

# MODULE 09 SOCIAL ENGINEERING LAB SCREENSHOTS

---

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE  
Course Code: T44-17520

## Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3>
2. <https://eccouncil.learnondemand.net/Lab/Launch/55228?AssignmentId=1340522&lang=>

## Username on EC-Council System

1. 2110886@uj.edu.sa

# Lab 01

The screenshot shows a Linux desktop environment with a Parrot Security theme. A terminal window titled '/setoolkit - Parrot Terminal' is open, displaying the Social-Engineer Toolkit (SET) menu. The menu includes options like 'Pen-source application.', 'READMED', 'CEHv12 Mo', 'Hacking', 'Server', and 'Applications'. The terminal also shows a 'Do you agree to the terms of service [y/n]:' prompt.

The task list on the right side of the screen lists the following steps:

7. Now, type `/setoolkit` and press `Enter` to launch Social-Engineer Toolkit.  
If a 'Do you agree to the terms of service [y/n]' question appears, enter `y` and press `Enter`.
8. The SET menu appears, as shown in the screenshot.
9. A list of options for Social-Engineering Attacks appears: type `2` and press `Enter` to choose Website Attack Vectors.
10. A list of options in Website Attack Vectors appears: type `3` and press `Enter` to choose Credential Harvester Attack Method.

The desktop interface includes a taskbar at the bottom with various icons and a system tray showing the date and time (Sun Mar 31, 08:43).

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Parrot Security Sun Mar 31, 08:44

/setoolkit - Parrot Terminal

```

Parrot File Edit View Search Terminal Help
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
attacker's home
----- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
README.LI
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:
Tras!
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
CEHv12 Mo
address. A browser doesn't know how to communicate with a private IP
Hacking' Server
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.
CEHv12 Mo set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]
Hacking' Applications

```

35 Minutes Remaining

Instructions Resources Help 100%

Social Engineering

11. Type 2 and press Enter to choose Site Cloner from the menu.

12. Type the IP address of the local machine (10.10.1.13) in the prompt for 'IP address for the POST back in Harvester/Tabnabbing' and press Enter.

0% Tasks Complete

Next: Lab 2: Detect a... >

31°C

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Parrot Security 33 Minutes Remaining

