Metasploit Pro

Phishing Quick Start Guide

What Is Phishing?

Phishing is a social engineering technique that attempts to acquire sensitive information from a human target. During a phishing attack, a target receives a bogus e-mail disguised as an e-mail from a trusted source. The e-mail contains a tracking link that opens an authentic looking web page that contains a form that you want the target to fill out. If the target fills out and submits the form, you can capture their information and use it as evidence.

This Quick Start Guide will guide you through the necessary steps to set up and run a phishing attack from Metasploit Pro.

What Do I Need to Set Up a Phishing Attack?

Component	Description
Campaign	A logical grouping of components that you need to perform a social engineering attack, such as a web page or e-mail. Each social engineering attack is configured from within a campaign. Only one campaign can run at a time.
Email	A campaign component that defines the header and body for the e-mail that you send to targets.
E-mail Server	A machine that acts as a mail transfer agent (MTA). Metasploit Pro does not provide an MTA for you to send email. You must supply Metasploit Pro with the SMTP settings for your mail server. Before you define the SMTP server, make sure that the port that your mail server uses is not blocked by the Metasploit instance. Generally, ports 25 and 587 are recommended SMTP ports.
Web Page	A campaign component that you use to create the web page that the target visits.
Web Server	A machine that serves the web pages for the campaign. Metasploit Pro creates a web server locally to serve the web page.
Tracking URL	A HTML link that appears in the body of the email that enables click-through tracking. Each link is unique for each human target on the target list.
Target List	A list that defines the targets that you want to e-mail a phishing attack.

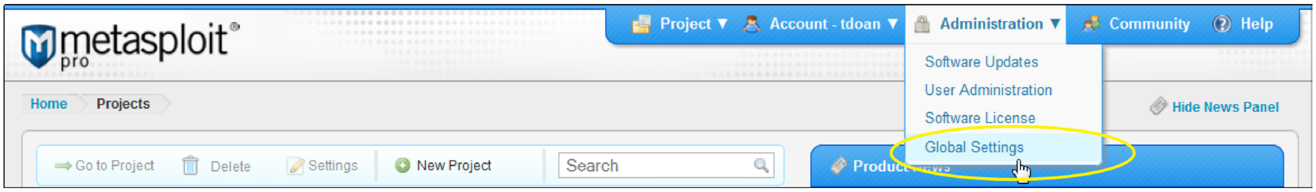
How Do I Set Up a Phishing Attack?

Task 1: Set up the SMTP settings for your mail server.
Task 2: Create a campaign.
Task 3: Create an e-mail that includes a link to your phishing web page.
Task 4: Clone a web page to create a fake web page.
Task 5: Set up the web server to host the web page.
Task 6: Generate a preview of the e-mail and the web page.
Task 7: Start the campaign.
Task 8: View the campaign findings.
Task 9: Stop the campaign when you are done and generate a report for the campaign.

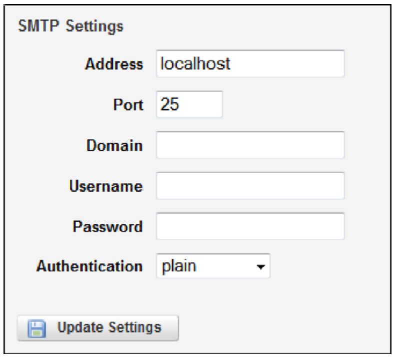
Set Up a Global Mail Server

If you intend to use the same mail server to send e-mails from Metasploit Pro, then you should set up your mail server through the global settings. After you globally define the SMTP settings for your mail server, Metasploit Pro will auto-fill the mail server information for your campaign.

1.) From the main menu, select **Administration > Global Settings**.



2.) When the Global Settings page appears, locate the SMTP settings.



SMTP Settings

Address	localhost
Port	25
Domain	
Username	
Password	
Authentication	plain

3.) Enter the following information to configure your SMTP settings:

- Address - The fully qualified mail server address (e.g., mail.domain.com).
- Port - The port that the mail server runs on.
- Domain - The hosted domain name for your mail server (e.g., domain.com)
- Username - The username that the system uses to authenticate the mail server.
- Password - The password that the system uses to authenticate the mail server.
- Authentication - The authentication type that the mail server uses.

