

Gerren Jerome

Footprinting and Reconnaissance

1. Perform footprinting through search engines (8 items)

- Gather information using advanced Google hacking techniques.

Screengrab: Step 5 – ECCouncil intitle login search

The screenshot shows a Google search results page. The search query is "intitle:login site:eccouncil.org". The results list several EC-Council login pages:

- Login - ASPEN - EC-Council**
Type your username and password. Login. Username *. Password *.
- Login**
Login To Your EC-Council Learning Account. Login To Your EC-Council Learning Account. Sign Into Your Account to Continue Building In-Demand Skills With ...
- Login to iLabs**
May 18, 2017 — Get Connected to iLabs. Anytime. Anywhere. CEHproductimage · Computer Forensics Exercises · Security Analyst Exercises · Ec-Council Secure ...

Screengrab: Step 7 – Find ECC pdfs related to the CEH program

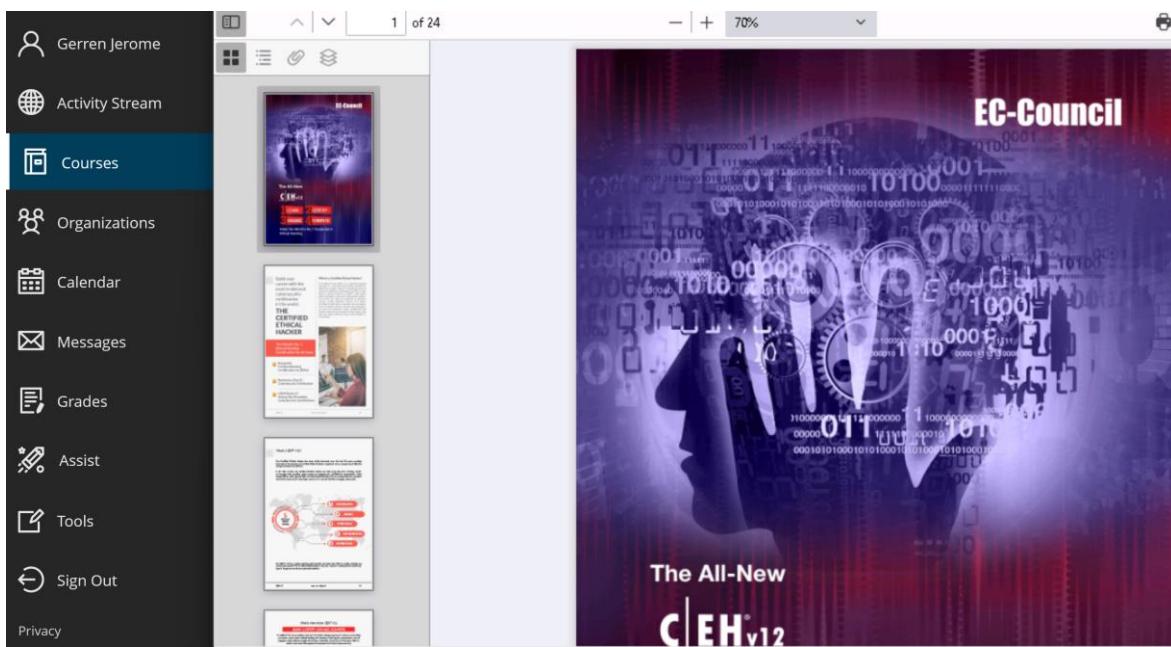
The screenshot shows a Google search results page. The search query is "ec-Council filetype:pdf ceh". The results list a PDF titled "CEH-brochure.pdf" from EC-Council:

CEH-brochure.pdf
A Certified Ethical Hacker is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to.
24 pages

People also ask :

- Is CEH from EC-Council worth it?
- Is CEH a hard exam?
- Why is CEH so expensive?

Screengrab: Step 9 – CEH-brochure.pdf



b) Gather information from video search engines.

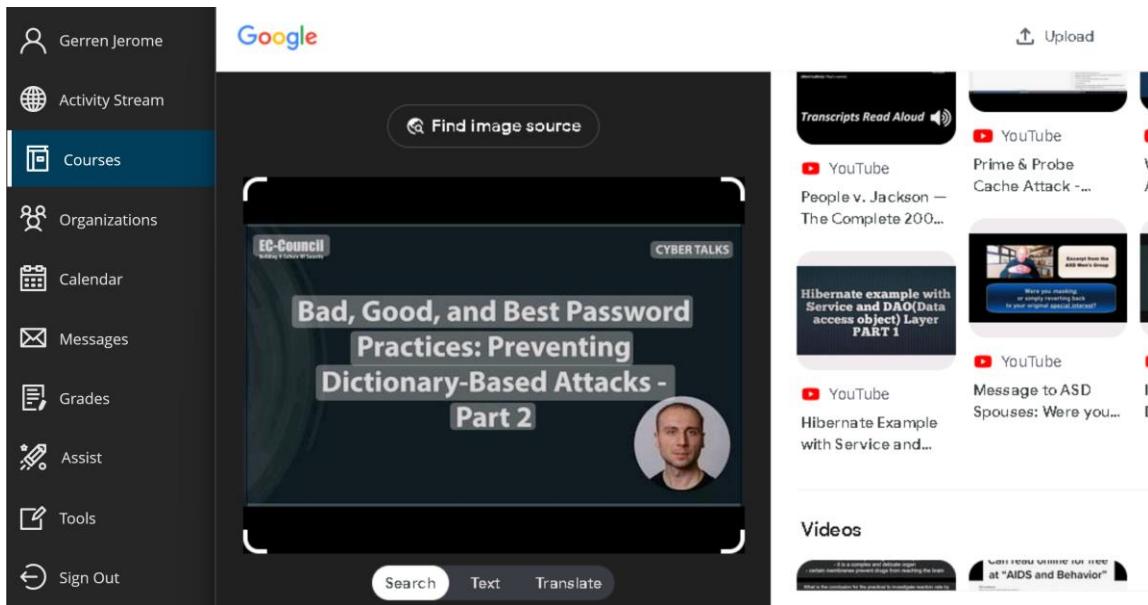
Text: Step 3 – Paste the link from the video you chose

http://www.youtube.com/watch?v=f_iVuHgCToA&pp=ygUKZWMtY291bmNpbA%3D%3D

Screengrab: Step 6 – The mattw.io Snippet section



Screengrab: Step 9 – Reverse Image Search



c) Gather information from FTP search engines

Screengrab: Step 4 – NAPALM-FTP search results

NAPALM
FTPindexer

microsoft

With all the words ▾

Search

Showing results 0 to 19 of about 10000 for "microsoft"

Order Date Desc Date Asc Size Desc Size Asc None

Related keywords

- raspbian
- pub
- archive
- org
- pool
- main
- mono
- libmono
- cil
- dfsg
- all
- deb
- microsoft
- deb10u1
- system
- json
- microsoft4
- csharp4
- build4
- build
- utilities
- web
- infrastructure1
- visualc10

/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/
libmono-system-json-microsoft4.0-cil_6.8.0.105+dfsg-3.5_all.deb

34.6 KB DOWNLOAD

Last checked: 2024-01-23 02:59 Similar files: [Browse]

/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/
libmono-system-json-microsoft4.0-cil_6.8.0.105+dfsg-3.3_all.deb

56.6 KB DOWNLOAD

Last checked: 2024-01-23 02:59 Similar files: [Browse]

/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/
libmono-system-json-microsoft4.0-cil_6.8.0.105+dfsg-3.3_all.deb

34.5 KB DOWNLOAD

Last checked: 2024-01-23 02:59 Similar files: [Browse]

/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/
libmono-system-json-microsoft4.0-cil_5.18.0.240+deb10u1_all.deb

55.1 KB DOWNLOAD

Last checked: 2024-01-23 02:59 Similar files: [Browse]

/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/

12.1 KB DOWNLOAD

d) Gather information from IoT search engines

Screengrab: Step 4 – shodan.io search results

The screenshot shows the Shodan search interface. On the left is a sidebar with user info (Geren Jerome), activity stream, courses, organizations, calendar, messages, grades, assist, tools, sign out, and privacy. The main area has tabs for SHODAN, Explore, Pricing, and a search bar with the query 'amazon'. Below is a summary section with 'TOTAL RESULTS' at 236,909 and 'TOP COUNTRIES' showing a world map with red dots. A detailed result for IP 54.196.179.133 is shown, which is an Amazon instance in the United States. Another result for 34.213.212.180 is also listed.

Country	Count
United States	113,649
Japan	35,454
Ireland	15,495
India	10,738
Singapore	9,115
More...	

IP Address	Count
54.196.179.133	202
34.213.212.180	202

2) Perform footprinting through web services (6 items)

a) Find the company's domains and sub-domains using Netcraft

Screengrab: Step 5 – Netcraft site report

The screenshot shows the Netcraft site report for EC-Council. The sidebar includes links for user profile, activity stream, courses, organizations, calendar, messages, grades, assist, tools, sign out, and privacy. The main report section starts with a 'Background' tab showing site title, rank, and risk rating. It then moves to a 'Network' tab displaying site details like Netblock Owner, Hosting company, Hosting country, and IPv4 address, along with their respective domain names and organization details.

Site	https://www.eccouncil.org	Domain
Netblock Owner	Cloudflare, Inc.	Nameserver
Hosting company	Cloudflare	Domain registrar
Hosting country	US	Nameserver organisation
IPv4 address	104.18.8.180 (VirusTotal)	Organisation

b) Gather personal information using PeekYou online people search service

Screengrab: Step 5 – PeekYou search results

The screenshot shows the PeekYou search interface. On the left is a sidebar with user profile, activity stream, courses, organizations, calendar, messages, grades, assist, tools, and sign out options. The main search bar at the top has fields for 'PEOPLE' (Satya), 'USERNAME' (Nadella), and 'All States'. Below the search bar is a 'Search People' section with 'First Name' and 'Last Name' input fields, and a 'Start Search' button. A blue banner below the search bar says 'for Satya Nadella from District Of Columbia, USA'. The main content area displays a 'Public Records & Background Search' section with four results for 'Satya Nadella' (age 55, 56, and two others). There is also a 'Background Check' link. To the right, there is a sidebar for 'Ask an Expert' featuring a profile for 'Ellen, Consultant' with a 5-star rating and 263 satisfied customers. A message from 'Pearl Wilson, Tech Expert's Assistant' is visible at the bottom.

c) Gather an email list using theHarvester

Screengrab: Step 9 – theHarvester search results

The screenshot shows theParrot Terminal window with the command 'theHarvester -d microsoft.com -l 200 -b baidu - Parrot Terminal' entered. The terminal output shows theHarvester version 4.0.0, credits to Christian Martorella, and contact information. It then lists the target as 'microsoft.com', searching Baidu, and finds no IPs, emails, or hosts.

```
theHarvester -d microsoft.com -l 200 -b baidu - Parrot Terminal
[!] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] No emails found.
[*] No hosts found.
```

d) Gather information using deep and dark web searching

Screengrab: Step 6 – Google search results

The screenshot shows a Google search results page with the query "hacker for hire". The sidebar on the left contains navigation links such as Institution Page, Gerren Jerome, Activity Stream, Courses (which is selected), Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The search results include a link to Upwork's page on freelance hackers, a list of 27 best freelance hackers, and a section titled "Discussions and forums" with links to Quora and Reddit.

Google search results for "hacker for hire":

- About 191,000,000 results (0.50 seconds)
- Upwork https://www.upwork.com › hire › hackers
- 27 Best Freelance Hackers For Hire In January 2024
- Hire the best Hackers · \$50/hr \$50 hourly. Victoria G. Hacker. 5.0/5 · \$48/hr \$48 hourly. Milan V. Hacker. 5.0/5 · \$75/hr \$75 hourly. Petar A. Hacker. 5.0/5 ...
- ★★★★★ Rating: 4.7 · 1,807 reviews

Discussions and forums:

- How to hire a hacker who receives payment after done - Quora
- www.quora.com · Sep 26, 2023 · 7 posts
- Are "hackers for hire" a thing? : r/hacking - Reddit
- www.reddit.com · Sep 20, 2021 · 43 posts

e) Determine target OS through passive footprinting

Screengrab: Step 2 – Censys search results

The screenshot shows a Censys search results page for the domain www.eccouncil.org. The sidebar on the left is identical to the one in the Google search results. The search bar shows the query "Hosts" and the URL "www.eccouncil.org". The results table has columns for IP, Hostname, OS, and Ports. It lists three hosts: 158.178.154.74, 95.99.176.253, and 2a00:ec1:0:1f:0:0:0:181, each with its respective details and network connections.

