Vulnerabilità e Difesa dei Sistemi Internet

A.K.A. ETHICAL HACKING

FRANCESCO MANCINI - francesco.mancini@uniroma2.it

PASQUALE CAPORASO - pasquale.caporaso@uniroma2.it

SARA DA CANAL - sara.da.canal@uniroma2.it

PIERCIRO CALIANDRO – pierciro.caliandro@uniroma2.it

Social Engineering

WHY WE START FROM HERE?

The Numbers Don’t Lie

48%

of enterprises have been victims of social engineering attacks

75%

Success rate with social engineering phone calls to businesses

What social engineering is?

"…the art of manipulating people into performing actions or divulging confidential information."

Wikipedia

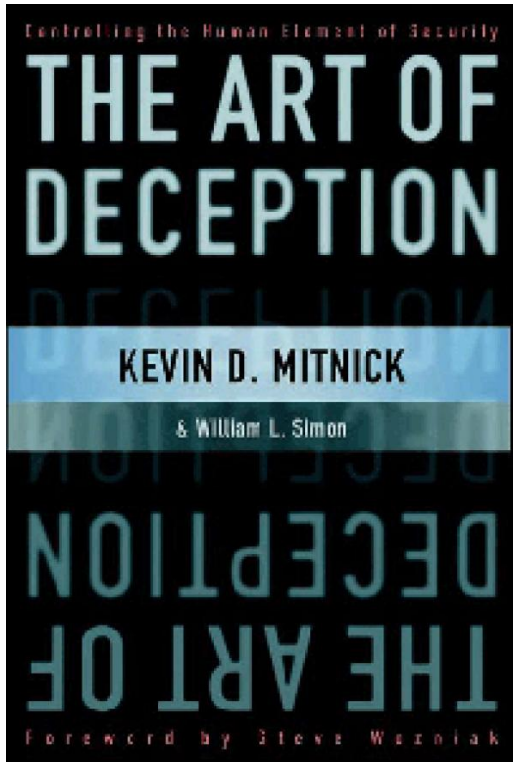
Social Engineering

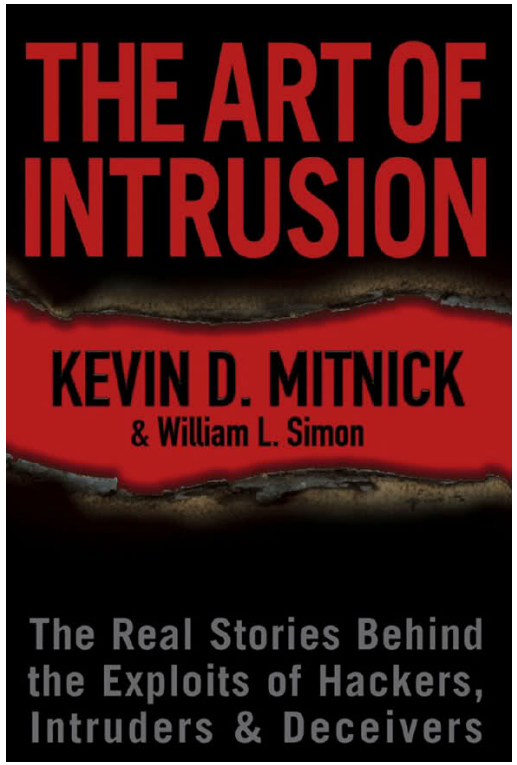
*"You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned **manipulation**."*

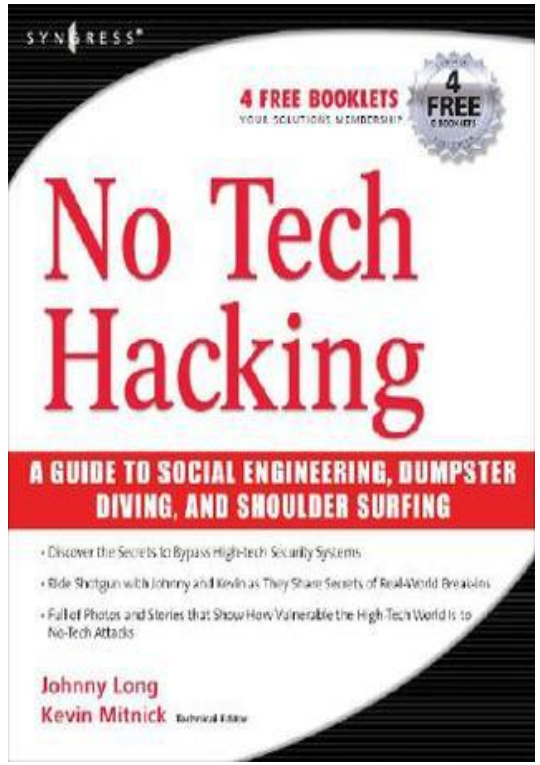
Kevin Mitnick

Motivation: Free Burgers!

Suggested books







Real World Examples: Robin Sage

Completely fake profile and no other real-life information

- Sage was offered consulting work with notable companies **Google** and **Lockheed Martin**
- Received dinner invitations by several of her male friends.
- Almost all of the FB friends were working for United States military, government or companies

Using these contacts

- Gained access to email addresses and bank accounts
- Learning the location of secret military units based on soldiers' Facebook photos and connections between different people and organizations
- She was also given private documents for review and was offered to speak at several conferences.

Source: *Ryan, Thomas (July 2010).* *"Getting in Bed with Robin Sage."*

Real World Examples: Paul Allen

An individual called into Citibank's customer service bureau claiming to be Paul Allen (Co-founder of Microsoft)

Caller claimed he had misplaced his debit card (did not want to report it stolen)

Caller was able to change the mailing address for the account to his residence in Pittsburgh over the phone

Had a new card overnighted

- Card was used to make a $658 payment to a bank loan account
- Attempted to make a $15,000 wire transfer and a purchase at Game Stop, but transactions were denied

citibank®

Source: "FBI Says Citibank Gave Paul Allen's Debit Card to Thief", http://www.wired.com/threatlevel/2012/03/paul-allen-debit-card-caper/

Real World Examples: Fake Employee

A man dressed as an employee of Brinks walked into a Wachovia branch in downtown Washington D.C. and walked out with more than $350,000.

Wasn’t until the real Brink’s driver showed up did they realize they had been robbed.

Source: http://www.schneier.com/blog/archives/2008/01/socialengineeri.html

Remote Social Engineering Tactics

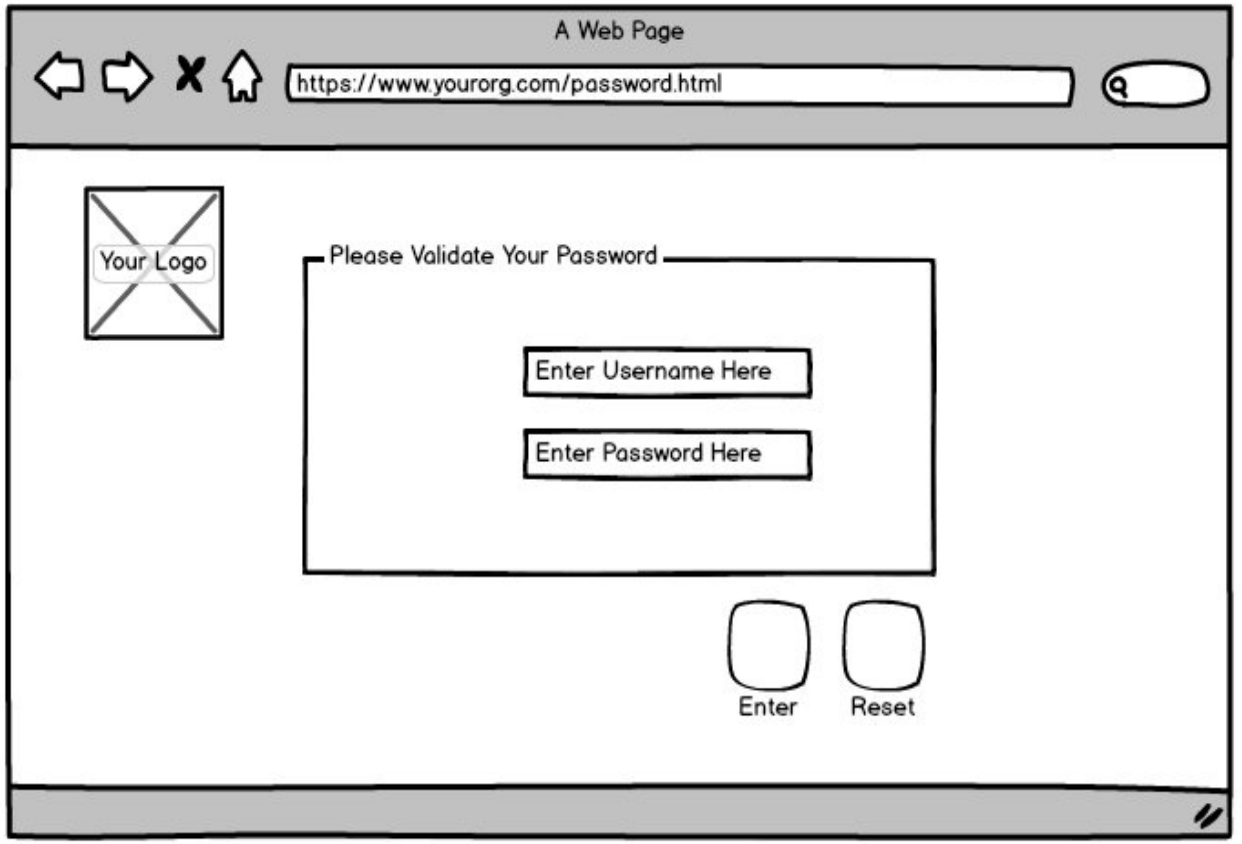
Help Us Out!

Scenario

- Inbound telephone calls to employees
- Caller attempts to persuade a user to provide sensitive information or to visit a fake website and enter his/her credentials to validate their password(s)
- Outbound caller ID is spoofed
- Captures usernames and passwords

Remote Social Engineering Tactics

Fake Site Example



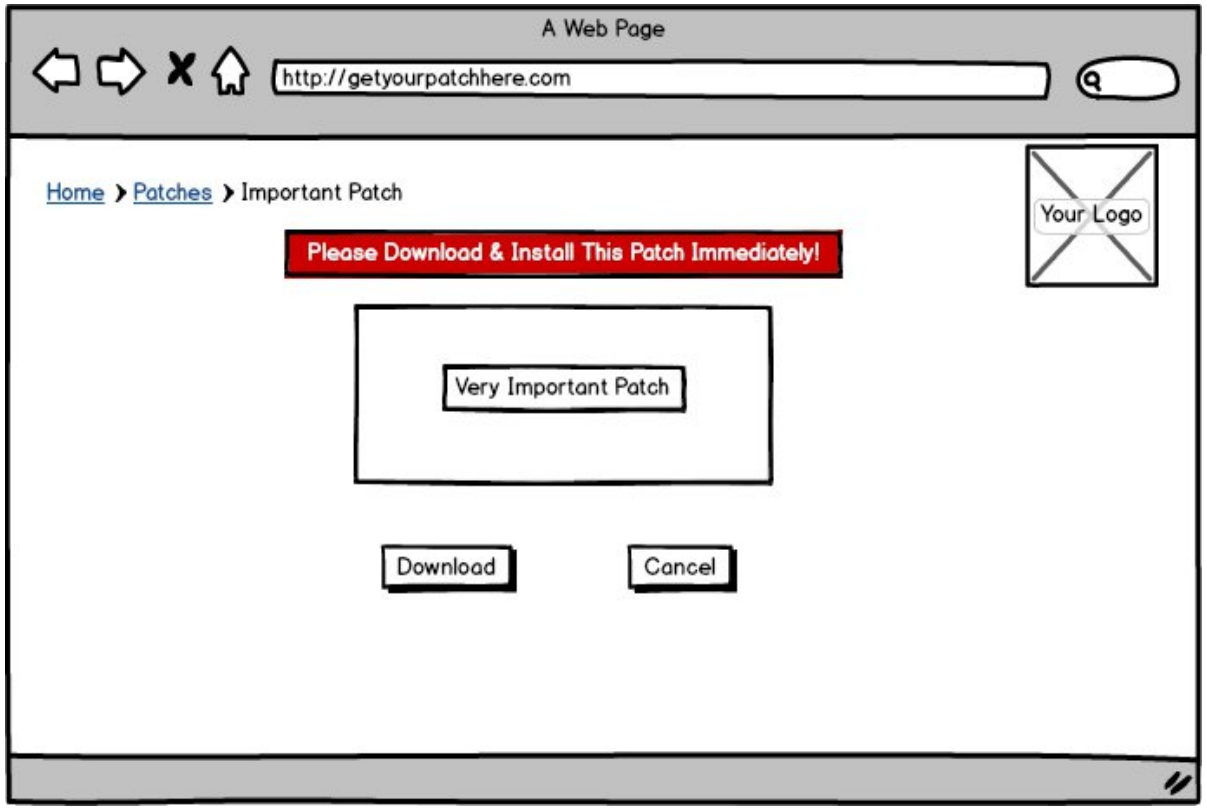
Remote Social Engineering Tactics

The Patch

Scenario

- Inbound telephone calls to employees
- Direct user to fake website to download and execute the “patch”
- Executable actually sends username, IP address and hostname to Internet

Sample Site


A Web Page
http://getyourpatchhere.com
Home › Patches › Important Patch
Your Logo
Please Download & Install This Patch Immediately!
Very Important Patch
Download
Cancel


PatchInstall.exe
Patch Install Success!
Installation 100% Complete
Thank You For Your Assistance
In Protecting Our Company!

Remote Social Engineering Tactics

The E-Mail Patch

- Send e-mails to targeted users to persuade them to visit a “patch” site to “fix” a zero-day vulnerability
- Similar to Scenario 2 (Phone)
- Executable actually sends username, IP address and hostname to Internet

Phishing / Spear Phishing

- “Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication".
- URL and Email Manipulation
- A URL like (http://www.company.com) looks almost identical to (http://www.cornpany.com)

Phishing

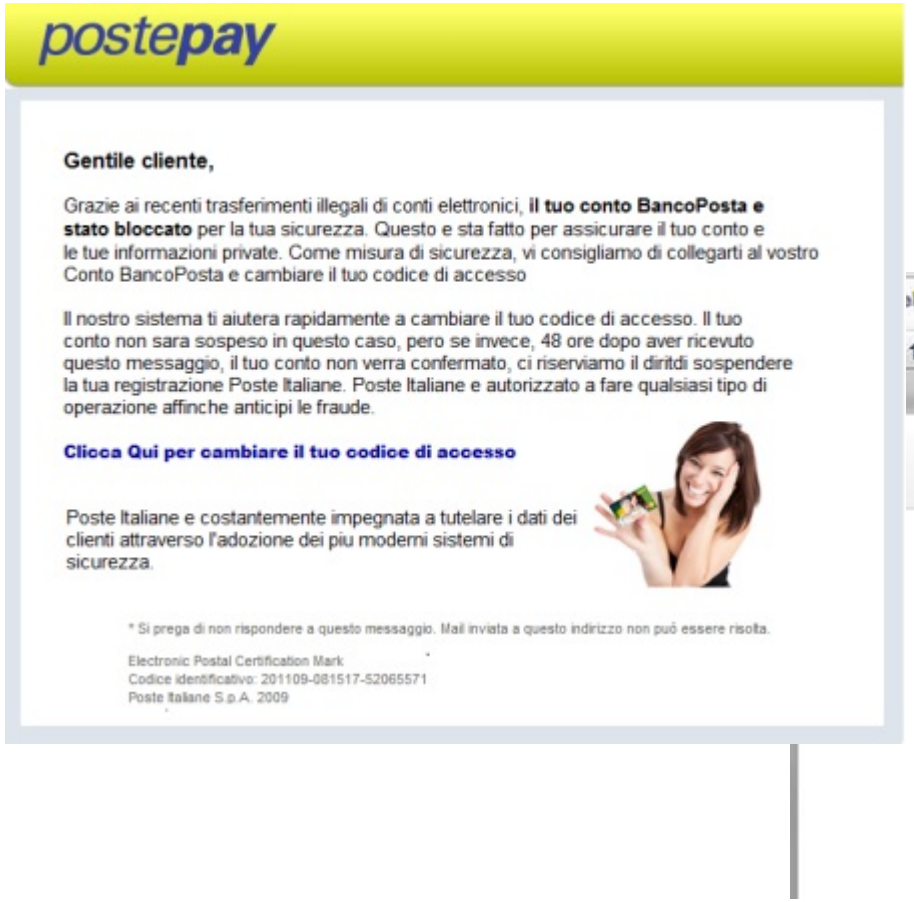
U.S. Department- of- State
National-Visa-Center
Rochester Avenue. Portsmouth NH. 35004.

