

Configure - Lab

October 2022

PurpleVPN - Lightsail Configuration

PUBLIC IP

34.214.33.251

+ Create static IP

PRIVATE IP

172.26.9.128

What is this for? [?](#)

Your public IPv4 address changes when you stop and start your instance. Attach a [static IPv4](#) address to your instance to keep it from changing.

IPv4 Firewall [?](#)

Create rules to open ports to the internet, or to a specific IPv4 address or range.

[Learn more about firewall rules](#) [?](#)

+ Add rule

Application	Protocol	Port or range / Code	Restricted to	
SSH	TCP	22	166.70.80.123 Lightsail browser SSH/RDP ?	✎ 🗑

IPv6 networking

Enable Internet Protocol version 6 to have an IPv6 address assigned to your resource.

[Learn more about IPv6](#) [?](#)

☒ **IPv6 networking is disabled**

This resource can communicate using only the IPv4 protocol.

I have an instance for the PurpleVPN and it shows the Public and Private IP Addresses

I have set up the restriction to only allow SSH from my IP Address

Disabled IPv6 Networking

PurpleVPN - Ansible Execution

```
PLAY [Configure openVPN] *****
TASK [Gathering Facts] *****
ok: [purpleVPN]

TASK [set_fact] *****
ok: [purpleVPN]

TASK [Change the hostname to ovpn] *****
changed: [purpleVPN]

TASK [apt Update packages] *****
changed: [purpleVPN]

TASK [Install Dependencies for OpenVPN] *****
changed: [purpleVPN]

TASK [Copy OpenVPN server files] *****
changed: [purpleVPN]

PLAY RECAP *****
purpleVPN : ok=6    changed=4    unreachable=0
```

This is what it looks like for the execution of the playbook of configPurpleVPN.yml

Changes the hostname


Installs the package dependencies

Copies the openvpn-install.sh script to /home/ubuntu

PurpleVPN - Install OpenVPN

```
thepcn3rd@rutgz:~/Ensign/ansible$ ssh -i keys/BSidesIF.pem ubuntu@34.214.33.251
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-1018-aws x86_64)

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



Login with your SSH Key and IP Address for the PurpleVPN Server

```
ubuntu@ovpn:~$ ls
openvpn-install.sh
ubuntu@ovpn:~$ sudo ./openvpn-install.sh
```

Execute with sudo the openvpn-install.sh

PurpleVPN - Configure OpenVPN

```
Welcome to this OpenVPN road warrior installer!

This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [34.214.33.251]:

Which protocol should OpenVPN use?
  1) UDP (recommended)
  2) TCP
Protocol [1]:

What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
  1) Current system resolvers
  2) Google
  3) 1.1.1.1
  4) OpenDNS
  5) Quad9
  6) AdGuard
DNS server [1]:

Enter a name for the first client:
Name [client]: bob
```

Should populate your external IP of the LightSail Server

UDP is Recommended

Port 1194 - Needs to be setup in LightSail firewall for access

Choose the DNS servers your clients will utilize

Each client needs a uniquely created ovpn file (You cannot reuse)

PurpleVPN - Configure OpenVPN

```
OpenVPN is already installed.

Select an option:
  1) Add a new client
  2) Revoke an existing client
  3) Remove OpenVPN
  4) Exit
Option: 1