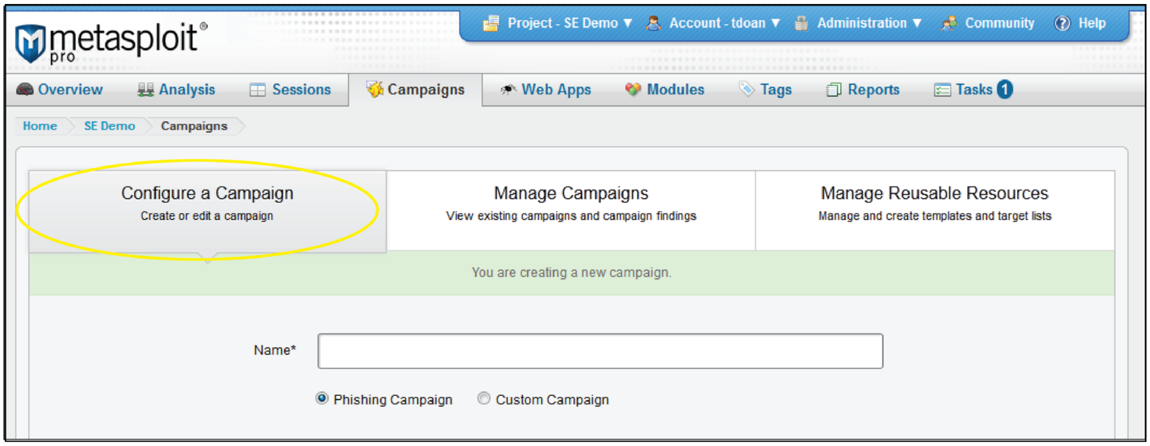
4.) Click the **Update Settings** button to save your changes.

Now you're ready to create a campaign.

Create a Campaign

1.) From within a project, click the **Campaigns** tab.

2.) Click the **Configure a Campaign** tab.

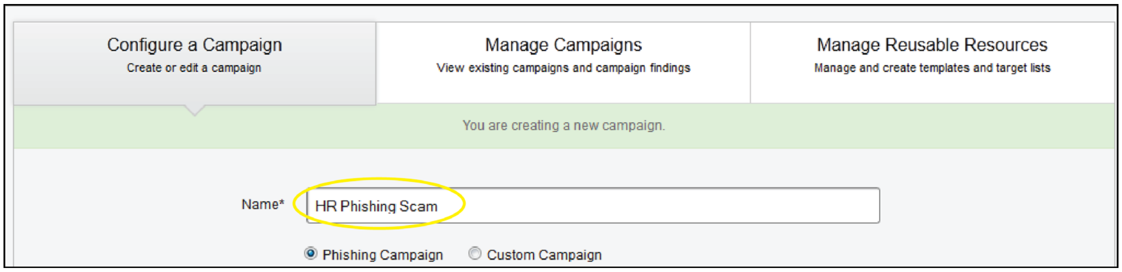


You are creating a new campaign.

Name*

● Phishing Campaign ○ Custom Campaign

3.) Enter a descriptive name for the campaign. For example, **HR Phishing Scam** helps you identify the campaign type and the targets.


Configure a Campaign
Create or edit a campaign
Manage Campaigns
View existing campaigns and campaign findings
Manage Reusable Resources
Manage and create templates and target lists

You are creating a new campaign.

Name* HR Phishing Scam

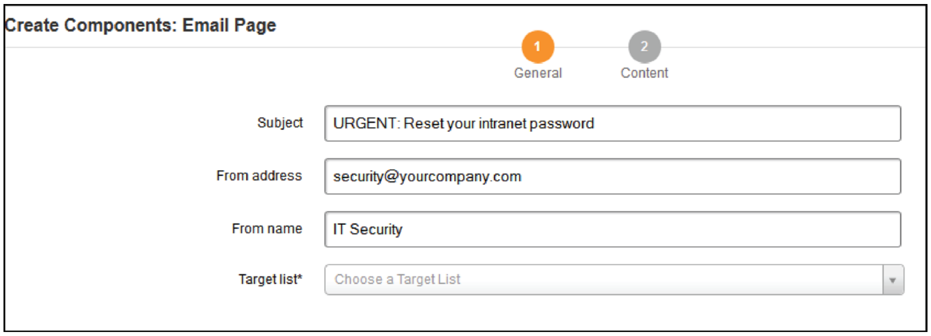
● Phishing Campaign ○ Custom Campaign

4.) Select **Phishing Campaign** as the setup option.

The next step is to configure the web page component.

Craft the E-mail

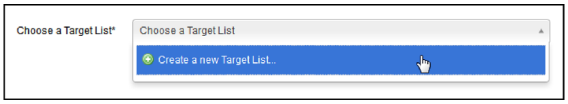
1.) From the **Campaign Components** area, click the **E-mail** icon.
2.) When the e-mail configuration page appears, enter the e-mail header information. You need to specify a name for the e-mail component, the e-mail subject line, the from address and the from name.



