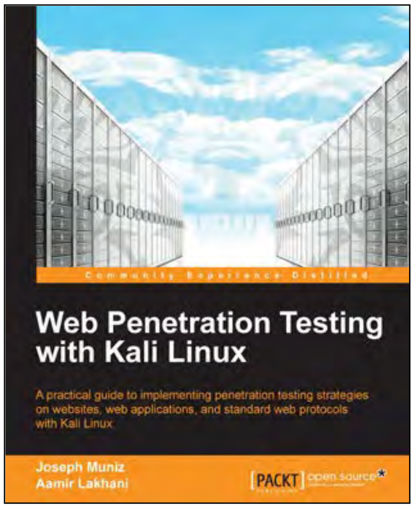
Web Penetration Testing with Kali Linux

Joseph Muniz

Aamir Lakhani


Community Experience Distilled
Web Penetration Testing with Kali Linux
A practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux
Joseph Muniz
Aamir Lakhani
PACKT open source

Chapter No. 2
"Reconnaissance"

In this package, you will find:

A Biography of the authors of the book

A preview chapter from the book, Chapter NO.2 "Reconnaissance"

A synopsis of the book’s content

Information on where to buy this book

About the Authors

Joseph Muniz is a technical solutions architect and security researcher. He started his career in software development and later managed networks as a contracted technical resource. Joseph moved into consulting and found a passion for security while meeting with a variety of customers. He has been involved with the design and implementation of multiple projects ranging from Fortune 500 corporations to large federal networks.

Joseph runs `TheSecurityBlogger.com` website, a popular resources regarding security and product implementation. You can also find Joseph speaking at live events as well as involved with other publications. Recent events include speaker for Social Media Deception at the 2013 ASIS International conference, speaker for Eliminate Network Blind Spots with Data Center Security webinar, speaker for Making Bring Your Own Device (BYOD) Work at the Government Solutions Forum, Washington DC, and an article on Compromising Passwords in PenTest Magazine – Backtrack Compendium, July 2013.

Outside of work, he can be found behind turntables scratching classic vinyl or on the soccer pitch hacking away at the local club teams.

> This book could not have been done without the support of my charming wife Ning and creative inspirations from my daughter Raylin. I also must credit my passion for learning to my brother Alex, who raised me along with my loving parents Irene and Ray. And I would like to give a final thank you to all of my friends, family, and colleagues who have supported me over the years.

Aamir Lakhani is a leading Cyber Security and Cyber Counterintelligence architect. He is responsible for providing IT security solutions to major commercial and federal enterprise organizations.

Lakhani leads projects that implement security postures for Fortune 500 companies, the US Department of Defense, major healthcare providers, educational institutions, and financial and media organizations. Lakhani has designed offensive counter defense measures for defense and intelligence agencies, and has assisted organizations in defending themselves from active strike back attacks perpetrated by underground cyber groups. Lakhani is considered an industry leader in support of detailed architectural engagements and projects on topics related to cyber defense, mobile application threats, malware, and Advanced Persistent Threat (APT) research, and Dark Security. Lakhani is the author and contributor of several books, and has appeared on National Public Radio as an expert on Cyber Security.

Writing under the pseudonym Dr. Chaos, Lakhani also operates the `DrChaos.com blog.` In their recent list of 46 Federal Technology Experts to Follow on Twitter, Forbes magazine described Aamir Lakhani as "a blogger, infosec specialist, superhero..., and all around good guy."

> I would like to dedicate this book to my parents, Mahmood and Nasreen, and sisters, Noureen and Zahra. Thank you for always encouraging the little hacker in me. I could not have done this without your support. Thank you mom and dad for your sacrifices. I would also additionally like to thank my friends and colleagues for your countless encouragement and mentorship. I am truly blessed to be working with the smartest and most dedicated people in the world.

Web Penetration Testing with Kali Linux

Kali is a Debian Linux based Penetration Testing arsenal used by security professionals (and others) to perform security assessments. Kali offers a range of toolsets customized for identifying and exploiting vulnerabilities in systems. This book is written leveraging tools available in Kali Linux released March 13th, 2013 as well as other open source applications.

Web Penetration Testing with Kali Linux is designed to be a guide for professional Penetration Testers looking to include Kali in a web application penetration engagement. Our goal is to identify the best Kali tool(s) for a specific assignment, provide details on using the application(s), and offer examples of what information could be obtained for reporting purposes based on expert field experience. Kali has various programs and utilities; however, this book will focus on the strongest tool(s) for a specific task at the time of publishing.

The chapters in this book are divided into tasks used in real world web application Penetration Testing. *Chapter 1, Penetration Testing and Setup*, provides an overview of Penetration Testing basic concepts, professional service strategies, background on the Kali Linux environment, and setting up Kali for topics presented in this book. *Chapters 2-6*, cover various web application Penetration Testing concepts including configuration and reporting examples designed to highlight if topics covered can accomplish your desired objective.

Chapter 7, Defensive Countermeasures, serves as a remediation source on systems vulnerable to attacks presented in previous chapters. *Chapter 8, Penetration Test Executive Report*, offers reporting best practices and samples that can serve as templates for building executive level reports. The purpose of designing the book in this fashion is to give the reader a guide for engaging a web application penetration with the best possible tool(s) available in Kali, offer steps to remediate vulnerability and provide how data captured could be presented in a professional manner.

What This Book Covers

Chapter 1, Penetration Testing and Setup, covers fundamentals of building a professional Penetration Testing practice. Topics include differentiating a Penetration Test from other services, methodology overview, and targeting web applications. This chapter also provides steps used to set up a Kali Linux environment for tasks covered in this book.

Chapter 2, Reconnaissance, provides various ways to gather information about a target. Topics include highlighting popular free tools available on the Internet as well as Information Gathering utilities available in Kali Linux.

Chapter 3, Server Side Attacks, focuses on identifying and exploiting vulnerabilities in web servers and applications. Tools covered are available in Kali or other open source utilities.

Chapter 4, Client Side Attacks, targets hosts systems. Topics include social engineering, exploiting host system vulnerabilities, and attacking passwords, as they are the most common means to secure host systems.

Chapter 5, Attacking Authentication, looks at how users and devices authenticate to web applications. Topics include targeting the process of managing authentication sessions, compromising how data is stored on host systems, and man-in-the-middle attack techniques. This chapter also briefly touches on SQL and Cross-Site Scripting attacks.

Chapter 6, Web Attacks, explores how to take advantage of web servers and compromise web applications using exploits such as browser exploitation, proxy attacks, and password harvesting. This chapter also covers methods to interrupt services using denial of service techniques.

Chapter 7, Defensive Countermeasures, provides best practices for hardening your web applications and servers. Topics include security baselines, patch management, password policies, and defending against attack methods covered in previous chapters. This chapter also includes a focused forensics section, as it is important to properly investigate a compromised asset to avoid additional negative impact.

Chapter 8, Penetration Test Executive Report, covers best practices for developing professional post Penetration Testing service reports. Topics include an overview of methods to add value to your deliverable, document formatting, and templates that can be used to build professional reports.

2
Reconnaissance

The term **Reconnaissance** by definition comes from the military warfare strategy of exploring beyond the area occupied by friendly forces to gain information about the enemy for future analysis or attack. Reconnaissance of computer systems is similar in nature, meaning typically a Penetration Tester or hacker will attempt to learn as much as possible about a target's environment and system traits prior to launching an attack. This is also known as establishing a *Footprint* of a target. Reconnaissance is typically passive in nature and in many cases not illegal (however, we are not lawyers and cannot offer legal advice) to perform as long as you don't complete a three-way handshake with an unauthorized system.

Examples of Reconnaissance include anything from researching a target on public sources such as Google, monitoring employee activity to learn operation patterns, and scanning networks or systems to gather information, such as manufacture type, operating system, and open communication ports. The more information that can be gathered about a target brings a better chance of identifying the easiest and fastest method to achieve a penetration goal, as well as best method to avoid existing security. Also, alerting a target will most likely cause certain attack avenues to close as a reaction to preparing for an attack. Kali's official slogan says this best:

> "*The quieter you become, the more you are able to hear*"

Reconnaissance services should include heavy documentation, because data found may be relevant at a later point in the penetration exercise. Clients will also want to know how specific data was obtained, and ask for references to resources. Examples are what tools were used to obtain the data or what publicfacing resources; for example, the specific search query in Google that was submitted to obtain the data. Informing a customer "you obtained the goal" isn't good enough, because the purpose of a Penetration Test is to identify weakness for future repairs.

Reconnaissance objectives

- **Target background**: What is the focus of the target's business?
- **Target's associates**: Who are the business partners, vendors, and customers?
- **Target's investment in security**: Are security policies advertised? What is the potential investment security, and user security awareness?
- **Target's business and security policies**: How does the business operate? Where are the potential weaknesses in operation?
- **Target's people**: What type of people work there? How can they become your asset for the attack?
- **Define targets**: What are the lowest hanging fruit targets? What should be avoided?
- **Target's network**: How do the people and devices communicate on the network?
- **Target's defenses**: What type of security is in place? Where is it located?
- **Target's technologies**: What technologies are used for e-mail, network traffic, storing information, authentication, and so on? Are they vulnerable?

Kali Linux contains an extensive catalog of tools titled **Information Gathering** specified for Reconnaissance efforts. It could fill a separate book to cover all tools and methods offered for Information Gathering. This chapter will focus on various web application Reconnaissance topics and relate the best tools found on the Internet as well as that offered by Kali Linux.

Initial research

Reconnaissance should begin with learning as much as possible about people and business associated with the target. *Sun Tzu* is credited with the phrase, "know your enemy" in the book, *The Art of War*. As a Penetration Tester, you need to know your target. If your target happens to be a website, you should look at all aspects of that website. It will give you a better understanding of how the site is maintained and run. Great Reconnaissance returns more possible vulnerabilities.

It is scary how much information is available on public sources. We have found the unimaginable, such as classified documents, passwords, vulnerability reports, undesirable photography, and access to security cameras. Many Penetration Testing project objectives start with leveraging information off public sources. Here are some starting points for gathering information from public sources.

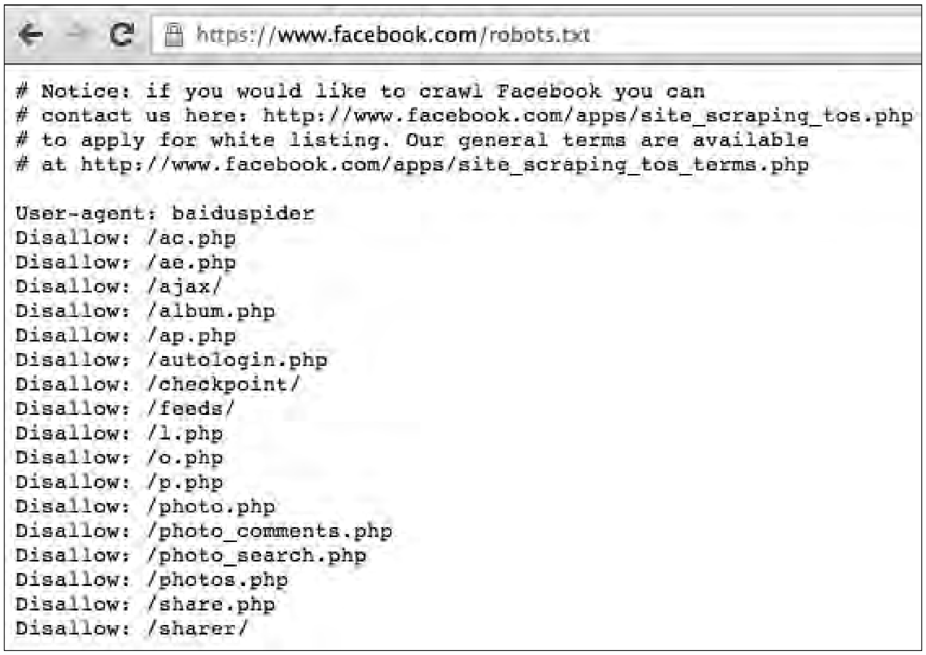
Company website

There is a lot of valuable information that can be obtained from a target's website. Most corporate websites list their executive team, public figures, and members from recruiting and human resource contacts. These can become targets for other search efforts and social engineering attacks.

More valuable information can be obtained by looking at what other companies are listed as partners, current job postings, business information, and security policies. Reconnaissance on a high-valued partner can be as important as the primary target, because partners may provide a new source for obtaining intelligence. An example is compromising a contracted resource that manages the helpdesk at a target's headquarters.

The `Robots.txt` file is publicly available and found on websites that gives instructions to web robots (also known as search engine spiders), about what is and not visible using the Robots Exclusion Protocol. The `Disallow: /` statement tells a browser not to visit a source; however, a Disallow can be ignored by giving a researcher intelligence on what a target hopes to not disclose to the public.

To view the `Robots.txt` file, find the `Robots.txt` file in the root directory of a target website. For example, adding the `Robots.txt` file to Facebook would look as shown in the following screenshot:

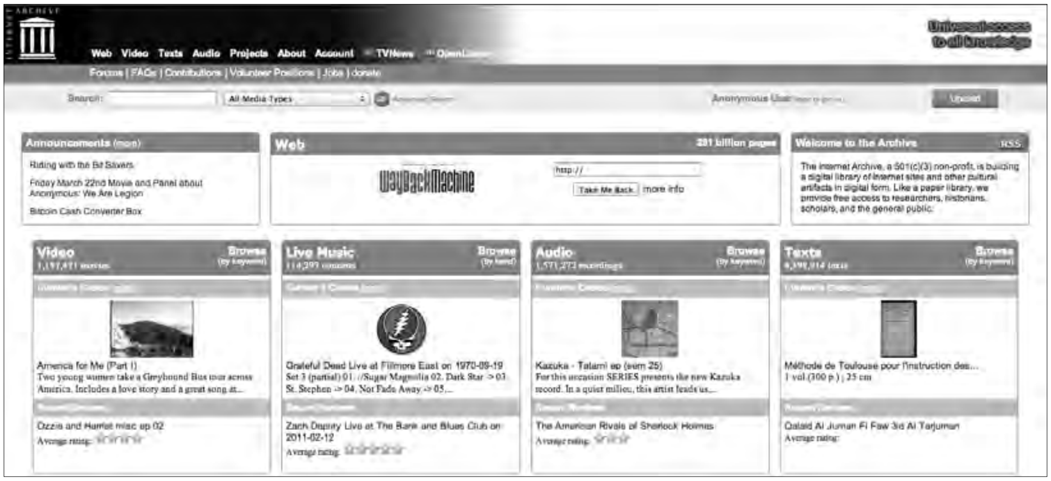


```
# Notice: if you would like to crawl Facebook you can
# contact us here: http://www.facebook.com/apps/site_scraping_tos.php
# to apply for white listing. Our general terms are available
# at http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: baiduspider
Disallow: /ac.php
Disallow: /ae.php
Disallow: /ajax/
Disallow: /album.php
Disallow: /ap.php
Disallow: /autologin.php
Disallow: /checkpoint/
Disallow: /feeds/
Disallow: /l.php
Disallow: /o.php
Disallow: /p.php
Disallow: /photo.php
Disallow: /photo_comments.php
Disallow: /photo_search.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /sharer/
```

Web history sources

There are archived versions of most public websites available on sources such as the **WayBack Machine** at `archive.org`. Interesting information can be found in an older version of a target's website, such as outdated organizational charts, phone numbers, customer intelligence, systems information listed in fields, such as `view source` or `/robots.txt`, older business partnerships, vulnerabilities fixed in later versions, and other useful data, the target doesn't want on the current website version. It is important to understand that the publicly available information is hard to remove completely, making historical sources a valuable place for Reconnaissance research.

To access the **WayBack Machine**, open up the web browser and navigate to `http://archive.org`, you will see the **Internet Archive WayBack Machine** in the middle of the page, as shown in the following screenshot:



Riding with the Bit Savers

Friday March 22nd Movie and Panel about Anonymous: We Are Legion

Bitcoin Cash Converter Box

The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public.

America for Me (Part I)
Two young women take a Greyhound Bus tour across America. Includes a love story and a great song at...

Ozzie and Harriet misc ep 02
Average rating:

Grateful Dead Live at Fillmore East on 1970-09-19
Set 3 (partial) 01. //Sugar Magnolia 02. Dark Star -> 03. St. Stephen -> 04. Not Fade Away -> 05....

Zach Deputy Live at The Bank and Blues Club on 2011-02-12
Average rating:

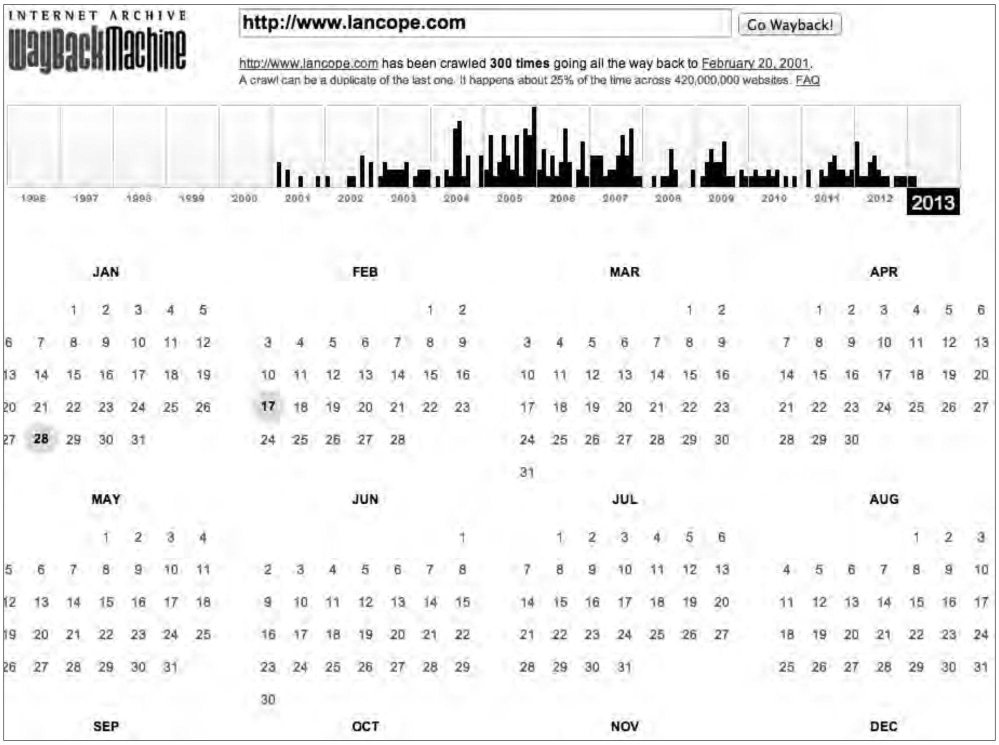
Kazuka - Tatami ep (sum 25)
For this occasion SERIES presents the new Kazuka record. In a quiet milieu, this artist leads us...