Provide a name for the client:
Name: Kristina
Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/openvpn/server/easy-rsa/pki/easy-rsa-9608.iXjMBn/tmp.8qqwma'
-----
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rsa-9608.iXjMBn/tmp.iL3qq9
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName                :ASN.1 12:'Kristina'
Certificate is to be certified until Sep 16 23:48:36 2032 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Kristina added. Configuration available in: /root/Kristina.ovpn
ubuntu@ovpn:~$
```

Rerun the installer for openvpn
then select “Add a new client”

Each additional ovpn file is created
under /root/<name>.ovpn

This file is provided to the person
connecting to your OVPN Server
remotely.

Note anyone connected to the
OVPN server can see other clients
connected.

PurpleVPN - Why OpenVPN?

Why setup an OpenVPN Server?

- Allows a connected client to connect to **ALL** of your private IP Addresses on Lightsail
- Access to insecure services to be hosted on the private IP Addresses
- Usage of forward connecting tools like crackmapexec, evil-winrm and many others work
- Webshells, shells and other connections work
- Simulates an internal compromised device
- Works great for a student environment as long as everyone plays nice!

Reverse Shells

- The openvpn and routing is not setup for reverse shells, however in the lab we will use SSH and work around the limitation




PurpleDC and PurpleMBR - Lightsail Configuration

IPv4 Firewall

Create rules to open ports to the internet, or to a specific IPv4 address or range.

[Learn more about firewall rules](#) 

 Add rule

Application	Protocol	Port or range / Code	Restricted to		
SSH	TCP	22	Any IPv4 address Lightsail browser SSH/RDP 		
RDP	TCP	3389	166.70.80.123 Lightsail browser SSH/RDP 		
Custom	TCP	5986	166.70.80.123		

IPv6 networking

Enable Internet Protocol version 6 to have an IPv6 address assigned to your resource.

[Learn more about IPv6](#) 



IPv6 networking is disabled

This resource can communicate using only the IPv4 protocol.

Setup the firewall to restrict based on IP Address, for whatever reason it does not let you filter by IP on SSH (Bug?!?)

Allow Port TCP/5986 and restrict by IP Address so ansible can authenticate OR connect to the OVPN server and use the private IP Address

purpleDC and purpleMBR

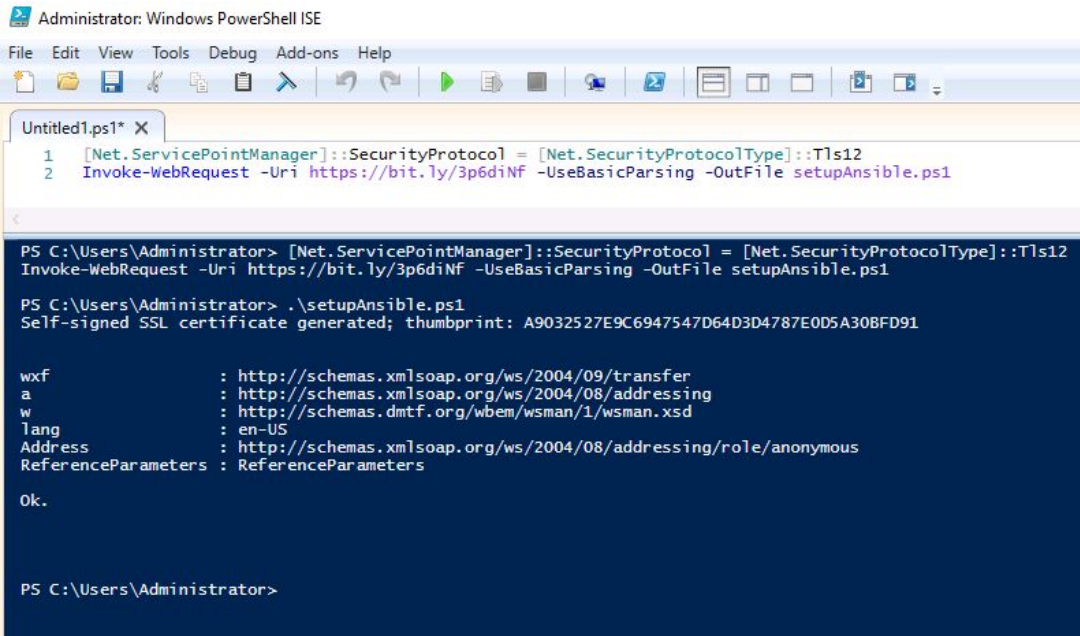
```
vars:
  ansible_python_interpreter: "/usr/bin/python3"
  ansibleDirectory: "/home/thepcn3rd/Ensign/ansible"
  domainName: "13lives.local"
  netbiosName: "13lives"
  # Needs to be updated to the internal IP of the Domain Controller
  dnsInternalServer: "172.26.6.32"
  # Needs to be updated to the administrator password of the domain controller
  domainPass: ""
  commonUser: "thepcn3rd"
  commonPass: "#Blast2022New!Year"
  lightsailUser: "ubuntu"
  lightsailPem: "/home/thepcn3rd/Ensign/ansible/keys/BSidesIF.pem"
  className: "BSides IF 2022"
```

Update the ansible_password for the respective host in the inventory.yml

Update the domainPass in the inventory.yml to be the administrator password for purpleDC

Update the dnsInternalServer to the private IP Address of the purpleDC

purpleDC and purpleMBR - Setup Ansible



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X
1 [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
2 Invoke-WebRequest -Uri https://bit.ly/3p6diNF -UseBasicParsing -OutFile setupAnsible.ps1

PS C:\Users\Administrator> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri https://bit.ly/3p6diNF -UseBasicParsing -OutFile setupAnsible.ps1

PS C:\Users\Administrator> .\setupAnsible.ps1
Self-signed SSL certificate generated; thumbprint: A9032527E9C6947547D64D3D4787E0D5A308FD91

wxsf      : http://schemas.xmlsoap.org/ws/2004/09/transfer
a         : http://schemas.xmlsoap.org/ws/2004/08/addressing
w         : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
lang      : en-US
Address   : http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
ReferenceParameters : ReferenceParameters

Ok.

PS C:\Users\Administrator>
```