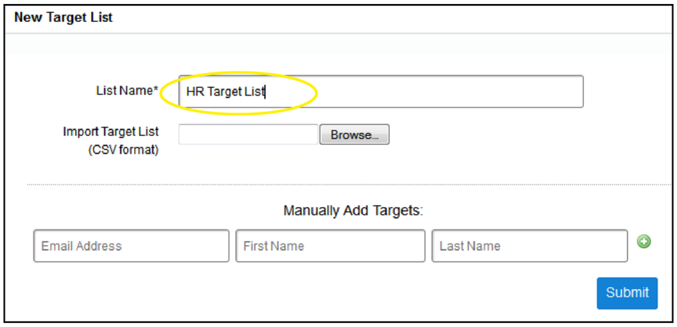
Create Components: Email Page

Subject: URGENT: Reset your intranet password
From address: security@yourcompany.com
From name: IT Security
Target list*: Choose a Target List

3.) Click the **Target list** dropdown and choose **Create a New Target List**.



4.) When the New Target List Window appears, enter a descriptive name for the list. For example, a name like **HR Targets List** helps identify the types of targets on the list.

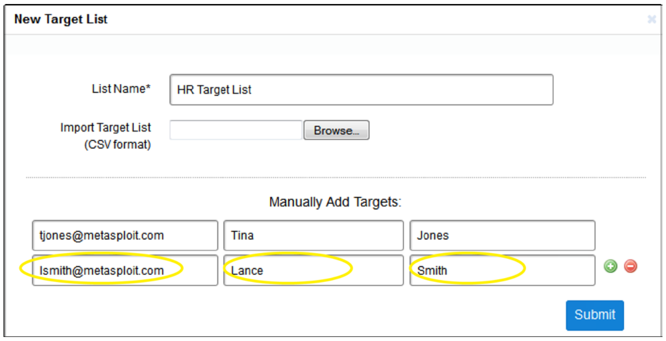


New Target List

List Name*: HR Target List

Manually Add Targets:

5.) Under **Manually Add Targets**, enter the e-mail address, first name, and last name for a target.



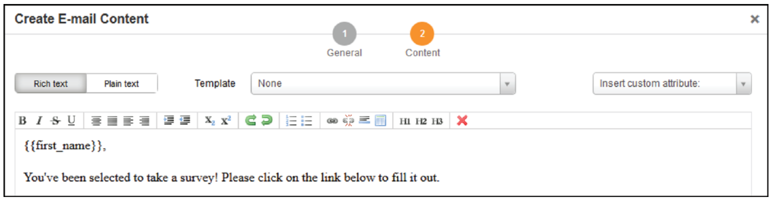
New Target List

List Name*: HR Target List

Manually Add Targets:

tjones@metasploit.com	Tina	Jones
lsmith@metasploit.com	Lance	Smith

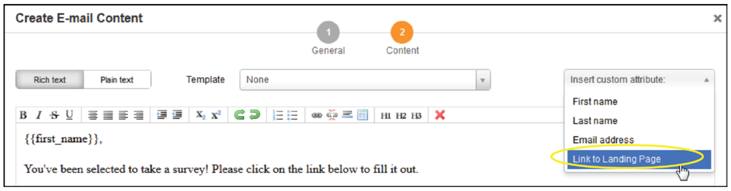
6.) Click the **('+') button** to add additional targets.
7.) Click the **Submit** button when you are done. This takes you back to the e-mail configuration page.
8.) Click **Next** to continue.
9.) In the **Content** box, enter the body of the e-mail.



{{first_name}},

You've been selected to take a survey! Please click on the link below to fill it out.

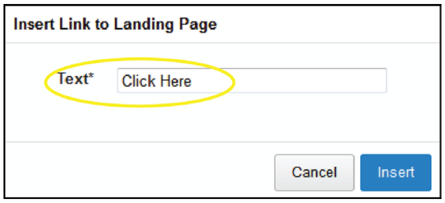
10.) After you create the content, use the **Link to Landing Page** attribute to insert the link into the e-mail.



{{first_name}},

You've been selected to take a survey! Please click on the link below to fill it out.

11.) When the **Insert a Link to Landing Page** window appears, enter the display text for the URL.

