USS FRANKENFORGE
NCC-1337

MISSION DEBRIEF
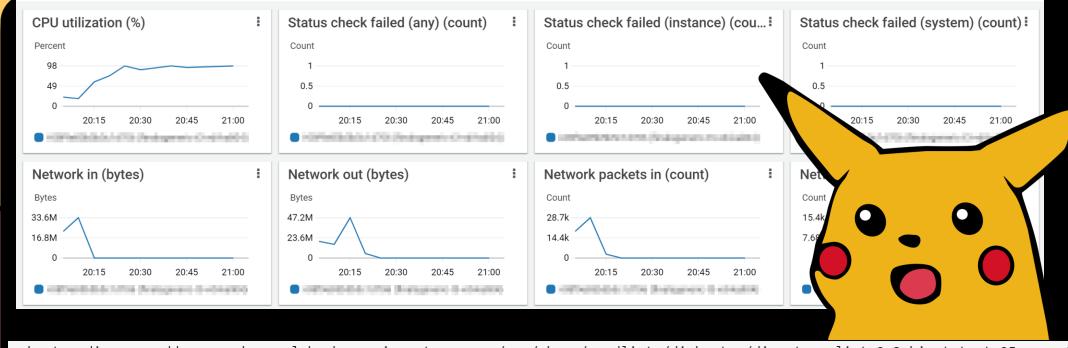
ME MAKING MEMES

LUCAS NOT LIKING JOKES

CPU utilization (%)

Percent

98

49

0

20:15   20:30   20:45   21:00

Status check failed (any) (count)

Count

1

0.5

0

20:15   20:30   20:45   21:00

Status check failed (instance) (cou...

Count

1

0.5

0

20:15   20:30   20:45   21:00

Status check failed (system) (count)

Count

1

0.5

0

20:15   20:30   20:45   21:00

Network in (bytes)

Bytes

33.6M

16.8M

0

20:15   20:30   20:45   21:00

Network out (bytes)

Bytes

47.2M

23.6M

0

20:15   20:30   20:45   21:00

Network packets in (count)

Count

28.7k

14.4k

0

20:15   20:30   20:45   21:00

Net...

Count

15.4k

7.68

```
gobuster dir -u rockbox.warehouse.lebonboncroissant.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-big.txt -t 25 -x mp3,
dirbuster -H -u http://10.0.17.10:80 -l /usr/share/wordlists/dirb/common.txt
dirbuster -H -u http://10.0.17.10:80 -l /usr/share/wordlists/dirb/big.txt
gobuster dir -u 10.0.17.11 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
gobuster dir --url https://10.0.17.10 --wordlist directory-big.txt -k
```
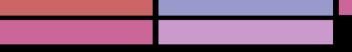
We did it, Patrick! We pentested the organization!

Junior Pentesters on the job for the first time

Kaboom?

Yes Rico, kaboom
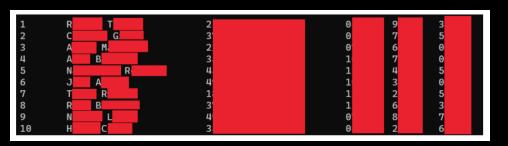
PENTEST FOIA

REDACTING IS GOOD UNTIL IT ISN'T

```
COPY billing.credit cards (id, name, number, expiration, ccv, zip) FROM stdin.
```

Image: Redacted login credential information with base64 encoded passwords from the MariaDB database.

PLC

TEAM 8

CPTC ADMINS

TEAM 8

CPTC ADMINS

YOU GET A ZIP BOMB

DIRBUSTER

DISCOVERY?

WE DID NOT MAKE A LARGE AMOUNT OF REQUESTS

SWAGGER

DOCUMENTATION IS NOT A VULN

UNAUTHENTICATED API CALLS MAY BE

BIZ VS TECH

BREAKOUT

COPYRIGHT ISSUES WITH MUSIC SERVER

PCI DOCUMENTATION ISSUES

WORLD / OSINT

Marked Safe From

Lucas

Today

Volume used t

3,093,984 MB

1,660,568 MB (

1,433,416 MB (4

DAY 2

Region

7-Jan Final (Day 1)   8-Jan Final (Day 2)   13-Nov Northeastern US Regional   13-Nov Western US Regional   23-Oct Central US Regional   23-Oct European Regional   23-Oct Middle East Regional   23-Oct New England US Regional
23-Oct South East US Regional

Command Filter (Support Wildcard)

*   Submit   Hide Filters

Command over time (MonStart=2022-01-08 08:00:00 EST, MonEnd=2022-01-08 18:00:00 EST)   ⚠

Refresh every minute

■ apt   ■ cat   ■ cd   ■ clear   ■ curl   ■ dig   ■ docker   ■ echo   ■ exit   ■ find   ■ git   ■ gobuster
■ hydra   ■ ip   ■ ls   ■ mpc   ■ msfconsole   ■ mysql   ■ nano   ■ nc   ■ nmap   ■ ping   ■ proxychains
■ ps   ■ psql   ■ rm   ■ ssh   ■ telnet   ■ tmux   ■ vim   ■ OTHER

Top Command Ranking   ⚠

Refresh every minute

	cmd_root ⬍	team_count ⬍	total_count ⬍
1	ls	15	2289
2	cd	15	1239
3	nmap	15	756
4	curl	15	748
5	cat	15	743
6	ssh	15	659
7	mpc	9	644
8	nc	15	547
9	vim	13	519
10	clear	12	303
11	hydra	12	277
12	ping	15	268
13	exit	15	242
14	echo	15	205
15	apt	15	203

« Prev   1   2   3   4   5   6   7   8   9   10   Next »

CHANGE CONTROL IS REAL

rule	count
CPTC Windows Password Change Detection	543
CPTC RDP IP Change Detection	30
CPTC Traffic To ICS From VDI Host - Inject	30
CPTC Large Outbound Transfer	24
CPTC Windows VDI Login From Unexpected IP Or Location	19
CPTC RDP Geographically Improbable Access Detected	8
CPTC DNS Tunnel Detection	7
CPTC Geographically Improbable Google Drive Upload Download	4
CPTC Google Drive Edit From Unexpected IP Or Location	2
CPTC HTTP Directory Brute Force Detection	2
CPTC Account Lockout Detection	1