Ethical Hacking - Theory

based on the slides of

Hacking Exposed 7

Network Security Secrets & Solutions

Book - Table of Contents

- **Part I Casing the Establishment**
  - **Footprinting**
  - **Scanning**
  - **Enumeration**

- **Part II Endpoint and Server Hacking**
  - **Hacking Windows (later)**
  - **Hacking UNIX (LAB)**
  - **Cybercrime and Advanced Persistent Threats**

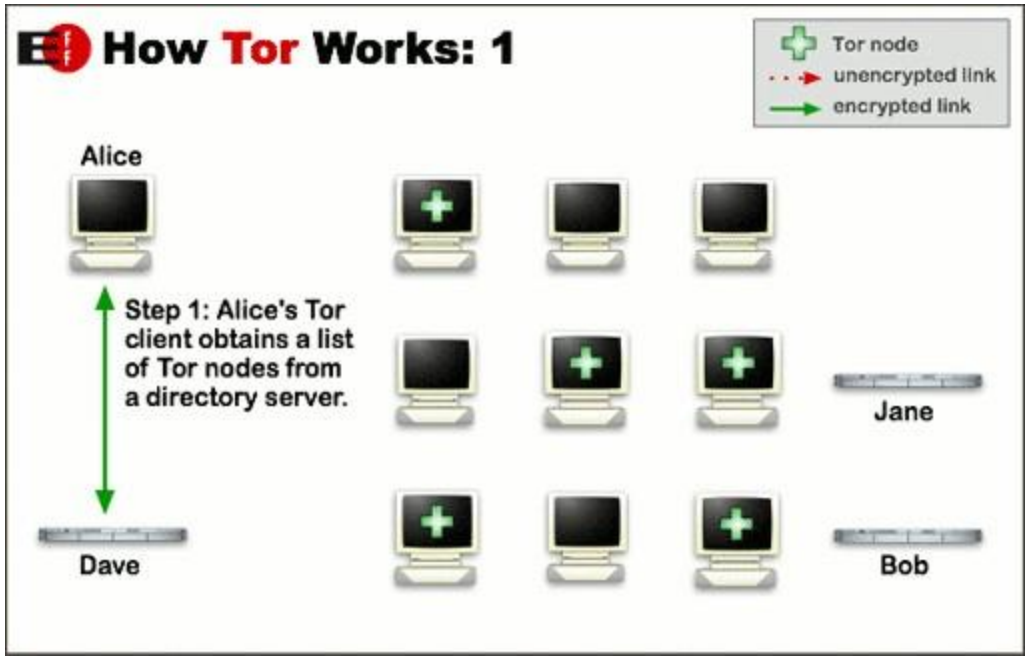
- **Part III Infrastructure Hacking**
  - **Remote Connectivity and VoIP Hacking**
  - **Wireless Hacking**
  - **Hacking Hardware**

- **Part IV Application and Data Hacking**
  - **Web and Database Hacking (LAB) (before)**
  - **Mobile Hacking**
  - **Countermeasures Cookbook**

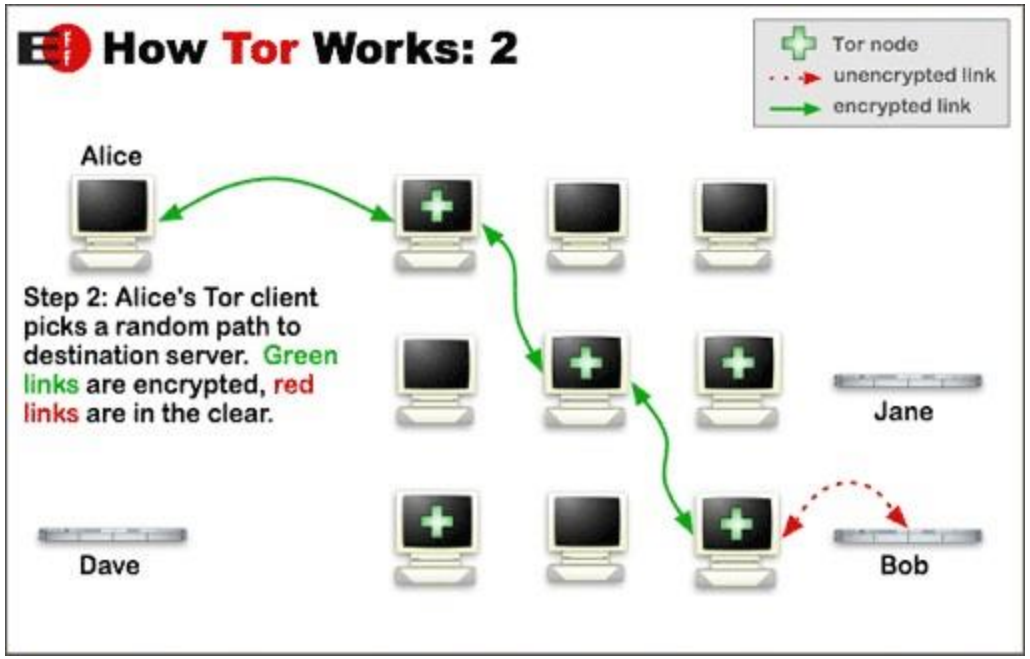
Part I Casing The Establishment Case Study: How A Hacker Works

- IAAAS (It's All About Anonymity, Stupid)
  - The Onion Router (Tor), www.torproject.org
    - Layered cryptography with SOCKS proxy
    - Anonymous outgoing TCP connections
  - Tor GUI client (Vidalia) and Privoxy (web filtering proxy)
  - Google on browser for juicy targets
  - tor-resolve instead of host for IP addresses
  - proxychains to force connections through Tor
    - Nmap to scan services on targets
  - socat to relay persistently
    - nc (netcat) to send requests to servers (check server version)
    - Exploit vulnerabilities to pwn (own or compromise)

The Onion Router (TOR) - Overview



TOR


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

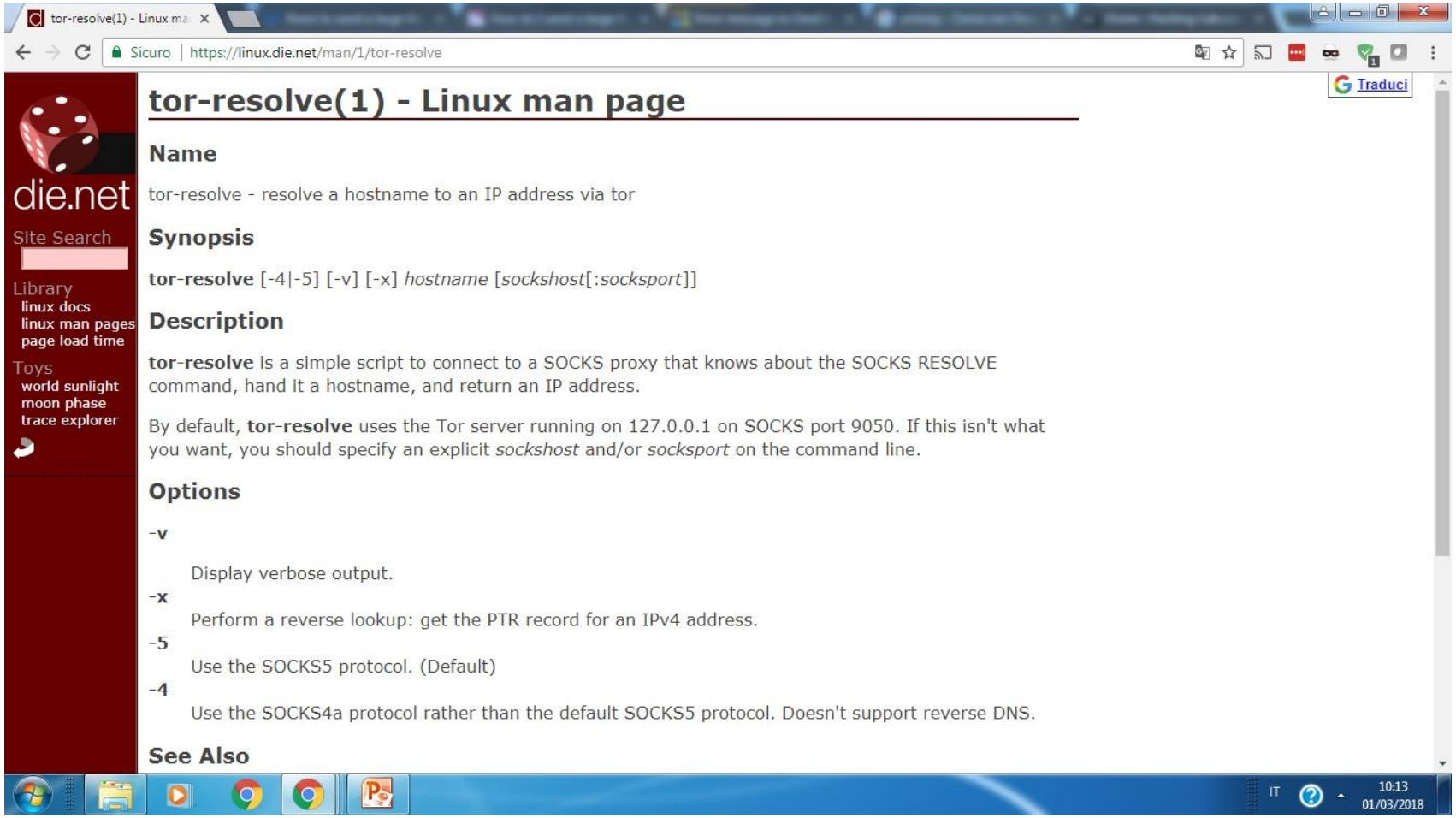
Vidalia

Vidalia is a discontinued cross-platform GUI for controlling Tor. It allows the user to start, stop or view the status of Tor

Privoxy

- **Privoxy** is a free web proxy for enhancing privacy, manipulating cookies and modifying web page data and HTTP headers before the page is rendered by the browser. E.g. filtering web pages and removing advertisements. Privoxy can be customized by users.

Tor-resolve



tor-resolve(1) - Linux man page

Name

tor-resolve - resolve a hostname to an IP address via tor

Synopsis

tor-resolve [-4|-5] [-v] [-x] *hostname* [*sockshost*[:*socksport*]]

Description

tor-resolve is a simple script to connect to a SOCKS proxy that knows about the SOCKS RESOLVE command, hand it a hostname, and return an IP address.

By default, **tor-resolve** uses the Tor server running on 127.0.0.1 on SOCKS port 9050. If this isn't what you want, you should specify an explicit *sockshost* and/or *socksport* on the command line.

Options

-v

Display verbose output.

-x

Perform a reverse lookup: get the PTR record for an IPv4 address.

-5

Use the SOCKS5 protocol. (Default)

-4

Use the SOCKS4a protocol rather than the default SOCKS5 protocol. Doesn't support reverse DNS.

See Also

```
bt ~ # tor-resolve www.example.com 10.10.10.100
```

Proxychains

NMAP


How can I scan my netw
Sicuro | https://www.oreilly.com/learning/how-can-i-scan-my-network-using-nmap
How can I scan my network using Nmap?
Learn how you can use Nmap to scan your network to find out which services and hosts are listening and may be vulnerable to compromise.
By Chad Russell. April 27, 2017
CHAD RUSSELL
Cyber Security Specialist
Author of Certified Ethical
king Series for O'Reilly
lishing
COURSE
O'REILLY
Certified Ethical Hacker (CEH) - Hacking Users and Their Devices
Gain hands-on experience with the techniques and tools used in sanctioned penetration testing exercises.
Start learning
IT
10:31
01/03/2018

NMAP

Nmap Cheat Sheet | Hac

Sicuro | https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

ONLINE SCANNERS TOOLS BLOG ABOUT MEMBERSHIP LOG IN

Nmap Target Selection

Scan a single IP	`nmap 192.168.1.1`
Scan a host	`nmap www.testhostname.com`
Scan a range of IPs	`nmap 192.168.1.1-20`
Scan a subnet	`nmap 192.168.1.0/24`
Scan targets from a text file	`nmap -iL list-of-ips.txt`

These are all default scans, which will scan 1000 TCP ports. Host discovery will take place.