IP	Hostname	OS	Ports
158.178.154.74	ORACLE-BMC-31898	Ubuntu Linux	22/SSH, 80/HTTP, 443/HTTP
95.99.176.253	253-176-99-95.ftth.glasoperator.nl	TMOBILE-THUIS (50266)	443/HTTP, 6881/KRPC
2a00:ec1:0:1f:0:0:0:181	GTS-BACKBONE GTS Telecom (5606)	GTS-BACKBONE GTS Telecom (5606)	80/HTTP, 443/HTTP

3) Perform footprinting through social networking sites (2 items)

a) Gather employees' information from LinkedIn using theHarvester

Screengrab: Step 6 – theHarvester search results

The screenshot shows a terminal window titled "theHarvester -d ecouncil -t 200 -b linkedin - Parrot Terminal". The output of the command is displayed, showing the tool's internal structure and the results of searching LinkedIn for the target "ecouncil".

```
theHarvester -d ecouncil -t 200 -b linkedin - Parrot Terminal
[...]
[*] Target: ecouncil
[*] LinkedIn Users found: 135
[+] Aaron Hardy - Sales Account Specialist - EC-Council
[+] Abdullateef Owoyemi - Cybersecurity Mentor
[+] Abhishek Chakraborty - Senior Regional Manager
```

b) Gather personal information from various social networking sites using Sherlock

Screengrab: Step 6 – Sherlock search results

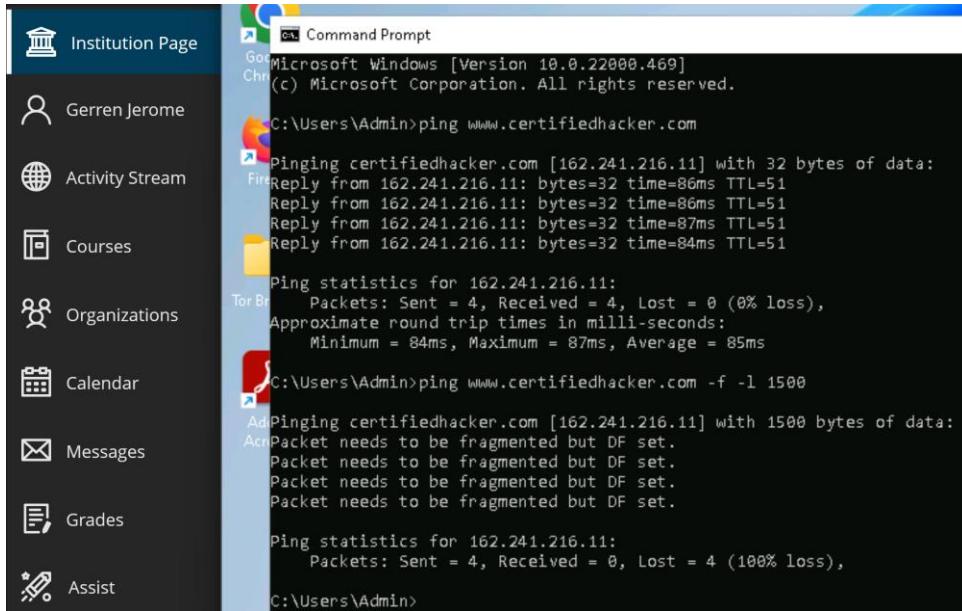
The screenshot shows a terminal window titled "python3 sherlock satya nadella - Parrot Terminal". The output of the command is displayed, showing the tool's findings across various social media and professional platforms for the user "satya".

```
python3 sherlock satya nadella - Parrot Terminal
[*] Checking username satya on:
[+] 7Cups: https://www.7cups.com/@satya
[+] About.me: https://about.me/satya
[+] Academia.edu: https://independent.academia.edu/satya
[+] AllMyLinks: https://allmylinks.com/satya
[+] Anilist: https://anilist.co/user/satya/
[+] Apple Developer: https://developer.apple.com/forums/profile/satya
[+] Apple Discussions: https://discussions.apple.com/profile/satya
[+] Archive of Our Own: https://archiveofourown.org/users/satya
[+] Archive.org: https://archive.org/details/@satya
[+] Asciinema: https://asciinema.org/~satya
[+] Ask Fedora: https://ask.fedoraproject.org/u/satya
[+] AskFM: https://ask.fm/satya
[+] Audiojungle: https://audiojungle.net/user/satya
[+] BLIP.fm: https://blip.fm/satya
[+] Bandcamp: https://www.bandcamp.com/satya
[+] Behance: https://www.behance.net/satya
[+] BiggerPockets: https://www.biggerpockets.com/users/satya
[+] Bikemap: https://www.bikemap.net/en/u/satya/routes/created/
[+] BitCoinForum: https://bitcoinform.com/profile/satya
[+] Blogger: https://satya.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/satya
```

4) Perform website footprinting (14 items)

a) Gather information about a target website using ping command line utility

Screengrab: Step 4 - finding the frame limit, part 1



The screenshot shows a Windows desktop environment. On the left is a dark sidebar menu with the following items:

- Institution Page
- Gerren Jerome
- Activity Stream
- Courses
- Organizations
- Calendar
- Messages
- Grades
- Assist

To the right of the sidebar is a Command Prompt window titled "Command Prompt". The window displays the following output:

```
Microsoft Windows [Version 10.0.22000.469]
Copyright (c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=86ms TTL=51
Reply from 162.241.216.11: bytes=32 time=86ms TTL=51
Reply from 162.241.216.11: bytes=32 time=87ms TTL=51
Reply from 162.241.216.11: bytes=32 time=84ms TTL=51

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 87ms, Average = 85ms

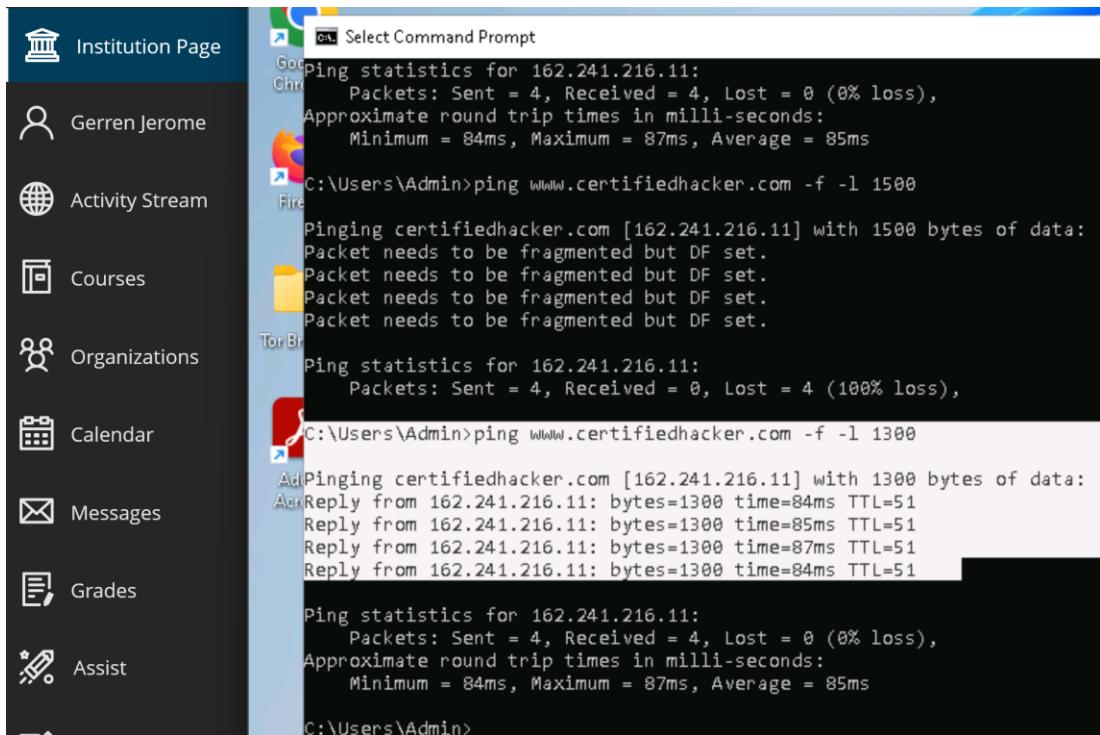
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 87ms, Average = 85ms

C:\Users\Admin>
```

Screengrab: Step 6 – finding the frame limit, part 2



The screenshot shows a Windows desktop environment. On the left is a dark sidebar menu with the following items:

- Institution Page
- Gerren Jerome
- Activity Stream
- Courses
- Organizations
- Calendar
- Messages
- Grades
- Assist

To the right of the sidebar is a Command Prompt window titled "Select Command Prompt". The window displays the following output:

```
Select Command Prompt
Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 87ms, Average = 85ms

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 87ms, Average = 85ms

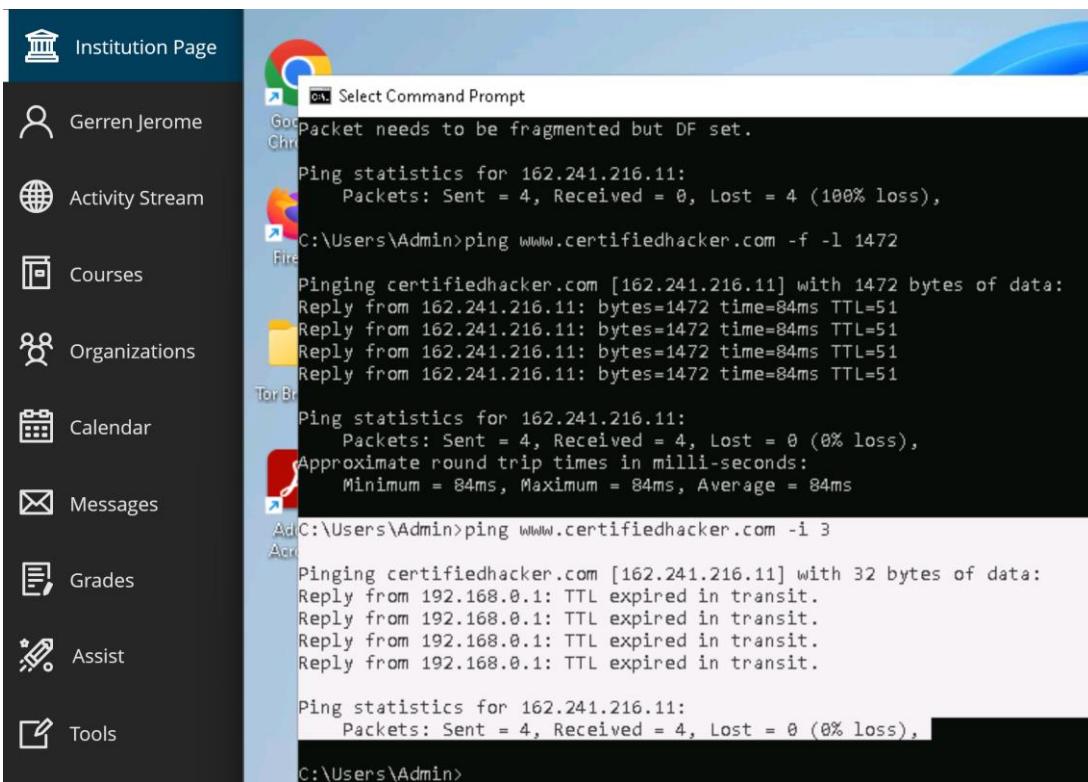
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1300

Pinging certifiedhacker.com [162.241.216.11] with 1300 bytes of data:
Reply from 162.241.216.11: bytes=1300 time=84ms TTL=51
Reply from 162.241.216.11: bytes=1300 time=85ms TTL=51
Reply from 162.241.216.11: bytes=1300 time=87ms TTL=51
Reply from 162.241.216.11: bytes=1300 time=84ms TTL=51

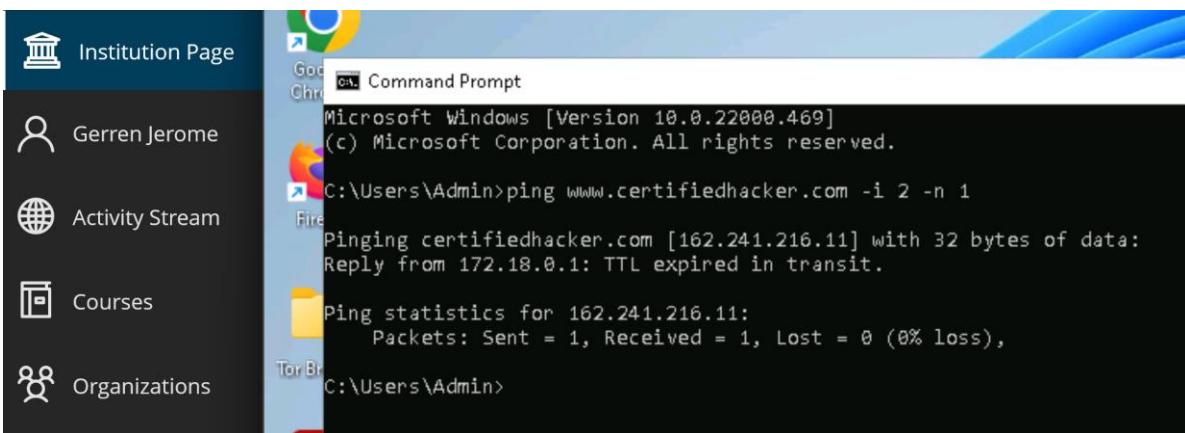
Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 87ms, Average = 85ms

C:\Users\Admin>
```

