

Gerren Jerome

Footprinting and Reconnaissance

1. Perform footprinting through search engines (8 items)

- a) Gather information using advanced Google hacking techniques.

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:

- eccouncil.org https://aspen.eccouncil.org > Account > Login
- Login - ASPEN - EC-Council**
Type your username and password. Login. Username *. Password *.
- eccouncil.org https://coded.eccouncil.org > login
- 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 ...
- eccouncil.org https://ilabs.eccouncil.org > login
- Login to iLabs**
May 18, 2017 — Get Connected to iLabs. Anytime. Anywhere. CEHproductimage · Computer Forensics Exercises · Security Analyst Exercises · Ec-Council Secure ...

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 the "CEH-brochure.pdf" document from EC-Council:

- EC-Council https://www.eccouncil.org > uploads > 2022/09 PDF
- 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

Below the results, there is a "People also ask" section with three expandable questions:

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

CEH-brochure.pdf

The screenshot shows a PDF viewer interface with a dark theme. On the left is a sidebar with navigation links: Gerren Jerome, Activity Stream, Courses (selected), Organizations, Calendar, Messages, Grades, Assist, Tools, Sign Out, and Privacy. The main area displays a PDF document titled "The All-New CEH v12". The cover features a purple and blue background with binary code patterns. The EC-Council logo is at the top right, and the title "The All-New CEH v12" is centered below it. The PDF content includes several sections and images related to the course.

Gather information from video search engines.

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

The mattw.io Snippet section

The screenshot shows a snippet of a video from mattw.io. The sidebar on the left is identical to the one in the previous screenshot. The main area shows a snippet titled "Bad, Good, and Best Password Practices: Preventing Dictionary-Based Attacks - Part 2". The snippet includes a thumbnail image of a man, the title, and a snippet of the video's JSON metadata. The URL for the video is also visible at the bottom.

```
{ "publishedAt": "2024-01-25T13:45:53Z", "channelId": "UCHf4HMh2W5S1Shi1N442-cA", "title": "Bad, Good, and Best Password Practices: Preventing Dictionary-Based Attacks: Part 2", "description": "Password protection requires maximum efficacy to prevent dictionary attacks from", "thumbnails": { "default": { "url": "https://i.ytimg.com/vi/f_iVuHgCToA/default.jpg", 
```

Bad, Good, and Best Password Practices: Preventing Dictionary-Based Attacks - Part 2

Reverse Image Search

The screenshot shows a user interface for a reverse image search. On the left is a vertical sidebar with a dark theme containing the following items:

- User profile: Gerren Jerome
- Activity Stream
- Courses** (highlighted in blue)
- Organizations
- Calendar
- Messages
- Grades
- Assist
- Tools
- Sign Out

The main area features a search bar with the text "Google" and a "Find image source" button. Below the search bar is a large thumbnail image of a presentation slide titled "Bad, Good, and Best Password Practices: Preventing Dictionary-Based Attacks - Part 2". The slide is from EC-Council CYBER TALKS. At the bottom of the main area are three buttons: "Search", "Text", and "Translate". To the right of the main area is a sidebar with the following sections:

- Upload** (with an upload icon)
- YouTube** (listing "People v. Jackson — The Complete 200...")
- Prime & Probe**
- Cache Attack**
- Hibernate example with Service and DAO(Data access object) Layer PART1**
- YouTube** (listing "Hibernate Example with Service and...")
- Message to ASD**
- Spouses: Were you...**
- Videos**
- AI**

Gather information from FTP search engines

NAPALM-FTP search results.

The screenshot shows the NAPALM-FTP indexer search results for the query "microsoft". The interface has a dark theme and includes the following elements:

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

Search Results:

File Path	Size	Action
/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
/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/libmono-system-json-microsoft4.0-cil_6.8.0.105+dfsg-3.3~deb10u1_all.deb	56.6 KB	DOWNLOAD
/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
/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/libmono-system-json-microsoft4.0-cil_5.18.0.240+dfsg-3+deb10u1_all.deb	55.1 KB	DOWNLOAD
/pub/3/archive.raspbian.org/raspbian/pool/main/m/mono/libmono-system-json-microsoft4.0-cil_5.18.0.240+dfsg-3+deb10u1_all.deb	121 KB	DOWNLOAD

Gather information from IoT search engines

shodan.io search results.

The screenshot shows the Shodan search interface. On the left is a sidebar with user navigation (Profile, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, Sign Out, Privacy) and a dark mode switch. The main area has a header with the Shodan logo, navigation links (Explore, Pricing), and a search bar with the query 'amazon'. Below the header is a 'TOTAL RESULTS' section showing '236,909' results. A 'TOP COUNTRIES' section lists the United States (113,649), Japan (35,454), Ireland (15,495), India (10,738), and Singapore (9,115). Two specific search results are shown: one for IP 54.196.179.133 (Amazon Linux, United States, Ashburn, cloud) and another for IP 34.213.212.180 (Amazon Technologies Inc., United States, West Virginia, cloud).

Perform footprinting through web services

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

Netcraft site report

The screenshot shows the Netcraft site report for 'Cybersecurity Courses Online | Best Cybersecurity Training'. The report includes sections for 'Background' (Site title: Cybersecurity Courses Online | Best Cybersecurity Training, Site rank: 1554, Description: Enroll in the best cybersecurity courses online by EC-Council. Boost your career with one of the best cybersecurity courses and training. Get certified now!, Primary language: English), 'Network' (Site: https://www.eccouncil.org, Netblock Owner: Cloudflare, Inc., Domain: Nameserver, Hosting company: Cloudflare, Domain registrar: Domain registrar, Hosting country: US, Nameserver organisation: Nameserver organisation), and 'IPv4 address' (104.18.8.180, VirusTotal link, Organisation: Organisation).

Gather personal information using PeekYou online people search service

PeekYou search results

The screenshot shows the PeekYou search interface. On the left is a sidebar with user profile (Gerren Jerome), Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, Sign Out, and Privacy options. The main search bar at the top has 'PEOPLE' selected, with 'Satya' in the first field and 'Nadella' in the second, both with dropdown menus for 'USERNAME' and 'All States'. Below the search bar is a 'Search People' section with 'First Name' and 'Last Name' fields, a 'Start Search' button, and a 'PeopleLooker' logo. 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) with 'View Full Report' links. To the right is a sidebar for 'Ask an Expert' featuring a profile of 'Ellen, Consultant' with a 5-star rating and 263 satisfied customers. At the bottom is a message from 'Pearl Wilson, Tech Expert's Assistant'.

Gather an email list using theHarvester

theHarvester search results

The screenshot shows a terminal window titled 'theHarvester -d microsoft.com -l 200 -b baidu - Parrot Terminal'. The terminal is running on the 'Parrot' distribution. The output of the command shows theHarvester version 4.0.0, credits to Christian Martorella, and contact information. It then lists targets: 'microsoft.com' and 'Baidu'. For 'microsoft.com', it shows 'Hacking Web Server' and '[*] No IPs found.' For 'Baidu', it shows 'Hacking Applications' and '[*] No emails found.' and '[*] No hosts found.'

