2018 BSIDES KNOXVILLE

Full Auto OSINT

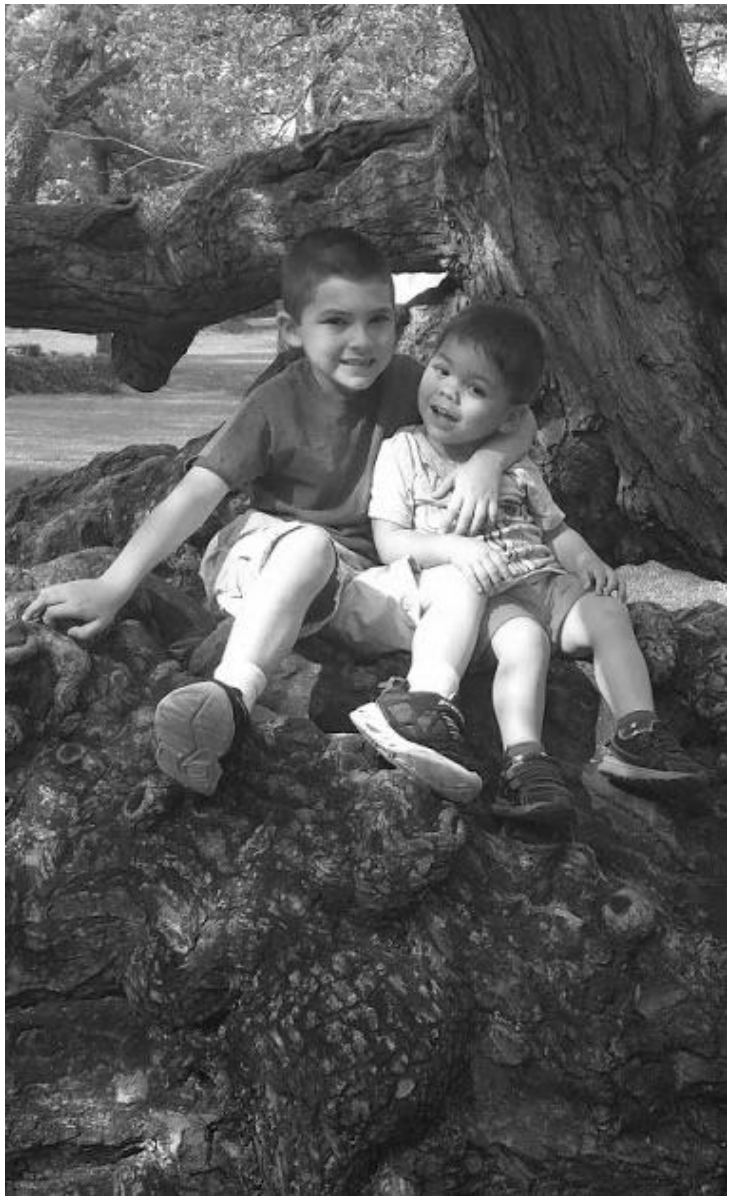
OSINT for Pentesters

RAPID7

Me Me Me...

- Who/What am I?

- Simple answer:
  - Father/Husband/Son/Brother
  - Programmer/Pentester/Researcher
  - Hillbilly



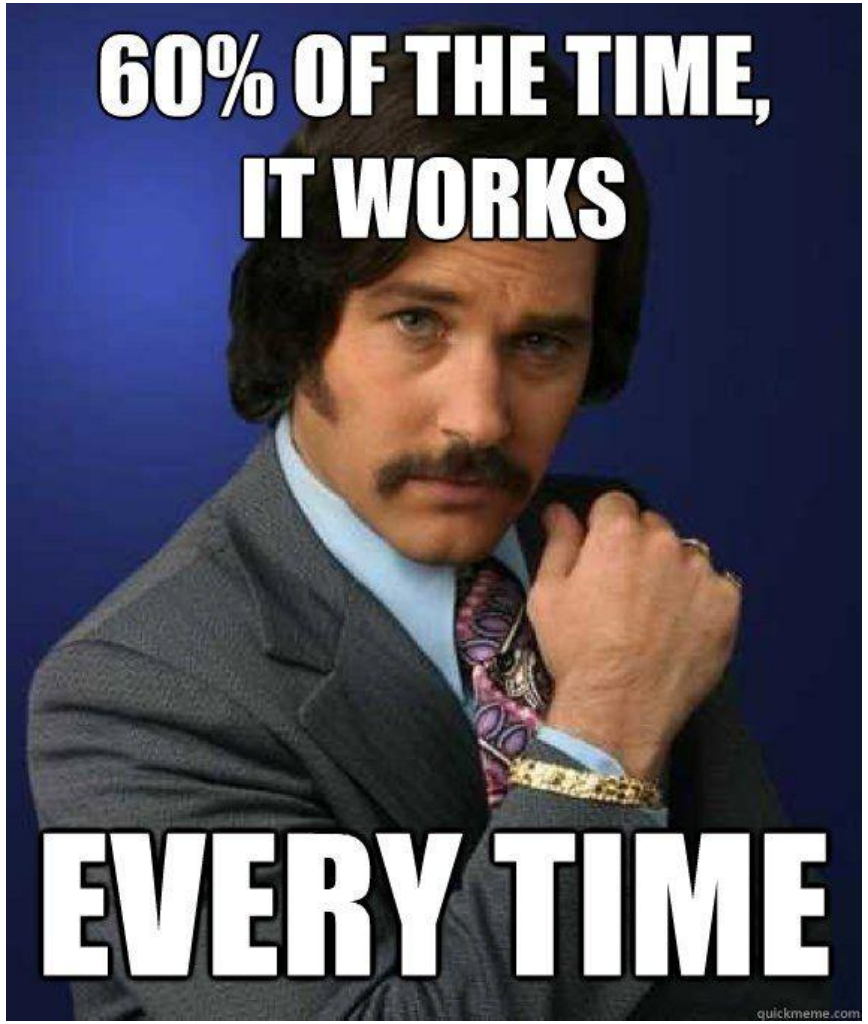
What is OSINT?

"Open Source Intelligence, often referred to as OSINT, can mean many things to many people. Officially, it is defined as any **intelligence produced from publicly available information** that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. For the CIA, it may mean information obtained from foreign broadcasts. For an attorney, it may mean data obtained from official government documents that are available to the public. For most people, it is publicly available content obtained from the internet."

--Michael Bazzell

Is it legal?

Why OSINT?



Goal oriented OSINT…

- What are you after?

Goal oriented OSINT...

- What are you after?
  - Usernames?
  - Passwords?
  - Personal details?
  - Locate someone?

Where/How to Gather OSINT

Where/How to Gather OSINT

- Internet
  - Search Engines
  - Social Media
  - Online Communities
  - Data Sharing/Hosting
  - Corporate

Where/How to Gather OSINT

- Internet
  - Search Engines
  - Social Media
  - Online Communities
  - Data Sharing/Hosting
  - Corporate
- Tools
  - System/OS Tools
  - Pentester Tools
  - APIs

To the webs!!!!


bel...uth
Slashdot:News for Nerds. Stuff that Matters. – Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward
Address http://slash
Links
About Internet Explorer
Microsoft
Internet
Explorer 4.0
Version 4.72.3110
Cipher Strength:
Update versions: ;SP1;
Product ID:
Copyright Information
OK
News for Nerds.
faq
code
awards
privacy
slashNET
older stuff
rob's page
preferences
andover.net
submit story
fixme:advapi:CryptAcquireContextA (0x40e2e7b4, (null), (null), 1, f0000000): stu
b!
Terminal
The GIMP
bellsouth
Sat Jan 05
10:14 PM

To the webs!!!!

- Search Engines
- Social Media
- Online Communities
- Data Sharing
- Corporate

Search Engines

DuckDuckGo

RAPID7

Social Media

Demo

Online Communities

reddit

GitHub

4chan

Pinterest

Data Sharing

PASTEBIN

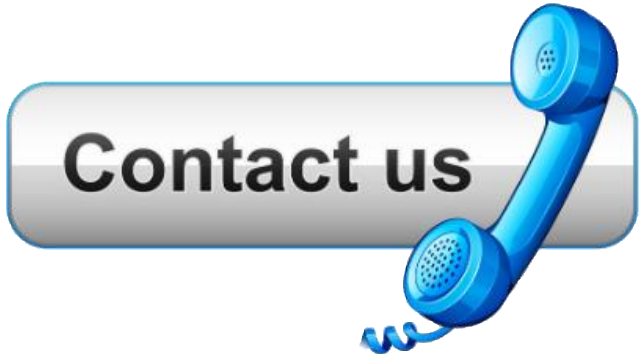
github:gist

slideshare

Scribd.

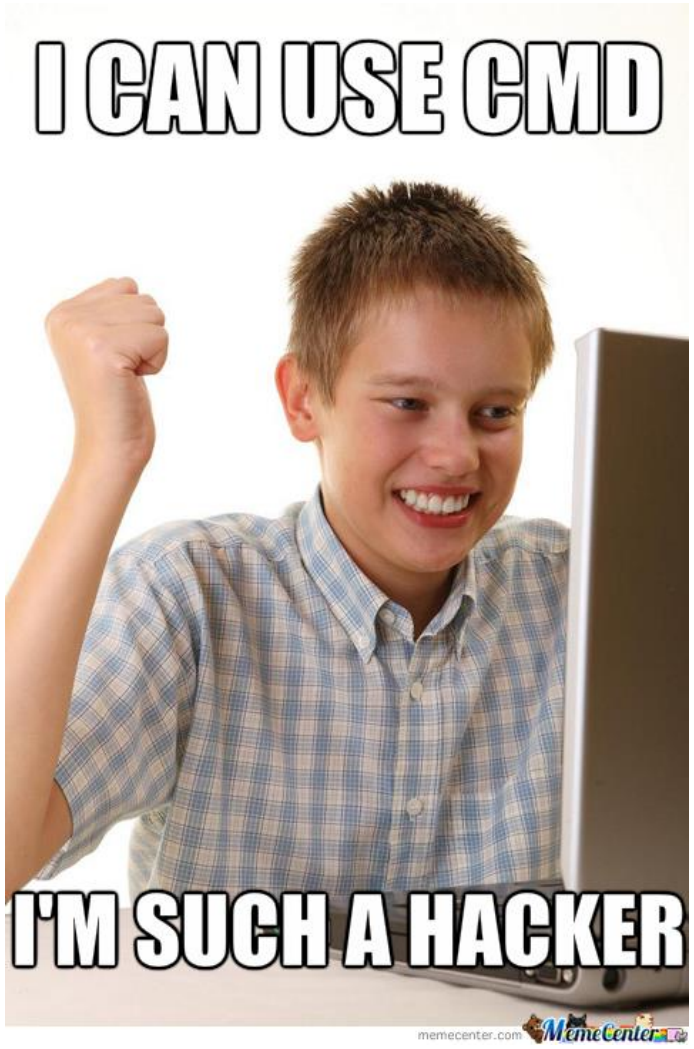
Demo

Corporate



Demo

Time for the command line!!!



Time for the command line!!!

- System Tools
- Pentester Tools
- APIs

System Tools

- dig
- whois
- traceroute

Pentester Tools

- theHarvester
- Sublist3r
- FOCA
- Recon-ng
- Metagoofil
- Fierce
- Spiderfoot
- Creepy
- Tinfoleak
- EyeWitness
- Instalooter
- ...

