

Hacking Exposed 7

Network Security Secrets & Solutions

Book - Table of Contents

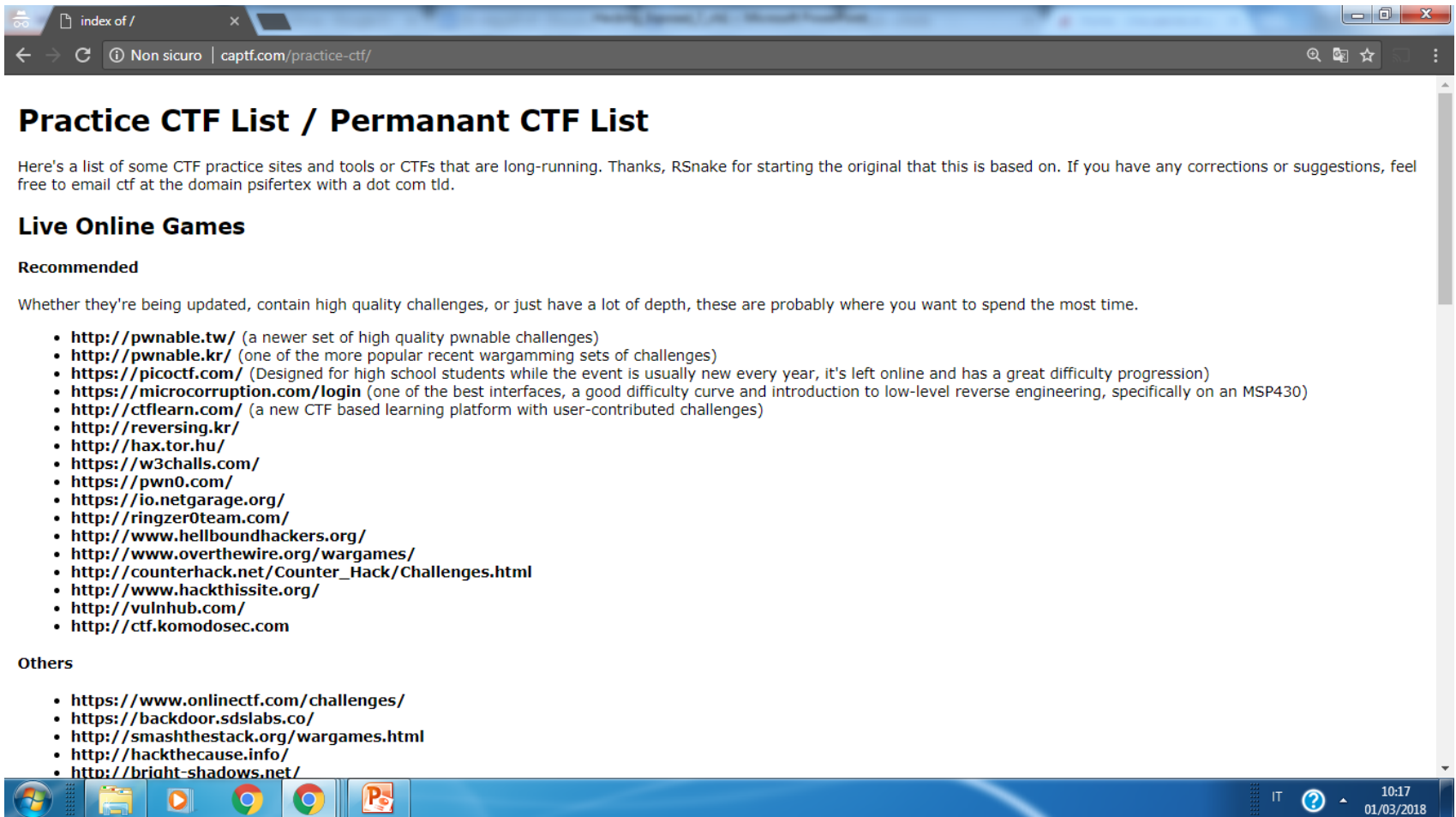
- **Part I Casing the Establishment**
 - Footprinting
 - Scanning
 - Enumeration
- **Part II Endpoint and Server Hacking**
 - Hacking Windows
 - Hacking UNIX
 - Cybercrime and Advanced Persistent Threats
- **Part III Infrastructure Hacking**
 - Remote Connectivity and VoIP Hacking
 - Wireless Hacking
 - Hacking Hardware
- **Part IV Application and Data Hacking**
 - Web and Database Hacking
 - 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)