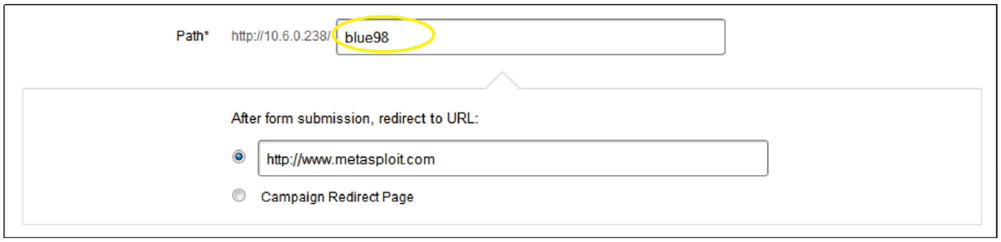


Text* Click Here

12.) Click the **Insert** button to insert the hyperlink into the e-mail. You'll see the link appear as {% campaign_web_link 'DISPLAY TEXT, 'Landing Page' %} in the e-mail content.
13.) Save the e-mail. The e-mail configuration page closes and takes you back to the campaign configuration page.

Create a Web Page

1.) From the **Campaign Components** area, click the **Landing Page** icon. The **Web Page** configuration page appears.
2.) Enter the URL that you want the page to be served at.



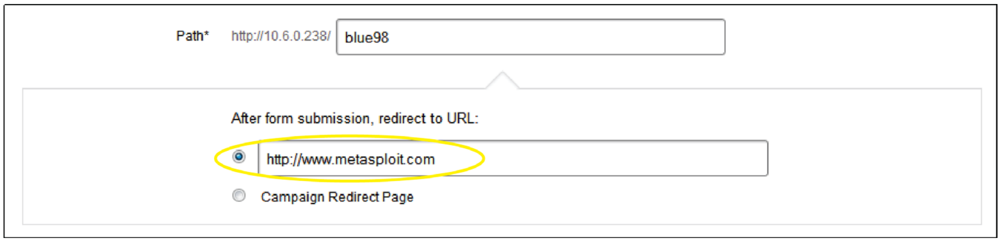
Path* http://10.6.0.238/ blue98

After form submission, redirect to URL:

● http://www.metasploit.com

○ Campaign Redirect Page

3.) Select the redirect page for the campaign. The redirect page can be a URL to a real web page or a web page that you create as part of your campaign. For the purpose of this Quick Start Guide, choose the **Redirect to URL** option and specify your company website.



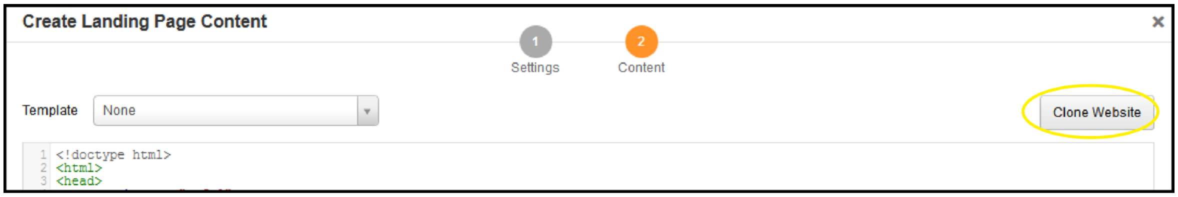
Path* http://10.6.0.238/ blue98

After form submission, redirect to URL:

● http://www.metasploit.com

○ Campaign Redirect Page

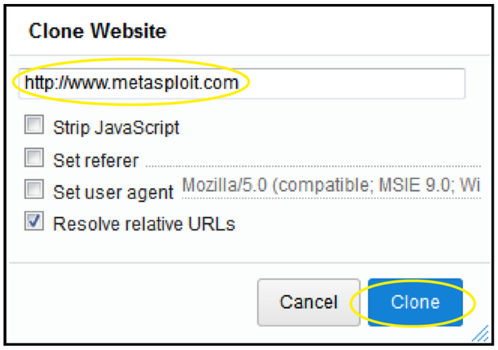
4.) Click the **Next** button to continue to the Content page.
5.) When the Content page appears, click the **Clone Website** button.



