

Lecture 2&3

Ethical Hacking

What are Ethical Hackers?

1. Ethical hackers are employed either through contracts or direct employment to test the security of an organization.
2. They use the same skills and tactics as a hacker but with permission from the system owner to carry out their attack against the system.
3. Ethical hackers work under contract for a company or client, and their contracts specify what is off-limits and what they are expected to do.
4. Their role depends on the specific needs of a given organization. In fact, some organizations keep teams on staff specifically to engage in ethical hacking activities.

Types of Hackers

Script Kiddies These hackers have limited or no training and know how to use only basic techniques or tools. Even then they may not understand any or all of what they are doing.

White-Hat Hackers These hackers think like the attacking party but work for the good guys. They are typically characterized by having a code of ethics that says essentially they will cause no harm. This group is also known as ethical hackers or Pen testers (*penetration testing*)

Types of Hackers

Gray-Hat Hackers These hackers straddle the line between good and bad and have decided to reform and become the good side. Once they are reformed, they still might not be fully trusted.

Black-Hat Hackers These hackers are the bad guys who operate on the opposite side of the law. They may or may not have an agenda. In most cases, black-hat hacking and outright criminal activity are not far removed from each other.

Suicide Hackers These hackers try to knock out a target to prove a point. They are not stealthy, because they are not worried about getting caught or doing prison time.

Code of Conduct and Ethics

1. Keep private and confidential information gained in your professional work.
2. Protect the intellectual property of others by relying on your own innovation and efforts.
3. Disclose to appropriate persons or authorities potential dangers to any e-commerce clients, the Internet community, or the public.
4. Never knowingly use software or a process that is obtained or retained either illegally or unethically.
5. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

Code of Conduct and Ethics

6. Not associate with malicious hackers nor engage in any malicious activities.
7. Ensure all penetration testing activities are authorized and within legal limits.
8. Not take part in any black-hat activity or be associated with any black-hat community
9. Not make inappropriate reference to the certification or misleading use of certificates, marks, or logos in publications, catalogues, documents, or speeches.
10. Not be in violation of any law of the land or have any previous conviction

Hacking language

Hack Value This term describes a target that may attract an above-average level of attention from an attacker.

Target of Evaluation A target of evaluation (TOE) is a system or resource that is being evaluated for vulnerabilities.

Attack This is the act of targeting and actively engaging a TOE.

Exploit This is a clearly defined way to breach the security of a system.

Zero Day This describes a threat or vulnerability that is unknown to developers and has not been addressed. It is considered a serious problem in many cases.

Security This is a state of well-being in an environment where only actions that are defined are allowed

Hacking language

Threat This is considered to be a potential violation of security

Vulnerability This is a weakness in a system that can be attacked and used as an entry point into an environment.

Daisy Chaining This is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action.

Hacking Steps

Footprinting means that you are using primarily passive methods of gaining information from a target prior to performing the later active methods. A myriad of methods are available to perform this task, such as Who is queries, Google searches, job board searches, and discussion groups.

Scanning is the phase in which you take the information gleaned from the footprinting phase. The idea here is to act on the information from the prior phase, not to blunder around without purpose and set off alarms

Enumeration is the next phase where you extract much more detailed information about what you uncovered in the scanning phase to determine its usefulness. Results of this step can include a list of usernames, groups, applications, banner settings, and auditing information.

System hacking follows enumeration. You can now plan and execute an attack based on the information you uncovered. You could, for example, start choosing user accounts to attack based on the ones uncovered in the enumeration phase. You could also start crafting an attack based on service information uncovered by retrieving banners from applications or services.

Hacking Methodologies

Escalation of privilege is the hacking phase, where you can start to obtain privileges that are granted to higher privileged accounts than you broke into originally. Depending on your skills, it might be possible to move from a low-level account such as a guest account all the way up to administrator or system-level access.

Covering tracks is the phase when you attempt to remove evidence of your presence in a system. You purge log files and destroy other evidence that might give away the valuable clues needed for the system owner to determine an attack occurred.

Planting of backdoors means to leave something behind that would enable you to come back later if you wanted. Items such as special accounts or Trojan horses come to mind.

Ethical Hacking Info Phases

Phase 1: Footprinting

- ❖ It is the first phase of the ethical hacking process.
- ❖ The goal is to gather as much information as is reasonable and useful about a potential Target.
- ❖ Information that can be gathered during this phase includes the following:
 - IP address ranges
 - Namespaces
 - Employee information
 - Phone numbers
 - Facility information
 - Job information

```
a = 'global a'
y = 'global y'
```

Global

```
def test_namespace():
    a = 'enclosing a'
```

Enclosing

```
def inner_namespace():
    a = 'local a'
    print(a)
    print(y)
```

Local

```
inner_namespace()
```

```
print(a)
```

```
test_namespace()
```

```
print(a)
```

```
local a
global y
enclosing a
global a
```

IPv4 address in dotted-decimal notation

172 . 16 . 254 . 1



10101100 . 00010000 . 11111110 . 00000001

└──────────┘ └──────────┘

8 bits

└──┘

32 bits (4 bytes)

Phase 2: Scanning

- ❖ It focuses on an active engagement of the target with the intention of obtaining more information.
- ❖ scanning determines which hosts are active and what the network looks like.
- ❖ During this phase tools such as these are used:
 - Pings
 - Ping sweeps
 - Port scans
 - Tracert : (Trace Route), a command-line utility that you can use to trace the path that an Internet Protocol (IP) packet takes to its destination.