Gather information using deep and dark web searching

Google search results

The screenshot shows a Google search results page with a sidebar on the left containing navigation links such as Institution Page, Gerren Jerome, Activity Stream, Courses (which is selected), Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main search bar contains the query "hacker for hire". Below the search bar are several filter buttons: Images, Videos, Shopping, Perspectives, News, Maps, Books, Flights, and Finance. The search results indicate approximately 191,000,000 results found in 0.50 seconds. The top result is from Upwork, titled "27 Best Freelance Hackers For Hire In January 2024", which lists various hackers with their ratings and hourly rates. Below this, there is a section titled "Discussions and forums" with links to a Quora post about hiring hackers and a Reddit thread on r/hacking.

Determine target OS through passive footprinting

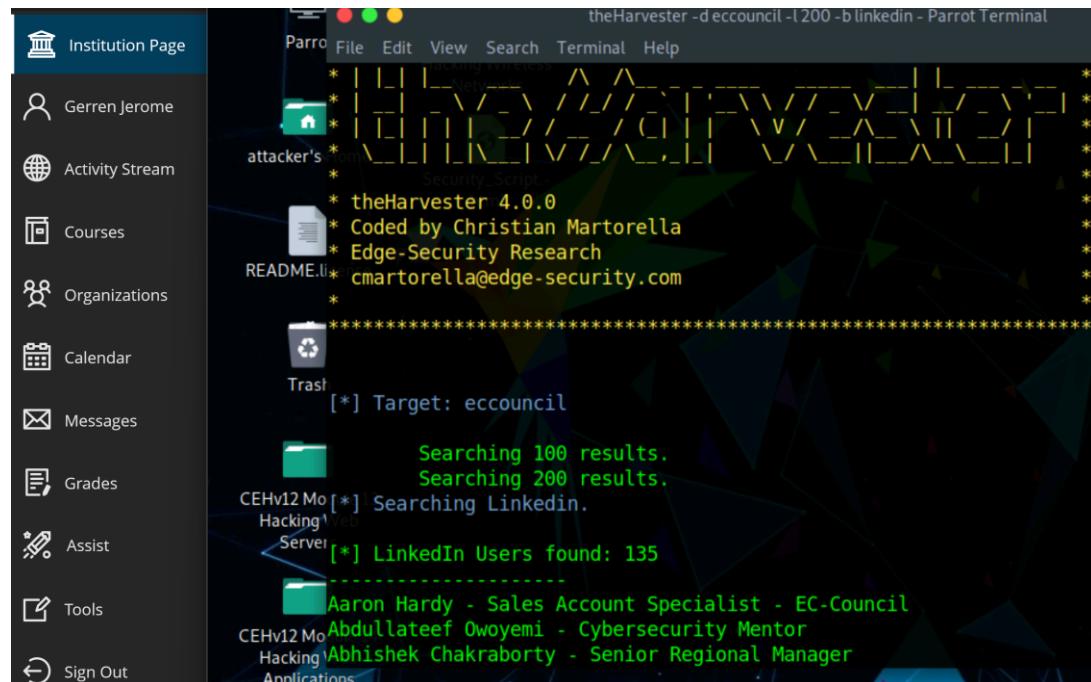
Censys search results

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 at the top has "Hosts" selected and contains the URL "www.eccouncil.org". The search results are displayed under the "Results" tab, showing 24 hosts found in 0.40s. The first result is 158.178.154.74, which is identified as running Ubuntu Linux on an ORACLE-BMC-31898 server in North Holland, Netherlands. It has multiple open ports: 22/SSH, 80/HTTP, and 443/HTTP. The second result is 95.99.176.253 (253-176-99-95.ftth.glasoperator.nl), running TMOBILE-THUIS (50266) in North Brabant, Netherlands, with ports 443/HTTP and 6881/KRPC. The third result is 2a00:ece1:0:1f:0:0:0:181, running GTS-BACKBONE GTS Telecom (5606) in Bucureşti, Romania, with ports 80/HTTP and 443/HTTP. Other results listed include various cloud providers and network equipment.

Perform footprinting through social networking sites

Gather employees' information from LinkedIn using theHarvester

theHarvester search results



The screenshot shows a Parrot OS desktop environment. On the left is a dark-themed sidebar with various icons and links: Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main window is a terminal titled "theHarvester -d ecouncil -t 200 -b linkedin - Parrot Terminal". The terminal output shows:

```
theHarvester 4.0.0
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com

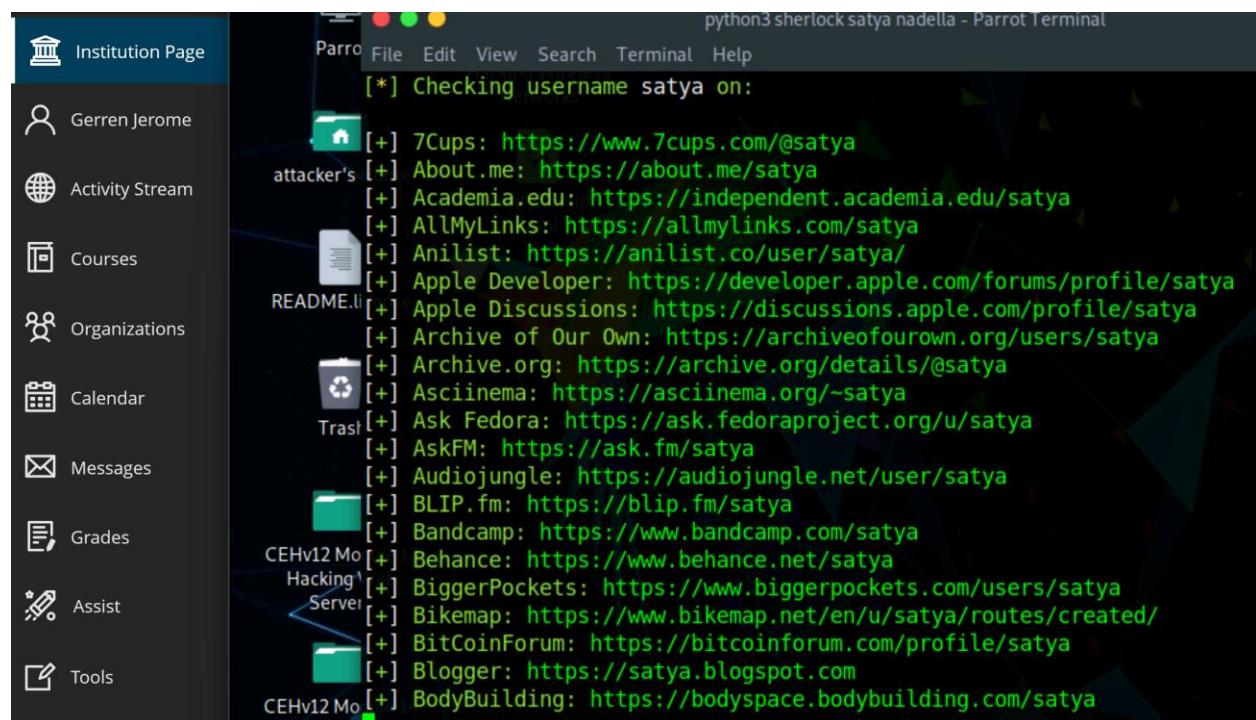
[*] Target: ecouncil

[*] LinkedIn Users found: 135

Aaron Hardy - Sales Account Specialist - EC-Council
Abdullateef Owoyemi - Cybersecurity Mentor
Hacking Applications
Abhishek Chakraborty - Senior Regional Manager
```