/setoolkit - Parrot Terminal

```

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:
Tras!
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:http://www.moviescope.com
[*] Cloning the website: http://www.moviescope.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, th
is captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

Instructions Resources Help 100%

Social Engineering

12. Type the IP address of the local machine (10.10.1.13) in the prompt for 'IP address for the POST back in Harvester/Tabnabbing' and press Enter.

In this case, we are targeting the Parrot Security machine (IP address: 10.10.1.13).

13. Now, you will be prompted for the URL to cloned: type the desired URL in 'Enter the url to clone' and press Enter. In this task, we will clone the URL http://www.moviescope.com.

You can clone any URL of your choice.

0% Tasks Complete

Next: Lab 2: Detect a... >

31°C

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Inbox (2,290) - laaraa56@gmail.com - Gmail - Mozilla Firefox

Parrot Security Sun Mar 31, 08:57

New Message

Recipients: http://www.moviescope.com/avail\_benefits:

Send

Compose

Inbox 2,290 Primary

Starred Snoozed Important Sent Drafts Categories

Labels Notes

Google 2 Google AlienVault OTX جو لسا جو لسا Discord

1–50 of 2,638

Social Engineering 22 Minutes Remaining

Instructions Resources Help 100%

21. The fake URL should appear in the message body, as shown in the screenshot.

22. Verify that the fake URL is linked to the correct cloned site; in Gmail, click the link; the actual URL will be displayed in a 'Go to link' pop-up. Once verified, send the email to the intended user.

23. Click Windows 11 to switch to the Windows 11 machine and click [Ctrl+Alt+Delete]. By default, Admin user profile is selected, click [T] Pa\$\$wOrD paste the password in the Password field and press Enter to login.

Alternatively, you can also click Pa\$\$wOrD under Windows 11 machine thumbnail in 0% Tasks Complete

Next: Lab 2: Detect a... >

31°C ملمس

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

from lara - laraalof56@gmail.com +

Gmail

البحث في البريد

البريد الوارد 1,521

المحكمة بخدمة المجلة أقرير المرسل المسوّدات البريد

الصيغات

البريد الوارد 1,521

المحكمة بخدمة المجلة أقرير المرسل المسوّدات البريد

الصيغات

Waiting for mail.google.com...

Social Engineering 19 Minutes Remaining

Instructions Resources Help 100%

25. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of www.moviescope.com.

26. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the Username and Password and clicks Login, he/she will be redirected to the legitimate MovieScope login page. Note the different URLs in the browser address bar for the cloned and real sites.

16% Tasks Complete

< Previous Next: Lab 2: Detect a... >

31°C ملمس

Social Engineering - Google Chrome

labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

from lara - laralof56@gmail.co Login - MovieScope

Not secure | 10.10.1.13

MOVIESCOPE

Home Features Trailers Photos Blog Contacts

Login

Username: sam

Password: ....

Login

If save credentials notification appears, click **Don't Save**.

Social Engineering

16 Minutes Remaining

Instructions Resources Help

1. a new tab opens up, and he/she will be presented with a replica of [www.moviescope.com](http://www.moviescope.com).

2. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.

16% Tasks Complete

Next: Lab 2: Detect a... >

31°C

Social Engineering - Google Chrome

labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

from lara - laralof56@gmail.co Login - MovieScope

Not secure | moviescope.com

MOVIESCOPE

Home Features Trailers Photos Blog Contacts

Login

Username:

Password:

Login

If save credentials notification appears, click **Don't Save**.

Social Engineering

16 Minutes Remaining

Instructions Resources Help

1. a new tab opens up, and he/she will be presented with a replica of [www.moviescope.com](http://www.moviescope.com).

2. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.

16% Tasks Complete

< Previous Next: Lab 2: Detect a... >

31°C

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Parrot Security File Edit View Search Terminal Help ./setoolkit - Parrot Terminal

[\*] The Social-Engineer Toolkit Credential Harvester Attack  
[\*] Credential Harvester is running on port 80  
[\*] Information will be displayed to you as it arrives below:

```
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET / HTTP/1.1" 200 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:02:45] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:03:05] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.11 - - [31/Mar/2024 09:03:25] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3Mj0zOTdkZH5l0cnJ+BtsUZt5M/WlqLFqT5uNaq6G+46A4bz6/sMl
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdARJUub9rbp0xjNNNjxtMLiRWMrtrRuIi9aE3DBG1DcnOGGcP002LAX9axRe6vMQj2F3f3Aw
SkugaAa3gX7Rfq070LdpacuhngPphrm03j16uMcylVYtnt+iQJOBgU=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=lara
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

10.10.1.11 - - [31/Mar/2024 09:03:33] "POST /index.html HTTP/1.1" 302 -

Social Engineering 15 Minutes Remaining Instructions Resources Help 100%

27. Now, click Parrot Security to switch back to the Parrot Security machine and switch to the terminal window.  
28. As soon as the victim types in his/her Username and Password and clicks Login, SET extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.  
29. Scroll down to find Username and Password displayed in plain text, as shown in the screenshot.



16% Tasks Complete

< Previous Next: Lab 2: Detect a... >

31°C 1 1

## Lab2:

Social Engineering - Google Chrome

from lara - laralof56@gmail.com Netcraft Mobile Apps, Email and labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

Netcraft.com/apps-extensions/

## Browser Protection

Netcraft's free browser extension provides real-time enhanced protection from malicious sites defending you from phishing, fake shops, and malicious scripts such as JavaScript skimmers and cryptocurrency miners.

The browser extension works with all major browsers, including Chrome, Firefox, Edge, and Opera.

[LEARN MORE](#)



Social Engineering  
13 Minutes Remaining

Instructions Resources Help Search 100%

Click Accept in the cookie notification in the lower section of the browser.



Protect yourself from cybercrime  
Use our Netcraft extension to ensure you don't get tricked by criminals. It's based on real-life incidents that protect billions of people around the world from phishing, fake apps, and other malicious threats.

