



PREPARING A NETWORK ATTACK: “FOOTPRINTING”

Corso di Laurea Magistrale in Ingegneria Informatica

Prof. Simon Pietro Romano

spromano@unina.it



HOW TO PREPARE A NETWORK ATTACK?

- Vital concepts for anyone looking to prepare, with knowledge, for launching an attack on a computer network:
 - Footprinting:
 - The art of gathering information on the network
 - Often referred to as "network reconnaissance"
 - Scanning:
 - a thorough inspection of the attack perimeter, looking for potential entry points
 - Enumeration:
 - probing the identified services to discover potential vulnerabilities

FOOTPRINTING

- Gathering information useful for creating a detailed profile (footprint) of an organization's security features involves:
 - determining the organization's presence on the internet
 - identifying remote access points to the organization's network
 - understanding the configuration of the organization's intranet/extranet
 - exploring business partners and their relationships with the organization
- When conducted systematically, footprinting activities allow for the structured collection of information, providing a comprehensive overview of a potential attack target's network profile

FOOTPRINTING: INTERNET/INTRANET

- Data of interest for footprinting include:
 - Domain names
 - Address blocks and subnets
 - IP addresses of systems accessible via the internet
 - TCP and UDP services running on identified systems
 - System architecture
 - Access control mechanisms (and lists)
 - Presence of Intrusion Detection Systems (IDS)
 - Usernames and/or user groups, system banners, routing tables
 - Management information (SNMP)
 - Hostnames



FOOTPRINTING: EXTRANET

- Data of interest:
 - Domain names
 - Source and destination of each connection
 - Types of connections
 - Access control mechanisms in use



FOOTPRINTING: REMOTE ACCESS

- Data of interest:
 - Phone numbers (analog and digital)
 - Type of remote system
 - Authentication mechanisms
 - Presence of Virtual Private Networks (VPN) and related protocols



FOOTPRINTING: CONSIDERATIONS

- One of the most complex activities in determining the security profile of an organization
- One of the most boring tasks for anyone eager to engage in hacking techniques
- The fundamental step for the subsequent development of an effective protection plan for the studied organization
- As always, footprinting is:
 - useful for potential attackers...
 - ...crucial for the security officers of any organization present on the network



FOOTPRINTING IN THE INTERNET

1. Publicly available information
2. WHOIS and DNS enumeration
3. DNS interrogation
4. Network Reconnaissance



1. PUBLIC INFORMATION

- a. Organization's web pages
- b. Related organizations
- c. Location details
- d. Employee information
- e. Current events involving the organization
- f. Privacy and security policies/mechanisms
- g. Archived information
- h. Search engines and data relationships related to the organization
- i. Other useful information...



1.a ORGANIZATION'S WEB SITE

- Many useful (and often sensitive) pieces of information are publicly available on organization websites:
 - details about security configurations
 - complete inventories of the organization's assets ...
- A thorough analysis of HTML code can reveal many surprises:
 - information contained within comments:
 - <!-- Sensitive data contained in a comment... -->
- Many websites often act as proxies to internal organization services:
 - webmail, access to Microsoft Exchange servers, remote access to mainframes (e.g., WebConnect), access to the corporate VPN, etc.



OFF-LINE WEB SITE ANALYSIS

- For a more thorough analysis of an organization's web resources, the following techniques are often used:
 1. Locally downloading a clone of the website for analysis:
 - Using tools like "Wget" (<http://www.gnu.org/software/wget/>)
 2. Searching for "hidden" information within the local clone of the website:
 - Hidden files and directories
 - This can be automated using brute force approaches
 - Recursively searching within the website for hidden directories and files, with a focus on extensions deemed more interesting (e.g., ".php," ".jsp," ".cgi," ".asp," etc.)



DirBuster: an example of the “Brute Force” technique

The screenshot shows two windows of the OWASP DirBuster tool. The left window is the configuration interface, and the right window is the results viewer.

Configuration Window (Left):

- Target URL: `http://www.pippozzo.com`
- Work Method: Auto Switch (HEAD and GET)
- Number Of Threads: 10 Threads
- Select scanning type: Pure Brute Force
- Char set: azA-Z0-9%20-_
- Min length: 1
- Max Length: 8
- Select starting options:
 - Standard start point (radio button selected)
 - URL Fuzz
 - Brute Force Dirs (checkbox checked)
 - Be Recursive (checkbox checked)
 - Brute Force Files (checkbox checked)
 - Use Blank Extension (checkbox unchecked)
- Dir to start with: /
- File extension: php
- URL to fuzz: `/test.html?url=(dir).asp`
- Buttons: Start, Stop, Exit

Results Window (Right):

