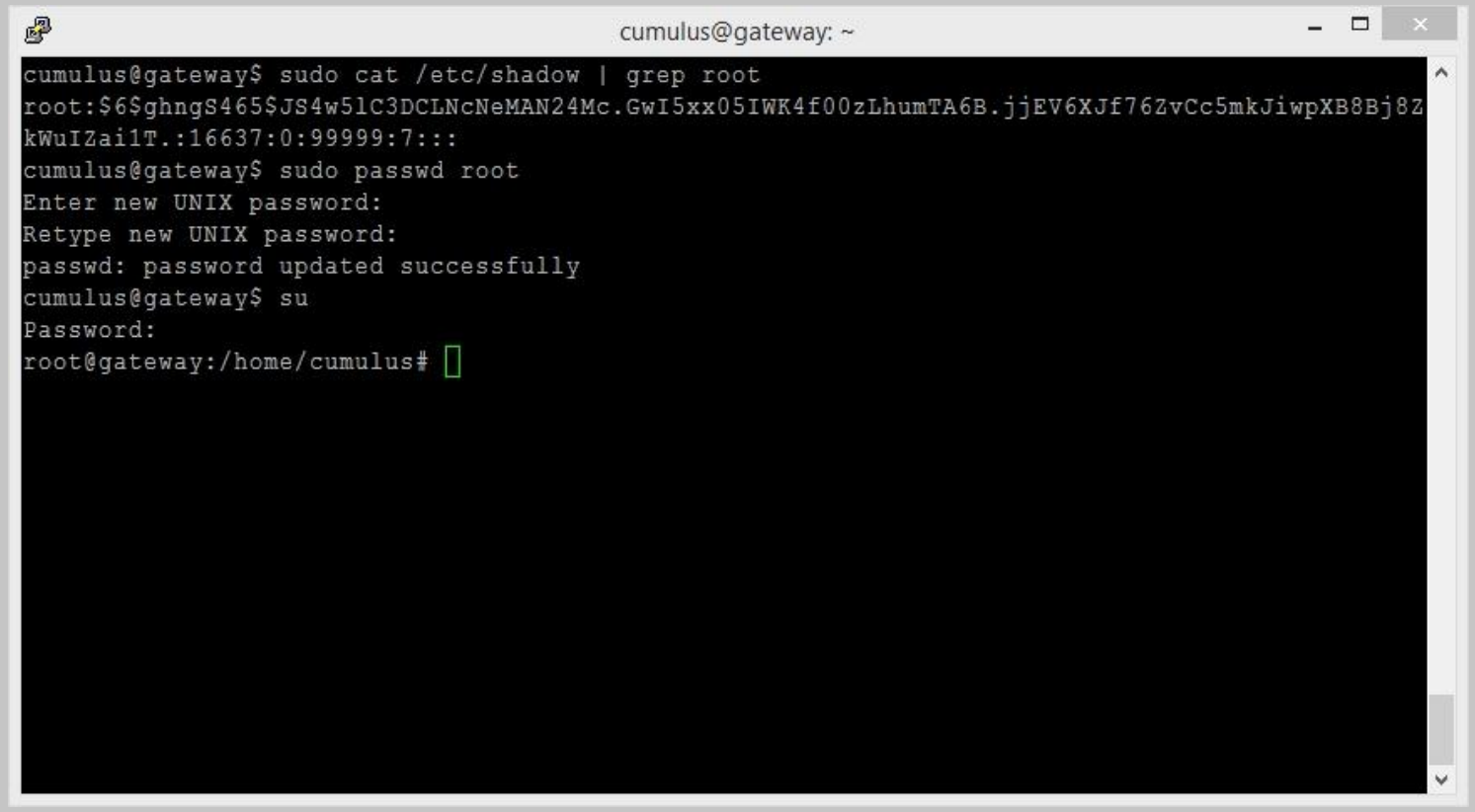


admin:x:0:0::/root:/usr/bin/pcli

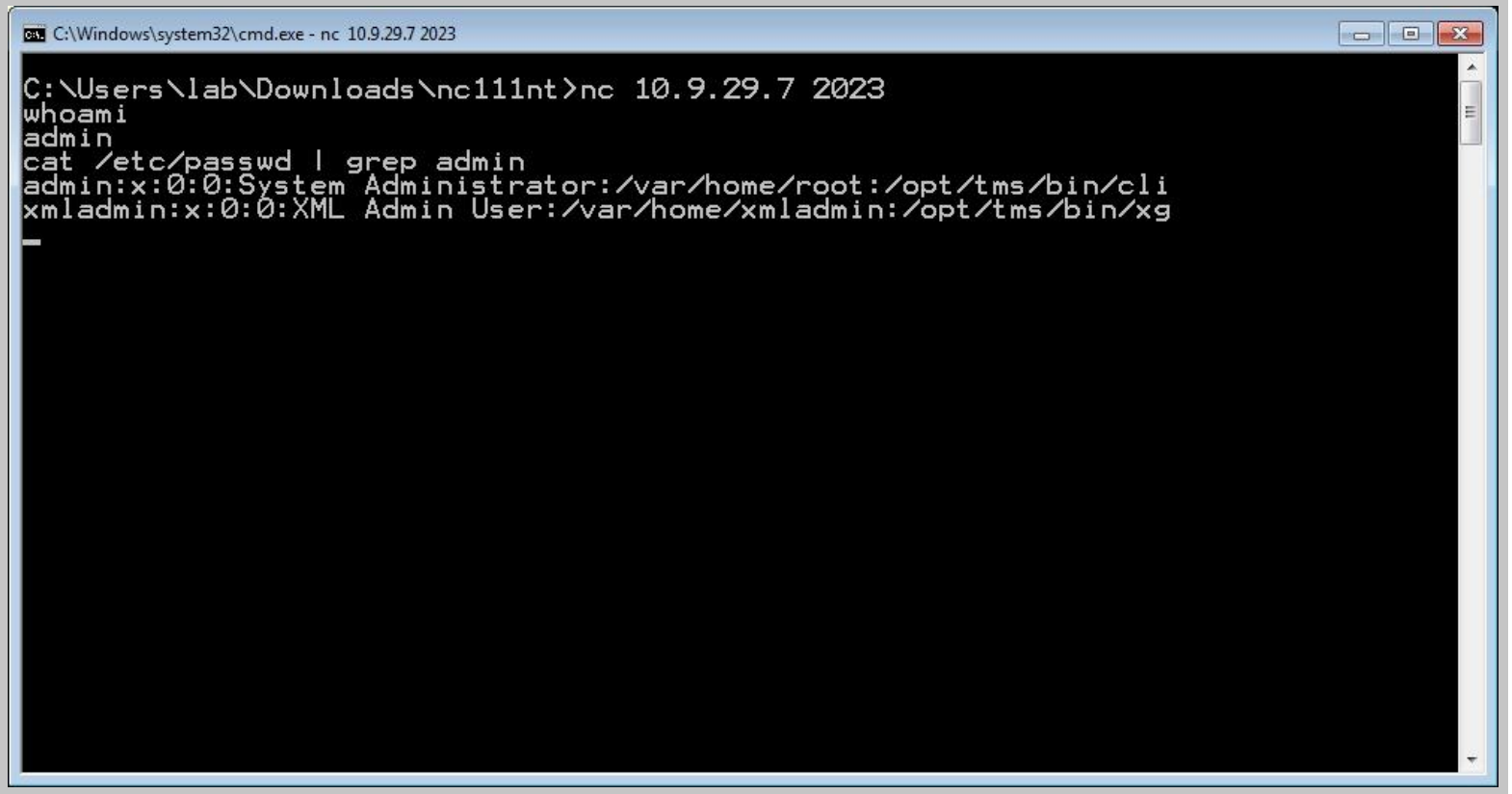
Switch Light (Exposed ONIE Partition)



Cumulus (sudo)



MLNX-OS (Backdoor)



