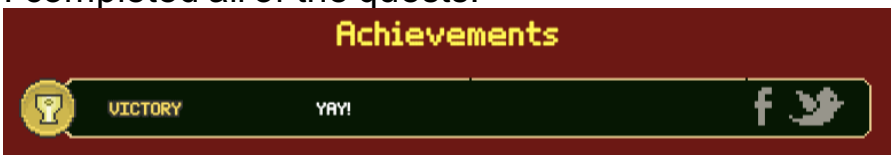
# Sans X-mas Elf on the Shelf

James Dietle

The full challenge was posted here:
https://holidayhackchallenge.com/

As far as the inside videogame was concerned:
I completed all of the quests!




I named my character after my new daughter Addy for luck. It seems to have worked at least for part of it.

Unfortunately, I ran out of time and was only able to get into one of the Supergnomes.

**Digging into the files:**

Looking in the pcap file there is a particular burst of traffic with ATNAS corporation. When following the stream we see that there are several weird bits of data that look encrypted in base64.

When decoded they appear with a command and data. Such as:

"EXEC:iwconfig"
There is a command 5 digits long followed by the command.

To rip out these bits of information you can look to Scapy file by Josh Dosis.

**Scapy**

```
#!/usr/bin/env python
# Copyright (c) 2105 Josh Dosis
import base64
from scapy.all import *     # This script requires Scapy

# Read the capture file into a list of packets
packets=rdpcap("giyh-capture.pcap")
```

```
# Open the output file to save the extracted content from the pcap
fp=open("JPGFile","wb")
# Output for Exec Commands
fs=open("EXECCommands","wb")


# Runs through the packets
for packet in packets:
   if (DNS in packet and hasattr(packet[DNS], 'an') and
hasattr(packet[DNS].an, 'rdata')):
       if packet.sport != 53: continue
       decode=base64.b64decode(packet[DNSRR].rdata)
# Write out File contents for a transferred file
       if decode[0:5] == "FILE:":
          fp.write(decode[5:])
# Write out all of the EXEC Commands
       if decode[0:5] == "EXEC:":
          fs.write(decode[5:)
fp.close()
fs.close()
```

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

   The following are seen over and over again.

   a. NONE:

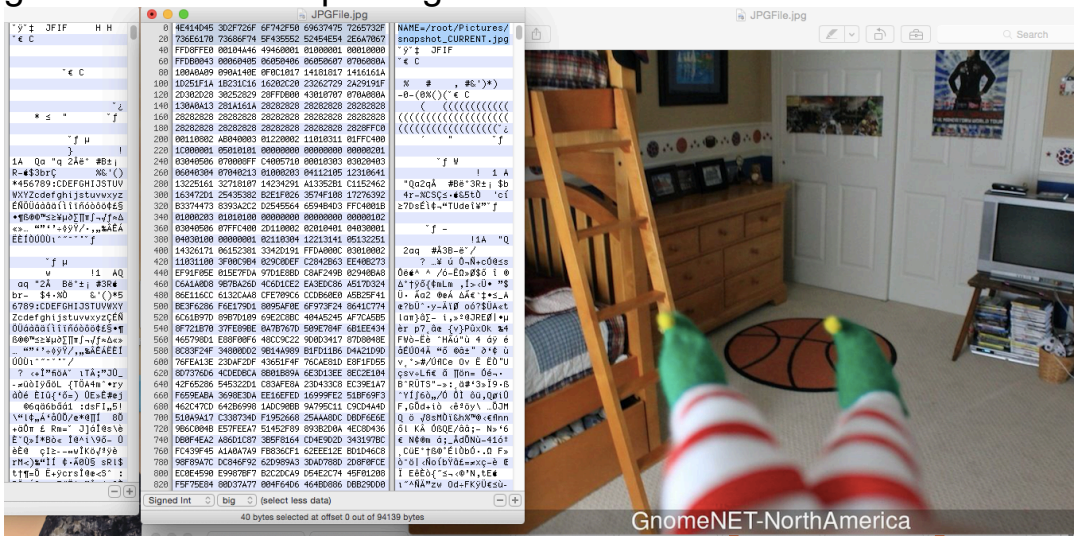
   b. EXEC:

   c. FILE:

   Attachment: Commands

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

   The file taken out has a bad header. Taking a hex editor the top can be altered. Comparing JPGs I copy the header over. The picture shows a gnome in an unsuspecting home.