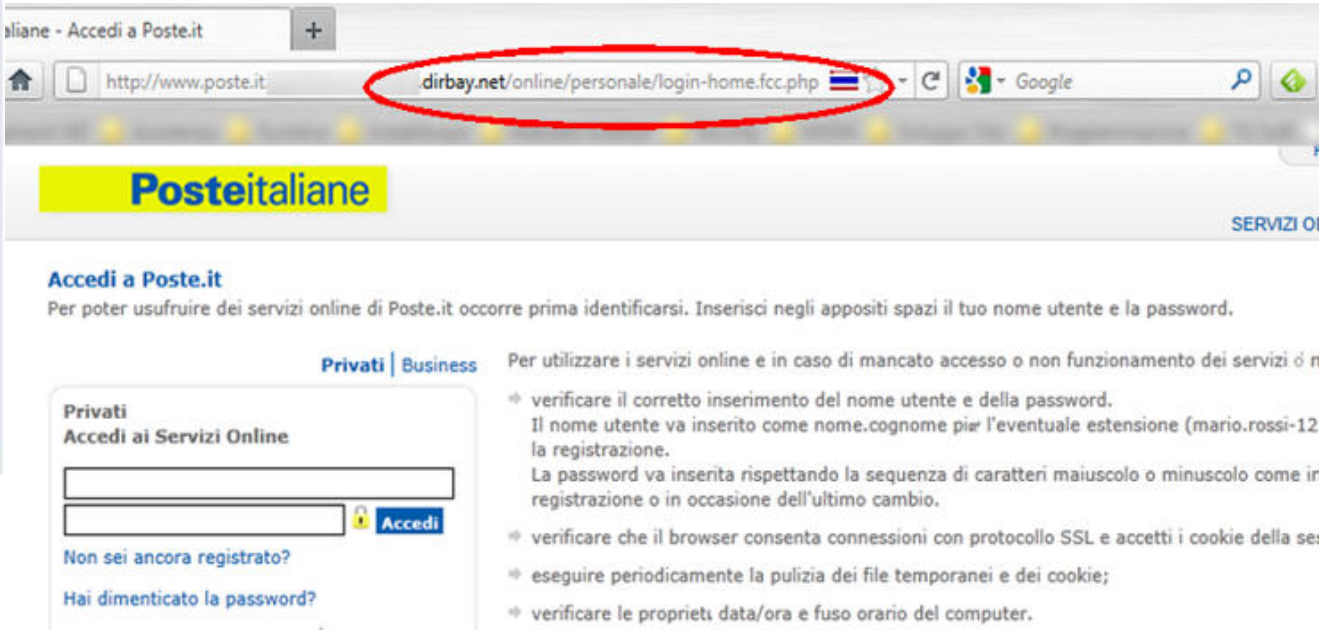
Winning-No: **WAC20147730094DD**

Dear Winner:,
Congratulation's!- We wish to notify you that you are among the selected lucky winners of the U.S visa Lottery (Green Card) through our email ballot lottery program held on the 22th of MARCH 2014 in Arkansas (USA) The Green Card email ballot lottery program was conducted under the terms of Section 203 of the Immigration and Nationality Act (INA) Section 131 of the Immigration Act of 2006 (Pub.L.101-649).

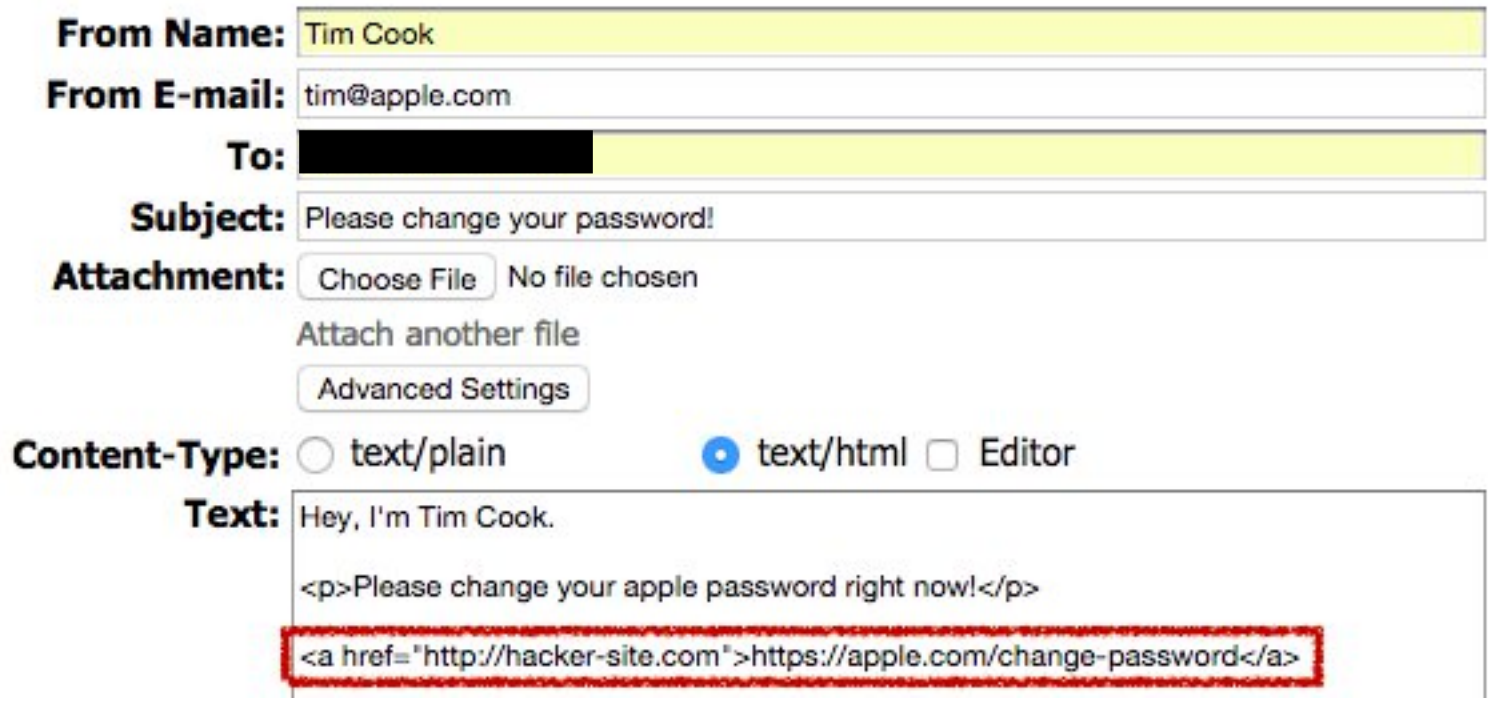
The aims and objectives of the program is to give free visa's to citizens of developing countries around the world who wishes to travel to U.S and start a new life and work. The green card Lottery is a matter of huge benefits for those who want to try themselves abroad. Your visa duration is 10 years multiple entries to the U.S, it is renewable upon expiration and it permits you to travel to U.S with your family.

Phishing

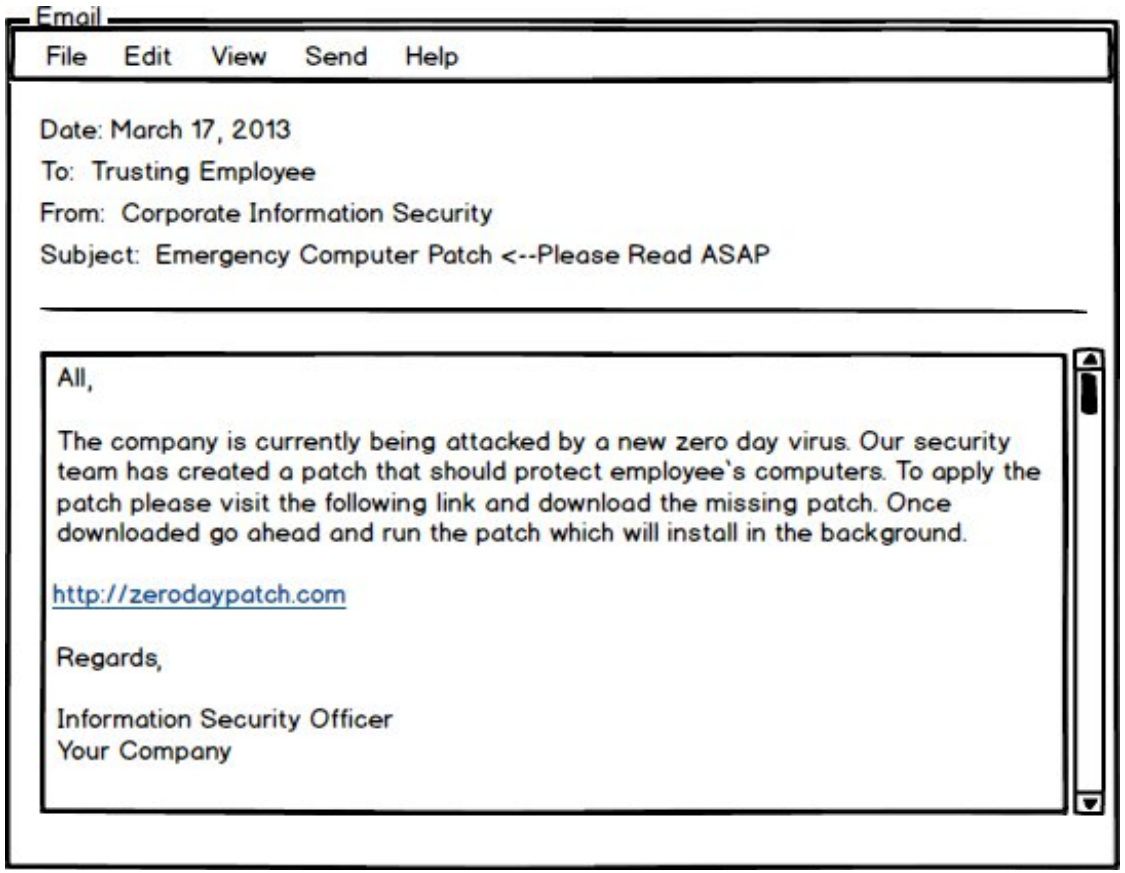

postepay
Gentile cliente,
Grazie ai recenti trasferimenti illegali di conti elettronici, il tuo conto BancoPosta e stato bloccato per la tua sicurezza. Questo e sta fatto per assicurare il tuo conto e le tue informazioni private. Come misura di sicurezza, vi consigliamo di collegarti al vostro Conto BancoPosta e cambiare il tuo codice di accesso
Il nostro sistema ti aiutera rapidamente a cambiare il tuo codice di accesso. Il tuo conto non sara sospeso in questo caso, pero se invece, 48 ore dopo aver ricevuto questo messaggio, il tuo conto non verra confermato, ci riserviamo il diritdi sospendere la tua registrazione Poste Italiane. Poste Italiane e autorizzato a fare qualsiasi tipo di operazione affinche anticipi le fraude.
Clicca Qui per cambiare il tuo codice di accesso
Poste Italiane e costantemente impegnata a tutelare i dati dei clienti attraverso l'adozione dei piu moderni sistemi di sicurezza.
* Si prega di non rispondere a questo messaggio. Mail inviata a questo indirizzo non può essere risolta.
Electronic Postal Certification Mark
Codice identificativo: 201109-081517-52065571
Poste Italiane S.p.A. 2009

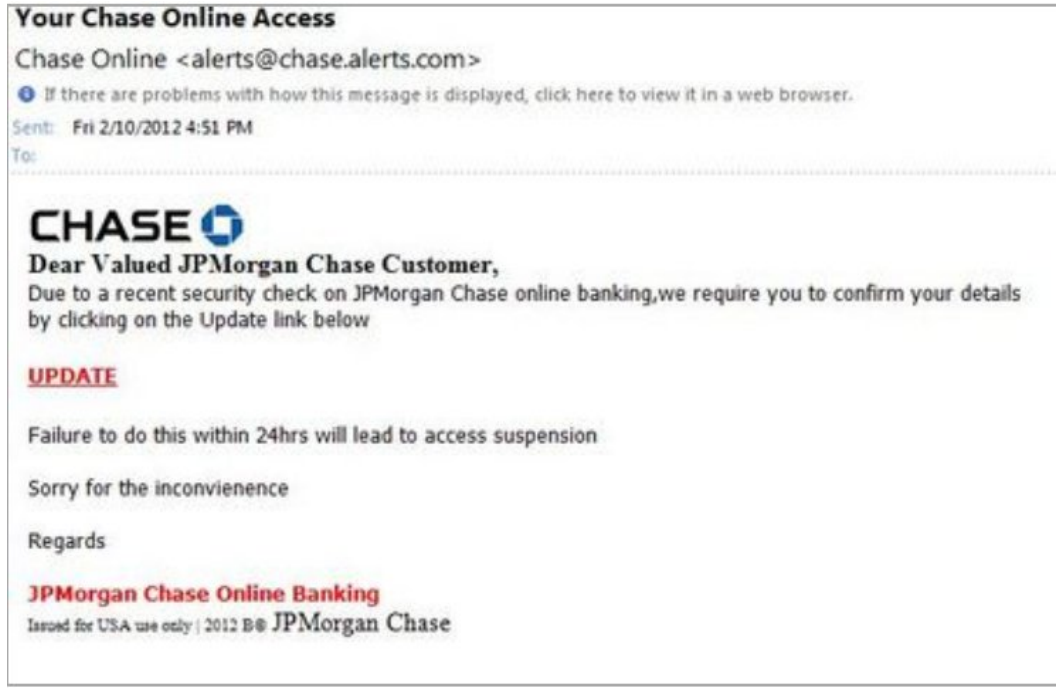

liane - Accedi a Poste.it
http://www.poste.it
dirbay.net/online/personale/login-home.fcc.php
Google
Posteitaliane
SERVIZI O
Accedi a Poste.it
Per poter usufruire dei servizi online di Poste.it occorre prima identificarsi. Inserisci negli appositi spazi il tuo nome utente e la password.
Privati | Business
Privati
Accedi ai Servizi Online
Accedi
Non sei ancora registrato?
Hai dimenticato la password?
Per utilizzare i servizi online e in caso di mancato accesso o non funzionamento dei servizi
verificare il corretto inserimento del nome utente e della password.
Il nome utente va inserito come nome.cognome pi l'eventuale estensione (mario.rossi-12
la registrazione.
La password va inserita rispettando la sequenza di caratteri maiuscolo o minuscolo come i
registrazione o in occasione dell'ultimo cambio.
verificare che il browser consenta connessioni con protocollo SSL e accetti i cookie della se
eseguire periodicamente la pulizia dei file temporanei e dei cookie;
verificare le proprieta data/ora e fuso orario del computer.