MOBILE  
Install app for Android & iOS & Amazon of mobile devices

4. Scroll-down and click Find out more button under BROWSER option on the webpage.



BROWSER  
Netcraft browser extension for Chrome & Firefox & Edge & Opera

Find out more  
21% Tasks Complete

< Previous Next: Lab 3: Audit... >

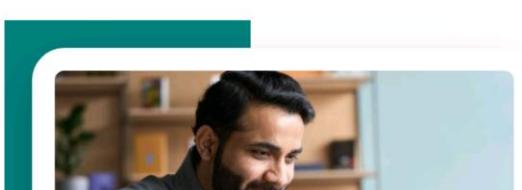
Social Engineering - Google Chrome

from lara - laralof56@gmail.com netcraft.com/apps-extensions/browser-extension/ labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

Download the extension today

The browser extension can be downloaded for free from your browser's store by clicking on an icon below



Social Engineering  
12 Minutes Remaining

Instructions Resources Help Search 100%

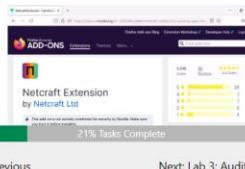
6. Click ellipsis icon (≡) again to close the menu.

7. You will be directed to the Get it now section; click the Firefox browser icon.



Get it now  
Want to protect your other platforms?  
We also have apps to help protect you from phishing for your mail and mobile

8. On the next page, click the Add to Firefox button to install the Netcraft extension.



ADD-ONS  
Netcraft Extension by Netcraft Ltd  
Add to Firefox  
21% Tasks Complete

< Previous Next: Lab 3: Audit... >

Social Engineering - Google Chrome

from lara - laraloof56@gmail.com X Netcraft Extension - Get this Ext... + labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

addons.mozilla.org/en-US/firefox/addon/netcraft-toolbar/?src=external-apps-download

Firefox Browser ADD-ONS Extensions Themes More... Log In Find add-ons

## Netcraft Extension by Netcraft Ltd

Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

You'll need Firefox to use this extension

Download Firefox and get the extension

Download file

4,454 Users 38 Reviews 4.4 Stars

5 ★ 30  
4 ★ 3  
3 ★ 1  
2 ★ 0  
1 ★ 4

Rate your experience Screenshots

8. On the next page, click the **Add to Firefox** button to install the Netcraft extension.

Social Engineering 12 Minutes Remaining Instructions Resources Help 100%

Want to protect your other platforms? We also have apps to help protect you from phishing for your mail and mobile.

8. On the next page, click the **Add to Firefox** button to install the Netcraft extension.

9. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay**.

21% Tasks Complete

Previous Next: Lab 3: Audit... >

31°C

Social Engineering - Google Chrome

from lara - laraloof56@gmail.com X Get Firefox for desktop - Mozilla + labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

mozilla.org/en-US/firefox/download/thanks/?s=direct&utm\_campaign=amo-fx-cta-1326&utm\_content=rta...

Open File - Security/Warning

Do you want to run this file?

Name: C:\Users\Admin\Downloads\Firefox Installer.exe  
Publisher: Mozilla Corporation  
Type: Application  
From: C:\Users\Admin\Downloads\Firefox Installer.exe

Run Cancel

Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

anyway" or change app recommendation settings.

Visit Support for More Details

Firefox installer.exe Show all

8. On the next page, click the **Add to Firefox** button to install the Netcraft extension.

9. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay**.