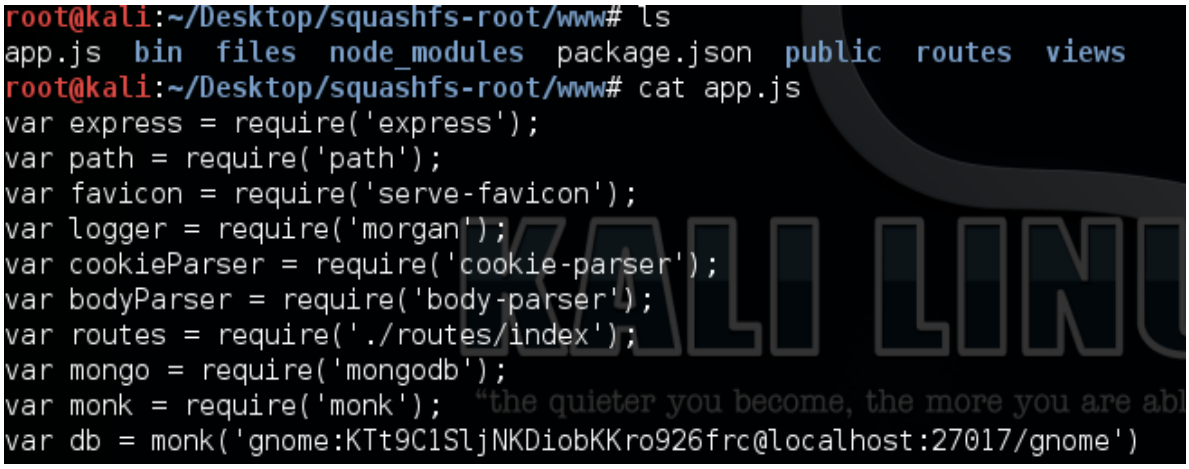
3) **What operating system and CPU type are used in the Gnome?**
Linux julia 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt2-1 (2014-12-08) x86_64 BOOST_LIB_VERSION=1_55

Binwalk allowed the file 29363.squashfs to be extracted.
While looking around for passwords I started to work on exercise 4. Obviously a Linux system i decided I would try to find out what was being supported.

**What type of web framework is the Gnome web interface built in?**

4) **What kind of a database engine is used to support the Gnome web interface?**
Mongodb

Looking in the www folder I saw that the web interface required the use of Mongodb.




**What is the plaintext password stored in the Gnome database?**
SittingOnAShelf.

The dialogue with the NPCs made me believe I needed to use the "ABCs" so I was looking for the hash. Looking around /etc I was disappointed that I did not find a shadow file, so I looked around other files. When I open the mongod.conf file I see some comments

files. When I open the mongod.conf file I see some comments:

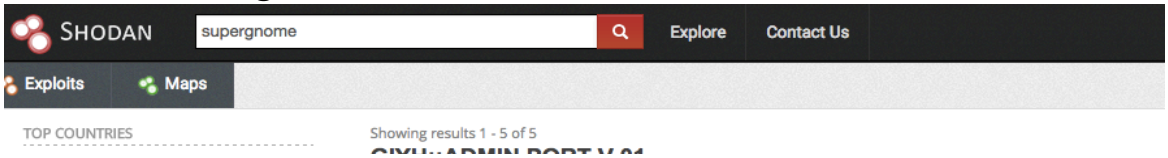
```
root@kali:~/Desktop/squashfs-root/etc# cat mongod.conf
# LOUISE: No logging, YAY for /dev/null
# AUGGIE: Louise, stop being so excited to basic Unix functionality
# LOUISE: Auggie, stop trying to ruin my excitement!

systemLog:
  destination: file
  path: /dev/null
  logAppend: true
storage:
  dbPath: /opt/mongodb
net:
  bindIp: 127.0.0.1
```