Gather personal information from various social networking sites using Sherlock

Sherlock search results



The screenshot shows a Parrot OS desktop environment. The sidebar on the left is identical to the previous one. The main terminal window is titled "python3 sherlock satya nadella - Parrot Terminal". The output shows:

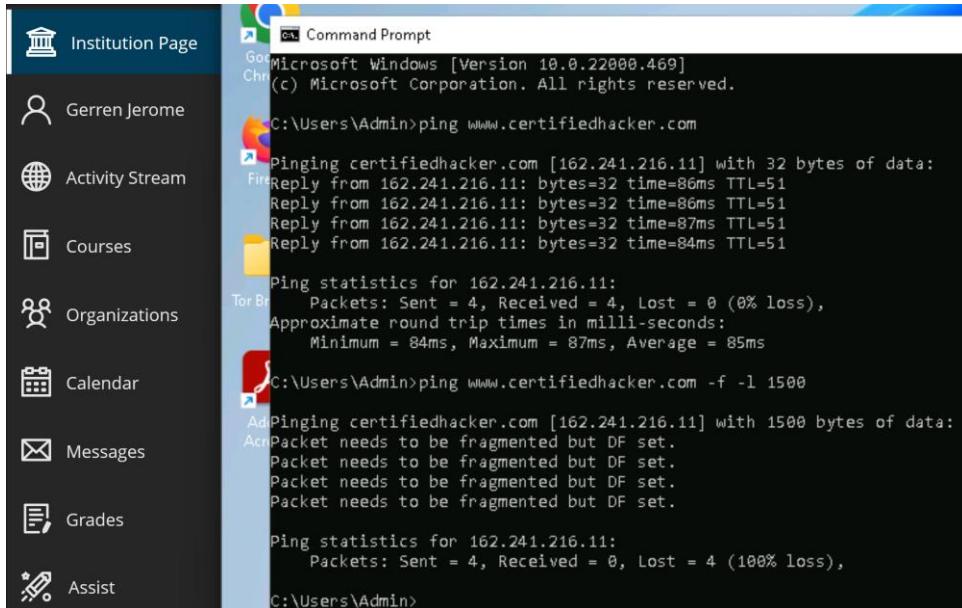
```
[*] Checking username satya on:

[+] 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
```

Perform website footprinting

Gather information about a target website using ping command line utility

finding the frame limit 1



The screenshot shows a Windows desktop environment. On the left, there is a sidebar with various icons and labels: Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, and Assist. On the right, a Command Prompt window is open with the following text:

```
Microsoft Windows [Version 10.0.22000.469]
Copyright © 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

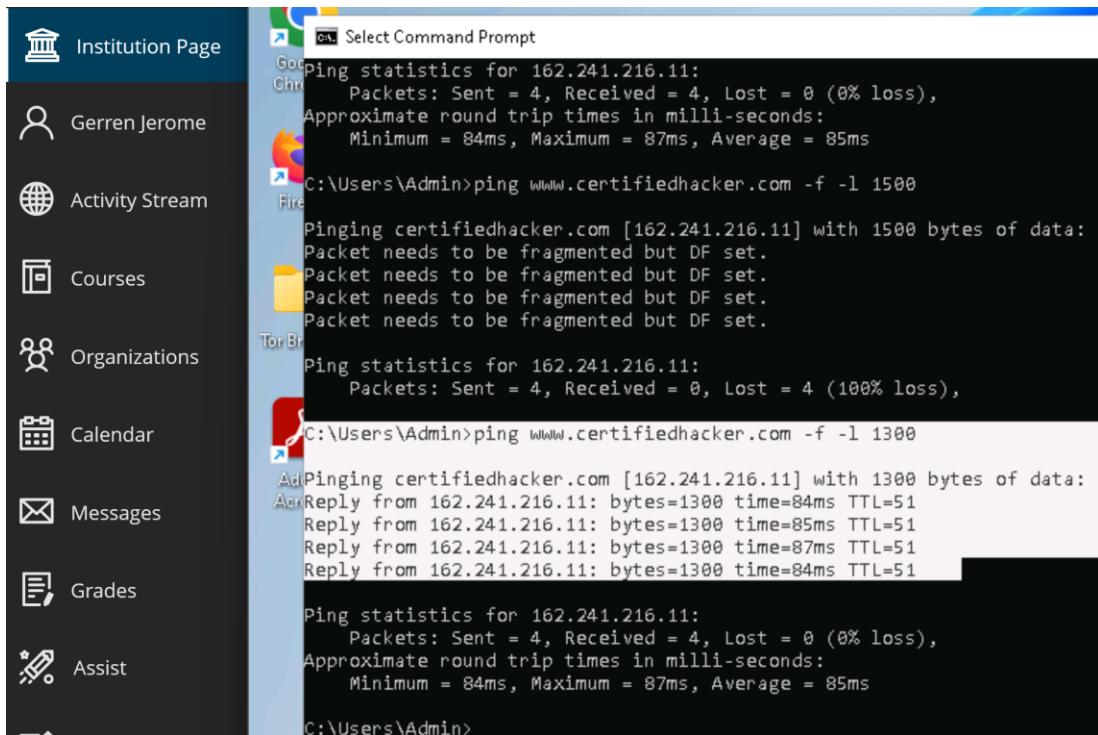
Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 87ms, Average = 85ms

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),
C:\Users\Admin>
```

finding the frame limit 2



The screenshot shows a Windows desktop environment. On the left, there is a sidebar with various icons and labels: Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, and Assist. On the right, a Command Prompt window is open with the following text:

```
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.

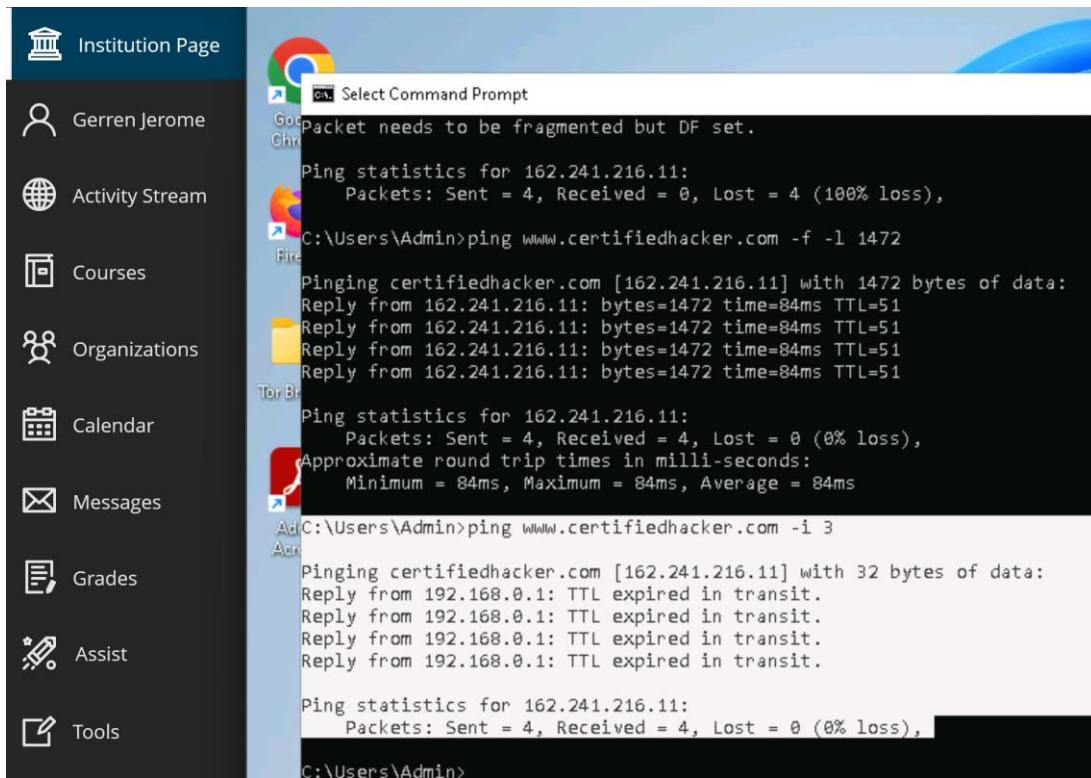
Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1300

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>
```