Hacking-Labs



index of / x

Non sicuro | captf.com/practice-ctf/

Practice CTF List / Permanent CTF List

Here's a list of some CTF practice sites and tools or CTFs that are long-running. Thanks, RSnake for starting the original that this is based on. If you have any corrections or suggestions, feel free to email ctf at the domain psifertex with a dot com tld.

Live Online Games

Recommended

Whether they're being updated, contain high quality challenges, or just have a lot of depth, these are probably where you want to spend the most time.

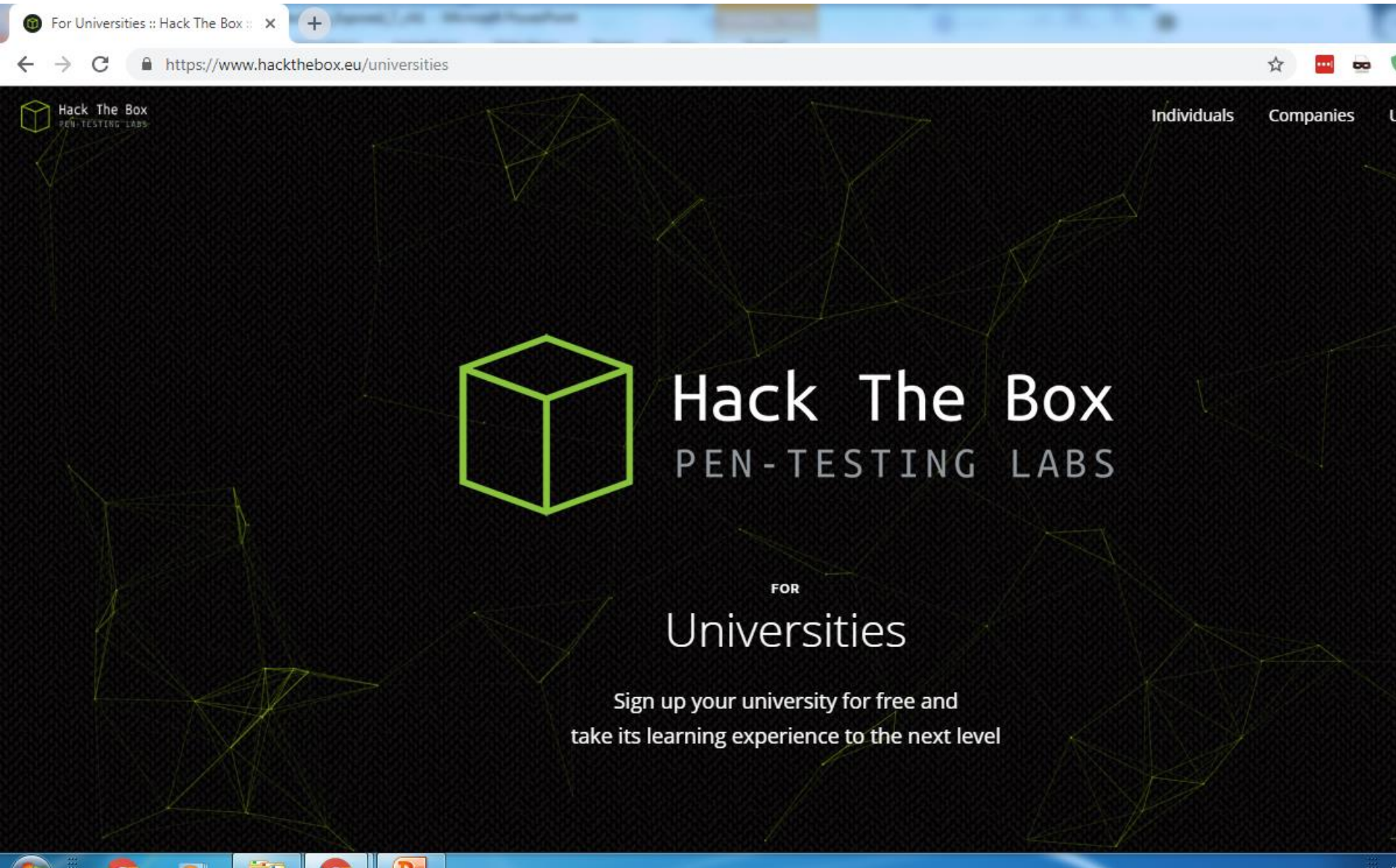
- <http://pwnable.tw/> (a newer set of high quality pwnable challenges)
- <http://pwnable.kr/> (one of the more popular recent wargaming sets of challenges)
- <https://picoctf.com/> (Designed for high school students while the event is usually new every year, it's left online and has a great difficulty progression)
- <https://microcorruption.com/login> (one of the best interfaces, a good difficulty curve and introduction to low-level reverse engineering, specifically on an MSP430)
- <http://ctflearn.com/> (a new CTF based learning platform with user-contributed challenges)
- <http://reversing.kr/>
- <http://hax.tor.hu/>
- <https://w3challs.com/>
- <https://pwn0.com/>
- <https://io.netgarage.org/>
- <http://ringzer0team.com/>
- <http://www.hellboundhackers.org/>
- <http://www.overthewire.org/wargames/>
- http://counterhack.net/Counter_Hack/Challenges.html
- <http://www.hackthissite.org/>
- <http://vulnhub.com/>
- <http://ctf.komodosec.com>

