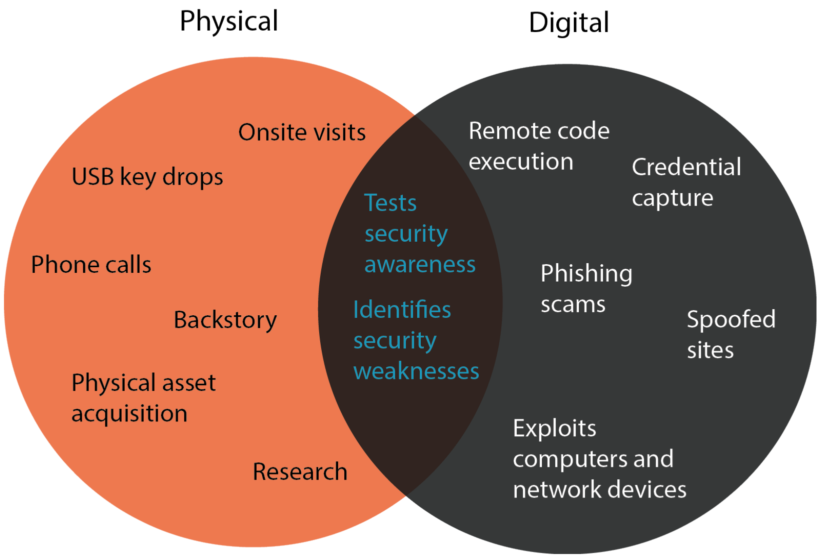
Best Practices for Social Engineering Attacks

Social engineering is an attack method that induces a person to unknowingly divulge confidential data or to perform an action that enables you to compromise their system. Typically, social engineering attacks utilize delivery-based methods, such as e-mail and USB keys, but they can also use other mechanisms, such as phone calls and onsite visits. Social engineering attacks are becoming more prevalent in the existing security landscape and are forcing many organizations to take a closer look at one of their most vulnerable targets: their employees.

As part of a penetration testing engagement or a security awareness program, you may be asked to perform social engineering tests to audit the organization's physical and IT security infrastructure. Before you can execute any type of social engineering test, you should sit down with the organization to clearly define the objectives of the engagement and to explicitly identify the goals that they wish to achieve. Most organizations will want to measure the effectiveness of their security training program or identify the weaknesses in their existing security policies and IT defense mechanisms. Once you have a clear understanding of the purpose of the assessment, you can build an attack plan that addresses all the areas of concern.

Generally, there are two distinct forms of social engineering penetration tests: digital and physical tests. A digital social engineering test focuses more on IT security and policy compliance whereas a physical social engineering test deals more with human behavior and tangible assets, like office spaces and company equipment. Depending on the goals of the engagement, you may utilize only one style of testing or you may incorporate both types.

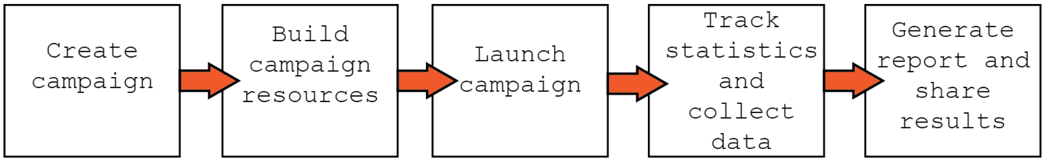


For example, if the organization wants to identify the metrics for employee security policy compliance, you may need to build a long-term plan that establishes an initial baseline before any social engineering attacks even take place. Once you have determined the baseline, you can implement social engineering attacks, like USB key drops and phishing scams, that test both the physical security perimeter as well as the protection of digital data.

Social Engineering with Metasploit Pro

Metasploit Pro's social engineering feature mainly focuses on computer-based attacks. Most computer-based social engineering attacks utilize a delivery mechanism, like e-mail, to send links to a spoofed website or attachments that contain a malicious file. With Metasploit Pro, you can create and distribute the necessary e-mails and files that are typically associated with digital attacks.

In Metasploit Pro, a social engineering penetration test is performed through a campaign. A campaign is the workspace that you use to manage and execute all social engineering related tasks. Additionally, a campaign tracks test findings and stores the resource files that you need to create social engineering attacks, such as web page templates, e-mail templates, malicious executables, and target lists.