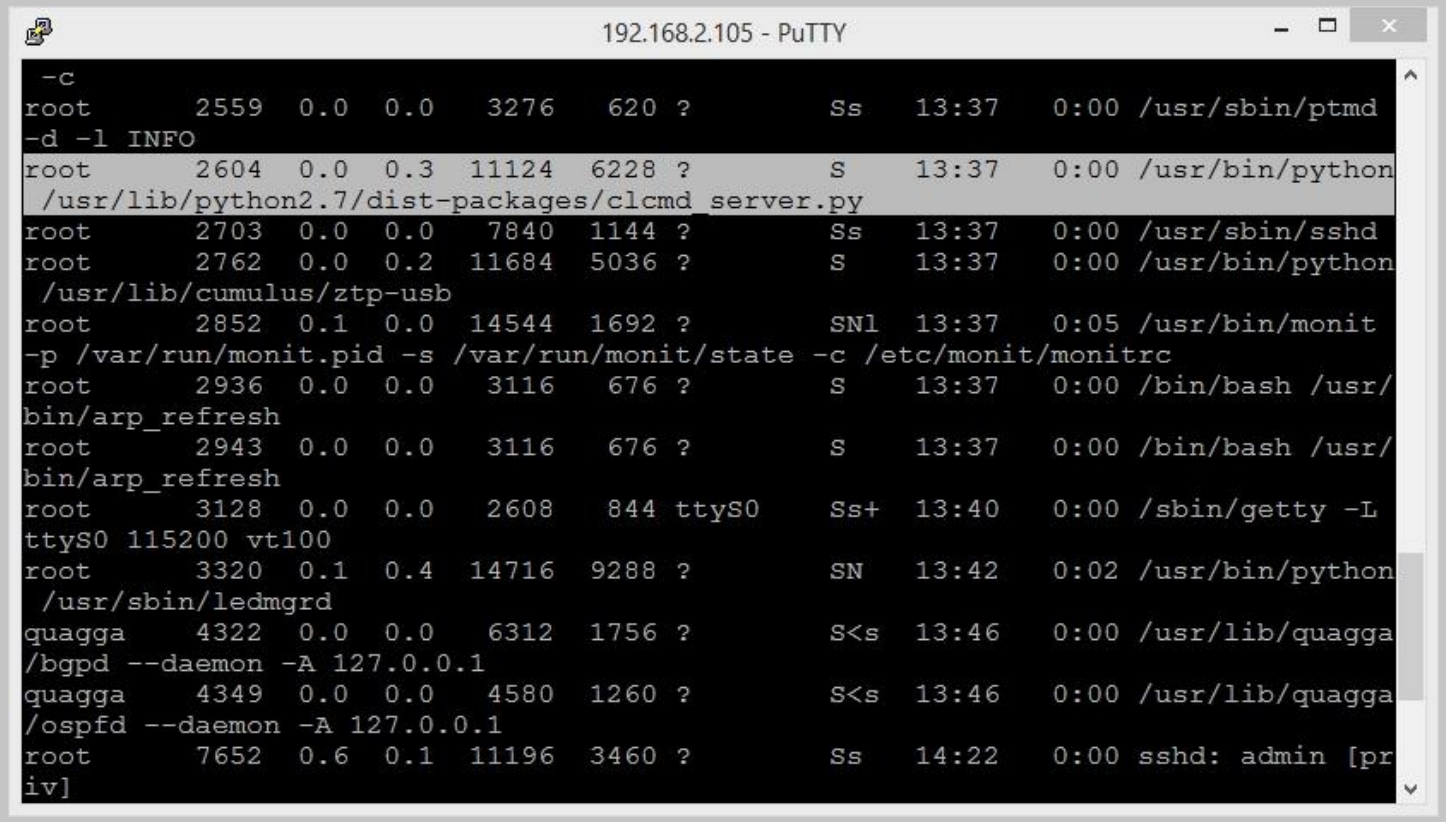
And Now Some Pwnage . . .

Sorry Cumulus Linux!

