Metasploit Pro

4.5 Release Guide

What's New in Metasploit Pro 4.5?

The Metasploit Pro 4.5 release focuses on streamlining and simplifying the abilty to create social engineering attacks. The goal is to provide an intuitive and user-friendly interface that makes social engineering an easier process than it currently is in Metasploit Pro 4.4.

With that said, Metasploit Pro 4.5 introduces a completely redesigned user interface for social engineering. The new user interface features an interactive dashboard made up of widgets, modal windows, and action links. These new user interface elements integrate together to provide a guided workflow that makes setting up a phishing scam or USB key drop a very simple process.

Read on to learn more about what's new in this release.

Getting Metasploit Pro 4.5

For existing users:
Before you install an update, make sure that your instance of Metasploit has the latest updates for your current release of Metasploit. To update Metasploit, select **Administration** > **Software Updates** from the Main menu. Then, click the **Check for Updates** button. If an update is available, you will see an install button. Click the **Install** button to update your system.

For new users:
Visit http://www.metasploit.com/download to download the installer for your operating system. Metasploit provides installers for Windows, Linux 32-bit, and Linux 64-bit systems. After you download the installer, read the Windows Installation Guide or the Linux Installation Guide for instructions on how to set up Metasploit.

New Product Terms

Product Term	Description
Campaign	A logical grouping of components, such as e-mails and web pages, that you need to perform a social engineering attack.
Campaign Component	An e-mail, web page, or portable file.
Human Target	The person who receives the social engineering attack or is part of a campaign.
Portable File	A campaign component that generates an executable file or file format exploit.
Reusable Resource	A web page template, e-mail template, or target list.
Target List	A list of human targets, or recipients, that you want to e-mail a social engineering attack.
Tracking GIF	A GIF that tracks when a human target opens a phishing e-mail.
Tracking String	A string that encodes the target and e-mail IDs. Campaigns use tracking strings to monitor the activity of a target.

A Tour of the New Social Engineering Interface

Metasploit Pro 4.5 introduces a complete redesign of the social engineering interface that was available in Metasploit Pro 4.4 and earlier. The new user interface is called the Campaign Dashboard, and it is available under the Campaigns area of Metasploit Pro.

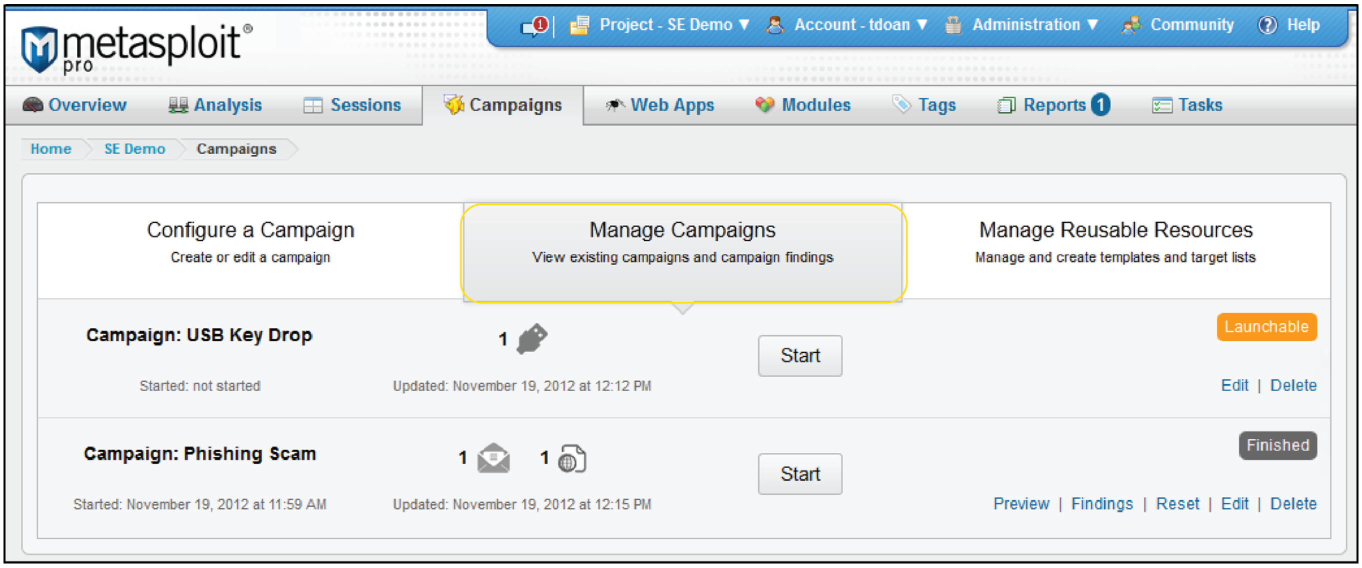
Let’s take a look at the new Campaign Dashboard and how to navigate around.