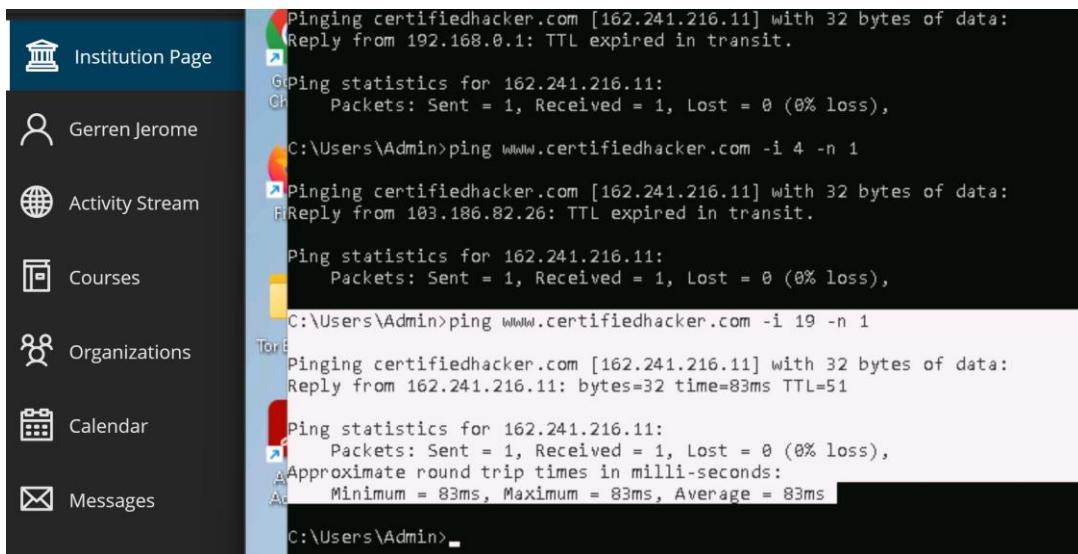
Screengrab: Step 10 – TTL manipulation



Screengrab: Step 12 – ping packet lifespan



Screengrab: Step 17 – find the hop

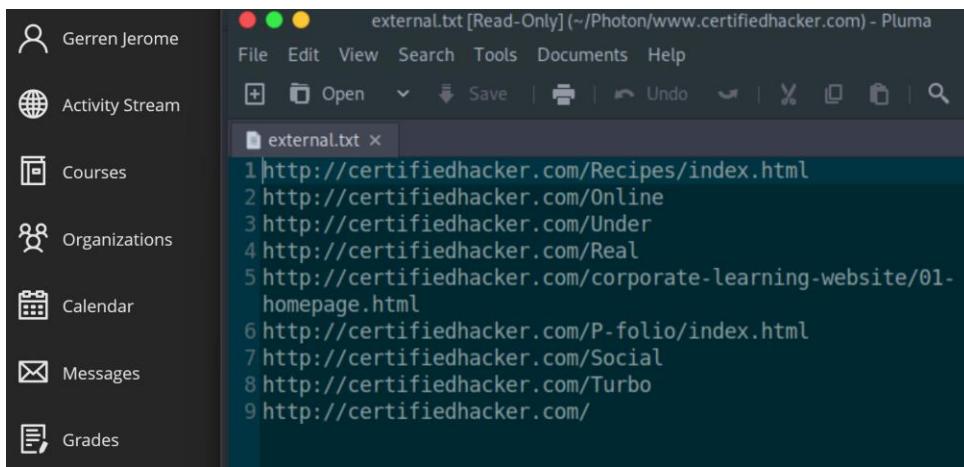


The screenshot shows a desktop interface with a sidebar on the left containing icons for Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, and Grades. There are two terminal windows open. The top window shows ping results for 192.168.0.1 and 162.241.216.11, both resulting in TTL expired errors. The bottom window shows ping results for www.certifiedhacker.com, which successfully replies from 103.186.82.26 with a TTL of 51. The command used was ping www.certifiedhacker.com -i 19 -n 1.

```
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:  
Reply from 192.168.0.1: TTL expired in transit.  
  
Ping statistics for 162.241.216.11:  
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),  
  
C:\Users\Admin>ping www.certifiedhacker.com -i 4 -n 1  
  
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:  
Reply from 103.186.82.26: TTL expired in transit.  
  
Ping statistics for 162.241.216.11:  
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),  
  
C:\Users\Admin>ping www.certifiedhacker.com -i 19 -n 1  
  
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:  
Reply from 162.241.216.11: bytes=32 time=83ms TTL=51  
  
Ping statistics for 162.241.216.11:  
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 83ms, Maximum = 83ms, Average = 83ms  
  
C:\Users\Admin>
```

b) Gather information about a target website using Photon

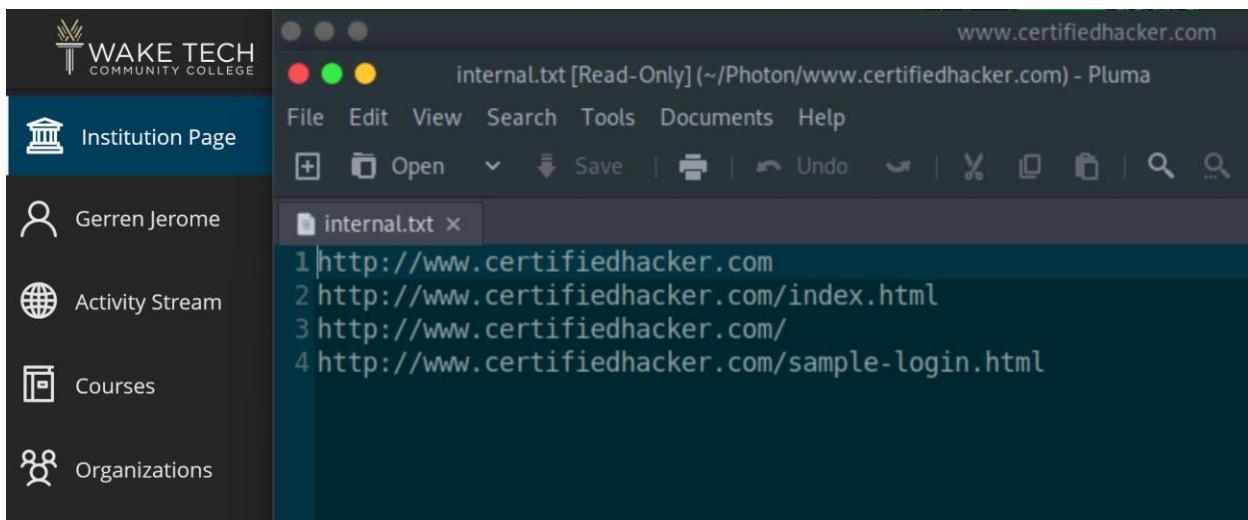
Screengrab: Step 15 – Photon results – external



The screenshot shows a desktop interface with a sidebar on the left containing icons for Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, and Grades. A terminal window is open with the title "external.txt [Read-Only] (~/Photon/www.certifiedhacker.com) - Pluma". The file contains a list of URLs, likely gathered by the Photon tool. The URLs listed are:

```
1 http://certifiedhacker.com/Recipes/index.html  
2 http://certifiedhacker.com/Online  
3 http://certifiedhacker.com/Under  
4 http://certifiedhacker.com/Real  
5 http://certifiedhacker.com/corporate-learning-website/01-homepage.html  
6 http://certifiedhacker.com/P-folio/index.html  
7 http://certifiedhacker.com/Social  
8 http://certifiedhacker.com/Turbo  
9 http://certifiedhacker.com/
```

Screengrab: Step 16 - Photon results – internal

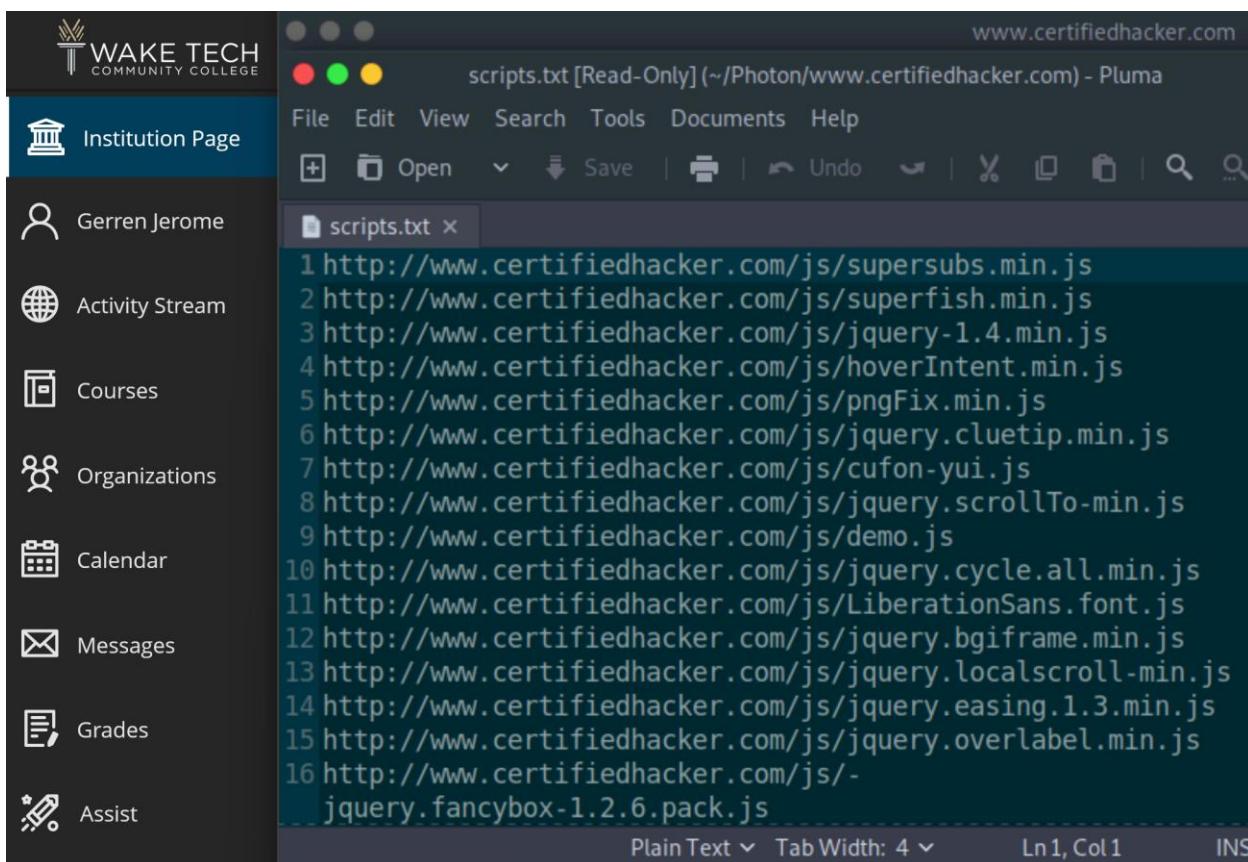


The screenshot shows a web browser window titled "internal.txt [Read-Only] (~/Photon/www.certifiedhacker.com) - Pluma". The browser interface includes a header with tabs, a menu bar (File, Edit, View, Search, Tools, Documents, Help), and a toolbar with various icons. The main content area displays a list of URLs:

```
1 http://www.certifiedhacker.com
2 http://www.certifiedhacker.com/index.html
3 http://www.certifiedhacker.com/
4 http://www.certifiedhacker.com/sample-login.html
```

The left sidebar of the browser shows the Wake Tech Community College navigation menu with links for Institution Page, Gerren Jerome, Activity Stream, Courses, and Organizations.

