



PREPARAZIONE DI UN ATTACCO IN RETE: “FOOTPRINTING”

Corso di Laurea Magistrale in Ingegneria Informatica

A.A. 2015/2016

Prof. Simon Pietro Romano

sromano@unina.it



COME SI PREPARA UN ATTACCO DI RETE?

- Concetti vitali per chiunque si voglia preparare, con cognizione di causa, a sferrare un attacco in una rete di calcolatori:
 - footprinting:
 - l'arte di raccogliere informazioni in rete
 - la cosiddetta “network reconnaissance”
 - scanning:
 - ispezione minuziosa del “perimetro” di attacco, alla ricerca di potenziali punti di ingresso
 - enumeration:
 - ‘probing’ dei servizi identificati, al fine di identificare potenziali vulnerabilità



FOOTPRINTING

- Raccolta di informazioni utili alla elaborazione di un profilo (*footprint*) dettagliato delle caratteristiche di sicurezza di una determinata organizzazione:
 - presenza in Internet
 - accesso remoto alla rete dell'organizzazione
 - configurazione della intranet/extranet dell'organizzazione
 - business partner e relative relazioni
- Se condotte in maniera strutturata, le attività di footprinting consentono di ottenere in modo sistematico un quadro dettagliato del profilo di rete di un qualsiasi potenziale target di attacco



FOOTPRINTING: INTERNET/INTRANET

- Dati di interesse:
 - nomi di dominio
 - blocchi di indirizzi e sottoreti
 - indirizzi IP di sistemi raggiungibili tramite Internet
 - servizi TCP ed UDP in esecuzione sui sistemi identificati
 - architettura di sistema
 - meccanismi (e liste) di controllo degli accessi
 - eventuale presenza di Intrusion Detection Systems (IDS)
 - nomi di utenti e/o gruppi di utenti, "banner" di sistema, tabelle di instradamento
 - informazioni di gestione (SNMP)
 - nomi degli host



FOOTPRINTING: EXTRANET

- Dati di interesse:
 - nomi di dominio
 - origine e destinazione di ogni singola connessione
 - tipo di connessioni
 - meccanismi di controllo degli accessi impiegati



FOOTPRINTING: ACCESSO REMOTO

- Dati di interesse:
 - numeri telefonici (analogici e digitali)
 - tipo di sistema remoto
 - meccanismi di autenticazione
 - presenza di Virtual Private Networks (VPN) e relativi protocolli



FOOTPRINTING: CONSIDERAZIONI

- Una delle attività più complesse nella determinazione del profilo di sicurezza di una organizzazione
- Uno dei compiti più noiosi per chiunque sia ansioso di cimentarsi con le tecniche di hacking
- Il passo fondamentale per la successiva elaborazione di un piano di protezione efficace dell'organizzazione oggetto di 'studio'
- Come sempre, il footprinting è:
 - utile per il potenziale attaccante...
 - ...fondamentale per i responsabili della sicurezza di una qualsiasi organizzazione presente in rete



FOOTPRINTING IN INTERNET

1. Informazioni disponibili pubblicamente
2. WHOIS e DNS enumeration
3. DNS interrogation
4. Network Reconnaissance



1. INFORMAZIONI PUBBLICHE

- a. Pagine web dell'organizzazione
- b. Organizzazioni correlate
- c. Dettagli sulla localizzazione
- d. Informazioni sui dipendenti
- e. Eventi di attualità che coinvolgono l'organizzazione
- f. Politiche/meccanismi legati alla privacy ed alla sicurezza
- g. Informazioni archiviate
- h. Motori di ricerca e relazioni tra dati relativi all'organizzazione
- i. Altre informazioni utili...



1.a SITO WEB DELL'ORGANIZZAZIONE

- Moltissime informazioni utili (e, spesso, sensibili) sono pubblicamente disponibili nei siti web delle organizzazioni:
 - dettagli sulle configurazioni di sicurezza
 - inventari completi degli 'asset' dell'organizzazione
 - ...
- Un'analisi approfondita del codice HTML può riservare moltissime 'sorprese':
 - informazioni contenute all'interno di commenti:
 - <!-- Dati sensibili contenuti in un commento... -->
- Molti siti web fanno spesso da 'proxy' verso servizi interni all'organizzazione:
 - webmail, accesso a server Microsoft Exchange, accesso remoto a mainframe (es: WebConnect), accesso alla VPN aziendale, ecc.



