



TRY HACK ME: Write-Up Phishing

Phishing

Learn what phishing is and why it's important to a red team engagement. You will set up phishing infrastructure, write a convincing phishing email and try to trick your target into opening your email in a real-world simulation.

[Help](#)

Task 2 Intro To Phishing Attacks -

Answer to the questions of this section-

What type of psychological manipulation is phishing part of?

Correct Answer

What type of phishing campaign do red teams get involved in?

Correct Answer

Task 3 Writing Convincing Phishing Emails -

Answer to the questions of this section-

What tactic can be used to find brands or people a victim interacts with?

Correct Answer

What should be changed on an HTML anchor tag to disguise a link?

Correct Answer

Task 4 Phishing Infrastructure –

Domain name; SSL/TLS certificates; Email Server/Account; DNS records; and Web Server

Email Server/Account: You'll need to either set up an email server or register with an SMTP email provider.

DNS Records: Setting up DNS Records such as SPF, DKIM, DMARC will improve the deliverability of your emails and make sure they're getting into the inbox rather than the spam folder.

Automation and Useful Software:

Some of the above infrastructures can be quickly automated by using the below tools.

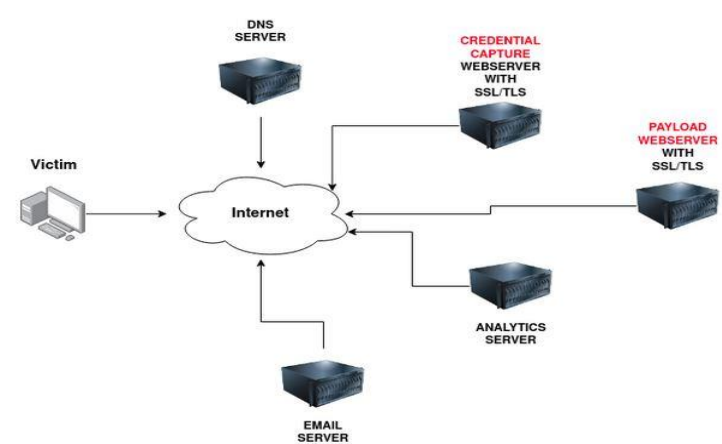
GoPhish - (Open-Source Phishing Framework) - getgophish.com

GoPhish is a web-based framework to make setting up phishing campaigns more straightforward. GoPhish allows you to store your SMTP server settings for sending emails, has a web-based tool for creating email templates using a simple WYSIWYG (What You See Is What You Get) editor. You can also schedule when emails are sent and have an analytics dashboard that shows how many emails have been sent, opened or clicked.

The Next task will talk you through how to launch a phishing campaign using this software.

SET - (Social Engineering Toolkit) - [trustedsec.com](https://www.trustedsec.com)

The Social Engineering Toolkit contains a multitude of tools, but some of the important ones for phishing are the ability to create spear-phishing attacks and deploy fake versions of common websites to trick victims into entering their credentials.



Answer to the questions of this section-

What part of a red team infrastructure can make a website look more authentic?

ssl/tls certificates

Correct Answer

What protocol has TXT records that can improve email deliverability?

dns

Correct Answer

What tool can automate a phishing campaign and include analytics?

gophish

Correct Answer


Task 5 Using GoPhish -

Firstly launch the virtual machine by clicking the green Start Machine button on the right; once loaded, click the following URL to open the GoPhish login page

https://LAB_WEB_URL.p.thmlabs.com:8443 (if you receive an Nginx error, wait another 30 seconds and try again).



Please sign in

 You have successfully logged out

Sign in

You should be able to log in with the **username: admin** and **password: tryhackme**

Sending Profiles:

Sending profiles are the connection details required to actually send your Phishing emails; this is just simply an SMTP server that you have access to. Click the Sending Profiles link on the left-hand menu and then click the "New Profile" button.

Next, add in the following information as per the screenshot below:

Name: Local Server

From: noreply@redteam.thm

Host: 127.0.0.1:25

Then click Save Profile.

Landing Pages:

Next, we're going to set up the landing page; this is the website that the Phishing email is going to direct the victim to; this page is usually a spoof of a website the victim is familiar with.

Click the Landing Pages link on the left-hand menu and then click the "New Page" button.