Screengrab: Step 16 - Photon results – scripts



The screenshot shows a web browser window titled "scripts.txt [Read-Only] (~/Photon/www.certifiedhacker.com) - Pluma". The browser interface includes a header with tabs, a menu bar (File, Edit, View, Search, Tools, Documents, Help), and a toolbar with various icons. The main content area displays a list of URLs:

```
1 http://www.certifiedhacker.com/js/supersubs.min.js
2 http://www.certifiedhacker.com/js/superfish.min.js
3 http://www.certifiedhacker.com/js/jquery-1.4.min.js
4 http://www.certifiedhacker.com/js/hoverIntent.min.js
5 http://www.certifiedhacker.com/js/pngFix.min.js
6 http://www.certifiedhacker.com/js/jquery.cluetip.min.js
7 http://www.certifiedhacker.com/js/cufon-yui.js
8 http://www.certifiedhacker.com/js/jquery.scrollTo-min.js
9 http://www.certifiedhacker.com/js/demo.js
10 http://www.certifiedhacker.com/js/jquery.cycle.all.min.js
11 http://www.certifiedhacker.com/js/LiberationSans.font.js
12 http://www.certifiedhacker.com/js/jquery.bgiframe.min.js
13 http://www.certifiedhacker.com/js/jquery.localscroll-min.js
14 http://www.certifiedhacker.com/js/jquery.easing.1.3.min.js
15 http://www.certifiedhacker.com/js/jquery.overlabel.min.js
16 http://www.certifiedhacker.com/-jquery.fancybox-1.2.6.pack.js
```

The left sidebar of the browser shows the Wake Tech Community College navigation menu with links for Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, and Assist.

c) Gather information about a target website using Central Ops

Screengrab: Step 3 – CentralOps results

The screenshot shows the CentralOps.net interface. On the left is a sidebar with user information (Geren Jerome) and various navigation links: Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, Sign Out, and Privacy. The main content area is titled "Domain Dossier" with the subtitle "Investigate domains and IP addresses". It shows a search bar with "domain or IP address" set to "www.certifiedhacker.com". Below the search bar are several checkboxes: "domain whois record" (checked), "DNS records" (checked), "traceroute" (unchecked), "network whois record" (checked), and "service scan" (unchecked). A "go" button is next to the checkboxes. Below these settings, it displays "user: anonymous [168.245.203.252]" and "balance: 46 units". At the bottom right of the main content area is the "centralops.net" logo.

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

canonical name certifiedhacker.com.
aliases www.certifiedhacker.com
addresses 162.241.216.11

Domain Whois record

Queried whois.internic.net with "dom certifiedhacker.com"...

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com

d) Extract a company's data using Web Data Extractor

Screengrab: Step 9 – WEDPro results

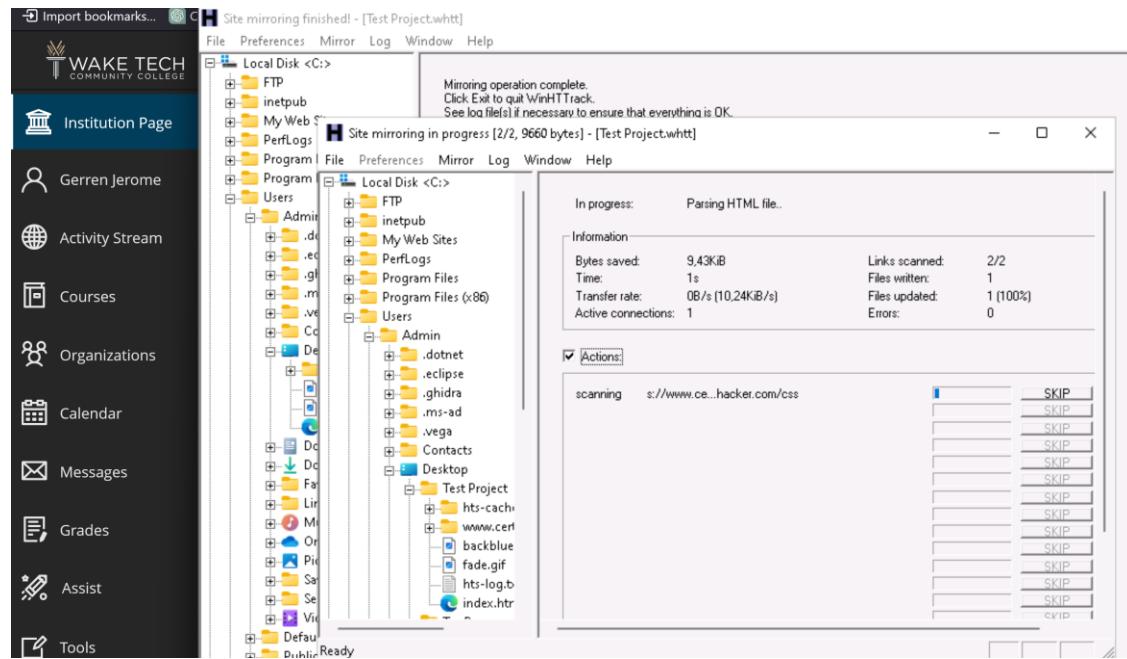
The screenshot shows the Web Data Extractor Pro 4.1 interface. On the left is a sidebar with user information (Geren Jerome) and various navigation links: Institution Page, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main content area has a title bar "Web Data Extractor Pro 4.1. Trial Version. You are on day 1 of your 15 day evaluation period." with standard window controls (minimize, maximize, close). Below the title bar are buttons for "new session", "edit session", "start", "pause", and "stop". To the right of these buttons is a progress bar showing "0 B/s" and an "options" button. The main interface is divided into sections: "Process log", "Results" (which is selected), "Bad URLs (12)", and "Stored Sessions". The "Results" section has tabs for "MetaTag (20)", "Email (10)", "Phone (130)", "Fax (129)", "Link (50)", and "Domain (1)". The "Results" table contains 20 rows of data, each with columns for Description, Keywords, Title, Url, and Host. The data includes various page titles and URLs from the certifiedhacker.com website, such as "Under the Trees", "Unite - Together is Better (...)", "Clear Construction", "Professional Real Estate S...", "Online Booking", "Turbo Max Theme - OwlTe...", "P-Folio", etc., all hosted on certifiedhacker.com.

Description	Keywords	Title	Url	Host
A brief description of this we...	keywords, or phrases, asso...	Certified Hacker	https://www.certifiedhacker.com/	certifiedhacker.com
		Under the Trees	https://certifiedhacker.com/corporate...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - Homepage	https://certifiedhacker.com/Under%20...	certifiedhacker.com
A brief description of this we...	keywords, or phrases, asso...	Unite - Together is Better (...)	https://certifiedhacker.com/Social%20...	certifiedhacker.com
Professional Real Estate Se...	real estate, real estate listin...	Professional Real Estate S...	https://certifiedhacker.com/Real%20...	certifiedhacker.com
Online Booking	booking, hotel, hotels, rese...	Online Booking	https://certifiedhacker.com/Online%20...	certifiedhacker.com
Turbo max powerful one pa...	Turbo max , owltemplates.c...	Turbo Max Theme - OwlTe...	https://certifiedhacker.com/Turbo%20...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - About us	https://certifiedhacker.com/P-Folio/in...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - Recipes d...	https://certifiedhacker.com/Recipes/...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - Menu	https://certifiedhacker.com/Recipes/...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - Recipes	https://certifiedhacker.com/Recipes/...	certifiedhacker.com
Online Booking	booking, hotel, hotels, rese...	Online Booking Sitemap	https://certifiedhacker.com/Online%20...	certifiedhacker.com
Online Booking	booking, hotel, hotels, rese...	Online Booking: Search	https://certifiedhacker.com/Online%20...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - Menu cate...	https://certifiedhacker.com/Recipes/...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - Recipes c...	https://certifiedhacker.com/Recipes/...	certifiedhacker.com
Online Booking	booking, hotel, hotels, rese...	Online Booking: Print Previ...	https://certifiedhacker.com/Online%20...	certifiedhacker.com
Online Booking	booking, hotel, hotels, rese...	Online Booking: Hotel Info	https://certifiedhacker.com/Online%20...	certifiedhacker.com

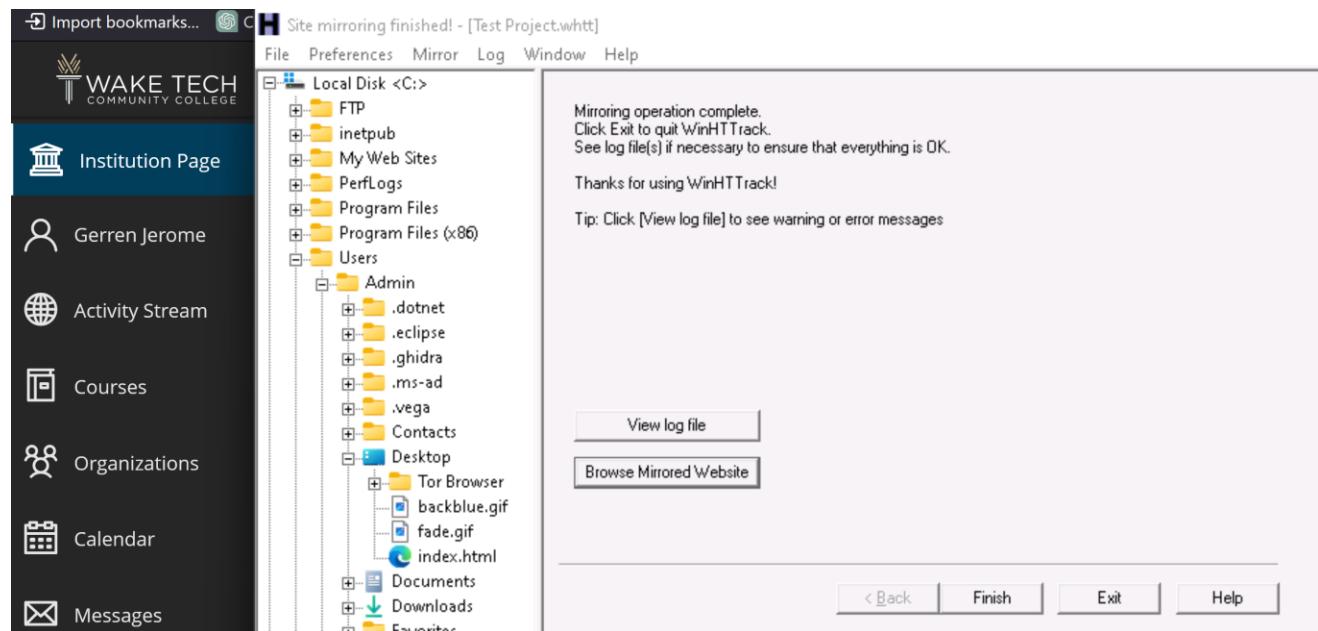
Processing time: 00:01:18.153 Sites processed: 67 / 83 Downloaded: 4,220 KB Avg. Speed: 390 KB/s

e) Mirror a target website using HTTrack Web Site Copier

Screengrab: Step 8 – Site mirroring progress



Screengrab: Step 11 – Completed mirroring results



f) Gather information about a target website using GRecon

Screengrab: Step 8 – GRecon results

```
python3 grecon.py - Parrot Terminal
[!] Switching Google TLDs...  
[>] Looking For Directory Listing...  
https://www.certifiedhacker.com/css/  
https://www.certifiedhacker.com/css/source/  
https://news.certifiedhacker.com/  
https://www.blog.certifiedhacker.com/  
https://iam.certifiedhacker.com/  
https://www.itf.certifiedhacker.com/  
https://fleet.certifiedhacker.com/  
https://www.sftp.certifiedhacker.com/  
[>] Looking For Public Exposed Documents...  
https://certifiedhacker.com/docs/923332.pdf  
https://certifiedhacker.com/docs/922990.pdf  
[>] Looking For WordPress Entries...  
[>] Looking in Pasting Sites...  
https://pastebin.com/KsT1zpQ0  
[>] Done...Happy Hunting  
[root@parrot]~[/home/attacker/GRecon]
```

g) Gather a wordlist from the target website using CeWL

Screengrab: Step 9 – Wordlist output from CeWL

```
wordlist.txt (~) - Pluma (as superuser)
File Edit View Search Tools Documents Help
+ Open Save Undo Undo Cut Copy Paste Find Replace
wordlist.txt x
1 Slide
2 Login
3 Content
4 Hacker
5 jQuery
6 Cycle
7 default
8 cufón
9 document
10 close
11 member
12 Register
13 account
14 Links
15 Copyright
16 Found
17 Certfied
18 Favorites
19 Style
```