ANALISI OFF-LINE DI SITI WEB

- Per una analisi più accurata delle risorse web di un'organizzazione, spesso si ricorre alle seguenti tecniche:
 1. Download in locale di un ‘clone’ del sito da analizzare:
 - uso di tool quali “Wget” (<http://www.gnu.org/software/wget/>)
 2. ricerca, all'interno del clone locale del sito web, di informazioni “nascoste”:
 - hidden files e directory
 - operazione automatizzabile tramite approcci cosiddetti “a forza bruta” (brute force)
 - ricerca ricorsiva, all'interno del sito, di directory e file e nascosti, con eventuale indicazione delle estensioni ritenute maggiormente interessanti (es: “.php”, “.jsp”, “.cgi”, “.asp”, ecc)



DirBuster: un Esempio Di Tecnica “Brute Force”

The screenshot shows two windows of the OWASP DirBuster tool. The left window displays the configuration settings for the scan, including the target URL (`http://www.pippozzo.com`), work method (Auto Switch), number of threads (10), and scanning type (Pure Brute Force). The right window shows the results of the scan, which has found 143 files. A context menu is open over a file named `/ND.php`, with options like "Open In Browser" and "View Response". The results table includes columns for Directory Structure, Response Code, and Response Size.

Directory Structure	Response Code	Response Size
/	200	278
/	200	278
/	200	278
/	200	278
/	301	446
/	200	278
/	200	85227
/	200	67923
/	301	446
/	301	446
/	301	446
/	301	446
/	301	446
/	301	446
/	301	446
/	301	446
/	302	270
/	301	446
/	301	446
/	301	446
/	301	446
/	200	278
/	302	289



1.b ORGANIZZAZIONI COLLEGATE

- Riferimenti o link ad organizzazioni in vario modo ‘collegate’ all’organizzazione target
 - es: molte aziende realizzano in outsourcing i propri siti web, sia per la fase di progettazione, che per quella di sviluppo e di consulenza grafica
- Informazioni sulle organizzazioni partner trapelano spesso dalla’analisi del sito web dell’organizzazione target:
 - es: commenti in pagine web contenenti l’indicazione (e l’affiliazione) dell’autore del codice e/o della parte grafica
 - librerie javascript, fogli di stile, ecc.



1.c DETTAGLI SULLA LOCALIZZAZIONE

- L'indirizzo fisico di un'organizzazione può risultare molto utile per sferrare attacchi di tipo 'non tecnico':
 - "dumpster-diving":
 - ebbene sì, cercare 'tesori di informazioni' nell'immondizia!
 - "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 Informazioni sui dipendenti

- Nomi di contatti, numeri di telefono, indirizzi e-mail...
 - da un indirizzo e-mail è spesso facile risalire ad un nome utente
 - un nome di un utente di dominio valido è fondamentale per passare alle fasi successive dell'attacco ed ottenere accesso alle risorse del sistema target
- Siti da utilizzare per raccogliere informazioni sui dipendenti di un'organizzazione:
 - siti social:
 - *facebook, myspace, reunion, classmates, twitter, flickr*, ecc.
 - siti professionali:
 - *linkedin, plaxo, monster, careerbuilder*, ecc.
 - siti a pagamento per contatti da utilizzare nelle campagne di marketing e commerciali:
 - es: *connect.data.com su Salesforce*



UN ESEMPIO: CONNECT.DATA.COM

The image displays two side-by-side screenshots of the connect.data.com website, illustrating the platform's features for managing company profiles.

Screenshot 1: Company Profile Overview

This screenshot shows the basic information for "Web Conferencing Central". Key details include:

- Website:** www.web-conferencing-central.com
- Headquarters:** 1639 Monrovia Ave, Site 1, Newport Beach, CA 92663-2852, United States (map)
- Phone:** +1.949.631.0274
- Industries:** Software & Internet, Software & Internet Other
- Employees:** 0 - 25
- Revenue:** \$0 - 1M
- Ownership:** Privately Held
- Last Updated:** PH2008 on 07/07/08

On the right, it shows "1 contacts at this company" with a breakdown of titles:

Title	Count
C-Level	1
VP-Level	0
Director-Level	0
Manager-Level	0
Staff	0
Other	0

Screenshot 2: Domain Management

This screenshot shows the management of domains for "Web Conferencing Central". It lists one domain:

Domain Name	Domain Type	Update	Delete
web-conferencing-central.com	Web URL and Email	Update	Delete

At the bottom of both screenshots, there are navigation links for Community, Are You in Data.com?, Developers, Enterprise Solutions, Email Marketing, Privacy, Terms of Use, Site Map, and Contact, along with the Salesforce logo.

