OSINT Basics

Jonathan Klein

Agenda

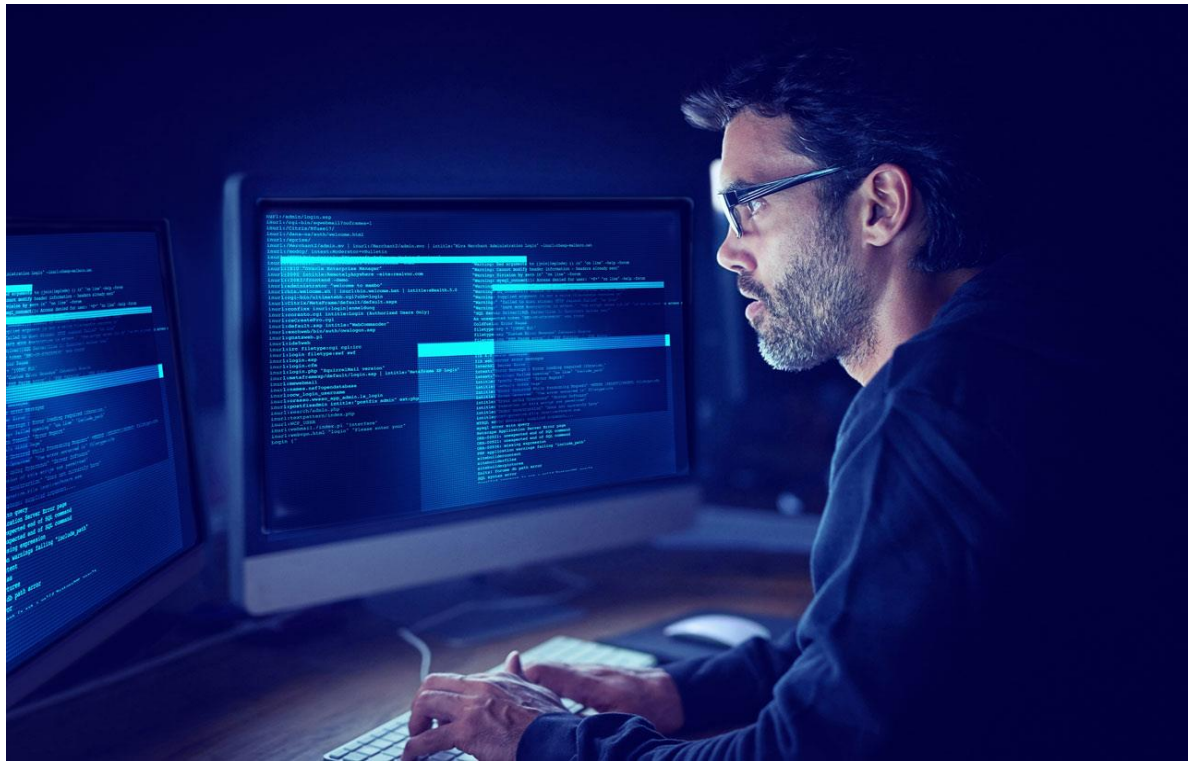
- Whoami
- What is Open Source Intelligence (OSINT)?
- What is OSINT used for?
- OSINT: Good vs Bad
- People OSINT
- Business OSINT
- Protect Your Privacy
- Sock Puppet
- VPN
- TOR
- TOR over VPN
- Pictures
- OSINT Tools
- Resources
- Education/Training
- Final Words

Whoami

- Jonathan Klein
- San Jose, CA native
- Network Engineer in IT for 10+ years
- US Army Officer for 7 years
- Looking to grow in a Blue Team role
- Enjoy Travel, Hiking, Reading, Football (American and European), podcasts, and true crime
- Never Stop Learning!

What is Open Source Intelligence (OSINT)?

- The process of gathering, collecting, and analyzing information which is acquired from public and open sources.



What is OSINT used for?