5) Perform email footprinting (2 items)

a) Gather information about a target by tracing emails using eMailTrackerPro

Screengrab: Step 13 – Tracing email header (Map and Summary)

The trace is complete, the information found is displayed on the right

Email Summary

From: 984239084569834576834@substack.com
To: unhinge.gj@gmail.com
Date: Fri, 26 Jan 2024 01:38:06 +0000
Subject: Important: Last Reminder for KYC Verification on Yo
Location: San Antonio, TX

Misdirected: No
Abuse Address: abuse@mailgun.org
Abuse Reporting: To automatically generate an email abuse
From IP: 161.38.197.240

System Information:

- There is no SMTP server running on this system (the)
- There is no HTTP server running on this system (the)
- There is no HTTPS server running on this system (the)
- There is no FTP server running on this system (the)

Network Whois

Domain Whois

Email Header

#	Hop IP	Hop Name	Location
1	10.10.1.2		
2	172.18.0.1		
3	192.168.0.1		
4	103.186.82.26	{Europe}	
5	103.186.82.3	{Europe}	
6	38.104.207.233	gi0-1-1-15.rcr21.iad01.atlas.cogeeDulles, VA, USA	
7	154.54.30.193	be2956.ccr41.iad02.atlas.cogeeDulles, VA, USA	
8	154.54.30.53	be3083.ccr41.dca01.atlas.cogenyWashington, DC, USA	
9	154.54.7.158	be2112.ccr41.at01.atlas.cogenyWashington, DC, USA	

You are on day 1 of a 15 day trial. To apply a licence [Click here](#) or for purchase information [Click here](#)

Screengrab: Step 13 – Tracing email header (Report)

eMailTrackerPro® Report

How to Report Email Abuse | eMailTrackerPro Manual | FAQ | Visualware Home | eMailTrackerPro Website | purchase eMailTrackerPro

Identification Report for 'Important: Last Reminder for KYC Verific'

You are on day 101 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to [purchase a product license](#) from the Visualware website or authorized reseller.

Computer 161.38.197.240 has been found. It is probably located in or around San Antonio, TX as this is where the organization or individual who manages the system is located.

Network Contact Information: The following details refer to the network that the system is on.

Mailgun Technologies Inc.
abuse@mailgun.org
+1-888-571-8972
112 E Pecan St. #1135 San Antonio TX 78205 US

[Click here to hide the in-depth information on this email \(more info\)](#)

- The sender's IP in this case is taken from a 'Received' header stamp from a different server to the one the sender first communicated with because the IP in that line was not usable. The closest tracable IP to the sender was - 161.38.197.240
- The sender of this email appeared to have the address 984239084569834576834@substack.com. This

6) Perform Whois footprinting (1 item)

a) Perform Whois lookup using DomainTools

Screengrab: Step 3 – WHOIS Records

The screenshot shows the DomainTools website interface. On the left is a sidebar with the Wake Tech Community College logo and links for Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, Sign Out, and Privacy. The main content area shows the WHOIS Record for CertifiedHacker.com. The record includes details such as Registrar (Network Solutions, LLC), Registrar Status (clientTransferProhibited), Dates (7,851 days old, Created 2002-07-30, Expires 2024-07-30, Updated 2023-08-22), Name Servers (NS1.BLUEHOST.COM, NS2.BLUEHOST.COM), IP Address (162.241.216.11), and IP Location (Utah - Provo - Unified Layer). To the right, there are sections for DomainTools Iris (Domain intelligence platform), Tools (Hosting History, Monitor Domain Properties, Reverse IP Address Lookup, Network Tools), and a preview of the full domain report.

7) Perform DNS footprinting (6 items)

a) Gather DNS information using nslookup command line utility and online tool

Screengrab: Step 12 – DNS recon with nslookup

The screenshot shows a terminal window titled "Select Command Prompt - nslookup". The user has run the command "nslookup" and is interacting with it via the command line. The output shows the configuration of the nslookup client, including setting the type to cname and specifying the server as dns.google. It then queries the domain certifiedhacker.com, which returns a non-authoritative answer from ns1.bluehost.com with the IP address 162.159.24.80. The user also attempts to query ns1.bluehost.com directly, which fails due to a connection error.

```
> set type=cname
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

certifiedhacker.com
primary name server = ns1.bluehost.com
responsible mail addr = dnsadmin.box5331.bluehost.com
serial = 2024011800
refresh = 86400 (1 day)
retry = 7200 (2 hours)
expire = 3600000 (41 days 16 hours)
default TTL = 300 (5 mins)

> set type=a
error> ns1.bluehost.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: ns1.bluehost.com
Address: 162.159.24.80

20020
The
real:
d=
```

Screengrab: Step 18 – KLOTH.NET results

The screenshot shows a sidebar with user information and a list of links: Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main content area is titled "NSLOOKUP: look up and find IP addresses in the DNS". It includes a query form with fields for Domain (certifiedhacker.com), Server (localhost), and Query type (A (IPv4 address)). A "Look it up" button is present. Below the form, a text box displays the nslookup result for certifiedhacker.com from server localhost, querytype=A:

```
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
```

[Query 1 of max 100]

b) Perform reverse DNS lookup using reverse IP domain check and DNSRecon

Screengrab: Step 3 – yougetsignal.com results

The screenshot shows a sidebar with user information and a list of links: Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main content area is titled "you get signal" and "Reverse IP Domain Check". It features a "Remote Address" input field containing www.certifiedhacker.com and a "Check" button. Below the input field, a message states "Found 15 domains hosted on the same web server as www.certifiedhacker.com (162.241.216.11)." A list of these domains is provided, along with a note about the database size and a link to purchase a domain list.

Reverse IP Domain Check

Remote Address Check

Found 15 domains hosted on the same web server as www.certifiedhacker.com (162.241.216.11).

100wwcbeaufort.org	biosis.ae
bongekile.com	box5331.bluehost.com
certifiedhacker.com	certifiedhacker.com
eis.qa	gaelicmemoriesphotography.ie
humancarehealth.com	mail.certifiedhacker.com
oakoffer.com	throntonchipsdepotencia.com
www.certifiedhacker.com	www.certifiedhacker.com
www.lsstl.org	

about

Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this [domain list for purchase](#).

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual [reverse IP](#) lookup tool. Knowing the other web sites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on [shared web hosting](#) plans.

[More about this tool.](#) [Set an API Key](#)

help me pay for school (PayPal)

Screengrab: Step 8 – DNSRecon results

```
[attacker@parrot] -[~/dnsrecon]
└─$ ./dnsrecon.py -r 162.241.216.0-162.241.216.255
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[+] PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
[+] PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
[+] PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
[+] PTR 162-241-216-7.unifiedlayer.com 162.241.216.7
[+] README.PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
[+] PTR box5331.bluehost.com 162.241.216.11
[+] PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
[+] PTR 5tIYGWP8Ew8 162.241.216.0
[+] PTR 162-241-216-13.unifiedlayer.com 162.241.216.13
[+] PTR 162-241-216-10.unifiedlayer.com 162.241.216.10
[+] PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[+] PTR 162-241-216-16.unifiedlayer.com 162.241.216.16
[+] PTR box5348.bluehost.com 162.241.216.17
[+] EHv12 M PTR 162-241-216-19.unifiedlayer.com 162.241.216.19
[+] HackingPTR 162-241-216-18.unifiedlayer.com 162.241.216.18
[+] ServePTR box5350.bluehost.com 162.241.216.20
[+] PTR 162-241-216-8.unifiedlayer.com 162.241.216.8
[+] PTR 162-241-216-21.unifiedlayer.com 162.241.216.21
[+] PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
[+] EHv12 M PTR 162-241-216-12.unifiedlayer.com 162.241.216.12
[+] HackingPTR 162-241-216-26.unifiedlayer.com 162.241.216.26
```

c) Gather information of subdomain and DNS records using SecurityTrails

Screengrab: Step 9 – SecurityTrails search results

The screenshot shows the SecurityTrails web interface. On the left is a dark sidebar with user navigation links: Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main content area displays the results of a DNS record search for the domain `certifiedhacker.com`. The results are presented in two sections: **A records** and **AAAA records**.

A records:

- Unified Layer
- 162.241.216.11

AAAA records:

- 162.241.216.11

At the bottom of the main content area, there is a message: "Unlock all access to Cybersecurity and DNS intelligence data and mitigate risk." Below this message are two buttons: "Upgrade to SurfaceBrowser™ now!" and "Activate W".

Screengrab: Step 10 – Historical data (A Record)

The screenshot shows a user profile on the left with options like Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main area displays historical A record data for the domain `certifiedhacker.com`. The search bar at the top shows "certifiedhacker.com historical A data". Below it is a table with columns: IP Addresses, Organization, First Seen, Last Seen, and Duration Seen. The table contains three entries:

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
162.241.216.11	Unified Layer	2017-11-14 (6 years)	2024-01-27 (today)	6 years
69.89.31.193	Unified Layer	2016-12-31 (7 years)	2017-11-14 (6 years)	11 months
69.89.31.193	Unified Layer	2016-12-25 (7 years)	2016-12-30 (7 years)	5 days