Nmap Port Selection

Scan a single Port	`nmap -p 22 192.168.1.1`
Scan a range of ports	`nmap -p 1-100 192.168.1.1`
Scan 100 most common ports (Fast)	`nmap -F 192.168.1.1`
Scan all 65535 ports	`nmap -p- 192.168.1.1`

IT 10:32 01/03/2018

socat

This commands opens a proxy listening on localhost:8080 and forwards all requests through Tor to the target 10.10.100:80

```
bt ~ # socat TCP4-LISTEN:8080, fork
SOCKS4a:127.0.0.1:10.10.10.100:80, socksport=9050 &
```

Chapter 1 Footprinting

- What is footprinting & why
- Internet footprinting
  1. Determine the scope of your activities
  2. Get proper authorization
  3. Publicly available information
  4. WHOIS & DNS enumeration
  5. DNS interrogation
  6. Network reconnaissance

What Is Footprinting?

- Footprint: profile of the target organization
- Why? It gives you a picture of what the hacker sees.
- Sun Tzu - The Art of War: Know yourself and your enemy!
- What to footprint/profile?
  - Internet: domain names, network blocks and subnets, IP addresses, TCP/UDP services, CPU arch, access control, IDS, system enumeration, DNS hostnames
  - Intranet: network protocols, internal domain names, network blocks, IP addresses, TCP/UDP services, CPU arch, access control, IDS, system enumeration
  - Remote access: phone numbers, remote system type, authentication mechanisms, VPN
  - Extranet: domain names, connection source and destination, type of connection, access control

Internet Footprinting

- Step 1: Determine the scope of your activities
  - Entire organization or subsidiaries?
  - Determine all, so as to secure them
- Step 2: Get proper authorization
  - Layers 8 and 9: politics and funding
  - Get-out-of-jail-free card
- Step 3: Publicly available information
  - Nothing short of amazing!

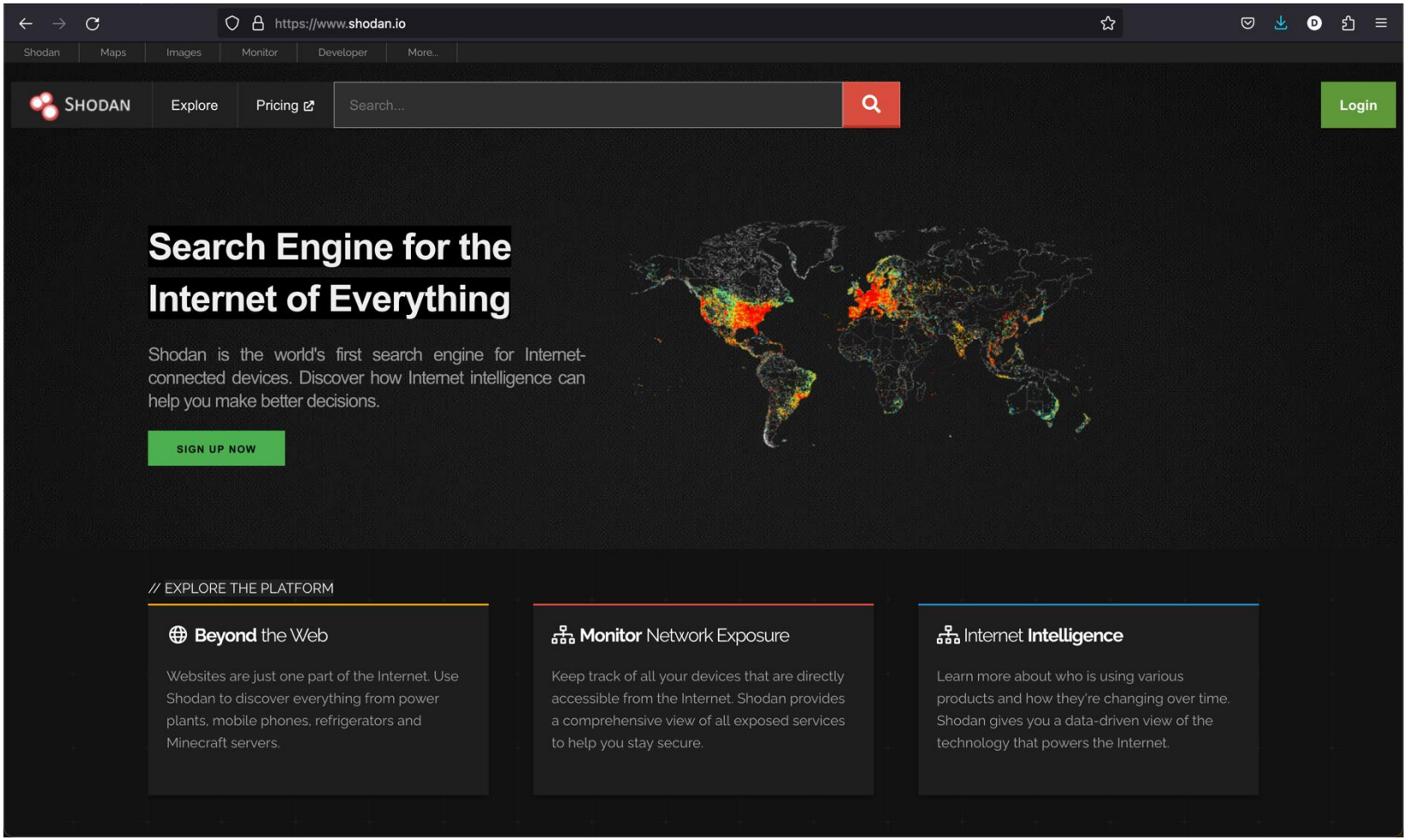
Publicly Available Information Company Web Pages