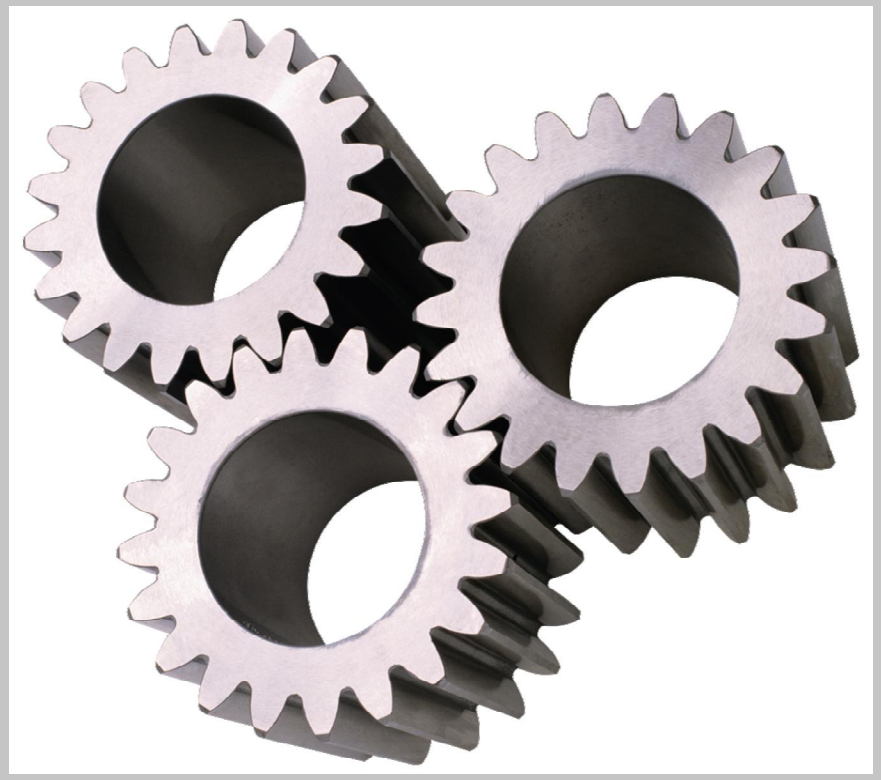
Zero-Day Exploit

- 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”