10. After the installation finishes, you may be asked to restart the browser. If so, click **Restart Now**.

11. If **Netcraft Extension has been added to Firefox** notification appears, click **Okay**.

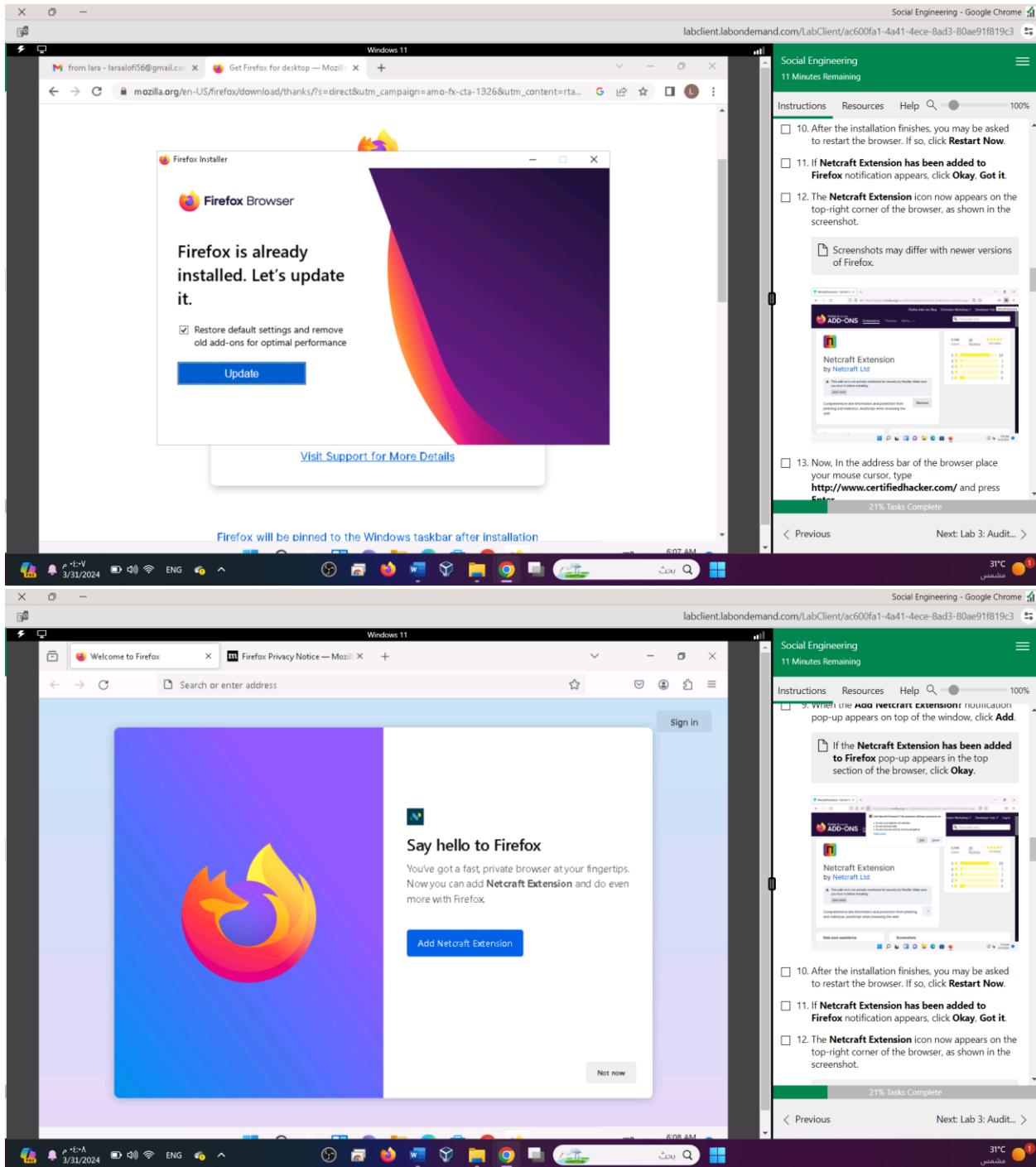
12. The **Netcraft Extension** icon now appears on the top-right corner of the browser, as shown in the screenshot.

Screenshots may differ with newer versions of firefox.

21% Tasks Complete

Previous Next: Lab 3: Audit... >

31°C



Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

Certified Hacker https://www.certifiedhacker.com

Site Report

Country: US Site rank: 10,752  
First seen: January 2018 Host: Unified Layer

Report malicious URL:

The URL of the site: https://www.certifiedhacker.com/

Add a reason

Your email address (to receive updates): you@example.com

Submit Report

netcraft California High School

Welcome to our website

Corporate learning resources have never been closer to the rest of the world. Online communications and advances in international transport mean local institutions and industries can easily participate in world markets. Our passion for encouraging other cultures and countries has earned the reputation of being best.