TTL manipulation



Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

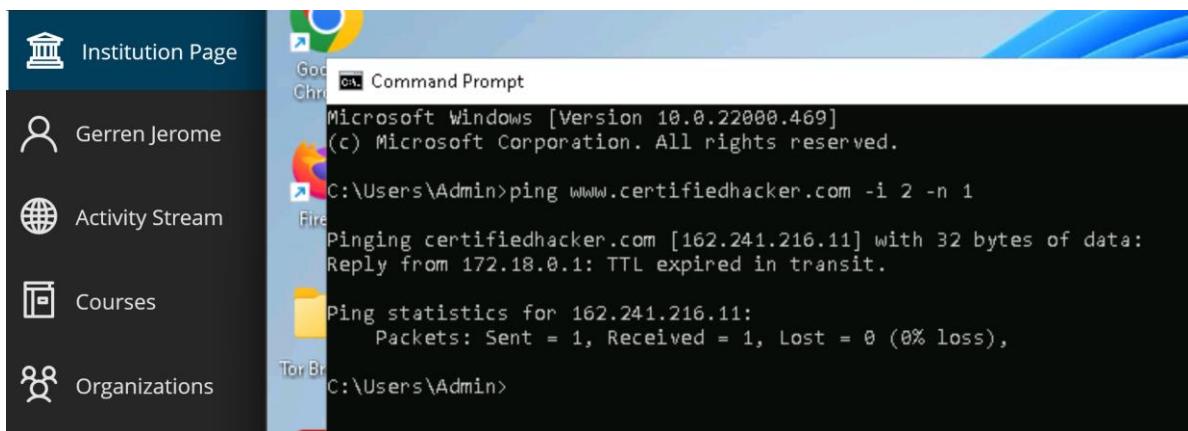
```
cmd Select Command Prompt
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472
Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 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 = 84ms, Average = 84ms
AdC:\Users\Admin>ping www.certifiedhacker.com -i 3
Acr
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 = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Admin>
```

ping packet lifespan



Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

```
cmd Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\Users\Admin>
```

find the hop

A screenshot of a desktop interface. On the left is a sidebar with icons and labels: Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, and Grades. The main area shows a terminal window with several ping commands being run against 'certifiedhacker.com' and 'www.certifiedhacker.com'. The terminal output includes:

```
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>
```

Gather information about a target website using Photon

Photon results – external

A screenshot of a desktop interface. On the left is a sidebar with icons and labels: Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, and Grades. The main area shows a terminal window titled 'external.txt [Read-Only] (~/Photon/www.certifiedhacker.com) - Pluma'. The file contains a list of URLs:

```
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/
```

Photon results – internal

The screenshot shows a web browser window for www.certifiedhacker.com. The title bar indicates the file is "internal.txt [Read-Only] (~/Photon/www.certifiedhacker.com) - Pluma". The menu bar includes File, Edit, View, Search, Tools, Documents, Help. Below the menu is a toolbar with icons for Open, Save, Undo, etc. A sidebar on the left lists institutional links: Institution Page, Gerren Jerome, Activity Stream, Courses, and Organizations. 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
```

Photon results – scripts

The screenshot shows a web browser window for www.certifiedhacker.com. The title bar indicates the file is "scripts.txt [Read-Only] (~/Photon/www.certifiedhacker.com) - Pluma". The menu bar includes File, Edit, View, Search, Tools, Documents, Help. Below the menu is a toolbar with icons for Open, Save, Undo, etc. A sidebar on the left lists institutional links: Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, and Assist. 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/js/
jquery.fancybox-1.2.6.pack.js
```

Gather information about a target website using Central Ops

CentralOps results

The screenshot shows the CentralOps.net interface. On the left is a sidebar with user profile (Gerren Jerome), activity stream, courses, organizations, calendar, messages, grades, assist, tools, sign out, and privacy options. The main area is titled "Domain Dossier" with the subtitle "Investigate domains and IP addresses". It shows the domain or IP address "www.certifiedhacker.com" entered. Under "domain whois record", "DNS records", and "traceroute" are checked. Under "network whois record", "service scan" is unchecked. A "go" button is present. Below this, it says "user: anonymous [168.245.203.252]" and "balance: 46 units". A "centralOps.net" logo is at the bottom right. A message box at the bottom left says "Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR."