Campaign Dashboard

The Campaign Dashboard provides you with access to all the tools you need to create and manage social engineering campaigns. It consists of widgets, modal windows, and actionable links that you can use to access the different areas of campaigns.

Click on a tab to switch between the three main areas of the Campaign Dashboard: campaign configuration, campaign managment, and reusable campaign resources. When you click on a tab, Metasploit Pro slides the new window into view.

To create a new campaign, click the **Configure a Campaign** tab. To run, manage, or view the findings for a campaign, visit the **Manage Campaigns** tab. To create and manage templates and target lists, go to the **Manage Reusable Resources** tab.



Campaign: USB Key Drop 1
Started: not started
Updated: November 19, 2012 at 12:12 PM

Campaign: Phishing Scam 1 1
Started: November 19, 2012 at 11:59 AM
Updated: November 19, 2012 at 12:15 PM

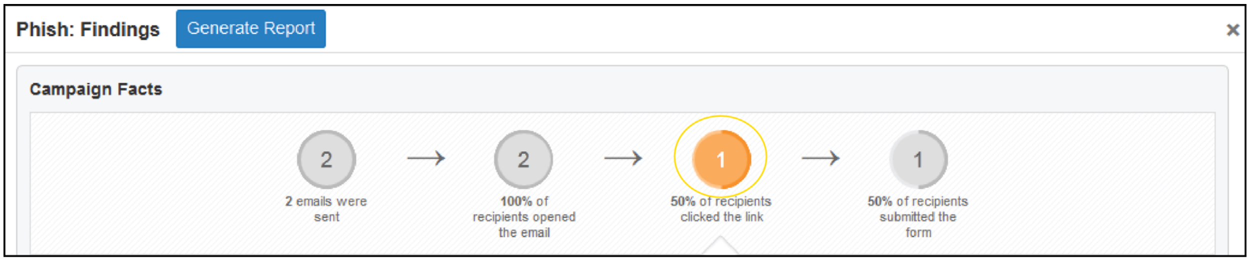
The Campaign Dashboard

Campaign Findings

The campaign findings provides a high-level summary of a campaign based on the data that Metasploit was able to collect from the human targets. Metasploit tracks the number of human targets that opened the phishing e-mail, clicked on the link, and submitted data through the spoofed webpage. Additionally, if the campaign delivers an exploit, Metasploit tracks the number of sessions that it was able to open.