- Header: OWASP DirBuster 1.0-RC1 – Web Application Brute Forcing
- Sub-header: Results - List View: Dirs: 0 Files: 143 Results - Tree View | Errors: 0 \
- Table: Directory Structure
| | Response Code | Response Size |
| --- | --- | --- |
| /ND.php | 200 | 85227 |
| └ aR | 200 | 67923 |
| └ bG | 200 | 446 |
| └ cA | 200 | 446 |
| └ cS | 200 | 446 |
| └ dA | 200 | 446 |
| └ dE | 200 | 446 |
| └ aiuto | 302 | 270 |
| └ da | 301 | 446 |
| └ de | 301 | 446 |
| └ dA | 301 | 446 |
| └ dE | 301 | 446 |
| └ h | 200 | 278 |
| └ ch | 302 | 289 |

Context menu for the 'h' directory entry:

 - Open in Browser
 - View Response

Bottom status bar:

 - Current speed: 0
 - Average speed: 0
 - Parse Queue Size: 0
 - Total Requests: 5512/647247276184365
 - Time To Finish: ~
 - Current number of running threads: 10
 - Buttons: Back, Pause, Stop, Change, Report



1.b RELATED ORGANIZATIONS

- References or links to organizations connected in various ways to the target organization:
 - for example, many companies outsource their websites, both for the design phase and for development and graphic consulting
- Information about partner organizations often leaks from the analysis of the target organization's website
 - e.g., comments on web pages containing the author(s) and affiliation of the code and/or graphics portion
 - JavaScript libraries, style sheets, etc.



1.c DETAILS ABOUT THE LOCATION

- The physical address of an organization can be very useful for launching 'non-technical' attacks:
 - Dumpster diving:
 - Yes, looking for 'information treasures' in the trash!
 - Surveillance
 - Social engineering

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using [social engineering](#) techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.



1.d Information about employees

- Contact names, phone numbers, email addresses...
 - from an email address it is often easy to trace a username
 - a valid domain user name is essential to move on to the next phases of the attack and gain access to the target system's resources
- Websites to use to gather information about an organization's employees:
 - social sites:
 - facebook, myspace, reunion, classmates, X, instagram, tik tok, etc.
 - professional sites:
 - linkedin, plaxo, monster, careerbuilder, etc.
 - paid contact sites for use in marketing and sales campaigns