Others

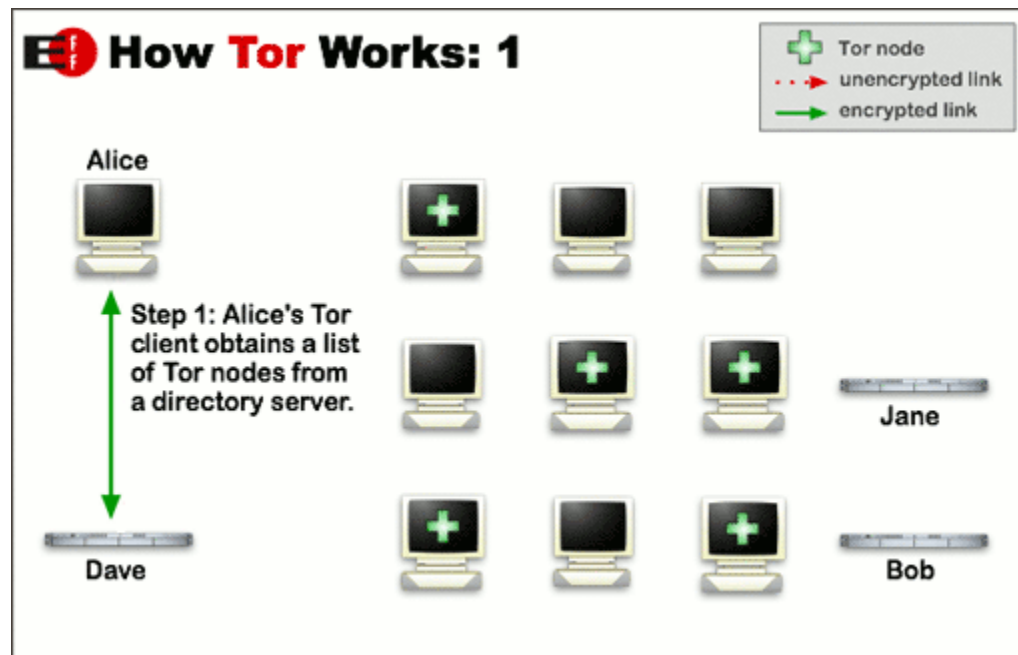
- <https://www.onlinectf.com/challenges/>
- <https://backdoor.sdslabs.co/>
- <http://smashthestack.org/wargames.html>
- <http://hackthecause.info/>
- <http://bright-shadows.net/>