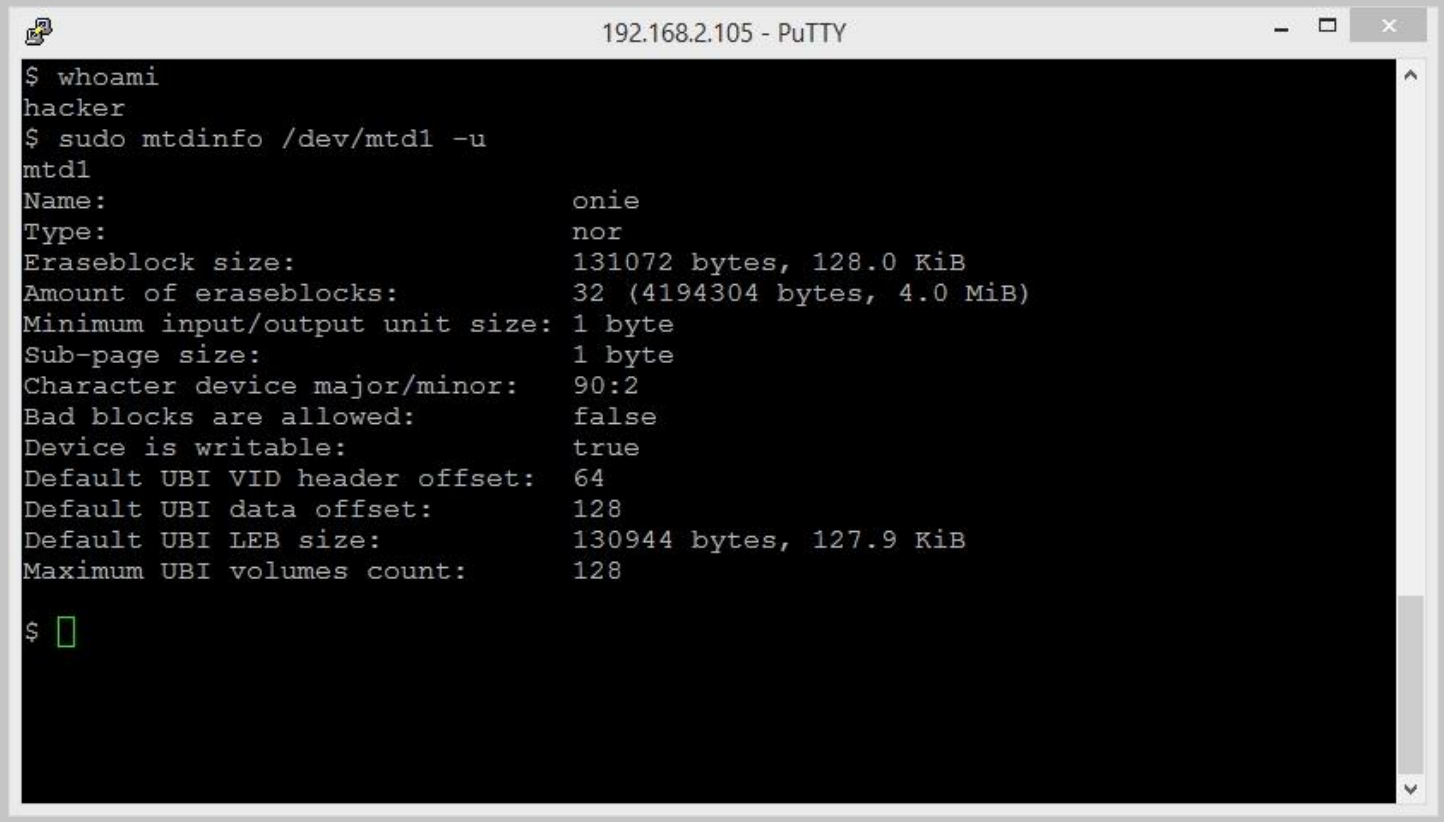
CLCMD-SERVER Running On A Switch