- Unexpected: security configuration, asset inventory spreadsheet, etc.
- HTML source code (offline faster)
  - Things buried in comment tags: <, !, --
  - Website mirroring tools for offline viewing: Wget (Linux), Teleport Pro (Windows)
- Enumerate hidden files and directories recursively
  - OWASP's DirBuster
    - Easy to be detected: proxy through privoxy
- Remote access to internal resources via browser
  - Proxy to internal servers (e.g. Microsoft Exchange server)
- Look for other sites beyond the main
  - www1, www2, web, test, etc.
  - VPN sites

Publicly Available Information
Related Organizations
Location Details

- Related organizations
  - Look for references and links to other organizations
    - Outsourced web development
      - Partners might not be security-minded
      - Social engineering attack
- Location details needed for
  - Dumpster-diving, surveillance, social engineering, unauthorized access, etc.
  - Images
    - Google Earth, Google Maps – Street View (Wi-Fi MAC addresses), Google Locations and Skyhook (MAC → location: "How I Met Your Girlfriend" – BlackHat 2010 demo)

Google tracking Wi-Fi



Publicly Available Information Employee Information (1/2)

- Names -> e-mail addresses, usernames
- Phone numbers → physical address, social engineering
  - Phonenumber.com, 411.com, yellowpages.com
- Other personal details
  - Blackbookonline.info, peoplesearch.com
    - Home phone number, address, social security number, credit history, criminal record, etc.
  - Social/information/professional networking, career, family ancestry, photo management sites
    - Facebook.com, Reunion.com, Classmates.com, Twitter.com, Linkedin.com, Plaxo.com, Monster.com, Careerbuilder.com, Dice.com, Ancestry.com, Flickr.com, Photobucket.com
- Business directory services:
  - JigSaw.com, FullContact, Insideview…
  - Used by sales teams
  - Paid-for services with incentive award points to new or update entries
- OSINT Search engine framework: https://osintframework.com/

Publicly Available Information Employee Information (2/2)

- Job posting and resumes
  - "Checkpoint firewalls and Snort IDS" tells much!
  - Google "*company* resume firewall" to get resumes from current and past employees
  - Search on job sites (monster.com, careerbuilder.com)
  - Watch disgruntled and ex-employees: revenge!
- Employee's home computers
  - Remote access to the target
  - Keystroke logger: free ride to the target!
    - Impersonate a trusted user!

Publicly Available Information Current Events

- Mergers, acquisitions, scandals, layoffs, rapid hiring, reorganization, outsourcing, temporary contractors
- Merger or acquisition
  - Blending of organizations' networks
    - Less or disabled security
- Human factor
  - Low morale → update resumes
  - Unauthorized guests
- SEC (Security and Exchange Commission) reports
  - Periodical reporting: 10-Q (quarter) and 10-K (annual)
  - Sec.gov → organizational charts
- Business info and stock trading sites
  - Yahoo!Finance message boards

https://www.sec.gov/edgar/search/

SEC.gov | EDGAR

FAQ Other search tools

Document word or phrase

Keywords to search for in filing documents

Company name, ticker, CIK number or individual's name

Company name, ticker, CIK number or individual's name

Filing category

Browse filing types

View all

Filed date range

Last 5 years

Filed from

2019-02-27

Filed to

2024-02-27

Principal executive offices in

View all

- less search options

SEARCH

Clear all

Accessibility | Budget & Performance | Careers | Contact | Contracts | Data | FOIA | Inspector General | Investor.gov | No FEAR Act & EEO Data | Ombudsman | Plain Writing | Privacy | Related Sites | Site Map | USA.gov | Votes | Vulnerability Disclosure Policy | Whistleblower Protection

Publicly Available Information

Privacy or Security Policies
Archived Information

- Privacy or security policies
  - Technical details indicating the types of security mechanisms in place
- Archived information
  - Archived copies > current copies
  - Archive.org & cached results at Google

https://archive.org/web/

INTERNET ARCHIVE | WEB | BOOKS | VIDEO | AUDIO | SOFTWARE | IMAGES | SIGN UP | LOG IN | UPLOAD

ABOUT | BLOG | PROJECTS | HELP | DONATE ♥ | CONTACT | JOBS | VOLUNTEER | PEOPLE

INTERNET ARCHIVE
WayBackMachine

Explore more than 866 billion web pages saved over time

http:// BROWSE HISTORY

Find the Wayback Machine useful? DONATE

Tools

Wayback Machine Availability API
Build your own tools.

WordPress Broken Link Checker
Banish broken links from your blog.

404 Handler for Webmasters
Help users get where they were going.

Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.

Save Page Now

https://

SAVE PAGE

Capture a web page as it appears now for use as a trusted citation in the future.

Only available for sites that allow crawlers.

FAQ | Contact Us | Terms of Service (Dec 31, 2014)

Publicly Available Information
Search Engines and Data Relationships

- Google.com, bing.com, yahoo.com, dogpile.com, ask.com
- Search strings used by hackers - Google Hacking Database (GHDB) at hackersforcharity.org/ghdb/
- Search Google's cache for vulnerabilities, errors, configuration issues, etc. – Athena (snakeoillabs.com), SiteDigger (foundstone.com), Wikto (sensepost.com/research/wikto)
- Analyze metadata in web files for info leaks – FOCA (informatica64.com/foca.aspx)
- Mining and linking relevant pieces of info on a subject – Maltego (paterva.com)

➢ Public Database Security Countermeasures:
  - ➢ Site Security Handbook: RFC 2196
  - ➢ Periodically review and remove public but sensitive data!