Template None

```
<!doctype html>
<html>
<head>
```

6.) When the **Clone Website** modal window appears, enter the web page that you want to clone and click the **Clone** button. The web page that you are cloning must contain a web form.



http://www.metasploit.com

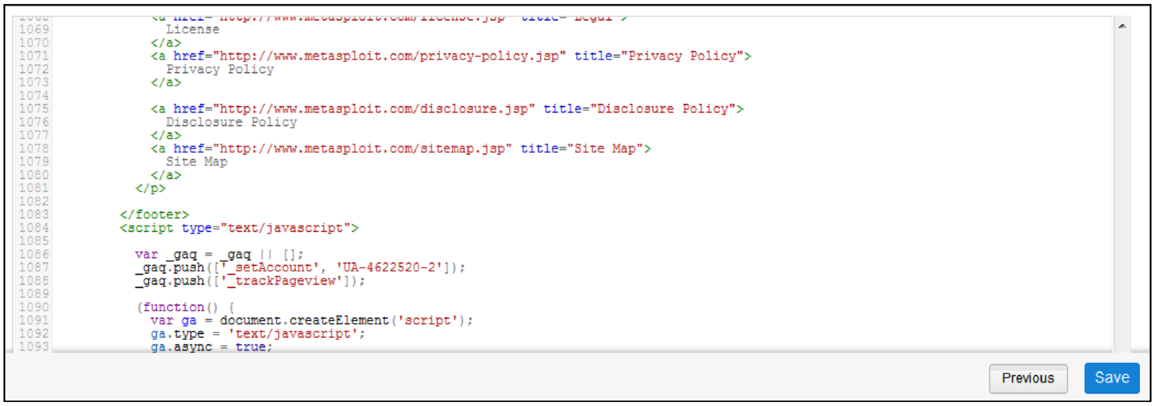
☐ Strip JavaScript

☐ Set referer

☐ Set user agent Mozilla/5.0 (compatible; MSIE 9.0; Wi

☑ Resolve relative URLs

When Metasploit Pro finishes cloning the web page, the HTML content will display in the Content Window.



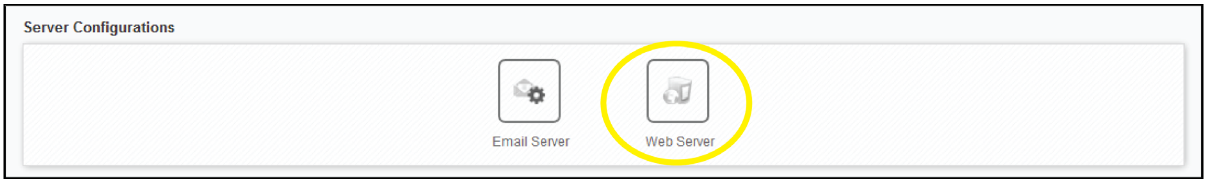
```
      License
    </a>
    <a href="http://www.metasploit.com/privacy-policy.jsp" title="Privacy Policy">
      Privacy Policy
    </a>

    <a href="http://www.metasploit.com/disclosure.jsp" title="Disclosure Policy">
      Disclosure Policy
    </a>
    <a href="http://www.metasploit.com/sitemap.jsp" title="Site Map">
      Site Map
    </a>
  </p>

</footer>
<script type="text/javascript">

  var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-4622520-2']);
  _gaq.push(['_trackPageview']);

  (function() {
    var ga = document.createElement('script');
    ga.type = 'text/javascript';
    ga.async = true;
```

7.) Click the **Save** button.

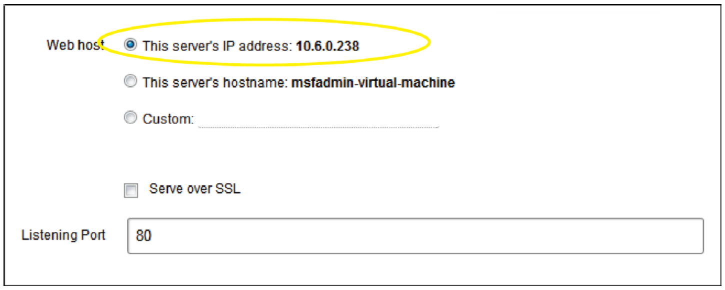
The Phishing Wizard takes you back to the **Configure a Campaign** page. The next step is to set up the e-mail component.

Set Up the Local Web Server

1.) Under **Server Configurations**, click the **Web Server** icon. The **Web Server** configuration page appears.