IT ? 10:17 01/03/2018

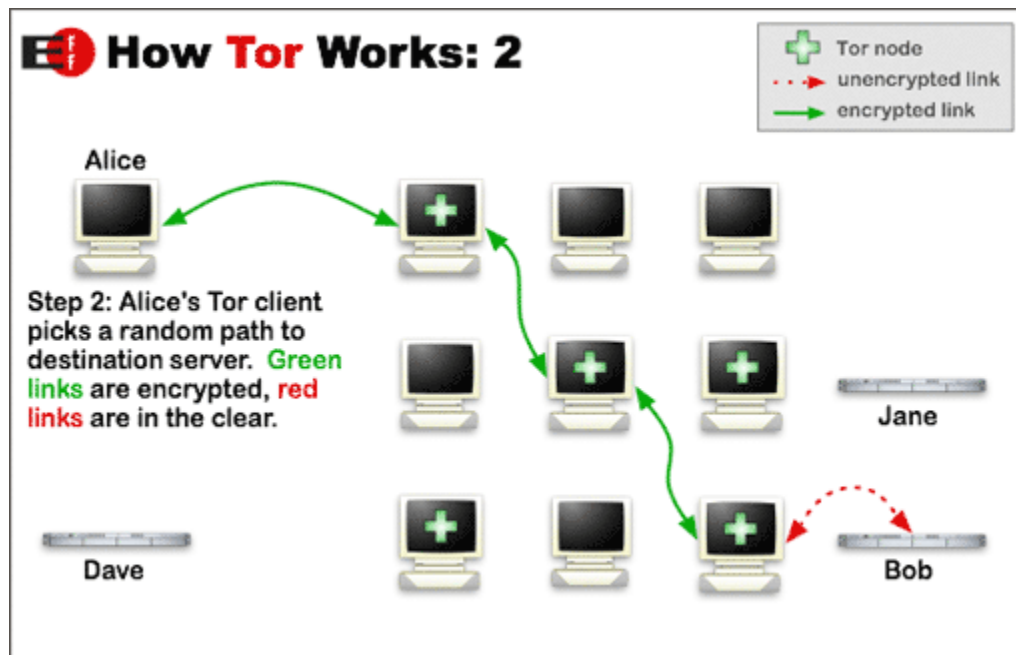
Hack The Box



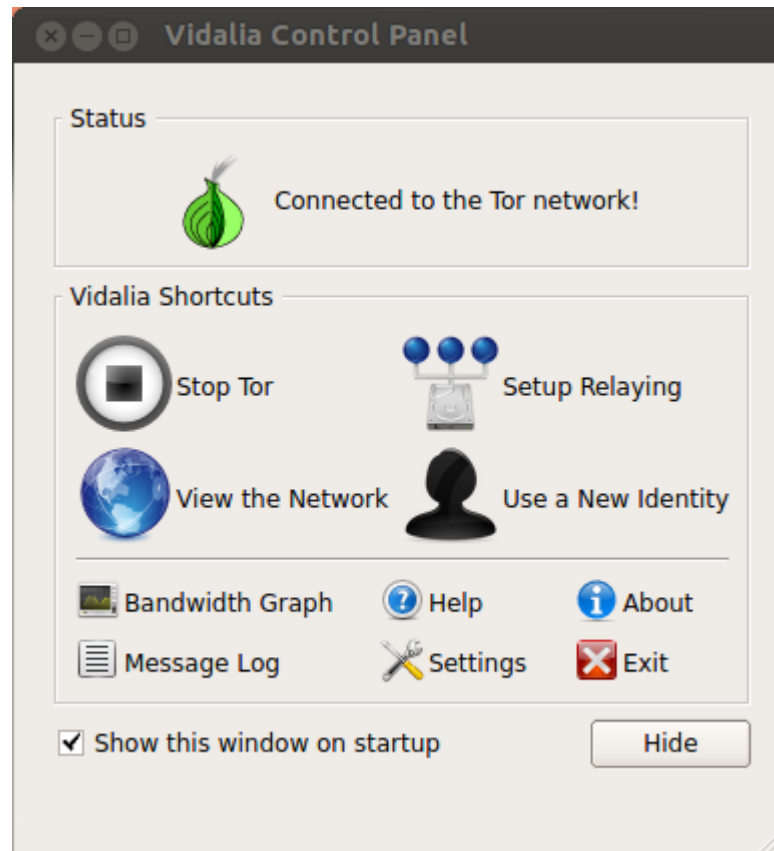
The Onion Router (TOR) - Overview



TOR



Vidalia