Create campaign
Build campaign resources
Launch campaign
Track statistics and collect data
Generate report and share results

To understand how social engineering works with Metasploit Pro, let's go over the most common types of social engineering attacks and the processes that you will use to implement them. Along the way, we will provide you with some best practice tips that will help you set up effective and useful social engineering tests.

Phishing

If you look in your SPAM folder, you will undoubtedly find phishing e-mails that have been perfectly crafted to look like they are from your bank, your friends in Nigeria, or pretty much anyone with whom you would share your most confidential information. These e-mails may look nearly identical to the real e-mails, or they may be terrible recreations of the original. Regardless, their purpose is to trick the reader into believing in their authenticity. The e-mail may contain header information, like the sender's e-mail address, that looks absolutely legitimate. The e-mail may also contain headers, footers, and logos that are near identical matches to the real ones.

```
Hey John,

Your password is about to expire.
Please visit Netsuite to update your
account. Use this link to access your
account directly.

Thanks,
IT
```

RAPID7

Ultimately, the goal is to get the reader to click on a link provided in the e-mail. The link directs them to a spoofed site that is set up to steal data and use the stolen information for nefarious purposes.

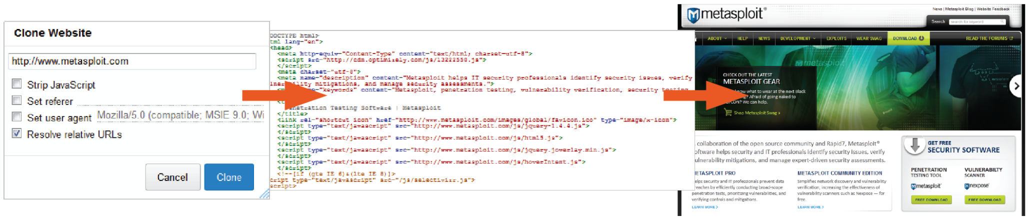
This is where Metasploit Pro comes into the picture. One of the major capabilities of the Metasploit Pro social engineering feature is the ability to easily create and send phishing e-mails. From within Metasploit Pro, you can create and set up the components that you need to run a phishing attack - including the phishing e-mail, spoofed website, mail server settings, and target list.

Now that you have a general overview of how phishing attacks work, and how Metasploit Pro helps you phish people, let's go over some tips that will help you set up successful phishing attacks.

Phishing Tip #1: Clone, clone, clone.

One of the most useful capabilities of the social engineering feature is the ability to clone a real, live web page. To clone a web page, you simply need to provide Metasploit Pro with the URL. Metasploit Pro makes a copy of the web page's HTML and imports it into the campaign. After the HTML has been imported, you can tweak the code to further customize or perfect the page.

Since the purpose of a spoofed web page is to trick a human target into believing in its authenticity, it is absolutely vital that the spoofed web page be a near replica of the real one. Therefore, unless you are creating a unique web page for the purposes of the campaign, you should always clone an existing web page. When you clone an existing web page, resources files, such as images, will be served from the cloned website and yield less setup overhead. Overall, the cloning feature makes it extremely fast and easy for you to get a web page up and running.



Clone Website

http://www.metasploit.com

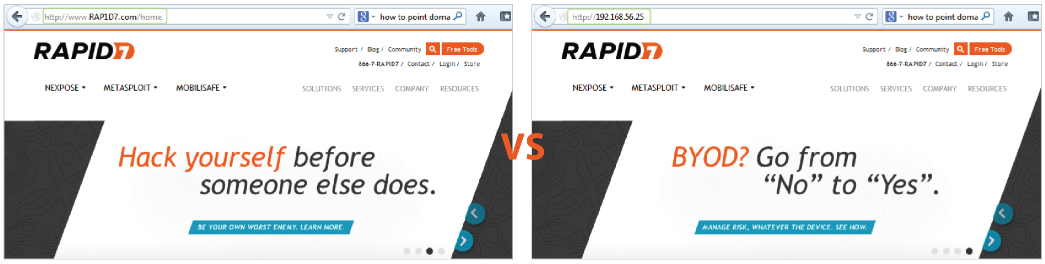
☐ Strip JavaScript
☐ Set referer
☐ Set user agent Mozilla/5.0 (compatible; MSIE 9.0; Wi
☑ Resolve relative URLs

```
DOCTYPE html>
tml lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <script src="http://cdn.optimizely.com/js/13222550.js">
  </script>
  <meta charset="utf-8">
  <meta name="description" content="Metasploit helps IT security professionals identify security issues, verify
lnerability mitigations, and manage security assessments.">
  <m        ="keywords" content="Metasploit, penetration testing, vulnerability verification, security testing
  <t
    netration Testing Software | Metasploit
  </title>
  <link rel="shortcut icon" href="http://www.metasploit.com/images/global/favicon.ico" type="image/x-icon">
  <script type="text/javascript" src="http://www.metasploit.com/js/jquery-1.4.4.js">
  </script>
  <script type="text/javascript" src="http://www.metasploit.com/js/html5.js">
  </script>
  <script type="text/javascript" src="http://www.metasploit.com/js/jquery.joverlay.min.js">
  </script>
  <script type="text/javascript" src="http://www.metasploit.com/js/hoverIntent.js">
  </script>
  <!--[if (gte IE 6)&(lte IE 8)]>
cript type="text/javascript" src="/js/selectivizr.js">
script>
```