Give the Landing Page the name ACME Login, next in the HTML box; you'll need to press the Source button to allow us to enter the HTML code as shown below:

```
<!DOCTYPE html>
```

```
<html lang="en">
```

```
<head>
```

```
  <meta charset="UTF-8">
```

```
  <title>ACME IT SUPPORT - Admin Panel</title>
```

```
<style>
```

```
  body { font-family: "Ubuntu", monospace; text-align: center }
```

```
  div.login-form { margin:auto; width:300px; border:1px solid #ecec; padding:10px;text-align:
left;font-size:13px;}
```

```
  div.login-form div input { margin-bottom:7px;}
```

```
div.login-form input { width:280px;}

div.login-form div:last-child { text-align: center; }

div.login-form div:last-child input { width:100px;}

</style>

</head>

<body>

<h2>ACME IT SUPPORT</h2>

<h3>Admin Panel</h3>

<form method="post">

  <div class="login-form">

    <div>Username:</div>

    <div><input name="username"></div>

    <div>Password:</div>

    <div><input type="password" name="password"></div>

    <div><input type="submit" value="Login"></div>

  </div>

</form>

</body>

</html>
```

Click the Source button again, and you should see a login box with username and password fields as per the image below, also click the Capture Submitted Data box and then also the Capture Passwords box and then click the Save Page button.

New Landing Page

Name:

HTML

ACME IT SUPPORT

Admin Panel

Username:

Password:

☒ Capture Submitted Data

☒ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

Email Templates:

This is the design and content of the email you're going to actually send to the victim; it will need to be persuasive and contain a link to your landing page to enable us to capture the victim's username and password. Click the Email Templates link on the left-hand menu and then click the New Template button. Give the template the name Email 1, the subject New Message Received, click the HTML tab, and then the Source button to enable HTML editor mode. In the contents write a persuasive email that would convince the user to click the link, the link text will need to be set to `https://admin.acmeitsupport.thm`, but the actual link will need to be set to `{{.URL}}` which will get changed to our spoofed landing page when the email gets sent, you can do this by highlighting the link text and then clicking the link button on the top row of icons, make sure to set the protocol dropdown to `<other>`.

TextHTML

✂

📄

📄

📄

📄

↶

↷

↶

↷

🔗

🗑

🗑

🗑

B

I

S

*I*_x

≡

≡

≡

≡

🔗 Link (98+K)

Link

Display Text

https://admin.acmeitsupport.thm

Protocol

<other>

URL

{{.URL}}

OK

Cancel

Your email should look similar to the screenshot below. Click Save Template once complete.

New Template

Name:

Email 1

Import Email

Subject:

New Message Received

TextHTML

✂

📄

📄

📄

📄

↶

↷

↶

↷

🔗

🗑

🗑

🗑

B

I

S

*I*_x

≡

≡

≡

≡

Styles

Format

Hello,

You've received a new message, please log in to the admin portal to view it

<https://admin.acmeitsupport.thm>.

Many Thanks

Online Team

Add Tracking Image

Add File

Show 10 entries

Search:

Name

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

Cancel

Save Template

Users & Groups

This is where we can store the email addresses of our intended targets. Click the Users & Groups link on the left-hand menu and then click the New Group button. Give the group the name Targets and then add the following email addresses:

`martin@acmeitsupport.thm`

`brian@acmeitsupport.thm`

`accounts@acmeitsupport.thm`

Click the Save Template button; once completed, it should look like the below screenshot:

New Group

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

[+ Add](#)

Show entries Search:

First Name	Last Name	Email	Position
		martin@acmeit...	
		brian@acmeits...	
		accounts@acm...	

Showing 1 to 3 of 3 entries Previous 1 Next

[Close](#) [Save changes](#)

Campaigns

Now it's time to send your first emails; click the Campaigns link on the left-hand menu and then click the New Campaign button. Set the following values for the inputs, as per the screenshot below:

Name: Campaign One

Email Template: Email 1

Landing Page: ACME Login

URL: `http://10.10.175.58`

Launch Date: For this lab set it to 2 days ago just to make sure there is no complication with different timezones, in a real operation this would be set correctly.

Sending Profile: Local Server

Groups: Targets

Once completed, click the Launch Campaign button, which will produce an Are You Sure prompt where you can just press the Launch button.

New Campaign

Name:

Campaign One

Email Template:

Email 1

Landing Page:

ACME Login

URL:

http://10.10.113.13

Launch Date

October 26th 2021, 5:07 pm

Send Emails By (Optional)

Sending Profile:

Local Server

Send Test Email

Groups:

Targets

Close

Launch Campaign

You'll then be redirected to the results page of the campaign.

Results

The results page gives us an idea of how the phishing campaign is performing by letting us know how many emails have been delivered, opened, clicked and how many users have submitted data to our spoof website.

You'll see at the bottom of the screen a breakdown for each email address; you'll notice that both Martin's and Brian's email has been sent successfully, but the account's email has resulted in an error.

Email	Position	Status
martin@acmeitsupport.thm		Email Sent
brian@acmeitsupport.thm		Email Sent
accounts@acmeitsupport.thm		Error

We can dig in the error more by clicking the dropdown arrow next to the account's row, and by viewing the details or the error, we can see an error message saying the user is unknown.