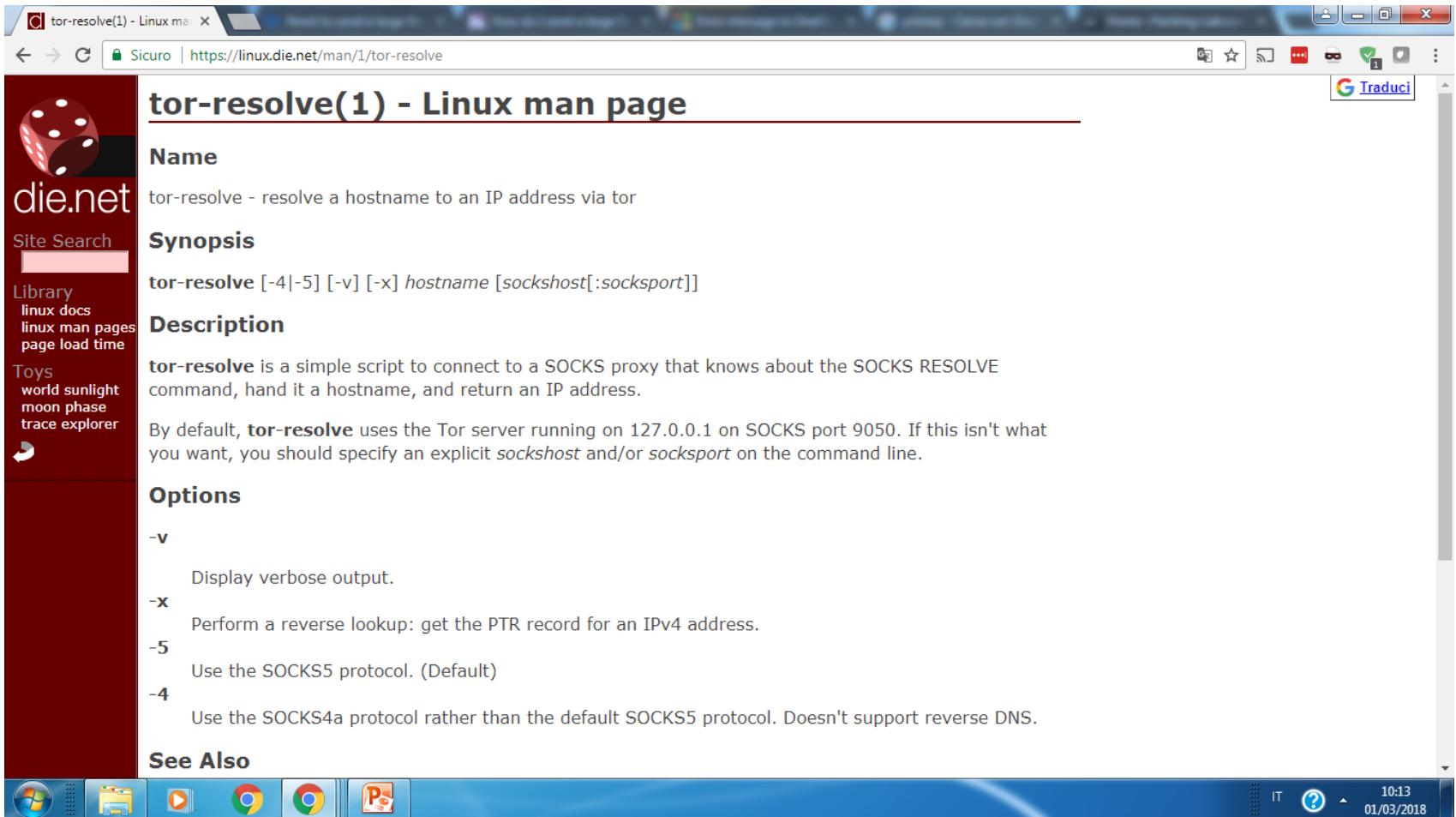


Vidalia is a discontinued cross-platform GUI for controlling Tor. It allows the user to start, stop or view the status of Tor