Phishing

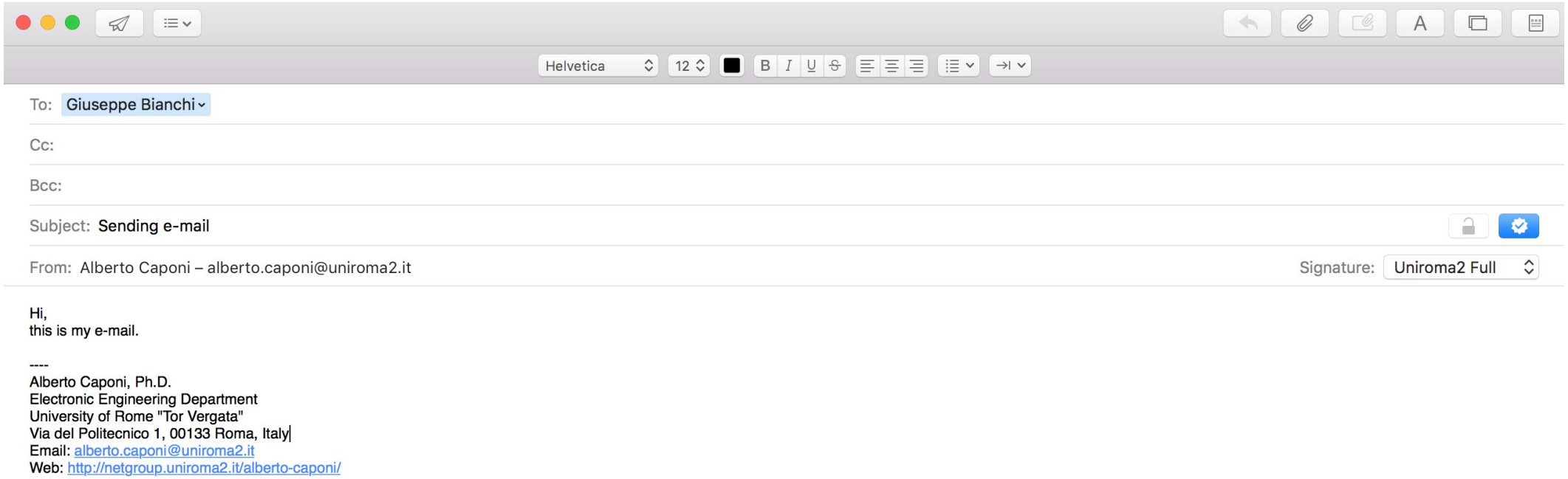

From Name:
Tim Cook
From E-mail:
tim@apple.com
To:
Subject:
Please change your password!
Attachment:
Choose File
No file chosen
Attach another file
Advanced Settings
Content-Type:
text/plain
text/html
Editor
Text:
Hey, I'm Tim Cook.
Please change your apple password right now!
https://apple.com/change-password

Fake Email

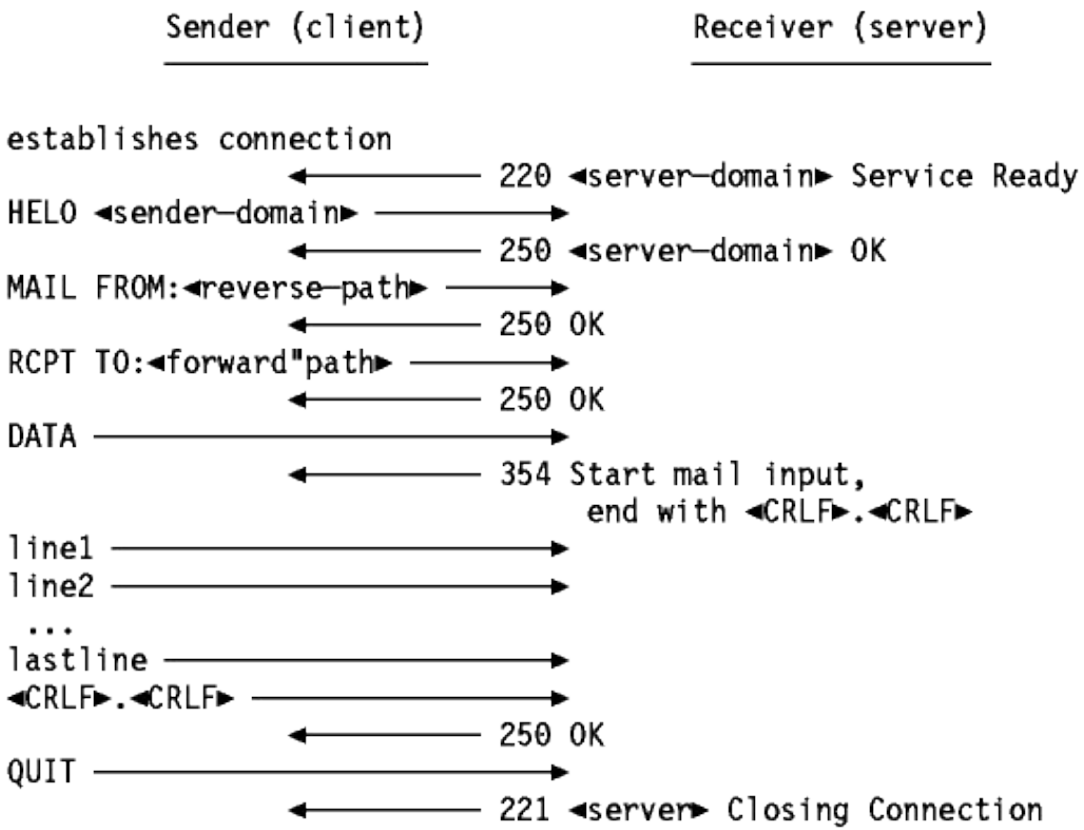

Email
File Edit View Send Help
Date: March 17, 2013
To: Trusting Employee
From: Corporate Information Security
Subject: Emergency Computer Patch <--Please Read ASAP
All,
The company is currently being attacked by a new zero day virus. Our security team has created a patch that should protect employee's computers. To apply the patch please visit the following link and download the missing patch. Once downloaded go ahead and run the patch which will install in the background.
http://zerodaypatch.com
Regards,
Information Security Officer
Your Company


Your Chase Online Access
Chase Online <alerts@chase.alerts.com>
If there are problems with how this message is displayed, click here to view it in a web browser.
Sent: Fri 2/10/2012 4:51 PM
To:
CHASE
Dear Valued JPMorgan Chase Customer,
Due to a recent security check on JPMorgan Chase online banking,we require you to confirm your details by clicking on the Update link below
UPDATE
Failure to do this within 24hrs will lead to access suspension
Sorry for the inconvienence
Regards
JPMorgan Chase Online Banking
Issued for USA use only | 2012 B© JPMorgan Chase

Exploit SMTP Protocol



SMTP Protocol: under the hood



The received header: TELNET

Received: from lmtpproxyd (mailfe00.uniroma2.it [10.1.6.61])
  by mailbe02.uniroma2.it (Cyrus v2.4.12) with LMTPA;
  Wed, 25 Mar 2015 17:45:22 +0100

Received: from mailfe00.uniroma2.it ([unix socket])
  by mailfe00.uniroma2.it (Cyrus v2.4.14) with LMTPA;
  Wed, 25 Mar 2015 17:45:22 +0100

Received: from smtp.uniroma2.it (smtp.uniroma2.it [160.80.6.23])
 by mailfe00.uniroma2.it (8.14.3/8.14.3/Debian-9.4) with ESMTP id t2PGjLAe011484
 for <alberto.caponi@uniroma2.it>; Wed, 25 Mar 2015 17:45:22 +0100

Received: from fake.com ([160.80.103.173])
 by smtp.uniroma2.it (8.13.6/8.13.6) with SMTP id t2PGOcc3015206
 for <alberto.caponi@uniroma2.it>; Wed, 25 Mar 2015 17:25:39 +0100

Date: Wed, 25 Mar 2015 17:24:38 +0100
Message-Id: <201503251625.t2PGOcc3015206@smtp.uniroma2.it>
from: "Fake Boy" <alberto.caponi@fake.com>
to: "Me" <alberto.caponi@uniroma2.it>
subject: I am fake

What do you think about fake mails?

The received header: EMKEI

Received: from lmtpproxyd (mailfe00.uniroma2.it [10.1.6.61])
 by mailbe02.uniroma2.it (Cyrus v2.4.12) with LMTPA;
 Wed, 25 Mar 2015 18:12:18 +0100

Received: from mailfe00.uniroma2.it ([unix socket])
 by mailfe00.uniroma2.it (Cyrus v2.4.14) with LMTPA;
 Wed, 25 Mar 2015 18:12:18 +0100

Received: from mx-02.uniroma2.it (mx-02.uniroma2.it [160.80.6.35])
 by mailfe00.uniroma2.it (8.14.3/8.14.3/Debian-9.4) with ESMTP id t2PHCGP2016971
 for <alberto.caponi@uniroma2.it>; Wed, 25 Mar 2015 18:12:17 +0100

Received: from emkei.cz (emkei.cz [46.167.245.71])
 by mx-02.uniroma2.it (8.14.3/8.14.3/Debian-5+lenny1) with ESMTP id 2PHC6oX002907
 for <alberto.caponi@uniroma2.it>; Wed, 25 Mar 2015 18:12:12 +0100

Received: by emkei.cz (Postfix, from userid 33)
 id D815CD5555; Wed, 25 Mar 2015 18:12:05 +0100 (CET)

The received header: SENDMAIL

Received: from lmtpproxyd (mailfe00.uniroma2.it [10.1.6.61])
 by mailbe02.uniroma2.it (Cyrus v2.4.12) with LMTPA;
 Wed, 25 Mar 2015 18:25:02 +0100

Received: from mailfe00.uniroma2.it ([unix socket])
 by mailfe00.uniroma2.it (Cyrus v2.4.14) with LMTPA;
 Wed, 25 Mar 2015 18:25:02 +0100

Received: from mx-02.uniroma2.it (mx-02.uniroma2.it [160.80.6.35])
 by mailfe00.uniroma2.it (8.14.3/8.14.3/Debian-9.4) with ESMTP id t2PHP1Rk018987
 for <alberto.caponi@uniroma2.it>; Wed, 25 Mar 2015 18:25:02 +0100

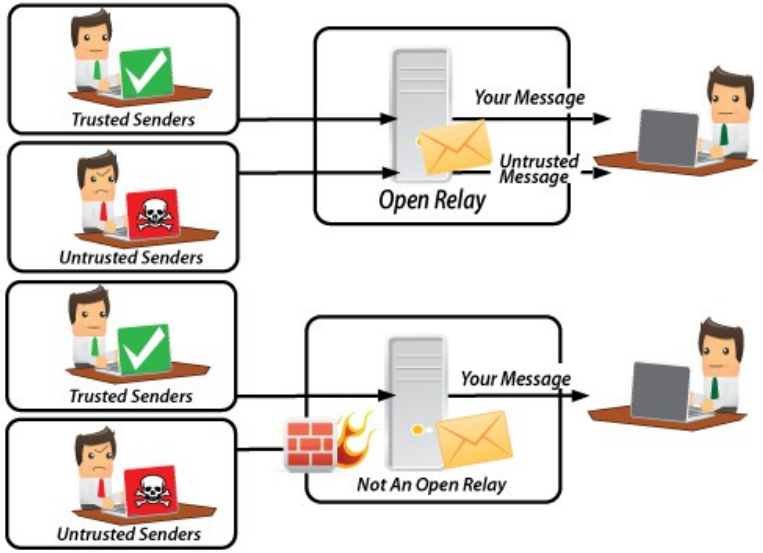
Received: from kali.lan ([160.80.103.173])
 by mx-02.uniroma2.it (8.14.3/8.14.3/Debian-5+lenny1) with ESMTP id t2PHOqa0005145
 for <alberto.caponi@uniroma2.it>; Wed, 25 Mar 2015 18:24:57 +0100

Received: from smtp.uniroma2.it (localhost [127.0.0.1])
 by kali.lan (8.14.4/8.14.4/Debian-4) with SMTP id t2PHMqBa004823
 for <alberto.caponi@uniroma2.it>; Wed, 25 Mar 2015 13:24:00 -0400

Spoofing mails

In order not to be considered "open", an e-mail relay should be secure and configured to accept and forward only the following messages:

- Messages from local IP addresses to local mailboxes
- Messages from local IP addresses to non-local mailboxes
- Messages from non-local IP addresses to local mailboxes
- Messages from clients that are authenticated and authorized



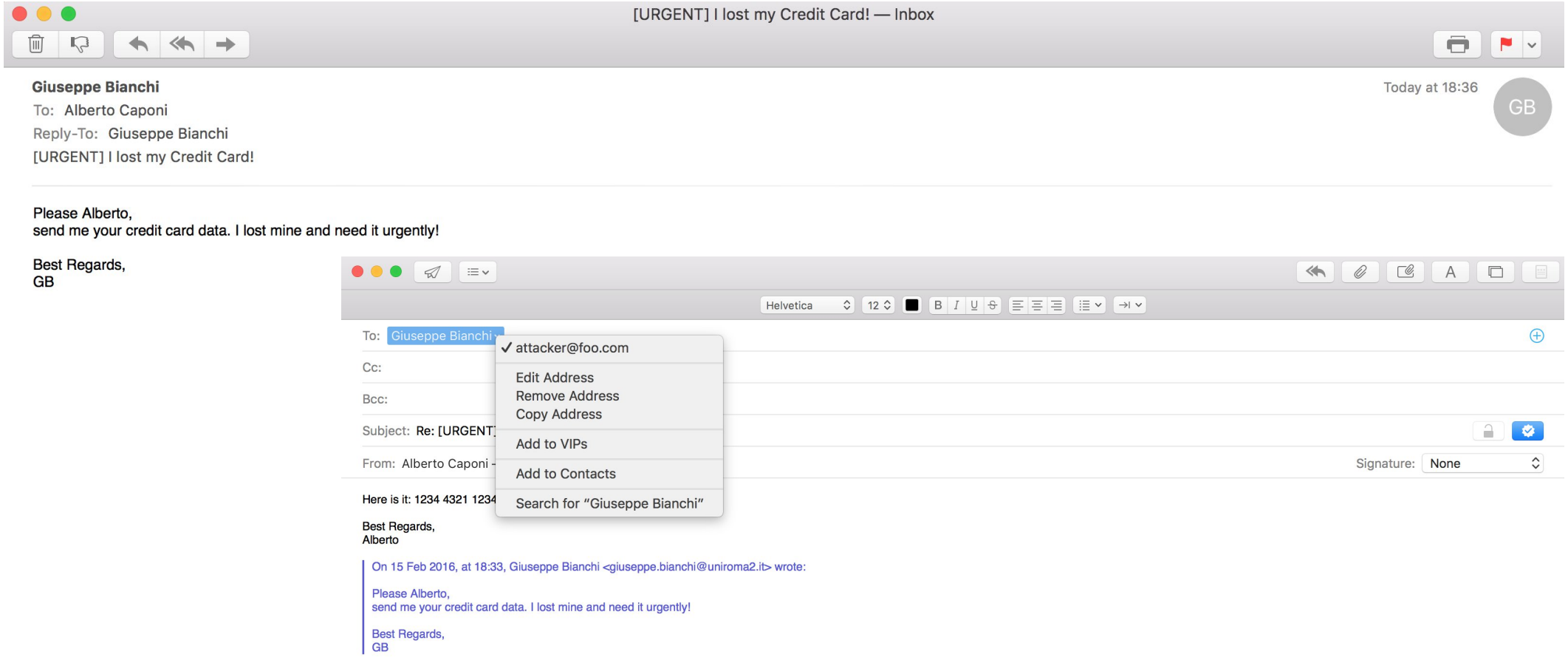
In particular, a properly secured SMTP mail relay should not

- accept and forward arbitrary e-mails from non-local IP addresses to non-local mailboxes
- by an unauthenticated or unauthorized user

No authentication…!

```
macbook-markin:~ markin$ telnet smtp.uniroma2.it 25
Trying 160.80.6.23...
Connected to smtp.uniroma2.it.
Escape character is '^]'.
220 smtp-2015.uniroma2.it ESMTP Sendmail 8.14.4/8.14.4/Debian-8; Mon, 15 Feb 2016 18:33:51 +0100; (No UCE/UBE) logging access from: [160.80.103.191](FA
IL)-[160.80.103.191]
HELO uniroma2.it
250 smtp-2015.uniroma2.it Hello [160.80.103.191], pleased to meet you
MAIL FROM:<giuseppe.bianchi@uniroma2.it>
250 2.1.0 <giuseppe.bianchi@uniroma2.it>... Sender ok
RCPT TO:<alberto.caponi@uniroma2.it>
250 2.1.5 <alberto.caponi@uniroma2.it>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
FROM: Giuseppe Bianchi <giuseppe.bianchi@uniroma2.it>
TO: Alberto Caponi <alberto.caponi@uniroma2.it>
Reply-To: Giuseppe Bianchi <attacker@foo.com>
SUBJECT: [URGENT] I lost my Credit Card!
Please Alberto,
send me your credit card data. I lost mine and need it urgently!

Best Regards,
GB
.
250 2.0.0 u1FHXpT8000719 Message accepted for delivery
quit
221 2.0.0 smtp-2015.uniroma2.it closing connection
Connection closed by foreign host.
macbook-markin:~ markin$
```

No authentication…!