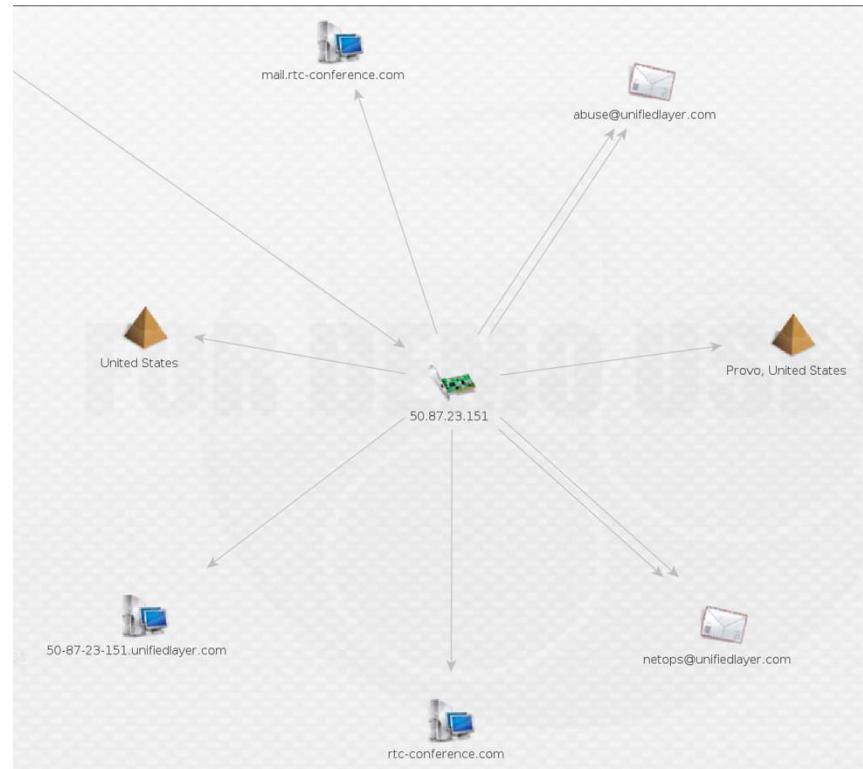
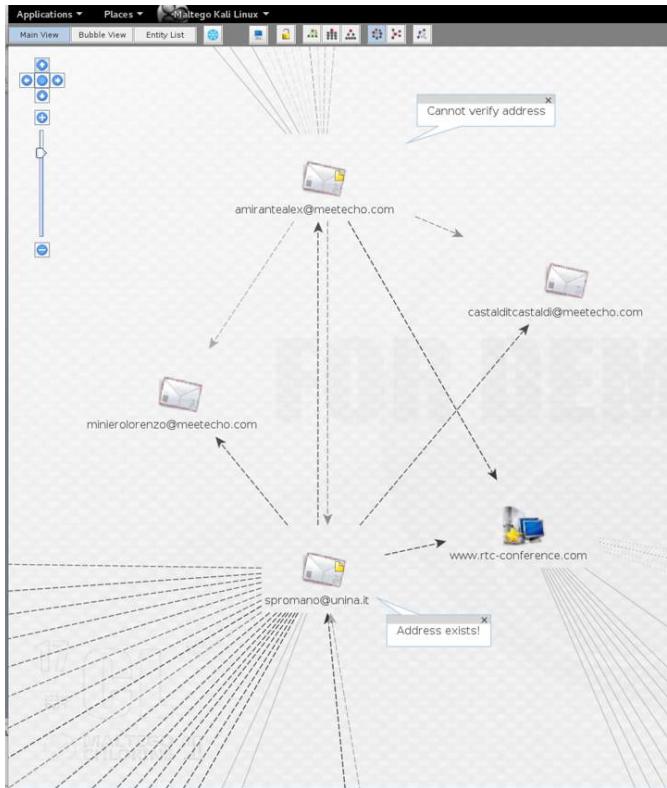


COME USARE TUTTI QUESTI DATI?