Extract a company's data using Web Data Extractor

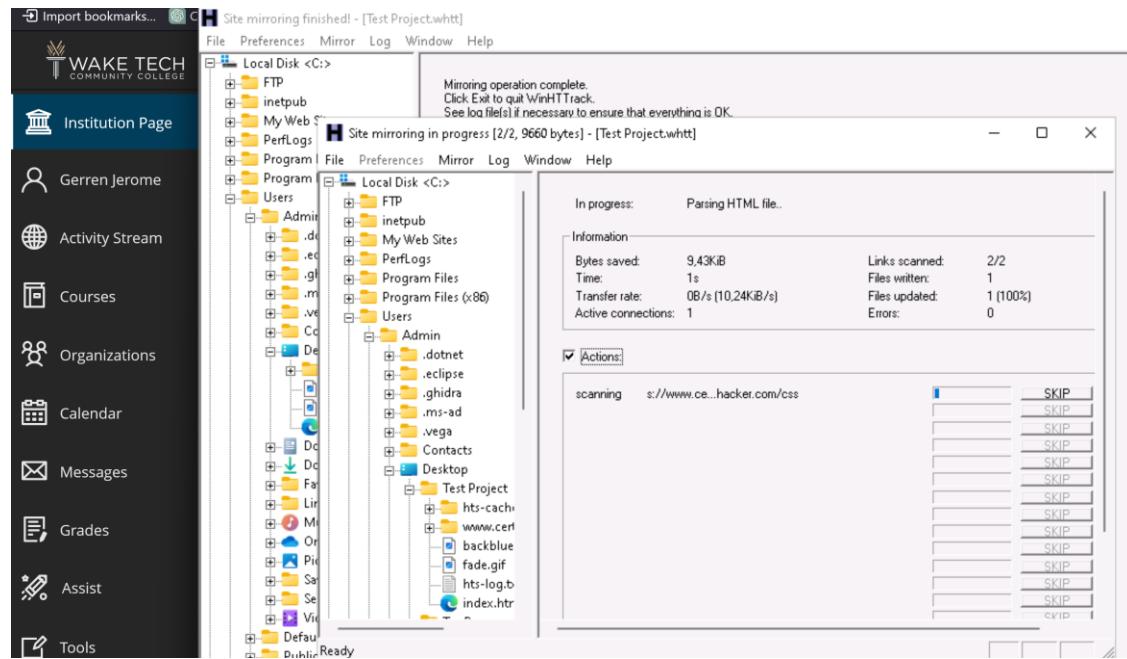
WEDPro results

The screenshot shows the Web Data Extractor Pro 4.1 interface. The sidebar includes Wake Tech Community College navigation (Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools) and session management (new session, edit session, start, pause, stop). The main window displays a table of extracted data from "Results" tab. The columns are MetaTag (20), Email (10), Phone (130), Fax (129), Link (50), and Domain (1). The table rows show various scraped items like descriptions, keywords, titles, URLs, and hosts. At the bottom, status bars show processing time (00:01:18.153), sites processed (67 / 83), download speed (4,220 KB), average speed (390 KB/s), and a progress bar.

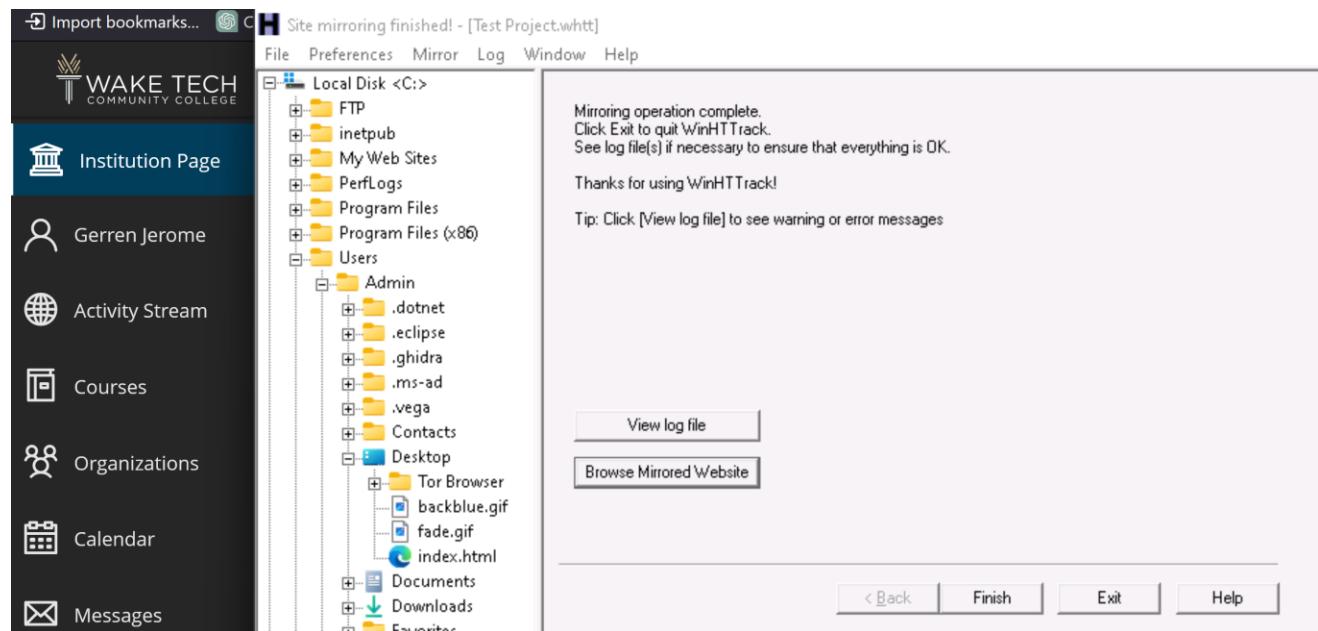
MetaTag (20)	Email (10)	Phone (130)	Fax (129)	Link (50)	Domain (1)
Description	Keywords	Title		Url	Host
A brief description of this we...	keywords, or phrases, asso...	Certified Hacker		https://www.certifiedhacker.com/	certifiedhacker.com
		Under the Trees		https://certifiedhacker.com/corporate...	certifiedhacker.com
A short description of your c...	Some keywords that best d...	Your company - Homepage		https://certifiedhacker.com/Under%2...	certifiedhacker.com
A brief description of this we...	keywords, or phrases, asso...	Unite - Together is Better (...		https://certifiedhacker.com/Social%2...	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%2...	certifiedhacker.com
Turbo max powerful one pa...	Turbo max , owltemplates.c...	Turbo Max Theme - OwlTe...		https://certifiedhacker.com/Turbo%2...	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%2...	certifiedhacker.com
Online Booking	booking, hotel, hotels, rese...	Online Booking: Search		https://certifiedhacker.com/Online%2...	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%2...	certifiedhacker.com
Online Booking	booking, hotel, hotels, rese...	Online Booking: Hotel Info		https://certifiedhacker.com/Online%2...	certifiedhacker.com

Mirror a target website using HTTrack Web Site Copier

Site mirroring progress



Completed mirroring results



Gather information about a target website using GRecon

GRecon results



WAKE TECH
COMMUNITY COLLEGE

Institution Page

Geren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

```
python3 grecon.py - Parrot Terminal
File Edit View Search Terminal Help
[!] Switching Google TLDs...
Hacking Wireless Networks
[>] 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]
#
```

Gather a wordlist from the target website using CeWL

Wordlist output from CeWL

The screenshot shows a Pluma text editor window titled "wordlist.txt (~) - Pluma (as superuser)". The menu bar includes File, Edit, View, Search, Tools, Documents, and Help. Below the menu is a toolbar with icons for Open, Save, Undo, Cut, Copy, Paste, and Find. The main content area displays a list of 19 items, each preceded by a number from 1 to 19 and a short word or phrase:

- 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

Perform email footprinting

Gather information about a target by tracing emails using eMailTrackerPro

Tracing email header (Map and Summary)

The screenshot shows the eMailTrackerPro interface. On the left is a sidebar with links like Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main window has tabs for Home and Subject: Important La... (with a close button). Below the tabs is a message: "The trace is complete, the information found is displayed on the right". There are buttons for New Trace and View Report. The right side is divided into sections: **Email Summary**, **Map** (a world map), **System Information** (a bulleted list), **Network Whois**, **Domain Whois**, and **Email Header**. The **Email Summary** section shows the following details:

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

Network Whois, **Domain Whois**, and **Email Header** sections are also visible.