Phishing Tip #2: Set up a real looking domain.

A domain name is the most obvious telltale of a suspicious website, so it's important that you use a domain name that is a close match to the real one. For example, the fake domain name for Rapid7 can be something like RAP1D7 or RAPID7. Obviously, a URL like http://www.RAPID7.com/home looks much less nefarious than http://196.184.132.24/home.

Since most people should be able to recognize a blatantly fake URL, you should use a real looking domain name. This will test a human target's ability to examine URLs and identify malicious links.


http://www.RAP1D7.com/home
how to point doma
RAPID7
Support / Blog / Community
Free Tools
866-7-RAPID7 / Contact / Login / Store
NEXPOSE
METASPLOIT
MOBILISAFE
SOLUTIONS
SERVICES
COMPANY
RESOURCES
Hack yourself before someone else does.
BE YOUR OWN WORST ENEMY. LEARN MORE.
VS
http://192.168.56.25
how to point doma
RAPID7
Support / Blog / Community
Free Tools
866-7-RAPID7 / Contact / Login / Store
NEXPOSE
METASPLOIT
MOBILISAFE
SOLUTIONS
SERVICES
COMPANY
RESOURCES
BYOD? Go from "No" to "Yes".
MANAGE RISK, WHATEVER THE DEVICE. SEE HOW.

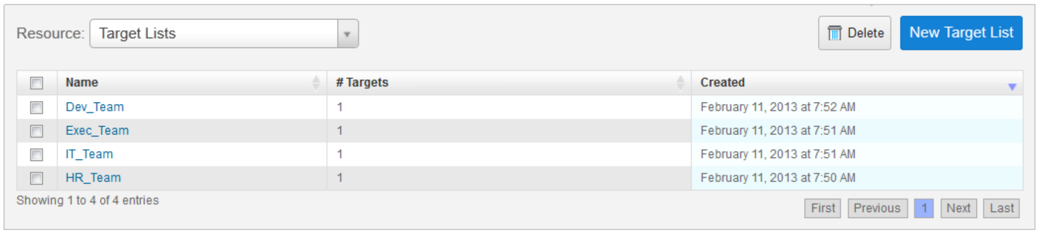
In order to set up a domain name for your Metasploit web server, you'll need to own and register the domain name. Once you have all of that set up, you'll need to point the domain name at the server running your Metasploit instance.

Phishing Tip #3: Target a smaller population.

To maintain the sanity of your IT team, you should use smaller target lists for the majority of your social engineering tests. With smaller target lists, you will be able to easily mitigate any issues and concerns that may arise.

Additionally, by limiting the number of human targets, you can control the sample of people participating in the test. For example, you may want to create a separate target list for your IT team because they may require a different type of social engineering test than the rest of the company.

However, there may be occasions where you want to run large scale tests. These tests will typically replicate a real attack scenario in which a large portion of the organization is affected. In these particular cases, you should create a large target list that includes all the targets in the organization. These large scale tests will help the organization understand their current security posture and identify where improvements need to be made in the IT and security infrastructure.



□	Name	# Targets	Created
□	Dev_Team	1	February 11, 2013 at 7:52 AM
□	Exec_Team	1	February 11, 2013 at 7:51 AM
□	IT_Team	1	February 11, 2013 at 7:51 AM
□	HR_Team	1	February 11, 2013 at 7:50 AM

Showing 1 to 4 of 4 entries

Phishing Tip #4: Use a SMTP relay service.

One of the most common issues you may encounter during a social engineering test is the inability to send e-mail through your local mail server. Most mail servers will perform a reverse DNS lookup to verify that the IP address of the server hosting Metasploit Pro matches the domain name of the e-mail that you are trying to spoof. If there's an issue with the reverse DNS lookup, the mail server will most likely reject the e-mail because it appears to originate from a suspicious source.

Since mail servers are configured to use the highest level of protection and to perform restrictive checks for spam, malicious e-mails, and e-mail abuse, it makes it very difficult to successfully deliver phishing e-mails.

To work around this issue, you should use an SMTP relay service, like Sendgrid, JangoSMTP, or Mandrill. Publicly available e-mail services, like Gmail, Hotmail, and Yahoo should not be used because they enforce the highest level of security and will most likely blacklist any e-mail that appears to be spam. Regardless of the provider you choose, always send yourself the phishing emails first to verify they get delivered with a low or zero spam rating to increase your chance of success.

Phishing Tip #5: Capture credentials.

If you intend to use a social engineering assessment to promote security awareness, you should use Metasploit Pro's phishing campaign to launch a spoofed website to capture credentials. Unfortunately, nothing affects change faster than stolen credentials.

The phishing campaign is preconfigured with the components that you will need to create the phishing e-mail, spoofed page, and redirect page. After you set up and launch the phishing campaign, you can observe the campaign findings in real-time. From the real-time findings, you can easily identify the human targets that have submitted their credentials and actually view the information that they have submitted.

Due to the open nature of spoofed page content, Metasploit Pro does not have the ability to hide credentials in the Social Engineering Campaigns Details report. Therefore, due to the sensitive nature of this content, the form submission content is not automatically included in the report. If you choose to create a custom report outside of Metasploit Pro, and opt to include the collected form submission content, please be sure to obfuscate a portion of the data - especially if you are showing sensitive data like passwords or credit card numbers.

Phishing Tip #6: Spoof the hover text.

The easiest way to identify a phishing e-mail is by hovering over the links embedded in the e-mail. To make the phishing e-mail more authentic looking, you should use the spoof hover text to URL option to modify the hover text. This option is available through the Link to web page attribute and changes the URL that displays in the hover text to any URL you want to use.

For example, if your Metasploit Pro instance runs on a web server that does not point to a DNS server, your web server URL will be something like http://1.2.3.4/blue123. If this is the case, you will want to change the hover text to display a URL that looks like it directs to a real web page, like http://www.rapid7.com.

USB Baiting

If you’ve ever been in an office environment, you may have noticed random USB keys scattered around. If these USB keys are left next to the copy machine or coffee machine, you may think that the owner has misplaced the key. So, your first instinct may be to install the USB key to examine its contents in order to identify the owner.

When you view the contents of the USB key, you may see a file that is aptly named to get you to open it. For example, you may be more likely to open a file name like “Joe_Resume.pdf” because it may contain useful, personal information about the owner of the USB key. Unfortunately, these files are usually not as innocuous as they seem. Opening one of these files can install malicious code onto your computer and give an attacker access to your system.

USB baiting, or a USB key drop, uses thumb drives to deliver malicious payloads and heavily relies on human curiousity to be successful. Most baiting schemes require that you have access to the comany’s office facilities, which may require you to utilize some creative techniques in order to get through the front door. For example, you may need to dress up like someone from technical support or you may spend some time building a relationship with someone in the company.

During a social engineering penetration test, you should leverage USB key drops to raise security awareness, ensure adherence to security procedures, and improve defense strategies within an organization.

Aside from phishing, one of the other major capabilities of Metasploit Pro is the ability to generate and download a malicious file, such as an executable or an infected file, that can be placed onto a USB key. You can create a malicious file, such as a PDF that contains the Adobe Cooltype exploit, with the portable file component. After you create the malicious file, you will need to download the file, save it to a USB key, and drop the key off in a high traffic area.

Now that you have a general overview of how baiting works, let’s go over some tips that will help you set up successful baits.

USB Baiting Tip #1: Carefully research and plan the attack.