- Moltissimi strumenti di *data mining* possono essere sfruttati per correlare opportunamente l'enorme quantità di informazioni raccolta
- Un esempio su tutti: *Maltego*
 - *un potentissimo tool di social engineering*
 - capace di:
 - estrapolare informazioni a vari livelli
 - elaborare (“trasformare”) le informazioni raccolte
 - correlare i dati
 - rappresentare il risultato delle elaborazioni sotto forma di “grafo sociale”



MALTEGO IN AZIONE





1.e Eventi che coinvolgono l'organizzazione

- Informazioni su:
 - fusioni aziendali, acquisizioni, scandali, fallimenti, cessione di attività in outsourcing, impiego massiccio di contratti di lavoro interinale, ecc.
 - tutti indicatori utili dello ‘stato di salute’ e delle modalità di gestione di una organizzazione
- Se l’organizzazione è un’azienda pubblica, moltissime informazioni sono disponibili in rete:
 - obbligo della trasparenza



1.f MECCANISMI DI PRIVACY E SICUREZZA

- Qualsiasi tipo di informazione che fornisca dettagli utili relativamente alle policy di sicurezza adottate dall'organizzazione target
- Dettagli di tipo tecnico riguardo l'infrastruttura hardware e software di cui l'organizzazione si è dotata a scopi di protezione



1.g INFORMAZIONI ARCHIVIATE

- Impiego di siti Internet che consentono di recuperare copie obsolete di informazioni non più rese disponibili dalla sorgente originale
 - possibilità di accedere a dati (sensibili) volutamente rimossi dall'organizzazione target per motivi di sicurezza
- Un esempio su tutti:
 - WayBack Machine
(www.archive.org)

The screenshot shows the Wayback Machine homepage. At the top, it features the "INTERNET ARCHIVE" logo and the "Wayback Machine" logo with a red "W". Below the logo is a search bar with the placeholder "http://". To the right of the search bar is a "BROWSE HISTORY" button. A banner below the search bar states "438 billion web pages saved over time." with a "DONATE" link. Below the banner is a grid of small thumbnail images representing saved web pages from various websites. At the bottom of the page, there are three main sections: "Tools" (with links to "Wayback Machine Availability API", "Build your own tools.", "WordPress Broken Link Checker", and "Banish broken links from your blog."), "Subscription Service" (with a description of Archive-It and a link to "Archive-It to build and browse the collections."), and "Save Page Now" (with a form for entering a URL and a "SAVE PAGE" button, and a note that it is "Only available for sites that allow crawlers").



1.h MOTORI DI RICERCA E RELAZIONI TRA DATI

- I motori di ricerca sono, oggi, tra i principali strumenti degli hacker
- Es: “allinurl:tsweb/default.htm”
 - server Microsoft che espongono un servizio di desktop remoto accessibile, via web...
 - ...potenzialmente vulnerabili ad attacchi di tipo “remote-to-local” tramite exploit del protocollo RDP (Remote Desktop Protocol)

The screenshot shows a Google search results page with the query "allinurl:tsweb/default.htm". The results are filtered under the "Web" tab. There are approximately 135 results found in 0.47 seconds. The results include:

- 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**
www.pcinx.it/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 ...
- 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, Buffo, 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 ▾ Traduci questa pagina
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 displaying the GHDB homepage. The URL in the address bar is <https://www.offensive-security.com/community-projects/google-hacking-database/>. The page features a navigation menu with links to Blog, Courses, Certifications, Online Labs, Penetration Testing, Projects, About, and a search icon. The main title is "Google Hacking Database (GHDB)" with the subtitle "Your Home for 'googledorks'". Below the title is a large black rectangular area containing the "GOOGLE HACKING-DATABASE" logo and a search bar with the query "inurl: * all t". There are two buttons: "Google Search" and "I'm Feeling Lucky". To the left, under the heading "What is the Google Hacking Database?", there is a brief description and a link to "GHDB : hosted and maintained by Offensive Security". To the right, under the heading "Feeling Lucky?", there is a call to action to "Give the GHDB a try for yourself. You can also contribute your own googledorks! Just be sure to search before submitting." A search bar with a dropdown menu and a "SEARCH" button is located at the bottom right.