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

die.net
Site Search
Library
linux docs
linux man pages
page load time
Toys
world sunlight
moon phase
trace explorer

10:13 01/03/2018

Proxychains

The screenshot shows a web browser window with the address bar displaying "Sicuro | https://www.cybrary.it/0p3n/tor-proxychains-tip-hacking-anonymous/". The website header includes the "CYBRARY" logo and navigation links: "COURSES", "0P3N", "APPS", "ALLIANCES", "EXPLORE", and "BUSINESS". In the top right corner, there are links for "Log in" and "REGISTER". The main content area features a video player with a dark background and a binary code pattern. The video title is "Tor and Proxychains – Tip for Hacking Anonymous". Below the title, the author's name "ryanshady" is displayed, along with the upload date "December 30, 2016" and the view count "Views: 13229". At the bottom of the video player, there are two buttons: "Save" and "Email". The Windows taskbar is visible at the bottom of the screen, showing various application icons and the system clock indicating "10:24 01/03/2018".

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 Hacking Series for O'Reilly Publishing

COURSE

O'REILLY

Server Manager • Dashboard

WELCOME TO SERVER MANAGER

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

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 →

10:31 01/03/2018

NMAP

Nmap Cheat Sheet | Hackertarget.com

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

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

Nmap Port Selection

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

socat

- This command opens a proxy listening on localhost:8080 and forwards all requests through Tor to the target 10.10.10.100:80

```
bt ~ # socat TCP4-LISTEN:8080,fork  
SOCKS4a:127.0.0.1:10.10.10.100:80,socksport=9050 4
```

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

The screenshot shows the Shodan website in a web browser window. The browser's address bar displays "https://www.shodan.io". The website's header includes the Shodan logo, a search bar, and navigation links: "Explore", "Enterprise Access", and "Contact Us". A green button labeled "Login or Register" is on the right. The main content area features a large banner with the text "The search engine for" and "Shodan is the world's first search engine for Internet-connected devices." Below this are two buttons: "Create a Free Account" and "Getting Started". The background of the banner shows a wireframe globe with red location markers and IP addresses like "67.20.69.105", "50.87.75.184", and "104.18.67.231". Below the banner are four feature sections, each with an icon and a description:

- Explore the Internet of Things** (Cloud icon): Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
- Monitor Network Security** (Eye icon): Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
- See the Big Picture** (Globe icon): Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
- Get a Competitive Advantage** (Dollar sign icon): Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

The bottom of the image shows a Windows taskbar with various application icons and a system clock displaying "12:52 07/03/2018".

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](#), [Myspace.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](#)
 - Used by sales teams
 - Paid-for services with incentive award points to new or update entries

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

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](https://archive.org) & cached results at Google

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 \(GHDB\)](http://GoogleHackingDatabase(GHDB)athackersforcharity.org/ghdb/) at hackersforcharity.org/ghdb/
- Search Google's cache for vulnerabilities, errors, configuration issues, etc. – [Athena \(snakeoillabs.com\)](http://Athena(snakeoillabs.com)), [SiteDigger \(foundstone.com\)](http://SiteDigger(foundstone.com)), [Wikto \(sensepost.com/research/wikto\)](http://Wikto(sensepost.com/research/wikto))
- Analyze metadata in web files for info leaks – [FOCA \(informatica64.com/foca.aspx\)](http://FOCA(informatica64.com/foca.aspx))
- Mining and linking relevant pieces of info on a subject – [Maltego \(paterva.com\)](http://Maltego(paterva.com))
- Public Database Security Countermeasures:
 - Site Security Handbook: RFC 2196
 - Periodically review and remove public but sensitive data!

