

Lab 5: Gathering Target Information - Footprinting and Social Engineering

Part 1: Explore Google Hacking:

“Google hacking” refers to the practice of using Google or other search engines’ advanced functionalities to better gather information about a target organization. We demonstrate this on The New York Times using various different google filters.

Figure 1: Normal Google Search For “New York Times”

The screenshot shows a Google search for "new york times". The search bar at the top contains the text "new york times" and a magnifying glass icon. Below the search bar, there are tabs for "All", "News", "Books", "Images", "Videos", and "More". The search results are displayed below the tabs, showing "About 3,980,000,000 results (1.33 seconds)".

The first result is from "https://www.nytimes.com" and is titled "The New York Times - Breaking News, US News, World News ...". Below the title, it says "Live news, investigations, opinion, photos and video by the journalists of The New York Times from more than 150 countries around the world." Below this result is a search bar with the text "Results from nytimes.com" and a magnifying glass icon.

Below the search bar, there are several links to "Today's Paper", "Wordle", "Spelling Bee", and "Opinion".

Below these links, there is a section titled "Latest from nytimes.com" which displays a grid of three news articles. The first article is titled "Three Meteorology Students Killed in Car Crash in Oklahoma" and is dated "2 hours ago". The second article is titled "Arkansas Sues Family Dollar Over Persistent Rodent Infestation" and is dated "5 hours ago". The third article is titled "Naomi Judd, of Grammy-Winning The Judds, Dies at 76" and is dated "6 hours ago".

Below the "Latest from nytimes.com" section, there is a section titled "https://twitter.com/nytimes" and "The New York Times (@nytimes) · Twitter". This section displays a grid of three tweets. The first tweet is about "At least 85 wild horses have died from an 'unknown yet highly contagious' disease at a facility in Colorado, the Bureau of Land Management said." The second tweet is about "Some of New York's nightlife scenes are less about dancing and more about eating. nyti.ms/3LzZDYH". The third tweet is about "As is true throughout rural Japan, many of the once-vibrant villages on the Kii Peninsula are aging into".

On the right side of the search results, there is a section titled "The New York Times" with the subtitle "Newspaper". Below this, there is a description of the newspaper and its history. Below the description, there are several links to "Founded", "Publisher", "Headquarters", "Format", "Editor-in-chief", "OCLC number", and "Awards".

At the bottom right of the search results, there is a section titled "See results about" which displays a list of related entities, including "The New York Times Company" and "Media company".

Figure 2: Applying The site: Filter

The image is a screenshot of a Google search results page. At the top left is the Google logo. To its right is a search bar containing the text 'site:nytimes.com'. Below the search bar is a horizontal navigation bar with links for 'All', 'Images', 'News', 'Shopping', 'Maps', and 'More'. Below this bar, the search results are displayed. The first line indicates 'About 38,500,000 results (0.28 seconds)'. The results are listed as follows:

- <https://www.nytimes.com> > ...
The New York Times Canada - Breaking News, US News ...
The New York Times provides live news, investigations, opinion and video from the United States, Canada and around the world. Our 1700 journalists report on ...
- <https://www.nytimes.com> > wirecutter
Wirecutter: New Product Reviews, Deals, and Buying Advice
Wirecutter tests and reviews the best tech, appliances, gear, and more. You can trust our veteran journalists, scientists, and experts to find the best ...
- <https://cooking.nytimes.com> > ourcooks
Melissa Clark - NYT Cooking - The New York Times
Melissa Clark has been a columnist for the Food section since 2007. She reports on trends, creates recipes and appears in videos linked to her column, A Good ...
- <https://www.nytimes.com> > section > todayspaper
Today's Paper - The New York Times
The S&P 500 plunged nearly 9 percent in April, its worst monthly decline since March 2020, as rising interest rates and high inflation raised concerns about ...
- <https://www.nytimes.com> > Opinion > Sunday Review
Exposures - The New York Times
Exposures is an Opinion forum for photography, curated by Jeffrey Henson Scales. It features among the finest photography, from photojournalism to more ...
- <https://cooking.nytimes.com> > tag > potato
Potato Recipes - NYT Cooking
Browse and save the best potato recipes on New York Times Cooking.
- <https://www.nytimes.com> > column > renters
Renters - The New York Times
Stories of New Yorkers who rent or lease: where they live, what they pay and what they get for it.
- <https://www.nytimes.com> > section > magazine
The New York Times Magazine
After the police officers who beat Rodney King were acquitted, Los Angeles went to war with itself. The violence lasted a week, but its causes stretched back ...
- <https://www.nytimes.com> > wirecutter > appliances
Home & Kitchen Appliances | Wirecutter - The New York Times
From dishwashers and refrigerators to vacuums and steam cleaners, our experts pick out the right appliances for all kinds of living situations, to help keep ...

Figure 3: Applying The inurl: Filter

The screenshot shows a Google search interface with the query 'inurl:nytimes.com' entered in the search bar. The search results are filtered to show only pages from the domain 'nytimes.com'. The top result is the main homepage of The New York Times, followed by 'Today's Paper'. Below these are several 'People also ask' questions related to accessing the site for free. Further down, there are links to 'Latest Russia-Ukraine War News', 'Wordle', 'World News', 'Opinion', and 'U.S. News' sections of the New York Times website.

Google

inurl:nytimes.com

Q All News Books Shopping Videos More Tools

About 39,900,000 results (0.46 seconds)

<https://www.nytimes.com>

The New York Times - Breaking News, US News, World News ...

Live news, investigations, opinion, photos and video by the journalists of The New York Times from more than 150 countries around the world.

[Today's Paper](#) · [World News](#) · [Opinion](#) · [US Politics](#)

<https://www.nytimes.com/section/todayspaper>

Today's Paper - The New York Times

The S&P 500 plunged nearly 9 percent in April, its worst monthly decline since ...

[The Front Page](#) · [National](#) · [Editorials, Op-Ed and Letters](#) · [Business Day](#)

People also ask

How can I read NY Times for free?

Is NY Times account free?

What kind of website is NY Times?

How do I access NY Times?

Feedback

<https://www.nytimes.com/live/2022/04/30/world/ukraine-russia-war>

Latest Russia-Ukraine War News: Live Updates - The New ...

2 hours ago — Ukraine said Russia was shifting troops from its far-eastern ...

<https://www.nytimes.com/games/wordle>

Wordle - The New York Times

Each guess must be a valid five-letter word. Hit the enter button to submit.

<https://www.nytimes.com/section/world>

World News - The New York Times

The latest international news, investigations and analysis from Africa, ...

<https://www.nytimes.com/section/opinion>

Opinion - The New York Times

New York Times Opinion columnists, editorials and guest essays.

<https://www.nytimes.com/section/us>

U.S. News - The New York Times

Breaking news, photos and videos from around the United States.

Figure 4: Applying The link: Filter

The screenshot shows a Google search interface with the query 'link:nytimes.com' entered in the search bar. The search results are displayed below the bar, showing approximately 1,060,000,000 results in 0.43 seconds. The results are filtered to show only links to nytimes.com. The first result is 'Linking - Help - The New York Times' from https://help.nytimes.com, which provides information on how to link to the site. The second result is 'FAQ: Linking to The New York Times on the Web' from https://archive.nytimes.com, which explains the URL to use for linking. Below these are four 'People also ask' questions related to getting, reading, and canceling a New York Times subscription. The third result is 'The New York Times - Breaking News, US News, World News ...' from https://www.nytimes.com, which is the main homepage. The fourth result is 'Find Your Home Delivery Subscription - myaccount.nytimes.com' from https://myaccount.nytimes.com, which provides information on how to connect a home delivery subscription to a NYTimes.com account. The fifth result is 'Obtaining and using Times content - Help - The New York Times' from https://help.nytimes.com, which provides information on how to link to NYTimes.com. The sixth result is 'Find Your Subscription - myaccount.nytimes.com' from https://myaccount.nytimes.com, which provides information on how to connect a subscription to a NYTimes.com account.

Google

link:nytimes.com

Search filters: All, News, Images, Videos, Shopping, More, Tools

About 1,060,000,000 results (0.43 seconds)

https://help.nytimes.com › 115014893268-Linking
Linking - Help - The New York Times
You can **link** directly to **NYTimes.com** without obtaining permission. Review the rest of the questions on this page for guidelines on how to **link** to our site.

https://archive.nytimes.com › info › help › linking
FAQ: Linking to The New York Times on the Web
A. The **URL** that is visible in the location bar when viewing an article on our website is the **URL** that should be used for the **link**. The **URL** that ...

People also ask

- How do I get New York Times Link?
- How can I read NYTimes for free?
- How do I cancel my New York Times subscription online?
- Is NYTimes com free?

Feedback

https://www.nytimes.com
The New York Times - Breaking News, US News, World News ...
Live news, investigations, opinion, photos and video by the journalists of **The New York Times** from more than 150 countries around the world.
[International](#) · [Today's Paper](#) · [World News](#) · [Opinion](#)

https://myaccount.nytimes.com › link › homedelivery
Find Your Home Delivery Subscription - myaccount.nytimes.com
For your free, unlimited access to **NYTimes.com**, just **connect** your Home Delivery subscription to **NYTimes.com** in two easy steps. **New York Times** International ...

https://help.nytimes.com › en-us › articles › 115014891...
Obtaining and using Times content - Help - The New York Times
For information about **linking** to **NYTimes.com**, see the Frequently Asked Questions About **Linking**. 2. Do I need permission to email an article?

https://myaccount.nytimes.com › link › inyt
Find Your Subscription - myaccount.nytimes.com
Start enjoying all your online benefits by connecting your **New York Times** International Edition subscription to an **NYTimes.com** account. **New York Times** Home ...

Figure 5: Applying The related: Filter

The image is a screenshot of a Google search results page. At the top left is the Google logo. The search bar contains the text 'related:nytimes.com' with a clear (X) button and a search (magnifying glass) button to its right. Below the search bar is a horizontal navigation bar with links for 'All', 'Images', 'Maps', 'Shopping', and 'More', followed by a 'Tools' link on the far right. The search results are displayed below this bar, starting with '8 results (0.38 seconds)'. The first result is from 'https://www.usatoday.com' with the title 'USA TODAY: Latest World and US News - USATODAY.com' and a description: 'USA TODAY delivers current local and national news, sports, entertainment, finance, technology, and more through award-winning journalism, photos, ...'. The second result is from 'https://www.washingtonpost.com' with the title 'The Washington Post: Breaking News, World, US, DC News ...' and a description: 'Breaking news and analysis on politics, business, world national news, entertainment more. In-depth DC, Virginia, Maryland news coverage including traffic, ...'. The third result is from 'https://www.reuters.com' with the title 'Reuters: Breaking International News & Views' and a description: 'Warren Buffett on Saturday used the annual meeting of Berkshire Hathaway Inc to reveal major new investments including a bigger stake in Activision Blizzard ...'. The fourth result is from 'https://www.bloomberg.com' with the title 'Bloomberg.com' and a description: 'Bloomberg delivers business and markets news, data, analysis, and video to the world, featuring stories from Businessweek and Bloomberg News.'. The fifth result is from 'https://www.ap.org' with the title 'The Associated Press - Video, photo, text, audio, data news ...' and a description: 'News and services that expand the reach of factual reporting.'. The sixth result is from 'https://www.bostonglobe.com' with the title 'The Boston Globe' and a description: '3 days ago — New England's best source for news, sports, opinion and entertainment. The Globe brings you breaking news, Spotlight Team investigations, ...'. The seventh result is from 'https://www.theatlantic.com' with the title 'The Atlantic' and a description: 'The Atlantic covers news, politics, culture, technology, health, and more, through its articles, podcasts, videos, and flagship magazine.'. The eighth result is from 'https://www.forbes.com' with the title 'Forbes' and a description: 'Forbes is a global media company, focusing on business, investing, technology, entrepreneurship, leadership, and lifestyle.'.

Google

related:nytimes.com

All Images Maps Shopping More Tools

8 results (0.38 seconds)

<https://www.usatoday.com> ▼

USA TODAY: Latest World and US News - USATODAY.com

USA TODAY delivers current local and national news, sports, entertainment, finance, technology, and more through award-winning journalism, photos, ...