SiteDigger

File Edit Tools Help

- FSDB(175)
  - Backup Files(12)
  - Configuration Managem
  - Error Messages(39)
  - Privacy Related(30)
  - Remote Administration(
  - Reported Vulnerabilities
  - Technology Profile(43)
- GHDB(1467)

Site/Domain: [Optional]

Cancel

Clear

Queries Scanned:

1 "Index of /backup" F142
2 intitle:"Index of" ".htpasswd" htpasswd.bak F31
3 intitle:"Index of" index.html.bak F1
4 intitle:"Index of" index.html.bak F176
5 intitle:"Index of" index.html~ F178
6 intitle:"Index of" index.jsp.bak F3
7 intitle:"Index of" index.php.bak F2
8 intitle:"Index of" index.php.bak F177
9 intitle:"Index of" index.php~ F179
10 intitle:index.of .bash_history F19
11 intitle:index.of .sh_history F20
12 inurl:backup intitle:index.of inurl:admin F141

Selected Entry Info:

software.informer.comhttp://www.mcafee.com/us/about/contact-us.aspx

Scanning

Results: [Double click a link to open in default browser]

URL	Query	Category

Google Hacking for Pene

Sicuro | https://www.amazon.com/Google-Hacking-Penetration-Testers-Third/dp/0128029641/ref=pd_lpo_sbs_14_t_0/143-4724252-3204714?_en

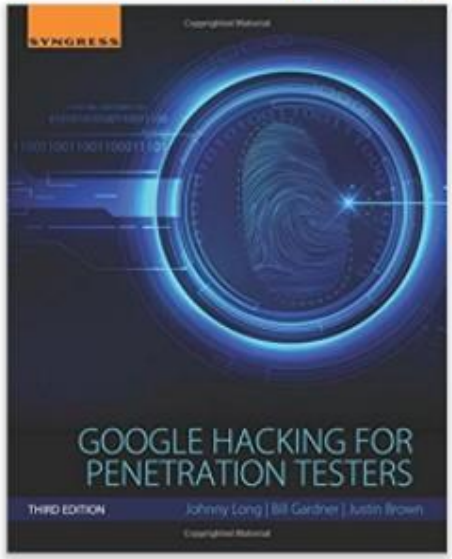
Kindle Monthly Deals Up to 80% off top titles › Browse now

Google Hacking for Penetration Testers, Third Edition 3rd Edition

by Johnny Long (Author), Bill Gardner (Author), Justin Brown (Author)

22 customer reviews

Look inside



ISBN-13: 978-0128029640
ISBN-10: 0128029641
Why is ISBN important?

Have one to sell? Sell on Amazon

Add to List

Share

Kindle $39.68 | **Paperback** $48.30 - $58.03 | Other Sellers See all 3 versions

Buy used

Buy new

In Stock.
Ships from and sold by Amazon.com. Gift-wrap available.

This item ships to **Italy**. **Want it Monday, March 12?** Order within **23 hrs 36 mins** and choose **AmazonGlobal Priority Shipping** at checkout. Learn more

Deliver to Italy

Qty: 1

Add

Turn on 1-Cl

More Buying Choices

24 New from $52.43 | 16 Used from $48.30

40 used & n

See All Buyi

prime student College student? Get FREE shipping and exclusive deals LEARN MORE

Google is the most popular search engine ever created, but Google's search capabilities are so powerful, they