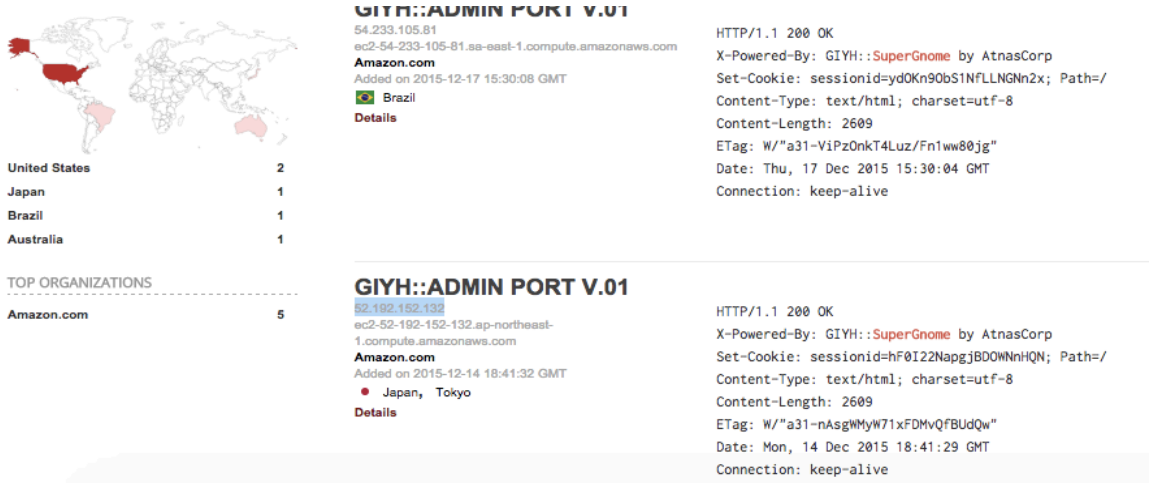
Without logging storage would be in /opt/mongodb. Navigating to that location I saw several files that I was unfamiliar with. A simple strings and grep latter pulled out a phrase that stuck out under admin and password. SittingOnAShelf worked.

```
root@kali:~/Desktop/squashfs-root/opt/mongodb# ls
gnome.0  gnome.ns  journal  local.0  local.ns  _tmp
root@kali:~/Desktop/squashfs-root/opt/mongodb# strings *| grep password -A4 -B4
DCBA
gnome.users
username
user
password
user
user_level
username
admin
password
SittingOnAShelf
user_level
DCBA
gnome.users.$_id_
```

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

Several hints suggest trying Shodan. If you try "SuperGnome" in Shodan you get the following IP addresses. "AtnasCorp" will provide the same results. Checking with Tom is confirms this.

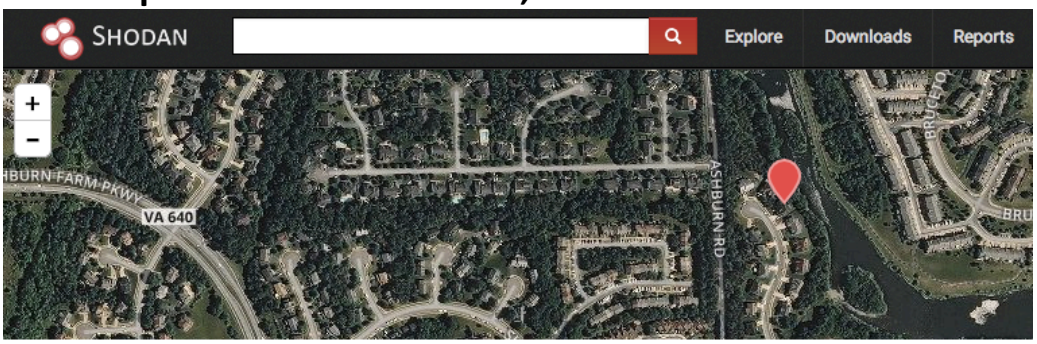


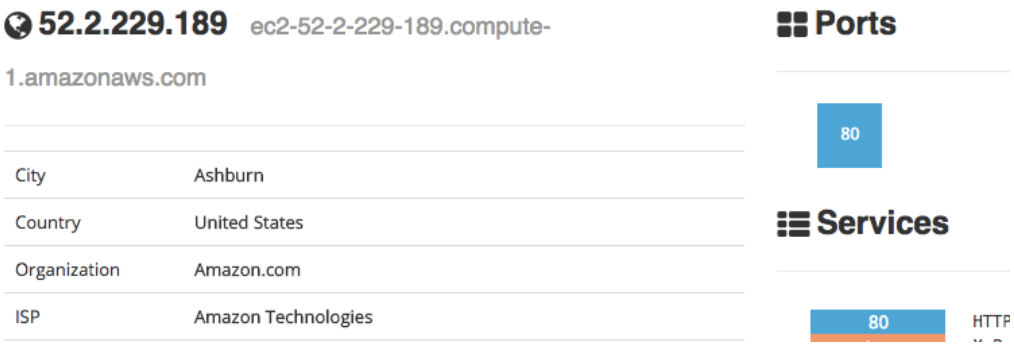



SuperGnome 01: http://52.2.229.189/
SuperGnome 02: http://52.34.3.80/
SuperGnome 03: http://52.64.191.71/
SuperGnome 04: http://52.192.152.132/
SuperGnome 05: http://54.233.105.81/

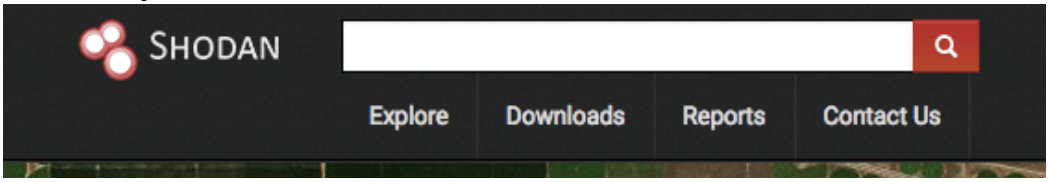
## 6) Where is each SuperGnome located geographically?