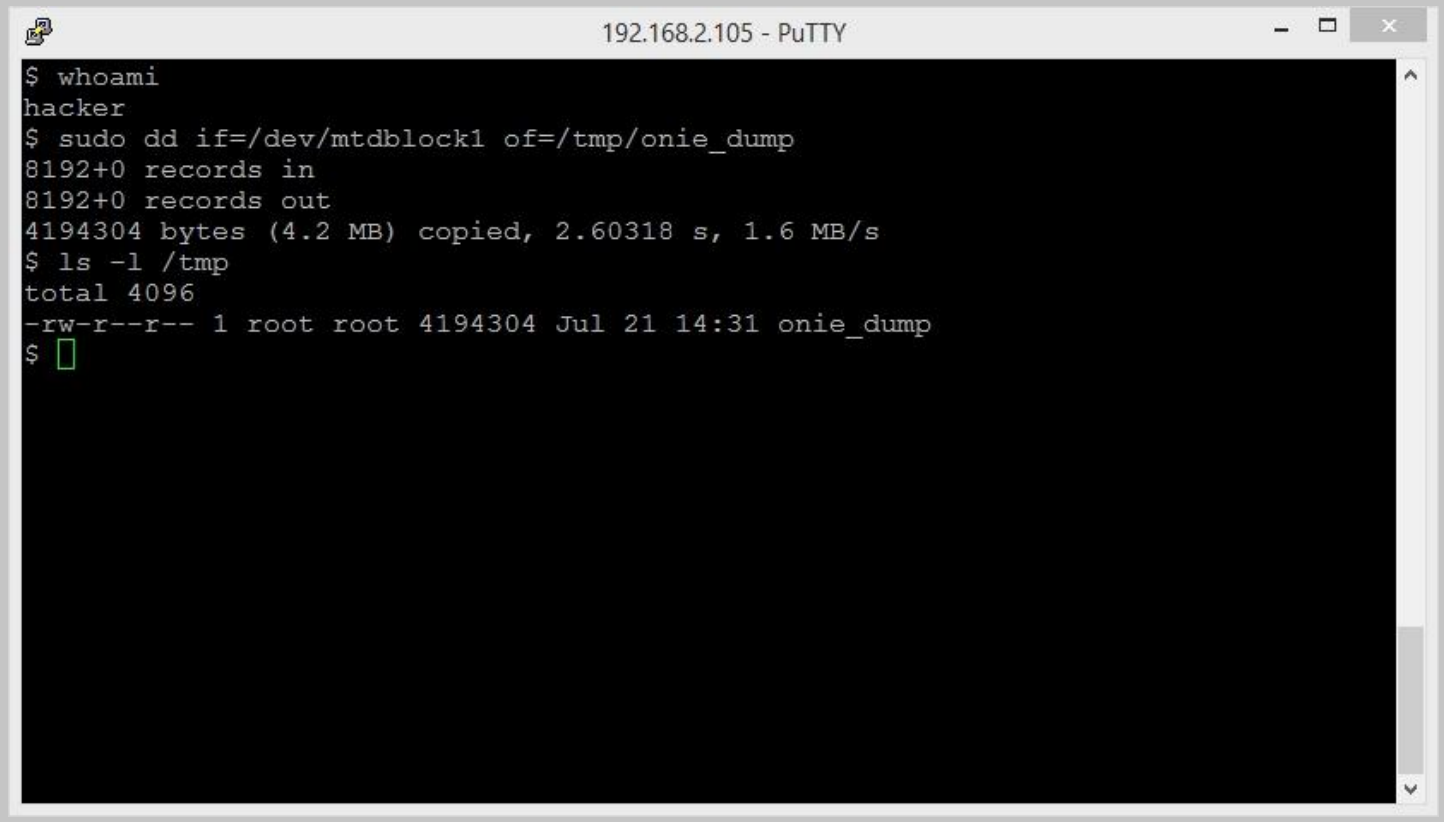
Demonstration



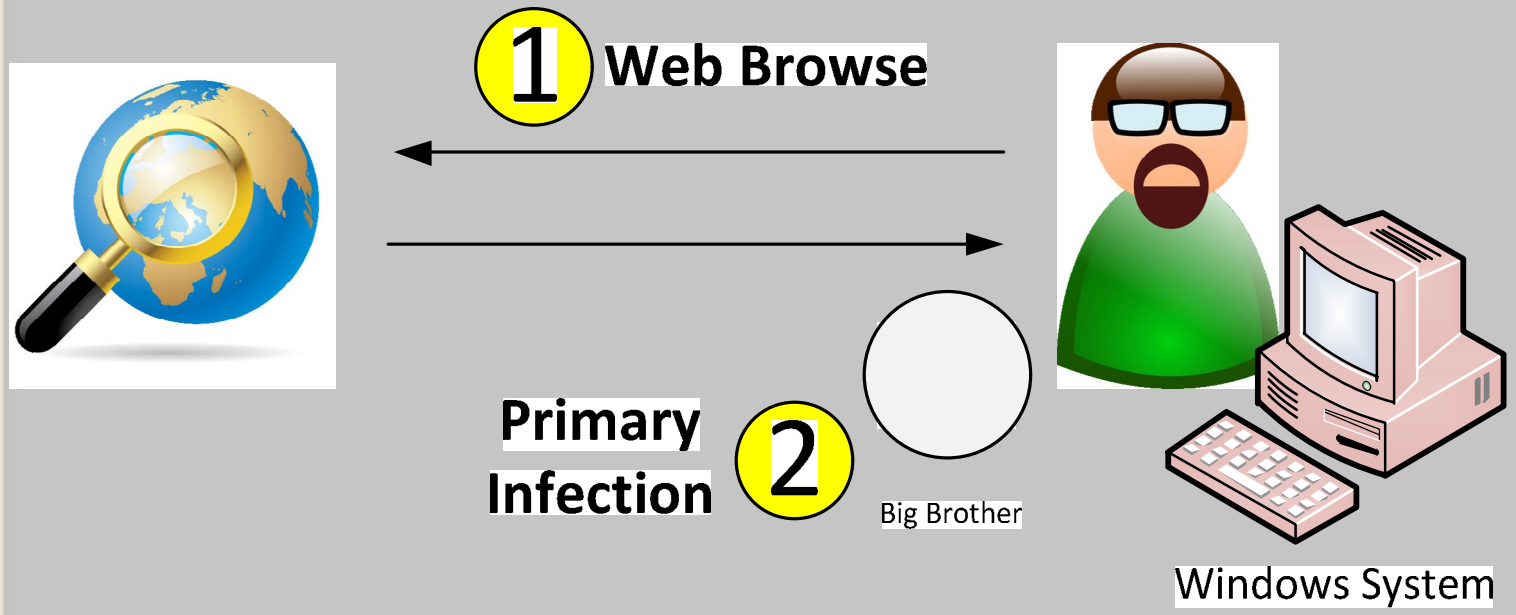