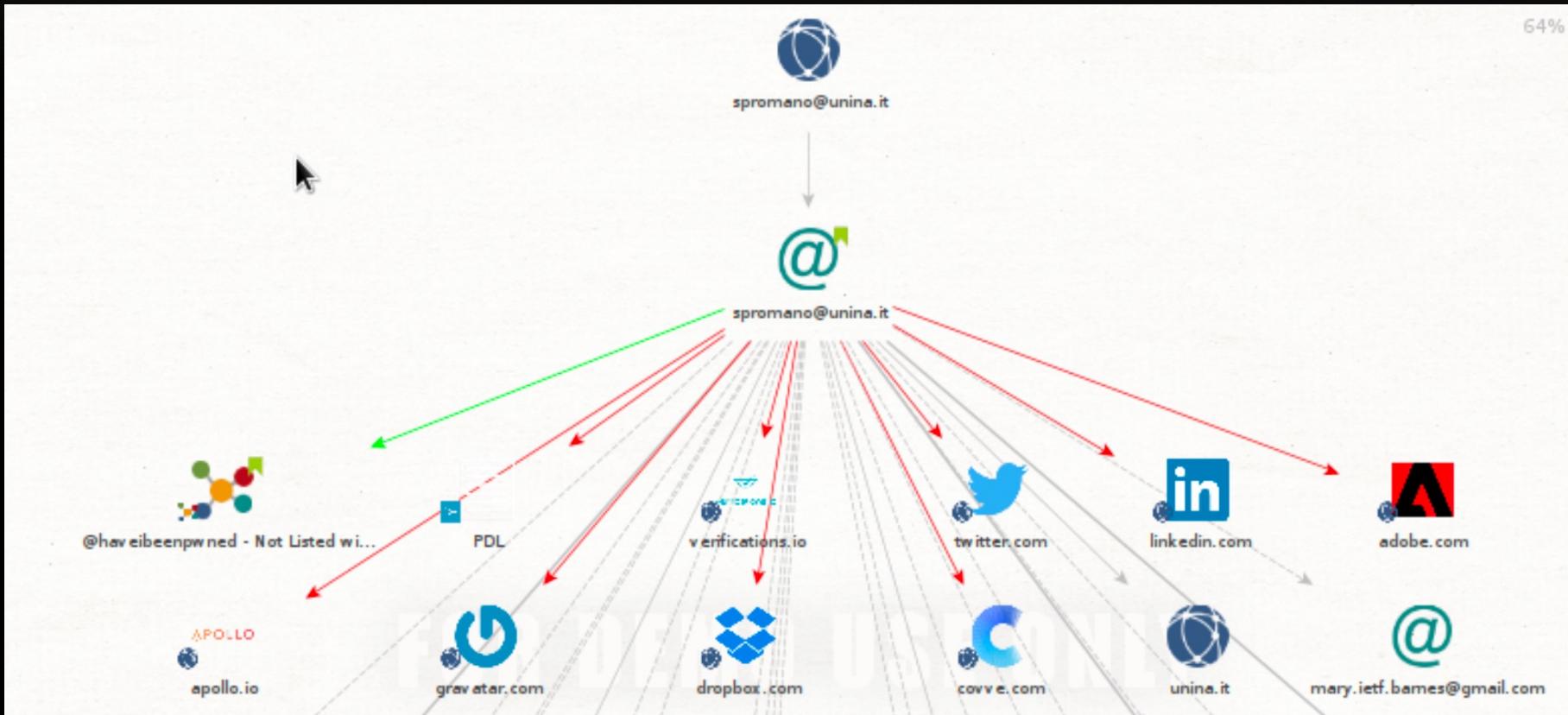


HOW TO USE ALL THIS DATA?

- Many data mining tools can be used to correlate the vast amount of collected information effectively
- One example is Maltego
 - a powerful social engineering tool
 - capable of
 - extracting information at various levels
 - processing ("transforming") the gathered information
 - correlating data
 - representing the result of these processes as a "social graph"



MALTEGO IN ACTION





1.e Events involving the organization

- Information on:
 - corporate mergers, acquisitions, scandals, bankruptcies, outsourcing activities, extensive use of temporary labor contracts, etc.
 - all useful indicators of the 'health' status and management practices of an organization
- If the organization is a public company, a lot of information is available online:
 - transparency requirement



1.f PRIVACY AND SECURITY MECHANISMS

- Any type of information that provides useful details about the security policies adopted by the target organization
- Technical details regarding the hardware and software infrastructure that the organization has implemented for security purposes



1.g ARCHIVED INFORMATION

- Use of websites that allow you to retrieve obsolete copies of information no longer available from the original source
- Possibility of accessing information (including sensitive data) intentionally removed by the target organization for security reasons.
- An example of this:
 - WayBack Machine (www.archive.org)

The screenshot shows the Wayback Machine homepage. At the top, it says "INTERNET ARCHIVE" and "WaybackMachine" with a search bar and a "BROWSE HISTORY" button. Below that, it displays "438 billion web pages saved over time." and a "DONATE" button. A row of thumbnail images shows various captured web pages. At the bottom, there are three sections: "Tools" (with links to "Wayback Machine Availability API", "Build your own tools.", "WordPress Broken Link Checker", "Banish broken links from your blog.", "404 Handler for Webmasters", and "Help users get where they were going."), "Subscription Service" (describing Archive-It and linking to its website), and "Save Page Now" (with a form to enter a URL and a "SAVE PAGE" button).



1.h SEARCH ENGINES AND DATA RELATIONSHIPS

- Search engines are now among the primary tools of hackers
- e.g.,: "allinurl:tsweb/default.htm"
 - reveals Microsoft servers that expose a web-accessible remote desktop service...
 - ...potentially vulnerable to remote-to-local attacks through RDP (Remote Desktop Protocol) exploits Protocol)

Google search results for "allinurl:tsweb/default.htm":

- Service Honda**
www.servicehonda.com/TSWeb/default.htm ▾ Traduci questa pagina
1600 then resWidth = 800 end if Response.Write resWidth %> HEIGHT=<% resHeight = Request.QueryString("rH") if resHeight < 200 or resHeight > 1200 then ...
- Terminal Server**
wwwpclnx.it/tsweb/default.htm ▾
1600 then resWidth = 800 end if Response.Write resWidth %> HEIGHT=<% resHeight = Request.QueryString("rH") if resHeight < 200 or resHeight > 1200 then ...
- Remote Desktop Web Connection**
www.enr.psu.edu/ae/...TSWeb/default.htm ▾ Traduci questa pagina
VPN to COE is required to establish a connection. More info here. Not sure what to put in for the AE Computer Name? Find one here. You MUST use Internet ...
- Remote Desktop Web Connection**
<https://www.ee.washington.edu/.../tsweb/default.htm> ▾ Traduci questa pagina
Server: Admin, Bose, Bufla, Copyserv, Exchange, Mir, Pcserv1, Pcserv2, Windows, Wins, Wisetrack. Resolution: Full-screen, 640 by 480, 800 by 600, 1024 by ...
- Connessione Web desktop remoto - Data Service**
www.dataservice.be/inetpub/wwwroot/tsweb/default.htm ▾
1600 then resWidth = 800 end if Response.Write resWidth %> HEIGHT=<% resHeight = Request.QueryString("rH") if resHeight < 200 or resHeight > 1200 then ...