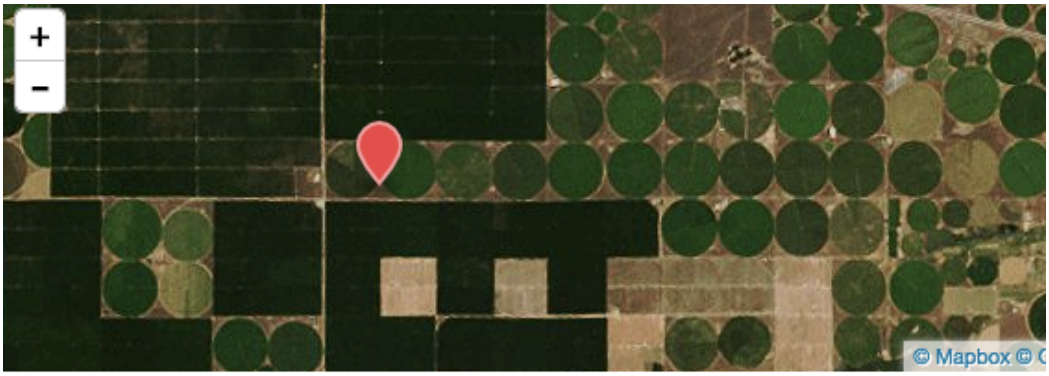
### SuperGnome 01: Ashburn, United States




### SuperGnome 02: Boardman, US






**52.34.3.80** ec2-52-34-3-80.us-west-2.compute.amazonaws.com

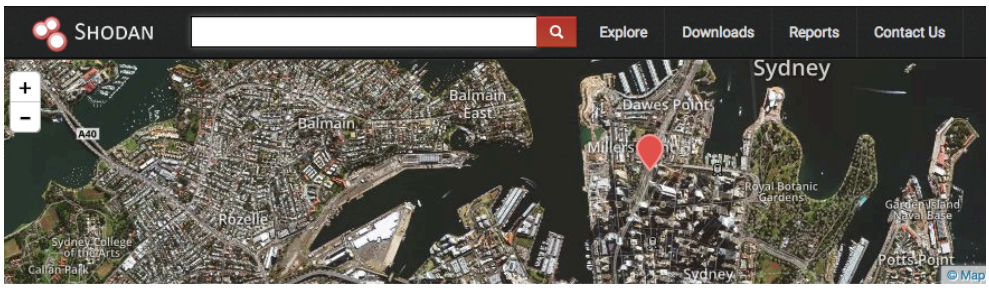
| | |
|---|---|
| City | Boardman |
| Country | United States |
| Organization | Amazon.com |

**Ports**

80

**Services**

## SuperGnome 03: Sydney, Australia




**52.64.191.71** ec2-52-64-191-71.ap-southeast-2.compute.amazonaws.com

| | |
|---|---|
| City | Sydney |
| Country | Australia |
| Organization | Amazon.com |
| ISP | Amazon Technologies |

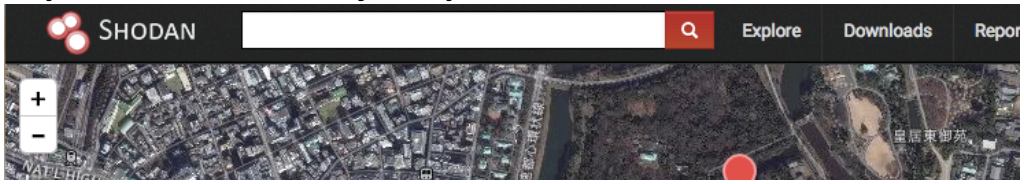
**Ports**

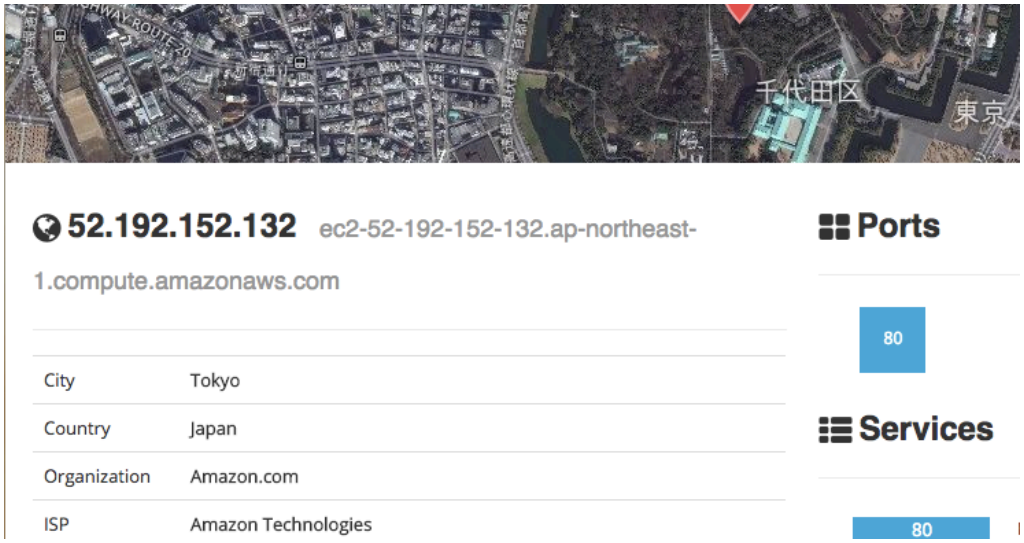
80

**Services**

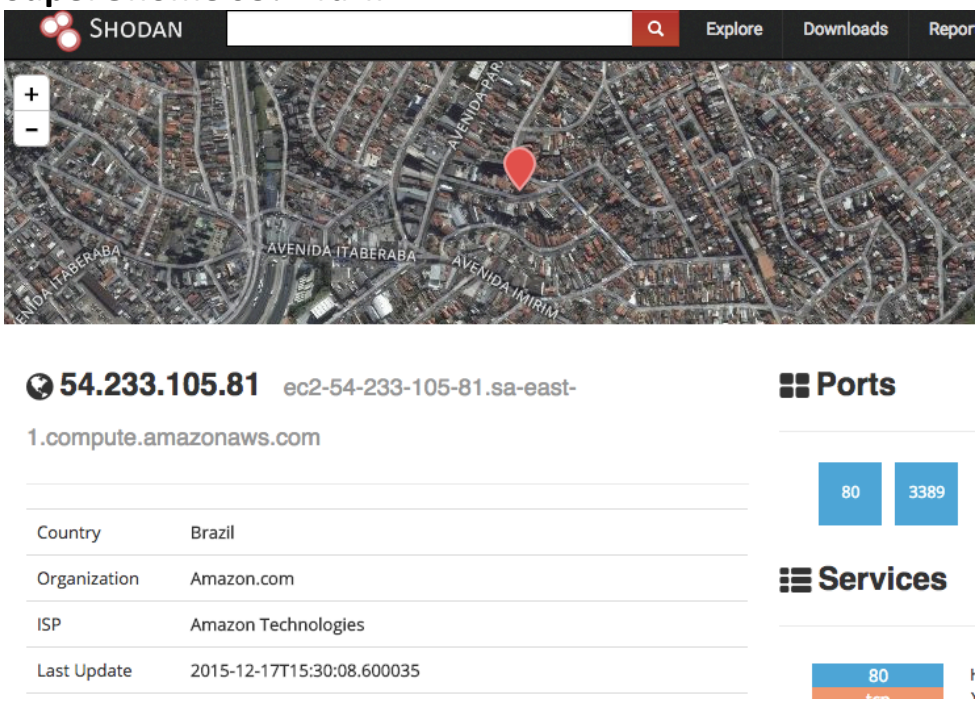
80 HTTP/1.1 200 OK

## SuperGnome 04: Tokyo, Japan






**SuperGnome 05: Brazil**




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

SuperGnome 01: Password Reuse. The password is the same that was found in the firmware.
SuperGnome 02:
PORT STATE SERVICE
80/tcp open http
4242/tcp closed vrml-multi-use
5555/tcp closed freeciv

SuperGnome 03:
SuperGnome 04:
SuperGnome 05:

**8) ONCE YOU GET APPROVAL OF GIVEN IN-SCOPE TARGET IP ADDRESSES FROM TOM HESSMAN IN THEDOSIS 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: Once you have logged into the admin console the gnome.conf file is under the tab files.
SuperGnome 02:
SuperGnome 03:
SuperGnome 04:
SuperGnome 05:

Other interesting finds.
gnome:KTt9C1SljNKDiobKKro926frc@localhost:27017/gnome

/etc/hosts
supergnome1.atnascorp.com
52.2.229.189