Exposed ONIE Partition



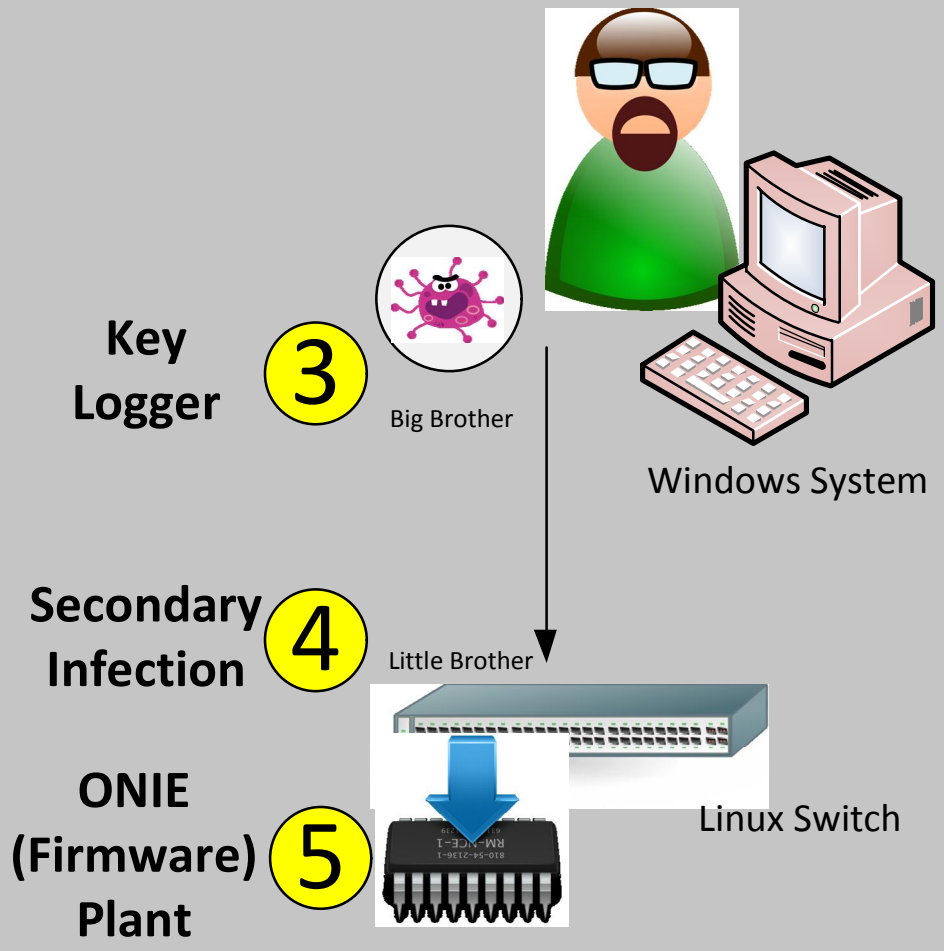