GOOGLE HACKING DATABASE

The screenshot shows a web browser window with the URL <https://www.offensive-security.com/community-projects/google-hacking-database/>. The page is titled "Google Hacking Database (GHDB)" and features the "OFFENSIVE® SECURITY" logo. A search bar contains the query "inurl: * all t". Below the search bar are two buttons: "Google Search" and "I'm Feeling Lucky".

What is the Google Hacking Database?

Originally created by Johnny Long of Hackers for Charity®, The **Google Hacking Database (GHDB)** is an authoritative source for querying the ever-widening reach of the Google search engine. In the GHDB, you will find search terms for files containing usernames, vulnerable servers, and even files containing passwords.

GHDB : hosted and maintained by Offensive Security

When The *Google Hacking Database* was integrated in The *Exploit Database*, the various googledorks contained in the thousands of exploit entries were entered into the GHDB. The direct mapping allows penetration testers to more rapidly determine if a particular web application has a publicly available exploit.

Feeling Lucky?

Give the GHDB a try for yourself. You can also contribute your own googledorks! Just be sure to search before submitting.

Any Category Free text search



SHODAN

- “Sentient Hyper-Optimized Data Access Network”
- Often referred to as "Google for Hackers"
- Designed to discover systems (computers, routers, webcams, refrigerators, "things") on the network
- Focus on identifying potential vulnerabilities in authentication and authorization mechanisms

The screenshot shows the Shodan search engine interface. At the top, it displays the URL <https://www.shodan.io>. Below the address bar is a navigation menu with links for "Search", "Dashboard", "Developers", and "View API". The main header features the Shodan logo and the tagline "The search engine for the Internet of Things". A large globe graphic shows a network of connections, with a yellow dot labeled "SHANGHAI". Below the header are two calls-to-action: "Create a Free Account" and "Getting Started". The central area contains four promotional cards: "Explore the Internet of Things" (using Shodan to find connected devices), "Monitor Network Security" (tracking accessible computers), "See the Big Picture" (discovering websites and other internet components), and "Get a Competitive Advantage" (using Shodan for market intelligence). A row of logos from various media outlets follows: CNNMoney, Dagbladet, The Washington Post, BBC News, WIRED, and CIO. The bottom section is titled "Analyze the Internet in Seconds" and includes a "Sample Report" button and a world map where countries are colored red or white.



SHODAN: A SAMPLE SEARCH

Shodan Scanhub Developers View All...

SHODAN asterisk+pbx

Exploits Maps Download Results [Create Report](#)

TOP COUNTRIES

Country	Count
United States	12,539
Russian Federation	2,966
Brazil	2,267
Germany	1,829
United Kingdom	1,813

TOP SERVICES

Service	Count
SIP	41,700
1024	32
65416	7
1026	5
1025	3

TOP ORGANIZATIONS

Organization	Count
Fastweb	740
Comcast Cable	705
OVH SAS	703
Comcast Business Communications	675
Verizon FIOS	218

TOP PRODUCTS

Product	Count
Asterisk PBX	16,532
Asterisk	10,298
Digium Switchvox PBX	1,530
Asterisk PBX 1.8.1.11	1,070
Asterisk PBX 1.8.32.3	258

50.73.47.53 mail.coop7.com

Comcast Business Communications

Address: 2015-09-24 16:47:23 GMT

122.111.243.53 d122-111-243-53.per01.wc.optusnet.com.au

Optus

Address: 2015-09-24 16:47:13 GMT

220.95.208.120 Korea Telecom

Address: 2015-09-24 16:47:05 GMT

181.63.251.65 181.63.251.65

Telmex Colombia S.A.

Address: 2015-09-24 16:47:48 GMT

50.73.47.53 mail.coop7.com

Comcast Business Communications

Address: 2015-09-24 16:47:23 GMT

122.111.243.53 d122-111-243-53.per01.wc.optusnet.com.au

Optus

Address: 2015-09-24 16:47:13 GMT

220.95.208.120 Korea Telecom

Address: 2015-09-24 16:47:05 GMT

Shodan Scanhub Developers View All...

181.63.251.65 Static-IP-cr1816325165.cable.net.co

Country: Colombia
Organization: Telmex Colombia S.A.
ISP: Telmex Colombia S.A.
Last Update: 2015-09-24T16:47:46.193648
Hostnames: Static-IP-cr1816325165.cable.net.co