Tracing email header (Report)

The screenshot shows a browser window displaying an eMailTrackerPro report. The URL is C:/Users/Admin/eMailTrackerPro/V8/rep... The title bar says "eMailTrackerPro v10.0b Advanced Edition Trial day 1 of 15". The page has a header with links: How to Report Email Abuse | eMailTrackerPro Manual | FAQ | Visualware Home | eMailTrackerPro Website | purchase eMailTrackerPro. The main content area is titled "Identification Report for 'Important: Last Reminder for KYC Verific'". It includes a message about the trial period and the location being San Antonio, TX. The "Network Contact Information" section lists the following details:

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

A link "Click here to hide the in-depth information on this email (more info)" is present. Below it is a list of bullet points:

- 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 traceable IP to the sender was - 161.38.197.240
- The sender of this email appeared to have the address 984239084569834576834@substack.com. This

Perform Whois footprinting

Perform Whois lookup using DomainTools

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 displays the WHOIS Record for CertifiedHacker.com. The record includes details such as Registrar (Network Solutions, LLC), Registrar Status (clientTransferProhibited), Dates (7,651 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 of the WHOIS data is a sidebar titled 'DomainTools Iris' with a 'Learn More' button, and a section titled 'Tools' with options for Hosting History, Monitor Domain Properties, Reverse IP Address Lookup, Network Tools, and Visit Website.

Perform DNS footprinting

Gather DNS information using nslookup command line utility and online tool

DNS recon with nslookup

The screenshot shows a terminal window with the title 'Select Command Prompt - nslookup'. The command 'nslookup' is used to query the domain 'certifiedhacker.com'. The output shows the domain's primary name server is 'ns1.bluehost.com', its responsible mail server is 'dnsadmin.box5331.bluehost.com', and its serial number is '2024011800'. It also shows the refresh, retry, expire, and default TTL values. A subsequent 'nslookup' command to 'ns1.bluehost.com' returns a non-authoritative answer with the name 'ns1.bluehost.com' and address '162.159.24.80'.

KLOTH.NET results

The screenshot shows the KLOTH.NET interface with a sidebar containing links like 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 instructions for querying a DNS domain nameserver. A form allows specifying the Domain (certifiedhacker.com), Server (localhost), and Query type (A (IPv4 address)). Below the form, the result for "certifiedhacker.com" from server localhost is shown, indicating the DNS server handling the query is localhost with address 127.0.0.1#53, and a non-authoritative answer with Name: certifiedhacker.com and Address: 162.241.216.11.

Perform reverse DNS lookup using reverse IP domain check and DNSRecon

yougetsignal.com results

The screenshot shows the yougetsignal.com interface with a sidebar containing links like Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main content area is titled "Reverse IP Domain Check". It features a search bar for "Remote Address" (www.certifiedhacker.com) and a "Check" button. The results section displays 15 domains hosted on the same web server as www.certifiedhacker.com (162.241.216.11). The listed domains include 100wwcbeaufort.org, bongekile.com, certifiedhacker.com, eis.qa, humancarehealth.com, oakoffer.com, www.certifiedhacker.com, and www.lsstl.org. To the right, a list of additional domains is shown: biosis.ae, box5331.bluehost.com, certifiedhacker.com, gaelicmemoriesphotography.ie, mail.certifiedhacker.com, thortonchipsdepotencia.com, and www.certifiedhacker.com. A note at the bottom states that the database has grown to over 100 million domain names and offers a domain list for purchase. A link to "More about this tool. Set an API Key" is also present.

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
[+] EHv12M 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
[+] EHv12M PTR 162-241-216-12.unifiedlayer.com 162.241.216.12
[+] HackingPTR PTR box5354.bluehost.com 162.241.216.26
```

Gather information of subdomain and DNS records using SecurityTrails

SecurityTrails search results

The screenshot shows the SecurityTrails web interface. On the left, there is a 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 for the domain `certifiedhacker.com` as of January 27, 2024. It includes sections for A records and AAAA records. Under A records, it shows a single entry for the Unified Layer with the IP address `162.241.216.11`. There is also a note at the bottom encouraging users to upgrade to SurfaceBrowser™.

Historical data (A Record)

The screenshot shows a user profile for "Gerren Jerome" on the left. The main content area displays "certifiedhacker.com historical A data" with a search bar and filter options for A, AAAA, MX, NS, SOA, and TXT records. A table lists IP addresses, their organization, first seen date, last seen date, and duration seen. The data includes:

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

Perform network footprinting

Locate the network range

ARIN.net search results

The screenshot shows a user profile for "Gerren Jerome" on the left. The main content area is titled "ARIN Whois/RDAP". It shows a search bar with "162.241.216.11" and a "Search" button. Below the search bar are links to "Search www.arin.net instead" and "Search Filter: Automatic", with a note about terms of use. The search results for "162.241.216.11" are displayed in a box titled "Network: NET-162-240-0-0-1". The results include:

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

Perform network tracerouting in Windows and Linux Machines

tracert results (WIN)

The screenshot shows a Windows desktop environment. On the left is the Start menu with various icons for Google Chrome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Sign Out. On the right is a terminal window titled 'cmd' with the following text:

```
-h maximum_hops      Maximum number of hops to search for target.  
-j host-list        Loose source route along host-list (IPv4-only).  
-w timeout          Wait timeout milliseconds for each reply.  
-R                 Trace round-trip path (IPv6-only).  
-S srcaddr          Source address to use (IPv6-only).  
-4                 Force using IPv4.  
-6                 Force using IPv6.  
  
C:\Users\Admin>tracert -h 5 www.certifiedhacker.com  
'tracert' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Users\Admin>tracert -h 5 www.certifiedhacker.com  
  
Tracing route to certifiedhacker.com [162.241.216.11]  
over a maximum of 5 hops:  
  
1 <1 ms <1 ms <1 ms 10.10.1.2  
2 1 ms 1 ms 1 ms 172.18.0.1  
3 1 ms <1 ms <1 ms 192.168.0.1  
4 1 ms 1 ms 1 ms 103.186.82.26  
5 3 ms 1 ms 1 ms 103.186.82.3  
  
Trace complete.  
C:\Users\Admin>
```

traceroute results (LNX)

The screenshot shows a Linux desktop environment. On the left is the Start menu with icons for Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. On the right is a terminal window titled 'Terminal' with the following text:

```
[attacker@parrot] ~$ traceroute www.certifiedhacker.com  
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte pac  
kets  
 1 10.10.1.2 (10.10.1.2) 1.690 ms 2.133 ms 2.624 ms  
 2 172.18.0.1 (172.18.0.1) 3.860 ms 4.885 ms 5.574 ms  
 3 192.168.0.1 (192.168.0.1) 7.069 ms 8.205 ms 8.516 ms  
 4 103.186.82.26 (103.186.82.26) 9.693 ms 10.081 ms 10.311 ms  
 5 103.186.82.3 (103.186.82.3) 10.867 ms 11.459 ms 11.635 ms  
 6 gi0-1-1-15.rcr21.iad01.atlas.cogentco.com (38.104.207.233) 12.402 ms 1.946  
 ms 2.788 ms  
 7 be2956.ccr41.iad02.atlas.cogentco.com (154.54.30.193) 3.379 ms 3.454 ms 4  
.274 ms rash  
 8 * telia.iad02.atlas.cogentco.com (154.54.12.62) 5.219 ms 6.113 ms  
 9 ash-bb2-link.ip.twelve99.net (62.115.123.124) 6.068 ms 6.386 ms rest-bb1-l  
 ink.ip.twelve99.net (62.115.138.191) 7.203 ms  
 10 lax-b23-link.ip.twelve99.net (62.115.137.37) 67.787 ms 65.143 ms lax-b22-l  
 ink.ip.twelve99.net (62.115.121.220) 63.157 ms  
 11 * * *  
 12 newfoldigital-ic-381440.ip.twelve99-cust.net (62.115.181.153) 61.269 ms 5  
 7.894 ms 68.159 ms  
 13 162-215-195-161.unifiedlayer.com (162.215.195.161) 61.051 ms 60.987 ms 162  
 -215-195-159.unifiedlayer.com (162.215.195.159) 56.824 ms  
 14 162-215-193-233.unifiedlayer.com (162.215.193.233) 86.743 ms 162-215-193-23
```

Perform footprinting using various footprinting tools

Footprinting a target using Recon-ng

confirm created workspace