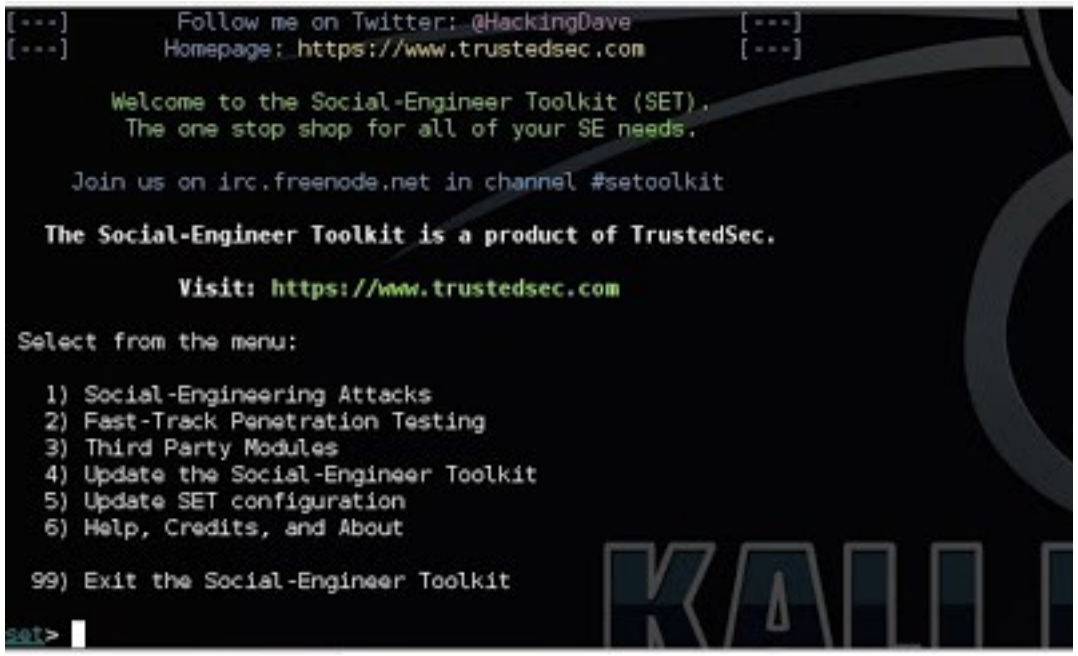


Remote Social Engineering Tactics

Baiting an USB drive named BonusPlan

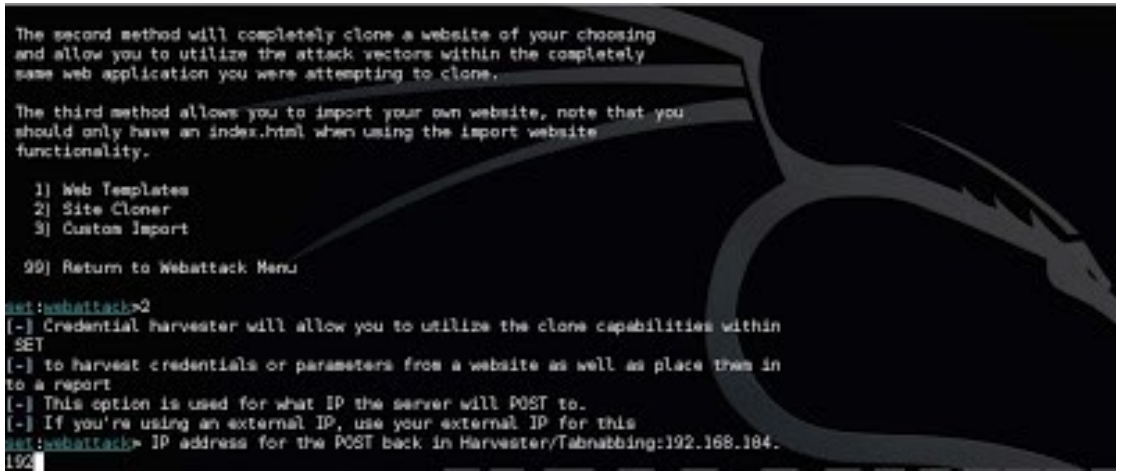
- The analyst will drop USB fobs in areas where employees congregate
- The test focuses on determining if employees will insert unknown removable media into corporate computers
- When inserted, Excel spreadsheets are shown with file names like “BonusPlan2016.xls”
- Excel does not open; the program silently sends the IP address, hostname and username of the individual to a DDI server

Social Engineering Toolkit

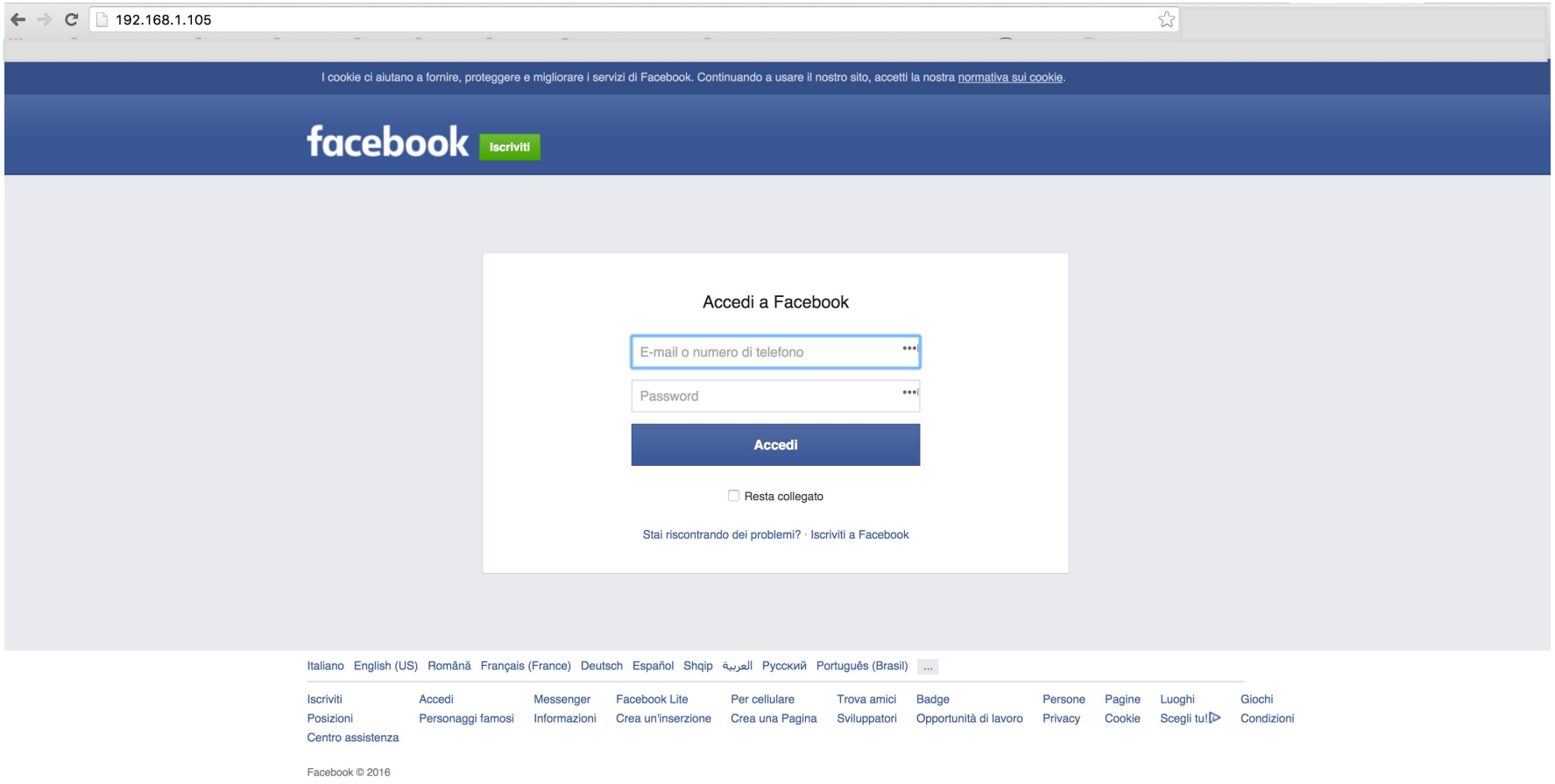


Social Engineering Toolkit

Social Engineering Toolkit



Social Engineering Toolkit



What Is Onsite Social Engineering?

Onsite Social Engineering uses several onsite testing methods, including…

- Attempting to gain physical access to the premises
- Attempting to obtain records, files, equipment, sensitive information, network access, etc.
- Attempting to garner information to permit unauthorized network access

Onsite Social Engineering Tactics

Scenario 1: New Employee

- The analyst pretends to be a new employee and enters through employee entrance
- Will typically have already “cased” the organization and will wear the appropriate attire
- Will already have a fake badge before they come onsite

Onsite Social Engineering Tactics

Scenario 2: Trusted Vendor

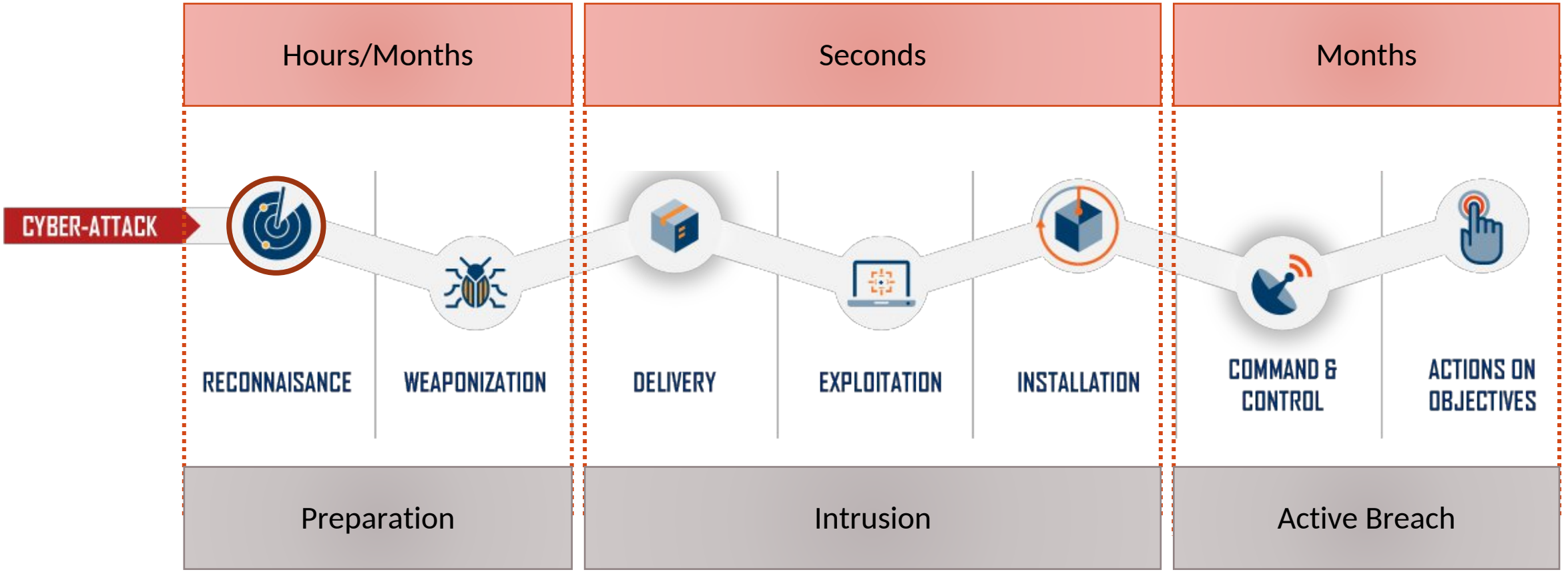
- The analyst pretends to be someone from a trusted vendor such as the local telephone company, A/C repair, etc.
- Will typically have already called in to see what firms the organization uses
- Shirts are easy to buy at local thrift stores or to have made

Onsite Social Engineering: Tailgating

Reconnaissance

OPEN SOURCE INFORMATION GATHERING: OSINT

How a cyber-attack starts?



The Killchain model

Step 1: Reconnaissance. The attacker gathers information on the target before the actual attack starts. He can do it by looking for publicly available information on the Internet.

Step 2: Weaponization. The attacker uses an exploit and creates a malicious payload to send to the victim. This step happens at the attacker side, without contact with the victim.

Step 3: Delivery. The attacker sends the malicious payload to the victim by email or other means, which represents one of many intrusion methods the attacker can use.

Step 4: Exploitation. The actual execution of the exploit, which is, again, relevant only when the attacker uses an exploit.

Step 5: Installation. Installing malware on the infected computer is relevant only if the attacker used malware as part of the attack, and even when there is malware involved, the installation is a point in time within a much more elaborate attack process that takes months to operate.

Step 6: Command and control. The attacker creates a command and control channel in order to continue to operate his internal assets remotely. This step is relatively generic and relevant throughout the attack, not only when malware is installed.

Step 7: Exfiltration. The attacker performs the steps to achieve his actual goals inside the victim's network. This is the elaborate active attack process that takes months, and thousands of small steps, in order to achieve.

Reconnaissance

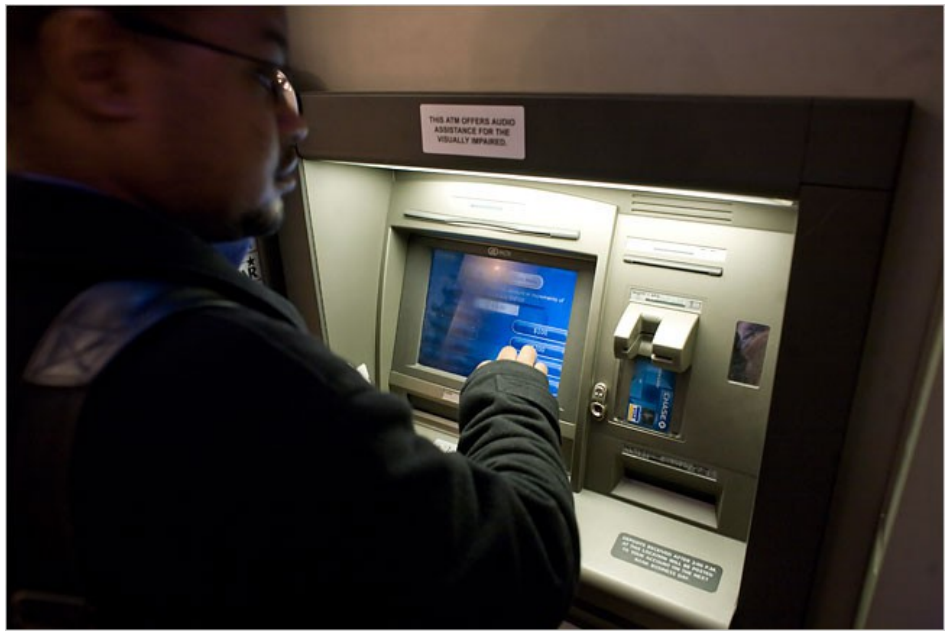
"The attacker gathers information on the target before the actual attack starts. He can do it by looking for publicly available information on the Internet."