The American Rivals of Sherlock Holmes
Average rating:

Méthode de Toulouse pour l'instruction des...
1 vol.(300 p.) ; 25 cm

Qalaid Al Juman Fi Faw 3id Al Tarjuman
Average rating:

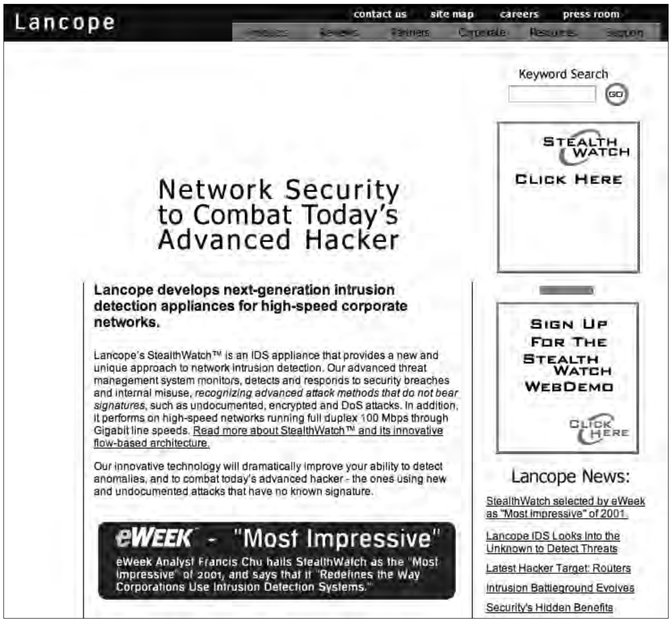
Type the URL you would like to browse and see if any archives have been captured. A history of the archive can be viewed here, as shown in the following screenshot:



http://www.lancope.com has been crawled **300 times** going all the way back to February 20, 2001.

A crawl can be a duplicate of the last one. It happens about 25% of the time across 420,000,000 websites. FAQ

As a Penetration Tester, this is a valuable tool, because it doesn't leave evidence of Reconnaissance on your target. In fact, your target is never even touched using this tool. All the information has been archived online in the **Wayback Machine**. The next two screenshots show `www.lancope.com` in 2002 compared to 2013:



Network Security to Combat Today's Advanced Hacker

Lancope develops next-generation intrusion detection appliances for high-speed corporate networks.

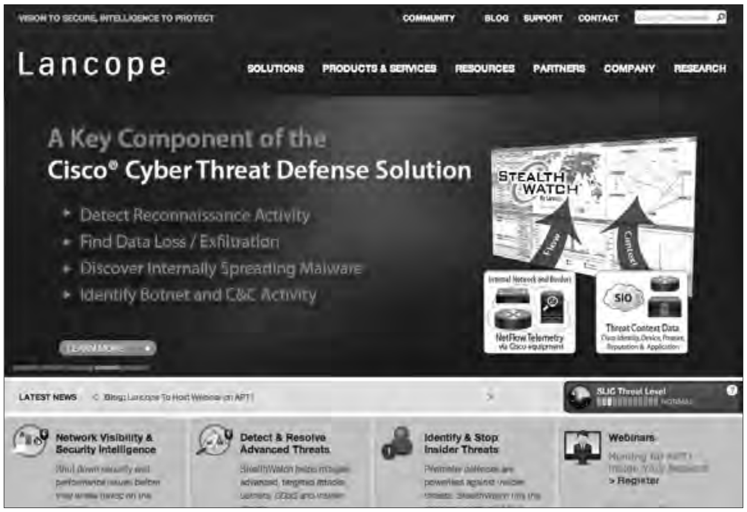
Lancope's StealthWatch™ is an IDS appliance that provides a new and unique approach to network intrusion detection. Our advanced threat management system monitors, detects and responds to security breaches and internal misuse, *recognizing advanced attack methods that do not bear signatures*, such as undocumented, encrypted and DoS attacks. In addition, it performs on high-speed networks running full duplex 100 Mbps through Gigabit line speeds. Read more about StealthWatch™ and its innovative flow-based architecture.

Our innovative technology will dramatically improve your ability to detect anomalies, and to combat today's advanced hacker - the ones using new and undocumented attacks that have no known signature.

eWEEK - "Most Impressive"
eWeek Analyst Francis Chu hails StealthWatch as the "Most Impressive" of 2001, and says that it "Redefines the Way Corporations Use Intrusion Detection Systems."

Lancope News:

- StealthWatch selected by eWeek as "Most Impressive" of 2001.
- Lancope IDS Looks Into the Unknown to Detect Threats
- Latest Hacker Target: Routers
- Intrusion Battleground Evolves
- Security's Hidden Benefits



A Key Component of the
Cisco® Cyber Threat Defense Solution

- Detect Reconnaissance Activity
- Find Data Loss / Exfiltration
- Discover Internally Spreading Malware
- Identify Botnet and C&C Activity

LATEST NEWS Blog: Lancope To Host Webinar on APT1

Network Visibility & Security Intelligence

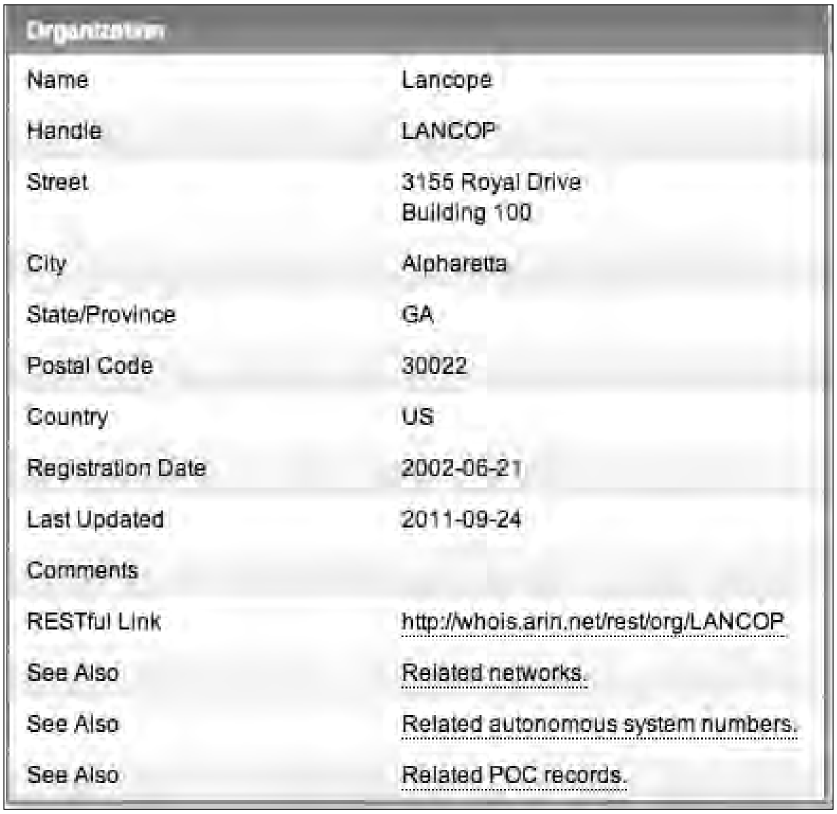
Detect & Resolve Advanced Threats

Identify & Stop Insider Threats

Webinars
> Register

Regional Internet Registries (RIRs)

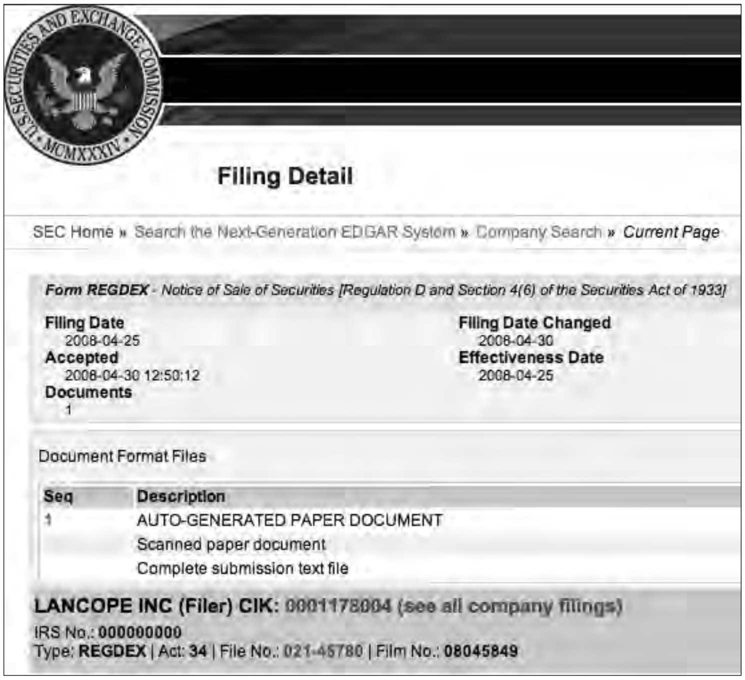
RIR is an organization that manages the allocation and registration of IP resources within a particular region of the world. There are five major RIRs: the USA, Canada, and parts of the Caribbean region can be found at `www.arin.net`. You can gather information on a target such as Lancope, as seen in the following screenshot:



Organization	
Name	Lancope
Handle	LANCOP
Street	3155 Royal Drive Building 100
City	Alpharetta
State/Province	GA
Postal Code	30022
Country	US
Registration Date	2002-06-21
Last Updated	2011-09-24
Comments	
RESTful Link	http://whois.arin.net/rest/org/LANCOP
See Also	Related networks.
See Also	Related autonomous system numbers.
See Also	Related POC records.

Electronic Data Gathering, Analysis, and Retrieval (EDGAR)

The EDGAR database contains registration statements, periodic reports, and other forms of information on companies since 1994. Companies in the United States of America are required by law to file, and all information is publicly available. The following two screenshots show public documents found while searching Lancope:



Filing Detail

SEC Home » Search the Next-Generation EDGAR System » Company Search » *Current Page*

Form REGDEX *- Notice of Sale of Securities [Regulation D and Section 4(6) of the Securities Act of 1933]*

Filing Date
2008-04-25
Accepted
2008-04-30 12:50:12
Documents
1

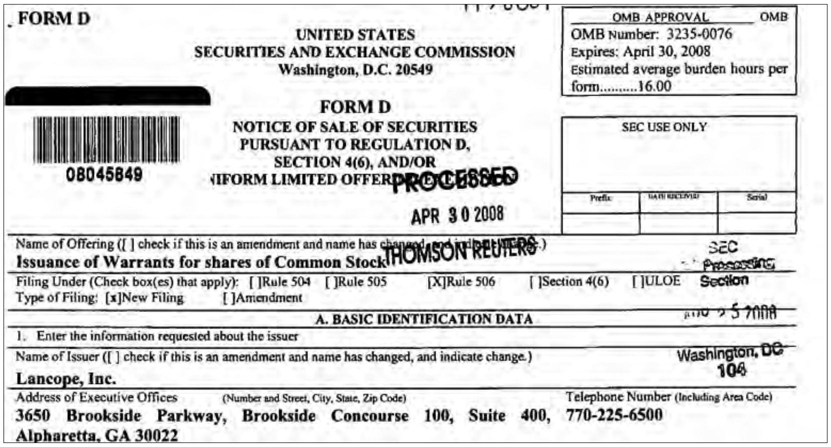
Filing Date Changed
2008-04-30
Effectiveness Date
2008-04-25

Document Format Files

Seq	Description
1	AUTO-GENERATED PAPER DOCUMENT
	Scanned paper document
	Complete submission text file

LANCOPE INC (Filer) CIK: 0001178004 (see all company filings)

IRS No.: **000000000**
Type: **REGDEX** | Act: **34** | File No.: 021-45780 | Film No.: **08045849**



FORM D

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

OMB APPROVAL OMB
OMB Number: 3235-0076
Expires: April 30, 2008
Estimated average burden hours per form..........16.00

[redacted]

08045849

FORM D
NOTICE OF SALE OF SECURITIES
PURSUANT TO REGULATION D,
SECTION 4(6), AND/OR
IIFORM LIMITED OFFER

PROCESSED
APR 3 0 2008
THOMSON REUTERS

SEC USE ONLY

Prefix	DATE RECEIVED	Serial

Name of Offering ([ ] check if this is an amendment and name has changed, and indicate change.)
Issuance of Warrants for shares of Common Stock

SEC
Processing
Section

Filing Under (Check box(es) that apply): [ ]Rule 504 [ ]Rule 505 [X]Rule 506 [ ]Section 4(6) [ ]ULOE
Type of Filing: [x]New Filing [ ]Amendment

5 2008

A. BASIC IDENTIFICATION DATA

1. Enter the information requested about the issuer

Name of Issuer ([ ] check if this is an amendment and name has changed, and indicate change.)
Lancope, Inc.

Washington, DC
104

Address of Executive Offices (Number and Street, City, State, Zip Code)
3650 Brookside Parkway, Brookside Concourse 100, Suite 400,
Alpharetta, GA 30022

Telephone Number (Including Area Code)
770-225-6500

Social media resources

Social media is everywhere, and in most cases, publicly accessible. Most people have a Facebook, LinkedIn, blogs, or other forms of cloud accounts containing valuable information. This information can be used as a means of social engineering intelligence from a target's current or previous staff. An example is searching `Glassdoor.com` to identify previous employees that are disgruntled, based on feedback.

There are many people finding web resources such as Maltego (found in Kali Linux) that can comb popular social media, public records, and job recruiting websites to fingerprint an individual based on limited information, such as a first and last name. A researcher could gather information such as everywhere an individual has lived, done business, people with which they socialize, special interests, favorite sport teams, and other useful data for future research and social engineering attacks.

Trust

Most people are naturally trusting and assume information posted on public sources is real. To test this concept, the writers of this book created a fake person through social media and pretended to be a new hire for a target company. The fake person would become friends with associates of our target, post fake holiday cards that are linked to a **BeEF** system designed to compromise vulnerable Internet browsers (using BeEF is covered later in this book), and captured sensitive information from compromised systems. We were able to map out the entire organization, obtain network information, and even had hardware shipped to us without an internal e-mail or phone number. Our fake person, Emily Williams isn't real, yet received job offers, was provided inside information, and access to events hosted by the target. Information is power, and people will give it to a requester who seems like they can be trusted.

More information on this project can be found at:
`http://www.thesecurityblogger.com/?p=1903`

Job postings

Job postings contain a wealth of knowledge about a target's environment. Job listings can provide details on what type of systems are installed, who manages them, how large the staff is, and the staff's skill level. Human Resource representatives are typically eager to share information with a potential new hire, which can be used as an avenue to inside information. An example is targeting a job posting for a Oracle developer to understand the hardware, version of Oracle, names of existing and previous administrators, existing operation issues, security gaps, and methods to access such as asking "can administrators work from home, and how do they access the systems?"

Another avenue to review is a job's expected salary, benefits, and turnover rate on popular job boards. These trends may uncover new vectors for attack. `Glassdoor.com` is an example of a popular source for this type of data.

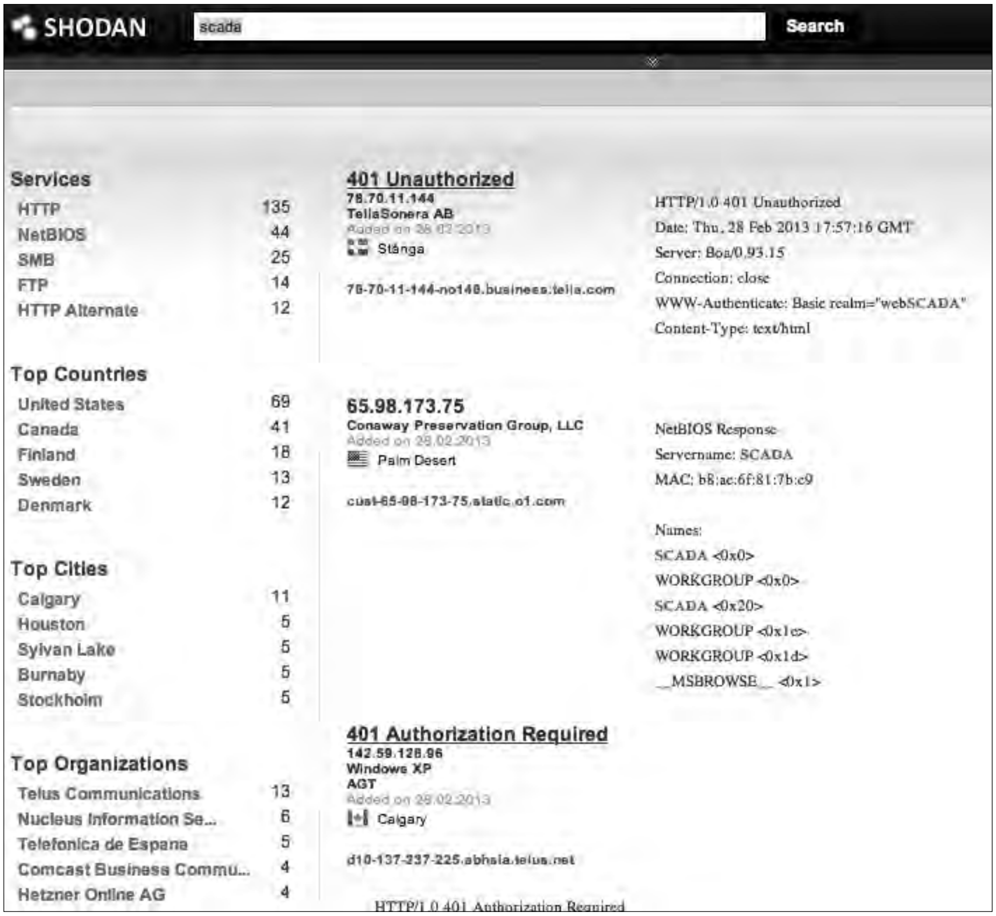
Location

The investment in cyber security for a target can typically be determined based on the level of physical security. One would assume a building with fences and armed guards would have a higher investment in cyber security than a target located within a public building. Online mapping sources such as Google maps can help identify where physical security is implemented, and trends on how people move to and from the target. Other areas of interest are identifying where a Penetration Tester could camp out to scan for wireless networks, and possible methods to bypass access controls, such as attire and badges used to obtain physical access.