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 SEARCH



SHODAN

- “*Sentient Hyper-Optimized Data Access Network*”
- Da molti definita: “Google for Hackers”
- Concepita per trovare sistemi (computer, router, webcam, frigoriferi, “cose”) in rete
- Particolare attenzione alla scoperta di potenziali falle nei meccanismi di autenticazione e di autorizzazione

The screenshot shows the Shodan search engine homepage. At the top, there's a navigation bar with links for "Dashboard", "Status", "Searchable", "Pie All...", "Explore", "Contact Us", "Blog", "Enterprise Access", "New to Shodan?", and "Logout/Register". Below the navigation is a search bar with the word "SHODAN" and a magnifying glass icon. A red banner across the top says "The search engine for the Internet of Things". Below the banner, it says "Shodan is the world's first search engine for Internet-connected devices." There are two buttons: "Create a Free Account" and "Getting Started". To the right of the banner is a large, dark circular map representing the Internet of Things, with a yellow dot labeled "SHANGHAI". Below the map are four promotional cards:

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

At the bottom of the page, there's a row of logos for "CNNMoney", "Dagbladet", "The Washington Post", "BBC NEWS", "WIRED", and "CIO". Below that, a call-to-action button says "Analyze the Internet in Seconds". At the very bottom, there's a "Sample Report" button and a world map where countries are colored red.



SHODAN: UN ESEMPIO DI RICERCA

SHODAN

asterisk+pbx

Explore Membership Contact Us Blog Enterprise Access

Exploits Maps Download Results Create Report

TOP COUNTRIES

Showing results 1 - 10 of 42,186

181.63.251.65
Telmex Colombia S.A.
Added on 2015-09-24 16:47:46 GMT
Colombia
Details

50.73.47.53
mail.coop.com
Comcast Business Communications
Added on 2015-09-24 16:47:20 GMT
United States, West Jordan
Details

122.111.243.53
d122-111-243-53.perf01.wa.optumnet.com.au
Optum
Added on 2015-09-24 16:47:13 GMT
Australia, Perth
Details

220.95.208.120
Korea Telecom
Added on 2015-09-24 16:47:05 GMT
Korea, Republic of
Details

SIP/2.0 404 Not Found
Via: SIP/2.0/UDP nn;brANCH=foo;received=xxxx.xxxx.xxxx;rport=26810
From: <sip:nn@nn>;tag=root
To: <sip:me2@nn>;tag=as3fbfc8bd8
Call-ID: 58000
CSeq: 42 OPTIONS
Server: Asterisk PBX SVN-branch-13-r434789M
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY,...

SIP/2.0 404 Not Found
Via: SIP/2.0/UDP nn;brANCH=foo;received=xxxx.xxxx.xxxx;rport=26810
From: <sip:nn@nn>;tag=root
To: <sip:me2@nn>;tag=as539f715b
Call-ID: 58000
CSeq: 42 OPTIONS
Server: Asterisk PBX 1.8.23.0
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH

SIP/2.0 404 Not Found
Via: SIP/2.0/UDP nn;brANCH=foo;received=xxxx.xxxx.xxxx;rport=26810
From: <sip:nn@nn>;tag=root
To: <sip:me2@nn>;tag=as6a6e63015
Call-ID: 58000
CSeq: 42 OPTIONS
Server: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH

SIP/2.0 404 Not Found
Via: SIP/2.0/UDP nn;brANCH=foo;received=xxxx.xxxx.xxxx;rport=26810
From: <sip:nn@nn>;tag=root
To: <sip:me2@nn>;tag=as870c72b5
Call-ID: 58000



CONTROMISURE?

- RFC 2196: Site Security Handbook:
 - una guida per la definizione e la messa in opera di politiche e procedure di sicurezza per organizzazioni che ‘espongono’ i propri sistemi in 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 E DNS ENUMERATION

- ICANN: Internet Corporation for Assigned Names and Numbers
 - una organizzazione di coordinamento tecnico per Internet
 - coordina l'assegnazione dei seguenti identificativi:
 - nomi di dominio
 - indirizzi IP
 - parametri dei protocolli e relativi numeri di porta
 - controlla che i root name server del DNS funzionino correttamente ed operino in maniere stabile
 - ha assunto (in realtà, sta ancora assumendo) le responsabilità un tempo assegnate, sotto contratto del governo americano, alla “Internet Assigned Numbers Authority” (IANA)