Timeline for

Email: accounts@acmeitsupport.thm
Result ID: igYlpCx

-  Campaign Created
-  Error Sending Email
 - ▼ View Details
 - Error** 550 5.1.1 : Recipient address rejected: User unknown in local recipient table

After a minute and providing you've followed the instructions correctly, you should see the status of brian change to Submitted Data.

Email	Position	Status
martin@acmeitsupport.thm		Email Sent
brian@acmeitsupport.thm		Submitted Data
accounts@acmeitsupport.thm		Error

Expanding Brian's details and then viewing the details for the submitted data, you should be able to see Brian's username and password, which will help you answer the question below.

Timeline for

Email: brian@acmeitsupport.thm
Result ID: UzCYnqg

-  Campaign Created October 26th 2021 9:41:46 pm
-  Email Sent October 26th 2021 9:41:46 pm
-  Submitted Data October 26th 2021 9:48:01 pm
 -  Ubuntu
 -  Firefox (Version: 93.0)
 - 
 - ▼ View Details

Parameter	Value(s)
password	
username	brian

Answer to the questions of this section-

What is the password for Brian?

p4\$\$w0rd!

Correct Answer

Task 6 Droppers –

Droppers are software that phishing victims tend to be tricked into downloading and running on their system. The dropper may advertise itself as something useful or legitimate such as a codec to view a certain video or software to open a specific file.

Answer to the questions of this section-

Do droppers tend to be malicious?

nay

Correct
Answer

Hint

Task 7 Choosing A Phishing Domain –

Expired Domains: Although not essential, buying a domain name with some history may lead to better scoring of your domain when it comes to spam filters. Spam filters have a tendency to not trust brand new domain names compared to ones with some history.

Typosquatting: Typosquatting is when a registered domain looks very similar to the target domain you're trying to impersonate. Here are some of the common methods:

Misspelling: goggle.com Vs google.com

Additional Period: go.ogle.com Vs google.com

Switching numbers for letters: g00gle.com Vs google.com

Phrasing: googles.com Vs google.com

Additional Word: googleresults.com Vs google.com

These changes might look unrealistic, but at a glance, the human brain tends to fill in the blanks and see what it wants to see, i.e. the correct domain name.

TLD Alternatives: A TLD (Top Level Domain) is the .com .net .co.uk .org .gov e.t.c part of a domain name, there are 100's of variants of TLD's now. A common trick for choosing a domain would be to use the same name but with a different TLD. For example, register tryhackme.co.uk to impersonate tryhackme.com.

IDN Homograph Attack/Script Spoofing: Originally domain names were made up of Latin characters a-z and 0-9, but in 1998, IDN (internationalized domain name) was implemented to support language-specific script or alphabet from other languages such as Arabic, Chinese, Cyrillic, Hebrew and more. An issue that arises from the IDN implementation is that different letters from different languages can actually appear identical. For example, Unicode character U+0430 (Cyrillic small letter a) looks identical to Unicode character U+0061 (Latin small letter a) used in English, enabling attackers to register a domain name that looks almost identical to another.

Answer to the questions of this section-

What is better, using an expired or new domain? (old/new)

old

Correct Answer

What is the term used to describe registering a similar domain name with a spelling error?

typosquatting

Correct Answer

Task 8 Using MS Office In Phishing –

Often during phishing campaigns, a Microsoft Office document (typically Word, Excel or PowerPoint) will be included as an attachment. Office documents can contain macros; macros do have a legitimate use but can also be used to run computer commands that can cause malware to be installed onto the victim's computer or connect back to an attacker's network and allow the attacker to take control of the victim's computer.

Answer to the questions of this section-

What can Microsoft Office documents contain, which, when executed can run computer commands?

macros

Correct Answer

Task 9 Using Browser Exploits –

Another method of gaining control over a victim's computer could be through browser exploits; this is when there is a vulnerability against a browser itself (Internet Explorer/Edge, Firefox, Chrome, Safari, etc.), which allows the attacker to run remote commands on the victim's computer.

Browser exploits aren't usually a common path to follow in a red team engagement unless you have prior knowledge of old technology being used on-site. Many browsers are kept up to date, hard to exploit due to how browsers are developed, and the exploits are often worth a lot of money if reported back to the developers.

Answer to the questions of this section-

Which recent CVE caused remote code execution?

cve-2021-40444

Correct Answer

Task 10 Phishing Practical-

"View Site" button to launch the Phishing Test website. Examine each email, including where it's from, its links and attachments and decide whether you think the email is safe or not.



Answer to the questions of this section-

What is the flag from the challenge?

THM{I_CAUGHT_ALL_THE_PHISH}

Correct Answer

This is all for this Write-up, hoping this will help you in solving Phishing Room. Have Fun and Enjoy Hacking!

Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumari