



Phishing

Social engineering is the psychological manipulation of people into performing or divulging information by exploiting weaknesses in human nature.

A term you'll come across and the type of phishing campaign a red team would participate in is **spear-phishing**, as with throwing a physical spear; you'd have a target to aim at, the same can be said with spear-phishing in that you're targeting an individual, business or organisation rather than just anybody as mass.

A red team could be contracted to solely carry out a phishing assessment to see whether a business is vulnerable to this type of attack or can also be part of a broader scale assessment and used to gain access to computer systems or services.

1. **What type of psychological manipulation is phishing part of?**

ans: **social engineering**

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

ans: **spear-phishing**

Task 3

Writing Convincing Phishing Emails

We have three things to work with regarding phishing emails: the sender's email address, the subject and the content.

The Senders Address

Ideally, the sender's address would be from a domain name that spoofs a significant brand, a known contact, or a coworker.

- Observe their social media account for any brands or friends they talk to.
- Searching Google for the victim's name and rough location for any reviews the victim may have left about local businesses or brands.
- Looking at the victim's business website to find suppliers.
- Looking at LinkedIn to find coworkers of the victim.

The Subject

You should set the subject to something quite urgent, worrying, or piques the victim's curiosity, so they do not ignore it and act on it quickly.

Examples of this could be:

1. Your account has been compromised.
2. Your package has been dispatched/shipped.
3. Staff payroll information (do not forward!)
4. Your photos have been published.

The Content

If impersonating a brand or supplier, it would be pertinent to research their standard email templates and branding (style, logo's images, signoffs etc.) and make your content look the same as theirs, so the victim doesn't expect anything.

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

ans: **OSINT**

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

ans: **anchor text**

Task 4

Phishing Infrastructure

A certain amount of infrastructure will need to be put in place to launch a successful phishing campaign.

Domain Name:

You'll need to register either an authentic-looking domain name or one that mimics the identity of another domain. See task 5 for details on how to create the perfect domain name.

SSL/TLS Certificates:

Creating SSL/TLS certificates for your chosen domain name will add an extra layer of authenticity to the attack.

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.

Web Server:

You'll need to set up web servers or purchase web hosting from a company to host your phishing websites. Adding SSL/TLS to the websites will give them an extra layer of authenticity.

Analytics:

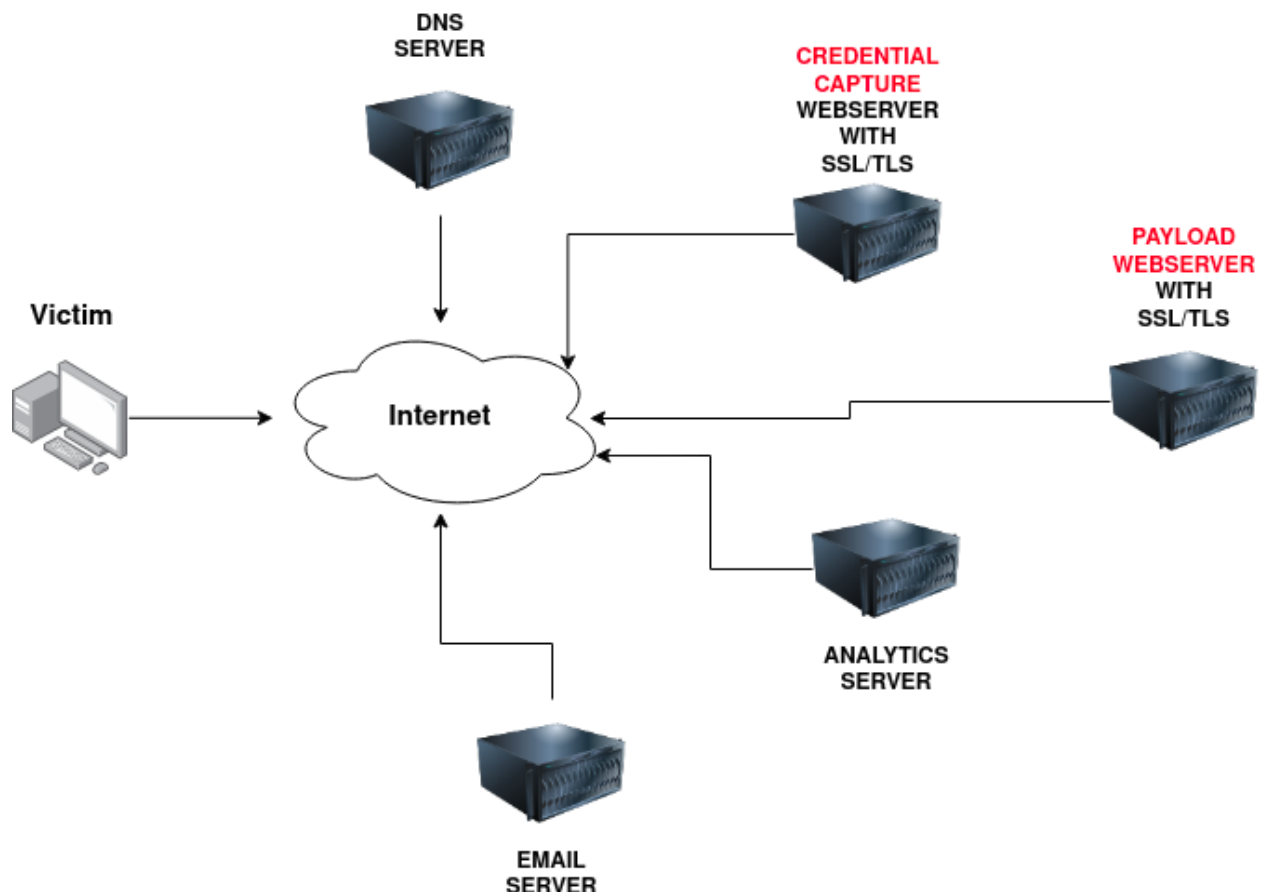
When a phishing campaign is part of a red team engagement, keeping analytics information is more important. You'll need something to keep track of the emails that have been sent, opened or clicked. You'll also need to combine it with information from your phishing websites for which users have supplied personal information or downloaded software.

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.

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.



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

ans: **SSL/TLS Certificates**

2. **What protocol has TXT records that can improve email deliverability?**

ans: **DNS**

3. **What tool can automate a phishing campaign and include analytics?**

ans: **Gophish**

Task 5

Using GoPhish

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.

in_lab

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>
```

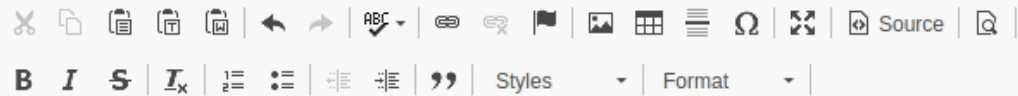
Click the **Source** button again, and you should see a login box with username and password fields as per the image below, also click the **Capture Submitted Data** box

and then also the **Capture Passwords** box and then click the Save Page button.

×

ACME Login

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!

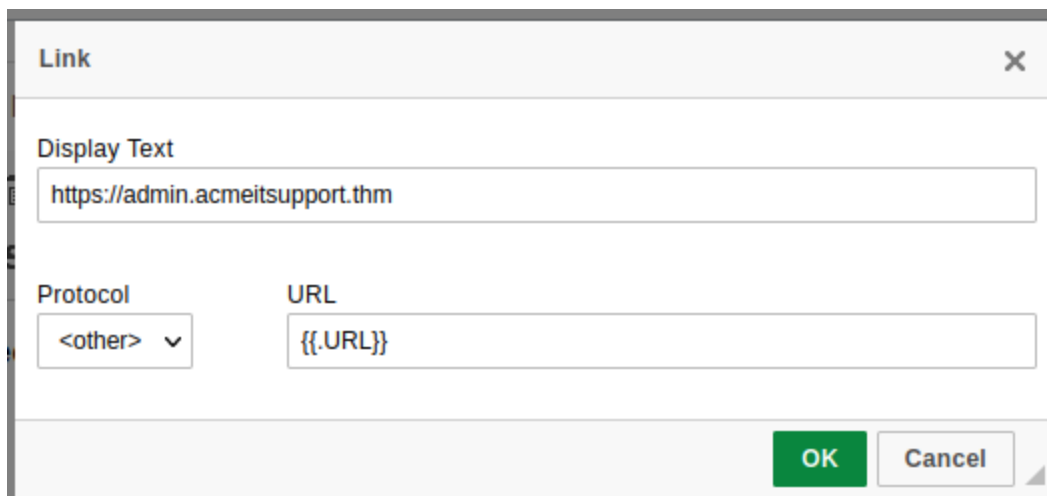
Redirect to: 

<http://example.com>

Save Page

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>**.



The screenshot shows a 'Link' dialog box with the following fields and controls:

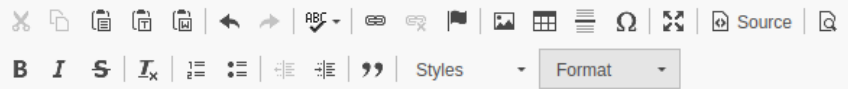
- Display Text:** A text input field containing the URL `https://admin.acmeitsupport.thm`.
- Protocol:** A dropdown menu currently showing `<other>`.
- URL:** A text input field containing the placeholder `{{.URL}}`.
- Buttons:** 'OK' (green) and 'Cancel' (grey) buttons at the bottom right.

×

Email 1

New Message Received

HTML



Online Team



+

10

▲

No data available in table

Showing 0 to 0 of 0 entries

Next

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

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](#)

Results

Email Sent



Clicked Link



Submitted Data



Email Reported



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.

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

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

Details

Show:

Search:

Name	Name	Email	Position	Status	Reported
▶		accounts@acmeitsupport.thm		Error	✕
▼		brian@acmeitsupport.thm		Submitted Data	✕

Timeline for

Email: brian@acmeitsupport.thm
Result ID: 07hUa9k

📧

Campaign Created

August 17th 2023 8:05:17 am

✉

Email Sent

August 17th 2023 8:05:17 am

!

Submitted Data

August 17th 2023 8:06:02 am

🖥

Linux (OS
Version: x86_64)

🦊

Firefox (Version: 115.0)

🔄 Replay Credentials

▼ View Details

Parameter	Value(s)
password	p4\$\$w0rd!
username	brian

▶

martin@acmeitsupport.thm

Email Sent

✕

Showing 1 to 3 of 3 entries

Previous1Next

1. **What is the password for Brian?**

ans: **p4\$\$w0rd!**

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.

The droppers are not usually malicious themselves, so they tend to pass antivirus checks. Once installed, the intended malware is either unpacked or downloaded from a server and installed onto the victim's computer. The malicious software usually connects back to the attacker's infrastructure. The attacker can take control of the victim's computer, which can further explore and exploit the local network.

1. **Do droppers tend to be malicious?**

ans: **no**

Task 7

Choosing A Phishing Domain

Choosing the right Phishing domain to launch your attack from is essential to ensure you have the psychological edge over your target. A red team engagement can use some of the below methods for choosing the perfect domain name.

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

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.

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

ans: **old**

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

ans: **Typosquatting**

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.

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

ans: **macros**

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.

That being said, it can happen, and as previously mentioned, it could be used to target old technologies on-site because possibly the browser software cannot be updated due to incompatibility with commercial software/hardware, which can happen quite often in big institutions such as education, government and especially health care.

An example of this is [CVE-2021-40444](#) from September 2021, which is a vulnerability found in Microsoft systems that allowed the execution of code just from visiting a

website.

1. Which recent CVE caused remote code execution?

ans: **CVE-2021-40444**

1. **What is the flag from the challenge?**

ans: **THM{I_CAUGHT_ALL_THE_PHISH}**