- Individual People
  - Finding a home
  - Job Search
  - Social Activities
- Businesses
  - Researching competitors
  - Market Trends
  - Prospective Employees
- Journalism
  - Investigating stories
- Law Enforcement
- Military
- Intelligence Agencies

OSINT: Good vs Bad

Good

- Business OPSEC
- House Hunting
- Job Hunting
- Working with vendors

Bad

- Business OPSEC
- Stalking
- Doxing

People OSINT

- People/public records search sites (ie https://www.familytreenow.com/)
- Social Media profiles (Facebook, Twitter, Linkedin, Instagram, etc)
- Data Breach Dumps
- Friends/Family/professional connections (social media)
- Dating Apps (Match, Plenty of Fish, OKCupid, etc)
- Spider out from family, friends, hobbies and place of work
- Image search
  - Google Reverse Image Search: https://images.google.com/
  - Yandex: https://yandex.com/images/

Business OSINT

- Business Website
  - Leadership
  - Partners
  - Office Locations
- Company Reviews (ie Glassdoor)
- Company profiles/insights (ie Linkedin)
- Job postings (ie. Linkedin, Indeed, Monster, etc)
- Social Media
  - Especially employee pictures
    - Possible ID badges
    - Employee faces
  - Company news
- Email addresses (https://hunter.io/)
- Google Maps

Protect Your Privacy

- Turn off Location/GPS Services
  - Example: Fitness app Strava lights up staff at military bases https://www.bbc.com/news/technology-42853072
  - Building the Global Heatmap: https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de
- Use a VPN service (ie. NordVPN, CyberGhost, ProtonVPN)
- Use TOR (The Onion Router)
- Show less detail in your pictures
- Sock puppet

Sock Puppet

- Creating a Sock Puppet
  - Creating account on Facebook, Twitter, Linkedin, etc
  - Encrypted email: ie ProtonMail
  - Burner Phone for each account
    - Purchase cheap on at Target, WalMart, BestBuy
    - Sim Card through Mintmobile.com
  - Profile picture: https://thispersondoesnotexist.com/
  - Profile information: https://www.fakenamegenerator.com/
- Use VPN or TOR
- Be realistic with target demographic