8) Perform network footprinting (3 items)

a) Locate the network range

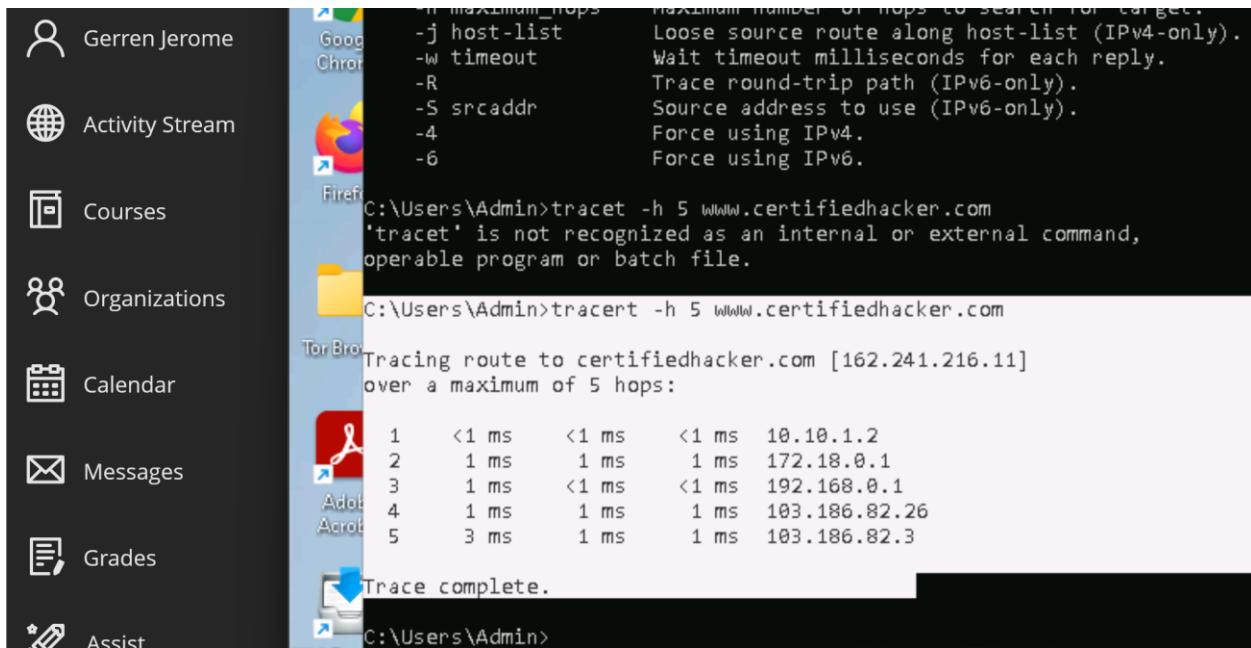
Screengrab: Step 3 – ARIN.net search results

The screenshot shows a user profile on the left with options like Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main area is the ARIN Whois/RDAP search results for the IP address `162.241.216.11`. The search bar at the top shows "162.241.216.11". The results page title is "ARIN Whois/RDAP". It includes a search bar with the result "162.241.216.11" and a "Search" button. There are links to "Search www.arin.net instead" and "Search Filter: Automatic". A note states "all requests subject to [terms of use](#)". The main content area shows the network information for "Network: NET-162-240-0-0-1":

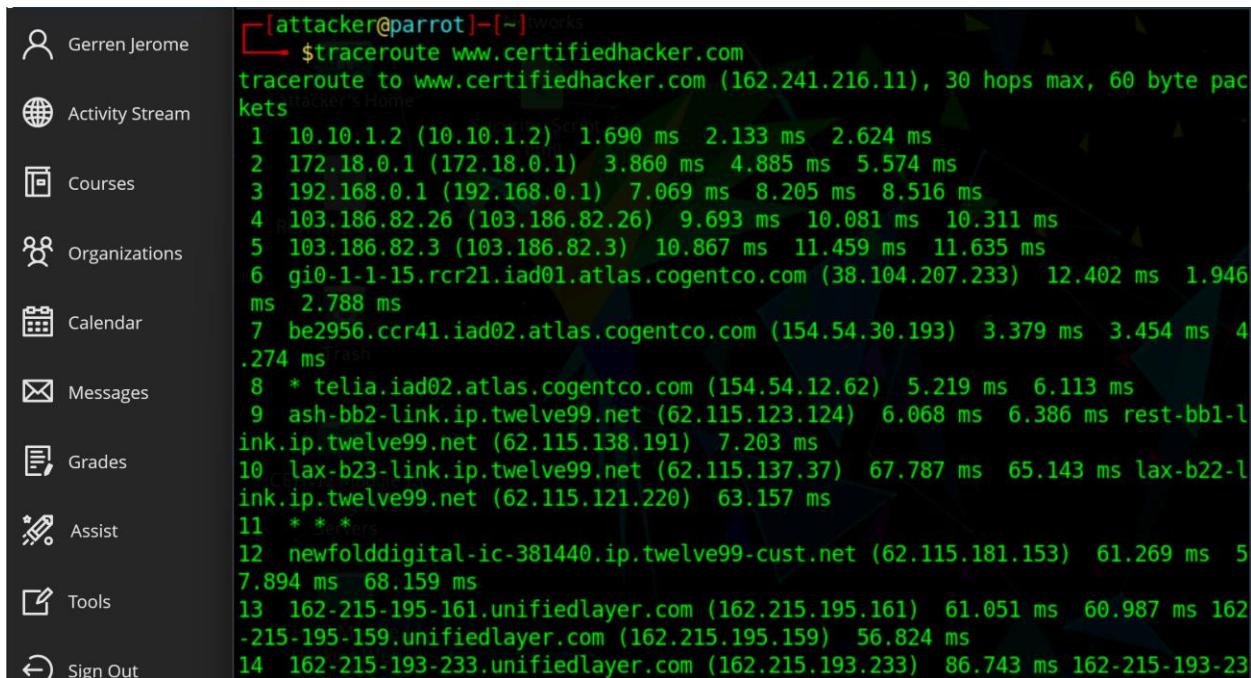
Source Registry	ARIN
Net Range	162.240.0.0 - 162.241.255.255
CIDR	162.240.0.0/15
Name	UNIFIEDLAYER-NETWORK-16
Handle	NET-162-240-0-0-1
Parent	NET-162-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	AS46606

b) Perform network tracerouting in Windows and Linux Machines

Screengrab: Step 3 – tracert results (WIN)



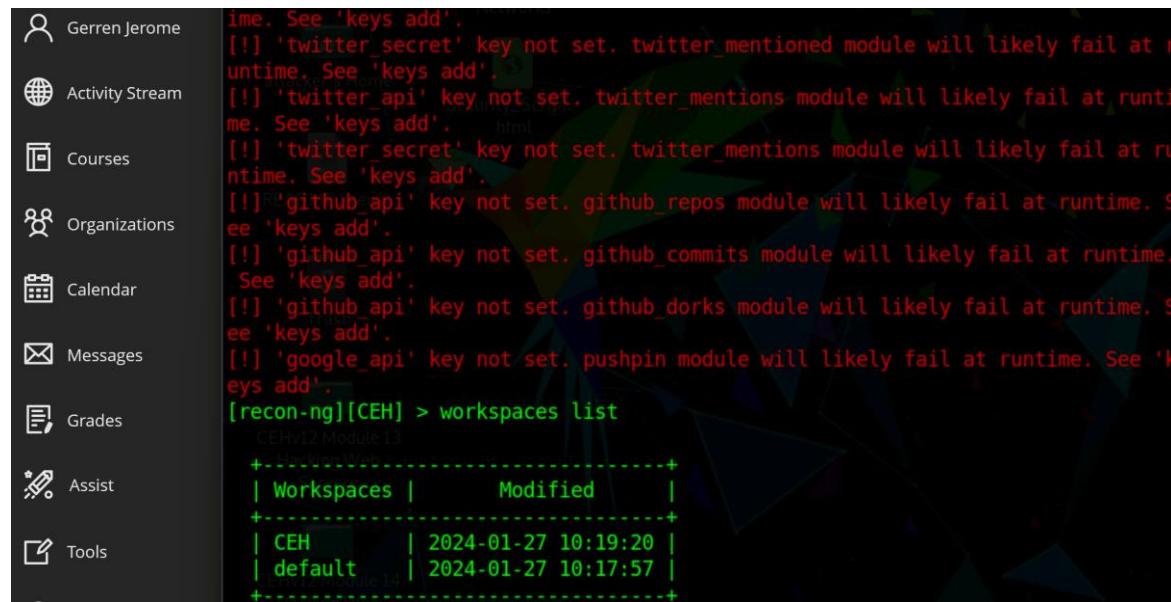
Screengrab: Step 7 - traceroute results (LNX)



9) Perform footprinting using various footprinting tools (19 items)

a) Footprinting a target using Recon-ng

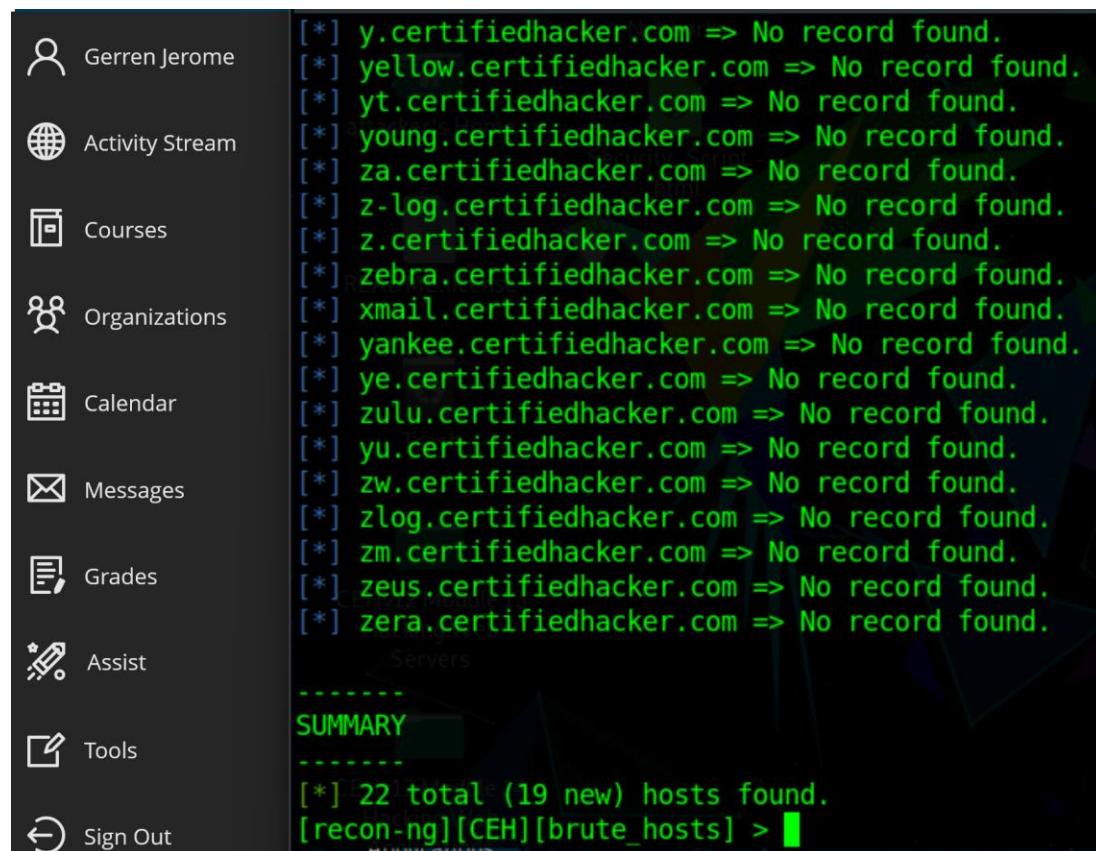
Screengrab: Step 14 – confirm created workspace



The screenshot shows the Recon-ng interface with a sidebar containing links like Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main area displays a command-line interface with several warning messages about missing API keys for various modules (twitter, github, google). Below this, the command [recon-ng][CEH] > workspaces list is run, showing a table of workspaces:

Workspaces	Modified
CEH	2024-01-27 10:19:20
default	2024-01-27 10:17:57

Screengrab: Step 23 – recon-ng results (brute_hosts)



The screenshot shows the Recon-ng interface with the same sidebar as the previous screenshot. The main area displays the output of the [recon-ng][CEH][brute_hosts] command. It lists numerous hosts (y.certifiedhacker.com, yellow.certifiedhacker.com, etc.) with the message "No record found" for each. At the bottom, it shows a summary and the total number of hosts found.

```
[*] y.certifiedhacker.com => No record found.  
[*] yellow.certifiedhacker.com => No record found.  
[*] yt.certifiedhacker.com => No record found.  
[*] young.certifiedhacker.com => No record found.  
[*] za.certifiedhacker.com => No record found.  
[*] z-log.certifiedhacker.com => No record found.  
[*] z.certifiedhacker.com => No record found.  
[*] zebra.certifiedhacker.com => No record found.  
[*] xmail.certifiedhacker.com => No record found.  
[*] yankee.certifiedhacker.com => No record found.  
[*] ye.certifiedhacker.com => No record found.  
[*] zulu.certifiedhacker.com => No record found.  
[*] yu.certifiedhacker.com => No record found.  
[*] zw.certifiedhacker.com => No record found.  
[*] zlog.certifiedhacker.com => No record found.  
[*] zm.certifiedhacker.com => No record found.  
[*] zeus.certifiedhacker.com => No record found.  
[*] zera.certifiedhacker.com => No record found.  
  
-----  
SUMMARY  
-----  
[*] 22 total (19 new) hosts found.  
[recon-ng][CEH][brute_hosts] >
```