Demo

APIs

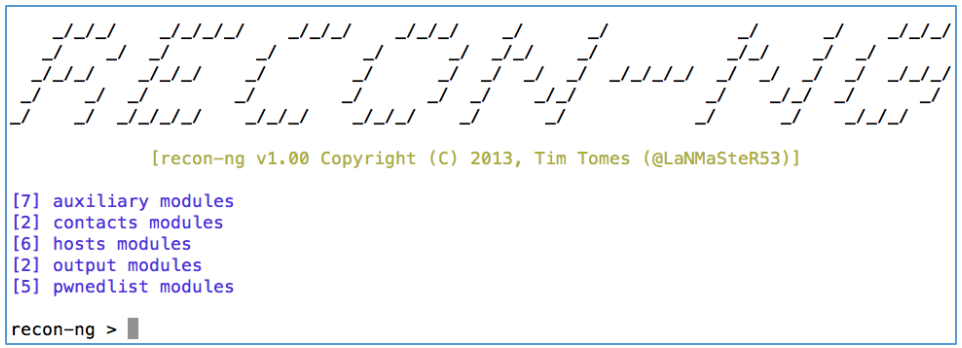
pipl

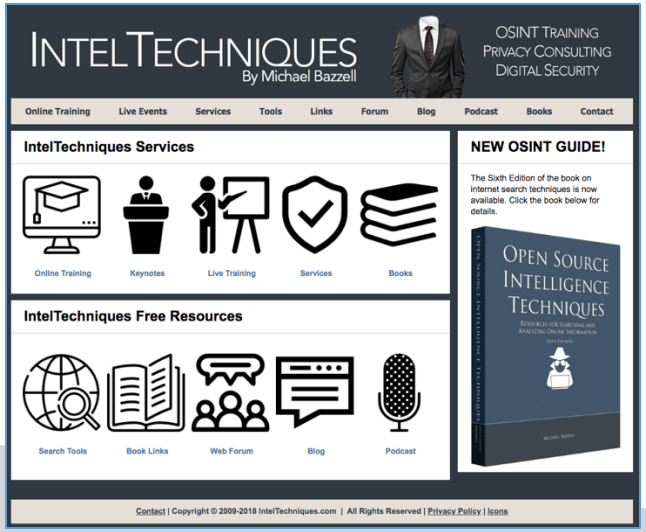
RAPID7

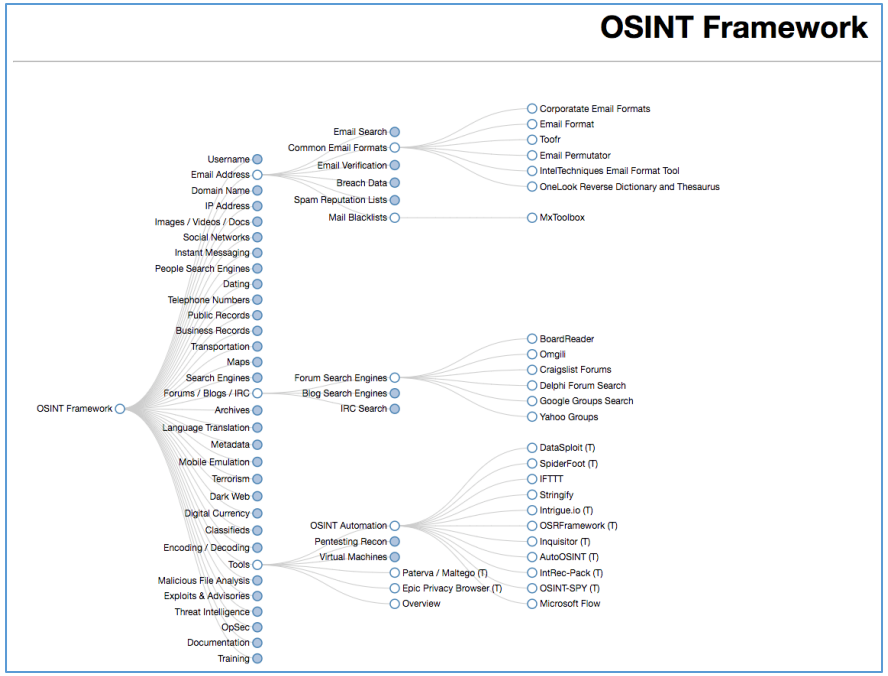
Demo

MultiTools

MALTEGO







RAPID7

Demo

Lets Automate It!!!

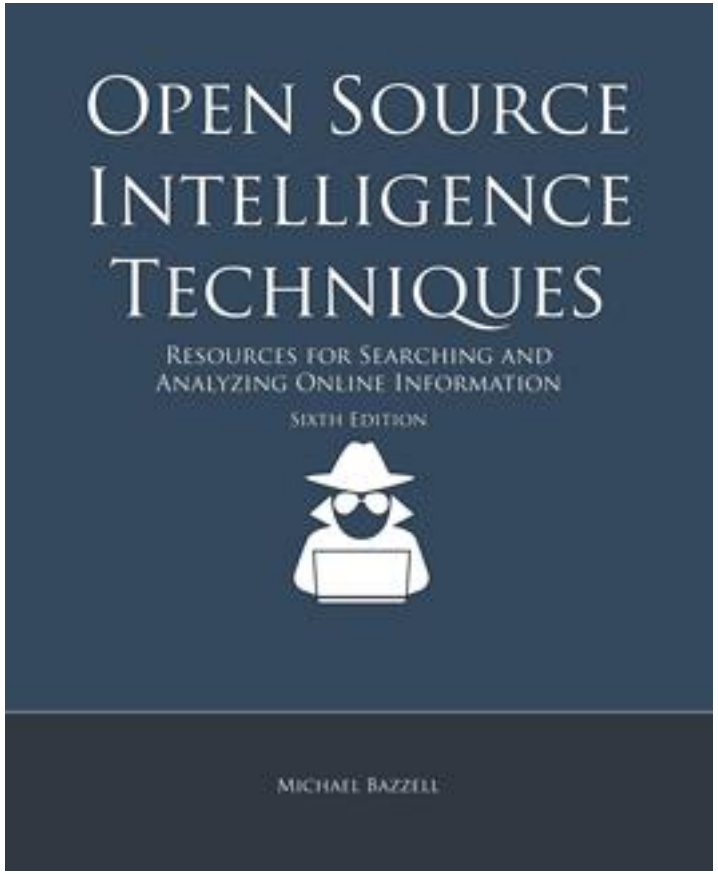
RAPID7

Demo … Not Quite Yet

Sorry ☹

Resources

- https://inteltechniques.com/
- https://start.me/p/m6XQ08/osint
- http://osintframework.com/
- https://github.com/Ph055a/awesome_osint



THANK YOU

Questions? Comments? Thoughts?

Contact Info:

- adam_compton@rapid7.com
- adam.compton@gmail.com
- @tatanus
- https://www.hillbillystorytime.com

RAPID7