Using VPN

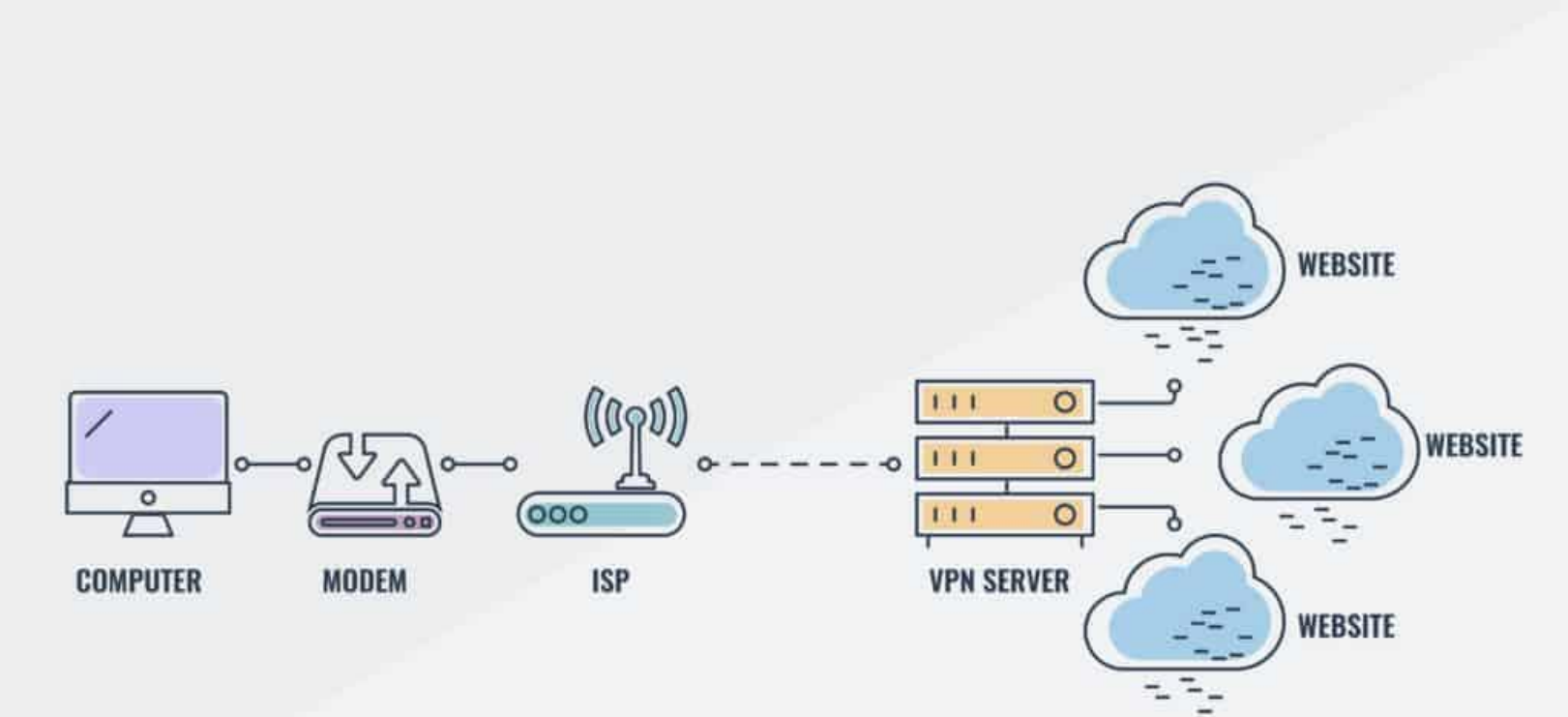