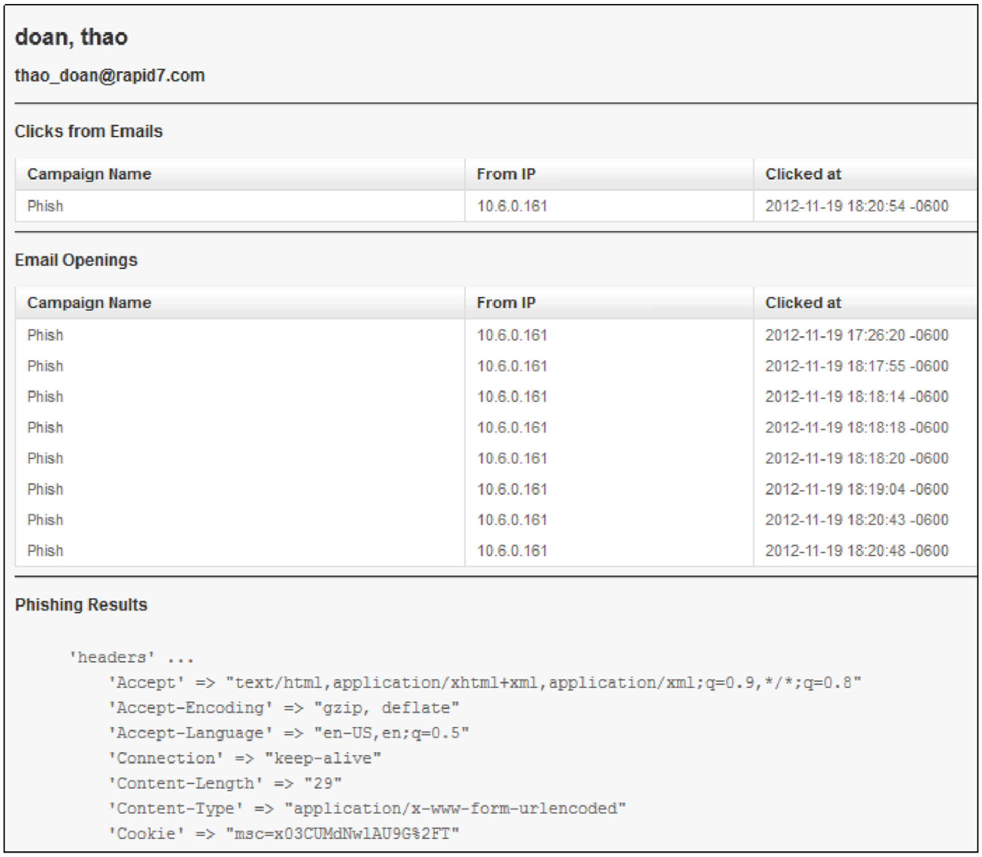
To view the Campaign Findings, select **Campaigns > Show Campaigns** from the Tasks menu. When the Manage Campaigns area appears, find the campaign whose results you want to view, and click the **Findings** link.

When the Campaign Findings window opens, you can click on any of the stat bubbles to view a list of human targets that are associated with that finding.


Phish: Findings
Generate Report
×
Campaign Facts
2
2 emails were sent
2
100% of recipients opened the email
1
50% of recipients clicked the link
1
50% of recipients submitted the form

Campaign Findings

Additionally, if you click on their e-mail address, you will the history page for the human target. This is where Metasploit stores the data that it tracks and collects for a human target.



doan, thao

thao_doan@rapid7.com

Clicks from Emails

Campaign Name	From IP	Clicked at
Phish	10.6.0.161	2012-11-19 18:20:54 -0600

Email Openings

Campaign Name	From IP	Clicked at
Phish	10.6.0.161	2012-11-19 17:26:20 -0600
Phish	10.6.0.161	2012-11-19 18:17:55 -0600
Phish	10.6.0.161	2012-11-19 18:18:14 -0600
Phish	10.6.0.161	2012-11-19 18:18:18 -0600
Phish	10.6.0.161	2012-11-19 18:18:20 -0600
Phish	10.6.0.161	2012-11-19 18:19:04 -0600
Phish	10.6.0.161	2012-11-19 18:20:43 -0600
Phish	10.6.0.161	2012-11-19 18:20:48 -0600

Phishing Results

```
'headers' ...
    'Accept' => "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
    'Accept-Encoding' => "gzip, deflate"
    'Accept-Language' => "en-US,en;q=0.5"
    'Connection' => "keep-alive"
    'Content-Length' => "29"
    'Content-Type' => "application/x-www-form-urlencoded"
    'Cookie' => "msc=x03CUMdNwlAU9G%2FT"
```

Historical Data for a Human Target

Frequently Asked Questions

The following collection of FAQs provide brief answers to a few of the questions you may encounter while working with the redesigned social engineering feature. Please read these FAQs and check out the community forums before you send a support request.

Legacy Campaigns

Will my old campaigns still work?

