OS

OPERATION CHIMERA

OPEN-SOURCE INTELLIGENCE MODULE // SECURITY BLUE TEAM

CONTENTS

This information has been gathered from public sources and combined with my own knowledge and experiences for the purpose of Operation Chimera, an online, live blue-team training operation conducted by myself under the alias Known Divide, for the SecurityBlueTeam community.

Useful Links:
[1] https://securitytrails.com/blog/top-20-intel-tools
[2] https://www.sans.org/course/open-source-intelligence-gathering
[3] https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it

If you've enjoyed this event, please consider donating whatever you can spare to buy me pizza, coffee, and help fund future events! (even £5/$5 will make a huge difference, and it only takes a few seconds).

PayPal.Me

https://paypal.me/KDMentoring

OPERATION CHIMERA – OSINT

This document is not 100% finished and will be updated within the next 24 hours. Thank you for your patience.

This module is designed to give a look into the world of Open-Source Intelligence gathering and utilization. It is aimed at individuals who are moving in to Cyber, so the material is aimed at an entry-level student. We strongly encourage further reading using the provided sources and any that you find yourself. Want to talk to other hackers about this specific module? Join the discussion in the "osint-module" channel within the "Operation Chimera" category in the SBT Discord server. There is also a Chimera mega-thread on Reddit. Please make use of this to ask questions and talk to other participants!

WHAT IS OPEN-SOURCE INTELLIGENCE?

"Open source intelligence (OSINT) is information collected from public sources such as those available on the Internet, although the term isn't strictly limited to the internet, but rather means all publicly available sources."

WHY IS IT USEFUL?

Information gained from OSINT sources can be useful in many different circumstances. Whether that's keeping up to date with the latest vulnerability releases and exploitation activity, tracking employees responsible use of social media in regard to their working lives, or using threat exchanges to check and share malicious IOCs, OSINT is a key aspect of cyber defense, and utilizing this freely available information is crucial. OSINT is also used by law enforcement agencies and governments to profile and track the activity of criminals and individuals of interest.

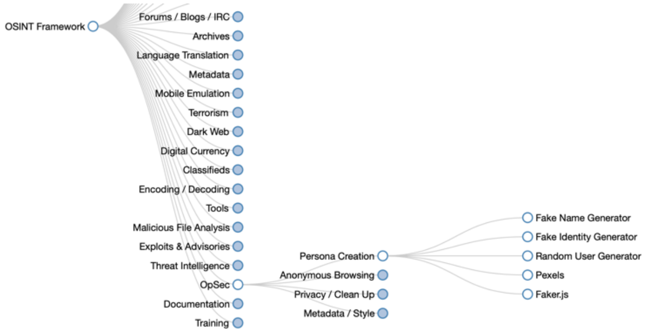
ASSOCIATED ROLES

The below roles generally contain work that includes utilizing Open-Source Intelligence for defensive cyber purposes:

- **Tier One SOC Analyst** (Junior Security Analyst)
  OSINT is used to perform searches on potentially malicious IPs, domains, and other IOCs. By checking threat exchanges, reputation reports can help investigations.
- **Tier Two SOC Analyst** (Security Analyst)
  OSINT is used to connect with organizations and groups that share not only malicious IOCs, but also defensive techniques, such as custom SIEM and IDS rules to help boost cyber defences.
- **Threat Intelligence Analyst**
  Using OSINT sources to keep up to date with the latest security news, including malicious campaigns, vulnerability releases, and exploitation activity.
- **Vulnerability Analyst**
  Using OSINT sources to keep up to date with the latest security news, including malicious campaigns, vulnerability releases, and exploitation activity.

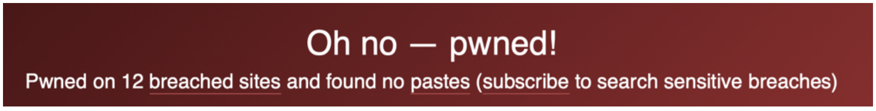
RECOMMENDED OSINT SOURCES

OSINT Framework: This web application is a hub for hundreds of OSINT sources, and is easily sorted so you can find the tool that you need quickly. Say I wanted to create a fake persona so I could launch some social-engineering attacks during a Red Team exercise at my company. By opening the OpSec arm, and then Persona Creation, I'm provided with 5 links to online tools that can help me with the task I'm trying to complete.



I strongly suggest you check out this tool and see what interesting sites and tools you can find from it. https://www.osintframework.com

HaveIBeenPwned: This collection of public data breaches has been combined and allows users to enter their email addresses to see if they have been mentioned in any breaches. This is the result of an old email address I have, that I now use as a phishing honeypot:



Oh no — pwned!

Pwned on 12 breached sites and found no pastes (subscribe to search sensitive breaches)

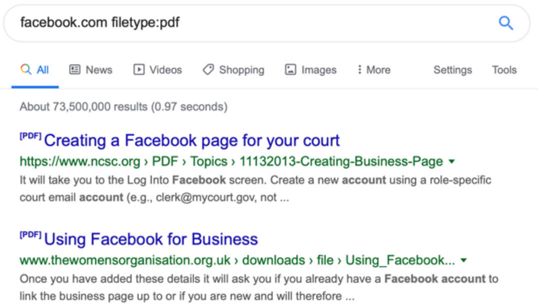
You can reverse this, and enter in the email address of a target, and see if they have been spotted in a breach. From there, you could try find access to a dump of the breach and see if their email was leaked with a password, or other information which could be used to conduct social engineering attacks (make sure this is in scope of your threat simulation engagement). Try it out yourself at https://haveibeenpwned.com (If you've been pwned, might be time to change your passwords!)

Maltego: Section Coming Soon!

Google Dorks: Google is pretty helpful in general, but Google Dorks are little hacks where we use special arguments in a normal Google query, to find specific information. Real-world examples of using Dorks include:

- Retrieving files from domains to analyze them for internal system leaked information, and for use in creating targeted password wordlists.
- Finding hidden webpages and login portals.
- Subdomain enumeration
- And more!

Dorks come in the format **operator:keyword**, an example of this would be **filetype:pdf**. So let's see what PDFs we can find, that have the keyword Facebook, using the complete query **Facebook.com filetype:pdf**



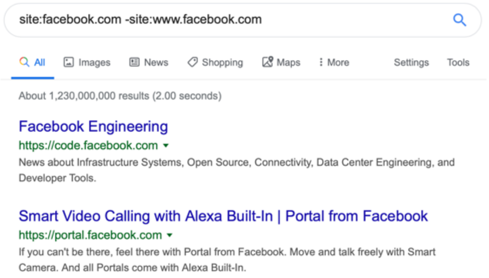
facebook.com filetype:pdf

About 73,500,000 results (0.97 seconds)

[PDF] Creating a Facebook page for your court
https://www.ncsc.org › PDF › Topics › 11132013-Creating-Business-Page
It will take you to the Log Into **Facebook** screen. Create a new **account** using a role-specific court email **account** (e.g., clerk@mycourt.gov, not ...

[PDF] Using Facebook for Business
www.thewomensorganisation.org.uk › downloads › file › Using_Facebook...
Once you have added these details it will ask you if you already have a **Facebook account** to link the business page up to or if you are new and will therefore ...

Now let's see how Dorks can be used to enumerate all subdomains of a domain, for passive reconnaissance purposes. For this, we will use Facebook again as the example, with the following query:
site:Facebook.com -site:wwwFacebook.com
(Look for sites that include Facebook.com) (but NOT www.Facebook.com)



site:facebook.com -site:www.facebook.com

About 1,230,000,000 results (2.00 seconds)

Facebook Engineering
https://code.facebook.com
News about Infrastructure Systems, Open Source, Connectivity, Data Center Engineering, and Developer Tools.

Smart Video Calling with Alexa Built-In | Portal from Facebook
https://portal.facebook.com
If you can't be there, feel there with Portal from Facebook. Move and talk freely with Smart Camera. And all Portals come with Alexa Built-In.

Here we can see the list begins with two subdomains, code.facebook.com, and portal.facebook.com. We have successfully enumerated subdomains using Google Dorks! Have a go yourself with any Domain you choose.
Google Dorks are very useful, so take a look at this list of common Dorks and use them yourself to really understand how they work, and how they could be used for defensive or offensive security.
https://securitytrails.com/blog/google-hacking-techniques

Tweetdeck: Twitter is an incredible source of information. Read my personal post about using Twitter and Tweetdeck for Defensive Monitoring and Threat Intelligence -
https://www.reddit.com/r/SecurityBlueTeam/comments/cmca63/using_tweetdeck_for_defensive_monitoring_threat/
You'll be using this in the OSINT Challenge, so make sure you've read this, and understand how to set it up using a throw-away Twitter account.

COUNTER-OSINT

In such a digital world, it's hard to maintain total privacy, especially with the popularity of social-media, and social expectations to share everything you do. However, over time laws and regulations regarding privacy have become more prominent, and now it's easier than ever to take control of who sees your content, as well as use products and services to keep your online life private. This section will cover three main areas, VPNs (Private Internet Access), Social Media, and Operational Security (OpSec).

VPNs
Section Coming Soon

Social Media
Section Coming Soon

OpSec
Section Coming Soon

MODULE CHALLENGE

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' on the first page before attempting the Challenge.

What will I need for this Challenge?

- Coming Soon

Challenge Brief:
Due to the nature of the OSINT Challenge, we are not able to release details about the activity you will be conducting, until the Challenge goes live. Please be patient. Expected launch date: 23rd /24th September