Shodan

Shodan is a search engine that can identify a specific device, such as computer, router, server, using a variety of filters, such as metadata from system banners. For example, you can search for a specific system, such as a Cisco 3850, running a version of software such as IOS Version 15.0(1)EX.

The following example is a use case searching for any SCADA system with public Internet access, which in theory isn't supposed to exist however, Shodan can show this is not necessarily true. SCADA systems control things like power management and water treatment, so identifying public accessible systems is extremely bad!



Services	
HTTP	135
NetBIOS	44
SMB	25
FTP	14
HTTP Alternate	12

Top Countries	
United States	69
Canada	41
Finland	18
Sweden	13
Denmark	12

Top Cities	
Calgary	11
Houston	5
Sylvan Lake	5
Burnaby	5
Stockholm	5

Top Organizations	
Telus Communications	13
Nucleus Information Se...	6
Telefonica de Espana	5
Comcast Business Commu...	4
Hetzner Online AG	4

401 Unauthorized
78.70.11.144
TeliaSonera AB
Added on 28.02.2013
Stånga

78-70-11-144-no148.business.telia.com

```
HTTP/1.0 401 Unauthorized
Date: Thu, 28 Feb 2013 17:57:16 GMT
Server: Boa/0.93.15
Connection: close
WWW-Authenticate: Basic realm="webSCADA"
Content-Type: text/html
```

65.98.173.75
Conaway Preservation Group, LLC
Added on 28.02.2013
Palm Desert

cust-65-98-173-75.static.o1.com

```
NetBIOS Response
Servername: SCADA
MAC: b8:ac:6f:81:7b:c9

Names:
SCADA <0x0>
WORKGROUP <0x0>
SCADA <0x20>
WORKGROUP <0x1e>
WORKGROUP <0x1d>
__MSBROWSE__ <0x1>
```

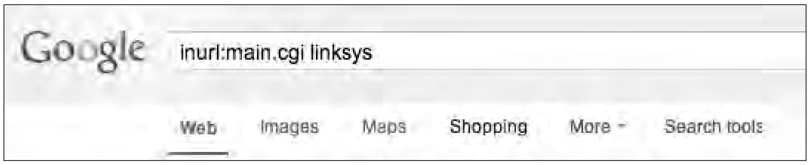
401 Authorization Required
142.59.128.96
Windows XP
AGT
Added on 28.02.2013
Calgary

d10-137-237-225.abhsia.telus.net

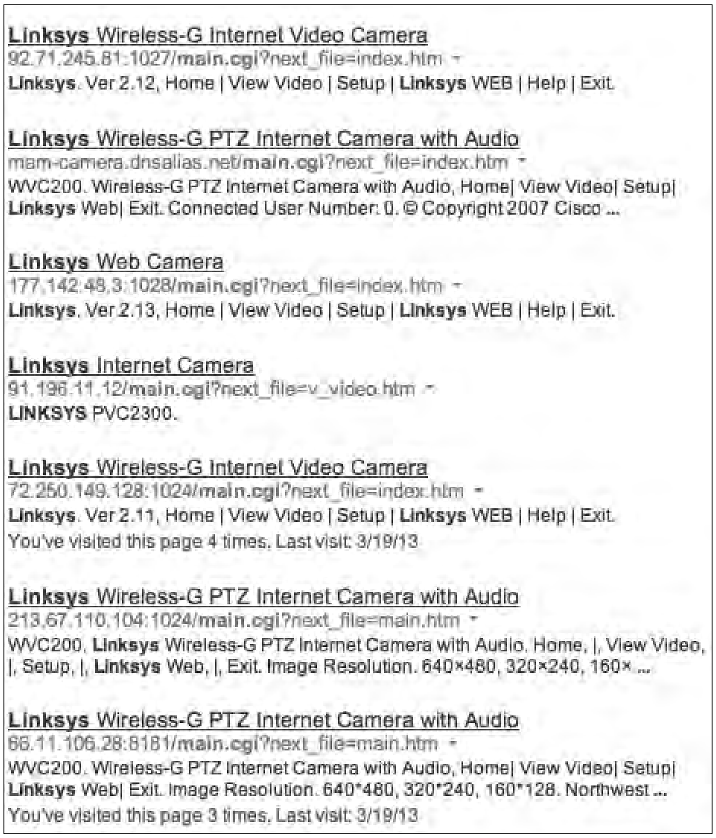
```
HTTP/1.0 401 Authorization Required
```

Google hacking

Google hacking is the most common form of search engine Reconnaissance of web applications. Google hacking uses advanced operations in the Google search engine to locate specific strings of text within search results. Search filters can zero in on specific versions of vulnerable web applications such as **Powered by Apache** in the `intitle:"index of"` operator or identify log files such as `ws_ftp.log`, containing sensitive IP information. The following few screenshots demonstrate using a Google search for Linksys to find publicly available Linksys cameras. The first screenshot shows the search command followed by some example results from issuing the search. The last screenshot shows a camera feed that could be found using this technique.



inurl:main.cgi linksys



Linksys Wireless-G Internet Video Camera
92.71.245.81:1027/main.cgi?next_file=index.htm
Linksys. Ver 2.12, Home | View Video | Setup | Linksys WEB | Help | Exit.

Linksys Wireless-G PTZ Internet Camera with Audio
mam-camera.dnsalias.net/main.cgi?next_file=index.htm
WVC200. Wireless-G PTZ Internet Camera with Audio, Home| View Video| Setup| Linksys Web| Exit. Connected User Number: 0. © Copyright 2007 Cisco ...

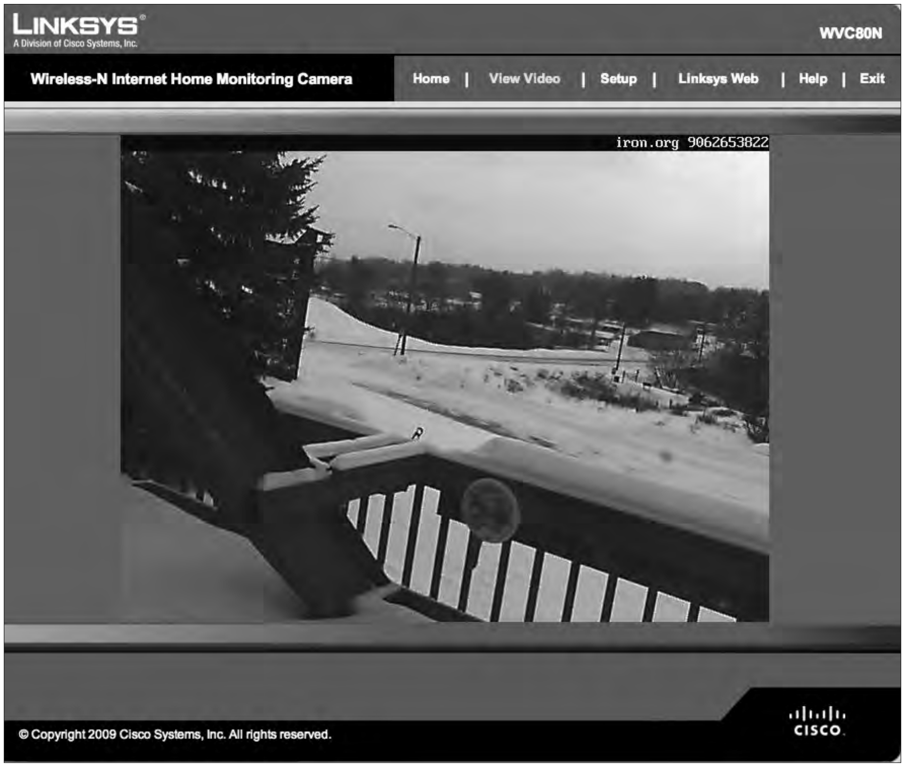
Linksys Web Camera
177.142.48.3:1028/main.cgi?next_file=index.htm
Linksys. Ver 2.13, Home | View Video | Setup | Linksys WEB | Help | Exit.

Linksys Internet Camera
91.196.11.12/main.cgi?next_file=v_video.htm
LINKSYS PVC2300.

Linksys Wireless-G Internet Video Camera
72.250.149.128:1024/main.cgi?next_file=index.htm
Linksys. Ver 2.11, Home | View Video | Setup | Linksys WEB | Help | Exit.
You've visited this page 4 times. Last visit: 3/19/13

Linksys Wireless-G PTZ Internet Camera with Audio
213.67.110.104:1024/main.cgi?next_file=main.htm
WVC200. Linksys Wireless-G PTZ Internet Camera with Audio. Home. |. View Video. |. Setup. |. Linksys Web. |. Exit. Image Resolution. 640×480, 320×240, 160× ...

Linksys Wireless-G PTZ Internet Camera with Audio
66.11.106.28:8181/main.cgi?next_file=main.htm
WVC200. Wireless-G PTZ Internet Camera with Audio, Home| View Video| Setup| Linksys Web| Exit. Image Resolution. 640*480, 320*240, 160*128. Northwest ...
You've visited this page 3 times. Last visit: 3/19/13


LINKSYS
A Division of Cisco Systems, Inc.
WVC80N
Wireless-N Internet Home Monitoring Camera
Home | View Video | Setup | Linksys Web | Help | Exit
iron.org 9062653822
© Copyright 2009 Cisco Systems, Inc. All rights reserved.
CISCO

Some example search queries are as follows:

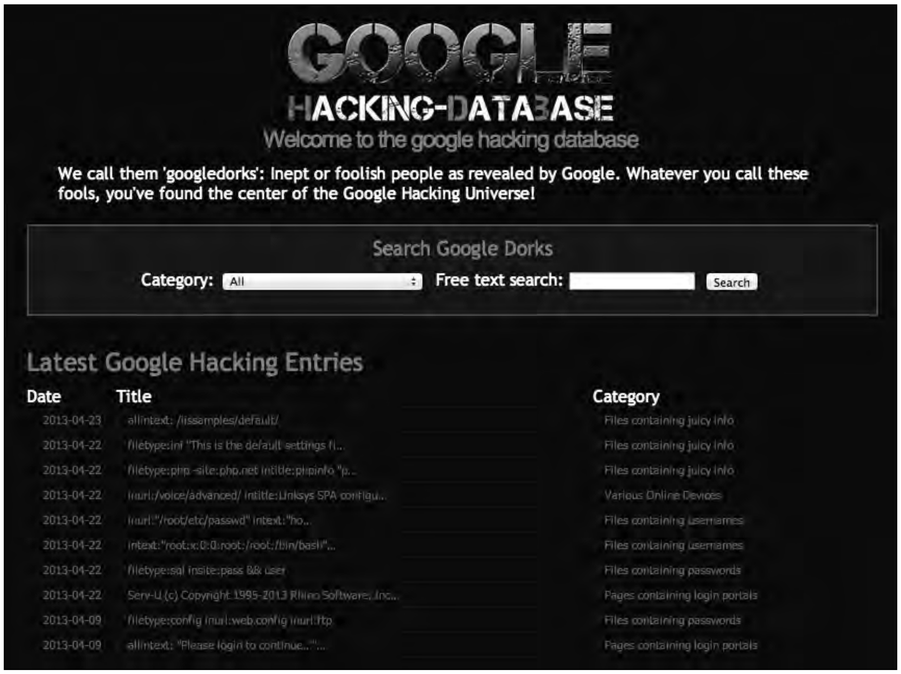
- Identifies sensitive documents: `intext: classified top secret`
- Identifies Linksys Camera Management GUIs (caution: you may not like what you find): `inurl:main.cgi`
- Identifies Nessus reports to find vulnerable systems: `inurl:NESSUSXXXXXXXX`

For more information on Google hacking, check out a very good book titled *Google Hacking for Penetration Testers* by *Johnny Long*, as well as his website at `http://johnny.ihackstuff.com`.

Google Hacking Database

The **Google Hacking Database** (**GHDB**) created by *Johnny Long* of *Hackers For Charity* (`http://www.hackersforcharity.org/`), is the definitive source for Google search queries. Searches for usernames, passwords, vulnerable systems, and exploits have been captured and categorized by Google hacking aficionados. The aficionados who have categorized the Google searches are affectingly known as Google dorks.

To access the GHDB, navigate to `http://www.exploit-db.com/google-dorks/`. You will see the latest GHDB searches listed on the web page. You can click on any of the search queries yourself.



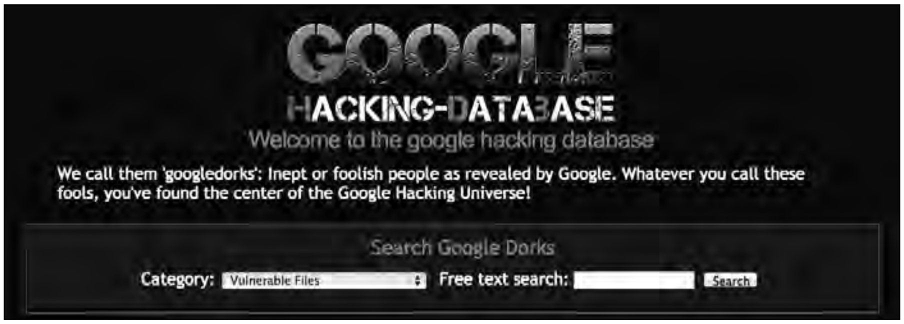
Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Latest Google Hacking Entries

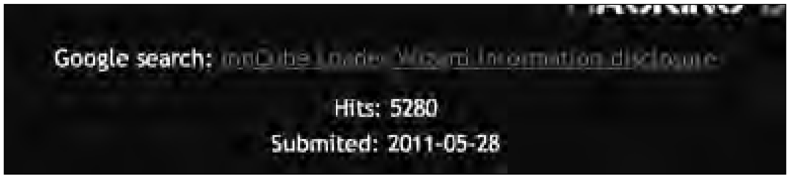
Date	Title	Category
2013-04-23	allintext: /iissamples/default/	Files containing juicy info
2013-04-22	filetype:ini "This is the default settings fi...	Files containing juicy info
2013-04-22	filetype:php -site:php.net intitle:phpinfo "p...	Files containing juicy info
2013-04-22	inurl:/voice/advanced/ intitle:Linksys SPA configu...	Various Online Devices
2013-04-22	inurl:"/root/etc/passwd" intext:"ho...	Files containing usernames
2013-04-22	intext:"root:x:0:0:root:/root:/bin/bash"...	Files containing usernames
2013-04-22	filetype:sql insite:pass && user	Files containing passwords
2013-04-22	Serv-U (c) Copyright 1995-2013 Rhino Software, Inc...	Pages containing login portals
2013-04-09	filetype:config inurl:web.config inurl:ftp	Files containing passwords
2013-04-09	allintext: "Please login to continue..."...	Pages containing login portals

You will find different categories of searches at the bottom of the page that have been saved. In the following example, we scroll to the category **Vulnerable Files** and select the query **ionCube Loader Wizard**.



Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

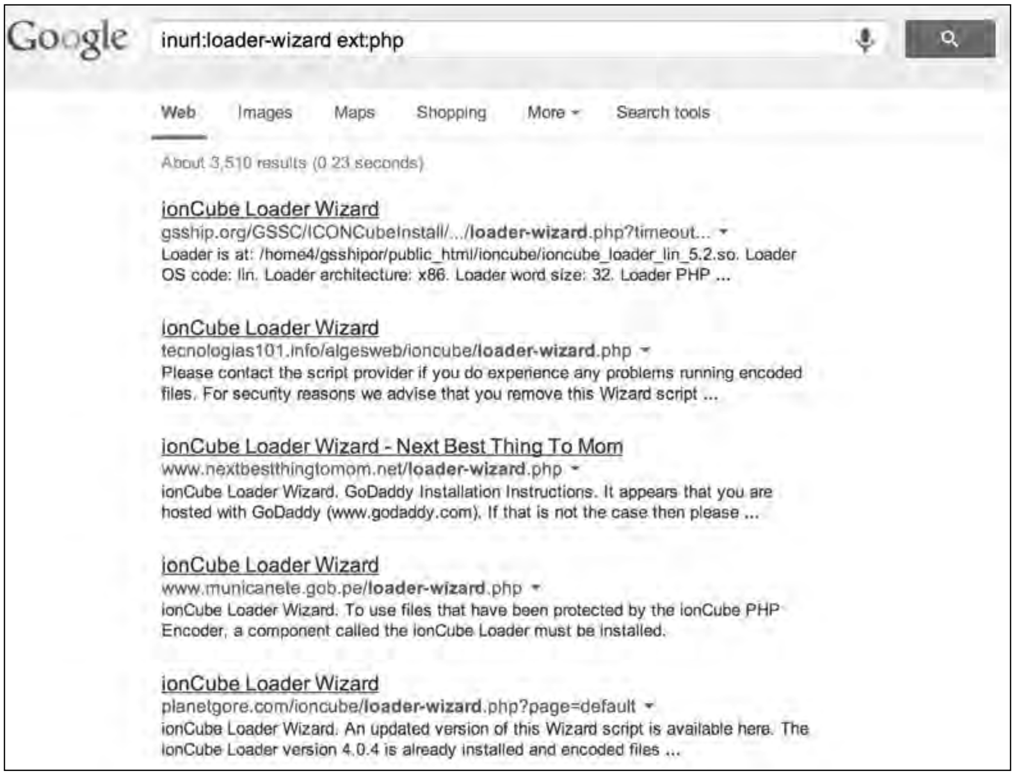


Google search: ionCube Loader Wizard Information disclosure

Hits: 5280

Submited: 2011-05-28

We can select the search query, and it will bring us to Google, performing the same search query.



About 3,510 results (0.23 seconds)

ionCube Loader Wizard
gsship.org/GSSC/ICONCubeInstall/.../loader-wizard.php?timeout...
Loader is at: /home4/gsshipor/public_html/ioncube/ioncube_loader_lin_5.2.so. Loader OS code: lin. Loader architecture: x86. Loader word size: 32. Loader PHP ...