Passive Information Gathering / Open Source Intelligence (OSINT)

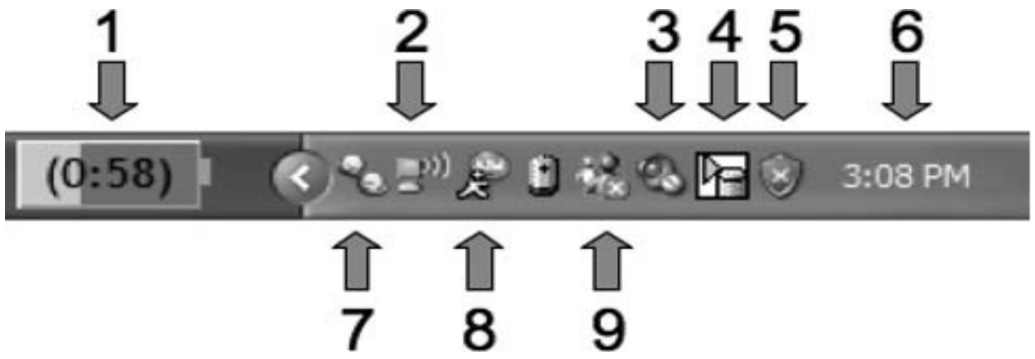
- Finding, selecting, and acquiring information from publicly available sources
- Never sending any traffic to the target organization neither from one of our hosts or "anonymous" hosts or services across the Internet
- Can only use and gather archived or stored information
- Can be out of date or incorrect as we are limited to results gathered from a third party

Active Information Gathering

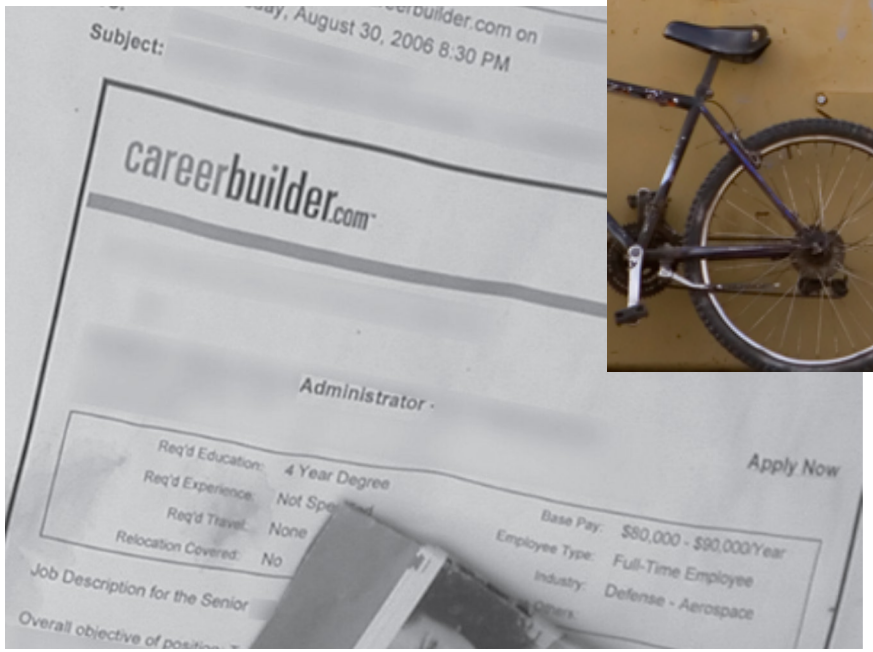
Reconnaissance: Shoulder Surfing

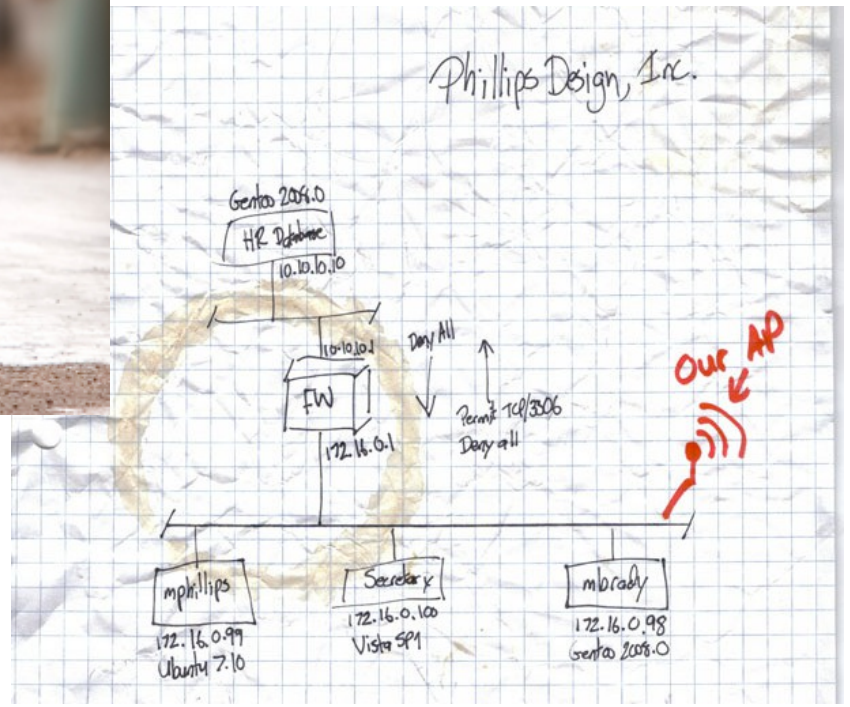


Reconnaissance: Shoulder Surfing

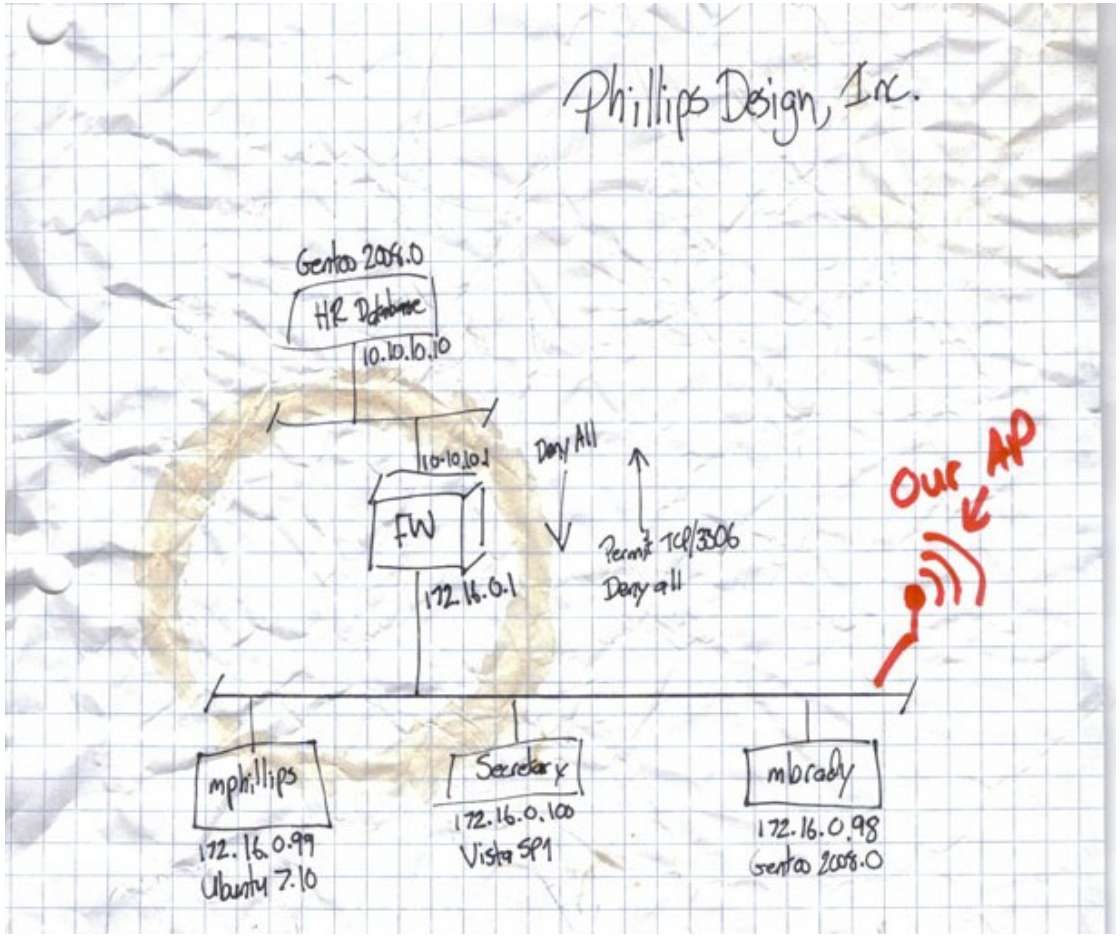


Reconnaissance: Dumpster Diving



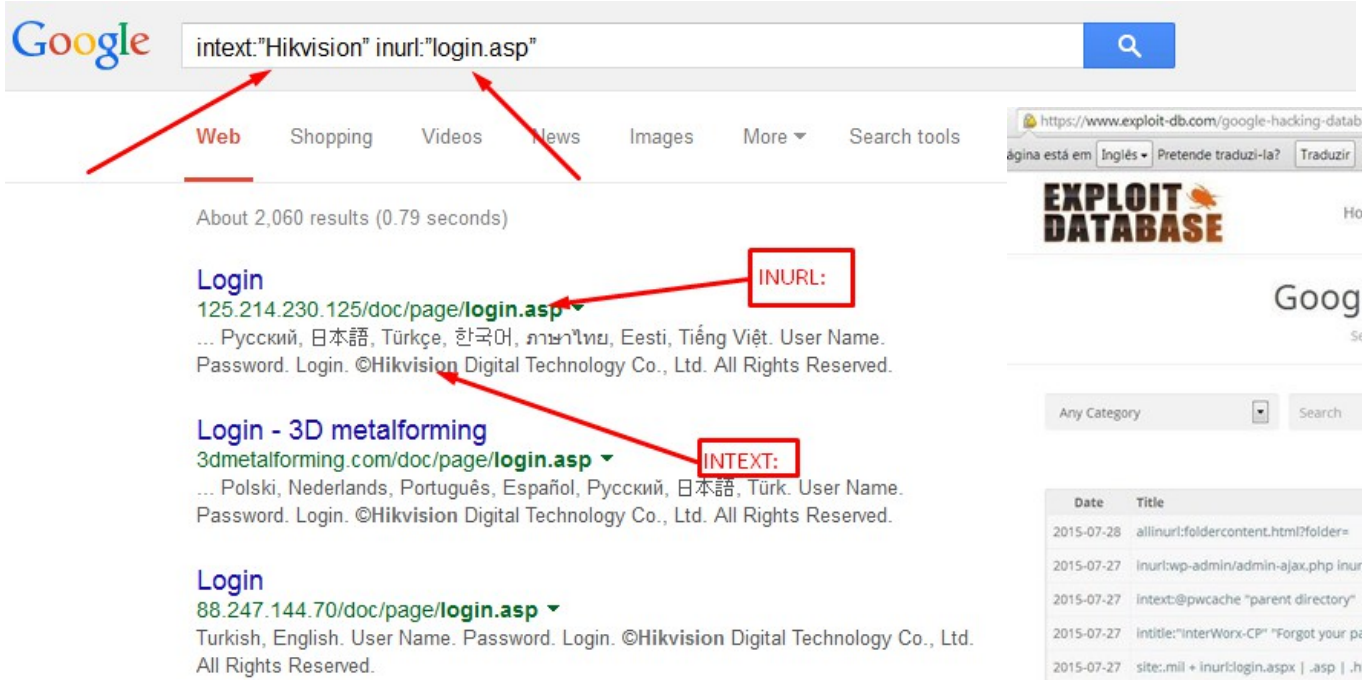


Reconnaissance: Dumpster Diving



Reconnaissance: Being a magician

Reconnaissance: Google Dorking



Reconnaissance: Google Dorking

filetype:pdf|txt|sql|...

allintext:”define('DB_PASSWORD',”

- Searches for multiple words within the body text of indexed pages. This is used in a similar fashion to allinurl:

allintitle:

- This works like intitle: but searches for multiple words in the title. For instance, use allintitle: channel conflict online retail to search for documents that contain all four of those words in the title. Note that there is a space after the colon when using this operator.

inanchor:

- The inanchor: operator will restrict your search to pages where the underlined text of inbound links matches your search word. For example, if you wanted to search for HTML site maps but confine your search to those pages with links that say “site map”, inanchor:”site map” would do the trick, since most sites link to their own site maps using the link text of “Site Map.”

allinanchor:

- This works like inanchor: but searches for multiple words in the anchor text. For example, the query seo tool allinanchor: download trial would invoke a search for pages relating to SEO tools that have the words download and trial in the anchor text.

inurl:”admin.php”

- Use the inurl: operator to restrict the search results to pages that contain a particular word in the URL. This can be especially useful if you want Google to display all the pages it has found with a particular script name, such as inurl:ToolPage site:www.vfinance.com. Again, there is no space after the colon when using this operator.

Reconnaissance: Google Dorking

allinurl:

This operator is similar in function to the inurl: operator but is used for finding multiple words in the URL. It eliminates the need to keep repeating inurl: in front of every word you want to search for in the URL. For instance, *allinurl: china exporting* is an equivalent and more concise form of the query*inurl:china inurl:exporting* to find Web pages that contain the words china and exporting anywhere in the URL, including the filename, directory names, extension, or domain. There *IS* a space after the colon when using the *allinurl:* operator.

intext:

Searches for a word in the main body text. This is used in a similar fashion to *inurl:*.

cache:

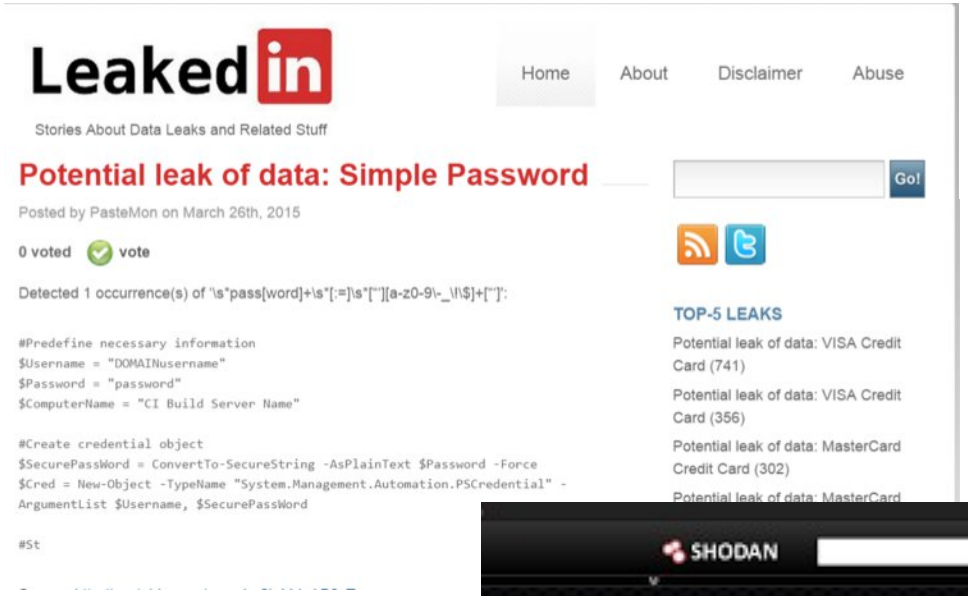
The cache: operator provides a snapshot view of a Web page as it looked when Googlebot last visited the page. Follow this operator with a Web address, such as cache:www.covario.com to view the page that Google has cached. Note that Googlebot must have downloaded the page in order for this to work.

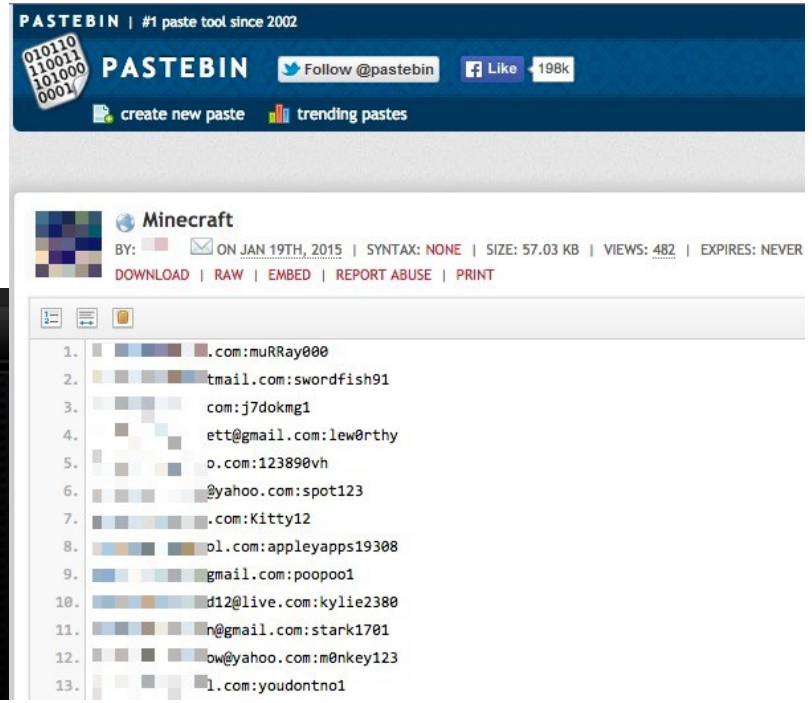
site:

You can search within a site or a domain by adding the site: operator followed by a site's domain name to your query. For example, you could search for me but restrict your search to only pages within the site with a query of *your name site:www.yoursitecom*. You can also add a subdirectory to the end of the domain in a site: query. For example *seo site:www.yourname/what-we-do/*. You can restrict your search to .com sites with site:com, to .gov sites with site:gov, or to .co.uk with site:co.uk. Combining Boolean logic with the site: operator will allow you to search within multiple sites simultaneously. For instance, *search marketing (site:marketingprofs.com | site:marketingsherpa.com | site:marketingpower.com)* searches the three sites simultaneously.

Use the site: operator by itself without other search words to get a list of all pages indexed, such as *site:actionableinsights.covario.com*. Again, note that there is no space after the colon when using this operator.

Reconnaissance: Online Platforms





Reconnaissance: ShodanHQ

SHODAN is a search engine that lets you find specific computers (routers, servers, etc.) using a variety of filters. Some have also described it as a public port scan directory or a search engine of banners.

- If you're interested in finding computers running a certain piece of software (such as Apache)
- If you want to know which version of Microsoft IIS is the most popular
- You want to see how many anonymous FTP servers there are
- A new vulnerability came out and you want to see how many hosts it could infect
  - *Look for specific brand of hardware (e.g. CISCO, TP-LINK, etc.)…*
  - *Spcific model…*
  - *In specific country (e.g. IT, US, UK, etc.)…*
  - *Etc…*

Reconnaissance: Cached Websites

There are times when we will be unable to access web site information due to the fact that the content may no longer be available from the original source.

- Being able to access archived copies of this information allows access to past information.

Perform Google searches using specially targeted search strings:

cache:<site.com>

Use the archived information from the Wayback Machine

http://www.archive.org

Reconnaissance: Job Openings

Bayt, http://bayt.com

Monster, http://www.monster.com

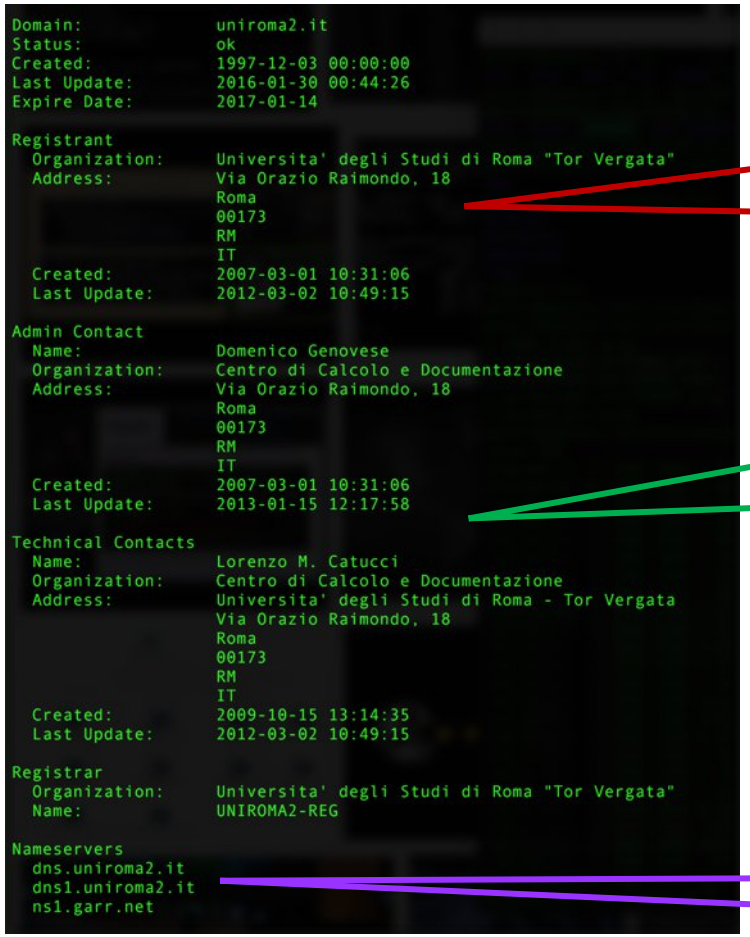
CareerBuilder, http://www.careerbuilder.com

Computerjobs.com, http://www.computerjobs.com

Indeed, LinkedIn, etc

Reconnaissance: Social Networks

Reconnaissance: Whois



```
Domain:             uniroma2.it
Status:             ok
Created:            1997-12-03 00:00:00
Last Update:        2016-01-30 00:44:26
Expire Date:        2017-01-14

Registrant
  Organization:     Universita' degli Studi di Roma "Tor Vergata"
  Address:          Via Orazio Raimondo, 18
                    Roma
                    00173
                    RM
                    IT
  Created:          2007-03-01 10:31:06
  Last Update:      2012-03-02 10:49:15

Admin Contact
  Name:             Domenico Genovese
  Organization:     Centro di Calcolo e Documentazione
  Address:          Via Orazio Raimondo, 18
                    Roma
                    00173
                    RM
                    IT
  Created:          2007-03-01 10:31:06
  Last Update:      2013-01-15 12:17:58

Technical Contacts
  Name:             Lorenzo M. Catucci
  Organization:     Centro di Calcolo e Documentazione
  Address:          Universita' degli Studi di Roma - Tor Vergata
                    Via Orazio Raimondo, 18
                    Roma
                    00173
                    RM
                    IT
  Created:          2009-10-15 13:14:35
  Last Update:      2012-03-02 10:49:15

Registrar
  Organization:     Universita' degli Studi di Roma "Tor Vergata"
  Name:             UNIROMA2-REG

Nameservers
  dns.uniroma2.it
  dns1.uniroma2.it
  ns1.garr.net
```

Registrant:
targetcompany (targetcompany.com)
Street Address
City, Province
State, Pin, Country
Domain Name: **targetcompany.com**

Administrative Contact:
Surname, Name (SNIDNo-ORG)
t**argetcompany@domain.com**
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

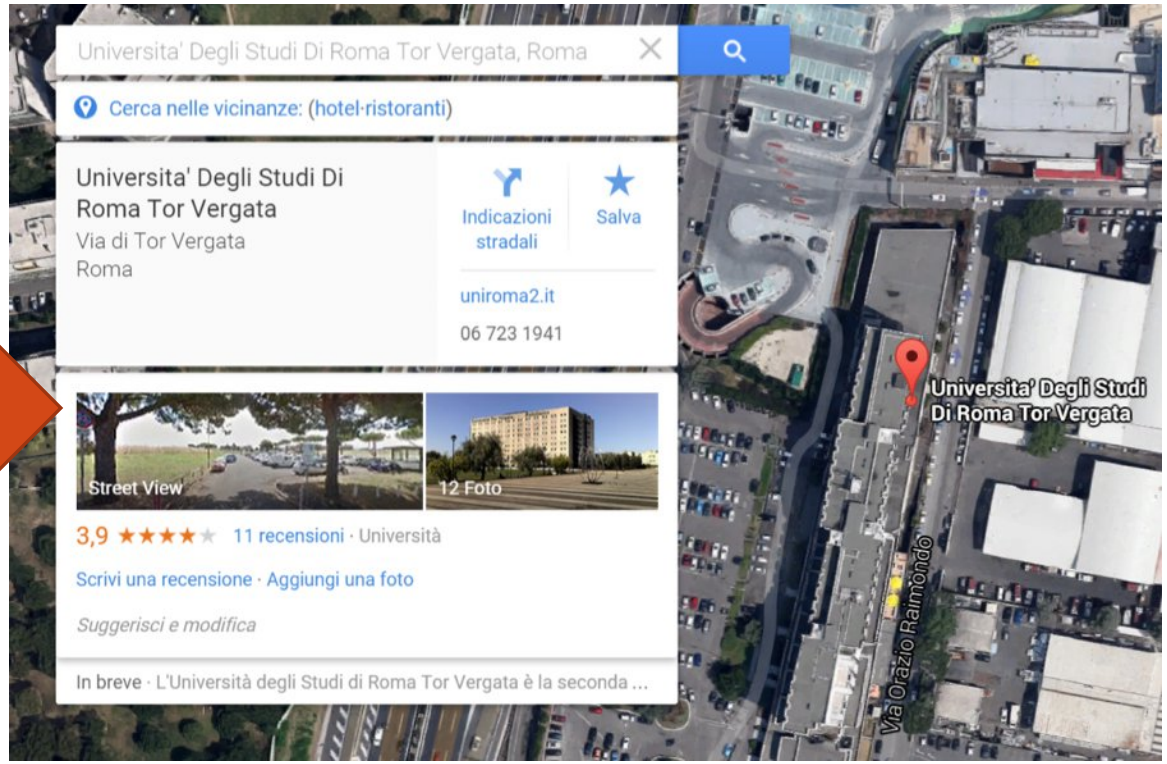
Technical Contact:
Surname, Name (SNIDNo-ORG)
t**argetcompany@domain.com**
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Domain servers in listed order:

NS1.WEBHOST.COM	**XXX.XXX.XXX.XXX**
NS2.WEBHOST.COM	**XXX.XXX.XXX.XXX**

Reconnaissance: Whois

```
Domain:             uniroma2.it
Status:             ok
Created:            1997-12-03 00:00:00
Last Update:        2016-01-30 00:44:26
Expire Date:        2017-01-14

Registrant
  Organization:     Universita' degli Studi di Roma "Tor Vergata"
  Address:          Via Orazio Raimondo, 18
                    Roma
                    00173
                    RM
                    IT
  Created:          2007-03-01 10:31:06
  Last Update:      2012-03-02 10:49:15

Admin Contact
  Name:             Domenico Genovese
  Organization:     Centro di Calcolo e Documentazione
  Address:          Via Orazio Raimondo, 18
                    Roma
                    00173
                    RM
                    IT
  Created:          2007-03-01 10:31:06
  Last Update:      2013-01-15 12:17:58

Technical Contacts
  Name:             Lorenzo M. Catucci
  Organization:     Centro di Calcolo e Documentazione
  Address:          Universita' degli Studi di Roma - Tor Vergata
                    Via Orazio Raimondo, 18
                    Roma
                    00173
                    RM
                    IT
  Created:          2009-10-15 13:14:35
  Last Update:      2012-03-02 10:49:15

Registrar
  Organization:     Universita' degli Studi di Roma "Tor Vergata"
  Name:             UNIROMA2-REG

Nameservers
  dns.uniroma2.it
  dns1.uniroma2.it
  ns1.garr.net
```



Reconnaissance: e-mails

Kind regards,
Name here

YOUR COMPANY
slogan here

Business Name Here
Address: 17 Main Street, Brisbane QLD 4000
PO Box 123, Brisbane QLD 4000
Phone: (07) 5484 4444
Mobile: 0400 000 000
Email: name@domainname.com.au
Website: www.domainname.com.au

Disclaimer here ... Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Reconnaissance: e-mail's header

Content-Type: multipart/mixed; boundary="------------040401080402030904040900"
Mime-Version: 1.0
X-Mailscanner-From: [redacted]@uniroma2.it
Return-Path: <[redacted]@uniroma2.it>
X-Sieve: CMU Sieve 2.4
X-Sieve: CMU Sieve 2.4
In-Reply-To: <517FBD3B.9060407@uniroma2.it>
X-Mailscanner-Information: Please contact the ISP for more information
X-Mailscanner: Found to be clean
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.9) Gecko/20100722 Eudora/3.0.4
Received: from lmtpproxyd (mailfe00.uniroma2.it [10.1.6.61]) by mailbe02.uniroma2.it (Cyrus v2.4.12) with LMTPA; Tue, 30 Apr 2013 16:25:08 +0200
Received: from mailfe00.uniroma2.it ([unix socket]) by mailfe00.uniroma2.it (Cyrus v2.4.14) with LMTPA; Tue, 30 Apr 2013 16:25:08 +0200
Received: from smtp.uniroma2.it (smtp.uniroma2.it [160.80.6.23]) by mailfe00.uniroma2.it (8.14.3/8.14.3/Debian-9.4) with ESMTP id r3UEP69v017639 for <alberto.caponi@uniroma2.it>; Tue, 30 Apr 2013 16:25:07 +0200
Received: from smtpauth.uniroma2.it (smtpauth.uniroma2.it [160.80.6.46]) by smtp.uniroma2.it (8.13.6/8.13.6) with ESMTP id r3UDCWIl007699 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=FAIL) for <alberto.caponi@uniroma2.it>; Tue, 30 Apr 2013 15:12:33 +0200
Received: from [160.80.82.29] ([160.80.82.29]) (authenticated bits=0) by smtpauth.uniroma2.it (8.14.3/8.14.3/Debian-9.4) with ESMTP id r3UEOwou018495 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <alberto.caponi@uniroma2.it>; Tue, 30 Apr 2013 16:24:59 +0200
Message-Id: <517FD438.6000002@uniroma2.it>
References: <517FA0D4.4030107@uniroma2.it> <517FBD3B.9060407@uniroma2.it>

E-mail’s header

Content-Type: multipart/mixed; boundary="------------040401080402030904040900"
Mime-Version: 1.0
X-Mailscanner-From: [redacted]@uniroma2.it
Return-Path: <[redacted]@uniroma2.it>
X-Sieve: CMU Sieve 2.4
X-Sieve: CMU Sieve 2.4
In-Reply-To: <517FBD3B.9060407@uniroma2.it>
X-Mailscanner-Information: Please contact the ISP for more information
X-Mailscanner: Found to be clean
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.9) Gecko/20100722 Eudora/3.0.4
Received: from lmtpproxyd (mailfe00.uniroma2.it [10.1.6.61]) by mailbe02.uniroma2.it (Cyrus v2.4.12) with LMTPA; Tue, 30 Apr 2013 16:25:08 +0200
Received: from mailfe00.uniroma2.it ([unix socket]) by mailfe00.uniroma2.it (Cyrus v2.4.14) with LMTPA; Tue, 30 Apr 2013 16:25:08 +0200
Received: from smtp.uniroma2.it (smtp.uniroma2.it [160.80.6.23]) by mailfe00.uniroma2.it (8.14.3/8.14.3/Debian-9.4) with ESMTP id r3UEP69v017639 for <alberto.caponi@uniroma2.it>; Tue, 30 Apr 2013 16:25:07 +0200
Received: from smtpauth.uniroma2.it (smtpauth.uniroma2.it [160.80.6.46]) by smtp.uniroma2.it (8.13.6/8.13.6) with ESMTP id r3UDCWll007699 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=FAIL) for <alberto.caponi@uniroma2.it>; Tue, 30 Apr 2013 15:12:33 +0200
Received: from [160.80.82.29] ([160.80.82.29]) (authenticated bits=0) by smtpauth.uniroma2.it (8.14.3/8.14.3/Debian-9.4) with ESMTP id r3UEOwou018495 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for <alberto.caponi@uniroma2.it>; Tue, 30 Apr 2013 16:24:59 +0200
Message-Id: <517FD438.6000002@uniroma2.it>
References: <517FA0D4.4030107@uniroma2.it> <517FBD3B.9060407@uniroma2.it>

Exercise

Choose an organization and use Google to gather as much information as possible about it

- Use the Google ***filetype*** search operator and look for interesting documents from the target organization
- Re-do the exercise on your company's domain. Can you find any data leakage you were not aware of?