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 [Email](#) [Facebook](#) [Twitter](#) [Pinterest](#)

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 to Cart](#)

[Turn on 1-Click](#)

More Buying Choices

24 New from \$52.43 | 16 Used from \$48.30

40 used & n

[See All Buy](#)

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

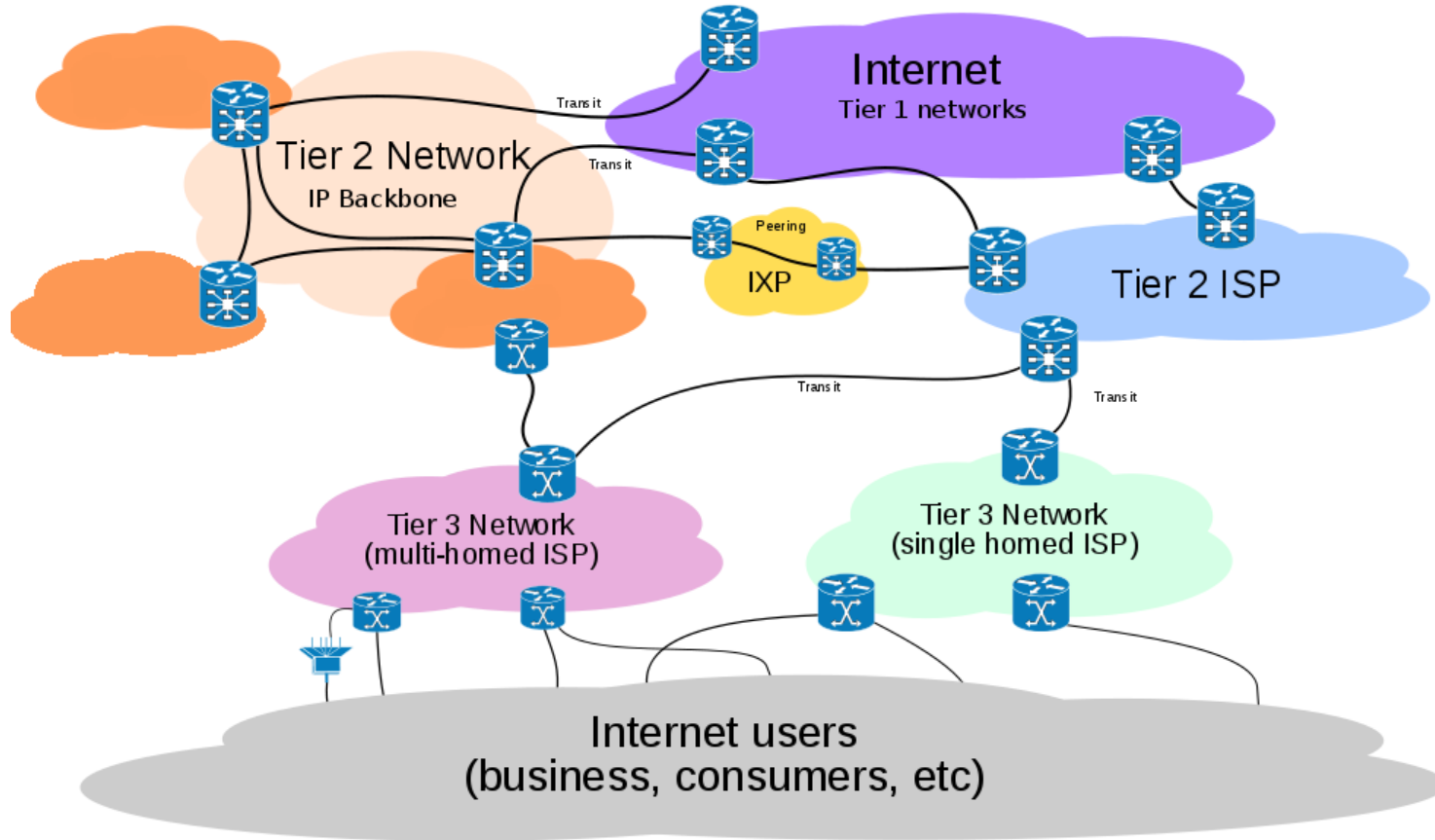
allinurl:tsweb/default.htm

- 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





 Your IPv4 address is 78.13.211.54

SEARCH Wh
all requests subj

NUMBER RESOURCES

PARTICIPATE

POLICIES

FEES & INVOICES

KNOWLEDGE


ABOUT

ARIN ONLINE

Username and password are
case sensitive.

username: new user?

password: assistance

log in 

[About ARIN Online](#)



Announcements



Friday, 2 March 2018
IANA Issues /21 to ARIN, 7
Waiting List Requests
Fulfilled

Tue, 27 Feb 2018
Extension of ACSP
Consultation: ASO Review
Consultation 2018

Mon, 26 Feb 2018
2018 ARIN Leadership

[Announcement Archives](#)



ARIN is a member of the
Number Resource
Organization.