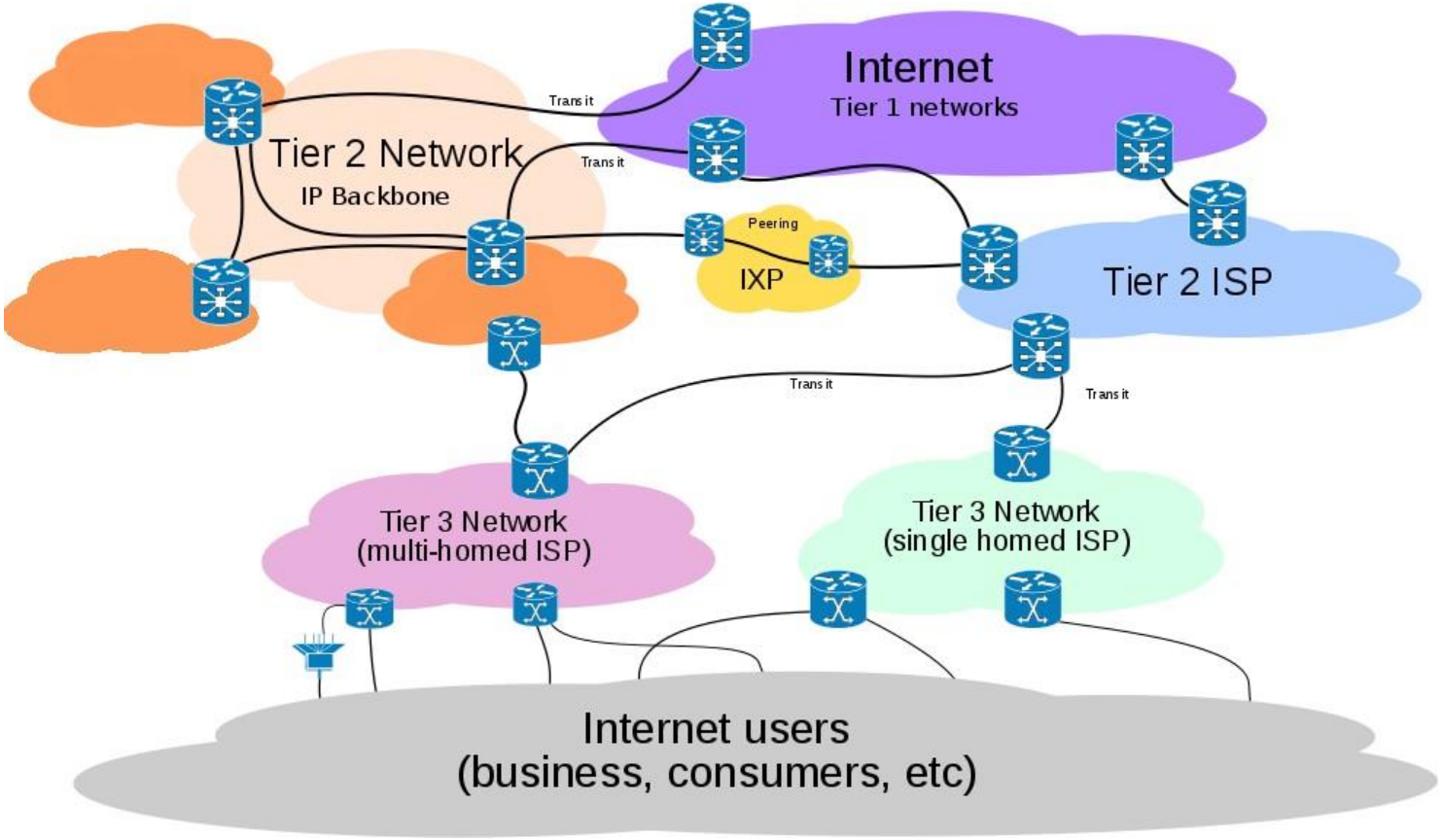
allinurl:tsweb/default.htm

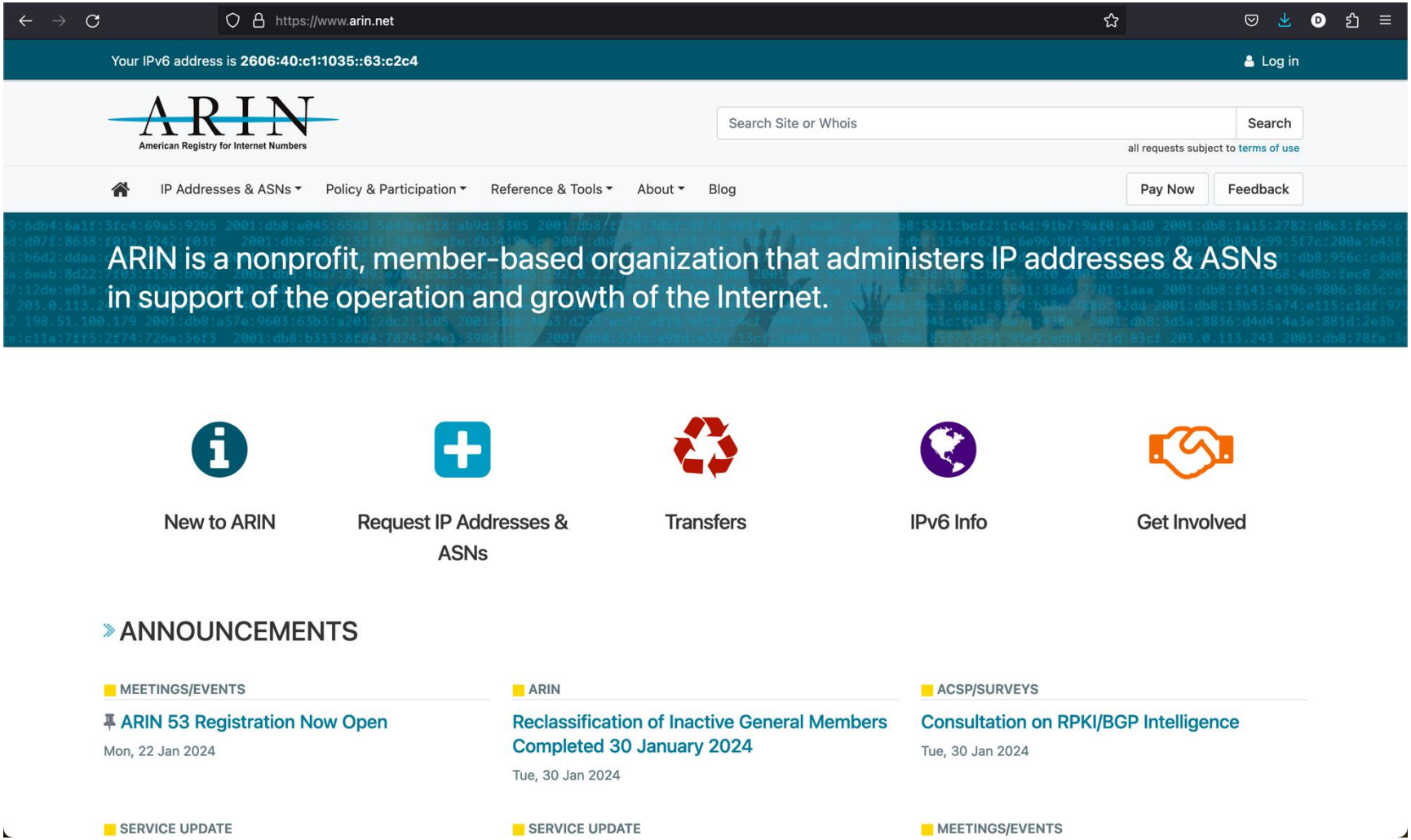
- Microsoft Windows servers with Remote Desktop Web Connection exposed
- Google Hacking Database (GHDB), found at hackersforcharity.org/ghdb/

Step 4: WHOIS and DNS Enumeration

- Domain names, IP addresses, port numbers
  - Centrally managed by ICANN (Internet Corporation for Assigned Names and Numbers)
  - Hierarchically stored in WHOIS/DNS servers
- Three R of WHOIS: registry, registrar, registrant
- To lookup keyhole.com, start from whois.iana.org
  - Find the registry and registrar for .com (verisign-grs.com) and then keyhole.com (markmonitor.com)
  - Find the registrant details of keyhole.com (for later spoofing)
  - Web whois or command-line whois
  - Automatic tools (allwhois, uwhois) and GUI tools (superscan, netscan tools pro)
- To lookup 61.0.0.2, start from arin.net
  - Find apnic.net, then find National Backbone of India
  - But keep in mind the IP address might be spoofed/masqueraded

Internet Infrastructure




https://www.arin.net
Your IPv6 address is 2606:40:c1:1035::63:c2c4
Log in
ARIN
American Registry for Internet Numbers
Search Site or Whois
Search
all requests subject to terms of use
IP Addresses & ASNs
Policy & Participation
Reference & Tools
About
Blog
Pay Now
Feedback
ARIN is a nonprofit, member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet.
New to ARIN
Request IP Addresses & ASNs
Transfers
IPv6 Info
Get Involved
ANNOUNCEMENTS
MEETINGS/EVENTS
ARIN 53 Registration Now Open
Mon, 22 Jan 2024
ARIN
Reclassification of Inactive General Members Completed 30 January 2024
Tue, 30 Jan 2024
ACSP/SURVEYS
Consultation on RPKI/BGP Intelligence
Tue, 30 Jan 2024
SERVICE UPDATE
SERVICE UPDATE
MEETINGS/EVENTS

Public Database Security Countermeasures

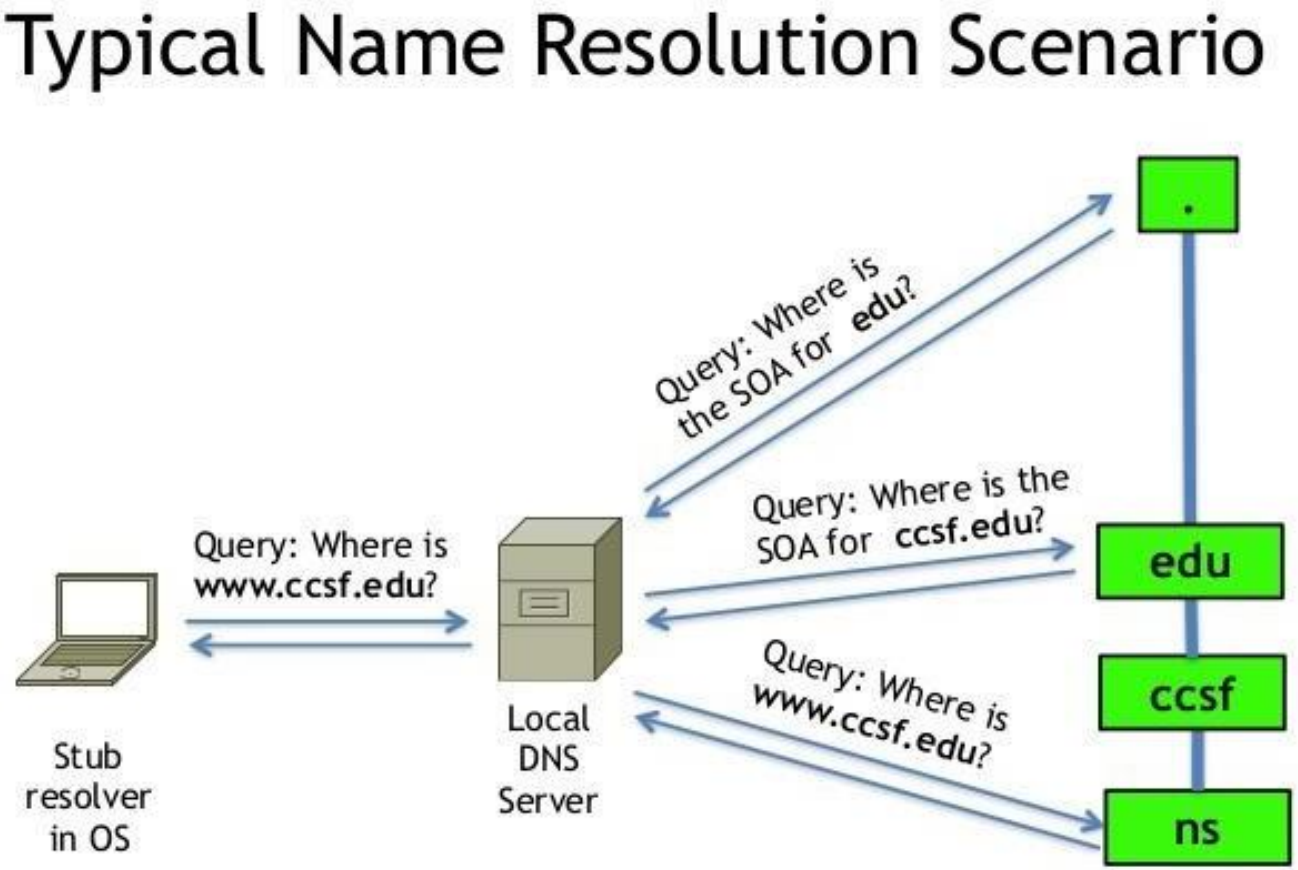
Administrative contacts, registered net blocks authoritative name servers

- Keep administrative contacts up-to-date
- *Anonymize* administrative contacts
- *Authenticate* updates rigidly to avoid *domain hijacking*

  Using passwords or PGP, not FROM field of email addresses

  – AOL in 1998: redirected traffic

DNS - Start Of Authority (SOA) record



DNS record types

DS	43	RFC 4034	signer	The record used to identify the DNSSEC signing key of a delegated zone
HINFO	13	RFC 8482	Host Information	Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY
HIP	55	RFC 8005	Host Identity Protocol	Method of separating the end-point identifier and locator roles of IP addresses.
IPSECKEY	45	RFC 4025	IPsec Key	Key record that can be used with IPsec
KEY	25	RFC 2535[3] and RFC 2930[4]	Key record	Used only for SIG(0) (RFC 2931) and TKEY (RFC 2930).[5] RFC 3445 eliminated their use for application keys and limited their use to DNSSEC.[6] RFC 3755 designates DNSKEY as the replacement within DNSSEC.[7] RFC 4025 designates IPSECKEY as the replacement for use with IPsec.[8]
KX	36	RFC 2230	Key Exchanger record	Used with some cryptographic systems (not including DNSSEC) to identify a key management agent for the associated domain-name. Note that this has nothing to do with DNS Security. It is Informational status, rather than being on the IETF standards-track. It has always had limited deployment, but is still in use.
LOC	29	RFC 1876	Location record	Specifies a geographical location associated with a domain name
MX	15	RFC 1035[1] and RFC 7505	Mail exchange record	Maps a domain name to a list of message transfer agents for that domain