Remember to setup ansible on these servers. I have provided a bit.ly link for convenience.

purpleDC and purpleMbr - ExecuteConfig

```
TASK [set_fact] *****
ok: [purpleDC]

TASK [Change the hostname to windc] *****
changed: [purpleDC]

TASK [Reboot] *****
changed: [purpleDC]

TASK [Install the domain controller] *****
changed: [purpleDC]

TASK [Install domain 13lives.local] *****
changed: [purpleDC]

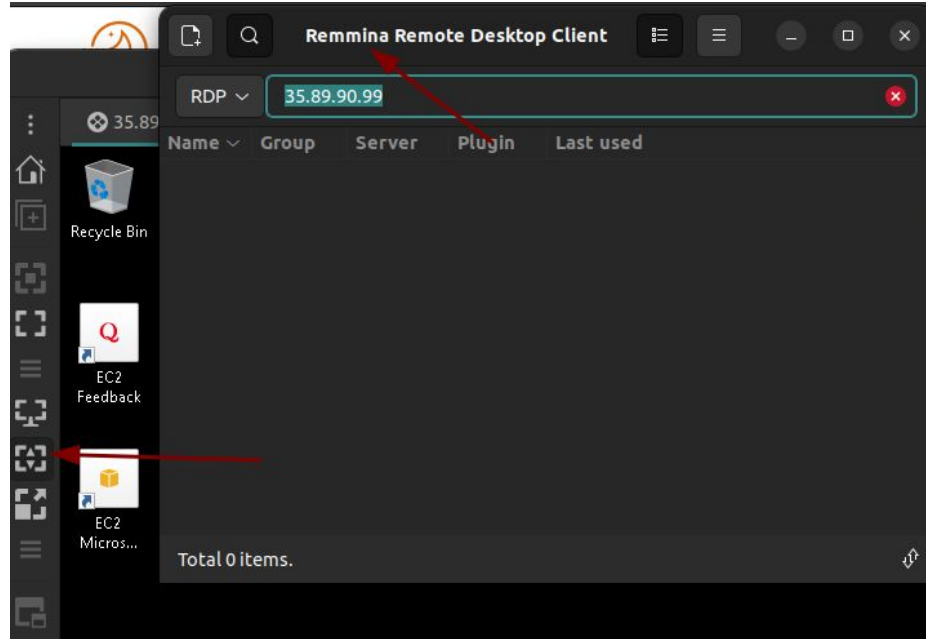
TASK [Ensure WinRM starts when the system has settled and is ready to work reliably] *****
changed: [purpleDC]

TASK [Reboot server and wait for initial setup] *****
[
```

While running ansible if ansible is setup, the port in Lightsail is configured for TCP/5986, passwords updated in the inventory.yml file no issues should occur

Rerun the executeConfig script and comment out the playbooks of systems that worked in the configure.yml

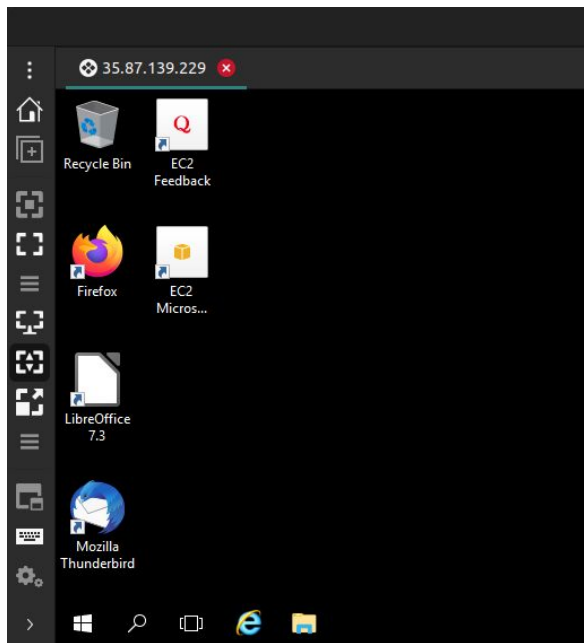
purpleDC - Remote Desktop



After installing the domain, I have had inconsistent connections using the “Connect to Remote Desktop” inside of Lightsail. I will use a tool called Remmina on Ubuntu to connect.