You cannot run a legacy campaign in Metasploit Pro 4.5 or migrate the campaign content over to the new style of campaigns. However, you can still access a legacy campaign to generate the Pre-4.5 Campaigns Report, which provides an audit of the configuration and findings of all legacy campaigns in a project.

How do I view my legacy campaigns?

Use the following URL: https://<metasploit_instance>:3790/workspaces/<n>/campaigns, where n represents the workspace ID assigned to a project. For example, the default project has a workspace ID of 1, so to access the old campaigns for that project on the local Metasploit instance, use the following URL: https://localhost:3790/workspaces/1/campaigns.

How do I migrate my legacy campaigns to the new style of campaigns?

The best way to migrate a legacy campaign is to create a new campaign that uses the same configuration as the legacy campaign. Metasploit Pro currently does not offer migration capabilities.

USB Drive Drops

Can I still generate an executable for manual delivery?

Yes. To generate an executable or file format exploit for delivery through an external storage device, you create a portable file campaign.

Campaign Reports and Findings

What type of data does Metasploit report on?

Metasploit reports on the number of recipients who opened the spoofed e-mail, clicked on the web page link, submitted data, and the number of sessions Metasploit was able to open.

How can I view the data that a human target has submitted?

From the Campaign Findings, click on a stat bubble. When the list of human targets appear, click on an e-mail address to open the history page for that human target. You'll see any data that the human target has submitted for any campaign that they are a part of.

Web Pages and E-mails

Can I reuse web pages and e-mails that I've created?

No, but you can create a template, which is reusable set of content and formatting that you can apply to an e-mail or web page. To create a template, go to the Manage Reusable Resources tab and choose the type of template that you want to create.

Can I clone a web page?

Yes. When you clone a web page, Metasploit Pro copies the HTML from the website and recreates the webpage for your campaign.

Can I clone an e-mail?

No, Metasploit currently does not provide the ability to clone an e-mail.

Can I use relative URLs when I create a web page?

No, you must use absolute URL paths.

Mail Server Settings

Does Metasploit provide an MTA?

No, Metasploit does not provide an MTA. You will need to provide Metasploit with the credentials and SMTP settings for a locally hosted mail server or an SMTP relay service.

What are some restrictions that may prevent me from using my mail server to send e-mail through Metasploit?

- Your mail server performs reverse DNS checks and has rejected mail from Metasploit because it thinks that the e-mail is spam. If this is the case, you need to use a mail server that has less restrictive checks for spam, malicious files, and any type of e-mail abuse. Although these checks are in place to ensure that your e-mail infrastructure is secure, they prevent you from sending e-mails from Metasploit Pro.

- The port that you are using to send mail is blocked. The most common port used to send mail is port 25. If this port is blocked, try ports 465, 587, or 2525.

- The mail server is unable to authenticate the login. Check the authentication type configured for your mail server. By default, Metasploit uses the plain auth type.

I set up my mail server, but it's not sending any e-mail. How can I troubleshoot this issue?

To troubleshoot this issue, you need to take a look at the task log. To access the task log, click the **Tasks** tab. Find the campaign task and click on the task name. When the task log appears, search for any text highlighted in red. Any red text indicates that Metasploit encountered an error while processing the task. Errors like "Server refused our mail" indicates an issue with the mail server being able to authenticate the login or send the e-mail.

Where do I configure the SMTP settings for my mail server?

You can define the SMTP settings through the Global Settings or directly through the campaign. If you define the SMTP settings globally, Metasploit uses the SMTP settings as the default settings for all new campaigns that you create.

To define global SMTP settings, select **Administration > Global Settings** from the Main menu. Find the SMTP Settings and fill out the domain and authentication informaion.

Support

How do I file a defect that I've found while working with Metasploit Pro?

Please send an e-mail to support@rapid7.com. Provide a detailed description of the issue you are encountering and describe the steps to reproduce the issue. The support team may ask you to provide the production log, which is located in /path/to/Metasploit/apps/pro/ui/log.

Where can I find tutorials and documentation for the new social engineering features?

/INSERT LINKS WHEN THEY ARE AVAILABLE.