ICANN: STRUTTURA

- Alcune sotto-organizzazioni di rilievo:
 - ASO: Address Supporting Organization
 - alloca blocchi di indirizzi IP ai vari Regional Internet Registries (RIR)...
 - ...che a loro volta allocano indirizzi agli ISP, ai National Internet Registries (NIR), o ai Local Internet Registries (LIR)
 - GNSO: Generic Names Supporting Organization
 - responsabile per i nomi dei cosiddetti “generic Top Level Domains” (gTLD):
 - .com, .net, .edu, .org, .info, ecc.
 - CCNSO: Country Code Domain Name Supporting Organization
 - responsabile per i nomi dei “country-code Top Level Domains” (ccTLD):
 - .it, .fr, .de, .jp, ecc.



RICERCHE SUI NOMI DI DOMINIO

- Le tre “R” del servizio WHOIS:
 - Registry
 - contiene informazioni sul Registrar presso il quale l’entità target ha effettuato la registrazione del proprio nome di dominio
 - Registrar
 - contiene dettagli sull’entità che ha effettuato la registrazione
 - Registrant
 - l’entità che ha effettuato la registrazione del proprio nome di dominio
- Ricordate che il DNS implementa un meccanismo di registrazione di tipo gerarchico:
 - il punto ideale da cui cominciare per una ricerca è la radice dell’albero:
 - 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 194.0.16.215 2001:678:12:0:194:0:16:215
nserver: DNS.NIC.IT 192.12.192.5 2a00:d40:11:0:0:0:5
nserver: M.DNS.IT 2001:1ac8:0:280:0:5d1:6004:2 217.29.76.4
nserver: NAMESERVER.CNR.IT 194.1.19.192.34 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=unina.it

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 12:46:57 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:	Universita' degli Studi di Napoli Federico II C.so Umberto I 80138 - Napoli (NA) it
Phone:	+39.81676643
Fax:	+39.81676628
E-Mail:	fpalmier@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:	Universita' 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:	Universita' degli Studi di Napoli Federico II C.so Umberto I 80138 - Napoli (NA) it
Phone:	+39.81676643
Fax:	+39.81676628
E-Mail:	fpalmier@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 DA LINEA DI COMANDO

```
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 2a00:40:1:1:0:0:0:5
nserver:     M.DNS.IT 2001:1ac0:0:200:0:a5d1:6004:2 217.29.76.4
nserver:     NAME SERVER.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: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 Palmieri
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 Palmieri
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
```



RICERCHE SUGLI INDIRIZZI IP

- Indirizzi IP:
 - gestiti dai Regional Internet Registries (RIR)
 - una query indirizzata ad un qualsiasi RIR ci darà:
 - le informazioni che cerchiamo, se l'indirizzo in questione è gestito da quel RIR
 - le informazioni sul RIR giusto da contattare, in caso contrario



QUERY SU INDIRIZZI IP

You searched for: **143.225.229.254**

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	



CI POSSIAMO FIDARE DEGLI INDIRIZZI IP?

- Chi si occupa di security, sa bene che fare affidamento sugli indirizzi IP sorgenti reperibili nei log di un attacco è quasi sempre un'idea fallimentare!
- Gli attaccanti seri non lasciano mai tracce così evidenti dei propri movimenti e si preoccupano di ‘lavare’ gli indirizzi che usano per sferrare l’attacco:
 - “*laundered*” IP addresses...



CONTROMISURE?

- Alcuni fornitori di nomi di dominio offrono (a pagamento) registrazioni di tipo privato:
 - non vengono pubblicate on-line informazioni sull'organizzazione, quali:
 - indirizzo reale, numero di telefono, indirizzo e-mail, ecc.
- A proposito di registrazioni di domini:
 - attenzione ai provider che offrono la possibilità di modificare la registrazione via e-mail!
 - rischio di “domain hijacking” → modifica info di registrazione e conseguente “redirezione” di tutto il traffico indirizzato al dominio originale
 - necessità di offrire tale tipo di servizi solo in contesti in cui i meccanismi di autenticazione siano affidabili
 - ...il campo “FROM” di una mail affidabile NON è!