Vision: This innovative thinking is reflected in the way we teach and learn. Our education system encourages inventive thinking and teaching techniques that reach far

Copyright © 2011 - Certified Hacker - All rights reserved.

Social Engineering 21 Minutes Remaining

Instructions Resources Help 100%

your mouse cursor, type http://www.certifiedhacker.com/ and press Enter.

14. The certifiedhacker.com webpage appears. Click the Netcraft Extension icon in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as Risk Rating, Site rank, First seen, and Host about the searched website.

certifiedhacker.com

31% Tasks Complete

Previous Next: Lab 3: Audit... >

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

Windows 11

Certified Hacker Site report for https://www.certifiedhacker.com

netcraft

Site rank 10752 Primary language English

Description Not Present

**Network**

Site	https://www.certifiedhacker.com	Domain	certifiedhacker.com
Netblock Owner	Unified Layer	Nameserver	ns1.bluehost.com
Hosting company	Newfold Digital	Domain registrar	networksolutions.com
Hosting country	US	Nameserver organisation	whois.domain.com
IPv4 address	162.241.218.11	Organisation	5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US
IPv4 autonomous systems	AS46606	DNS admin	dnsadmin@box5331.bluehost.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Unknown

Transferring data from c.tile.openstreetmap.org... box5331.bluehost.com

Social Engineering 20 Minutes Remaining

Instructions Resources Help 100%

If a Site information not available pop-up appears, ignore it.

Site report for http://www.certifiedhacker.com

Background

Network

Commercial entities (.com)

21% Tasks Complete

Previous Next: Lab 3: Audit... >

Social Engineering - Google Chrome

labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

**netcraft**

Legend:

- Advertised country
- Multilaterated location

Connecting to csp.netcraft.com...

Social Engineering

20 Minutes Remaining

Instructions Resources Help Search 100%

Network

IP Geolocation

History

21% Tasks Complete

Previous Next: Lab 3: Audit... >

31°C

Social Engineering - Google Chrome

labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

**Certified Hacker**

Site report for https://www.certifiedhacker.com

Server Not Found

https://smbc.ctad-co.com/m

Hmm. We're having trouble finding that site.

We can't connect to the server at smbctad-co.com.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Try Again

Enter.

Here, for demonstration purposes, we are using <https://smbc.ctad-co.com/m> phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

19. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click [Visit anyway](#) to browse it; otherwise, click [Report mistake](#) to report an incorrectly blocked URL.

If you are getting an error in opening the website (<https://smbc.ctad-co.com/m>), try to open other phishing website.

OR

You will get a **Suspected Phishing** page in the **Firefox** browser.

If you get **Secure Connection Failed** webpage, then use some other phishing website to get the result, as shown in the screenshot.

34% Tasks Complete

Previous Next: Lab 3: Audit... >

31°C

## Lab 2 -task 2

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

PhishTank is operated by Cisco Talos Intelligence Group.

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:

http:// Is it a phish?

Recent Submissions

You can help! Sign In or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
8511360	https://osf.contraxhost.com/Portal/Documents/Docu...	cleanmx ✓
8511359	https://resolve.cleverpal.live/	cleanmx ✓
8511357	https://dpv20.muddybots.biz/2001/Tasks>List/Index...	cleanmx ✓
8511356	https://is.gd/Ayg6t	cleanmx ✓
8511355	https://sparkworkds.com/	n0x6fb0x6fdv
8511354	https://sparkassechein.com/	n0x6fb0x6fdv
8511353	https://aktivieren-pushtan.com/de/startseite/	n0x6fb0x6fdv
8511352	https://aktivieren-pushtan.com/de/startseite	n0x6fb0x6fdv

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...

Social Engineering 16 Minutes Remaining

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

1. In the Windows 11 machine, Launch any browser, in this lab we are using Mozilla Firefox. In the address bar of the browser place your mouse cursor, type <https://www.phishtank.com> and press Enter.
2. The PhishTank webpage appears, displaying a list of phishing websites under Recent Submissions.
3. Click on any phishing website ID in the Recent Submissions list (in this case, 7486626) to view detailed information about it.
  - If a notification appears asking Would you like Firefox to save this login for phishtank.com? click Don't Save.
  - If you are redirected to the page asking captcha, enter the captcha to proceed.

