OPEN-SOURCE INTELLIGENCE MODULE CHALLENGE

If you have any questions, please ask them in the ""osint-module" channel, under the "Operation Chimera" category on the SBT Discord server.

If you feel you're familiar with what OSINT is, and how to gather information effectively, then you may be ready for the Challenge! We suggest you still do some of your own research using the 'Useful Links' in the training material before attempting the Challenge.
.

What will I need for this Challenge?

- Virtualbox (https://www.virtualbox.org/wiki/Downloads)
- Kali Linux VM (https://www.kali.org/downloads/)
- A Twitter account (You can use a legitimate account or a throwaway)

Challenge Brief:

Throughout the following tasks there will be a mixture of flags, which can be submitted for points.

Part One) Setup your own Tweetdeck monitoring panel. Create 3 columns to monitor for security-related activity (see my Tweetdeck blog post above). Create a fourth column which is performing the following search: #Unc4gedSq4d AND flag

Part Two) Use Google Dorks to find all pages (visible and hidden) of SecurityBlue.Team (site:"securityblue.team"). If you can't find the secret page, try taking a look at the site's Robots.txt file!

1. How many pages can you find this way?
2. What is the name of the page that features my Tweetdeck image?
3. What is the flag on the "secret" page? (Use a different Dork for this!)
4. What is the name of the first PDF result under the domain Twitter.com?

Part Three) Use The Harvester to perform OSINT reconnaissance on any domain you choose. You will be asked to submit a short report on what information was discovered, and how this could be useful to both an Attacker and a Defender..

Read to submit your Challenge? Head over to the website and click on the 'Challenge Submission' button under the OSINT module.

Part One) Tweetdeck	
What is your first custom search query? (Max points for complexity/originality, don't go simple!) **[10 Marks]**	
What is your second custom search query? (Max points for complexity/originality, don't go simple!) **[10 Marks]**	
What is your third custom search query? (Max points for complexity/originality, don't go simple!) **[10 Marks]**	
What is the flag value from entering in the query provided in the training PDF? **[10 Marks]**	
Part Two) Google Dorks	
How many pages did you find for SecurityBlue.Team using the Dork Query: site:"securityblue.team" -site:"www.securityblue.team"? **[10 Marks]**	
What is the title of the page that has my Tweetdeck image? **[10 Marks]**	
What is the flag on the "secret" page? (Can't find it with Dorks? Look into what Robots.txt is!) **[10 Marks]**	
What is the name of the first PDF result under the domain Twitter.com? **[10 Marks]**	
Part Three) The Harvester	
What domain did you target using The Harvester? **[10 Marks]**	
Run scans using AT LEAST two different data sources (google, linkedin, bing, etc). Provide a short report on what information was obtained from the scan, and how this information could be useful to both an Attacker and Defender **[30 Marks]**	