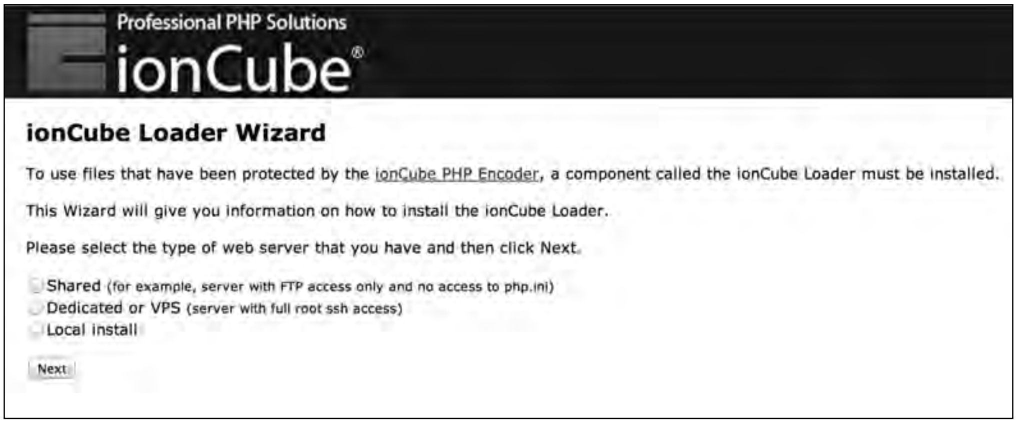
ionCube Loader Wizard
tecnologias101.info/algesweb/ioncube/loader-wizard.php
Please contact the script provider if you do experience any problems running encoded files. For security reasons we advise that you remove this Wizard script ...

ionCube Loader Wizard - Next Best Thing To Mom
www.nextbestthingtomom.net/loader-wizard.php
ionCube Loader Wizard. GoDaddy Installation Instructions. It appears that you are hosted with GoDaddy (www.godaddy.com). If that is not the case then please ...

ionCube Loader Wizard
www.municanete.gob.pe/loader-wizard.php
ionCube Loader Wizard. To use files that have been protected by the ionCube PHP Encoder, a component called the ionCube Loader must be installed.

ionCube Loader Wizard
planetgore.com/ioncube/loader-wizard.php?page=default
ionCube Loader Wizard. An updated version of this Wizard script is available here. The ionCube Loader version 4.0.4 is already installed and encoded files ...

The preceding example shows Google has found a few results. The **ionCube Loader** is apparently not configured or misconfigured. The **ionCube Loader** is actually a great piece of software that protects software written in PHP from being viewed or changed from unlicensed computers. However, in this case, administrators left the default wizard running without any configuration.



ionCube Loader Wizard

To use files that have been protected by the ionCube PHP Encoder, a component called the ionCube Loader must be installed.

This Wizard will give you information on how to install the ionCube Loader.

Please select the type of web server that you have and then click Next.

○ Shared (for example, server with FTP access only and no access to php.ini)
○ Dedicated or VPS (server with full root ssh access)
○ Local install

When we click on the first link, we get the home screen to configure the software.

The GHDB essentially turns Google into a limited web application scanner for a Penetration Tester. In this case, good software that can increase security can now potentially be used against a web server by an attacker.

Researching networks

Many people do not understand the true purpose of researching the network of a target prior to launching an attack. Amateur Penetration Testers understand the need to pick a target before they can perform a Penetration Test. After all, a Penetration Tester needs someplace at which to point their arsenal of tools. Many amateurs will run Nmap, ping sweeps, or other noisy tools to determine what targets are available disrupting the environment, which later yields poor results.

Network Reconnaissance is about selecting a target. A seasoned network security professional will tell you good Reconnaissance is about selecting a quality target, spending the majority of their time watching, rather than acting. The first step of every Penetration Test is accurately finding and selecting quality targets.

From a client's viewpoint, Penetration Testers will encounter individuals that gain satisfaction in stopping Penetration Testers to prove their value as employees, as well as how well prepared they are for cyber attacks. It is highly recommended that a professional Penetration Tester does not get into a conflict with a client's staff while penetration services are being performed. A Penetration Tester should focus on security awareness, and reveal what vulnerabilities exist with the least amount of interaction with a target's staff during a service engagement.

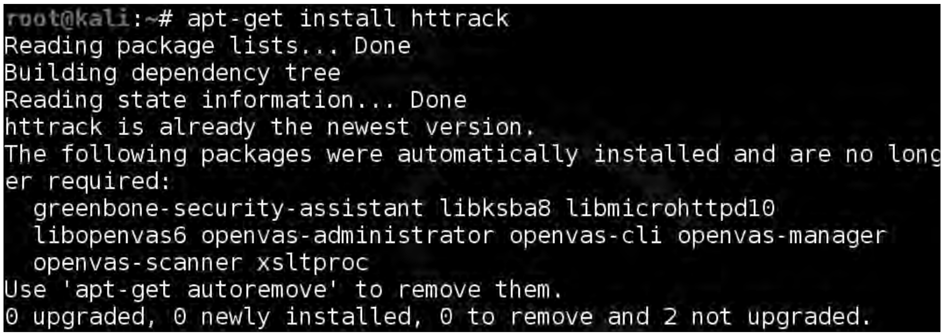
The following are the best available tools in Kali for web application Reconnaissance. Other tools may be available for web applications or different target types however, the focus of this chapter is enabling a reader for evaluating web application-based targets.

HTTrack – clone a website

HTTrack is a tool built into Kali. The purpose of HTTrack is to copy a website. It allows a Penetration Tester to look at the entire content of a website, all its pages, and files offline, and in their own controlled environment. In addition, we will use HTTrack for social engineering attacks in later chapters. Having a copy of a website could be used to develop fake phishing websites, which can be incorporated in other Penetration Testing toolsets.

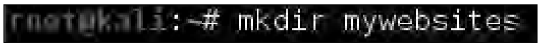
To use HTTrack, open a **Terminal** window and type in `apt-get install httrack` as shown in the following screenshot.

Some versions of Kali do not have this built-in.



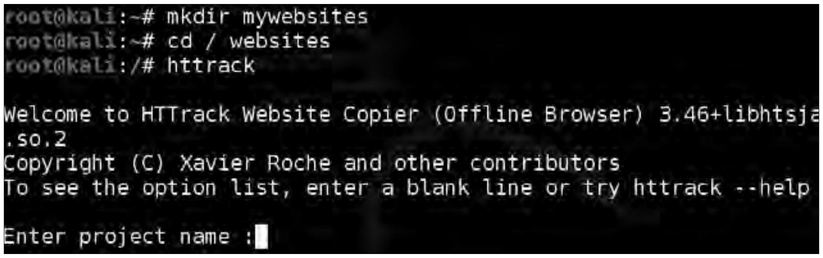
```
root@kali:~# apt-get install httrack
Reading package lists... Done
Building dependency tree
Reading state information... Done
httrack is already the newest version.
The following packages were automatically installed and are no long
er required:
  greenbone-security-assistant libksba8 libmicrohttpd10
  libopenvas6 openvas-administrator openvas-cli openvas-manager
  openvas-scanner xsltproc
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

You will want to create a directory to store your copied website. The following screenshot shows a directory created named `mywebsites` using the `mkdir` command.



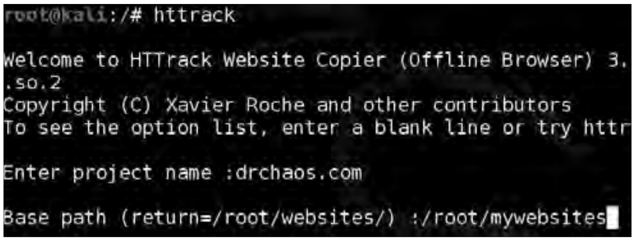
```
root@kali:~# mkdir mywebsites
```

To start HTTrack, type `httrack` in the command window and give the project a name, as shown in the following screenshot:



```
root@kali:~# mkdir mywebsites
root@kali:~# cd / websites
root@kali:/# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.46+libhtsja
.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :
```

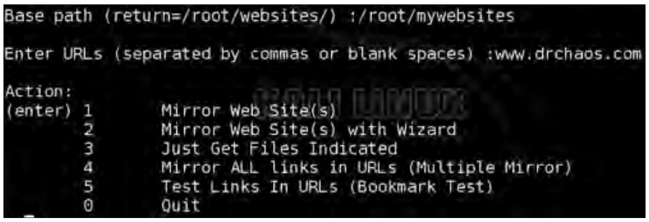
The next step is to select a directory to save the website. The example in the following screenshot shows the folder created in the previous step `/root/mywebsites`, used for the directory:



```
root@kali:/# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.
.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httr

Enter project name :drchaos.com

Base path (return=/root/websites/) :/root/mywebsites
```

Enter the URL of the site you want to capture. The example in the following screenshot shows `www.drchaos.com`. This can be any website. Most attacks use a website accessed by clients from your target, such as popular social media websites or the target's internal websites.

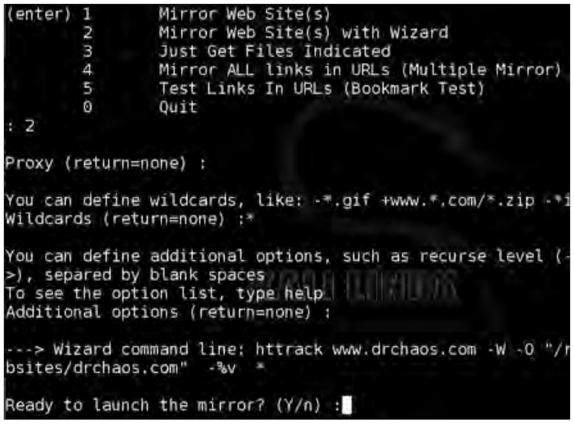
The next two options are presented regarding what you want to do with the captured site. Option 2 is the easiest method, which is a mirror website with a wizard as shown in the following screenshot:



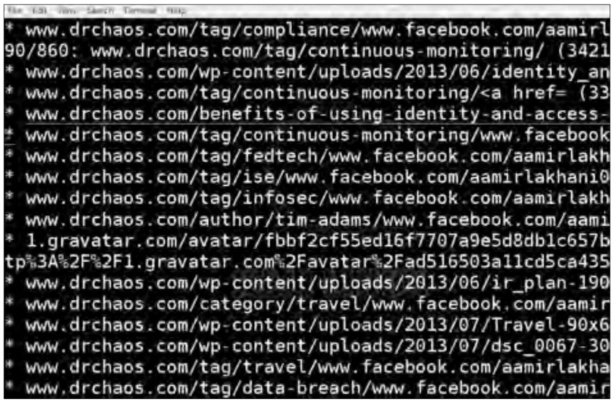
```
Base path (return=/root/websites/) :/root/mywebsites

Enter URLs (separated by commas or blank spaces) :www.drchaos.com

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
```

Next, you can specify if you want to use a proxy to launch the attack. You can also specify what type of files you want to download (the example in the following screenshot shows `*` for all files). You can also define any command line options or flags you might want to set. The example in the following screenshot shows no additional options.

Before `httrack` runs, it will display the command that it is running. You can use this command in the future if you want to run httrack without going through the wizard again. The following two screenshots show `hhtrack` cloning `www.drchaos.com`:

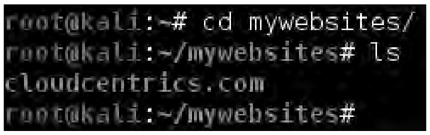


```
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
: 2

Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*i
Wildcards (return=none) :*

You can define additional options, such as recurse level (-
>), separed by blank spaces
To see the option list, type help
Additional options (return=none) :

---> Wizard command line: httrack www.drchaos.com -W -O "/r
bsites/drchaos.com"  -%v  *

Ready to launch the mirror? (Y/n) :
```



```
* www.drchaos.com/tag/compliance/www.facebook.com/aamirl
90/860: www.drchaos.com/tag/continuous-monitoring/ (3421
* www.drchaos.com/wp-content/uploads/2013/06/identity_an
* www.drchaos.com/tag/continuous-monitoring/<a href= (33
* www.drchaos.com/benefits-of-using-identity-and-access-
* www.drchaos.com/tag/continuous-monitoring/www.facebook
* www.drchaos.com/tag/fedtech/www.facebook.com/aamirlakh
* www.drchaos.com/tag/ise/www.facebook.com/aamirlakhani0
* www.drchaos.com/tag/infosec/www.facebook.com/aamirlakh
* www.drchaos.com/author/tim-adams/www.facebook.com/aami
* 1.gravatar.com/avatar/fbbf2cf55ed16f7707a9e5d8db1c657b
tp%3A%2F%2F1.gravatar.com%2Favatar%2Fad516503a11cd5ca435
* www.drchaos.com/wp-content/uploads/2013/06/ir_plan-190
* www.drchaos.com/category/travel/www.facebook.com/aamir
* www.drchaos.com/wp-content/uploads/2013/07/Travel-90x6
* www.drchaos.com/wp-content/uploads/2013/07/dsc_0067-30
* www.drchaos.com/tag/travel/www.facebook.com/aamirlakha
* www.drchaos.com/tag/data-breach/www.facebook.com/aamir
```

After you are done cloning the website, navigate to the directory where you saved it. Inside, you will find all your files and webpages, as shown in the following screenshot:



```
root@kali:~# cd mywebsites/
root@kali:~/mywebsites# ls
cloudcentrics.com
root@kali:~/mywebsites#
```

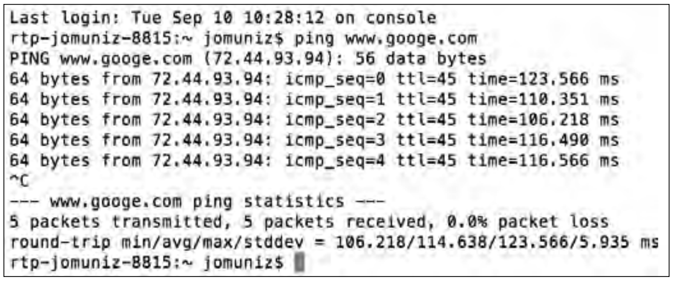
You are now ready to research your target's website and possibly build a customized penetration tool or exploit user access to a cloned website.

ICMP Reconnaissance techniques

The `ping` and `traceroute` commands are good ways to find out basic information about your target. When information travels across networks, it usually does not go directly from source to destination. It usually traverses through several systems, such as routers, firewalls, and other computer systems before it gets to its destination. The `traceroute` command identifies each system the data travels across, along with the time it takes for the data to move between systems. The tool is installed in every modern operating system. For most high-value targets, the `ping` and `traceroute` commands will most likely be disabled, and excessive use of these services will most likely trigger alerts on network security systems. Many firewalls or other systems are set up not to respond to number B24RYE routes. If systems do respond to `traceroute`, using this too excessively can trigger security events. These tools are noisy, and when used indiscriminately, they will set off alarms and logs. If your goal is to be stealthy, you have just been defeated, giving your target an opportunity to set up and deploy counter measures against your Penetration Test.

An ICMP sweep simply sends out an echo request and looks for a reply. If a reply is returned, then, as a Penetration Tester, you know there is a possible target. The problem with ICMP scans is that ICMP is usually blocked by most firewalls. That means any scans from outside going to an internal target network will be blocked by an ICMP scanner.

The `ping` command is the most basic way to start an ICMP sweep. You simply type in `ping` followed by a hostname or IP address to see what will respond to the ICMP echo request. The following screenshot shows a ping of `www.google.com`:



```
Last login: Tue Sep 10 10:28:12 on console
rtp-jomuniz-8815:~ jomuniz$ ping www.googe.com
PING www.googe.com (72.44.93.94): 56 data bytes
64 bytes from 72.44.93.94: icmp_seq=0 ttl=45 time=123.566 ms
64 bytes from 72.44.93.94: icmp_seq=1 ttl=45 time=110.351 ms
64 bytes from 72.44.93.94: icmp_seq=2 ttl=45 time=106.218 ms
64 bytes from 72.44.93.94: icmp_seq=3 ttl=45 time=116.490 ms
64 bytes from 72.44.93.94: icmp_seq=4 ttl=45 time=116.566 ms
^C
--- www.googe.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 106.218/114.638/123.566/5.935 ms
rtp-jomuniz-8815:~ jomuniz$ 
```

If you get any responses back, you will know that your host is alive. If you get any timeouts, your ICMP request is being blocked, or no destination host has received your request.

The problem with the `ping` command is that it only allows you to use ICMP to check on one host at a time. The `fping` command will allow you ping multiple hosts with a single command. It will also let you read a file with multiple hostnames or IP addresses and send them using ICMP echo requests packets.

To use the `fping` command to run an ICMP sweep on a network, issue the following command:

```
fping-asg network/host bits
fping -asg 10.0.1.0/24
```

Although the `a` flag will return the results via IP address of live hosts only, the `s` flag displays statistics about the scan, the `g` flag sets `fping` in quite mode, which means it does show the user the status of each scan, only the summary when it has completed.

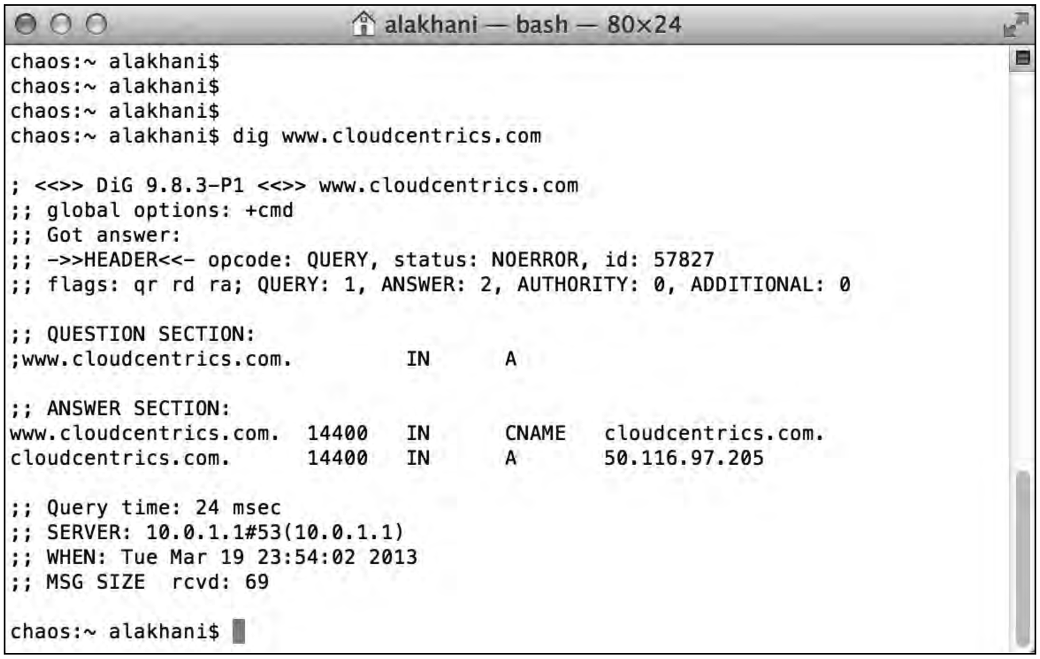
> The Nmap provides similar results as the `fping` command.

DNS Reconnaissance techniques

Most high-value targets have a DNS name associated to an application. DNS names make it easier for users to access a particular service and add a layer of professionalism to their system. For example, if you want to access Google for information, you could open a browser and type in `74.125.227.101` or type `www.google.com`.

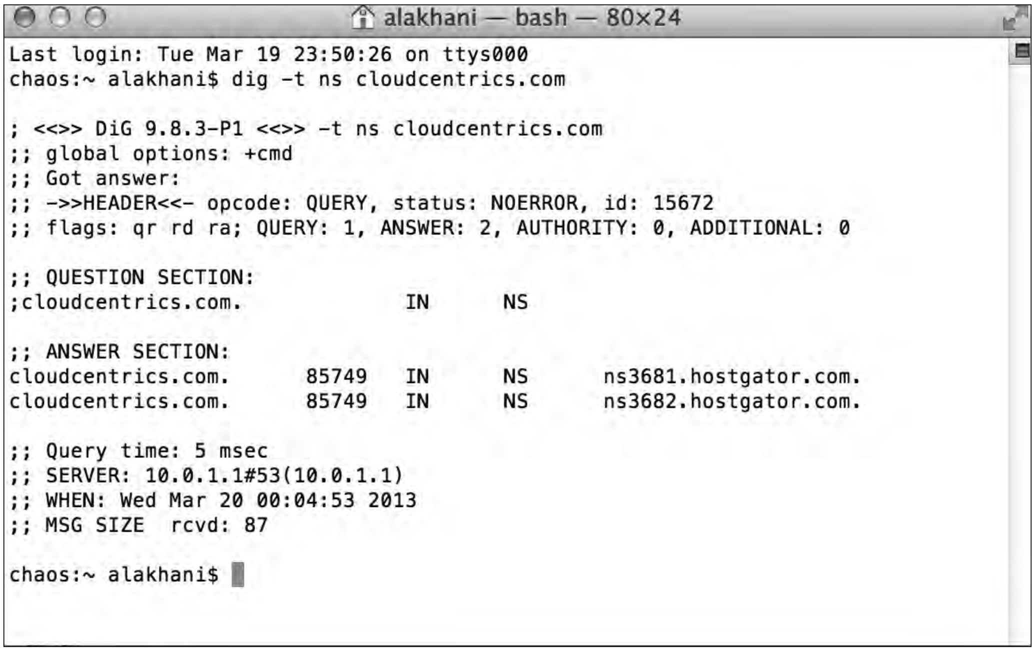
DNS information about a particular target can be extremely useful to a Penetration Tester. DNS allows a Penetration Tester to map out systems and subdomains. Older DNS attacks transfer a zone file from an authoritative DNS, allowing the tester to examine the full contents of the zone file to identify potential targets. Unfortunately, most DNS servers today do not allow unauthenticated zone transfers. However, all is not lost! DNS by its very nature is a service that responds to queries; therefore, an attacker could use a word list query containing hundreds of names with a DNS server. This attack vector is an extremely time consuming task; however, most aspects can be automated.

Dig (**domain information groper**) is one the most popular and widely used DNS Reconnaissance tools. It queries DNS servers. To use Dig, open a command prompt and type `dig` and hostname, where hostname represents the target domain. Dig will use your operating systems default DNS settings to query the hostname. You can also configure Dig to query custom DNS servers by adding `@<IP>` to the command. The example in the following screenshot illustrates using Dig on `www.cloudcentrics.com`.



```
chaos:~ alakhani$
chaos:~ alakhani$
chaos:~ alakhani$
chaos:~ alakhani$ dig www.cloudcentrics.com

; <<>> DiG 9.8.3-P1 <<>> www.cloudcentrics.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57827
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.cloudcentrics.com.         IN      A

;; ANSWER SECTION:
www.cloudcentrics.com.  14400   IN      CNAME   cloudcentrics.com.
cloudcentrics.com.      14400   IN      A       50.116.97.205

;; Query time: 24 msec
;; SERVER: 10.0.1.1#53(10.0.1.1)
;; WHEN: Tue Mar 19 23:54:02 2013
;; MSG SIZE  rcvd: 69

chaos:~ alakhani$
```

The `-t` option in Dig will delegate a DNS zone to use the authoritative name servers. We type `dig -t ns cloudcentrics.com` in the example in the following screenshot:



```
Last login: Tue Mar 19 23:50:26 on ttys000
chaos:~ alakhani$ dig -t ns cloudcentrics.com

; <<>> DiG 9.8.3-P1 <<>> -t ns cloudcentrics.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15672
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cloudcentrics.com.             IN      NS

;; ANSWER SECTION:
cloudcentrics.com.      85749   IN      NS      ns3681.hostgator.com.
cloudcentrics.com.      85749   IN      NS      ns3682.hostgator.com.

;; Query time: 5 msec
;; SERVER: 10.0.1.1#53(10.0.1.1)
;; WHEN: Wed Mar 20 00:04:53 2013
;; MSG SIZE  rcvd: 87

chaos:~ alakhani$ 
```

We see from the results we have two authoritative DNS servers for the domain `www.cloudcentrics.com`; they are `ns3681.hostgator.com` and `ns3682.hostgator.com`.

Congratulations, you have just found the authoritative DNS server for your target DNS.

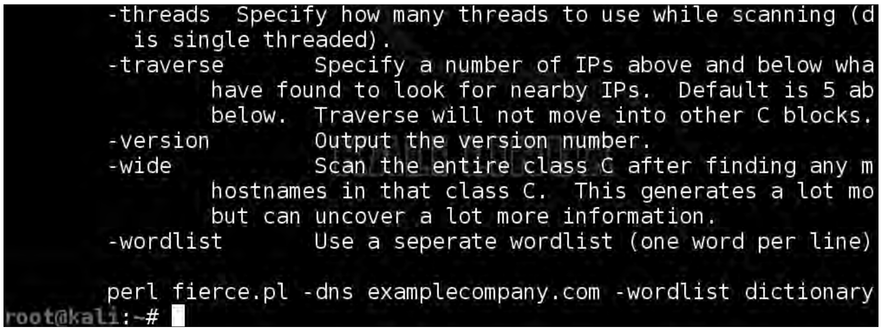
DNS target identification

Now that you have found the authoritative DNS servers for a domain, you might want to see what hosts have entries on that domain. For example, the domain `drchaos.com` may have several hosts. such as `cloud.drchaos.com`, `mail. drchaos.com`, `sharepoint.drchaos.com`. These all could be potential applications and potentially high value targets.

Before we randomly start choosing hosts, we should query the DNS server to see what entries exist. The best way to do that is to ask the DNS server to tell us. If the DNS server is configured to allow zone transfers, it will give us a copy of all its entries.

Kali ships with a tool named Fierce. Fierce will check to see if the DNS server allows zone transfers. If zone transfers are permitted, Fierce will execute a zone transfer and inform the user of the entries. If the DNS server does not allow zone transfers, Fierce can be configured to brute force host names on a DNS server. Fierce is designed as a Reconnaissance tool before you use a tool that requires you to know IP addresses, such as Nmap.

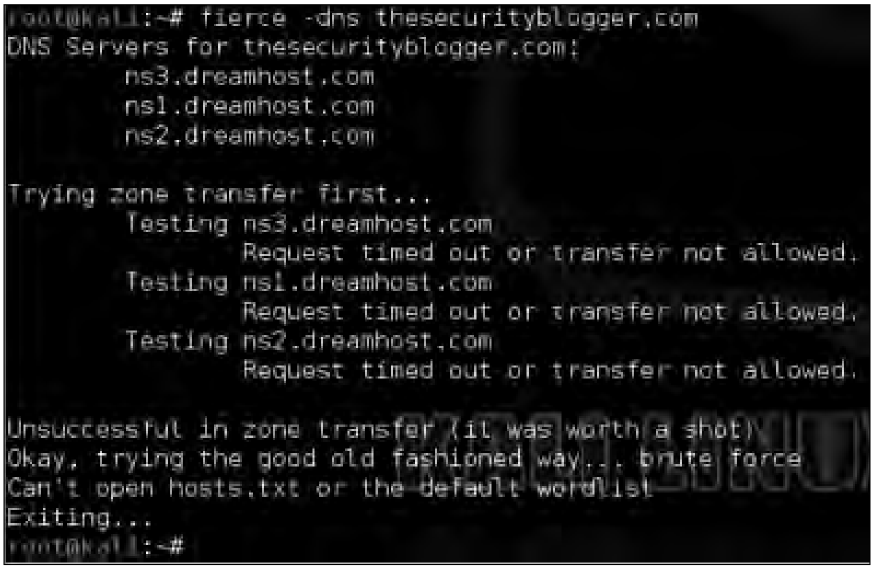
To use Fierce, navigate to **Information Gathering | DNS Analysis | Fierce**. Fierce will load into a terminal window as shown in the following screenshot.



```
        -threads  Specify how many threads to use while scanning (d
          is single threaded).
        -traverse       Specify a number of IPs above and below wha
                have found to look for nearby IPs.  Default is 5 ab
                below.  Traverse will not move into other C blocks.
        -version        Output the version number.
        -wide           Scan the entire class C after finding any m
                hostnames in that class C.  This generates a lot mo
                but can uncover a lot more information.
        -wordlist       Use a seperate wordlist (one word per line)

        perl fierce.pl -dns examplecompany.com -wordlist dictionary
root@kali:~# 
```

To run the `Fierce` script, type the following command:

```
fierce.pl -dns thesecurityblogger.com
```



```
root@kali:~# fierce -dns thesecurityblogger.com
DNS Servers for thesecurityblogger.com:
        ns3.dreamhost.com
        ns1.dreamhost.com
        ns2.dreamhost.com