Exposed ONIE Partition



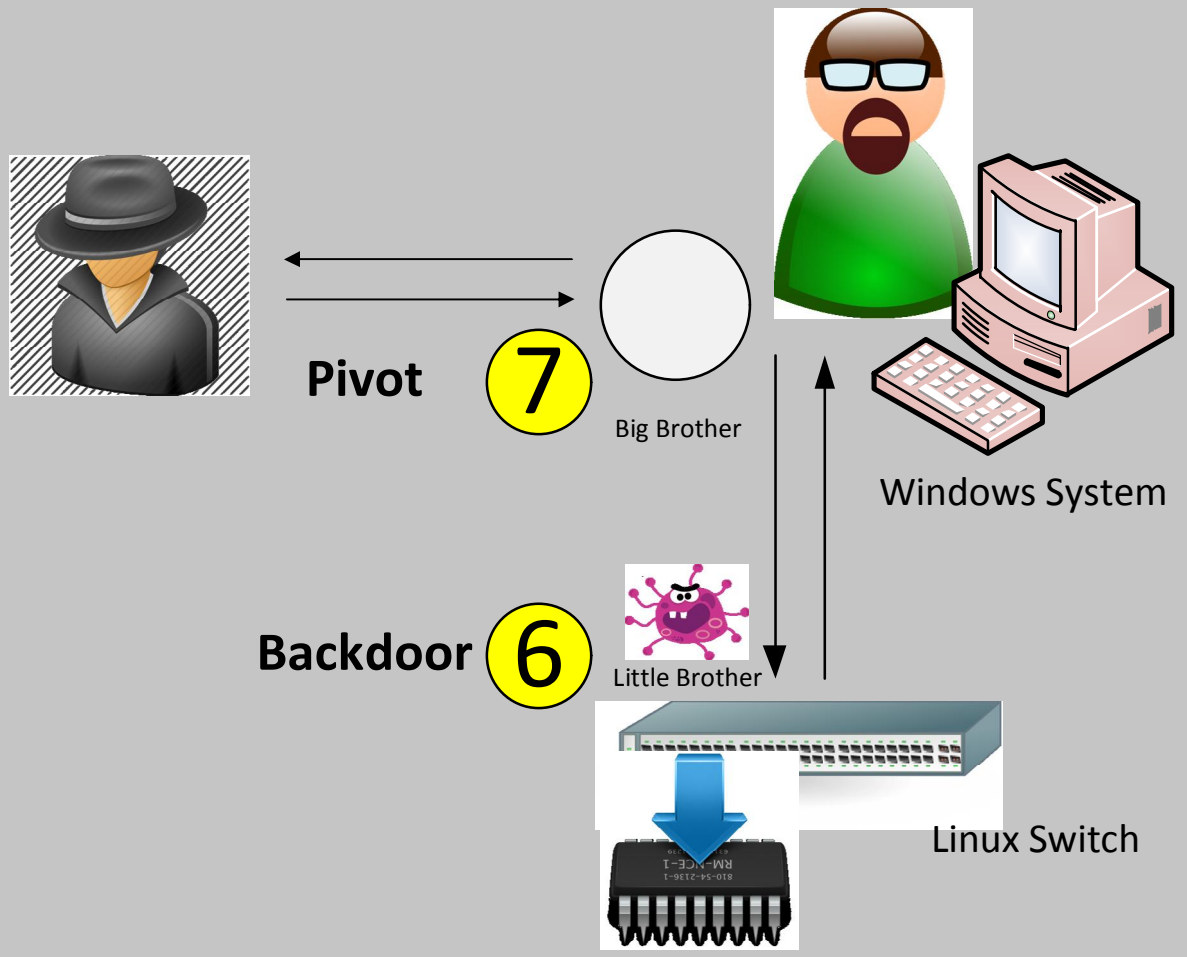
Demonstration (Scenario)