As with any other penetration test, research and planning play a vital role in setting up a successful USB key drop. USB key drops are different from standard phishing attacks because they require you to physically access an unfamiliar location and attack systems with possibly very little reconnaissance. Therefore, two of the most important elements you should research are the location and the potential target systems.

For a USB key drop to be successful, you need to identify an area in your targeted location that gets the most traffic. A high traffic area will most likely yield a higher possibility that someone will pick up a USB key and install it onto their system. Additionally, if you do not have direct access to the targeted location, you may need to create a back story to gain entry into the location. For example, you may want to pretend to be part of a maintenance crew or delivery service, which may require you to obtain the appropriate uniform and props to play the role.

When researching the location, you will need to ask yourself questions like:

“How will I get in?”

“What’s my story for being there?”

“Where are the high traffic areas located?”

“Who might I encounter?”

Answering questions like these will help you prepare and plan for a USB key drop.

Since you cannot control who picks up the USB key, you do not know if their system will be vulnerable to the exploit on the USB key. Therefore, it is important that you gather as much information as you can about the systems within the organization so that you can choose the most relevant and effective exploits. For example, if you know that most systems run Windows, you can tailor your attack to use Windows only exploits. Or if you know that most systems have Adobe Reader, you can use PDFs to deliver your exploits.

With extensive research, you can build an effective and strategic plan of attack that will provide clear insight into the organization.

USB Baiting Tip #2: Use descriptive and enticing file names.

When someone finds a USB key, their natural inclination may be to insert the USB key to find the owner or to view the contents of the drive. Therefore, you should always use file names that indicate that the file contains personal or confidential information. For example, a file name like “ContactInfo.pdf” or “payroll.exe” will be more likely to lure someone into opening it.

Malicious Attachments

A malicious attachment is a file format exploit or executable file that is e-mailed to a human target. The e-mail appears to come from a trusted source and always contains an attachment that must urgently be downloaded.

Some of the most prolific social engineering attacks have started with the innocuous act of the opening an e-mail attachment. The attached file contains an exploit that delivers a malicious payload to the target's system, which in turn, makes the system vulnerable to viruses, malware, spyware, and trojans. In some cases, the attack creates a chain of events that can compromise the entire network.

Most likely, the recipient was completely unaware that the attachment was harmful because the e-mail appeared to originate from a familiar source. Similarly to phishing attacks, the attacker has manipulated the recipient into believing that the e-mail was authentic and that the attached file was trustworthy. For example, personalized corporate e-mails about stock options and health insurance are more likely to lure someone into reading them and downloading any files attached to them than generic e-mails about sales figures.

As a social engineering penetration tester, you need to identify the potential risks that malicious attachments pose to an organization and provide solutions that can mitigate those risks. It is important to provide employees with the necessary skills to reduce the risk that they pose to an organization and to identify the most pervasive vulnerabilities that the organization needs to address.

Now that you have a general overview of malicious attachments, let's go over some tips that will help create malicious e-mails and attachments.

Malicious Attachments Tip #1: Craft a convincing and legitimate looking e-mail.

To appeal to a human target's sense of trust and curiosity, you need to create an e-mail that not only looks legitimate, but contains information that is of interest to the human target.

Any e-mail you create should use the same logo, font, and colors that the real one would. If you are spoofing a corporate e-mail, you should use a real e-mail as a model so that you can accurately recreate the exact header, footer, and signature. These elements provide visual cues to the target that the e-mail comes from a trusted and familiar source.

In order to convince the human target to actually open an attachment, you need to persuade them that the attachment contains information that they absolutely need to view. Typically, people will want to view any information that they think will impact them directly. For example, an e-mail about annual bonuses with an attachment named 2013_bonus_plan.pdf will probably get more views than an e-mail about a new corporate handbook.

Malicious Attachments Tip #2: Use a common file format exploit.

Depending on the information you have gathered about the target systems, you should use exploits that are delivered using a common file format type. For example, most Windows systems in an corporate environment will have Microsoft Windows or Adobe Reader. Therefore, when choosing a file format exploit, you should factor in the likelihood that the target will have the necessary software to open the file.

Malicious Attachments Tip #3: Zip attached files.

Most e-mail services will not deliver an executable file attached directly to an e-mail. So, if you want to attach an executable file to an e-mail, you should always send the file in a Zip file. This reduces the possibility of the attachment being flagged as a malicious file.