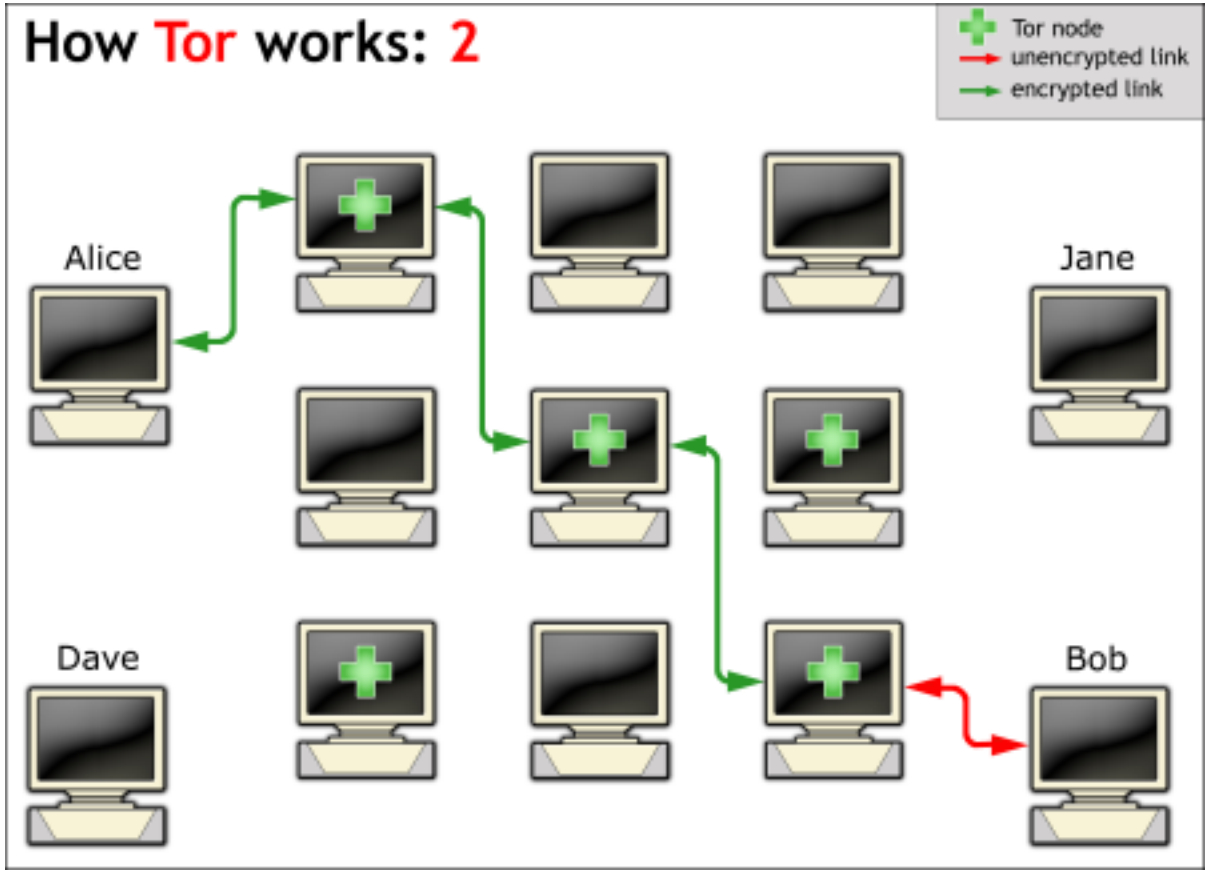
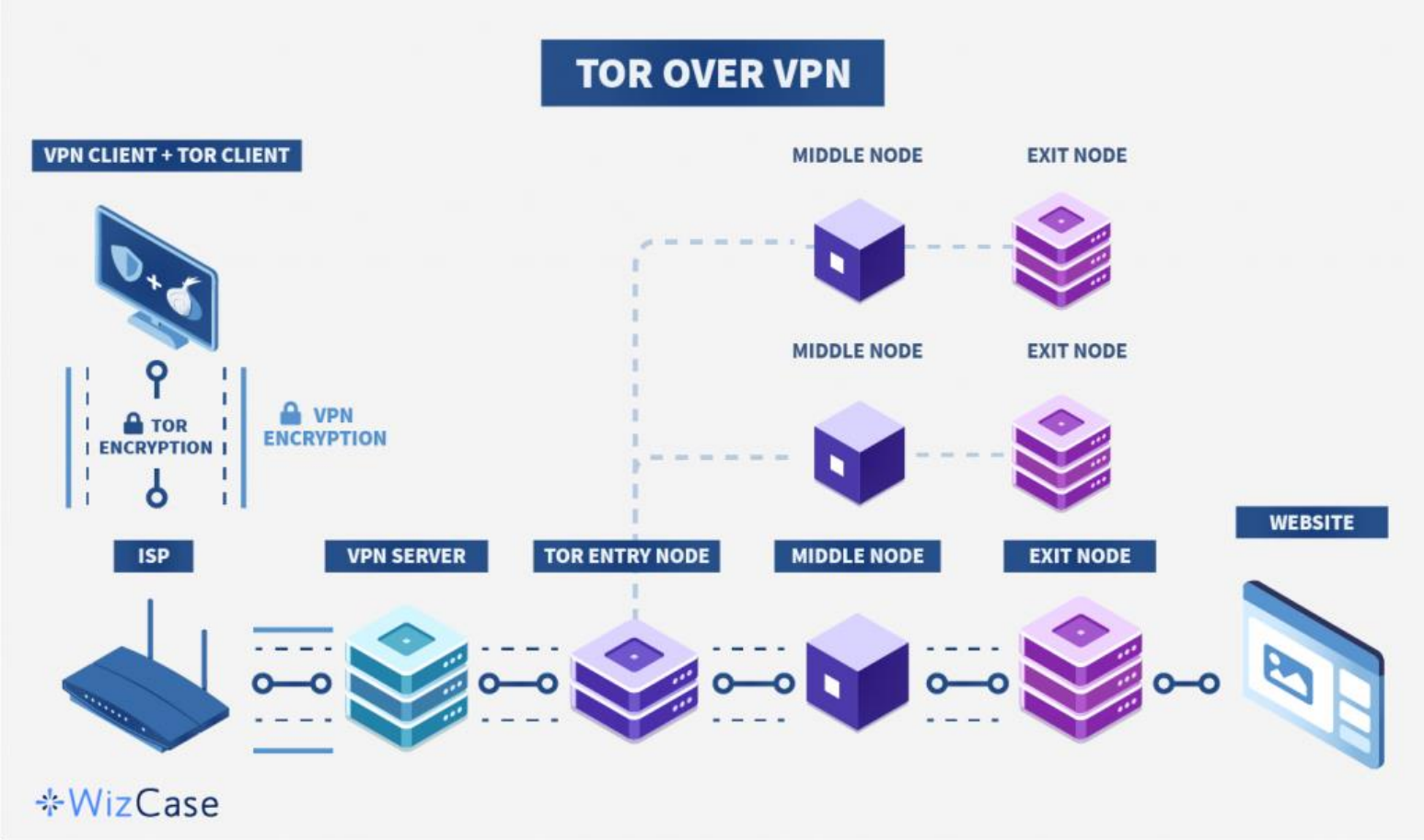


