Intro To OSINT

Intelligence collection tactics for investigations

Who am I?

Hi! I'm Kody Kinzie, a cybersecurity researcher (aka hacker) that specializes in OSINT investigations and WI-Fi security.

I currently work for a company called Varonis as a researcher, and prior to that I created a popular YouTube channel called Null Byte which teaches ethical hacking and OSINT skills to beginners.

I'm passionate about breaking things, finding data wherever it lives, and teaching people the skills we need to make the world a better place.

Follow me on Twitter @KodyKinzie!

Why am I teaching you OSINT?

Nowadays, humans have the capacity to simultaneously create, process, and act on data in real time like no time in history. Because of this, nearly any data you're looking for exists, or can be derived by existing data.

OSINT researchers share the same core mission as intelligence services, to hunt down relevant data and process information into insights.

Today, I hope to bring you up to speed on intelligence collection using OSINT, and make you aware of the tools at your disposal during an investigation.

Need a reference?

We'll be covering a lot in this course, and I'll try to answer any questions that come up!

However, if you have more questions or need a walkthrough guide, I've written many walk-through articles and videos online which are freely available online.

To find all my written OSINT guides, Google:

site:null-byte.wonderhowto.com "osint" "kody"

To find all my OSINT videos, Google:

site:youtube.com "osint" "kody"

Let’s get started!

To begin, we’ll be covering:

Intro to OSINT investigations

Technical skills & anti-leak best practices

Browser extensions for OSINT

VPN basics

The intelligence collection cycle

Collection tactics: OSINT, HUMINT, SIGINT

...

And also...

Investigation workflows

Google Dorking, alerts

Introduction to public databases

Technical Skills & Anti-Leak Best Practices

Prepare a computer or virtual machine for your investigations and do not mix your personal and work computer. **Do not sign into social media accounts that aren’t part of your investigation on your investigation computer.**

Part of the skills needed to be a good investigator include not blowing your own cover. LinkedIn is a perfect example of this. If you research a business person using LinkedIn and forget you’re signed in, they will be immediately alerted even if you don’t interact with the page.

We also need to make sure our system is secure, and that we’re using applications that won’t leak our data – provided we use them correctly.

Keep Your System Updated & Clear of Malware

Always apply the latest security updates as soon as possible, journalists are a huge target for APT’s because of the nature of your work.

Use 2FA on all accounts, never re-use the same password. Members of the press get free 1Password accounts – Use it!

Download CCleaner to remove unwanted files and cookies left by websites or installations.

For MacOS - Use ObjectiveSee tools

Use 2FA FIDO Keys for Critical Accounts

For critical accounts (especially Google) use a 2FA hardware key, but keep several. I have detailed instructions on how to set this up on YouTube.

Use FIDO for personal devices:

https://null-byte.wonderhowto.com/how-to/use-u2f-security-keys-your-smartphone-access-your-google-account-with-advanced-protection-0182760/

Use FIDO keys for Google accounts:

https://null-byte.wonderhowto.com/how-to/use-u2f-security-keys-your-smartphone-access-your-google-account-with-advanced-protection-0182760/

Using Browsers for Investigations

Firefox is the preferred browser for investigations due to its emphasis on privacy and performance.

Browser add-ons give investigators tools to search for data, forensic document evidence, analyze technical information, or dig for hidden metadata, and much more.

Go to Preferences and deselect “remember passwords for sites” and under “Firefox Will” select “Use custom settings for history.” Then uncheck both options to remember browser and search history.

Customizing Settings

To reduce how our device can be tracked, we'll need to customize some settings.

Type **about:config** in the browser and set privacy.trackingprotection.enabled to true, and geo.enabled to false.

Also set to false: browser.safebrowsing.enabled, browser.safebrowsing.malware.enabled, dom.event.clipboardevents.enabled (shows copy and pastes), media.navigator.enabled, dom.battery.enabled, extensions.pocket.enabled, media.peerconnection.enabled, media.peerconnection.video.enabled

Set media.peerconnection.turn.disabled to true

Why did we do that?

On your normal device, browse to this link:

https://grabify.link/9KQNOQ

After it loads, go here to see what your device leaked:

https://grabify.link/track/N6GWW7

Now, Try it With The Tor Browser

Open the Tor browser in Buscador and navigate to the link again.

Do not resize the window! The window size, if unique, can be recorded and can uniquely identify your device.

The goal when using your investigative system is to reduce the number of unique identifiers your system exposes to websites it connects to