Screengrab: Step 29 – harvested host results (Attacker Window)

```
-----  
SUMMARY  
-----  
[*] 1 total (1 new) hosts found.  
[recon-ng][CEH][reverse_resolve] > show hosts  
+-----+  
| rowid | host | ip_address | region | country |  
| latitude | longitude | notes | module |  
+-----+  
| 1 | autodiscover.certifiedhacker.com | 162.241.216.11 | | |  
| 2 | blog.certifiedhacker.com | 162.241.216.11 | | |  
| 3 | events.certifiedhacker.com | 162.241.216.11 | | |  
| 4 | certifiedhacker.com | | | brute_hosts |  
| 5 | ftp.certifiedhacker.com | | | brute_hosts |  
| 6 | ftp.certifiedhacker.com | 162.241.216.11 | | |  
+-----+
```

Screengrab: Step 43 - harvested host results (HTML report)

Recon-ng Reconnaissance Report

host	ip_address	region	country	latitude	longitude	notes
autodiscover.certifiedhacker.com	162.241.216.11					
blog.certifiedhacker.com	162.241.216.11					
box5331.bluehost.com	162.241.216.11					
certifiedhacker.com						
events.certifiedhacker.com	162.241.216.11					
ftp.certifiedhacker.com						
imap.certifiedhacker.com	162.241.216.11					
imap.certifiedhacker.com	162.241.216.11					
localhost.certifiedhacker.com	127.0.0.1					
mail.certifiedhacker.com						
mail.certifiedhacker.com	162.241.216.11					
news.certifiedhacker.com	162.241.216.11					
pop.certifiedhacker.com						
pop.certifiedhacker.com	162.241.216.11					
smtb.certifiedhacker.com						

Screengrab: Step 56 – WHOIS_POCS results

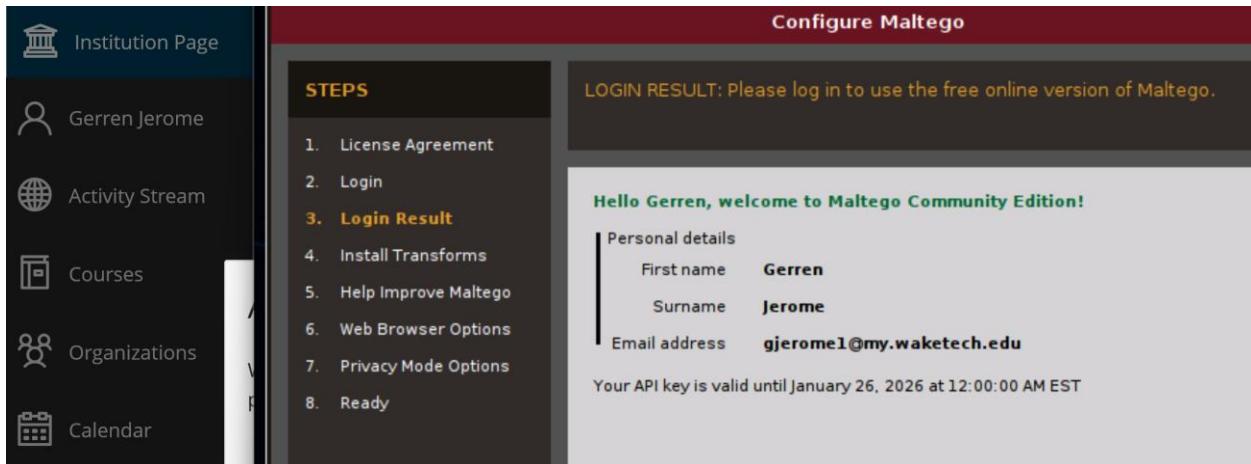
```
[recon-ng][reconnaissance][whois_pocs] > run Networks
-----
FACEBOOK.COM
Attacker's Home
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*]
-----
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
```

Screengrab: Step 66 – HackerTarget results

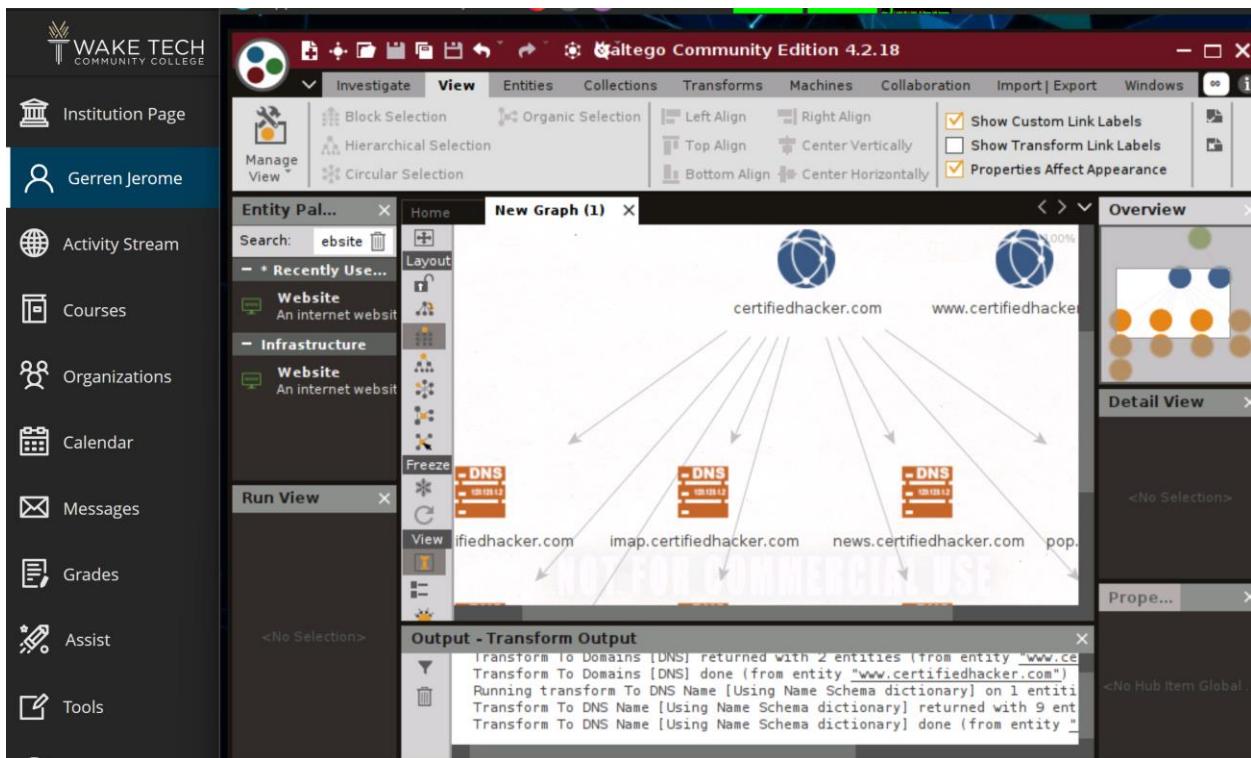
 Gerren Jerome	[recon-ng][default][hackertarget] > run ----- CERTIFIEDHACKER.COM ----- [*] Country: None ois.arin.net/rest/pocs;domain=facebook.com [*] Host: autodiscover.certifiedhacker.com [*] Ip_Address: 162.241.216.11 [*] Latitude: None Random [*] Longitude: None [*] Notes: None None [*] Region: None [*] ----- [*] Country: None go.il [*] Host: blog.certifiedhacker.com [*] Ip_Address: 162.241.216.11 [*] Latitude: None ois.arin.net/rest/poc/OPERA82-ARIN [*] Longitude: None United States [*] Notes: None in@facebook.com [*] Region: None None [*] ----- [*] Country: None
 Activity Stream	
 Courses	
 Organizations	
 Calendar	
 Messages	
 Grades	
 Assist	
 Tools	

b) Footprinting a target using Maltego

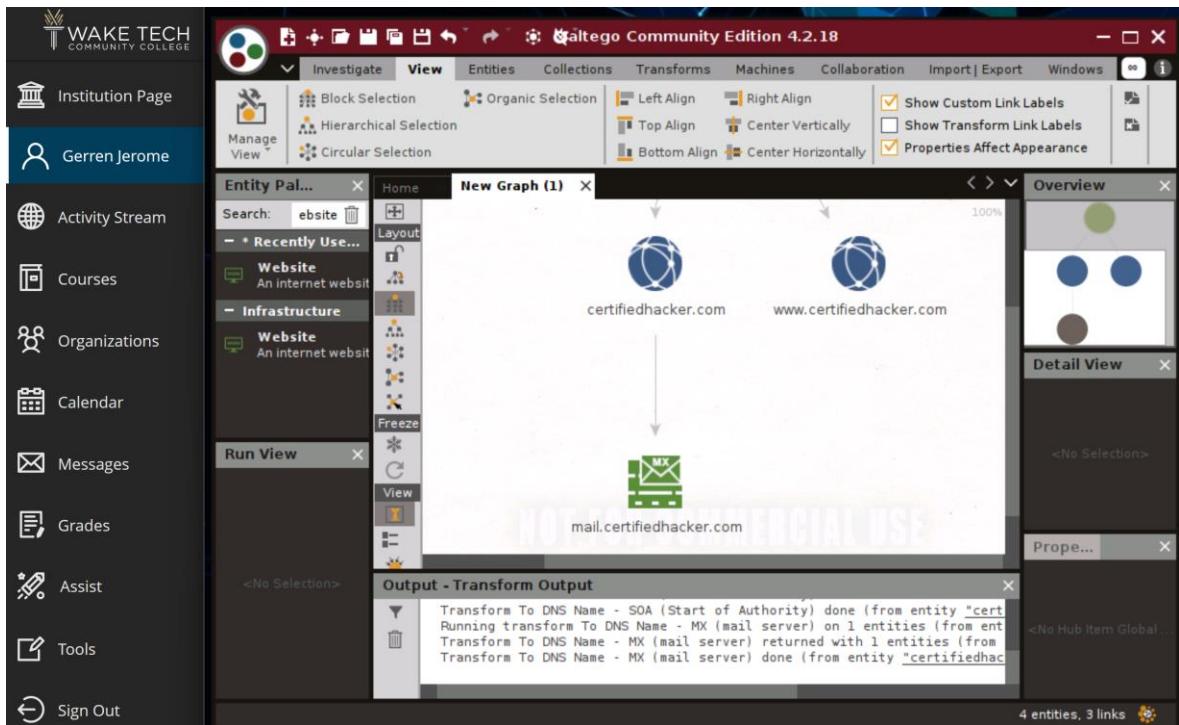
Screengrab: Step 11 – Login Successful



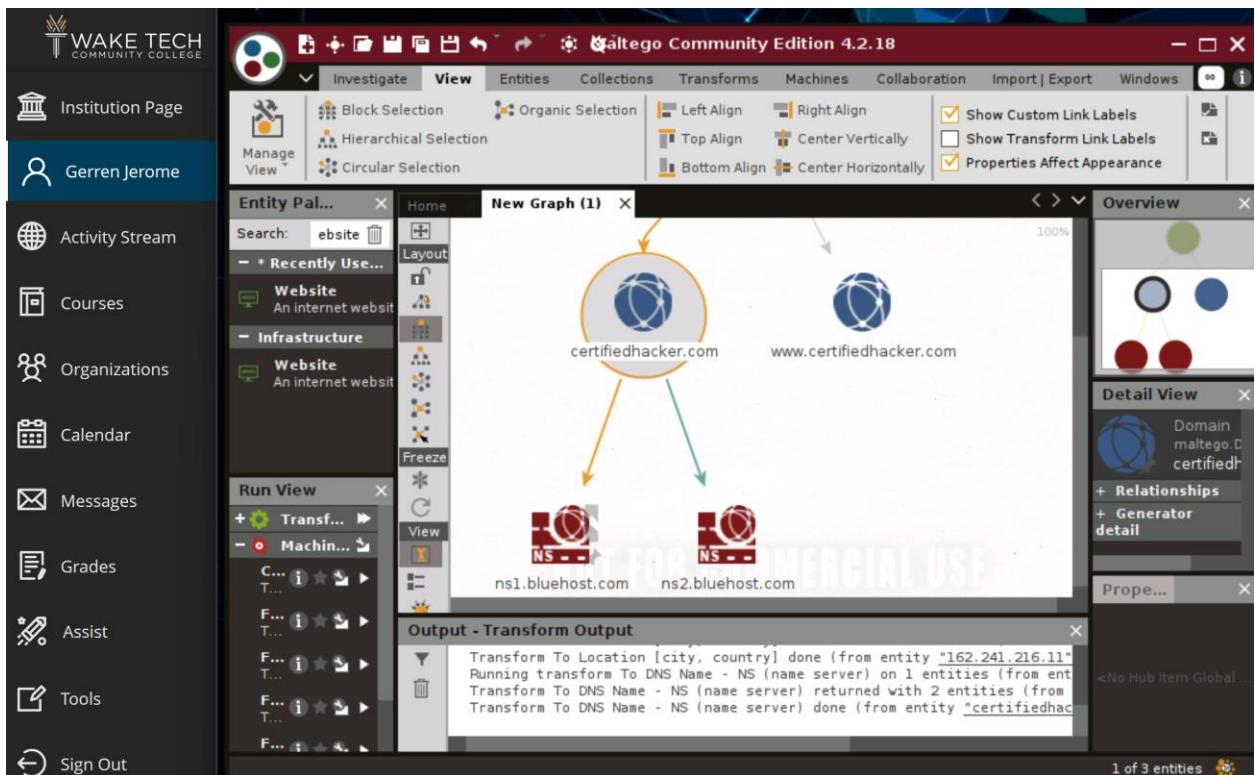
Screengrab: Step 27 – Transform (DNS) – identify and parse