```
ime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[recon-ng][CEH] > workspaces list
CEHV12 Module 13
+-----+
| Workspaces |      Modified      |
+-----+
| CEH        | 2024-01-27 10:19:20 |
| default    | 2024-01-27 10:17:57 |
+-----+
```

recon-ng results (brute_hosts)

```
[*] 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] >
```

harvested host results (Attacker Window)

The screenshot shows the Recon-NG interface with a sidebar on the left containing user profile, activity stream, courses, organizations, calendar, messages, grades, assist, tools, and sign out options. The main window displays a summary of harvested hosts:

```
-----  
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 | | |  
+-----+
```

harvested host results (HTML report)

The screenshot shows a web browser window titled "Recon-NG Reconnaissance Report" displaying the harvested host results. The browser's address bar shows the URL as "file:///home/attacker/Desktop/results". The page content is a table titled "[-] Hosts" with the following data:

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						
ftp.certifiedhacker.com	162.241.216.11					
imap.certifiedhacker.com						
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					
smtplib.certifiedhacker.com						

WHOIS POCS results

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

[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

HackerTarget results

 Gerren Jerome	[recon-ng][default][hackertarget] > run ----- CERTIFIEDHACKER.COM ----- [*] Country: None [*] Host: autodiscover.certifiedhacker.com [*] Ip_Address: 162.241.216.11 [*] Latitude: None [*] Longitude: None [*] Notes: None [*] Region: None [*] ----- [*] Country: None [*] Host: blog.certifiedhacker.com [*] Ip_Address: 162.241.216.11 [*] Latitude: None [*] Longitude: None [*] Notes: None in@facebook.com [*] Region: None [*] ----- [*] Country: None
 Activity Stream	
 Courses	
 Organizations	
 Calendar	
 Messages	
 Grades	
 Assist	
 Tools	

Footprinting a target using Maltego

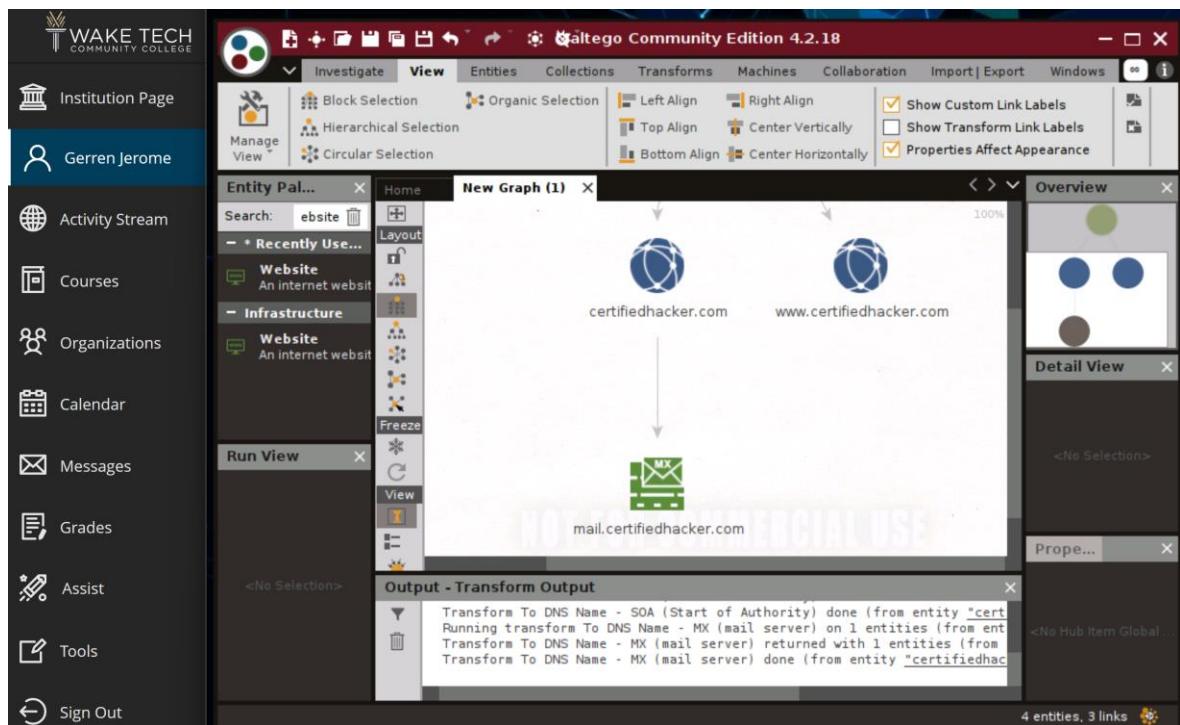
Login Successful

The screenshot shows the Maltego Community Edition login interface. On the left, there's a sidebar with icons for Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, and Calendar. The main area has a title "Configure Maltego" and a message "LOGIN RESULT: Please log in to use the free online version of Maltego." Below this, it says "Hello Gerren, welcome to Maltego Community Edition!" and displays personal details: First name (Gerren), Surname (Jerome), and Email address (gjerome1@my.waketech.edu). It also states that the API key is valid until January 26, 2026 at 12:00:00 AM EST.

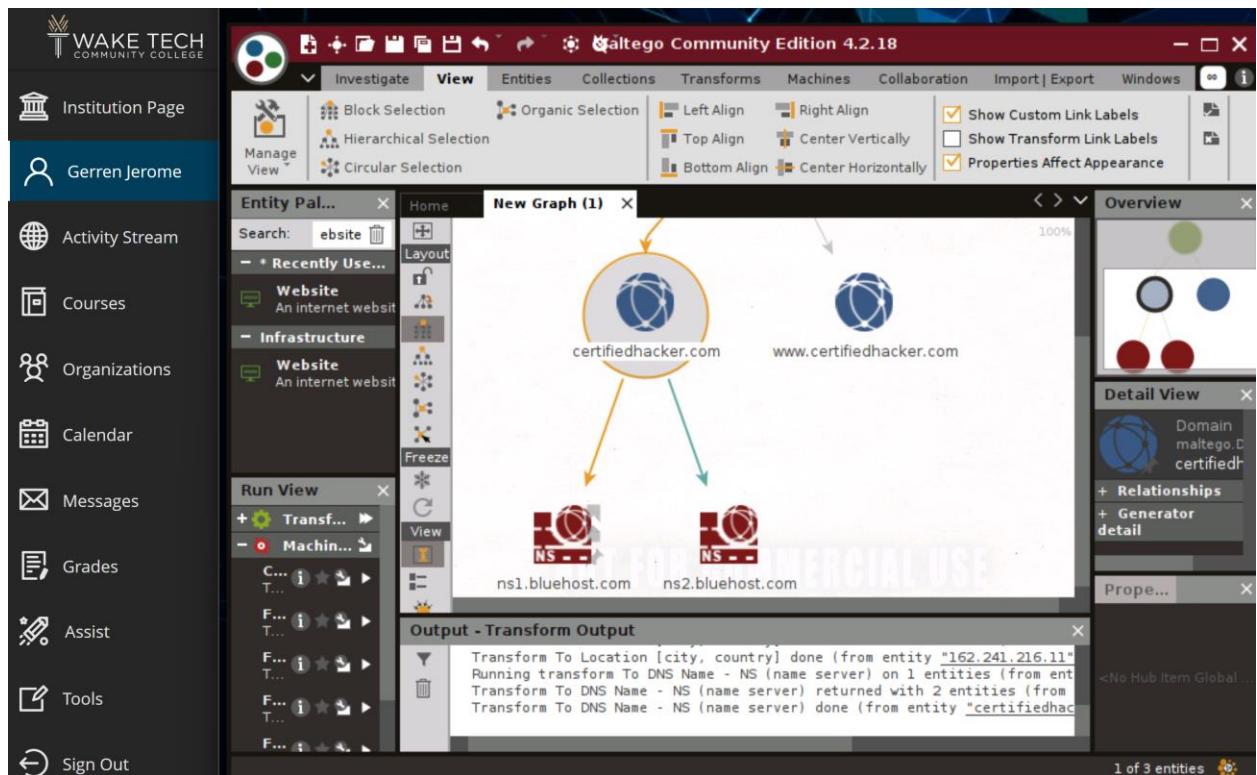
Transform (DNS) – identify and parse

The screenshot shows the Maltego Community Edition interface with a graph titled "New Graph (1)". The graph displays several entities: "certifiedhacker.com" and "www.certifiedhacker.com" at the top, with arrows pointing down to "imap.certifiedhacker.com", "news.certifiedhacker.com", and "pop.certifiedhacker.com". Each of these three entities has a "DNS" transform applied to it, represented by small orange boxes labeled "DNS". The interface includes various toolbars and panels like "Entity Pal...", "View", "Transforms", and "Output - Transform Output" which shows the results of the DNS transforms.

Transform (MX) - identify and parse



Transform (NS) - identify and parse



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". An arrow points down to a location pin labeled "(United States)". To the right of the graph are panels for "Overview" (with three colored dots), "Detail View" (<No Selection>), and "Properties" (with a "Prop..." button). At the bottom, a "Run View" panel shows "<No Selection>". A "Output - Transform Output" panel contains 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")
```