The second arrow points to dynamically adjust the resolution based on the size of the window. I like this setting, sometimes it distorts the view

purpleMbr - Build Vulnerable User Profile



After the installation of PurpleMBR is complete, setup is required for the scenario to work. Login as prayut.c and setup his profile. (Information is in playbooks/configPurpleDC.yml)

Login as prayut.c

Password: ExpRRQvwn24SJv<xxxx>

This builds the profile for the user that needs some configuration

Observe Firefox, Thunderbird, LibreOffice and the JDK should be installed. We need to configure them

purpleMbr - Create Yahoo Account and Setup Thunderbird

Set Up Your Existing Email Address

To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.

Your full name

Email address

Password

☒ Remember password

[Configure manually](#)

Cancel

Continue

Your credentials will only be stored locally on your computer.

Setup Thunderbird with a yahoo account that you create (Personal Opinion: Yahoo is lacking controls that end-users need in-place)

Configure the mailbox as IMAP

Authenticate

Set as Default

You should see a couple of emails in your inbox from spam

purpleMbr - Install Add-on FiltaQuilla

Search Results for "filtaquilla"

Sort by: **Relevance** | Most Users | Top Rated | Newest | More ▾



FiltaQuilla

Adds many new mail filter actions - launch a file, suppress notification, remove star or tag, mark replied or unread, copy as "read", append text to subject.

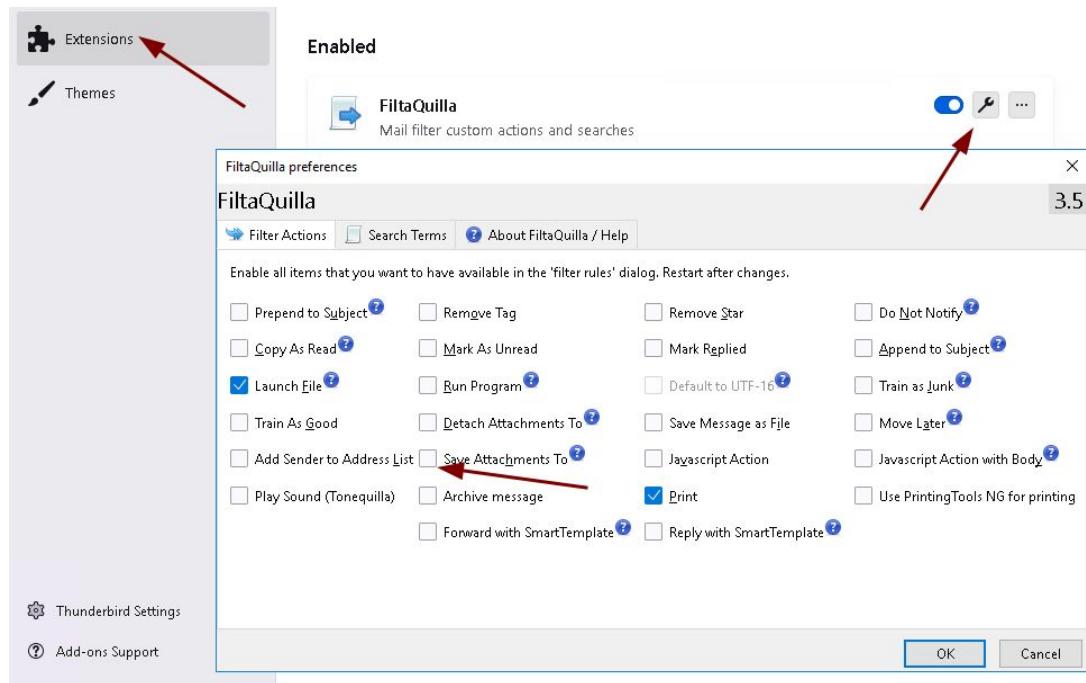
★★★★★ (94) · 13,838 users

+ Add to
Thunderbird

Top-right of thunderbird click
the options menu and
Add-ons and Themes

Search for and "Add to
Thunderbird" FiltaQuilla

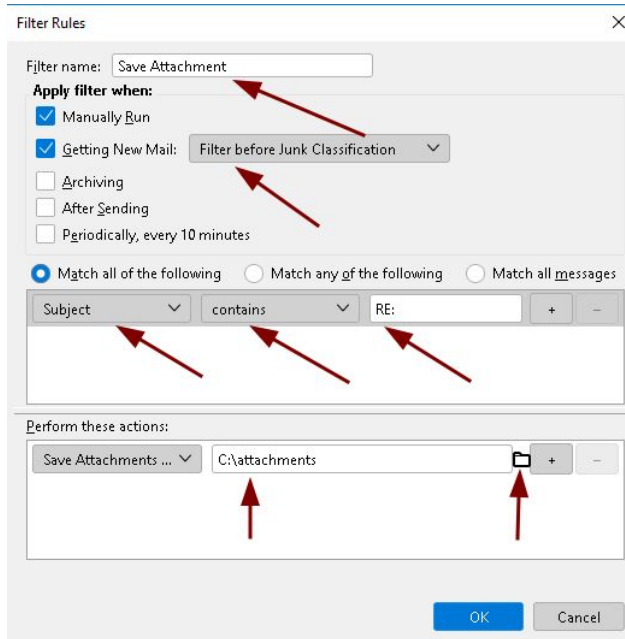
purpleMbr - Configure FiltaQuilla



After installation click on extensions, then the configure wrench icon and select Save Attachments To.

Then go back to the options menu, select Tools and Message Filters

purpleMbr - Setup Message Filter



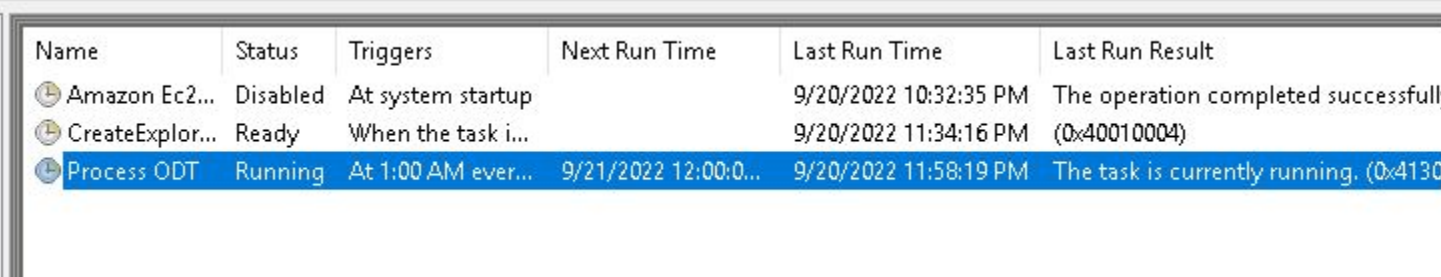
Name the filter you are creating

I setup the Subject contains a keyword like “RE:” so I can control which emails this executes against

Then configure the attachments of a received email to save to c:\attachments

The c:\attachments folder is where the powershell script triggered by a scheduled task will run the macros that exist inside of an odt file.

purpleMbr - Check Scheduled Task




Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
Amazon Ec2...	Disabled	At system startup		9/20/2022 10:32:35 PM	The operation completed successfully.
CreateExplor...	Ready	When the task i...		9/20/2022 11:34:16 PM	(0x40010004)
Process ODT	Running	At 1:00 AM ever...	9/21/2022 12:00:0...	9/20/2022 11:58:19 PM	The task is currently running. (0x4130)

Verify the scheduled task of “Process ODT” is executing. You may have to stop and restart the task. It should say in the “Last Run Result” the task is currently running.

Launch LibreOffice to create some necessary files

purpleMbr - pwshProcessODT.ps1

```
pwshProcessODT.ps1 X
1 $process_dir = "C:\attachments"
2
3 while($true) {
4     # If any odt files in attachments, load the file and then archive:
5     $files = ls $process_dir\*.odt
6     if ( $files.length -gt 0 ) {
7         # Copy the registrymodifications.xcu file back in-place to remove the document recovery
8         Copy-Item -Force -Path "C:\files\registrymodifications.xcu" -Destination "C:\users\administrator\AppData\Roaming\LibreOffice\4\
9         Start-Sleep -s 15
10
11         # launch odt files
12         Invoke-Item "$($process_dir)\*.odt"
13         Start-Sleep -s 60
14
15         # kill libre office, sleep
16         Stop-Process -Name soffice*
17         Start-Sleep -s 60
18         Remove-Item -Recurse -force -Path $process_dir\*
19         Remove-Item -Force -Path "c:\users\administrator\AppData\Roaming\LibreOffice\4\user\registrymodifications.xcu"
20     }
21     Start-Sleep -s 60
22 }
23
```



This script executes and pauses for up to 195 seconds, note that in sending in your ODT files as attachments

This also recreates the registrymodifications.xcu file, this is to reset the settings in OpenOffice for relaxed Macro security and it removes an issue of LibreOffice trying to recover the last document that crashed (Interesting Vulnerability)

purpleLin - Initial Setup

Website Settings

Website Name:

Website URL:

☐ Use Fancy URLs - Requires that your host has mod_rewrite enabled

Custom Permalink Structure:

[more](#)

Flush All Caches

User Profile

Username:

Email Address:

Previously setup GetSimpleCMS with a registered DNS that I own.

I setup the yahoo account for BSidesIF 2022

The website password is not the same as the email password

The password for **chanin.w** is provided only to simulate an administrator logging into the site for the Persistent XSS vulnerability to work

purpleLin - Google Auth Setup

Setup google authenticator following the below page:

<https://www.digitalocean.com/community/tutorials/how-to-set-up-multi-factor-authentication-for-ssh-on-ubuntu-18-04>

Run google-authenticator for the admin user. Only change the token for the admin user for the purposes of the Lab. The admin user is not a privileged account, this account is used for purposes of the lab.

purpleLin - Google Authenticator Setup

```
ubuntu@purplelin:/etc/ssh$ vim sshd_config
ubuntu@purplelin:/etc/ssh$ su - admin
Password:
ubuntu@purplelin:/etc/ssh$ sudo su -
root@purplelin:~# su - admin
admin@purplelin:~$ ls
admin@purplelin:~$ google-authenticator


Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/a
```

From the SSH session of your Ubuntu user on PurpleLin, switch over to the admin account and execute “google-authenticator”

Setup the token to be time-based, allow multiple connections, and your choice on hardening from brute force.

purpleLin - Google Auth Token (Step 2)

```
admin@purplelin:~$ cat .google_authenticator
DHMYRRWAVUOBGW4TH67QLOH57E
" WINDOW_SIZE 17
" TOTP_AUTH
26944323
45578006
90606482
74780016
50250740
admin@purplelin:~$
```



Modify the token in
/home/admin/.google-authenticator to
have the same secret key as is
contained in the web server file
/var/www/html/floatinglogs/db/floatin
glogs.db

purpleLin - Setup SSH Authorized_Keys


```
admin@purplelin:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
admin@purplelin:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC0hFiWT+geyxWbkt5d+tgN55ZhKCTWY90r17mg1c5h
8ZWMwxIUEli7xL9Wk5URD+wPTcpt+CqZIOatw6iAMwZZmIx/bmT1ljowXVFWUcHLfbHyU8P5ncVbCek1
o6KzWg8R9sRT3ZNqz6cQbf1+7K6RmH0hs17e9w8Z6X2Y3KWKhMn0NVygTYCKVaRG1xgsjx0wApqAHG1z
VbTgqKM5aNl5VK63vtybnV6YUumuQ72ODDW/9YAeyYCup3eI0egvjRU25uLttwyLWsuVFrwWmeDPuKX
HD2107zZXFTm917SJfI1VBV0ueVlK+ef53arrHEaJayDnmsWo0lY9jnwsZPb BSidesIF
admin@purplelin:~/.ssh$
```

To create the .ssh directory and appropriate files I execute “ssh-keygen” as the user (This can be done manually)

Copy or create the same authorized_keys file from /home/ubuntu/.ssh/authorized_keys for the admin user. This allows the BSidesIF SSH key to be utilized in conjunction with the google auth token.

purpleLin - Setup SSH GatewayPorts

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
GatewayPorts yes
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
```



Modify /etc/ssh/sshd_config and change GatewayPorts from being commented out and set to yes.

This is for convenience of allowing a SSH reverse tunnel to listen on the 172.16.x.x private IP Address. (Other tools could be used like socat)

This reverse tunnel is used from the phishing that we will conduct.