Screengrab: Step 35 – Transform (MX) - identify and parse



Screengrab: Step 39 – Transform (NS) - identify and parse



Screengrab: Step 46 – Location (city, country)

The screenshot shows the Galtego Community Edition interface. On the left is a sidebar with links: Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main area is titled "New Graph (1)" and displays a network diagram. A central node is labeled "162.241.216.11". Below it is a location pin labeled "(United States)". To the right is an "Overview" panel with three colored circles (green, yellow, red) and a "Detail View" panel showing "<No Selection>". At the bottom is an "Output - Transform Output" panel with the following text:

```
Transform To IP Address [DNS] done (from entity "www.certifiedhacker.com")
Running transform To Location [city, country] on 1 entities (from entity
Transform To Location [city, country] returned with 1 entities (from ent
Transform To Location [city, country] done (from entity "162.241.216.11")
```

c) Footprinting a target using OSRFramework

Screengrab: Step 6 – Domainfy results

The screenshot shows the OSRFramework interface. The sidebar on the left includes: Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main window displays the output of a "Domainfy" command. The output is timestamped "2024-01-27 11:42:05.709880" and shows "24 results obtained:".

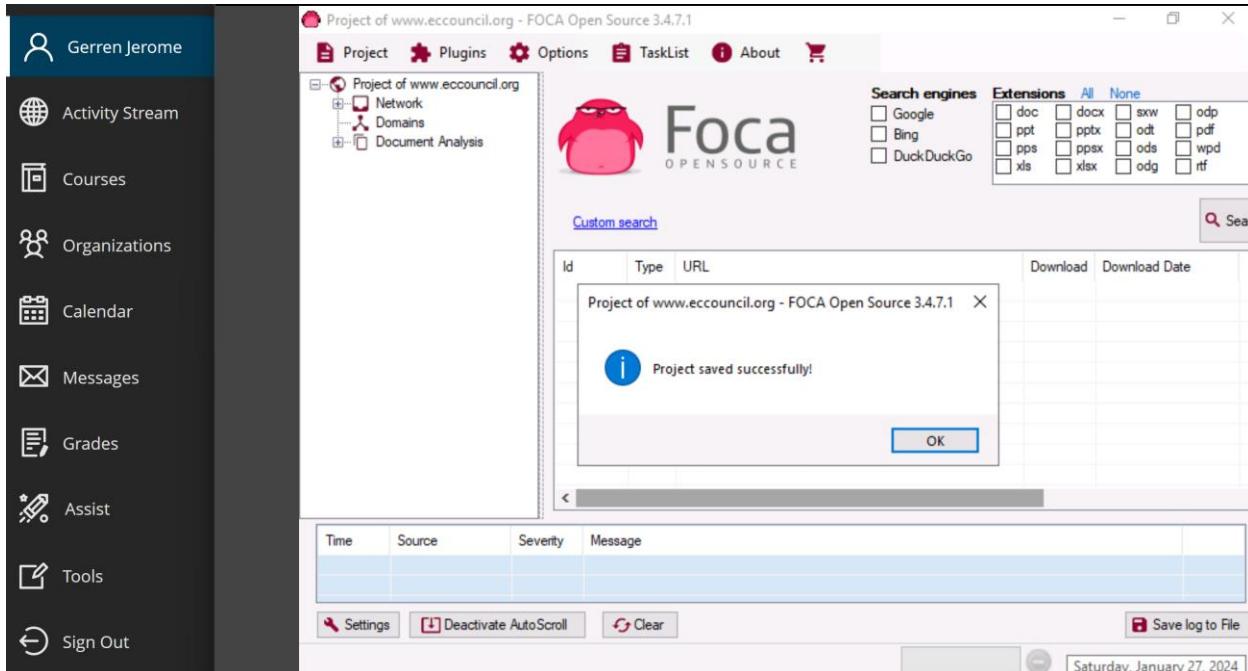
Sheet Name	Objects recovered (2024-1-27_11h42m).
com.i3visio.Domain	com.i3visio.IPv4
eccouncil.com	104.18.22.3
eccouncil.org	104.18.8.180
eccouncil.net	208.91.197.27
eccouncil.tv	66.129.123.226
eccouncil.co	18.233.124.157
eccouncil.pk	104.21.23.138
eccouncil.in	162.241.85.161
eccouncil.us	208.91.197.27

Screengrab: Step 8 – Searchfy results

A screenshot of a terminal window titled "searchfy -q \"Tim Cook\" - Parrot Terminal". The command "searchfy -q \"Tim Cook\" - Parrot Terminal" was run at 2024-01-27 11:43:52.407852. The results obtained show a network diagram with nodes like "com.i3visio.Platform", "com.i3visio.Email", "com.i3visio.URI", "com.i3visio.Alias", and "com.i3visio.Domain". It also lists several email addresses and their corresponding URLs, such as "cooktim800@gmail.com" and "tkcook@bigfoot.com".

d) Footprinting a target using FOCA

Screengrab: Step 8 – Project saved successfully!



Screengrab: Step 12 – Search All results

The screenshot shows the FOCA Open Source interface on a Windows Server 2019 system. The left sidebar contains links for Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main window displays the 'Project of www.eccouncil.org' with a tree view under 'Project'. The 'Network' node has 'Clients (0)' and 'Servers (0)' listed. The 'Domains' node has 'eccouncil.org' listed. The 'Document Analysis' node is collapsed. On the right, there's a search configuration section with 'Search engines' (Google, Bing, DuckDuckGo) and 'Extensions' (doc, docx, ppt, pptx, pps, ppsx, xls, xlsx, odt, ods, wpd, odg, rtf) checkboxes. Below it is a 'Custom search' table showing search results:

ID	Type	URL	Download	Download Date
0	pdf	https://www.eccouncil.org/wp-content/uploads/2023/0...	x	-
1	pdf	https://www.eccouncil.org/wp-content/uploads/2023/0...	x	-
2	pdf	https://www.eccouncil.org/wp-content/uploads/2023/1...	x	-
3	pdf	https://www.eccouncil.org/wp-content/uploads/2023/0...	x	-
4	pdf	https://www.eccouncil.org/wp-content/uploads/2022/1...	x	-
5	pdf	https://www.eccouncil.org/wp-content/uploads/2022/1...	x	-
6	pdf	https://www.eccouncil.org/wp-content/uploads/2023/0...	x	-
7	pdf	https://www.eccouncil.org/wp-content/uploads/2016/0...	x	1

Below the table is a log table:

Time	Source	Severity	Message
8:54:49 ...	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden..
8:54:52 ...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 0
8:54:52 ...	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 74

At the bottom are buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File.

Screengrab: Step 20 – Crawling results

The screenshot shows the FOCA Open Source interface on a Windows Server 2019 system. The left sidebar contains links for Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main window displays the 'Project of www.eccouncil.org' with a tree view under 'Project'. The 'Network' node has 'Clients (0)' and 'Servers (0)' listed. The 'Domains' node has 'eccouncil.org' listed. The 'Document Analysis' node is collapsed. On the right, there's a 'Technology recognition' section with tabs for Crawling (selected), Log, Google, Bing, and DuckDuckGo. Below it is a table for the domain 'eccouncil.org':

Files (0 found)	Folders (0 found)	Documents published (0 found)	Parameterized (0 found)
File			

Below the table is a log table:

Time	Source	Severity	Message
8:58:54 ...	Crawling	medium	Domain found: aware.eccouncil.org
8:58:54 ...	Crawling	medium	Domain found: cert.eccouncil.org
8:58:54 ...	Crawling	medium	Domain found: cyberbrief.eccouncil.org
8:58:55 ...	Crawling	medium	Domain found: cyberq.eccouncil.org
8:58:55 ...	Crawling	medium	Domain found: accesscomputertraining.eccouncil.org
8:58:56 ...	Crawling	medium	Domain found: campaigns.eccouncil.org
8:58:56 ...	Crawling	medium	Domain found: cybersmoothmarketing.eccouncil.org

At the bottom are buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File. A status bar at the bottom right shows the date: Saturday, January 27, 2024.

e) Footprinting a target using BillCipher (**NSFW language in the interface)

Screengrab: Step 10 – Results: DNS Lookup

```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
4) Subnet Lookup 16
5) Port Scanner 17
6) Page Links 18
oud)
7) Zone Transfer 19
8) HTTP Header 20
9) Host Finder 21
10) IP-Locator 22
11) Find Shared DNS Servers
12) Get Robots.txt

What information would you like to collect? (1-20): 1
A : 162.241.216.11
MX : 0 mail.certifiedhacker.com.
NS : ns1.bluehost.com.
NS : ns2.bluehost.com.
TXT : "v=spf1 a mx ptr include:bluehost.com ?all"
CNAME : certifiedhacker.com.
CEHv20_2024011800_86400_7
Ha200 3600000 300
servers
Do you want to continue? [Yes/No]:
```

Screengrab: Step 15 – Results: GeolP Lookup

```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
2) Whois Lookup 16
3) GeoIP Lookup 17
4) Subnet Lookup 18
5) Port Scanner 19
6) Page Links 20
oud)
7) Zone Transfer 21
8) HTTP Header 22
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt

What information would you like to collect? (1-20): 3
IP Address: 162.241.216.11
Country: United States
State:
City:
CEHv20_2024011800_86400_7
HaLongitude: -97.822
servers
Do you want to continue? [Yes/No]:
```

Screengrab: Step 20 - Results: Subnet Lookup

python3 billcipher.py - Parrot Terminal

File Edit View Search Terminal Help

4) Subnet Lookup Module 16 16) Subdomain listing (use Sublist3r)
5) Port Scanner 17) Find Admin login site (use Breacher)
6) Page Links Networks 18) Check and Bypass CloudFlare (use Hat
oud) 19) Website Copier (use httrack)
7) Zone Transfer 20) Host Info Scanner (use WhatWeb)
8) HTTP Header 21) About BillCipher
9) Host Finder 22) Fuck Out Of Here (Exit)
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt

What information would you like to collect? (1-20): 4

Address = 162.241.216.11
Network = 162.241.216.11 / 32
Netmask = 255.255.255.255
Broadcast = not needed on Point-to-Point links
Wildcard Mask = 0.0.0.0
Hosts Bits = 0
Max. Hosts = 1 (2^0 - 0)
Host Range = { 162.241.216.11 - 162.241.216.11 }

Do you want to continue? [Yes/No]:

f) Footprinting a target using OSINT Framework

Eyes only