FIG: Simplified VPN Connection

Using TOR


How Tor works: 2
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob

Using TOR over VPN




MAYSER HÜTE
ZECHBAUER ZIGARREN
GALERIA
KAUFhof
Konica
BOSCH
gore
Sonnenstraße
Maroni


Deutscher Herold
Spatten
Restaurant
Hauptmarkt


THANK YOU G.I.'s
ALLIED FORCES
BERATED ME FROM
NTRATION CAMP
IN 1945


P
ACCÉS BC
CASINO
BARCELONA

OSINT Tools


www.ethicalhackersacademy.com
TOP OPEN SOURCE INTELLIGENCE TOOLS USED IN CYBERSECURITY
1 OSINT Framework
2 CheckUserNames
3 HavelbeenPwned
4 BeenVerified
5 Censys
6 BuiltWith
7 Google Dorks
8 Maltego
9 Recon-Ng
10 theHarvester
11 Shodan
12 Jigsaw
13 SpiderFoot
14 Creepy
15 Nmap
16 WebShag
17 OpenVAS
18 Fierce
19 Unicornscan
20 Foca
21 ZoomEye
22 Spyse
23 IVRE
24 Metagoofil
25 Exiftool
Ethical Hackers Academy

Resources

- OSINT Framework (https://osintframework.com/)
- OSINT Curious (https://osintcurio.us/)
  - YouTube: (https://www.youtube.com/channel/UCjzceWf-OT3ImIKztzGkipA)
- Michael Bazzell's Open Source Intelligence Techniques Book
  - 8th Edition as of 1/1/21
- Bellingcat (https://www.bellingcat.com/)
- Hunting Cyber Criminals by Vinny Troia
- How to Disappear by Frank M. Ahearn
- Gray Man by Matthew Dermody
- The Ultimate OSINT Collection (@hatless1der on Twitter)
  - https://start.me/p/DPYPMz/the-ultimate-osint-collection
- ATP 2-22.9 Open-Source Intelligence, July 2012, Department of the Army

Education/Training

- The OSINTion: https://www.theosintion.com/courses/
- OSINT Combine: https://academy.osintcombine.com/
- Plessas: https://academy.plessas.net/
- GeoGuessr: https://www.geoguessr.com/
- Udemy
  - Open-Source Intelligence (OSINT) Fundamentals by Heath Adams (The Cyber Mentor)
  - The Ultimate Dark Web, Anonymity, Privacy, and Security course by Zaid Sabih (zSecurity)

Final Words

- Pay Attention to Detail
- Always keep looking
- Picture is worth a thousand words
- Small information can be very big in an investigation