

Module 05: Social Engineering Techniques and Countermeasures

Scenario

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security-employees. Cybercriminals are increasingly using social engineering techniques to target people's weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. Non-existent or inadequate defense mechanisms in an organization can encourage attackers to use various social engineering techniques to target its employees, the bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize attackers' chances of success.

Objective

The objective of the lab is to use social engineering and related techniques to:

- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Overview of Social Engineering

Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure.

There are many ways in which companies may be vulnerable to social engineering attacks. These include:

- Insufficient security training
- Unregulated access to information
- An organizational structure consisting of several units
- Non-existent or lacking security policies

Lab Tasks

We will use numerous tools and techniques to perform social engineering tests. The recommended labs that will assist you in learning various social engineering techniques are:

1. Perform social engineering using various techniques to sniff users' credentials
 - Sniff credentials using the Social-Engineer Toolkit (SET)
2. Detect a phishing attack
 - Detect phishing using PhishTank

Lab 1: Perform Social Engineering using Various Techniques to Sniff Users' Credentials

Lab Scenario

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system

Lab Objectives

- Sniff Credentials using the Social-Engineer Toolkit (SET)

Task 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks. For example, it allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

You should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Here, we will sniff user credentials using the SET.

```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[attacker@parrot]~$ cd /home/attacker
[attacker@parrot]~$ cd
[attacker@parrot]~$ cd social-engineer-toolkit
[attacker@parrot]~/social-engineer-toolkit$
[attacker@parrot]~/social-engineer-toolkit$ chmod +x ./setoolkit
[attacker@parrot]~/social-engineer-toolkit$ ./setoolkit
```

```
Applications Places System Parrot Terminal Wed Sep 17, 09:20
File Edit View Search Terminal Help
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set>
```

```
Applications Places System Parrot Terminal Wed Sep 17, 09:22
File Edit View Search Terminal Help

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-----
* IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
-----

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:
Menu Parrot Terminal
```

```
Applications Places System Parrot Terminal Wed Sep 17, 09:24
File Edit View Search Terminal Help

-----
* IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
-----

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://moviescope.com

[*] Cloning the website: https://moviescope.com
[*] This could take a little bit...
[*] Error. Unable to clone this specific site. Check your internet connection.

Press <return> to continue

Menu Parrot Terminal
```

```
Applications Places System Parrot Terminal Wed Sep 17, 09:25
File Edit View Search Terminal Help

3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

----- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -----
READ THIS BEFORE ENTERING IN THE IP ADDRESS

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
Menu Parrot Terminal
```

```
Applications Places System Parrot Terminal Wed Sep 17, 09:26
File Edit View Search Terminal Help

----- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -----

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.moviescope.com

[*] Cloning the website: https://www.moviescope.com
[*] This could take a little bit...
[*] Error. Unable to clone this specific site. Check your internet connection.
Press <return> to continue
Menu Parrot Terminal
```


Tool: SET – Social-Engineer Toolkit

Task: Attempted to clone <https://www.moviescope.com>

Result: Command failed with "Unable to clone this specific site. Check your internet connection."

