Hijacking the Cloud: Systematic Risk in Datacenter Management Networks

SESSION ID: CSV-W04A

Michael Cotton

Chief Security Architect
Digital Defense Inc.
@mcotton256

Out of Band Vectors…

- Renewed Focus in Security
  - Break Traditional Paradigms
  - Not CVE / Common-Config Flaws
  - Trust Relationships / Network Architecture
- Not a Theoretical Talk
  - Technical Details
  - Highlight Specific Tactics
  - Video Demonstrations

<<[[[IPMI PXE DEMO]]]>>
Sector size (logical/physical): 512B/512B
Stealing Password Hashes ...
Changing Desktop Wallpaper ...
acer

Datacenter Management Networks

- Central Command and Control Networks for Large Deployments
  - Large Datacenters: 1,000+ Servers: Can't manage manually
  - Still need to do Inventory / Power-Control / BIOS etc.
- Handles Tasks Typically Associated with Physical Access
  - Network Controllable Power/On-Off Control
  - BIOS Reconfiguration and Remote Access
  - KVM and Remote CD-ROM Capability
  - Node Re-Imaging / Re-Installation

Side-Channel Attack Vectors

- Side-Channels present a tremendous threat
  - Break Traditional Security Controls
  - Completely Bypass Existing Protections (examples)
    - RSA 4096 Bit Key Extraction Attack (Dec. 2013)
    - Extracting Passwords using Laser Microphone
    - Reading Keystrokes from Computers on Same Power Segment
  - One – Huge Limiting Factor
    - Typically they require *Physical Proximity*

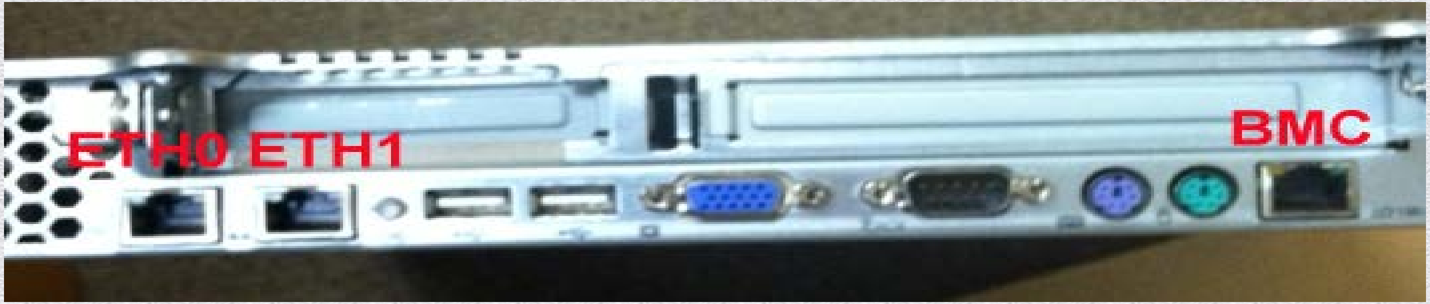
Datacenter Networks & Side-Channels

- But Physical Proximity isn't Always Necessary
  - Some Vectors Contain:
    - All the Advantages of Traditional Side-Channel Attacks
    - Without the Need for Physical Proximity
  - Two Attack Surfaces Come to Mind in Relation to Datacenters:
    - Virtualization / Physical Layer Attack Surface
      - People have talked about this to death (intense scrutiny)
    - Networked Baseboard Attack Surface
      - This is what we'll be covering today (Lateral Movement)

Management Network Access

VLAN Segmentation & Shared NIC

- Baseboard controllers, used to typically come on dedicated NICS.
  - Now everyone switching to Shared NIC / VLAN segmentation
    - Dedicated “BMC” slot (pictured) replaced in low/mid server range
    - ETH0 now has one RJ-45 jack, two MAC addresses:

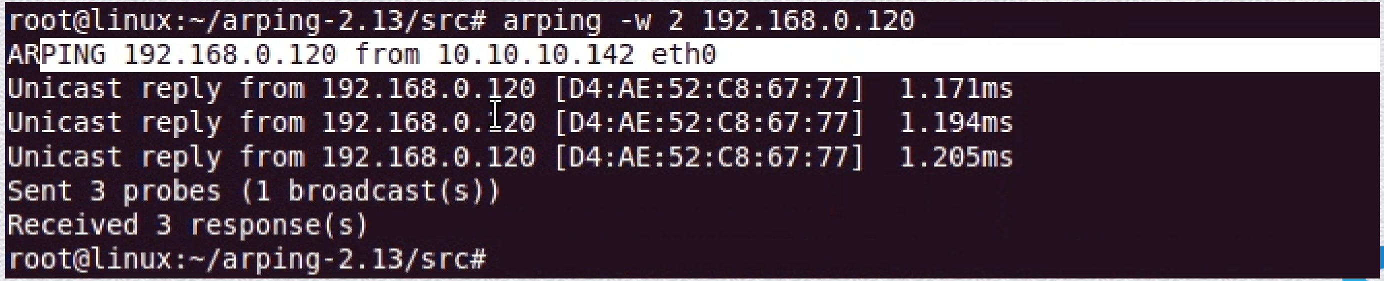


Baseboards: Network Recon

- Shared NIC makes this really interesting
  - Normal Method: Send RMCP-Hello Message to Every IP Address
  - Indirect Method: Finds cloaked / misconfigured BMCs using MAC (large subnets)
    - Can Give you ‘Side Door’ Access into important systems (Domain Controller etc.)
    - If model has two onboard ETH controllers the following is often true:
      - ETH0: d4:ae:52:c8:67:75
      - ETH1: d4:ae:52:c8:67:76 (eth0+1)
      - ETH0/BMC: d4:ae:52:c8:67:77 (eth0+2)
    - Correlation can also be done off-subnet:
      - Depends on environment: netbios/snmp/etc hand arp out

Baseboard Recon: Cloaked Addresses

- Using MAC to find the side-door into important systems:
  - Use Thomas Habets version of arping w/ RARP
    - Can locate cloaked ip's on large subnets: (vendor/moved/dhcp/etc.)
      - arping –w 2 d4:ae:52:c8:67:77 (use +mac method)
      - arping –w 2 192.168.0.120 (vendor static default)



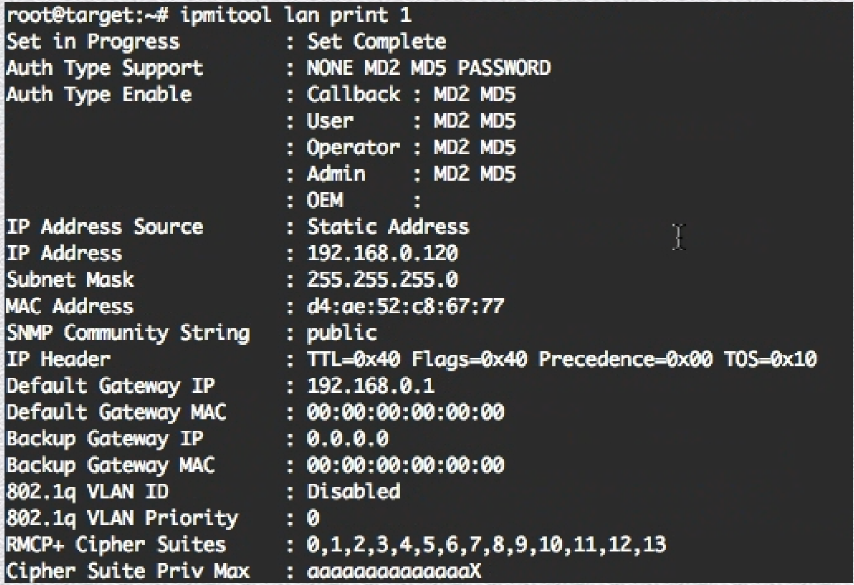
```
root@linux:~/arping-2.13/src# arping -w 2 192.168.0.120
ARPING 192.168.0.120 from 10.10.10.142 eth0
Unicast reply from 192.168.0.120 [D4:AE:52:C8:67:77]  1.171ms
Unicast reply from 192.168.0.120 [D4:AE:52:C8:67:77]  1.194ms
Unicast reply from 192.168.0.120 [D4:AE:52:C8:67:77]  1.205ms
Sent 3 probes (1 broadcast(s))
Received 3 response(s)
root@linux:~/arping-2.13/src#
```