Trying zone transfer first...
        Testing ns3.dreamhost.com
                Request timed out or transfer not allowed.
        Testing ns1.dreamhost.com
                Request timed out or transfer not allowed.
        Testing ns2.dreamhost.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Can't open hosts.txt or the default wordlist
Exiting...
root@kali:~#
```

The domain `thesecurityblogger.com`, shown in the preceding screenshot, has a few hosts associated with it. We have accomplished our task. However, you can see Fierce failed at completing a zone transfer. Fierce will try and brute force a zone transfer using a word list or dictionary file if you have one defined. We did not, because the goal of this section is to determine what hosts exist on the domain, not necessarily at this point carry out a zone transfer attack. However, if your goal is more inclusive than targeting web applications, you may want to explore this further on your own.

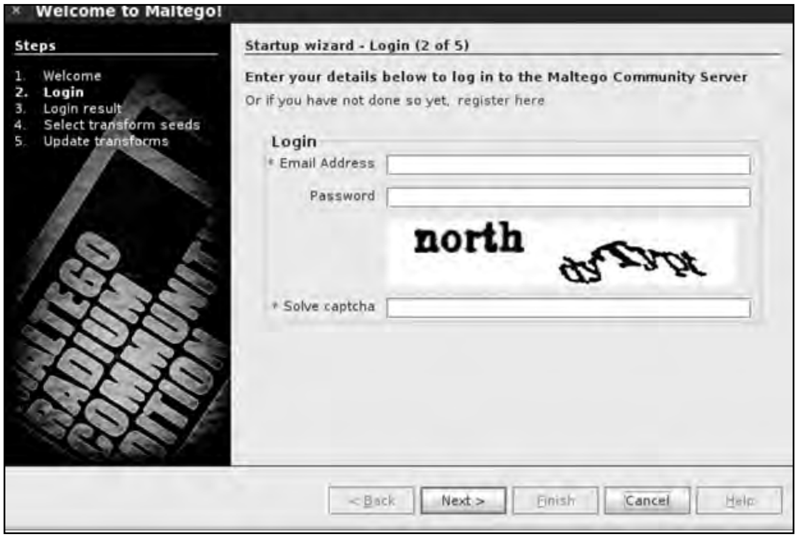
We can now target a particular host and use tools like Nmap to proceed further in mapping out our target. An important aspect of using Fierce is selecting a target using very little network traffic, which is important for avoiding detection. We will use Nmap to gather more information about our target later in this chapter.

Maltego – Information Gathering graphs

Maltego is a Reconnaissance tool built into Kali developed by Paterva. It is a multipurpose Reconnaissance tool that can gather information using open and public information on the Internet. It has some built-in DNS Reconnaissance, but goes much deeper into fingerprinting your target and gathering intelligence on them. It takes the information and displays the results in a graph for analysis.

To start Maltego, navigate to **Application** menu in Kali, and click on the **Kali** menu. Then select **Information Gathering** | **DNS Analysis** | **Maltego**.

The first step when you launch Maltego is to register it. You cannot use the application without registration.



Welcome to Maltego!

Steps

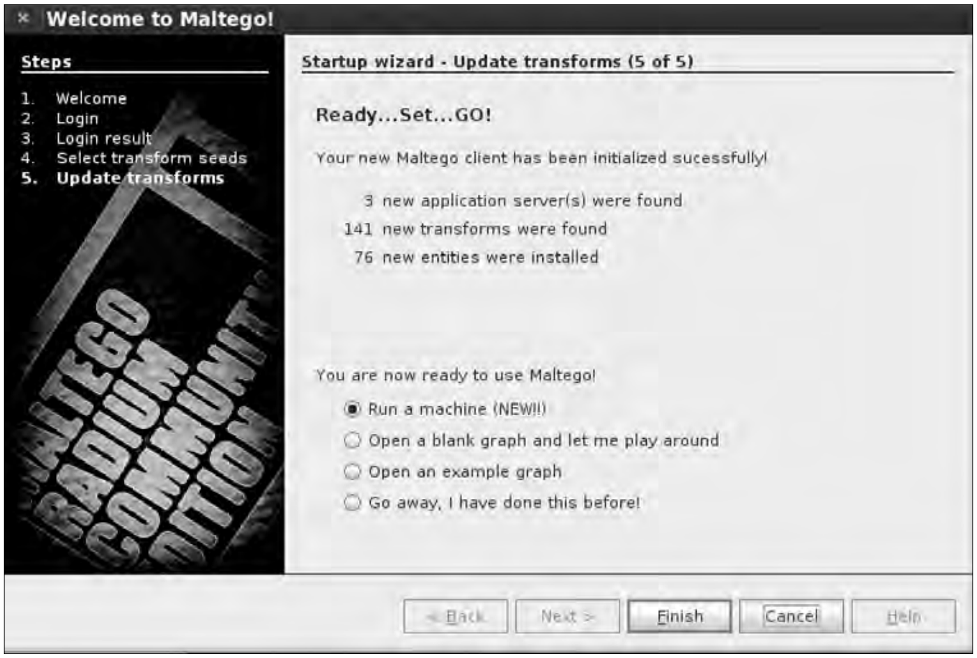
1. Welcome
2. Login
3. Login result
4. Select transform seeds
5. Update transforms

Startup wizard - Login (2 of 5)

Enter your details below to log in to the Maltego Community Server

Or if you have not done so yet, register here

When you complete registration, you will be able to install Maltego and start using the application.


Welcome to Maltego!

Steps

1. Welcome
2. Login
3. Login result
4. Select transform seeds
5. **Update transforms**

Startup wizard - Update transforms (5 of 5)

Ready...Set...GO!

Your new Maltego client has been initialized sucessfully!

3 new application server(s) were found
141 new transforms were found
76 new entities were installed

You are now ready to use Maltego!

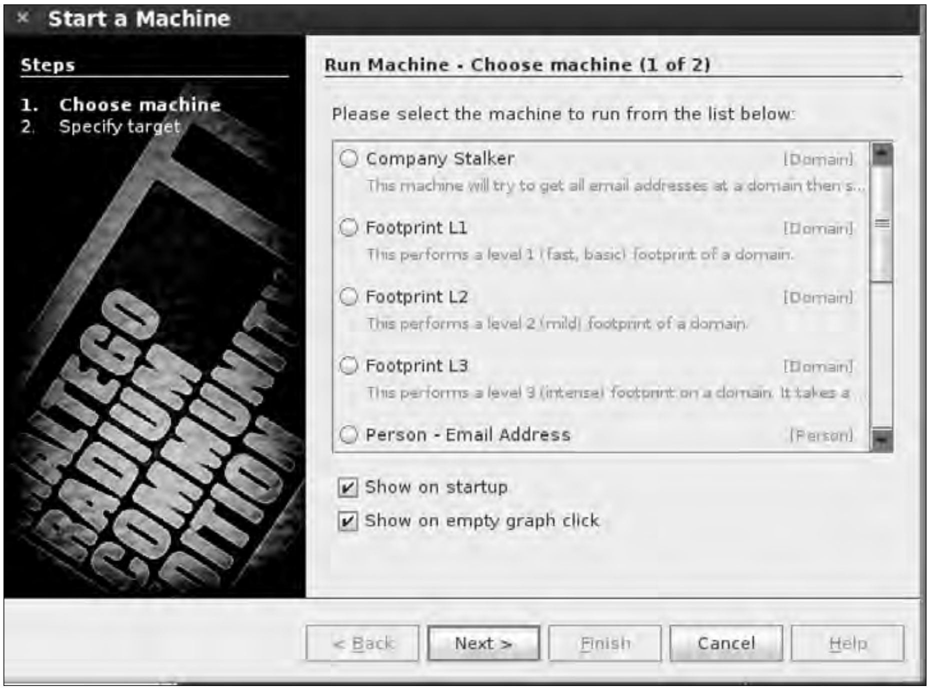
● Run a machine (NEW!!)
○ Open a blank graph and let me play around
○ Open an example graph
○ Go away, I have done this before!

Maltego has numerous methods of gathering information. The best way to use Maltego is to take advantage of the startup wizard to select the type of information you want to gather. Experienced users may want to start with a blank graph or skip the wizard all together. The power of Maltego is that it lets you visually observe the relationship between a domain, organization, and people. You can focus around a specific organization, or look at an organization and its related partnerships from DNS queries.

Depending on the scan options chosen, Maltego will let you perform the following tasks:

- Associate an e-mail address to a person
- Associate websites to a person
- Verify an e-mail address
- Gather details from Twitter, including geolocation of pictures

Most of the features are self-explanatory and include how they are used under the feature description. Maltego is used commonly to gather information and sometimes used as the first step during a social engineering attack.



Start a Machine

Steps

1. Choose machine
2. Specify target

Run Machine - Choose machine (1 of 2)

Please select the machine to run from the list below:

○ Company Stalker [Domain]
This machine will try to get all email addresses at a domain then s...

○ Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.

○ Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.

○ Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a

○ Person - Email Address [Person]

☑ Show on startup

☑ Show on empty graph click

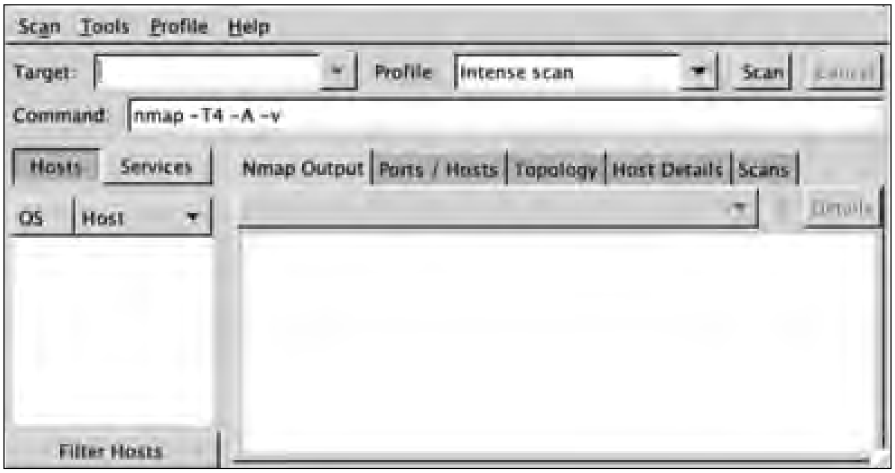
Nmap

Nmap stands for Network Mapper, and is used to scan hosts and services on a network. Nmap has advanced features that can detect different applications running on systems as well as services and OS fingerprinting features. It is one of the most widely used network scanners making it very effective, but also very detectable. We recommend using Nmap in very specific situations to avoid triggering a target's defense systems.

For more information on how to use Nmap, see `http://nmap.org/`.

Additionally, Kali comes loaded with Zenmap. Zenmap gives Nmap a graphical user interface (GUI) to run commands. Although there are many purists who will tell you the command-line version is the best version because of its speed and flexibility, Zenmap has come a long way and has incorporated most of the Nmap features. Zenmap also offers exclusive features not offered in Nmap, such as developing graphical representations of a scan, which can be used later by other reporting systems.

To open **Zenmap**, go to the **Backtrack** menu. Navigate to **Information Mapping | DNS Analysis**, and launch **Zenmap**.

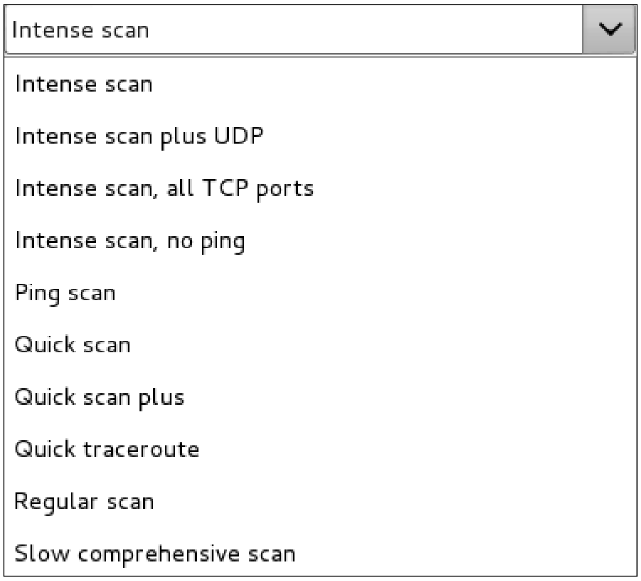


Target:

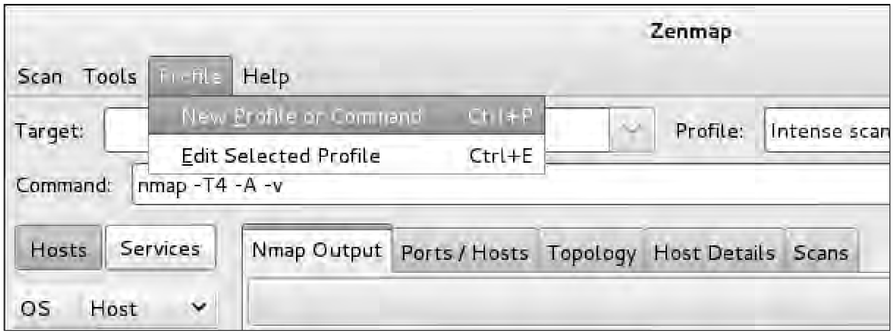
Profile: Intense scan

Command: nmap -T4 -A -v

You will notice under the **Profile** menu that there are several options to determine what type of scan you would like to run, as shown in the following screenshot:



The first step is creating a new profile. A profile in Zenmap allows a Penetration Tester to create what type of scan to execute and what different options to include. Navigate to the **Profile** menu and select **New Profile or Command** to create a new profile, as shown in the following screenshot:



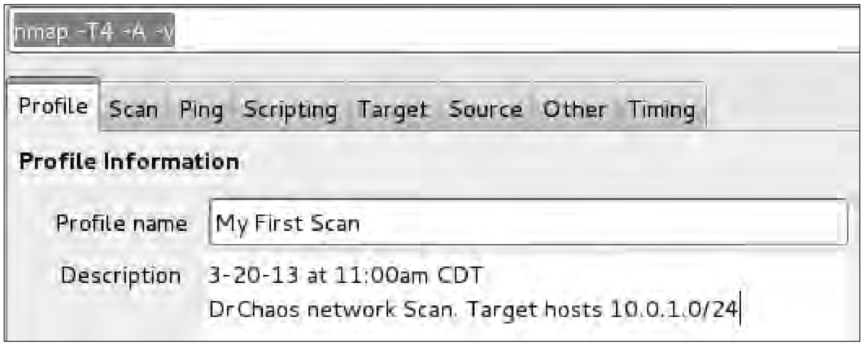
Target:

Profile: Intense scan

Command: nmap -T4 -A -v

When you select **New Profile or Command**, the profile editor will launch. You will need to give your profile a descriptive name. For example, you can call the profile `My First Scan` or anything else you would like.

Optionally, you can give the profile a description. During your course of using Zenmap you will probably create many profiles and make multiple scans. A natural reflex may be to delete profiles post execution. Here is a word of advice: profiles don't take any space and come handy when you want to recreate something. We recommend being extremely descriptive in profile names and come up with a standard naming method. I start all my profile description with the date, time, description of my location, my target network scan location, and customer name.



nmap -T4 -A -v

Profile Information

Profile name: My First Scan

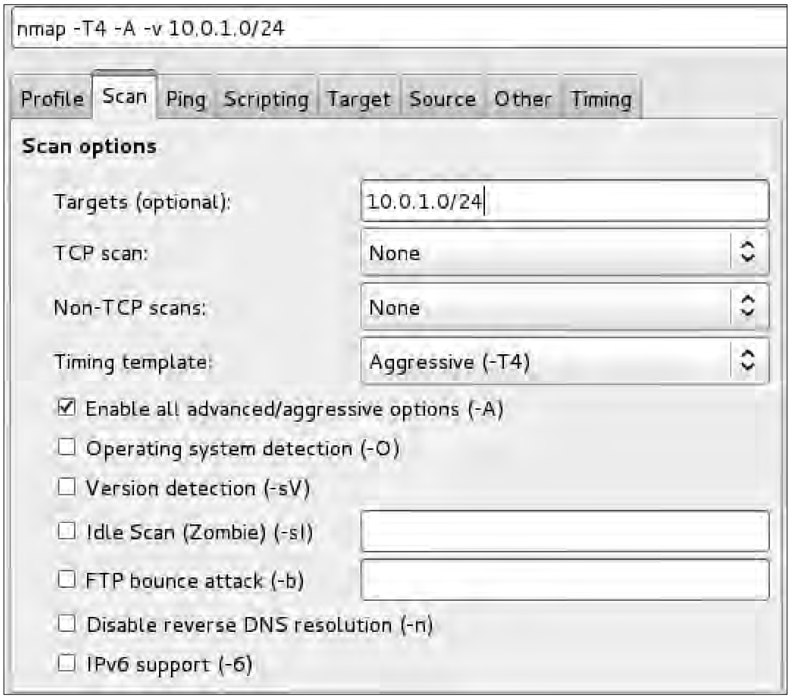
Description: 3-20-13 at 11:00am CDT
DrChaos network Scan. Target hosts 10.0.1.0/24

When you completed your description, click on the **Scan** tab. In the **Targets** section, you will add what hosts or networks you would like to scan. This field can take a range of IP addresses (10.0.1.1-255) or it can take a network in CIDR format (10.0.1.0/24).

You can see option **-A** is selected by default to enable aggressive scanning. Aggressive scanning will enable OS detection (**-O**), version detection (**-sV**), script scanning (-sC) and traceroute (--traceroute). Essentially, aggressive scanning allows a user to turn on multiple flags without the need of having to remember them.

Aggressive scan is considered intrusive, meaning it will be detected by most security devices. An aggressive scan may go unnoticed if your target is an extremely specific host, but regardless of the situation, it's recommended you have the permission to scan before using this or scanning option. As a reminder, completing the ACK in the three-way handshake with an unauthorized system is considered illegal by the US standards.

We can use the information we received from our DNS Reconnaissance exercise to target a very specific host. Before we do that, let's set a few common options first.



```
nmap -T4 -A -v 10.0.1.0/24
```

Scan options

Targets (optional): 10.0.1.0/24

TCP scan: None

Non-TCP scans: None

Timing template: Aggressive (-T4)

☑ Enable all advanced/aggressive options (-A)

☐ Operating system detection (-O)

☐ Version detection (-sV)

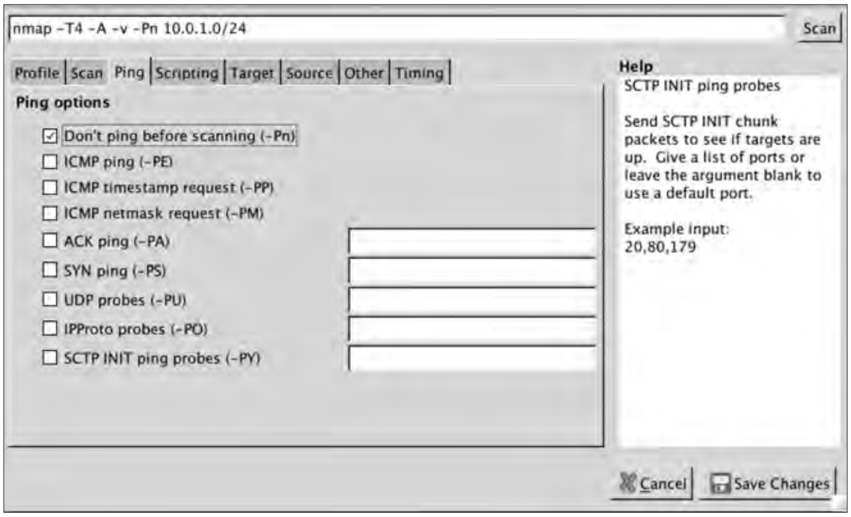
☐ Idle Scan (Zombie) (-sI)

☐ FTP bounce attack (-b)

☐ Disable reverse DNS resolution (-n)

☐ IPv6 support (-6)

Click on the **Ping** tab. Select the **-Pn** flag option so Nmap will not ping the host first. When this flag is not set, Nmap will ping your target hosts and networks. Default settings only perform scans on hosts that are considered alive or reachable. The -Pn flag tells Nmap to scan a host even without a ping response. Although this makes the scan considerably more lengthy, the **–Pn** flag allows Nmap to avoid a common problem of not receiving a ping response when the ping requests are blocked by security defenses.



```
nmap -T4 -A -v -Pn 10.0.1.0/24
```

Ping options

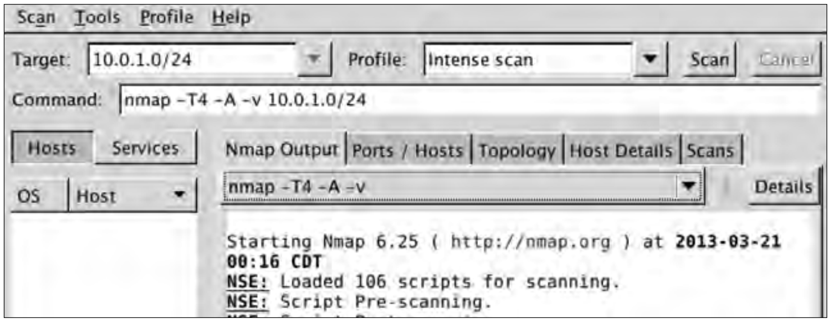
☑ Don't ping before scanning (-Pn)
☐ ICMP ping (-PE)
☐ ICMP timestamp request (-PP)
☐ ICMP netmask request (-PM)
☐ ACK ping (-PA)
☐ SYN ping (-PS)
☐ UDP probes (-PU)
☐ IPProto probes (-PO)
☐ SCTP INIT ping probes (-PY)

Help
SCTP INIT ping probes

Send SCTP INIT chunk packets to see if targets are up. Give a list of ports or leave the argument blank to use a default port.

Example input:
20,80,179

Save changes made by clicking on the **Save Changes** button in the lower-right hand corner. Once saved, select the **Scan** button on the top-right side of the screen to start the scan. Notice your options and target that you configured in the profile editor are listed.



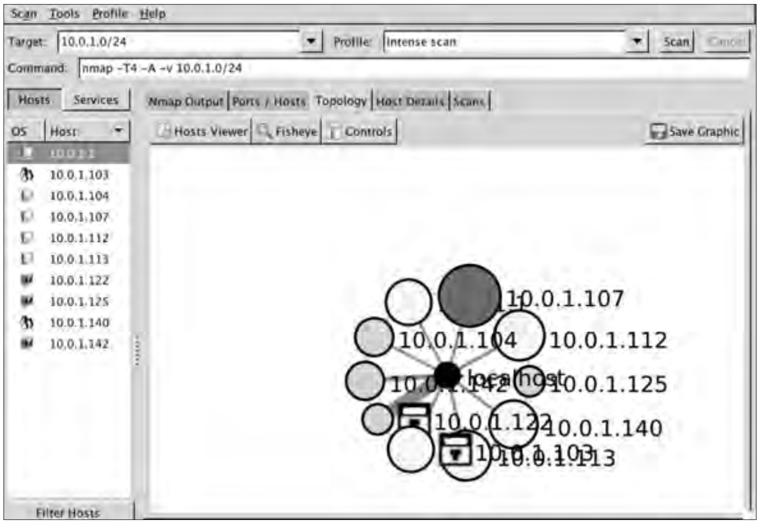
Target: 10.0.1.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 10.0.1.0/24

nmap -T4 -A -v

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-21
00:16 CDT
NSE: Loaded 106 scripts for scanning.
NSE: Script Pre-scanning.
```

The network **Topology** tab will give you a quick look at how your scan on the target network was completed, and if you had to cross any routers. In this example, you see the scan stayed local to the network.

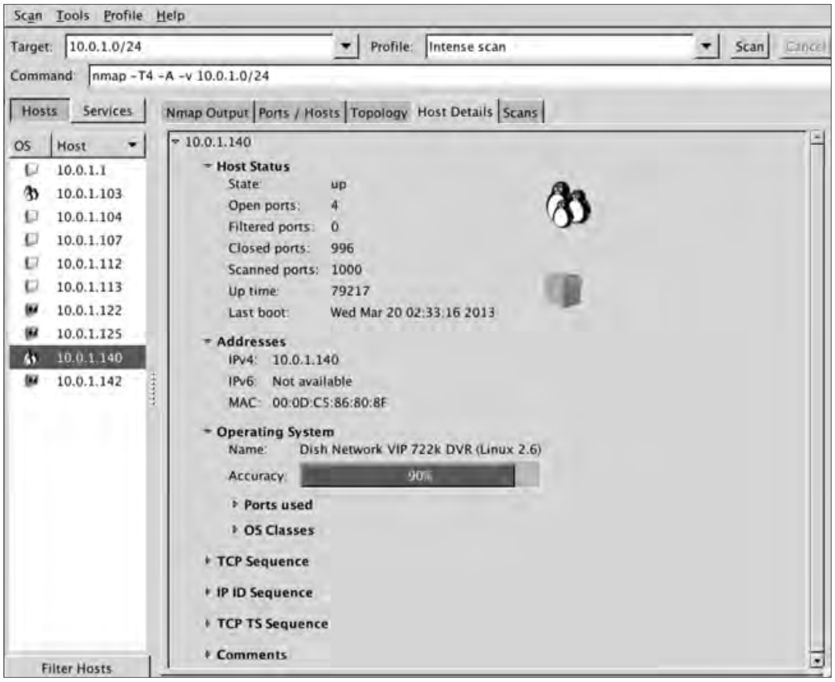
The **Hosts** tab will give a list of the hosts discovered.



Target: 10.0.1.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 10.0.1.0/24

10.0.1.1
10.0.1.103
10.0.1.104
10.0.1.107
10.0.1.112
10.0.1.113
10.0.1.122
10.0.1.125
10.0.1.140
10.0.1.142

When a host is selected, Zenmap will display a detailed list of the hosts, their operating systems, and common services. In the following screenshot, you can see one of our hosts is a satellite DVR/receiver combo.