3 entities, 2 links

Footprinting a target using OSRFramework

Domainfy results

The screenshot shows the OSRFramework interface. The left sidebar includes: Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main output area displays the following text:

```
2024-01-27 11:42:05.709880      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 |
+-----+
```

Searchfy results

WAKE TECH
COMMUNITY COLLEGE

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

File Edit View Search Terminal Help

[*] Launching search using the KeyServerUbuntu module...

2024-01-27 11:43:52.407852 Networks Results obtained:

```
Sheet Name: Objects recovered (2024-1-27_11h43m).
+-----+
| com.i3visio.Platform | com.i3visio.Email |
| com.i3visio.URI      | com.i3visio.Domain |
| com.i3visio.Alias    | com.i3visio.Domain |
+-----+
+-----+
| KeyServerUbuntu     | cooktim800@gmail.com | https://keyserver.u
buntu.com/pks/lookup?fingerprint=on&op=index&search=cooktim800@gmail.com
| cooktim800          | gmail.com           |
+-----+
+-----+
| KeyServerUbuntu     | tkcook@bigfoot.com | https://keyserver.u
buntu.com/pks/lookup?fingerprint=on&op=index&search=tkcook@bigfoot.com
```

Footprinting a target using FOCA

Project saved successfully!

Project of www.eccouncil.org - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project of www.eccouncil.org

Network Domains Document Analysis

Foca
OPENSOURCE

Custom search

Search engines: Google, Bing, DuckDuckGo

Extensions: All None

doc docx sxw odp
ppt ppts odt pdf
pps ppsx ods wpd
xls xlxs odg rtf

Project saved successfully!

OK

Time Source Severity Message

Settings Deactivate AutoScroll Clear Save log to File

Saturday, January 27, 2024

Search All results

The screenshot shows the FOCA Open Source interface on Windows Server 2019. The left sidebar includes links for Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main window displays a search interface for the project 'Project of www.eccouncil.org'. The search engines section lists Google, Bing, and DuckDuckGo with checkboxes. The extensions section lists various file types like doc, ppt, pps, xls, docx, ptx, ppss,lsx, odt, ods, ogd, odp, pdf, wps, ods, and rtf. A 'Custom search' table shows 8 entries, all of which are PDF files. Below the table is a log table with three entries related to search engines. At the bottom, there are buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File.

Crawling results

The screenshot shows the FOCA Open Source interface on Windows Server 2019, similar to the previous one but with a lightning bolt icon in the top-left corner of the main window. The left sidebar is identical. The main window shows the 'Project of www.eccouncil.org' interface. The 'Technology recognition' section shows Google, Bing, and DuckDuckGo crawling. The 'Domain: eccouncil.org' section shows files, folders, documents published, and parameterized items found. The 'File' table at the bottom shows a list of domains found during the crawl. The log table at the bottom shows 8 entries related to domain discoveries. The status bar at the bottom right indicates Saturday, January 27, 2024.

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

Results: DNS Lookup

```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
4) Subnet Lookup 16) Subdomain listing (use Sublist3r)
5) Port Scanner 17) Find Admin login site (use Breacher)
6) Page Links 18) Check and Bypass CloudFlare (use HatCl
oud)
7) Zone Transfer 19) Website Copier (use httrack)
8) HTTP Header 20) Host Info Scanner (use WhatWeb)
9) Host Finder 21) About BillCipher
10) IP-Locator 22) Fuck Out Of Here (Exit)
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.
SOA : ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2024011800 86400 7
Ha200 3600000 300
Do you want to continue? [Yes/No]:
```

Results: GeoIP Lookup

```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
2) Whois Lookup 14) Reserve IP Lookup
3) GeoIP Lookup 15) Email Gathering (use Infoga)
4) Subnet Lookup 16) Subdomain listing (use Sublist3r)
5) Port Scanner 17) Find Admin login site (use Breacher)
6) Page Links 18) Check and Bypass CloudFlare (use HatCl
oud)
7) Zone Transfer 19) Website Copier (use httrack)
8) HTTP Header 20) Host Info Scanner (use WhatWeb)
9) Host Finder 21) About BillCipher
10) IP-Locator 22) Fuck Out Of Here (Exit)
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:
Latitude: 37.751
Longitude: -97.822
Do you want to continue? [Yes/No]:
```

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)
7) Zone Transfer 19) Website Copier (use httrack)
8) HTTP Header 20) Host Info Scanner (use WhatWeb)
9) Host Finder 21) About BillCipher
10) IP-Locator 22) Fuck Out Of Here (Exit)
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]: