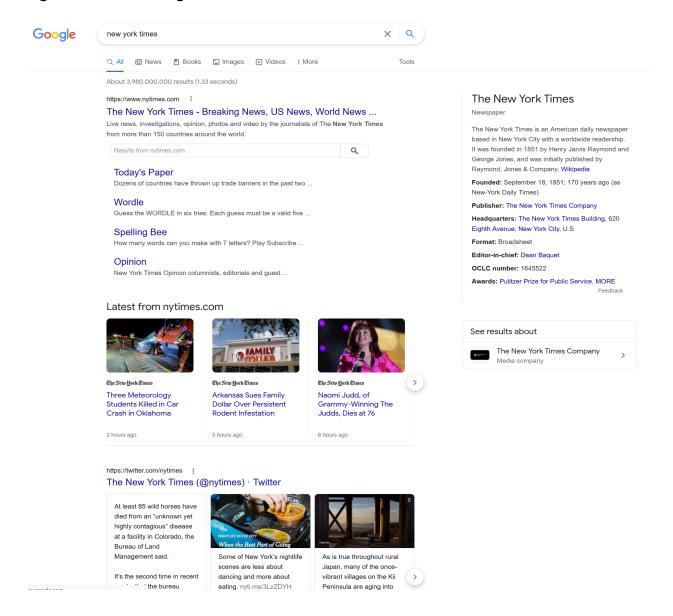
## Lab 5: Gathering Target Information - Footprinting and Social Engineering

### 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"



## Figure 2: Applying The site: Filter

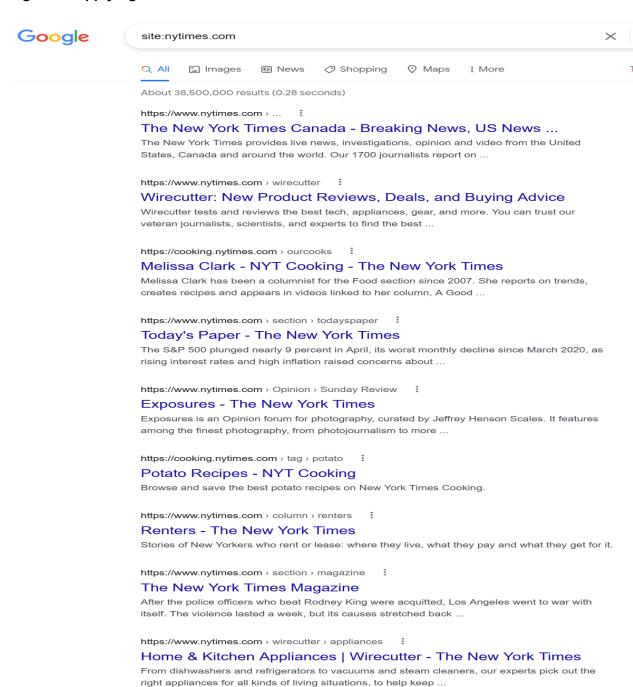


Figure 3: Applying The inurl: Filter

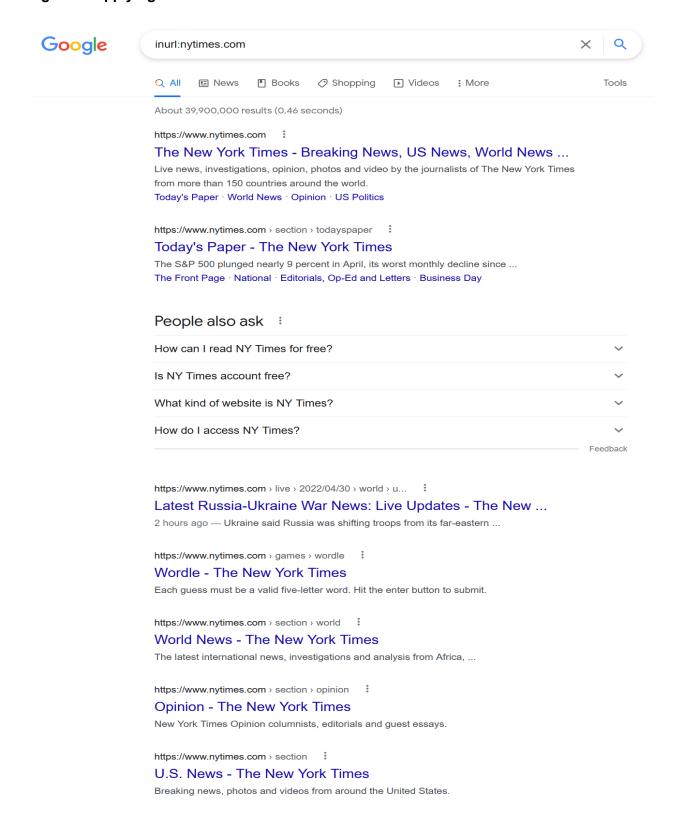
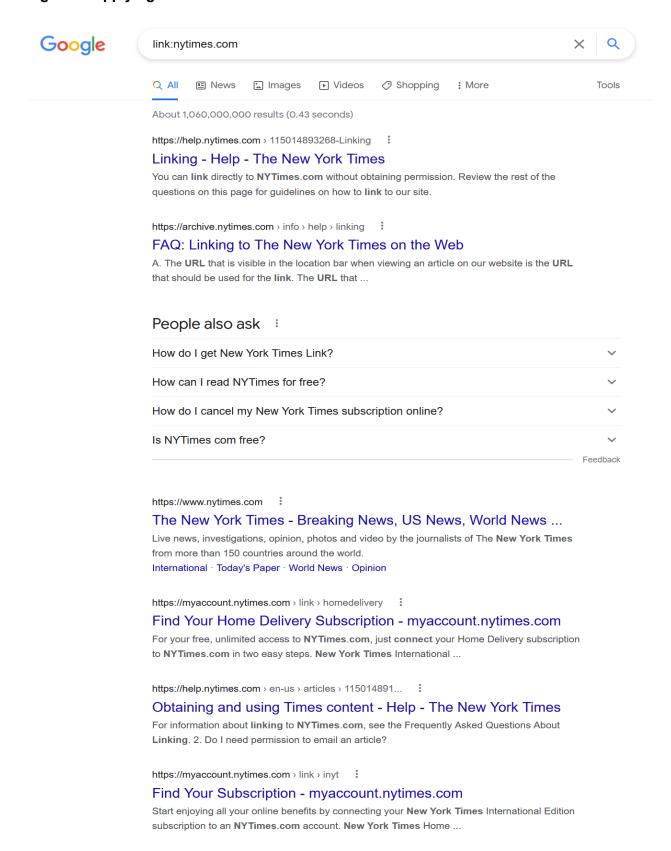
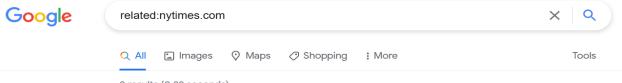


Figure 4: Applying The link: Filter



## Figure 5: Applying The related: Filter



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. Indepth 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

 $3~{\rm days}$  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

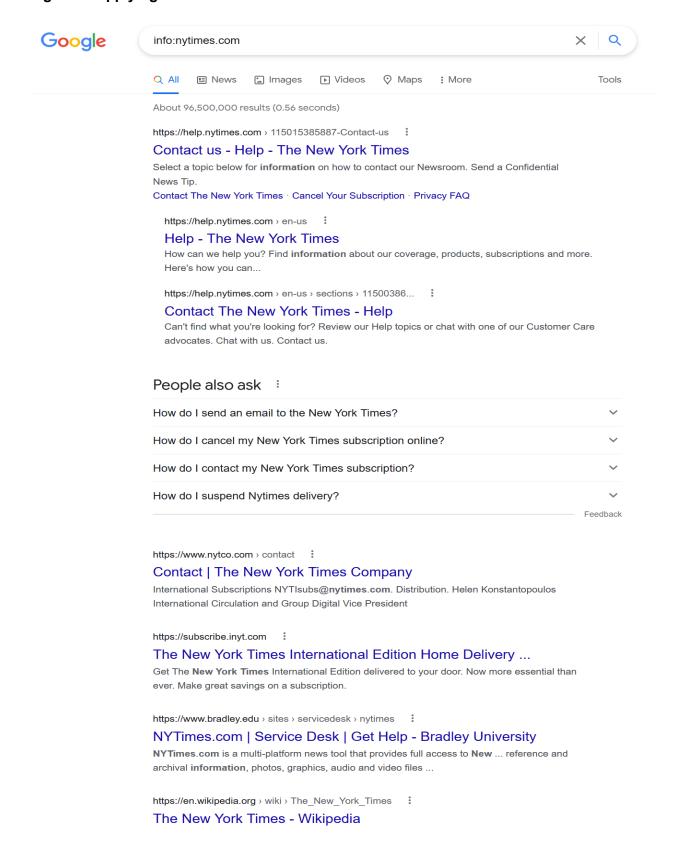
The Atlantic covers news, politics, culture, technology, health, and more, through its articles, podcasts, videos, and flagship magazine.

https://www.forbes.com •

### **Forbes**

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

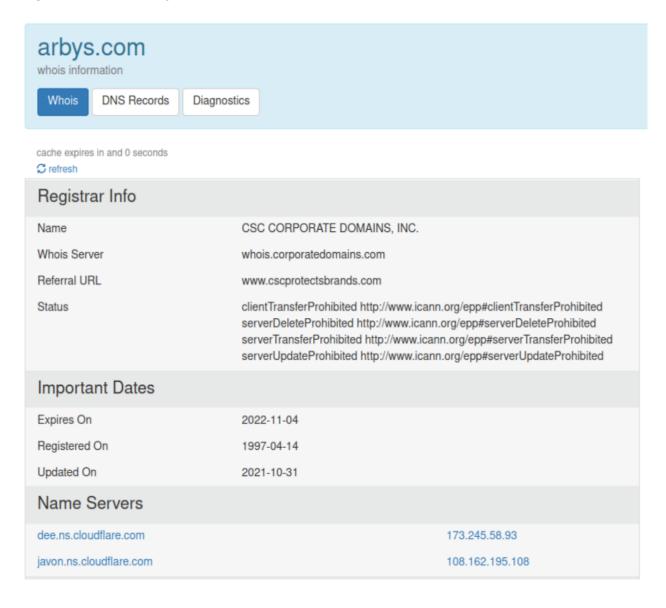
Figure 6: Applying The info: Filter



## 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



## 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
        +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)-[~]
```

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 NS zonetransfer.me
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.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 nsztm1.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
                                308179 IN
                                                      NS
                                                                  k.root-servers.net.
                                                                 f.root-servers.net.
                                                                b.root-servers.net.
                                                                l.root-servers.net.
                                                               c.root-servers.net.
j.root-servers.net.
h.root-servers.net.
                                                                d.root-servers.net.
                                                                g.root-servers.net.
e.root-servers.net.
                                                                i.root-servers.net.
                                                                a.root-servers.net.
                                                                  m.root-servers.net.
                                                    RRSIG NS 8 0 518400 20220513170000 20220430160000 476
1 . U54Jh0Yyk1o7HuQk628T3xAI2tDyIB/Jqlfz5TjpvQRKVrcvx050hvmU w3P+AHvTAwKgi3jWThI9qRFrU0XAaKeMt
PKLNV3d6XApCuL5wl7Rl5e bmoYHjUQ7E4SF6p32qnpiGFRPURVBSH6AoPx2bSM5VJ60xzK79HTzOiy 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 footpring an organization along with "Google Hacking" and DNS reconnaissance. TheHarverster 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/-Itsamp-iit/
http://mypages.iit.edu/-Itsamp-iit/
http://mytestillo.banner.iit.edu
http://voices.iit.edu/scafo/cs53fo/s536/intro/mips5.htm
https://alumni.cs.iit.edu/co-cstbics-discussion?bbeml=tp-eedIiK9_DUuz9aUDcc2V6g.jTx20tH0NGUmPcPVnYTyN8w.rZe0PhIZCGk-8MCo_LUGvSA.lUHqXT4er3EeG7Y7ZtXYpIQ
https://alumni.iit.edu/co-cethics-discussion?bbeml=tp-eedIiK9_DUuz9aUDcc2V6g.jTx20tH0NGUmPcPVnYTyN8w.rZe0PhIZCGk-8MCo_LUGvSA.lUHqXT4er3EeG7Y7ZtXYpIQ
https://alumni.iit.edu/co-cethics-discussion?bbeml=tp-eedIiK9_DUuz9aUDcc2V6g.jTx20tH0NGUmPcPVnYTyN8w.rZe0PhIZCGk-8MCo_LUGvSA.lUHqXT4er3EeG7Y7ZtXYpIQ
https://alumni.iit.edu/cas/login
https://alumni.kentlaw.iit.edu/journal=jalgstat
https://alumni.kentlaw.iit.edu/journal=jalgstat
https://login.iit.edu/cas/login?service-https%3A%2F%2Flogin.iit.edu%2Fiit-sso-gateway%2Flogin
https://login.iit.edu/cas/login?service-https%3A%2F%2Flogin.iit.edu%2Fiit-sso-gateway%2Flogin
https://si.iit.edu/windex.php/Organic_Male_Enhancement_And_Can_A_Penis_Grow
https://stuart.iit.edu/
https://stuart.iit.edu/horbar/services/wellness-resources
https://www.ish.iit.edu/shwc/insurance
https://www.ish.iit.edu/fspca/courses/intentional-adulteration
https://www.ifsh.iit.edu/fspca/courses/intentional-adulteration
https://www.ifsh.iit.edu/fspca/courses/intentional-adulteration
https://www.iit.edu/bursar/payment_methods.shtml.
https://www.iit.edu/vlevaser
https://www.iit.edu/vlevaser
https://www.iit.edu/vlevaser
https://www.iit.edu/vlevaser
https://www.iit.edu/ushursar/payment_methods.shtml.
```

Figure 15: List of hosts in the Domain

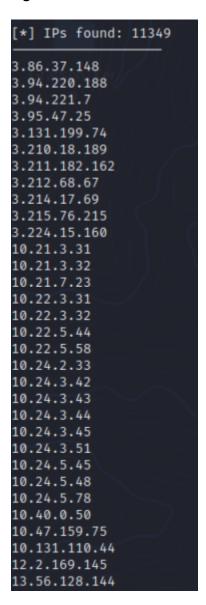


Figure 16: Configuring The Harvster With Command Line Flags

```
(kali⊛kali)-[~]
 -$ theHarvester -d iit.edu -l 500 -b bing
 theHarvester 4.0.2
        Searching 0 results.
[*] 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
```