09 Feb 2018
NRO EC and ASO AC Joint
Response to the 2017
Independent ASO Review
Recommendations

25 Jan 2018
ASO Review Consultation
2018

[NRO Archives](#)

Highlights

[Request Resources](#)

[Waiting List for Unmet
Requests](#)

[Draft Policies & Proposals](#)

[Internet Governance](#)

[Resource Revocation,
Returns, and Reinstatement](#)



REGISTRATION OPEN



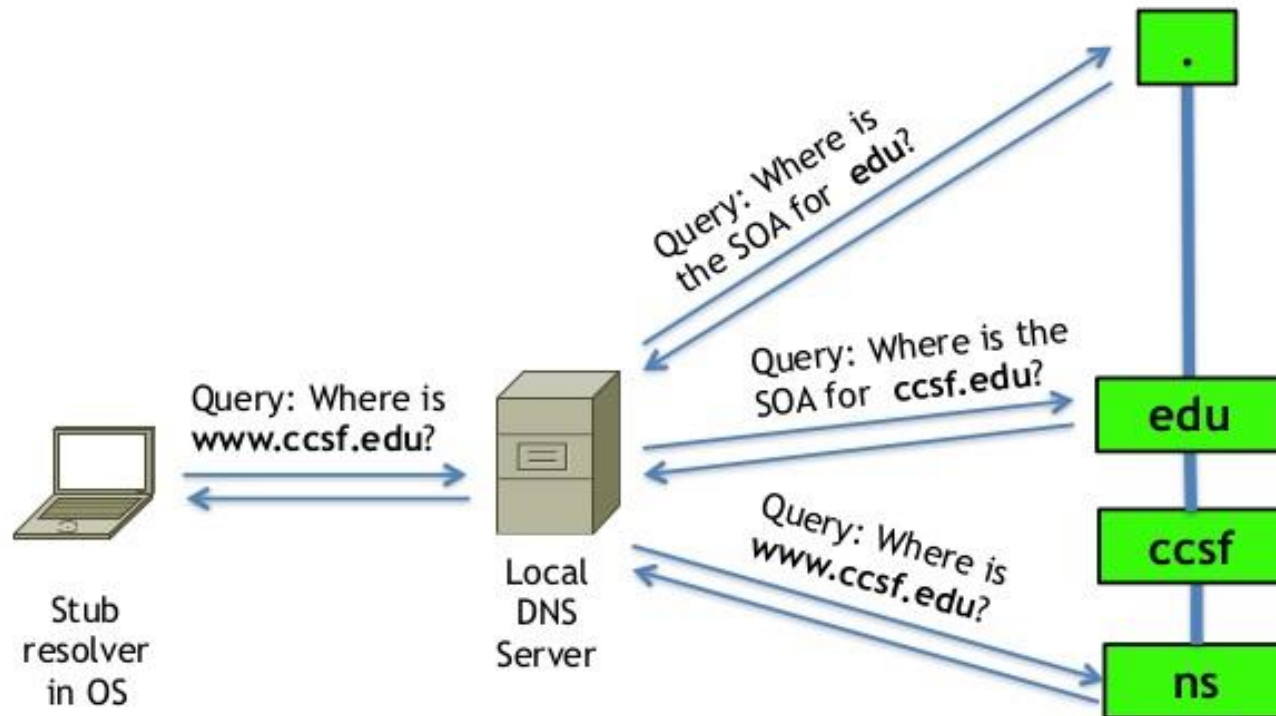
Public Database Security Countermeasures

Administrative contacts, registered net blocks authoritative name servers

- Keep administrative contacts up-to-date
- *Anonymize* administrative contacts
- *Authenticate* updates rigidly to avoid *domain hijacking*
 - AOL in 1998: redirected traffic

DNS - Start Of Authority (SOA) record

Typical Name Resolution Scenario



DNS record types

DS	43	RFC 4034	DNSSEC 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**

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
 - 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

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.