<https://www.washingtonpost.com> ▼

The Washington Post: Breaking News, World, US, DC News ...

Breaking news and analysis on politics, business, world national news, entertainment more. In-depth DC, Virginia, Maryland news coverage including traffic, ...

<https://www.reuters.com> › ... ▼

Reuters: Breaking International News & Views

Warren Buffett on Saturday used the annual meeting of Berkshire Hathaway Inc to reveal major new investments including a bigger stake in Activision Blizzard ...

<https://www.bloomberg.com> ▼

Bloomberg.com

Bloomberg delivers business and markets news, data, analysis, and video to the world, featuring stories from Businessweek and Bloomberg News.

<https://www.ap.org> ▼

The Associated Press - Video, photo, text, audio, data news ...

News and services that expand the reach of factual reporting.

<https://www.bostonglobe.com> ▼

The Boston Globe

3 days ago — New England's best source for news, sports, opinion and entertainment. The Globe brings you breaking news, Spotlight Team investigations, ...

<https://www.theatlantic.com> ▼

The Atlantic

The Atlantic covers news, politics, culture, technology, health, and more, through its articles, podcasts, videos, and flagship magazine.

<https://www.forbes.com> ▼

Forbes

Forbes is a global media company, focusing on business, investing, technology, entrepreneurship, leadership, and lifestyle.

Figure 6: Applying The info: Filter

The screenshot shows a Google search results page for the query 'info:nytimes.com'. The search bar at the top contains the query and a magnifying glass icon. Below the search bar, there are navigation links for 'All', 'News', 'Images', 'Videos', 'Maps', and 'More', along with a 'Tools' link on the right. The search results are displayed below the navigation links. The first result is from 'https://help.nytimes.com' and is titled 'Contact us - Help - The New York Times'. The second result is also from 'https://help.nytimes.com' and is titled 'Help - The New York Times'. The third result is from 'https://help.nytimes.com' and is titled 'Contact The New York Times - Help'. Below the search results, there is a section titled 'People also ask' which contains four questions: 'How do I send an email to the New York Times?', 'How do I cancel my New York Times subscription online?', 'How do I contact my New York Times subscription?', and 'How do I suspend Nytimes delivery?'. Below the 'People also ask' section, there are three more search results. The first is from 'https://www.nytco.com' and is titled 'Contact | The New York Times Company'. The second is from 'https://subscribe.inyt.com' and is titled 'The New York Times International Edition Home Delivery ...'. The third is from 'https://www.bradley.edu' and is titled 'NYTimes.com | Service Desk | Get Help - Bradley University'. The final result is from 'https://en.wikipedia.org' and is titled 'The New York Times - Wikipedia'.

Google

info:nytimes.com

Search

All News Images Videos Maps More Tools

About 96,500,000 results (0.56 seconds)

<https://help.nytimes.com> › 115015385887-Contact-us

Contact us - Help - The New York Times

Select a topic below for **information** on how to contact our Newsroom. Send a Confidential News Tip.

[Contact The New York Times](#) · [Cancel Your Subscription](#) · [Privacy FAQ](#)

<https://help.nytimes.com> › en-us

Help - The New York Times

How can we help you? Find **information** about our coverage, products, subscriptions and more. Here's how you can...

<https://help.nytimes.com> › en-us › sections › 11500386...

Contact The New York Times - Help

Can't find what you're looking for? Review our Help topics or chat with one of our Customer Care advocates. Chat with us. Contact us.

People also ask

- How do I send an email to the New York Times?
- How do I cancel my New York Times subscription online?
- How do I contact my New York Times subscription?
- How do I suspend Nytimes delivery?

Feedback

<https://www.nytco.com> › contact

Contact | The New York Times Company

International Subscriptions NYTIsubs@nytimes.com. Distribution. Helen Konstantopoulos
International Circulation and Group Digital Vice President

<https://subscribe.inyt.com>

The New York Times International Edition Home Delivery ...

Get The **New York Times** International Edition delivered to your door. Now more essential than ever. Make great savings on a subscription.

<https://www.bradley.edu> › sites › servicedesk › nytimes

NYTimes.com | Service Desk | Get Help - Bradley University

NYTimes.com is a multi-platform news tool that provides full access to **New ...** reference and archival **information**, photos, graphics, audio and video files ...

<https://en.wikipedia.org> › wiki › The_New_York_Times

The New York Times - Wikipedia

Part 2: Explore the WHOIS Database:

The WHOIS database is another valuable resource for organizational footprinting and reconnaissance operations. It acts as a basic DNS lookup service that an attacker can use to gather the IP addresses of the organization they wish to attack or defend. The screenshots below show the results of using the WHOIS database to look up our target organization Arbys.

Figure 7: WHOIS Arbys

arbys.com
whois information

Whois DNS Records Diagnostics

cache expires in and 0 seconds
[refresh](#)

Registrar Info	
Name	CSC CORPORATE DOMAINS, INC.
Whois Server	whois.corporatedomains.com
Referral URL	www.cscprotectsbrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited

Important Dates	
Expires On	2022-11-04
Registered On	1997-04-14
Updated On	2021-10-31

Name Servers	
dee.ns.cloudflare.com	173.245.58.93
javon.ns.cloudflare.com	108.162.195.108

Part 4: Using Domain Dossier WHOIS Function

CentralOps is an alternative to the WHOIS lookup done in the Kali VM. The information displayed by centralops is generally much more verbose, as the figures below demonstrate.

Figure 8: Domain Dossier of MIT:

Address lookup

canonical name mit.edu.
aliases
addresses 104.105.224.130
2600:1407:a800:181::255e
2600:1407:a800:193::255e

Domain Whois record

Queried whois.educause.net with "mit.edu"...

Domain Name: MIT.EDU

Registrant:

Massachusetts Institute of Technology
77 Massachusetts Ave
Cambridge, MA 02139
USA

Administrative Contact:

Mark Silis
Massachusetts Institute of Technology
MIT Room W92-167, 77 Massachusetts Avenue
Cambridge, MA 02139-4307
USA
+1.6173245900
mark@mit.edu

Technical Contact:

MIT Network Operations
Massachusetts Institute of Technology
MIT Room W92-167, 77 Massachusetts Avenue
Cambridge, MA 02139-4307
USA
+1.6172538400
noc@mit.edu

Name Servers:

EUR5.AKAM.NET
USW2.AKAM.NET
ASIA1.AKAM.NET
USE5.AKAM.NET
USE2.AKAM.NET
ASIA2.AKAM.NET
NS1-173.AKAM.NET
NS1-37.AKAM.NET

Domain record activated: 23-May-1985
Domain record last updated: 08-Jun-2021
Domain expires: 31-Jul-2024

-- end --

[URL for this output](#) | [return to CentralOps.net](#), a service of Hexillion

Figure 9: Domain Dossier of Arbys

Address lookup

canonical name www.arbys.com.

aliases

addresses 104.18.33.167
172.64.154.89
2606:4700:4400::6812:21a7
2606:4700:4400::ac40:9a59

Domain Whois record

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

```
Domain Name: ARBYS.COM
Registry Domain ID: 3167276_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2021-10-31T05:10:35Z
Creation Date: 1997-04-14T04:00:00Z
Registry Expiry Date: 2022-11-04T18:59:49Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: DEE.NS.CLOUDFLARE.COM
Name Server: JAVON.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-05-01T05:18:19Z <<<
```

Queried whois.corporatedomains.com with "Arbys.com"...

Part 5: DNS Reconnaissance

The host utility built into our Kali VM can be used for dns lookup purposes, as shown in the screenshots below. Hackers can use the DNS footprint of organizations to determine what subdomains to attack/which subdomains of an organization are vulnerable to attack.

Figure 10: Using host For DNS Lookup

```
(kali㉿kali)-[~]
$ host facebook.com
facebook.com has address 157.240.18.35
facebook.com has IPv6 address 2a03:2880:f127:283:face:b00c:0:25de
facebook.com mail is handled by 10 smtpin.vvv.facebook.com.

(kali㉿kali)-[~]
$ host Arbys.com
Arbys.com has address 104.18.33.167
Arbys.com has address 172.64.154.89
Arbys.com has IPv6 address 2606:4700:4400::6812:21a7
Arbys.com has IPv6 address 2606:4700:4400::ac40:9a59
Arbys.com mail is handled by 20 alt1.us.email.fireeyecloud.com.
Arbys.com mail is handled by 30 alt2.us.email.fireeyecloud.com.
Arbys.com mail is handled by 40 alt3.us.email.fireeyecloud.com.
Arbys.com mail is handled by 10 primary.us.email.fireeyecloud.com.

(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ host 157.240.18.35
35.18.240.157.in-addr.arpa domain name pointer edge-star-mini-shv-02-ort2.facebook.com.

(kali㉿kali)-[~]
$ host 172.64.154.89
Host 89.154.64.172.in-addr.arpa. not found: 3(NXDOMAIN)

(kali㉿kali)-[~]
$ host 104.18.33.167
Host 167.33.18.104.in-addr.arpa. not found: 3(NXDOMAIN)
```

Figure 11: DNS servers for zonetransfer.me

```
(kali㉿kali)-[~]  
$ host -t ns zonetransfer.me  
zonetransfer.me name server nsztm1.digi.ninja.  
zonetransfer.me name server nsztm2.digi.ninja.
```

```
(kali㉿kali)-[~]  
$ host -t ns zonetransfer.me 8.8.8.8  
Using domain server:  
Name: 8.8.8.8  
Address: 8.8.8.8#53  
Aliases:  
  
zonetransfer.me name server nsztm2.digi.ninja.  
zonetransfer.me name server nsztm1.digi.ninja.
```

Using the default DNS server

Figure 12: Using host to view DNS records

```
(kali㉿kali)-[~]  
$ host -t MX zonetransfer.me  
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.  
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.  
zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.COM.  
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.  
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.  
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.  
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.
```

```
(kali㉿kali)-[~]  
$ host -t NS zonetransfer.me  
zonetransfer.me name server nsztml.digi.ninja.  
zonetransfer.me name server nsztml2.digi.ninja.
```

```
(kali㉿kali)-[~]  
$ host -t TXT zonetransfer.me  
zonetransfer.me descriptive text "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04  
VLMewxA"
```

```
(kali㉿kali)-[~]  
$ host -t cname zonetransfer.me  
zonetransfer.me has no CNAME record
```

```
(kali㉿kali)-[~]  
$ host -t SOA zonetransfer.me  
zonetransfer.me has SOA record nsztml.digi.ninja. robin.digi.ninja. 2019100801 172800 900 12096  
00 3600
```

Figure 13: Using dig for DNS lookup and Tracing

```
(kali㉿kali)-[~]  
$ dig zonetransfer.me +short  
5.196.105.14  
  
(kali㉿kali)-[~]  
$ dig zoneedit.com +short  
64.68.200.42
```

```
(kali㉿kali)-[~]  
$ dig zonetransfer.me +trace  
  
<<>> DiG 9.17.19-3-Debian <<>> zonetransfer.me +trace  
; global options: +cmd  
308179 IN NS k.root-servers.net.  
308179 IN NS f.root-servers.net.  
308179 IN NS b.root-servers.net.  
308179 IN NS l.root-servers.net.  
308179 IN NS c.root-servers.net.  
308179 IN NS j.root-servers.net.  
308179 IN NS h.root-servers.net.  
308179 IN NS d.root-servers.net.  
308179 IN NS g.root-servers.net.  
308179 IN NS e.root-servers.net.  
308179 IN NS i.root-servers.net.  
308179 IN NS a.root-servers.net.  
308179 IN NS m.root-servers.net.  
481021 IN RRSIG NS 8 0 518400 20220513170000 20220430160000 476  
1 . U54Jh0Yyk1o7HuQk628T3xAI2tDyIB/Jqlfz5TjpvQRKVrcvx050hvmU w3P+AHvTAWKgi3jWThI9qRFRU0XAaKeMt  
PKLNV3d6XApCuL5wL7Rl5e bmoYHjUQ7E4SF6p32qnpIGFRPURVBSh6AoPx2bSM5VJ60xzK79HTz0iy ges7pBsJ78pEK2  
Zyd/YeyFjS/PcDuqgE8gZ9WHjkaKkvI4C3aRN/7vD 2FZ/FoF5V4sMtSyUyzD7LIivK0vIaq+kVq/Md3qmehY+Lf+AwYzA  
J3TU P40UNX+LLJ0ZdAxxJP0H0Do+l8bIJEdk8tN986030Dw1fUlVFYSFDqSh PVfPKQ=  
; Received 1137 bytes from 216.47.143.106#53(216.47.143.106) in 1088 ms
```

Part 6: Collecting Information With TheHarvester

TheHarvester is a widely used command line utility employed by ethical hackers to footprint an organization along with “Google Hacking” and DNS reconnaissance. TheHarvester is particularly good at crawling the web for various bits of information regarding a target. And can be configured with a wide variety of command line flags to suit almost any application.

Figure 14: Using TheHarvester to Find Interesting URLs In the iit Domain

```
[*] Interesting Urls found: 26
http://hawk.iit.edu
http://mice.iit.edu/interdit.phantesques.oufement/amassent/mycelium/biot
http://mypages.iit.edu/~Ilsamp-iit/
http://mytest110.banner.iit.edu
http://voices.iit.edu/search_results
http://www.cs.iit.edu/~cs561/cs350/intro/mips5.htm
https://alumni.iit.edu/coc-ethics-discussion?bbeml=tp-eedIiK9_DUuz9aUDcc2V6g.jTx20tH0NGUmPcPVnYTyN8w.rZe0PhIZCGk-8MCo_LUGvSA.lUHqXT4er3Ee67Y7ZtXYpIQ
https://alumni.iit.edu/umil-scholarship
https://alumni.kentlaw.iit.edu/admin/home
https://jalgstat.library.iit.edu/?journal=jalgstat
https://login.iit.edu/cas/login
https://login.iit.edu/cas/login?service=https%3A%2F%2Flogin.iit.edu%2Fiit-sso-gateway%2Flogin
https://ots.iit.edu/help-and-support
https://sga.iit.edu/w/index.php/Organic_Male_Enhancement_And_Can_A_Penis_Grow
https://stuart.iit.edu/
https://web.iit.edu/
https://web.iit.edu/shwc/insurance
https://web.iit.edu/shwc/services/wellness-resources
https://www.ifsh.iit.edu/
https://www.ifsh.iit.edu/fspca
https://www.ifsh.iit.edu/fspca/courses/intentional-adulteration
https://www.iit.edu/
https://www.iit.edu/bursar/payment_methods.shtml
https://www.iit.edu/elevate
https://www.iit.edu/utp
https://www.kentlaw.iit.edu/
```

Figure 15: List of hosts in the Domain

```
[*] IPs found: 11349
3.86.37.148
3.94.220.188
3.94.221.7
3.95.47.25
3.131.199.74
3.210.18.189
3.211.182.162
3.212.68.67
3.214.17.69
3.215.76.215
3.224.15.160
10.21.3.31
10.21.3.32
10.21.7.23
10.22.3.31
10.22.3.32
10.22.5.44
10.22.5.58
10.24.2.33
10.24.3.42
10.24.3.43
10.24.3.44
10.24.3.45
10.24.3.51
10.24.5.45
10.24.5.48
10.24.5.78
10.40.0.50
10.47.159.75
10.131.110.44
12.2.169.145
13.56.128.144
```

Figure 16: Configuring TheHarvester With Command Line Flags

```
(kali㉿kali)-[~]
$ theHarvester -d iit.edu -l 500 -b bing

*****
*
* [TheHarvester]
*
* theHarvester 4.0.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: iit.edu

    Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 1
____
finaid@iit.edu

[*] Hosts found: 6
____
blackboard.iit.edu:107.20.37.166, 52.45.145.243
ethics.iit.edu:216.47.147.243
my.iit.edu:216.47.143.60
ots.iit.edu:50.19.226.237
www.iit.edu:50.19.226.237
www.kentlaw.iit.edu:50.19.226.237
```