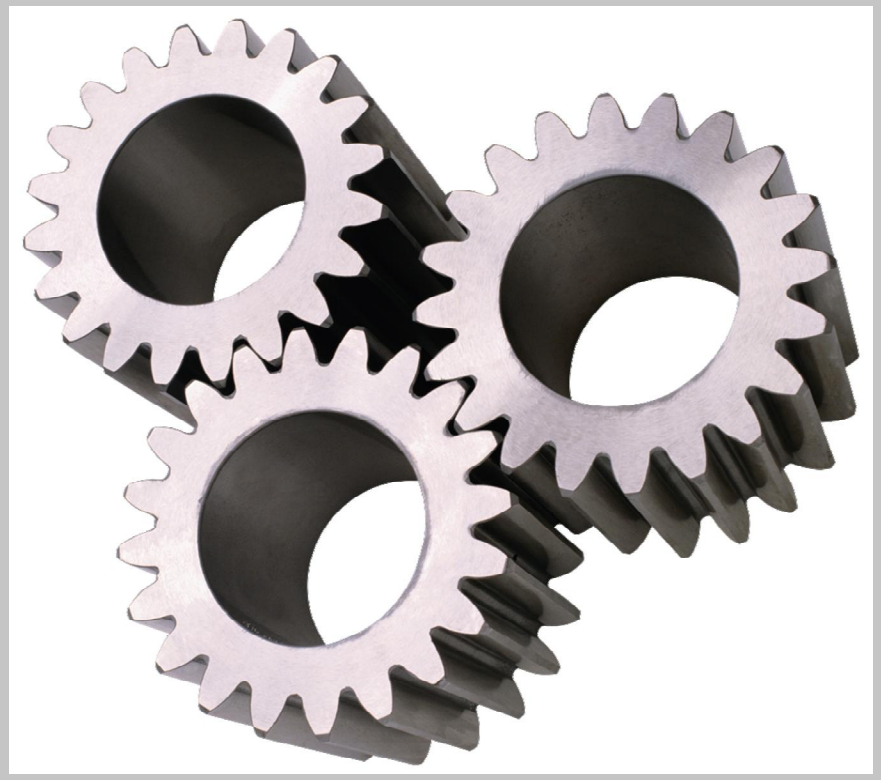
Demonstration (Scenario)



Demonstration (Scenario)



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

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

- 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 presense 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://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=MTX_8adfcbf6e0834d5a82564b4825
- https://github.com/mellanox-openstack/mellanox-eswitchd
- http://zeromq.org/intro:read-the-manual


Q&A