Target: 10.0.1.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 10.0.1.0/24

10.0.1.1
10.0.1.103
10.0.1.104
10.0.1.107
10.0.1.112
10.0.1.113
10.0.1.122
10.0.1.125
10.0.1.140
10.0.1.142

10.0.1.140

Host Status

State: up
Open ports: 4
Filtered ports: 0
Closed ports: 996
Scanned ports: 1000
Up time: 79217
Last boot: Wed Mar 20 02:33:16 2013

Addresses

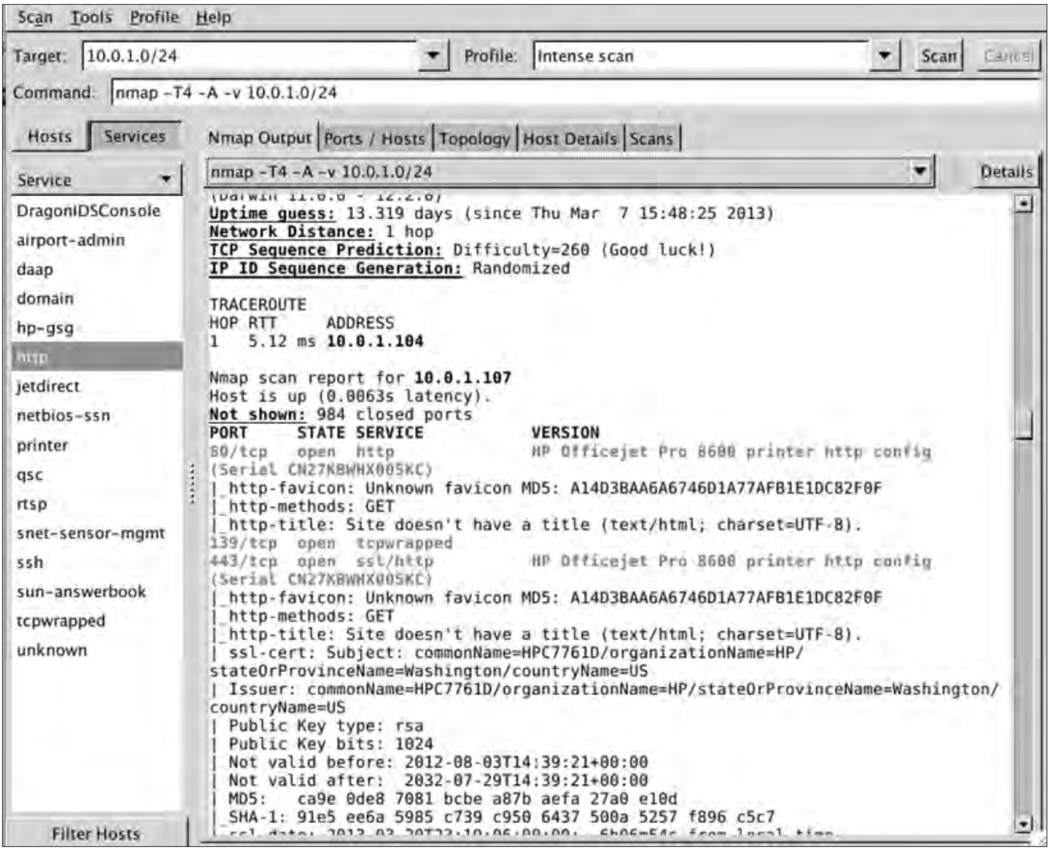
IPv4: 10.0.1.140
IPv6: Not available
MAC: 00:0D:C5:86:80:8F

Operating System

Name: Dish Network VIP 722k DVR (Linux 2.6)
Accuracy: 90%

Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments

If you look at the scan window, you will not only see what ports are open on specific hosts, but also what applications are running on those hosts. Notice that Nmap can determine things, such as a server is running IIS 5.0 as a web server over port 80. The scan results will yield the IP address of the server, the operating system the server is running, as well as the web applications running on the host. Penetration Testers will find these results valuable when they are searching for exploits against this host.



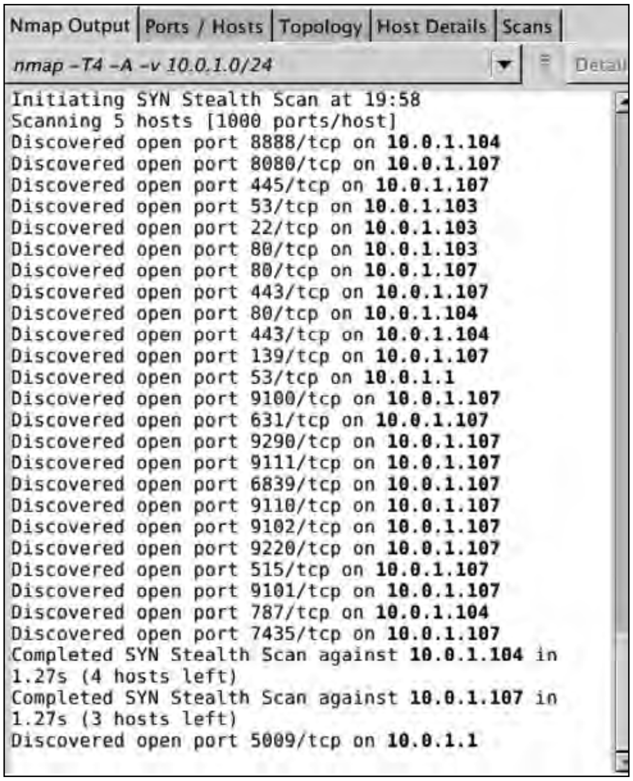
Target: 10.0.1.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 10.0.1.0/24

```
nmap -T4 -A -v 10.0.1.0/24
(Darwin 11.0.0 - 12.2.0)
Uptime guess: 13.319 days (since Thu Mar  7 15:48:25 2013)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE
HOP RTT     ADDRESS
1   5.12 ms 10.0.1.104

Nmap scan report for 10.0.1.107
Host is up (0.0063s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE           VERSION
80/tcp    open  http              HP Officejet Pro 8600 printer http config
(Serial CN27KBWHX005KC)
|_http-favicon: Unknown favicon MD5: A14D3BAA6A6746D1A77AFB1E1DC82F0F
|_http-methods: GET
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
139/tcp   open  tcpwrapped
443/tcp   open  ssl/http          HP Officejet Pro 8600 printer http config
(Serial CN27KBWHX005KC)
|_http-favicon: Unknown favicon MD5: A14D3BAA6A6746D1A77AFB1E1DC82F0F
|_http-methods: GET
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| ssl-cert: Subject: commonName=HPC7761D/organizationName=HP/
stateOrProvinceName=Washington/countryName=US
| Issuer: commonName=HPC7761D/organizationName=HP/stateOrProvinceName=Washington/
countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Not valid before: 2012-08-03T14:39:21+00:00
| Not valid after:  2032-07-29T14:39:21+00:00
| MD5:   ca9e 0de8 7081 bcbe a87b aefa 27a0 e10d
|_SHA-1: 91e5 ee6a 5985 c739 c950 6437 500a 5257 f896 c5c7
|_ssl-date: 2013-03-20T23:10:06+00:00; -6h06m54s from local time.
```

It is now possible for you to concentrate your efforts on the target's running web services or port 80, because it is open.

Zenmap is the best way to get output from Nmap scans. Zenmap offers a rich graphical user interface that displays scans that can be exported into different formats, such as text or Microsoft Excel.

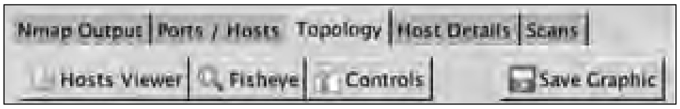
Although there are many ways to get outputs from Nmap (for example, the authors in this book prefer the command-line techniques) we have included this technique because it is constantly referenced in many web penetration standards and is a common way for people to use it.



```
nmap -T4 -A -v 10.0.1.0/24
```

```
Initiating SYN Stealth Scan at 19:58
Scanning 5 hosts [1000 ports/host]
Discovered open port 8888/tcp on 10.0.1.104
Discovered open port 8080/tcp on 10.0.1.107
Discovered open port 445/tcp on 10.0.1.107
Discovered open port 53/tcp on 10.0.1.103
Discovered open port 22/tcp on 10.0.1.103
Discovered open port 80/tcp on 10.0.1.103
Discovered open port 80/tcp on 10.0.1.107
Discovered open port 443/tcp on 10.0.1.107
Discovered open port 80/tcp on 10.0.1.104
Discovered open port 443/tcp on 10.0.1.104
Discovered open port 139/tcp on 10.0.1.107
Discovered open port 53/tcp on 10.0.1.1
Discovered open port 9100/tcp on 10.0.1.107
Discovered open port 631/tcp on 10.0.1.107
Discovered open port 9290/tcp on 10.0.1.107
Discovered open port 9111/tcp on 10.0.1.107
Discovered open port 6839/tcp on 10.0.1.107
Discovered open port 9110/tcp on 10.0.1.107
Discovered open port 9102/tcp on 10.0.1.107
Discovered open port 9220/tcp on 10.0.1.107
Discovered open port 515/tcp on 10.0.1.107
Discovered open port 9101/tcp on 10.0.1.107
Discovered open port 787/tcp on 10.0.1.104
Discovered open port 7435/tcp on 10.0.1.107
Completed SYN Stealth Scan against 10.0.1.104 in
1.27s (4 hosts left)
Completed SYN Stealth Scan against 10.0.1.107 in
1.27s (3 hosts left)
Discovered open port 5009/tcp on 10.0.1.1
```

In addition, several places in GUI for Zenmap allow the user to export graphics and certain parts of the report in CSV files or image files. These exports are extremely valuable when creating reports.



FOCA – website metadata Reconnaissance

Did you know every time you create a document, such as a Microsoft PowerPoint presentation, Microsoft Word document, or PDF, metadata is left in the document?

What is metadata? Metadata is data about data. It is descriptive information about a particular data set, object, or resource, including how it is formatted as well as when and by whom it was collected. Metadata can be useful to Penetration Testers, because it contains information about the system where the file was created, such as:

- Name of users logged into the system
- Software that created the document
- OS of the system that created the document

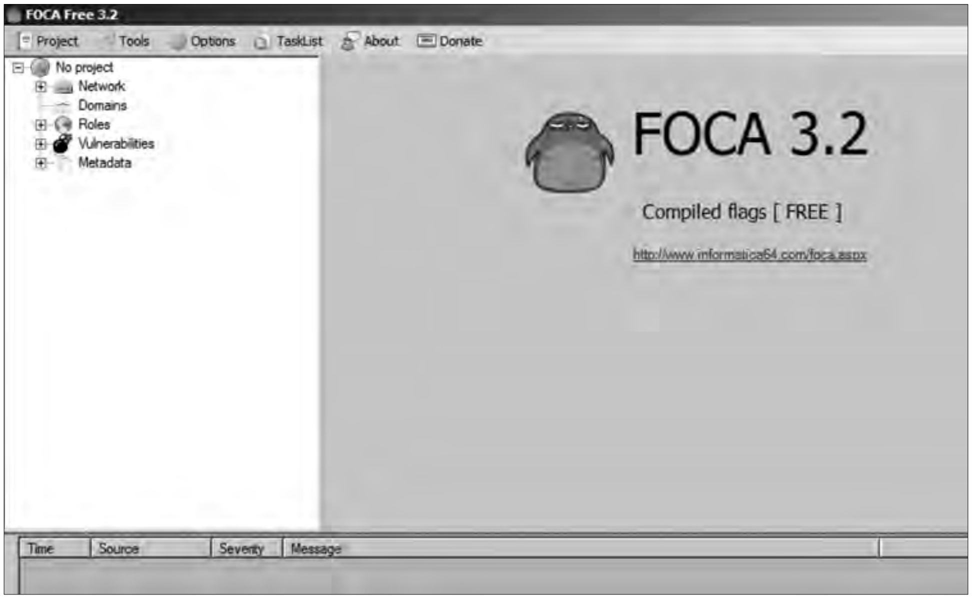
FOCA is a security-auditing tool that will examine metadata from domains. You can have FOCA use search engines to find files on domains or use local files.

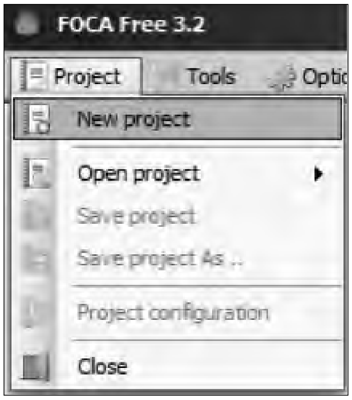
FOCA is built into Kali; however, the version is dated. Best practice is downloading the newest version. FOCA has traditionally been a Windows tool, and the newer versions may be only available for Windows.

The latest version of FOCA can be downloaded at: `http://www.informatica64.com/DownloadFOCA` (use Google Translate to see the page in English).

You will need to give your e-mail address at the bottom of the screen. You will receive an e-mail with the download link. You will also receive updates when FOCA has new releases.

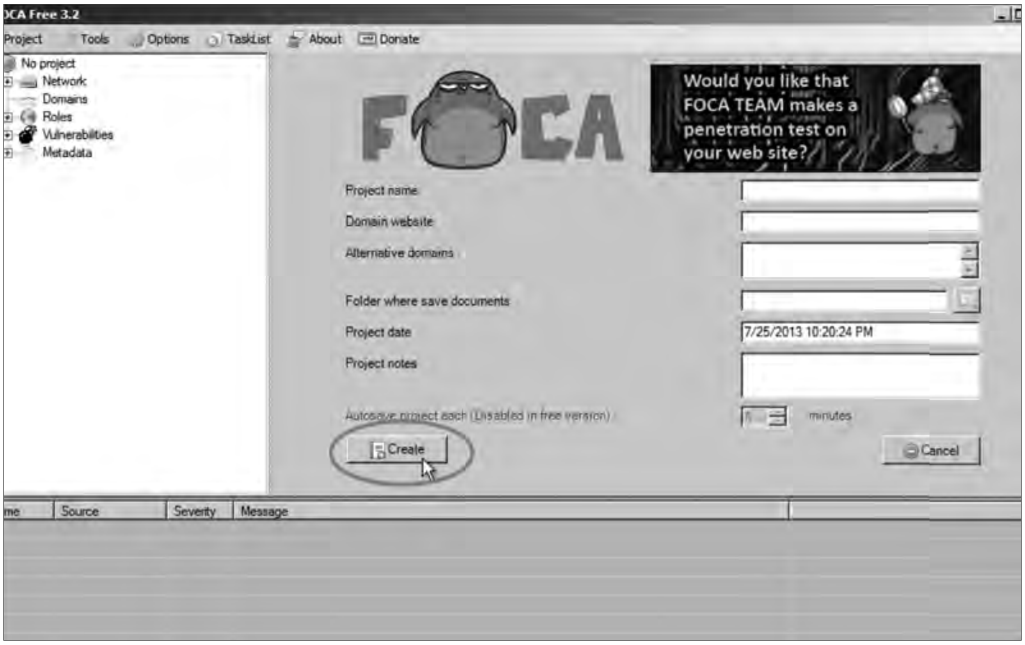
1. The first thing to do after launching FOCA is create a new project, as shown in the following screenshots:.





We recommend keeping all project files in one place. You should create a new folder for each project.

2. Once you name your project and decide where you want to store the project files, click on the **Create** button, as shown in the following screenshot:



Project name

Domain website

Alternative domains

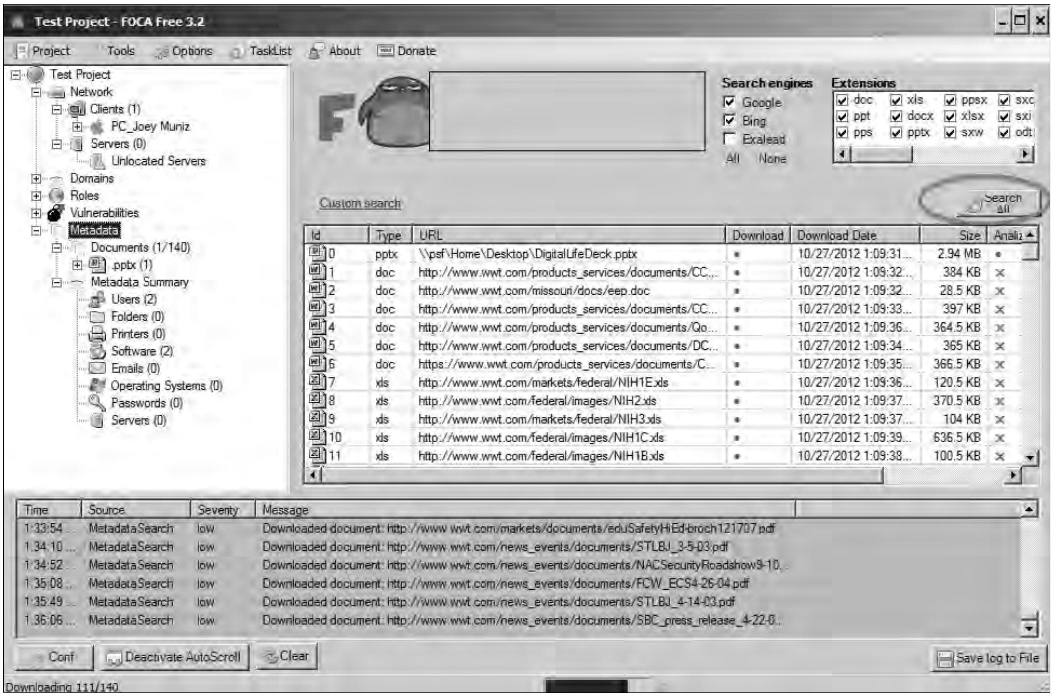
Folder where save documents

Project date 7/25/2013 10:20:24 PM

Project notes

Autosave project each (Disabled in free version) 5 minutes

3. Next thing to do is save your project file. Once you saved the project, click on the **Search All** button so FOCA will use search engines to scan for documents. Optionally, you can use local documents as well.