Step 5: DNS Interrogation

- Obtain revealing info about the organization by querying DNS servers (domain name <-> IP addresses)
- DNS zone transfer by untrusted users
  - Due to misconfiguration
  - From primary server to secondary server
  - Private DNS info: internal hostnames and IP addresses
  - dnsrecon
- nslookup
  - mapping and getting all resource records (A, RP, MX, HINFO, etc.)
  - HINFO: host info
  - Search with grep, sed, awk, perl
  - Scripts: dnsenum, dnsmap, fierce, host

Step 5: DNS Interrogation

```
[bash]$ nslookup
Default Server: nsl.example.com
Address: 10.10.20.2
> 192.168.1.1
Server: ns1.example.com
Address: 10.10.20.2
Name: gate.example.com
Address: 192.168.1.1
> set type=any
> ls -d example.com. ›|> /tmp/zone out
```

Step 5: DNS Interrogation

```
bash]$ more zone_out
acct18        ID IN A   192.168.230.3
           ID IN HINFO "Gateway2000" "WinWKGRPS"
           ID IN MX   0 exampleadmin-smtp
           ID IN RP   bsmith.rci bsmith.who
           ID IN TXT   "Location:Telephone Room"
ce          ID IN CNAME  aesop
au          ID IN A    192.168.230.4
           ID IN HINFO  "Aspect" "MS-DOS"
           ID IN MX   0 andromeda
           ID IN RP   jcoy.erebus jcoy.who
           ID IN TXT   "Location: Library"
acct21        ID IN A    192.168.230.5
           ID IN HINFO  "Gateway2000" "WinWKGRPS"
           ID IN MX    0 exampleadmin-smtp
           ID IN RP    bsmith.rci bsmith.who
           ID IN TXT    "Location:Accounting"

[bash]$ grep -I test /tmp/zone_out |wc -l
  96
```

DNS Security Countermeasures

- Restrict zone transfer to only authorized servers
  - named.conf in BIND
- Configure a firewall to deny unauthorized inbound connections to TCP port 53 (thwart zone transfer) DNS - Domain Name System.
- Configure not to provide *internal* DNS info
- Discourage the use of HINFO records

Step 6: Network Reconnaissance

- Network topology and access path diagram
- traceroute, tracert, visualroute, McAfee's NeoTrace, Foundstone's Trout, Owasp AMASS
  - Find the exact path (IP nodes – routers, firewall, etc.)
  - Leverage TTL and ICMP
- Thwarting Network Reconnaissance Countermeasures
  - Intrusion detection: snort, bro
  - Configure border routers to limit ICMP and UDP traffic to specific systems

Step 6: Network Reconnaissance

```
[bash]$ traceroute example.com
traceroute to example.com (192.168.1.7), 30 hops max, 38 byte
packets
1 (10.1.1.1) 4.264 ms 4.245 ms 4.226 ms
2 (10.2.1.1) 9.155 ms 9.181 ms 9.180 ms
3 (192.168.10.90) 9.224 ms 9.183 ms 9.145 ms
4 (192.168.10.33) 9.660 ms 9.771 ms 9.737 ms
5 (192.168.10.217) 12.654 ms 10.145 ms 9.945 ms
6 (192.168.11.173) 10.235 ms 9.968 ms 10.024 ms
7 (192.168.12.97) 133.128 ms 77.520 ms 218. 464 ms
8 (192.168.13.78) 65.065 ms 65.189 ms 65.168 ms
9 (192.168.14.252) 64.998 ms 65.021 ms 65.301 ms
10 (192.168.100.130) 82.511 ms 66.022 ms 66.170
11 www.example.com (192.168.1.7 82.355 ms 81.644 ms 84. 238 ms
```

Summary

- Footprinting: tedious works to be done regularly
- Automate tasks by shell, Python, Perl scripts
- Minimize info leaks
- Implement monitoring

Homework #1

1. (20 points) Select a web site.
   1) Use “Wget” or “Teleport Pro” to mirror the site. Look for comments within comment tags. Give screen dumps and explain what you found.
   2) Use “DirBuster” with a proxy feature through “privoxy” to enumerate hidden files and directories. Screen dump and explain the hidden files and directories you found.
2. (20 points) Lookup “How I met your girlfriend” in the BlackHat 2010 demo to explain, in 0.5 page, how this was done.
3. (20 points) Select a person. Use on-line sites for phone book, social network, information, job, photo management, business directory, jigsaw.com, etc. to summarize, with screen dumps and explanations, what information you can get. If your target is not in US nor native English speaker, you might need to use on-line sites different from the textbook.
4. (20 points) Google “XYZ resume firewall” and “XYZ resume intrusion detection” where “XYZ” is the name of your target company. Screen dump “useful” results and explain what you got.
5. (20 points) Lookup Archive.org and Google cached results, and select a target web site. Compare the differences between an archived and cached copy with its current on-line web site. Give screen dump and explain the differences.
6. (20 points) Find Google Hacking Database at hackersforcharity.org/ghdb/. Summarize what it has and select 3 strings to search. Screen dump and explain what you got.
7. (20 points) Select a web site. Start from whois.iana.org to find its registry, registrar, and registrant. Also select an IP address. Start from arin.net to find who owns the IP address. Show your screen dump and explain.
8. (20 points) Select a domain name. Use nslookup to dump its DNS records. Show your screen dump and explain.
9. (20 points) Select a domain name. Use traceroute or similar tools to find the access path to that domain. Show your screen dump and explain.
10. (bonus: 40 points) Follow the case study right before chapter 1. Select one target and run through all tools (Tor, Vidalia, Privoxy, tor-resolve, proxychains, Nmap, socat, nc). Screen dump the process and explain what you got in your screen.