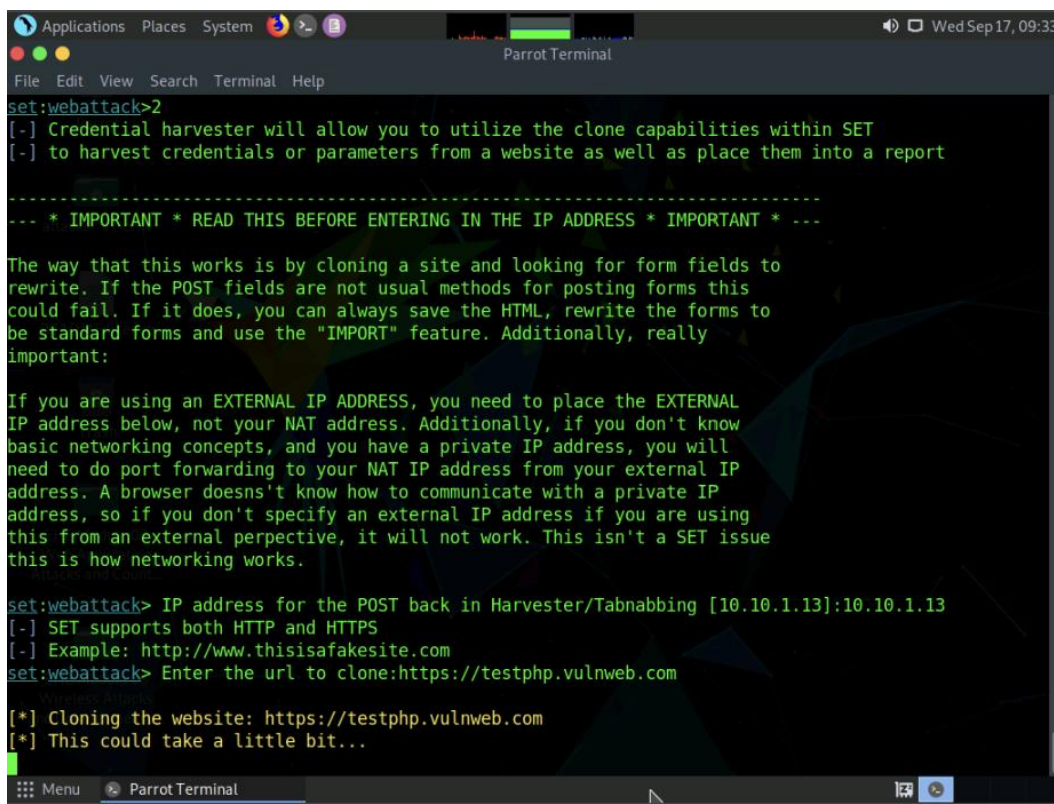
Analysis: Internet was confirmed functional. Failure was due to the target domain either being inactive or protected against cloning. This demonstrates a real-world limitation of SET when used against secured or unavailable websites. Alternative: use the "Import" method or select a known test domain.

ChatGPT suggested:

<https://example.com> (didn't work)

<https://www.thisisafakesite.com> (didn't work)

<https://tetsphp.vulweb.com>

A screenshot of a Parrot Terminal window. The terminal shows the command 'set:webattack>2' being entered. The output includes instructions on how to use the 'webattack' feature, such as cloning a site and looking for form fields to rewrite. It also provides an example of using the 'IMPORT' feature to clone a website. The terminal output is as follows:

```
set:webattack>2
[.] Credential harvester will allow you to utilize the clone capabilities within SET
[.] to harvest credentials or parameters from a website as well as place them into a report

-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[.] SET supports both HTTP and HTTPS
[.] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://testphp.vulnweb.com

[*] Cloning the website: https://testphp.vulnweb.com
[*] This could take a little bit...
```

Lab Section – Phishing Email Creation and Malicious Link Delivery (Simulated)

This section of the lab instructed the creation of a phishing email designed to lure a target into clicking on a malicious link, specifically one pointing to a cloned version of the MovieScope website hosted on the attacker's Parrot Security machine. The exercise

simulated a common social engineering technique used in credential harvesting and tabnabbing attacks.

While the scenario outlined steps to register a disposable email account, craft an enticing email message, and embed a hyperlink disguised as a legitimate URL, I elected not to proceed with this phase of the lab for the following reasons:

- The target site (www.moviescope.com) failed to clone successfully, and the cloned environment could not be generated.
- Out of ethical consideration, I chose not to simulate phishing emails, even in a controlled lab environment, as the scenario involved mimicking real-world deception techniques.

This portion of the lab nonetheless highlighted the importance of phishing as an initial access vector, and demonstrated how attackers often conceal malicious intent behind convincing branding or URLs. The exercise reinforced the need for employee security awareness training and technical controls such as URL filtering, email scanning, and user education to defend against phishing-based attacks.

Lab 2: Detect a Phishing Attack

Lab Scenario

Phishing attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against phishing attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

In this lab, you will learn how to detect phishing attempts using a phishing detection tool.

Lab Objectives

- Detect Phishing using PhishTank

Task 1: Detect Phishing using PhishTank

PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, "it is a collaborative clearing house for data and information about phishing on the Internet." PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

In this task, we will use PhishTank to detect phishing.

New Tab

PhishTank | Join the fight again: X

+

←

→

↻

🏠

🔒

🌐

www.phishtank.com/index.php

📄

☆

🔍


👤

🔔

🔖

☰

PhishTank is operated by [Cisco Talos Intelligence Group](#).