Ports

- 22
- 23
- 53
- 80
- 1723
- 5060

Services

- 22** ssh

SSH-2.0-OpenSSH_5.5p1

Key type: ssh-dss

Key: AAAAB3NzaC1kc3MAAACBAPKE+BE+IuxMASifdvaEp3K2B0yEfpoqas5nbyZcLzTzvq910@twdBktkj1187B8EGehgDk2kQunMPkbvTev8BYTy0AJhjPNfTz1eC0yyfjSaodYjMop7whF9xE90laV75j1yR983J3c75PjXEm9Wf/ys3vHybw03ebqg3AAAFQCaNxRK65pJnplq7Kssw7uj11mWAIA1AVWg1gbRYIPb0l0X+k10hC5y1WfYbb0ExsGtojdomsR4K+wJ1E8+h3DBjMh0NcuLoB29/GZD8v9Mgbj0jEfnpJpwqrxxuonBlD/1ScHABxyptQkEDAGTrfc08Ht/ndng2XHrcR8Mbvr5D07My7yG21zCRDPI6@QAAMhUgpt1Cwyg4FPH1bcdohtVtD07V/oPAhoyfb1kL5+mV1U2jgnSyr1y7h77OrTCBn8L1SP9m8dnAEI082412Nw61mxv11vcyTMFS1ukvdGE87

Fingerprint: 93:fc:f5:ec:27:f3:36:a2:d1:49:fc:02:be:f1:5d
- 23** telnet

MikroTik v5.18

Login:
- 53** dns-udp

Recursion: enabled
- 80** http

HTTP/1.1 200 OK

Connection: Keep-Alive

Content-Length: 6997

Content-Type: text/html

Expires: 0
- 1723** pptp

Firmware: 1

Hostname: MikroTik

Vendor: MikroTik



COUNTERMEASURES?

- RFC 2196: Site Security Handbook:
 - a guide for defining and implementing security policies and procedures for organizations that expose their systems on the Internet

Network Working Group
Request for Comments: 2196
FYI: 8
Obsoletes: 1244
Category: Informational

B. Fraser
Editor
SEI/CMU
September 1997

Site Security Handbook

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This handbook is a guide to developing computer security policies and procedures for sites that have systems on the Internet. The purpose of this handbook is to provide practical guidance to administrators trying to secure their information and services. The subjects covered include policy content and formation, a broad range of technical system and network security topics, and security incident response.



2. WHOIS AND DNS ENUMERATION

- ICANN: Internet Corporation for Assigned Names and Numbers
 - an organization responsible for technical coordination of the Internet
 - coordinates the assignment of the following identifiers:
 - Domain names
 - IP addresses
 - Protocol parameters and their port numbers
 - monitors the proper functioning and stability of DNS root name servers
 - has taken over responsibilities once held, under contract from the U.S. government, by the Internet Assigned Numbers Authority (IANA)



ICANN: STRUCTURE

- Some notable sub-organizations include:
 - ASO: Address Supporting Organization
 - Allocates IP address blocks to various Regional Internet Registries (RIRs)..
 - ...which, in turn, allocate addresses to ISPs, National Internet Registries (NIRs), or Local Internet Registries (LIRs)
 - GNSO: Generic Names Supporting Organization
 - Responsible for the names of "generic Top-Level Domains" (gTLDs):
 - .com, .net, .edu, .org, .info, etc.
 - CCNSO: Country Code Domain Name Supporting Organization
 - Responsible for the names of "country-code Top-Level Domains" (ccTLDs):
 - .it, .fr, .de, .jp, etc.



DOMAIN NAME RESEARCH

- The three R's of the WHOIS service:
 - Registry
 - contains information about the Registrar where the target entity registered its domain name
 - Registrar
 - contains details about the entity that registered the domain
 - Registrant
 - the entity that registered its domain name
- Remember that the DNS implements a hierarchical registration mechanism:
 - the ideal starting point for a search is the root of the tree:
 - ICANN (IANA)!



WHOIS.IANA.ORG

www.iana.org/whois?q=it

IANA WHOIS Service

The IANA WHOIS Service is provided using the WHOIS protocol on port 43. This web gateway will query this server and return the results. Accepted query arguments are domain names, IP addresses and AS numbers.

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain: IT

organisation: IIT - CNR
address: Via Moruzzi, 1
address: Pisa I-56124
address: Italy

contact: administrative
name: Domenico Laforenza
organisation: IIT - CNR
address: Via Moruzzi, 1
address: Pisa I-56124
address: Italy
phone: +39 050 315 2112
fax-no: +39 050 315 2113
e-mail: direttore@iit.cnr.it

contact: technical
name: Maurizio Martinelli
organisation: IIT - CNR
address: Via Moruzzi, 1
address: Pisa I-56124
address: Italy
phone: +39 050 315 2087
fax-no: +39 050 315 2207
e-mail: maurizio.martinelli@iit.cnr.it

nserver: A.DNS.IT.194.8.16.215.2001:67812:0:194:0:16:215
nserver: DNS.NIC.IT.192.12.192.5.2a00:d40:1:190:0:0:5
nserver: M.DNS.IT.2001:1ac0:0:200:0:asd1:6004:2.217.29.76.4
nserver: NAMESERVER.CNR.IT.194.119.192.34.2a00:1620:c0:220:194:119:192:34
nserver: R.DNS.IT.193.206.141.46.2001:760:ffff:ffff:0:0:0:ca
nserver: S.DNS.IT.194.146.106.30.2001:67c:1010:7:0:0:0:53