3. INTERROGAZIONE DEL DNS

- Domain Name System (DNS)
 - un servizio distribuito per la traduzione di nomi simbolici in indirizzi IP
- DNS configurato in maniera non sicura:
 - moltissime informazioni su di un'organizzazione possono trapelare ed essere sfruttate da un attaccante
- Due problemi su tutti:
 - Zone Transfers
 - Analisi dei record di tipo MX (Mail eXchange)



ZONE TRANSFERS

- Un “trasferimento di zona” si verifica quando:
 - un master server secondario aggiorna il proprio database di zona a partire dal database di un server primario
- Utile per motivi di ridondanza:
 - in caso di guasto al primary master server, un server secondario può immediatamente sostituirlo
- Problema:
 - il trasferimento di zona dovrebbe essere consentito solo tra server primario e server secondari...
 - ...in caso di configurazioni errate, una copia del file di zona viene invece resa disponibile a chiunque ne faccia richiesta!



ZONE TRANSFER E DATI INTERNI

- Il Zone Transfer verso tutti risulta problematico quando l'organizzazione non fa uso di una politica sul DNS di tipo “pubblico/privato”:
 - pubblico:
 - cosiddetto DNS esterno, visibile a chiunque in rete
 - privato:
 - DNS interno, vale a dire nomi degli host ed indirizzi IP interni all'azienda
- Fornire ad un attaccante le informazioni sul DNS interno equivale a regalargli una “radiografia” della struttura della propria organizzazione!



ZONE TRANSFER: I TOOL

- “*nslookup*”
 - il client DNS maggiormente diffuso
- “*host*”, “*dig*”
 - molto utilizzati in ambiente Unix per operazioni cosiddette di “troubleshooting” legate al DNS
- “*dnsrecon*”
 - un programma di utilità per il trasferimento ricorsivo di file di zona



NSLOOKUP: UN ESEMPIO

```
[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: UN ESEMPIO

```
[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!!
```



E SE IL ZONE TRANSFER È DISABILITATO?

- Moltissimi tool utilizzano tecniche alternative per ottenere, più o meno, il medesimo risultato:
 - DNS reverse lookup:
 - indirizzo IP → nome simbolico
 - WHOIS
 - ARIN
 - DNS “brute-forcing”
 - tentativo di enumerare i nomi degli host tramite approccio a forza bruta su nomi di “sotto-domini” comuni (www, mail, blog, admin, ns1, ecc).



DNS BRUTE-FORCING CON IL TOOL “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          10.10.0.1
    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: CONTROMISURE (1/2)

- Limitare i trasferimenti di zona ai soli server autorizzati
 - es: BIND (implementazione DNS per sistemi UNIX)
 - direttiva “allow-transfer” nel file di configurazione “named.conf”
- Lato rete:
 - filtrare tutte le connessioni TCP, non autorizzate, sulla porta 53
 - NB: DNS → porta 53, ma:
 - “name lookup” → UDP
 - “zone transfer” → TCP
 - Problema di questa soluzione:
 - violazione dell’RFC del DNS, la quale afferma che lookup sui nomi di dimensioni superiori ai 512 byte debbano essere spedite via TCP ☺



ZONE TRANSFER: CONTROMISURE (2/2)

- Impiegare tecniche basate su “Cryptographic Transaction Signatures” (TSIG) per consentire solo ad host fidati di effettuare trasferimenti di file di zona
- Separare nettamente il dominio interno dal dominio esterno dell'organizzazione
 - esporre pubblicamente SOLO i name server esterni
- Evitare quanto più possibile l'impiego dei record DNS di tipo “HINFO”, che consentono di individuare, con precisione estrema, il tipo di sistema operativo di un host di rete



4. NETWORK RECONNAISSANCE

- Ricerca di informazioni sulla topologia di rete
- Ricerca di potenziali percorsi di accesso alla rete dell'organizzazione target
- Tool principale in questo ambito:
 - *traceroute*
 - un programma per la scoperta di percorsi di rete
 - basato sull'impiego ‘intelligente’ del campo Time To Live (TTL) presente nei pacchetti IP



ESEMPI DI TRACEROUTE

Pacchetti sonda (UDP)
bloccati dal firewall
dell'organizzazione target

```
[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 * * *
```

Pacchetti sonda (UDP)
mascherati da query DNS
(porta 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: CONTROMISURE

- Impiego di un Network Intrusion Detection System (NIDS)
- Configurazione dei router di frontiera dell'organizzazione:
 - limitare opportunamente il traffico UDP ed ICMP in ingresso



DOMANDE?