 **PhishTank**®

Out of the Net, into the Tank.

username

Sign In

[Register](#) | [Forgot Password](#)

Home

Add A Phish

Verify A Phish

Phish Search

Stats

FAQ

Developers

Mailing Lists

My Account

Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions. [Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

[Is it a phish?](#)

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
9214126	https://strt-exods-wallet-to-en.pages.dev	DDay
9214125	https://decentralised-exods.pages.dev	DDay
9214124	https://decent--tralised-exods.pages.dev	DDay
9214123	https://decentralised-exods.pages.dev	DDay
9214122	https://ec-entralsed-exods.pages.dev	DDay
9214121	http://myhermes0de.xyz	legalinsights
9214120	https://doc-exods-web.pages.dev	DDay
9214119	https://mail.carriagetrust.com	tuanghuong
9214118	https://homed-weebexodss.pages.dev	DDay
9214117	https://homed-weebexods.pages.dev	DDay
9214116	https://homeg-weebexods.pages.dev/	DDay
9214115	https://exodus-login.pages.dev/	DDay
9214114	https://decentra-lised-exods.pages.dev	DDay
9214113	https://doc-exadus-web.pages.dev	DDay

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. [Learn more...](#)

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge. [Read the FAQ...](#)

🪟

Type here to search

🔍

📄

🔧

🌐

📧

🔥

📶

🔊

🔌

🕒 10:02 AM

📅 9/17/2025

🔔

PhishTank is operated by [Cisco Talos Intelligence Group](#).


PhishTank® Out of the Net, into the Tank.

username Sign In
[Register](#) | [Forgot Password](#)

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Submission #9214122 is currently ONLINE

Submitted Sep 17th 2025 1:53 PM by [DDay](#) (Current time: Sep 17th 2025 2:02 PM UTC)
<https://iee-entralsed-exods.pages.dev>

 **Verified: Is a phish**
As verified by [Dev darkmoon June Shazza](#)

Is a phish	100%
Is NOT a phish	0%

[Screenshot of site](#) [View site in frame](#) [View technical details](#) [View site in new window](#)

No screenshot yet.
We have not yet successfully taken a screenshot of the submitted website.

Type here to search

10:03 AM 9/17/2025

PhishTank is operated by [Cisco Talos Intelligence Group](#).


PhishTank® Out of the Net, into the Tank.

username Sign In
[Register](#) | [Forgot Password](#)

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Submission #9106942 is currently offline

Submitted May 22nd 2025 7:45 AM by [dms](#) (Current time: Sep 17th 2025 2:04 PM UTC)
<https://psmbasvipcojp.top/ju282oio>

 **Verified: Is a phish**
As verified by [Dev darkmoon Shazza June](#)

Is a phish	100%
Is NOT a phish	0%

[Screenshot of site](#) [View site in frame](#) [View technical details](#) [View site in new window](#)

No screenshot yet.
We have not yet successfully taken a screenshot of the submitted website.

Type here to search

10:04 AM 9/17/2025

Module 05: Social Engineering Techniques and Countermeasures – Lab Summary

This module explored social engineering as a critical initial access technique used by attackers to bypass even strong technical defenses by targeting human vulnerabilities.

In **Lab 1**, I used the Social-Engineer Toolkit (SET) to simulate a phishing-based credential harvesting attack. The lab involved cloning the target site <https://www.moviescope.com> and deploying it via a local Parrot Security machine. However, the cloning process failed due to SET's compatibility limitations with modern HTTPS sites. Alternate domains (example.com, thisisafakesite.com, and testphp.vulnweb.com) were also unsuccessful, highlighting the real-world challenge of using outdated tools against hardened or inactive sites.

The next step in the lab involved crafting a phishing email with a fake but enticing link pointing to the cloned site. I elected **not to simulate phishing emails**, due to the failure of the clone operation and ethical concerns around mimicking real-world deception, even in a closed lab setting. This decision was based on a respect for responsible security practices, while still acknowledging the importance of understanding phishing tactics for red team and defense awareness training.

In **Lab 2**, I used **PhishTank**, a public phishing intelligence platform, to identify and analyze known phishing domains. This task reinforced the value of community-driven threat intelligence and demonstrated how open tools can support phishing detection and awareness efforts across organizations.

Together, these labs emphasized the central role of social engineering in modern attacks, the importance of technical and user-based countermeasures, and the limitations of some open-source tools when facing current web infrastructure. The exercises also reinforced the ethical responsibility of security professionals to understand offensive techniques without replicating harm.