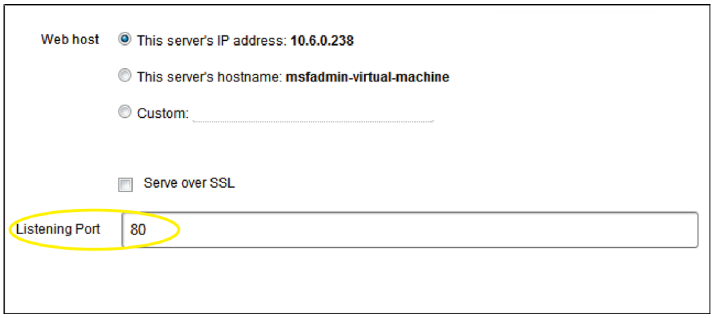


2.) Enter the address, or URL, that you want to use to link to the web page. You can use the IP address for your local Metasploit Pro machine or if you have DNS set up, you can specify the domain name instead.



Web host ● This server's IP address: **10.6.0.238**
○ This server's hostname: **msfadmin-virtual-machine**
○ Custom:
☐ Serve over SSL
Listening Port 80

3.) Enter the port that you want to use to run the website. You should specify a port that's typically used for HTTP traffic, such as 8080 or 80.



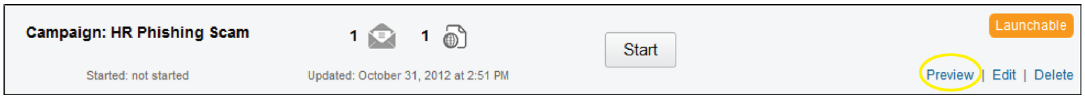
Web host ● This server's IP address: **10.6.0.238**
○ This server's hostname: **msfadmin-virtual-machine**
○ Custom:
☐ Serve over SSL
Listening Port 80

4.) Click **Save** to save the web server settings.
5.) From the campaign configuration page, click **Done** to save the campaign.

Please note that targets can view the web page only if they are able to access Metasploit Pro from their location on the network. If the target cannot reach the web server, tracking and web content may not work as intended.

Preview the E-mail and Web Page

1.) From the **Manage Campaigns** area, find the campaign you just created.
2.) Click the **Preview** link.

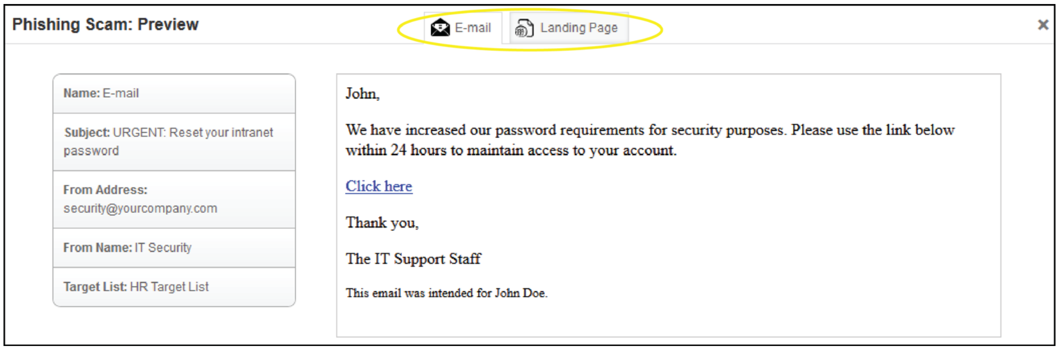


Campaign: HR Phishing Scam

Started: not started

Updated: October 31, 2012 at 2:51 PM

3.) The preview window appears and shows you what the generated e-mail and web page will look like. Use the **E-mail** and **Landing Page** tabs to switch between previews.



Phishing Scam: Preview

Name: E-mail

Subject: URGENT: Reset your intranet password

From Address: security@yourcompany.com

From Name: IT Security

Target List: HR Target List

John,

We have increased our password requirements for security purposes. Please use the link below within 24 hours to maintain access to your account.

Click here

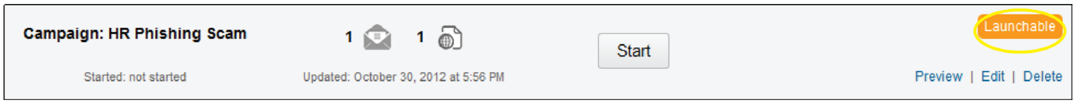
Thank you,

The IT Support Staff

This email was intended for John Doe.

Start the Phishing Attack

1.) From the **Manage Campaigns** tab, find the campaign you just created. If you successfully created the campaign, the campaign status should indicate that it is launchable.