34% Tasks Complete

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

PhishTank is operated by Cisco Talos Intelligence Group.

Submission #8511360 is currently ONLINE

Submitted Mar 31st 2024 1:00 PM by cleanmx (Current time: Mar 31st 2024 1:18 PM UTC)

[https://osf.contraxhost.com/Portal/Documents/Document.aspx?record\\_id=35744567](https://osf.contraxhost.com/Portal/Documents/Document.aspx?record_id=35744567)

Sign in or Register to verify this submission. This submission needs more votes to be confirmed or denied.

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.

Social Engineering 15 Minutes Remaining

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

4. If the site is a phishing site, PhishTank returns a result stating that the website "Is a phish" as shown in the screenshot.
5. Navigate back to the PhishTank home page by clicking the Back button in the top-left corner of the browser.
6. In the Found a phishing site? text field, type a

34% Tasks Complete

Windows 11

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

PhishTank

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: http://be-ride.ru/confirm Is it a phish?

Recent Submissions

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

ID	URL	Submitted by
8511360	https://osf.contraxhost.com/Portal/Documents/Docu...	cleanmx
8511359	https://resolve.cleverpath.live/	cleanmx
8511357	https://dpu20.muddyboots.biz/2001/Tasks>List/Index...	cleanmx
8511356	https://is.gd/Ayg66t	cleanmx
8511355	https://sparkworks.com/	n0x6fb0:6fdv
8511354	https://sparkassechein.com/	n0x6fb0:6fdv
8511353	https://aktivieren-pushtan.com/de/startseite/	n0x6fb0:6fdv
8511352	https://aktivieren-pushtan.com/de/startseite	n0x6fb0:6fdv
8511351	https://webde-106246.weeblysite.com/	kkalmus
8511346	https://lesskins.ru/	tuanchuong
8511345	https://whales.network/stake/	tuanchuong
8511344	https://agoravoicepodesolictar.tech	NialCottrell
8511343	https://rzeeq2l.square.site/	prodigyalabuse
8511342	http://crzeqq2l.square.site/	prodigyalabuse
8511330	http://www.ass-global.com	r3perses

See more suspected phishes...

6:19 AM

Social Engineering

14 Minutes Remaining

Instructions Resources Help

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...](#)

5. Navigate back to the PhishTank home page by clicking the Back button in the top-left corner of the browser.

6. In the Found a phishing site? text field, type a website URL to be checked for phishing (in this example, the URL entered is `be-ride.ru/confirm`). Click the Is it a phish? button.

PhishTank

Join the fight against phishing. Submit suspected phishes, verify other users' submissions, develop software with our free API.

Recent Submissions

You can help! Sign in or register to verify these suspected phishes.

6:19 AM

31°C

3/31/2024

ENG

Previous Next: Lab 3: Audit... >

Windows 11

Social Engineering - Google Chrome labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

PhishTank

Out of the Net, into the Tank.

Submission #2205890 is currently offline

Submitted Jan 2nd 2014 10:56 AM by [knack](#) (Current time: Mar 31st 2024 1:20 PM UTC)

<http://be-ride.ru/confirm/>

Verified: Is a phish

As verified by [buava eaulch](#), [NotBunnysoft](#), [phishbucker](#)

Is a phish 100%  
Is NOT a phish 0%

Screenshot of site View site in frame View technical details View site in new window

Personal Business Email address  Password  Log in

PayPal Buy Sell Transfer

Redesigned with you in mind.

6:20 AM

Social Engineering

14 Minutes Remaining

Instructions Resources Help

You can examine any website of your choice for phishing.

7. If the site is a phishing site, PhishTank returns a result stating that the website **"Is a phish"**, as shown in the screenshot.

PhishTank

Submission #2205890 is currently offline

Redesigned with you in mind.

8. This concludes the demonstration of detecting phishing using PhishTank.

34% Tasks Complete

Previous Next: Lab 3: Audit... >

31°C

3/31/2024

ENG