The Harvester

Email harvesting useful to find e-mails, and possibly usernames, belonging to an organization.

These emails are useful in many ways

- providing us a potential list for client side attacks
- revealing the naming convention used in the organization
- mapping out users in the organization.

One of the tools in Kali Linux that can preform this task is **theharvester**

- Can search Google, Bing, and other sites for email addresses

- **theharvester -d <domain> -b google**
- **theharvester -d <domain> -b bing**
- **theharvester -d <domain> -b all -h**

Recon NG

Recon NG is a full featured web reconnaissance framework

- Complete with independent modules
- Database interaction
- Built-in convenience functions
- Look and feel similar to the Metasploit Framework

- **show modules**

- **use recon/domains-contacts/whois_pocs**
- **use recon/domains-hosts/hackertarget**
- **use recon/domains-hosts/google_site_web**

Vulnerabilità e Difesa dei Sistemi Internet

ACTIVE RECONNAISSANCE

Reconnaissance

"The attacker gathers information on the target before the actual attack starts. He can do it by looking for publicly available information on the Internet."

Passive Information Gathering / Open Source Intelligence (OSINT)

- Finding, selecting, and acquiring information from publicly available sources
- Never sending any traffic to the target organization neither from one of our hosts or "anonymous" hosts or services across the Internet
- Can only use and gather archived or stored information
- Can be out of date or incorrect as we are limited to results gathered from a third party

Active Information Gathering

- During this stage we are actively mapping network infrastructure
- Actively enumerating and/or vulnerability scanning the open services
- Actively searching for unpublished directories, files, and servers

Hosts discovery

EXPLOITING THE DNS

Reconnaissance

"The attacker gathers information on the target before the actual attack starts. He can do it by looking for publicly available information on the Internet."

Passive Information Gathering / Open Source Intelligence (OSINT)

- Finding, selecting, and acquiring information from publicly available sources
- Never sending any traffic to the target organization neither from one of our hosts or "anonymous" hosts or services across the Internet
- Can only use and gather archived or stored information
- Can be out of date or incorrect as we are limited to results gathered from a third party

Active Information Gathering

- During this stage we are actively mapping network infrastructure
- Actively enumerating and/or vulnerability scanning the open services
- Actively searching for unpublished directories, files, and servers

Domain Name System

On ARPANet, host names were mapped to IP addresses in a “hosts” file stored on a single server

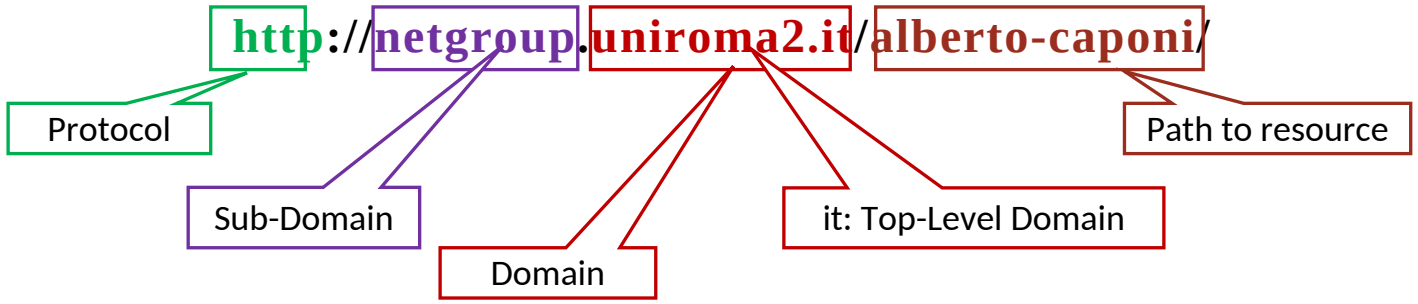
- Other machines downloaded copies of hosts.txt periodically
- Unix stored this information in /etc/hosts
- This technique didn't scale well…DNS started in 1983

1. Distributed storage
   - DNS data split across many servers
   - Smaller storage requirements for each server
   - Faster transfer of information
   - No single point of failure
2. Hierarchical organization of data
   - Allows local control of names and avoids name conflicts

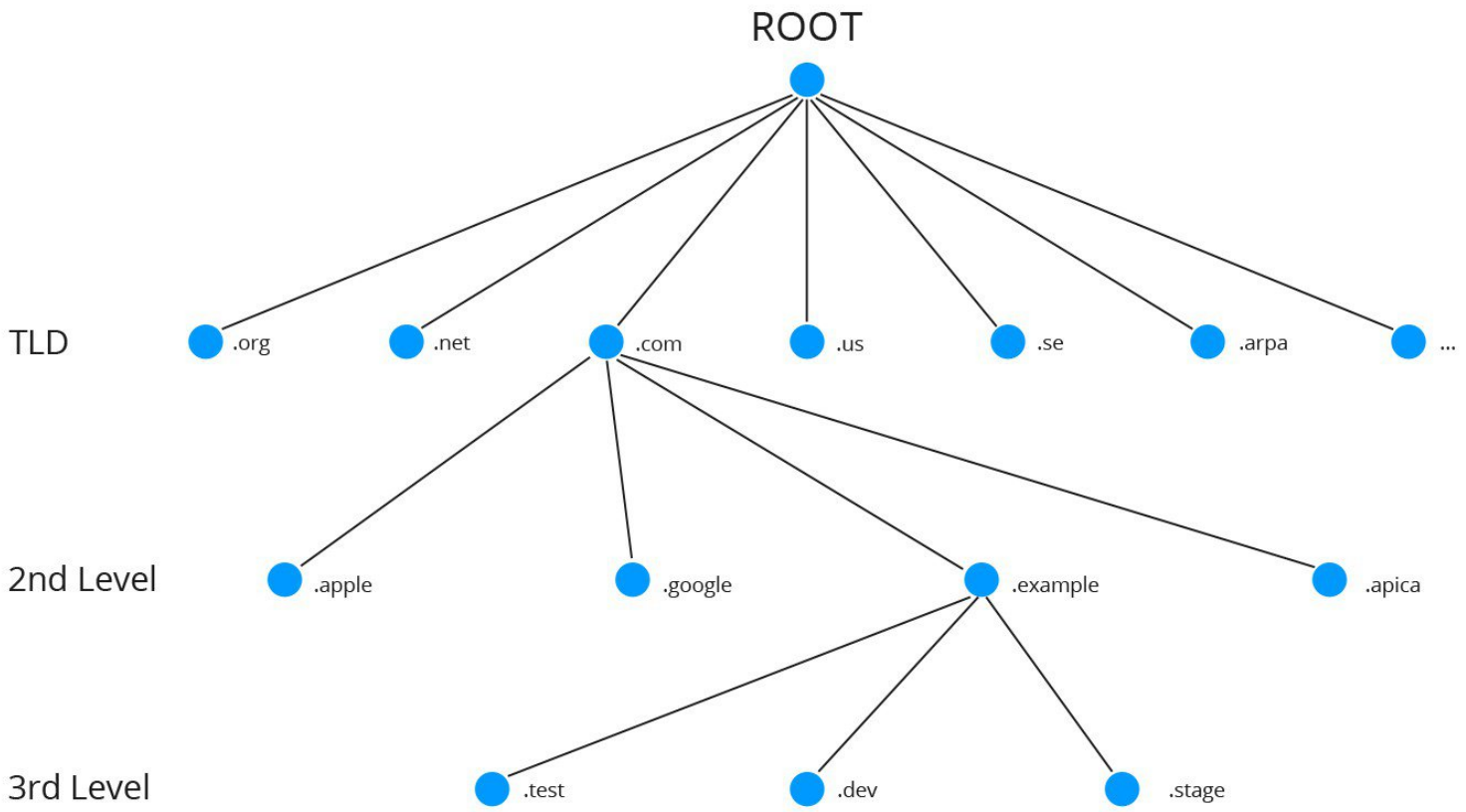
Where we use DNS?

a resource (i.e a file), specified by a
URL: Uniform Resource Locator.

e.g. my home page:



Hierarchical DNS Namespace

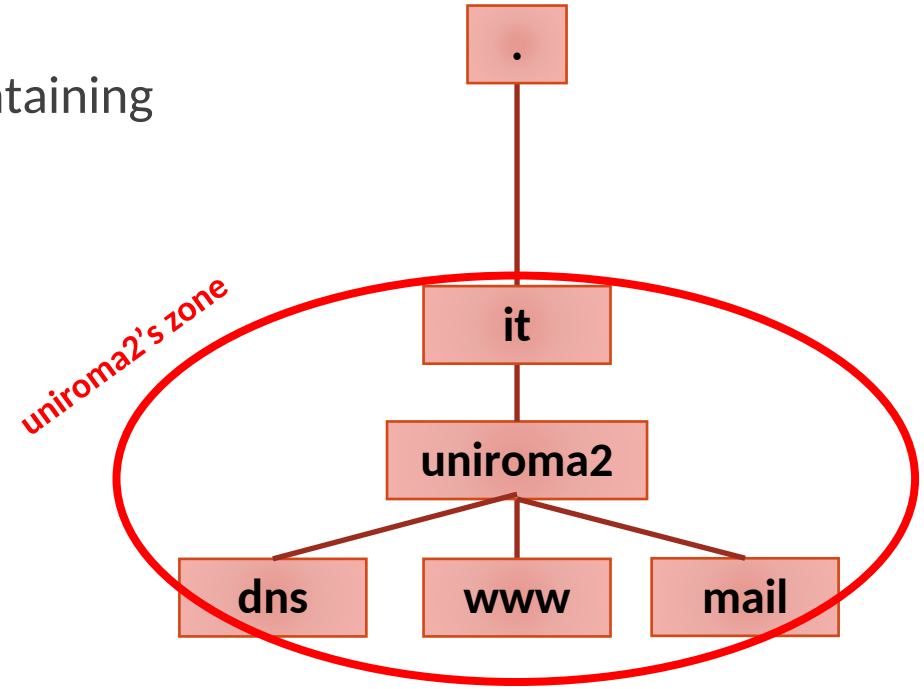


DNS Zones

Data for a domain and all or some of its subdomains is called a zone

All of uniroma2 could be one zone, containing

- dns.uniroma2.it
- www. uniroma2.it
- mail.uniroma2.it



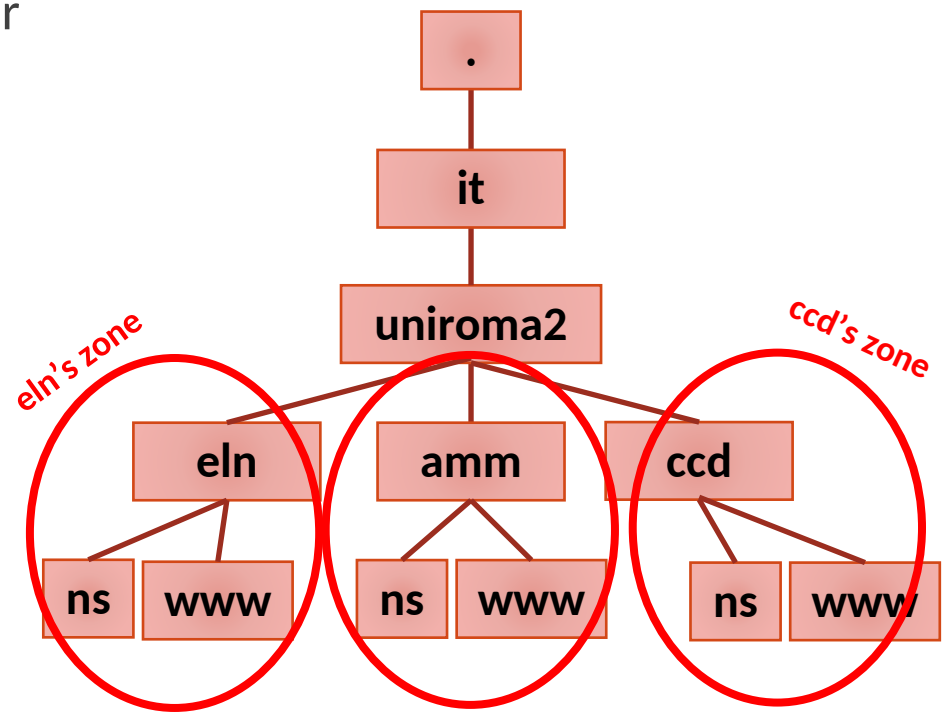
DNS Zones

Uniroma2 could have separate nameservers on each department, each responsible for their own subdomain

The parent domain would delegate responsibility for a subdomain to each department, making many zones

URLs would be longer

- www.eln.uniroma2.it
- ftp.netgroup.uniroma2.it



DNS Clients, Servers, and Resolvers

DNS Client

- A program like a Web browser using a domain name like www.uniroma2.it

DNS Server

- Stores and serves DNS data

DNS Resolver

- Software that accepts a query from a client, queries one or more DNS servers, and replies to the client

DNS Queries

Recursive query

- Server will find the answer, even if it has to query other servers to get it
- Server will not respond with a referral to another server

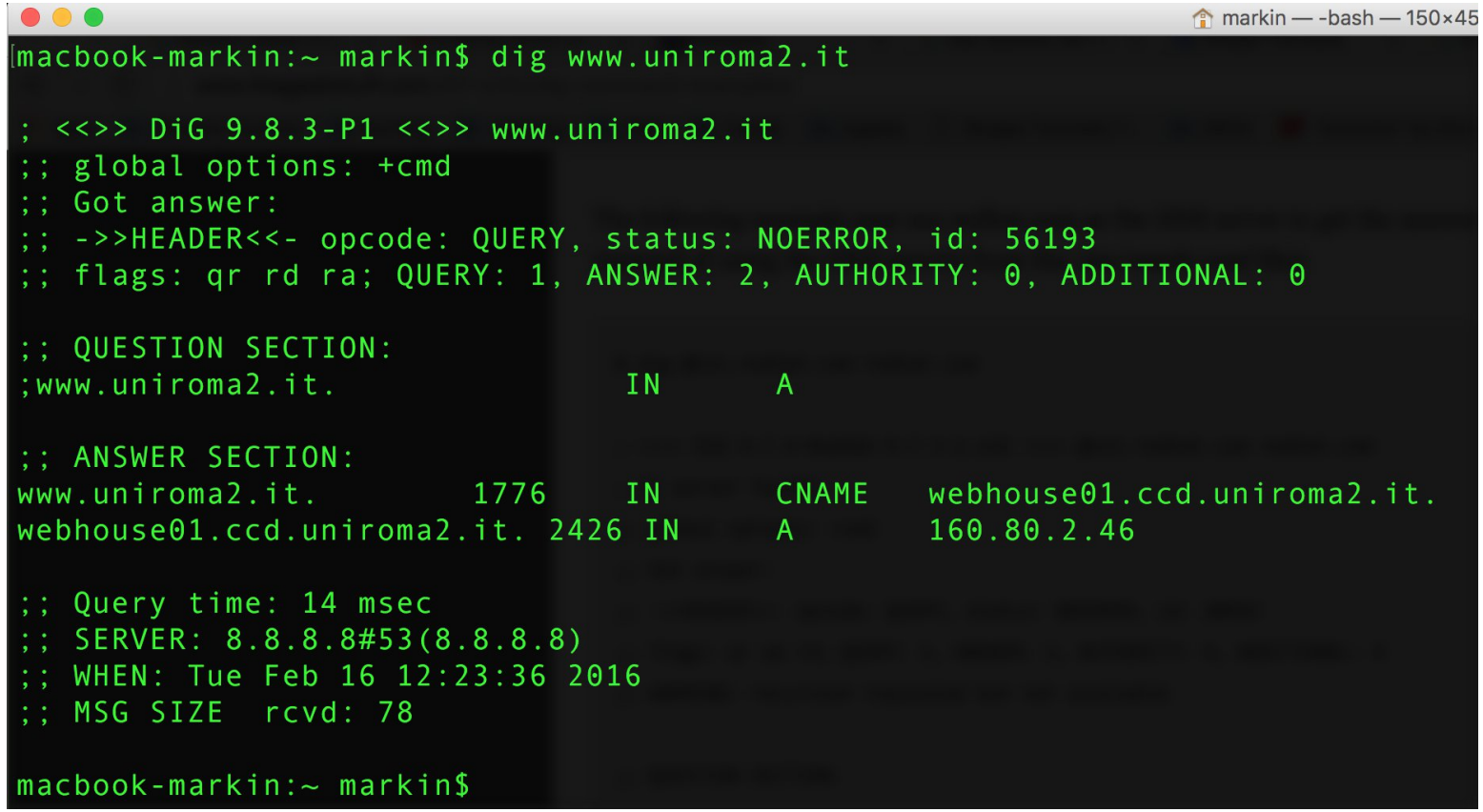
Iterative query

- If server does not have the answer, it will send a referral to another DNS server
- Requester has to send another query to hunt for the answer