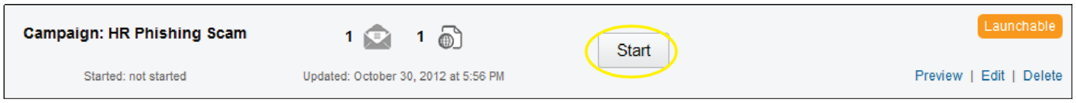


Campaign: HR Phishing Scam

Started: not started

Updated: October 30, 2012 at 5:56 PM

2.) Click the **Start** button.

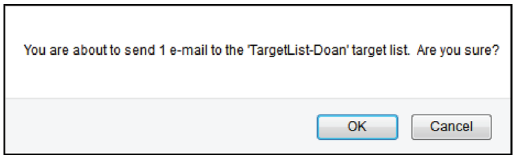


Campaign: HR Phishing Scam

Started: not started

Updated: October 30, 2012 at 5:56 PM

3.) A confirmation window appears and prompts you to confirm that you want to send the phishing e-mail. Click **OK** to start the campaign.



You are about to send 1 e-mail to the 'TargetList-Doan' target list. Are you sure?

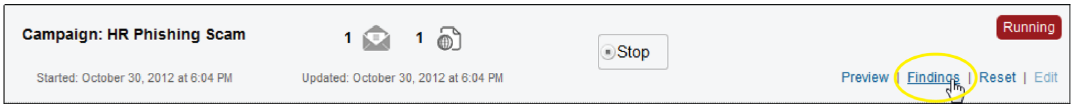
When you start the campaign, the campaign status changes from launchable to running. This status indicates that phishing e-mail has been sent and the web page is online and accessible to any human target that can reach the Metasploit Pro instance.

Metasploit Pro starts to track the human target after they open the e-mail, which contains a tracking GIF that alerts the campaign when an e-mail is opened. When the human target clicks on the link provided in the e-mail and visits the spoofed web page, a cookie is set in order to accurately track the future actions taken by the human target.

You will be able to see the statistics for the campaign update in real-time from the Campaign Findings. For example, if the target submits their credentials through a login page, you will see the statistics for form submissions increment and you will be able to click on the stat bubble to see who has submitted the form.

View Real-Time Stats

1.) From the **Manage Campaigns** tab, find the campaign that you just launched.
2.) Click the **Findings** link.



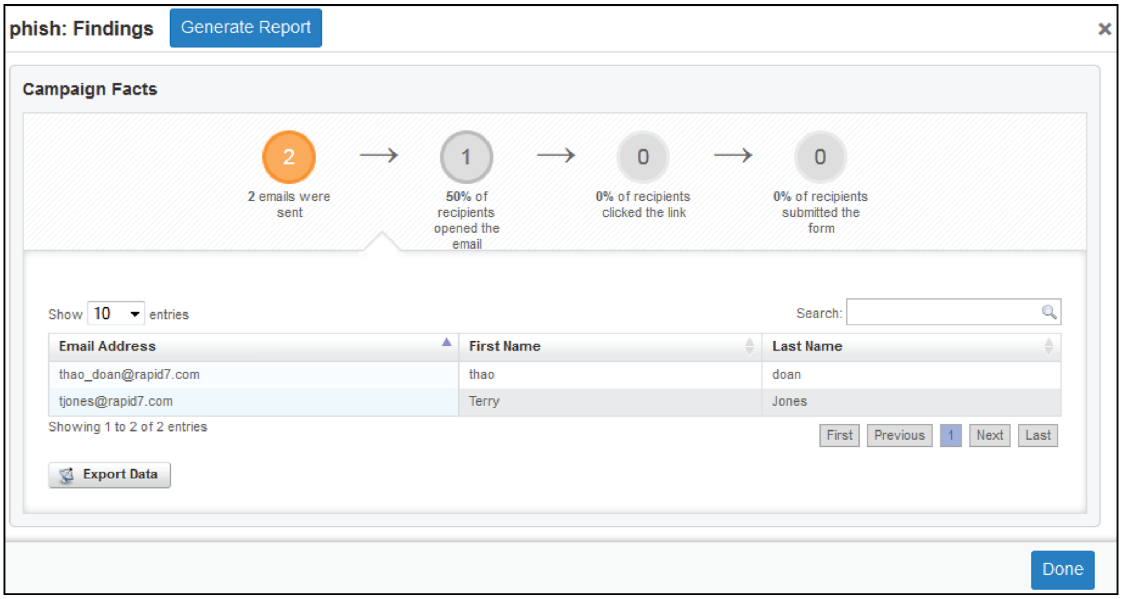
Campaign: HR Phishing Scam 1 1

Started: October 30, 2012 at 6:04 PM

Updated: October 30, 2012 at 6:04 PM

The **Findings** window appears and shows you the current statistics for the campaign. It shows a high level breakdown of how the targets responded to the phishing attack and reveals the level of success that the phishing attack had on the targets. You can click on any of the stat bubbles to see a list of targets associated with a particular finding.