whois: whois.nic.it

status: ACTIVE
remarks: Registration information: http://www.nic.it/

created: 1987-12-23
changed: 2015-06-05
source: IANA
```



web-whois.nic.it/result

Domain	
Domain:	unina.it
Status:	ok
Created:	Jan 29, 1996 12:00:00 AM CET
Expire:	Jan 29, 2016 CET
Last Update:	Feb 14, 2015 10:46:57 AM CET

Registrant	
Organization:	CISED - Universita' di Napoli
Address:	C.so Umberto I 80138 - Napoli (NA) It
Nationality:	It
Phone:	+39.81676643
Fax:	+39.81676628
E-Mail:	contactcenter@unina.it
Created:	Mar 1, 2007 10:47:26 AM CET
Last Update:	Mar 24, 2011 11:01:07 AM CET

Admin Contact	
Name:	Francesco Palmieri
Address:	Universitat degli Studi di Napoli Federico II C.so Umberto I 80138 - Napoli (NA) It
Phone:	+39.81676643
Fax:	+39.81676628
E-Mail:	f.palmieri@unina.it
Created:	Mar 1, 2007 10:47:26 AM CET
Last Update:	Mar 24, 2011 11:01:08 AM CET

Technical Contacts	
Name:	Amerigo Izzo
Address:	Universitat degli Studi di Napoli Federico II C.so Umberto I 80138 - Napoli (NA) It
Phone:	+39.81676643
Fax:	+39.81676628
E-Mail:	izzo@unina.it
Created:	Jul 15, 1999 12:00:00 AM CET
Last Update:	Mar 24, 2011 11:01:09 AM CET
Name:	Francesco Palmieri
Address:	Universitat degli Studi di Napoli Federico II C.so Umberto I 80138 - Napoli (NA) It
Phone:	+39.81676643
Fax:	+39.81676628
E-Mail:	f.palmieri@unina.it
Created:	Mar 1, 2007 10:47:26 AM CET
Last Update:	Mar 24, 2011 11:01:08 AM CET

Registrar	
Organization:	Consortium GARR
Name:	GARR-REG
Web:	http://www.garr.it



WHOIS FOM THE COMMAND LINE

```
root@kali:~# whois it -h whois.iana.org
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:      IT

organisation: IIT - CNR
address:      Via Moruzzi, 1
address:      Pisa I-56124
address:      Italy

contact:     administrative
name:        Domenico Laforenza
organisation: IIT - CNR
address:      Via Moruzzi, 1
address:      Pisa I-56124
address:      Italy
phone:       +39 050 315 2112
fax-no:      +39 050 315 2113
e-mail:      direttore@iit.cnr.it

contact:     technical
name:        Maurizio Martinelli
organisation: IIT - CNR
address:      Via Moruzzi, 1
address:      Pisa I-56124
address:      Italy
phone:       +39 050 315 2087
fax-no:      +39 050 315 2207
e-mail:      maurizio.martinelli@iit.cnr.it

nserver:     A.DNS.IT 194.0.16.215 2001:678:12:0:194:0:16:215
nserver:     DNS.NIC.IT 192.12.192.5 2a00:d40:1:1:0:0:5
nserver:     M.DNS.IT 2001:1ac0:0:200:0:a5d1:6004:2 217.29.76.4
nserver:     NAMESERVER.CNR.IT 194.119.192.34 2a00:1620:c0:220:194:119:192:34
nserver:     R.DNS.IT 193.206.141.46 2001:760:ffff:ffff:0:0:0:ca
nserver:     S.DNS.IT 194.146.106.30 2001:67c:1010:7:0:0:0:53

whois:       whois.nic.it

status:      ACTIVE
remarks:    Registration information: http://www.nic.it/

created:    1987-12-23
changed:   2015-06-05
source:     IANA
```



```
root@kali:~# whois unina.it -h whois.nic.it
*****
* Please note that the following result could be a subgroup of
* the data contained in the database.
*
* Additional information can be visualized at:
* http://www.nic.it/cgi-bin/Whois/whois.cgi
****

Domain:      unina.it
Status:      ok
Created:    1996-01-29 00:00:00
Last Update: 2015-02-14 00:46:57
Expire Date: 2016-01-29

Registrant
Organization: CISED - Universita' di Napoli
Address:      C.so Umberto I
              Napoli
              80138
              NA
              IT
Created:    2007-03-01 10:47:26
Last Update: 2011-03-24 11:01:07

Admin Contact
Name:        Francesco Palomieri
Address:    Universita' degli Studi di Napoli Federico II
              C.so Umberto I
              Napoli
              80138
              NA
              IT
Created:    2007-03-01 10:47:26
Last Update: 2011-03-24 11:01:08

Technical Contacts
Name:        Amerigo Izzo
Address:    Universita' degli Studi di Napoli Federico II
              C.so Umberto I
              Napoli
              80138
              NA
              IT
Created:    1999-07-15 00:00:00
Last Update: 2011-03-24 11:01:09

Name:        Francesco Palomieri
Address:    Universita' degli Studi di Napoli Federico II
              C.so Umberto I
              Napoli
              80138
              NA
              IT
Created:    2007-03-01 10:47:26
Last Update: 2011-03-24 11:01:08

Registrar
Organization: Consortium GARR
Name:        GARR-REG
Web:         http://www.garr.it

Nameservers
```



IP ADDRESS SEARCHES

- IP addresses:
 - managed by Regional Internet Registries (RIRs)
 - a query directed to any RIR will provide us with:
 - the information we seek if the address in question is managed by that RIR...
 - ...information on the correct RIR to contact if it is not



IP ADDRESS SEARCHES

Network	
Net Range	143.224.0.0 - 143.225.255.255
CIDR	143.224.0.0/15
Name	RIPE-ERX-143-224-0-0
Handle	NET-143-224-0-0-1
Parent	NET143 (NET-143-0-0-0-0)
Net Type	Early Registrations, Transferred to RIPE NCC
Origin AS	
Organization	RIPE Network Coordination Centre (RIPE)
Registration Date	2003-11-12
Last Updated	2003-11-12
Comments	These addresses have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at https://www.ripe.net/whois
RESTful Link	https://whois.arin.net/rest/net/NET-143-224-0-0-1
See Also	Related organization's POC records.

ARIN

Search results

This is the RIPE Database search service. The objects are in RPSL format.
The RIPE Database is subject to [Terms and Conditions](#).

Note: this output has been filtered.

RIPE

Abuse contact info: cert@garr.it Update

inetnum: 143.225.0.0 – 143.225.255.255
netname: UNINA-NET
org: ORG-UDSD37-RIPE
descr: Universita' degli Studi di Napoli Federico II
country: IT
admin-c: MM29511-RIPE
tech-c: MM29511-RIPE
tech-c: CP8504-RIPE
status: LEGACY
remarks: For information on "status:" attribute read <https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources>
remarks: This prefix is statically assigned
remarks: To notify abuse mailto: cert@garr.it
remarks: Centro di servizi Didattico Scientifico
remarks: GARR – Italian academic and research network
mnt-irt: IRT-GARR-CERT
mnt-by: GARR-LIR
created: 1970-01-01T00:00:00Z
last-modified: 2015-05-05T02:18:00Z
source: RIPE # Filtered



CAN WE TRUST IP ADDRESSES?

- Those involved in security are well aware that relying on source IP addresses found in attack logs is almost always a futile idea!
- Serious attackers never leave such obvious traces of their movements and take care to "clean" the addresses they use to launch the attack:
 - *"laundered"* IP addresses...



COUNTERMEASURES?

- Some domain name providers offer (for a fee) private registrations:
 - they do not publish organization information such as the real address, phone number, email address, etc.
- Regarding domain registrations:
 - be cautious of providers that offer the possibility to modify the registration via email!
 - there is a risk of "domain hijacking" which involves modifying registration info and redirecting all traffic to the original domain
 - such services should only be offered in contexts where authentication mechanisms are reliable
 - the "FROM" field of an email is not!



3. DNS QUERIES

- Domain Name System (DNS)
 - a distributed service for translating symbolic names into IP addresses
- Insecurely configured DNS:
 - many pieces of information about an organization can leak and be exploited by an attacker
- Two main issues:
 - Zone Transfers
 - Analysis of MX (Mail eXchange) records



ZONE TRANSFERS

- A "zone transfer" occurs when:
 - a secondary master server updates its zone database from the database of a primary server
- Useful for redundancy purposes:
 - in case of a failure of the primary master server, a secondary server can immediately take its place
- Problem:
 - Zone transfers should only be allowed between primary and secondary servers...
 - ...in case of misconfigurations, a copy of the zone file may be made available to anyone who requests it!



ZONE TRANSFER AND INTERNAL DATA

- Allowing zone transfers to everyone can be problematic when an organization does not implement a "public/private" DNS policy:
 - Public DNS
 - visible to anyone on the internet
 - contains information about external-facing services
 - Private DNS
 - holds internal hostnames and IP addresses
 - is used just within the organization
- Providing an attacker with information from the internal DNS is like giving them a blueprint of the organization's structure!



ZONE TRANSFER: THE TOOLS

- "nslookup"
 - the most widely used DNS client
- "host" and "dig"
 - commonly used in Unix environments for DNS-related troubleshooting
- "dnsrecon"
 - a utility program for recursive zone file transfers



NSLOOKUP: AN EXAMPLE

```
[bash]$ nslookup
Default Server: ns1.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
```

```
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"
```



DNSRECON: AN EXAMPLE

```
[bash]$ python dnsrecon.py -x -d internaldomain.com
[*] Performing General Enumeration of Domain: internaldomain.com
[-] Wildcard resolution is enabled on this domain
[-] It is resolving to 10.10.10.5
[-] All queries will resolve to this address!!
[*] Checking for Zone Transfer for internaldomain.com name servers
[*] Trying NS server 10.10.10.1
[*] Zone Transfer was successful!!
```



WHAT IF ZONE TRANSFER IS NOT ENABLED?

- Many tools use alternative techniques to achieve more or less the same result:
 - DNS reverse lookup:
 - IP address → symbolic name
 - WHOIS
 - ARIN
 - DNS "brute-forcing":
 - attempting to enumerate host names through brute force on common subdomain names like www, mail, blog, admin, ns1, etc.



DNS BRUTE-FORCING WITH “FIERCE”

```
bt5 ~ # ./fierce -dns internallabdomain.com
Fierce 2.0-r412 ( http://trac.assembla.com/fierce )

Starting Fierce Scan at Sun Dec 25 18:19:37 2011
Scanning domain internallabdomain.com at Sun Dec 25 18:19:37 2011 ...

internallabdomain.com - 10.10.10.5

Nameservers for internallabdomain.com:
    ns1.internallabdomain.com          10.10.9.1
    ns2. internallabdomain.com         10.10.9.2
ARIN lookup "internallabdomain":
Zone Transfer:
    ns1.internallabdomain.com          Failed
    ns2.internallabdomain.com          Failed
Wildcards:
Prefix Bruteforce:
Found Node! (10.10.10.5 / 0.internallabdomain.com)
based on a search of: 0. internallabdomain.com.
Found Node! (10.10.10.11 / av.internallabdomain.com)
based on a search of: av.internallabdomain.com.
Found Node! (10.10.10.6 / webmail.internallabdomain.com)
based on a search of: autodiscover.internallabdomain.com.
Found Node! (10.10.10.25 / dev.internallabdomain.com)
based on a search of: dev. internallabdomain.com.
Found Node! (10.10.10.17 / tx.internallabdomain.com)
```



ZONE TRANSFER: COUNTERMEASURES (1/2)

- Limit zone transfers to authorized servers only
 - e.g., in BIND (DNS implementation for UNIX systems)
 - use the "allow-transfer" directive in the "named.conf" configuration file
- On the network side
 - filter all unauthorized TCP connections on port 53
 - please note: DNS → port 53, but:
 - “name lookup” → UDP
 - “zone transfer” → TCP
 - this solution may violate the DNS RFC, which states:
 - lookups for names larger than 512 bytes should be sent via TCP ☹



ZONE TRANSFER: COUNTERMEASURES (2/2)

- Employ techniques based on Cryptographic Transaction Signatures (TSIG) to allow only trusted hosts to perform zone file transfers
- Clearly separate the internal domain from the external domain of the organization
 - expose ONLY the external name servers to the public
- Minimize the use of DNS records of type "HINFO" as they can provide extremely precise information about the operating system of a network host



4. NETWORK RECONNAISSANCE

- Network Topology Information Search
- Search for potential access routes to the target organization's network
- Primary tool in this area:
 - Traceroute
 - a program for discovering network paths
 - based on intelligent use of the Time To Live (TTL) field in IP packets



TRACEROUTE EXAMPLES

Probe packets (UDP) blocked by the firewall of the target organization

```
[bash]$ traceroute 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets

1 gate (192.168.10.1) 11.993 ms 10.217 ms 9.023 ms
2 rtr1.example.com (10.10.12.13) 37.442 ms 35.183 ms 38.202 ms
3 rtr2.example.com (10.10.12.14) 73.945 ms 36.336 ms 40.146 ms
4 hssitrt.example.com (10.11.31.14) 54.094 ms 66.162 ms 50.873 ms
5 * * *
6 * * *
```

Probe packets (UDP) disguised as DNS queries (port 53)!

```
[bash]$ traceroute -S -p53 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets

1 gate (192.168.10.1) 10.029 ms 10.027 ms 8.494 ms
2 rtr1.example.com (10.10.12.13) 36.673 ms 39.141 ms 37.872 ms
3 rtr2.example.com (10.10.12.14) 36.739 ms 39.516 ms 37.226 ms
4 hssitrt.example.com (10.11.31.14) 47.352 ms 47.363 ms 45.914 ms
5 10.10.10.2 (10.10.10.2) 50.449 ms 56.213 ms 65.627 ms
```



NETWORK RECONNAISSANCE: COUNTERMEASURES

- Use of a Network Intrusion Detection System (NIDS)
- Configuration of the organization's border routers:
 - appropriately limit incoming UDP and ICMP traffic

QUESTIONS?