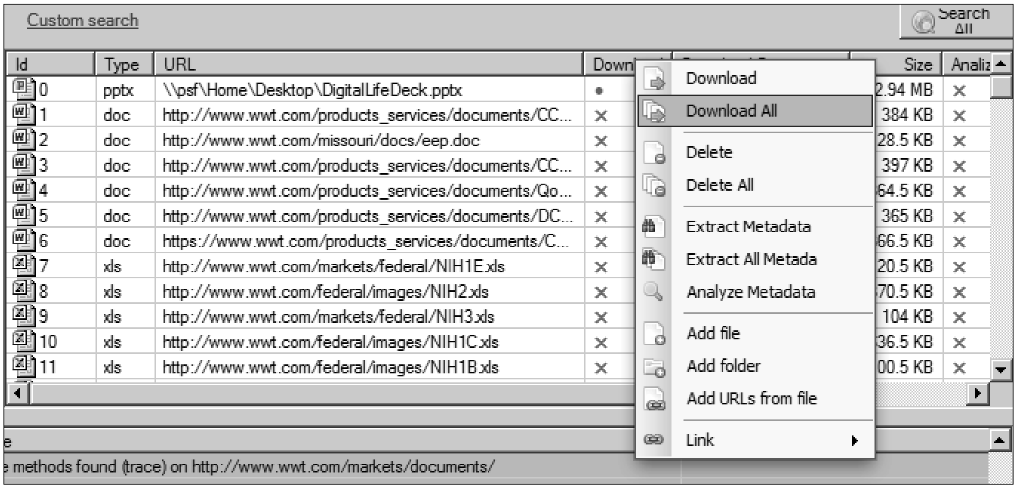


Id	Type	URL	Download	Download Date	Size	Analiz
0	pptx	\\psf\Home\Desktop\DigitalLifeDeck.pptx	•	10/27/2012 1:09:31...	2.94 MB	•
1	doc	http://www.wwt.com/products_services/documents/CC...	•	10/27/2012 1:09:32...	384 KB	×
2	doc	http://www.wwt.com/missouri/docs/eep.doc	•	10/27/2012 1:09:32...	28.5 KB	×
3	doc	http://www.wwt.com/products_services/documents/CC...	•	10/27/2012 1:09:33...	397 KB	×
4	doc	http://www.wwt.com/products_services/documents/Qo...	•	10/27/2012 1:09:36...	364.5 KB	×
5	doc	http://www.wwt.com/products_services/documents/DC...	•	10/27/2012 1:09:34...	365 KB	×
6	doc	https://www.wwt.com/products_services/documents/C...	•	10/27/2012 1:09:35...	366.5 KB	×
7	xls	http://www.wwt.com/markets/federal/NIH1E.xls	•	10/27/2012 1:09:36...	120.5 KB	×
8	xls	http://www.wwt.com/federal/images/NIH2.xls	•	10/27/2012 1:09:37...	370.5 KB	×
9	xls	http://www.wwt.com/markets/federal/NIH3.xls	•	10/27/2012 1:09:37...	104 KB	×
10	xls	http://www.wwt.com/federal/images/NIH1C.xls	•	10/27/2012 1:09:39...	636.5 KB	×
11	xls	http://www.wwt.com/federal/images/NIH1B.xls	•	10/27/2012 1:09:38...	100.5 KB	×

```
Time       Source          Severity  Message
1:33:54 ...  MetadataSearch  low       Downloaded document: http://www.wwt.com/markets/documents/eduSafetyHiEd-broch121707.pdf
1:34:10 ...  MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/STLBJ_3-5-03.pdf
1:34:52 ...  MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/NACSecurityRoadshow9-10...
1:35:08 ...  MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/FCW_ECS4-26-04.pdf
1:35:49 ...  MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/STLBJ_4-14-03.pdf
1:36:06 ...  MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/SBC_press_release_4-22-0...
```

Downloading 111/140

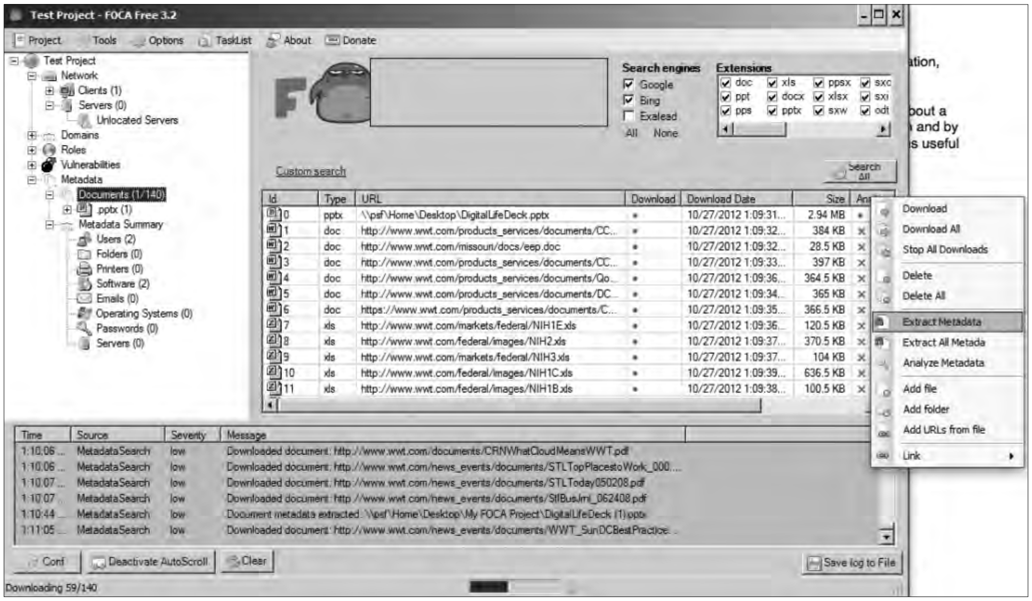
4. Right-click on the file and select the **Download** option, as shown in the following screenshot:



Id	Type	URL	Down	Size	Analiz
0	pptx	\\psf\Home\Desktop\DigitalLifeDeck.pptx	•	2.94 MB	×
1	doc	http://www.wwt.com/products_services/documents/CC...	×	384 KB	×
2	doc	http://www.wwt.com/missouri/docs/eep.doc	×	28.5 KB	×
3	doc	http://www.wwt.com/products_services/documents/CC...	×	397 KB	×
4	doc	http://www.wwt.com/products_services/documents/Qo...	×	64.5 KB	×
5	doc	http://www.wwt.com/products_services/documents/DC...	×	365 KB	×
6	doc	https://www.wwt.com/products_services/documents/C...	×	66.5 KB	×
7	xls	http://www.wwt.com/markets/federal/NIH1E.xls	×	20.5 KB	×
8	xls	http://www.wwt.com/federal/images/NIH2.xls	×	70.5 KB	×
9	xls	http://www.wwt.com/markets/federal/NIH3.xls	×	104 KB	×
10	xls	http://www.wwt.com/federal/images/NIH1C.xls	×	36.5 KB	×
11	xls	http://www.wwt.com/federal/images/NIH1B.xls	×	00.5 KB	×

```
e
e methods found (trace) on http://www.wwt.com/markets/documents/
```

5. Right-click on the file and select the **Extract Metadata** option, as shown in the following screenshot:

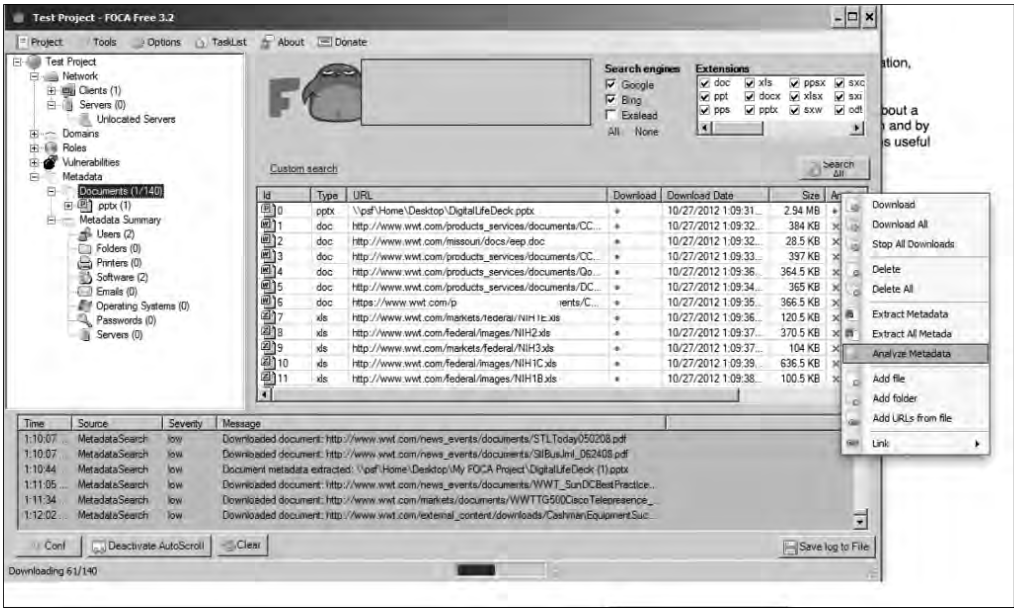


Id	Type	URL	Download	Download Date	Size	An
0	pptx	\\psf\Home\Desktop\DigitalLifeDeck.pptx	•	10/27/2012 1:09:31...	2.94 MB	•
1	doc	http://www.wwt.com/products_services/documents/CC...	•	10/27/2012 1:09:32...	384 KB	×
2	doc	http://www.wwt.com/missouri/docs/eep.doc	•	10/27/2012 1:09:32...	28.5 KB	×
3	doc	http://www.wwt.com/products_services/documents/CC...	•	10/27/2012 1:09:33...	397 KB	×
4	doc	http://www.wwt.com/products_services/documents/Qo...	•	10/27/2012 1:09:36...	364.5 KB	×
5	doc	http://www.wwt.com/products_services/documents/DC...	•	10/27/2012 1:09:34...	365 KB	×
6	doc	https://www.wwt.com/products_services/documents/C...	•	10/27/2012 1:09:35...	366.5 KB	×
7	xls	http://www.wwt.com/markets/federal/NIH1E.xls	•	10/27/2012 1:09:36...	120.5 KB	×
8	xls	http://www.wwt.com/federal/images/NIH2.xls	•	10/27/2012 1:09:37...	370.5 KB	×
9	xls	http://www.wwt.com/markets/federal/NIH3.xls	•	10/27/2012 1:09:37...	104 KB	×
10	xls	http://www.wwt.com/federal/images/NIH1C.xls	•	10/27/2012 1:09:39...	636.5 KB	×
11	xls	http://www.wwt.com/federal/images/NIH1B.xls	•	10/27/2012 1:09:38...	100.5 KB	×

```
Time       Source          Severity  Message
1:10:06 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/documents/CRNWhatCloudMeansWWT.pdf
1:10:06 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/STLTopPlacestoWork_000....
1:10:07 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/STLToday050208.pdf
1:10:07 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/StlBusJml_062408.pdf
1:10:44 ... MetadataSearch  low       Document metadata extracted: \\psf\Home\Desktop\My FOCA Project\DigitalLifeDeck (1).pptx
1:11:05 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/WWT_SunDCBestPractice...
```

Downloading 59/140

6. Right-click on the file and select the **Analyze Metadata** option, as shown in the following screenshot:

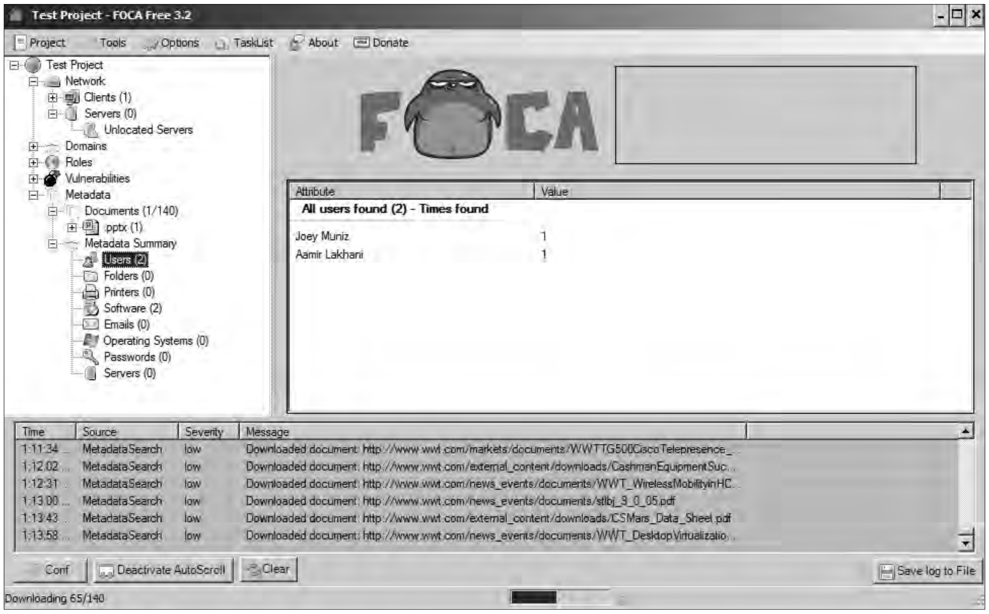


Id	Type	URL	Download	Download Date	Size	An
0	pptx	\\psf\Home\Desktop\DigitalLifeDeck.pptx	•	10/27/2012 1:09:31...	2.94 MB	•
1	doc	http://www.wwt.com/products_services/documents/CC...	•	10/27/2012 1:09:32...	384 KB	×
2	doc	http://www.wwt.com/missouri/docs/eep.doc	•	10/27/2012 1:09:32...	28.5 KB	×
3	doc	http://www.wwt.com/products_services/documents/CC...	•	10/27/2012 1:09:33...	397 KB	×
4	doc	http://www.wwt.com/products_services/documents/Qo...	•	10/27/2012 1:09:36...	364.5 KB	×
5	doc	http://www.wwt.com/products_services/documents/DC...	•	10/27/2012 1:09:34...	365 KB	×
6	doc	https://www.wwt.com/p ents/C...	•	10/27/2012 1:09:35...	366.5 KB	×
7	xls	http://www.wwt.com/markets/federal/NIH1E.xls	•	10/27/2012 1:09:36...	120.5 KB	×
8	xls	http://www.wwt.com/federal/images/NIH2.xls	•	10/27/2012 1:09:37...	370.5 KB	×
9	xls	http://www.wwt.com/markets/federal/NIH3.xls	•	10/27/2012 1:09:37...	104 KB	×
10	xls	http://www.wwt.com/federal/images/NIH1C.xls	•	10/27/2012 1:09:39...	636.5 KB	×
11	xls	http://www.wwt.com/federal/images/NIH1B.xls	•	10/27/2012 1:09:38...	100.5 KB	×

```
Time       Source          Severity  Message
1:10:07 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/STLToday050208.pdf
1:10:07 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/StlBusJml_062408.pdf
1:10:44 ... MetadataSearch  low       Document metadata extracted: \\psf\Home\Desktop\My FOCA Project\DigitalLifeDeck (1).pptx
1:11:05 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/WWT_SunDCBestPractice...
1:11:34 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/markets/documents/WWTTG500CiscoTelepresence_...
1:12:02 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/external_content/downloads/CashmanEquipmentSuc...
```

Downloading 61/140

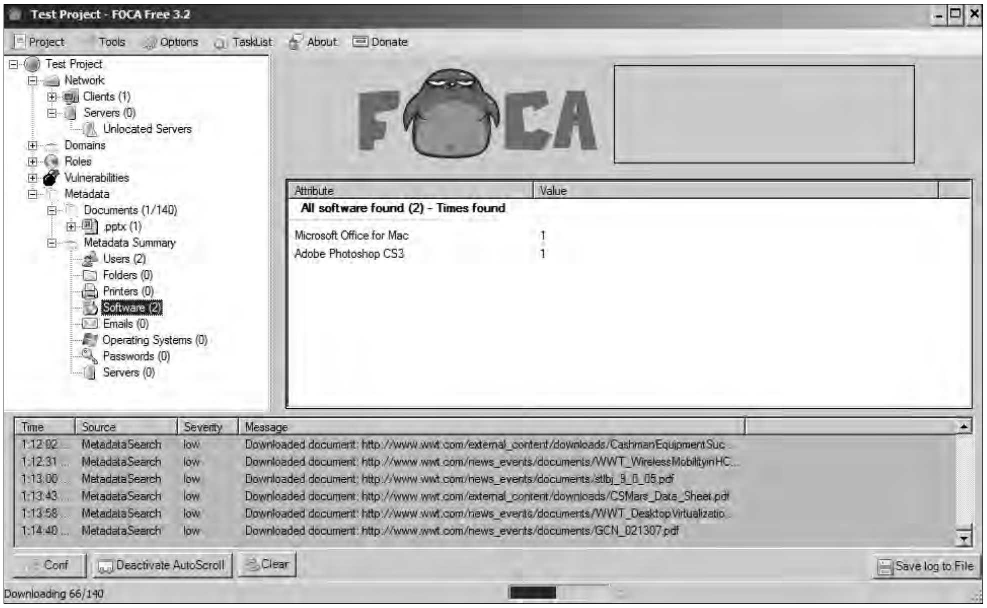
In the following screenshot, you can see two people opened this document.



Attribute	Value
All users found (2) - Times found	
Joey Muniz	1
Aamir Lakhani	1

```
Time        Source          Severity  Message
1:11:34 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/markets/documents/WWTTG500CiscoTelepresence_...
1:12:02 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/external_content/downloads/CashmanEquipmentSuc...
1:12:31 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/WWT_WirelessMobilityinHC...
1:13:00 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/stlbj_9_0_05.pdf
1:13:43 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/external_content/downloads/CSMars_Data_Sheet.pdf
1:13:58 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/WWT_DesktopVirtualizatio...
```

You can also determine Microsoft Office for the Mac and Adobe Photoshop were used to create this document as shown in the following screenshot:



Attribute	Value
All software found (2) - Times found	
Microsoft Office for Mac	1
Adobe Photoshop CS3	1

```
Time        Source          Severity  Message
1:12:02 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/external_content/downloads/CashmanEquipmentSuc...
1:12:31 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/WWT_WirelessMobilityinHC...
1:13:00 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/stlbj_9_0_05.pdf
1:13:43 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/external_content/downloads/CSMars_Data_Sheet.pdf
1:13:58 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/WWT_DesktopVirtualizatio...
1:14:40 ... MetadataSearch  low       Downloaded document: http://www.wwt.com/news_events/documents/GCN_021307.pdf
```

In many cases, attackers will be able to see much more information and gather intelligence about a target.

FOCA allows the user to save and index a copy of all the metadata. In addition, each type of metadata file can be saved and copied. This gives a Penetration Tester a wealth of information. Screenshots are usually used to give an overview of the indexed files, along with a listing of all individual files. Finally, FOCA will allow a Penetration Tester to download individual files that can be used as examples.

Summary

Reconnaissance is typically the most critical step in a Penetration Testing exercise and can be the most time consuming. Any actions taken against a target is customized around results from Reconnaissance previously performed. The more data known about a target equates to the less likely to trigger alarms, as well as better chance of identifying a way to compromise the target. It is recommended to look at this chapter as a prerequisite to the remaining chapters in this textbook.

In this chapter, we focused on various ways to gather information about a target. We showcased some popular free tools available on the Internet, as well as Information Gathering utilities available in Kali Linux. At this point, you should be ready to evaluate targets identified through Reconnaissance for possible exploitation.

The next chapter will focus on identifying and exploiting vulnerabilities in web applications and web servers.

Where to buy this book

You can buy Web Penetration Testing with Kali Linux from the Packt Publishing website: `http://www.packtpub.com/web-penetration-testing-with-kali-linux/book`.

Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.

[PACKT] PUBLISHING open source community experience distilled

www.PacktPub.com