BMC: VLAN Segmentation

- This doesn’t bother most IT professionals because
  - BMC’s should *always* be separated on their own VLANs
  - We’re not here to talk about bad-network setups…
- Some Typical VLAN Network Access Controls:
  - VLAN-ID: BMC Can be Queried through Local Bus
  - NIC Port: Same RJ-45 Jack (Not Port Controlled)
  - MAC Address: Layer 2 Controllable (Spoofable)
    - ifconfig eth0 hw ether 02:08:5C:3F:05

Flipping The NIC:

- Leverage System-Bus Trump
    - Local Bus PW Override
    - Dedicated Hosting Scenario
    - Shared NIC Hardware
        - Query VLAN Information
        - Knock BMC NIC Off
        - Put Eth0 Online
            - Spoof MAC
            - Same IP / VLAN Etc.



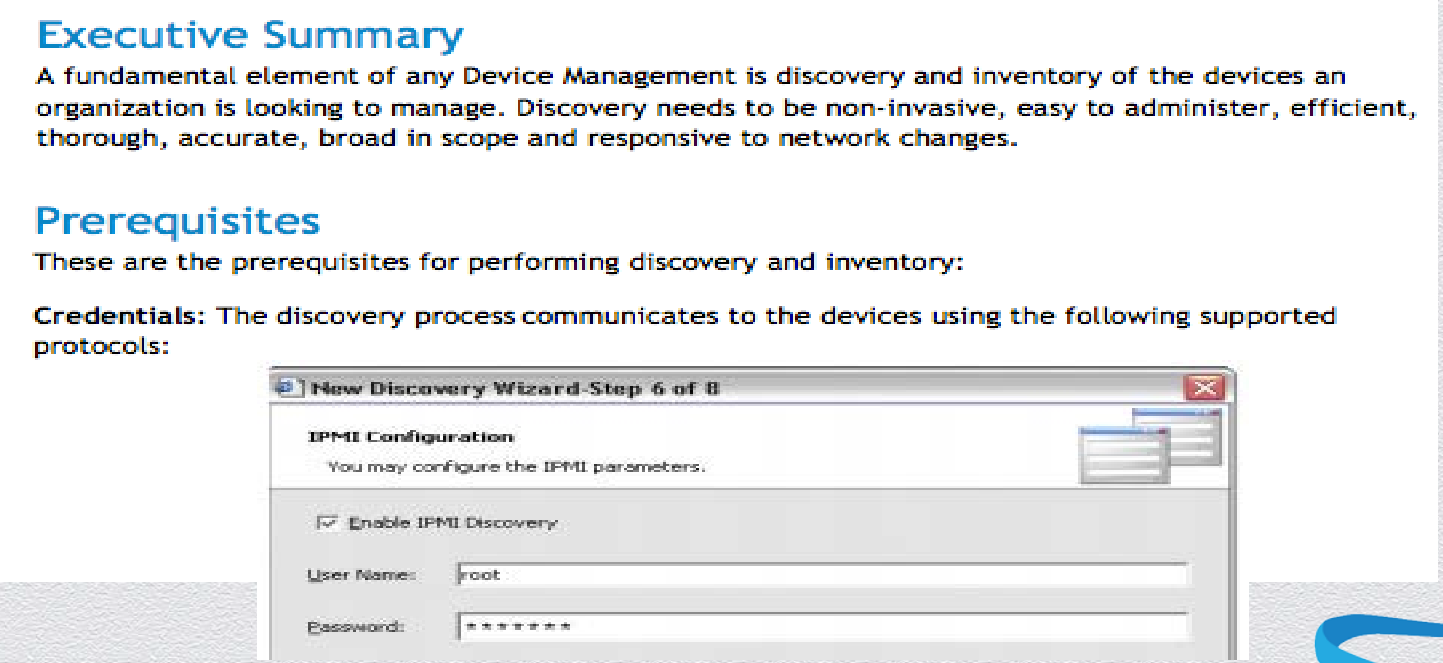
```
root@target:~# ipmitool lan print 1
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 PASSWORD
Auth Type Enable        : Callback : MD2 MD5
                        : User     : MD2 MD5
                        : Operator : MD2 MD5
                        : Admin    : MD2 MD5
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 192.168.0.120
Subnet Mask             : 255.255.255.0
MAC Address             : d4:ae:52:c8:67:77
SNMP Community String   : public
IP Header               : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
Default Gateway IP      : 192.168.0.1
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 0,1,2,3,4,5,6,7,8,9,10,11,12,13
Cipher Suite Priv Max   : aaaaaaaaaaaaaaaX
```

We’re Online, Now What?

- Target Management Server
  - Large deployments usually do:
    - Inventory sweeps for new hosts using RMCP/IPMI…
    - Send Power On/Off/Reboot Through RMCP/IPMI
  - You don’t need to go to the management server…
    - The management server will come to you
    - All it needs is a plausible peer to talk to
    - Often can do this ‘on demand’ through client hosting apps.

IPMI Discovery & Inventory…

- Sweeping for Inventory: NMS



Executive Summary

A fundamental element of any Device Management is discovery and inventory of the devices an organization is looking to manage. Discovery needs to be non-invasive, easy to administer, efficient, thorough, accurate, broad in scope and responsive to network changes.

Prerequisites

These are the prerequisites for performing discovery and inventory:

Credentials: The discovery process communicates to the devices using the following supported protocols:

New Discovery Wizard-Step 6 of 8

IPMI Configuration

You may configure the IPMI parameters.

☑ Enable IPMI Discovery

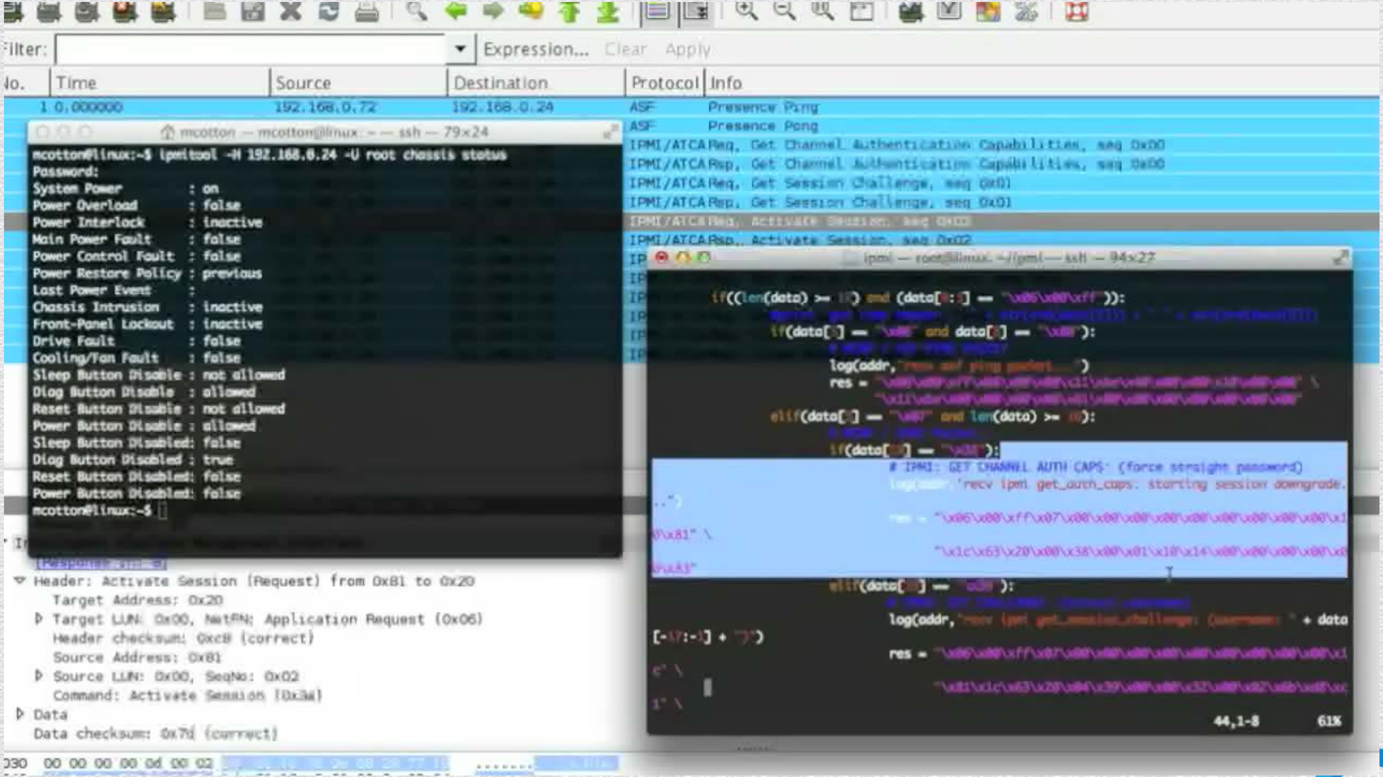
User Name: root

Password: *******

Rogue Agent: Session Downgrade Attacks

- Discovery sweeps encourage 1 username/pass
  - Typically very complex: password capture == massive exposure
- Tools try to be *very* compatible
  - Client will talk at highest level of security *the agent allows*
  - (Similar to SNMPv3 vs. SNMPv2 management systems)
  - If agent only claims to support lower, they’ll downgrade (straight-key)
- NMS inventory/monitor sweep subnets, authing to 623/udp
  - Used for both discovery of new nodes, status checks of existing nodes.
  - rogue agent => straight-key-auth downgrade => password

Rogue Agent: Password Capture (Demo)