Common Record Types

Type	Description
A	IPv4 address of host
AAAA	IPv6 address of host
MX	Mail exchange
PTR	Host name corresponding to IP address. Unlike a CNAME, DNS processing stops and just the name is returned.
NS	Host name of SOA name server. Delegates a DNS zone to use the given authoritative name servers.
CNAME	Canonical Name: alias of one name to another. The DNS lookup will continue by retrying the lookup with the new name.
SOA	Identifies the DNS server responsible for the domain information, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.
TXT	General human-readable information

Interacting with DNS



Dig for DNS Info

The domain information groper, or dig, is a command that is built into every distribution of Linux and UNIX.

- It is designed to be able to grab and display for the user key DNS info.
- Let's open a terminal and start digging!

- ***dig hostname***
- ***dig hostname record-name***
- ***dig @dns-server hostname record-name***
- ***dig @dns-server hostname any***

Dig for DNS Info

```
markin@alberto-UX31E:~$ dig @dns.uniroma2.it uniroma2.it any

; <<>> DiG 9.9.5-4.3ubuntu0.2-Ubuntu <<>> @dns.uniroma2.it uniroma2.it any
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19417
;; flags: qr aa rd; QUERY: 1, ANSWER: 10, AUTHORITY: 0, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uniroma2.it.                   IN      ANY

;; ANSWER SECTION:
uniroma2.it.            3600    IN      NAPTR   2 0 "s" "SIP+D2U" "" _sip._udp.uniroma2.it.
uniroma2.it.            3600    IN      MX      25 mx-03.uniroma2.it.
uniroma2.it.            3600    IN      MX      25 mx-04.uniroma2.it.
uniroma2.it.            3600    IN      MX      20 mx-01.uniroma2.it.
uniroma2.it.            3600    IN      MX      20 mx-02.uniroma2.it.
uniroma2.it.            3600    IN      MX      20 mx-05.uniroma2.it.
uniroma2.it.            3600    IN      SOA     dns.uniroma2.it. postmaster.uniroma2.it. 2015033000 86400 7200 604800 86400
uniroma2.it.            3600    IN      NS      ns1.garr.net.
uniroma2.it.            3600    IN      NS      dns1.uniroma2.it.
uniroma2.it.            3600    IN      NS      dns.uniroma2.it.

;; ADDITIONAL SECTION:
mx-01.uniroma2.it.      3600    IN      A       160.80.6.34
mx-02.uniroma2.it.      3600    IN      A       160.80.6.35
mx-05.uniroma2.it.      3600    IN      A       160.80.6.38
mx-03.uniroma2.it.      3600    IN      A       160.80.6.36
mx-04.uniroma2.it.      3600    IN      A       160.80.6.37
dns.uniroma2.it.        3600    IN      A       160.80.1.3
dns.uniroma2.it.        3600    IN      AAAA    2001:760:4016:1::3
dns1.uniroma2.it.       3600    IN      A       160.80.5.8
_sip._udp.uniroma2.it.  3600    IN      SRV     0 0 5060 proxysip.ccd.uniroma2.it.

;; Query time: 11 msec
;; SERVER: 160.80.1.3#53(160.80.1.3)
;; WHEN: Thu Apr 09 00:27:46 CEST 2015
;; MSG SIZE  rcvd: 494
```

Interacting with DNS

A DNS server will usually divulge

- DNS and mail server information for the domain it has authority over.
- This is a necessity, as public requests for mail and DNS server addresses make up the basic Internet experience

- **host -t ns megacorpone.com**
- **host -t mx megacorpone.com**

Lookup for specific hosts:

- **host www.megacorpone.com**
- **host manager.megacorpone.com**

Forward Lookup Bruteforce

We can automate the DNS Lookup of common host names

- Bash script the lookup
- Guess valid names of servers by attempting to resolve a given name
- If the name you have guessed does resolve, the results might indicate the presence and even functionality of the server

- **echo www > list.txt**
- **echo ftp >> list.txt**
- **echo mail >> list.txt**
- **echo proxy >> list.txt**
- **echo router >> list.txt**
- **for ip in $(cat list.txt);do host $ip.megacorpone.com;done**

Reverse Lookup Bruteforce

If the DNS administrator of configured PTR records for the domain

- We might find out some more domain names that were missed during the forward lookup brute force phase
- By probing the range of IP addresses in a loop

- **for ip in $(seq 1 255);do host 38.100.193.$ip;done | grep -v "not found”**
- …add | grep megacorpone

DNS Zone Transfer

DNS Zone transfer is the process where a DNS server passes a copy of part of it's database (a zone) to another DNS server.

- It's how you can have more than one DNS server able to answer queries about a particular zone
- There is a Master DNS server and Slave DNS servers
  - the slave asks he master for a copy of the records for that zone.

A basic DNS Zone Transfer Attack

- Just pretend you're a slave, ask the master for a copy of the zone records, and it sends you them.
- May reveal a lot of topological information about your internal network
- In particular, if someone plans to subvert your DNS, by poisoning or spoofing it, for example, they'll find having a copy of the real data very useful.

So best practice is to restrict Zone transfers

- You tell the master what the IP addresses of the slaves are and not to transfer to anyone else.

DNS Zone Transfer

Handle the corporate network layout on a silver plate:

- All the names, addresses, and functionality of the servers can be exposed
- Could results in a complete map of the internal and external network structure.
- A successful zone transfer does not directly result in a network breach

- **host -t ns megacorpone.com | cut -d " " -f 4**
  - Or using dig…

- **host -l megacorpone.com ns1.megacorpone.com**
- **host -l megacorpone.com ns2.megacorpone.com**
- **host -l megacorpone.com ns3.megacorpone.com**

DNS Zone Transfer

Try to dig zonetransfer.me for nameserver:

- nsztm1.digi.ninja
- nsztm2.digi.ninja

Let’s transfer DNS a zone:

- dig axfr @nsztm1.digi.ninja zonetransfer.me

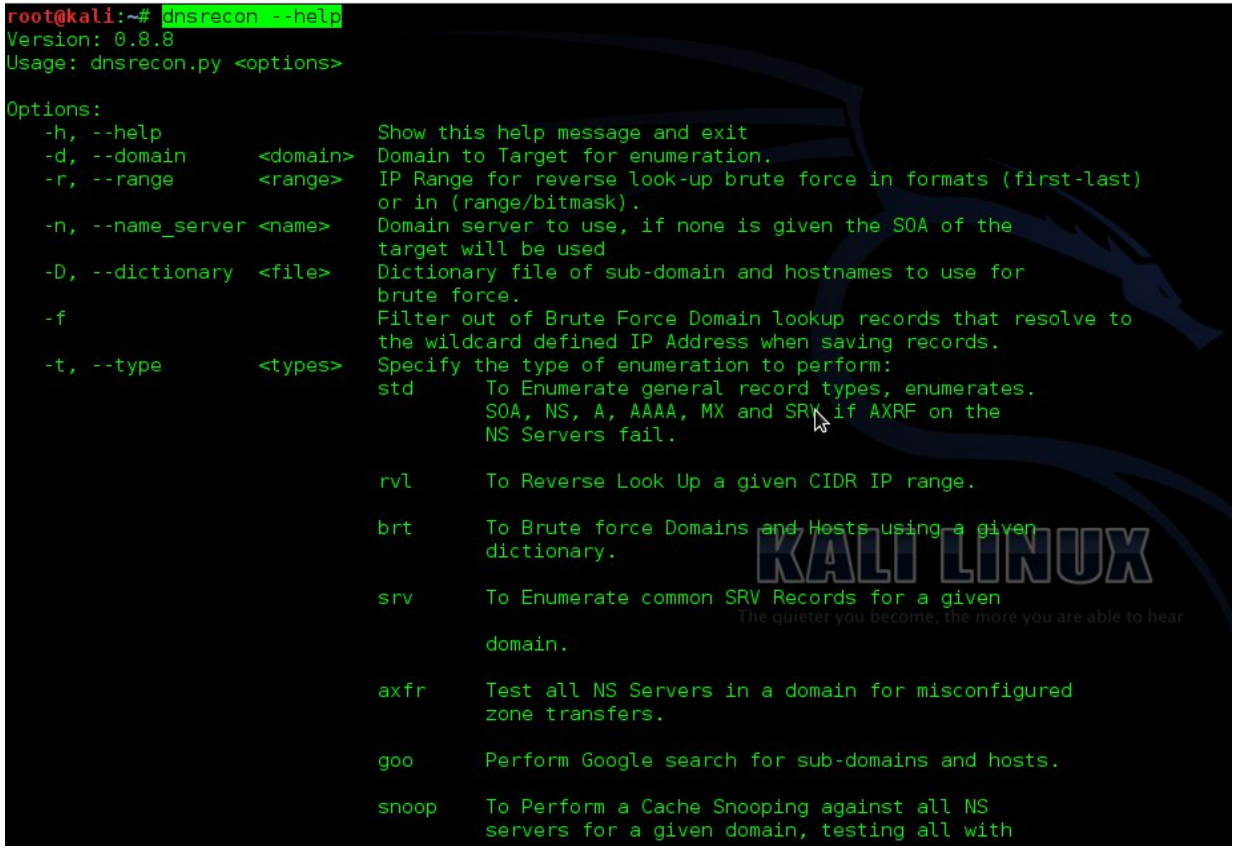
- What they use for e-mail?
- Do you see informations about persons?
- IP address of hosts?
- Other “sensitive” info?

Scripting DNS Zone Transfer

```
#/bin/bash

# Simple Zone Transfer Bash Script
# $1 is the first argument given after the bash script
# Check if argument was given, if not, print usage

if [ -z "$1" ]; then
echo "[*] Simple Zone transfer script"
echo "[*] Usage : $0 <domain name> "
exit 0
fi

# if argument was given, identify the DNS servers for the domain
for server in $(host -t ns $1 |cut -d" " -f4);do
# For each of these servers, attempt a zone transfer
host -l $1 $server | grep "has address"
done
```

DNSRecon

It is used for gathering the dns information of any given target.



DNSRecon: Zone Transfer

DNSRecon provides the ability to perform Zone Transfers with the commands:

dnsrecon.py -d <domain> -a

or

dnsrecon.py -d <domain> -t axfr

DNSRecon: Reverse Lookup

DNSRecon can perform a reverse lookup for PTR (Pointer) records against IPv4 and IPv6 address ranges.

- To run reverse lookup enumeration the command

dnsrecon.py -r <startIP-endIP>

- Also reverse lookup can be performed against all ranges in SPF records with the command

dnsrecon.py -d <domain> -s

DNSRecon: Domain Brute-Force

For performing this technique all we have to do is to give a name list and it will try to resolve the A, AAA and CNAME records against the domain by trying each entry one by one.

- In order to run the Domain Name Brute-Force we need to type:

dnsrecon.py -d <domain> -D <namelist> -t brt

DNSenum

DNSEnum is another popular DNS enumeration tool

- Run this script against the **zonetransfer.me** domain, which specifically allows zone transfers

- **dnsenum zonetransfer.me**

Fierce

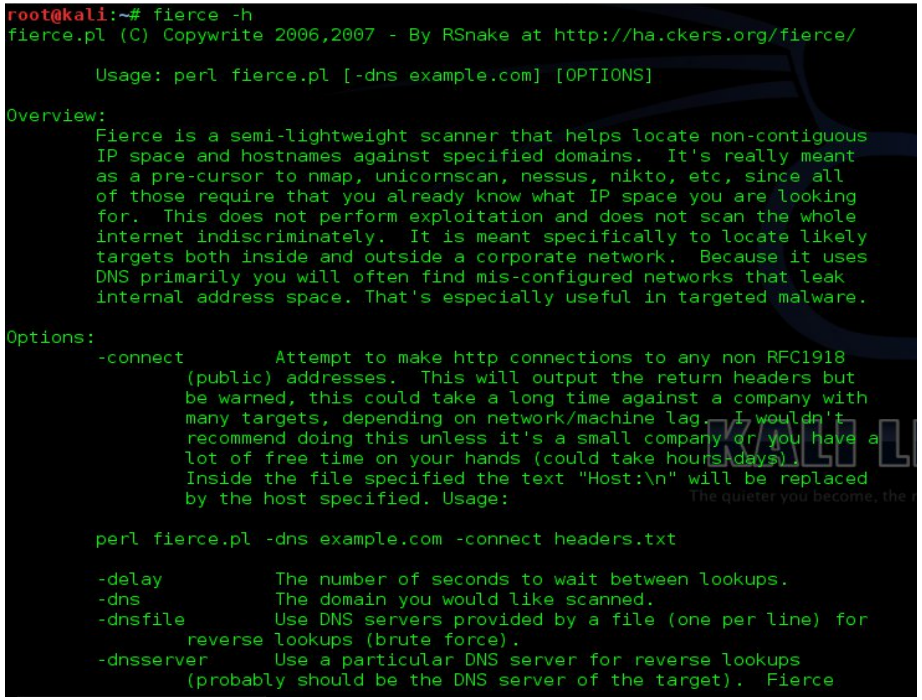
It is a great tool and it helps up in finding the

- IP space and hostnames against specified domains it locate the non-contiguous space both inside and outside the organization/target.

Fierce can do many tasks like

- DNS zone transfer
- Reverse lookup
- DNS brute force

- fierce --dns <domain name>



DNS Transfer mitigation

```
zone "example.com"
{
    type master;
    notify yes;
    allow-transfer
    {
        203.0.113.1;
    };
    file "/var/lib/bind/db.example.com";
};
```

```
options
{
    notify yes;
    allow-transfer
    {
        203.0.113.1;
    };
    // ...
};
```

Restricted Zone Transfer

```
options
{
    notify yes;
    allow-transfer
    {
        any;
    };
    // ...
};
```

Unrestricted Zone Transfer

Do it at home

1. Find the DNS servers for the megacorpone.com domain
2. Write a small Bash script to attempt a zone transfer from megacorpone.com
3. Use **dnsrecon** to attempt a zone transfer from megacorpone.com
4. Find the DNS servers for the uniroma2.it domain
5. Collect as much as possible "open-source" information about uniroma2.it

Exercises

- Hack the box
  - DNS enumeration using python: https://academy.hackthebox.com/module/details/27

Conclusion

THAT ALL FOLKS!

Thank you for your attention 😄 !