# OSINT Essential Training

with Mike Wylie

LEARNING

| Chapter | Video | Title | |
|---|---|---|---|
| **1. What is OSINT?** | 1. OSINT overview | What is OSINT? | https://www.dni.gov/index.php/what-we-do/what-is-intelligence |
| | 2. Understanding the value of OSINT | Penetration testing frameworks | • Open Source Security Testing Methodology Manual (OSSTMM)<br>• National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115<br>• The Penetration Testing Execution Standard (PTES) |
| | 3. Introduction to passive reconnaissance | Netcraft | https://www.netcraft.com/ |
| | | Shodan | https://www.shodan.io/ |
| | 4. Introduction to active reconnaissance | Metasploit | https://www.metasploit.com/ |
| | | OpenVAS | https://www.openvas.org/ |
| | | Sqlmap | https://github.com/sqlmapproject/sqlmap |
| | | WPScan | https://github.com/wpscanteam/wpscan |
| | | Burp Suite | https://portswigger.net/burp |
| | | Zed Attack Proxy | https://www.zaproxy.org/ |
| | 6. Introduction to sources of OSINT | OSINT sources | https://osintframework.com/ |
| | | Tails OS | https://tails.boum.org/ |
| | 7. Introduction to VPN and anonymizers | Tor | https://www.torproject.org/ |
| | | AmIUnique | https://amiunique.org/faq |

| | | | |
|---|---|---|---|
| | 1. Introduction to locations and addresses fingerprinting | Voter Registration Records | https://voterrecords.com/ |
| | 2. Using breach data for OSINT | Sony Pictures breach | https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/ |
| | | WikiLeaks | https://wikileaks.org/ |
| **2. Organizational OSINT** | | Pastebin | https://pastebin.com/ |
| | | Have I Been Pwned? | https://haveibeenpwned.com/ |
| | 3. Introduction to using business records for OSINT | List of official business registers | https://en.wikipedia.org/wiki/List_of_official_business_registers |
| | | National Association of Secretaries of State | https://www.nass.org/ |
| | | Business Records | https://guides.library.harvard.edu/c.php?g=845958&p=6047910#s-lg-box-wrapper-22618757 |
| | | SEC Filings | https://www.sec.gov/edgar/searchedgar/companysearch.html |
| | 4. Using job posts for OSINT | List of employment websites | https://en.wikipedia.org/wiki/List_of_employment_websites |
| **3. Employee OSINT** | 1. Using OSINT to find employees | FTC Consumer Sentinel Network (July 29, 2019) | https://public.tableau.com/profile/federal.trade.commission#!/vizhome/ConsumerSentinel/Infographic |

| | | | |
|---|---|---|---|
| **3. Employee OSINT** | 2. Using OSINT to find phone numbers | Phone number lookup tools | • Pipl<br>• WhoCalld<br>• CallerID Test<br>• ThatsThem – reverse phone lookup<br>• Twillio lookup<br>• Fone Finder<br>• Truecaller |
| | 3. Using OSINT to find email addresses | Recon-ng | https://github.com/lanmaster53/recon-ng |
| | | theHarvester | https://github.com/laramies/theHarvester |
| | | Common email address naming conventions | • First initial then last name<br>◦ htwill@HPlusSport.com<br>• First name dot last name<br>◦ henry.twill@HPlusSport.com<br>• First name only<br>◦ henry@HPlusSport.com |
| | | Spokeo | https://www.spokeo.com/ |
| | | Pipl | https://pipl.com/ |
| | | ThatsThem | https://thatsthem.com/ |
| | | EmailHippo | https://www.emailhippo.com/ |
| | | Have I Been Pwned? | https://haveibeenpwned.com/ |
| | 4. Using social media sites for OSINT | List of social networking sites | https://en.wikipedia.org/wiki/List_of_social_networking_services |

| | | | |
|---|---|---|---|
| **3. Employee OSINT** | 5. Extracting metadata from images | EXIF data | https://www.exifdata.com/ |
| | | Pic2Map | https://www.pic2map.com/ |
| **4. Technological OSINT** | 1. Introducing domain names and DNS discovery | DNS record types | https://en.wikipedia.org/wiki/List_of_DNS_record_types |
| | | DNS records and DNS proxy | https://support.cloudflare.com/hc/en-us/articles/360019093151-Managing-DNS-records-in-Cloudflare |
| | 2. Crawling websites to gather OSINT data | Nikto | https://github.com/sullo/nikto |
| | | BuiltWith | https://builtwith.com/ |
| | | Webalizer | http://www.webalizer.org/ |
| | | Burp Suite | https://portswigger.net/burp |
| | | Zed Attack Proxy | https://www.zaproxy.org/ |
| | 3. Finding deleted information in web archives | Wayback Machine | https://archive.org/ |

| | | | |
|---|---|---|---|
| **4. Technological OSINT** | 4. Introduction to using search engines for OSINT | Search engines | • Google<br>• Bing<br>• DuckDuckGo<br>• Yahoo<br>• Startpage<br>• Yandex<br>• Baidu<br>• iBoogie<br>• iZito<br>• Ixquick<br>• Instya<br>• Hulbee |
| | 5. Google hacking or dorking for OSINT | Google Hacking Database | https://www.exploit-db.com/google-hacking-database |
| | | inurl: | Value is contained somewhere in the URL. |
| | | site: | Value is contained somewhere in the URL. |
| | | filetype: | Search only for files, not webpages. |
| | | allinurl: | Search all of the following words in the URL. |
| | | intext: | Search the body of the webpage for specific text. |
| | | related: | Find website results that are related to your search term. |
| | | info: | Find supplemental information Google may have on this page. |
| | | link: | Find other pages indexed by Google that reference this link. |

| | | | |
|---|---|---|---|
| **4. Technological OSINT** | 6. Discovering OSINT data in the dark web | Tor | https://www.torproject.org/ |
| | | TorBot | https://github.com/DedSecInside/TorBot |
| | | DarkSearch | https://darksearch.io/ |
| | | Hunchly Report | https://www.hunch.ly/darkweb-osint/ |
| | | Report something on the dark web | https://www.missingkids.org/HOME |
| | 7. Introduction to RIRs | RIPE NCC | https://www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system |
| | | APNIC | https://www.apnic.net/manage-ip/manage-resources/address-status/by-rir/ |
| | | ARIN | https://www.arin.net/reference/research/statistics/rir/ |
| | | LACNIC | https://www.lacnic.net |
| | | NRO | https://www.nro.net/about/rirs/ |
| | | AFRINIC | https://afrinic.net/ |