Filter:
Expression...
Clear
Apply
mcotton — mcotton@linux: ~ — ssh — 79×24
ipmi — root@linux: ~/ipmi — ssh — 94×27

```
No.  Time        Source        Destination   Protocol  Info
   1 0.000000    192.168.0.72  192.168.0.24  ASF       Presence Ping
                                             ASF       Presence Pong
                                             IPMI/ATCA Req, Get Channel Authentication Capabilities, seq 0x00
                                             IPMI/ATCA Rsp, Get Channel Authentication Capabilities, seq 0x00
                                             IPMI/ATCA Req, Get Session Challenge, seq 0x01
                                             IPMI/ATCA Rsp, Get Session Challenge, seq 0x01
                                             IPMI/ATCA Req, Activate Session, seq 0x02
                                             IPMI/ATCA Rsp, Activate Session, seq 0x02
```

```
mcotton@linux:~$ ipmitool -H 192.168.0.24 -U root chassis status
Password:
System Power         : on
Power Overload       : false
Power Interlock      : inactive
Main Power Fault     : false
Power Control Fault  : false
Power Restore Policy : previous
Last Power Event     :
Chassis Intrusion    : inactive
Front-Panel Lockout  : inactive
Drive Fault          : false
Cooling/Fan Fault    : false
Sleep Button Disable : not allowed
Diag Button Disable  : allowed
Reset Button Disable : not allowed
Power Button Disable : allowed
Sleep Button Disabled: false
Diag Button Disabled : true
Reset Button Disabled: false
Power Button Disabled: false
mcotton@linux:~$
```

```
        if((len(data) >= [illegible]) and (data[[illegible]] == "\x06\x00\xff")):
            [illegible]
            if(data[[illegible]] == "[illegible]" and data[[illegible]] == "[illegible]"):
                [illegible]
                log(addr,"[illegible]")
                res = "[illegible]" \
                      "[illegible]"
            elif(data[[illegible]] == "[illegible]" and len(data) >= [illegible]):
                [illegible]
                if(data[[illegible]] == "[illegible]"):
                    # IPMI: GET CHANNEL AUTH CAPS (force straight password)
                    log(addr,"recv ipmi get_auth_caps: starting session downgrade...")
                    res = "\x06\x00\xff\x07\x00\x00\x00\x00\x00\x00\x00\x00\x00\x1[illegible]\x81" \
                          "\x1c\x63\x20\x00\x38\x00\x01\x10\x14\x00\x00\x00\x00\x0[illegible]\x43"
                elif(data[[illegible]] == "[illegible]"):
                    [illegible]
                    log(addr,"[illegible]" + data[-17:-1] + "[illegible]")
                    res = "\x06\x00\xff\x07\x00\x00\x00\x00\x00\x00\x00\x00\x00\x1[illegible]" \
                          "\x81\x1c\x63\x20\x04\x39\x00\x00\x32\x00\x02[illegible]" \
                                                                    44,1-8        61%
```

```
▾ I[illegible]
  [illegible]
  ▽ Header: Activate Session (Request) from 0x81 to 0x20
      Target Address: 0x20
    ▷ Target LUN: 0x00, NetFN: Application Request (0x06)
      Header checksum: 0xc8 (correct)
      Source Address: 0x81
    ▷ Source LUN: 0x00, SeqNo: 0x02
      Command: Activate Session (0x3a)
  ▷ Data
    Data checksum: 0x7d (correct)
030  00 00 00 00 0d 00 02 [illegible]   .......[illegible]
```

VLAN Internal Firewall Rules

- Somewhat different for every site:
  - Often times MAC filtering / VLAN-ID is the only traffic protection in place.
  - Often times can bypass basic ACLs due to nature of protocol:
    - Dealing with a UDP connectionless protocol for RMCP/IPMI
    - Client can request simple-session; Spoof commands blindly
    - Know Control Server: src_ip, src_mac, ~dst_ip, dst_port
    - Also know when server is doing inventory sweeps
      - Ideal case for Firewall Rule Bypass Tactics
      - Related / Establish Rule Sets etc.

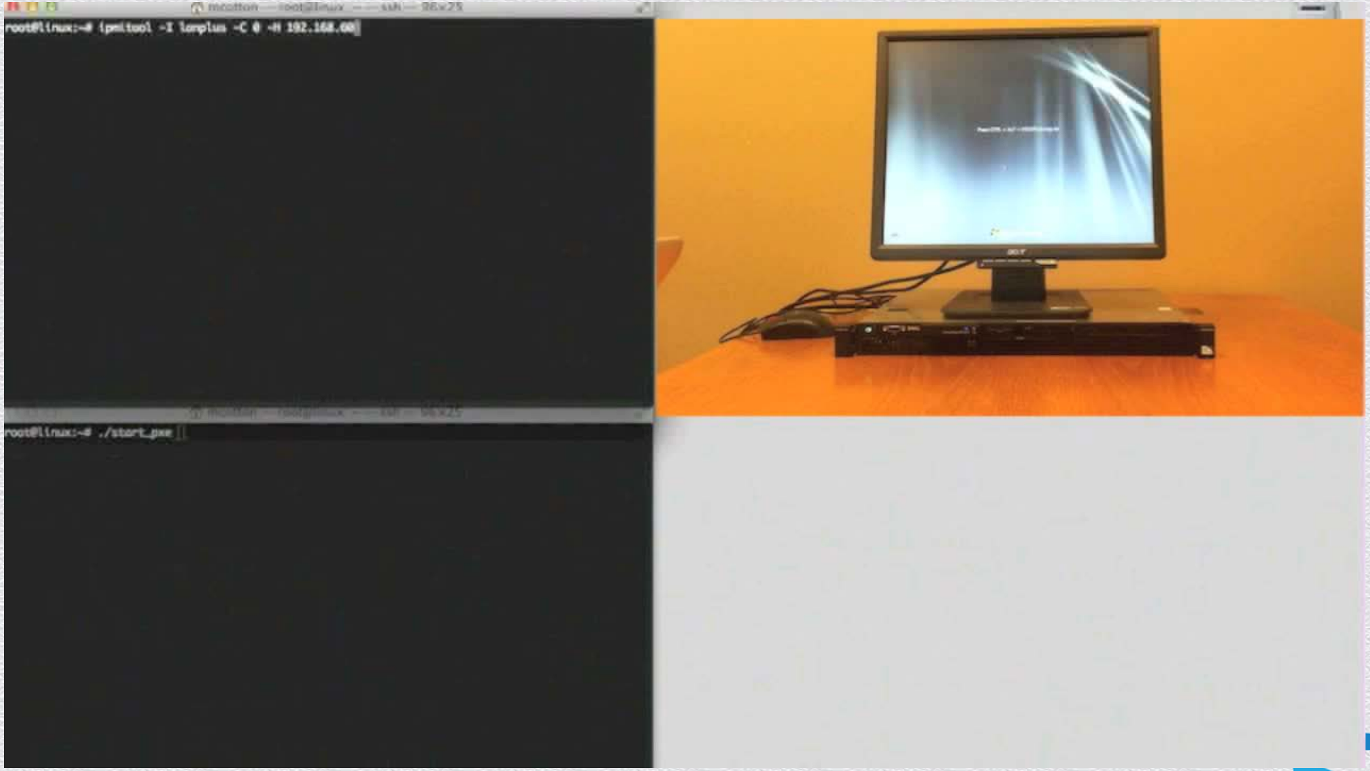
Management VLAN: Node Re-Imaging:

- Typically Done using either Remote-ISO or Network Boot (PXE):
  - Quick Install of ‘Gold’ OS’s
    - Power Cycle Node
    - Change Boot Device
    - Boot to Imaging Ramdisk
    - Partition & Copy - Gold-Image
  - Quickly Turn up Dedicated Hosts
    - Install Client Configuration / Accounts.
    - Setup Hostname / IP Etc.

How an Attacker Might Use it (Demo)

- Take System Offline / Force Remote Boot
- RamDisk boots & modifies installed OS (slightly)
  - Detect OS partitions (parted)
  - Mount offline ntfs/ext4 partitions (r/w)
    - Backdoor binaries (No kernel protections anymore)
    - Dump hashes (true system32/config/sam access)
      - No need to rely on repair sam anymore
    - Steal data etc.
  - Clean Up & Reboot Back to Primary OS

Baseboard: Offline Attacks (Demo)



mcotton — root@linux — — ssh — 96x25

```
root@linux:~# ipmitool -I lanplus -C 0 -H 192.168.00
```

mcotton — root@linux — — ssh — 96x25

```
root@linux:~# ./start_pxe
```

SOLUTIONS

Management Network: Solutions

- Ensure Integrity of Management Network (Degrades)
  - Heavily Protected / Segmented VLAN Access
  - Review: Internal Firewall Rules Against Rogue Agent Vectors
  - Be Aware of Shared NIC Issues
- Lock Down: Network Management Systems
  - Focus on Client Protocol Lock-Down As Well
  - Ban Straight-Key Auth: Force at least MD5 (salted)
  - Use Full Allowed Password/Key Length (16 or 20)

Wrap Up / Takeaways:

- Look Outside Traditional Paradigms
  - Datacenters Have Complex Security Boundaries
  - Consider Non-CVE/Common Configuration Vulns
  - Consider Creative Attacker Tactics
- Examine Trust Relationships
  - Often Times at Play in recent Data Breaches
  - Don’t Blindly Associate Network Position w/ Trust
  - Don’t Neglect Security on ‘Segmented’ Interfaces

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank You!

Questions: Mike.Cotton@ddifrontline.com