Additionally, if you want generate a report at this point, you can click on the **Generate Report** button that is available on the **Campaign Findings** window.



2 → 1 → 0 → 0

2 emails were sent

50% of recipients opened the email

0% of recipients clicked the link

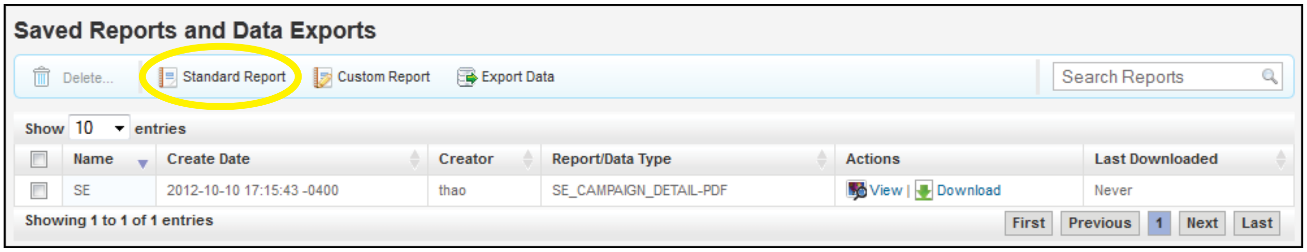
0% of recipients submitted the form

Email Address	First Name	Last Name
thao_doan@rapid7.com	thao	doan
tjones@rapid7.com	Terry	Jones

Showing 1 to 2 of 2 entries

View the Report

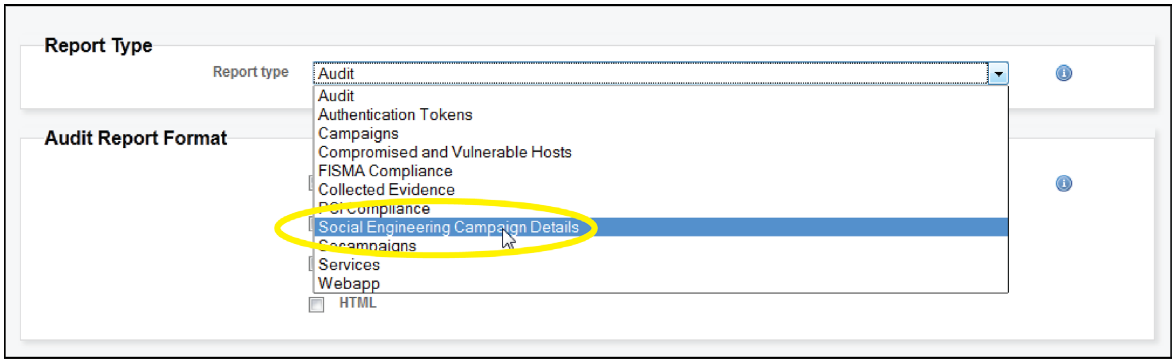
1.) From the Manage Campaigns tab, click the **Stop** button to stop the campaign.
2.) Select the **Reports** tab from the Tasks bar. The **New Report** page appears.



☐	Name	Create Date	Creator	Report/Data Type	Actions	Last Downloaded
☐	SE	2012-10-10 17:15:43 -0400	thao	SE_CAMPAIGN_DETAIL-PDF	View | Download	Never

Showing 1 to 1 of 1 entries

3.) Click the **Report Type** dropdown and select **Social Engineering Campaign Details**. This report provides a high-level graphical breakdown of the statistics collected by Metasploit Pro, like the number of targets who opened the e-mail, clicked on the link, and submitted the form. Additionally, you'll see the configuration for the campaign, including the component settings and an expanded target list.



Report type: Audit

4.) Choose the file format you want to use to generate the report. PDF is a good choice.
5.) Enter a name for the report.
6.) Select the campaign that you want to generate a report for.
7.) Keep the default report sections and report options.
8.) Generate the report. The Tasks log displays and shows the generation of the report.
9.) After the report generation finishes, go back to the Reports area.
10.) Find the report that you just generated and click **View**.

The report opens and displays the data that is available for the phishing campaign. There's a lot of data for you to peruse. For a quick overview, go to the Social Engineering Funnel section. You'll see a high-level breakdown of response types from your human targets.