Phase 3: Enumeration

- ❖ It is the systematic probing of a target with the goal of obtaining user lists, routing tables, and protocols from the system.
- ❖ It is the initial transition from being on the outside looking in to moving to the inside of the system to gather data. This information is carried forward into the attack phase.
- ❖ The information gathered during phase 3 typically includes, but is not limited to, the following:
 - Usernames
 - Group information
 - Passwords
 - Hidden shares
 - Device information
 - Network layout
 - Protocol information
 - Server data
 - Service information

Information gathering

- ❖ Usually the first step of every attack
- ❖ Before getting contact with the target we need to prepare for the attack
- ❖ General information gathering covers all the efforts that is done for collecting all the information from the target
- ❖ The collected information should be analysed as well in order to filter the important information
- ❖ Sometimes it is not obvious which information will be useful later, all information should be systemized
- ❖ The result of the information gathering is a huge dataset with dedicated information (e.g. user lists, etc.)

Methods of gathering information

- Google and all search engines are best friends ☐
 - Simple search engine queries
 - Specific search engine queries (google hacking, see later)
 - Cached data (data that are not online right now, but can be restored)
- The social media is another best friend ☐
- Companies and persons spread lots of information from themselves
- We can create personal and company profiles
- We can identify key persons and other key information

Simple information Gathering using Google

Default website (domain name), other sites

- History, several public data (faculties, number of staff members)

N.B For the opposite figure, have a look on the information surrounded by a box.

helwan university - Google Search

google.com/search?q=helwan+university&oq=helwan+university&aqs=chrome..69i57j

About 1,820,000 results (0.64 seconds)

www.helwan.edu.eg - Translate this page
جامعة حلوان | جامعة حلوان
الندوة العامة للتقدم بالحطة الاستراتيجية للعام المالي 2022/2021 لجهات الجامعة المختلفة في إطار تنفيذ الحطة الاستراتيجية لجامعة حلوان التفاصيل أعمال تطوير ...

Results from helwan.edu.eg

نتائج الإمتحانات
نتائج الإمتحانات: نتائج إمتحانات جميع الكليات
بالجامعة لجميع ...

Helwan University
Helwan University is a university of technology and applications , it ...

الكشف الطبي
هناك جذا يشارن مواعيد الكشف الطبي لأكسجوع
القديم على جميع الطلاب ...

الطلاب الوافدين
International Students
الوافدين ... تعلن جامعة حلوان عن ...

الكليات والمعاهد
الكليات والمعاهد ...

تشعيب الكليات
التقديم لشعبة اللغات والبرامج الجديدة بكلية
التجارة (Eng) -BIS- ...

Map data ©2020

Hours

A Helwan University
University
Al Sikka Al Hadid Al Gharbeya
02 25569061

B Faculty of Education, Helwan University
College
Closed - Opens 7AM Mon - 02 25548193

C Faculty of Social Work, Helwan University
College
Closed - Opens 8AM Mon - 0120 141 1471

View all

en.wikipedia.org › wiki › Helwan_University
Helwan University - Wikipedia
Helwan University is a public university based in Helwan, Egypt, which is part of Greater Cairo.
It comprises 21 faculties as well as 50 research centers and ...

Location: Cairo, Egypt
Academic staff: 4,120 (2018)

Established: July 26, 1975
President: Dr. Maged Fahmy Negm

Helwan University
Public university in Helwan

helwan.edu.eg

Helwan University is a public university based in Helwan, Egypt, which is part of Greater Cairo. It comprises 21 faculties as well as 50 research centers and productive units which connect the university with the problems of the Egyptian society. Wikipedia

Students: 109,455 (2018)
President: Dr. Maged Fahmy Negm
Number of students: 109,455 (2018)
Founded: July 26, 1975
Headquarters: Helwan

Notable alumni

Nagui Asaad
Ahmad Nady
Dalia El Behery
Abdel Moneim About Fo...
Sherif Nour

Profiles

Facebook

People also search for

Ain Shams University
Cairo

Menoufiya University
Shebeen El-Kom

Suez Canal University
Ismailia

جامعة المنصورة
Mansoura

Tanta University
Tanta

Feedback

Simple information Gathering using google

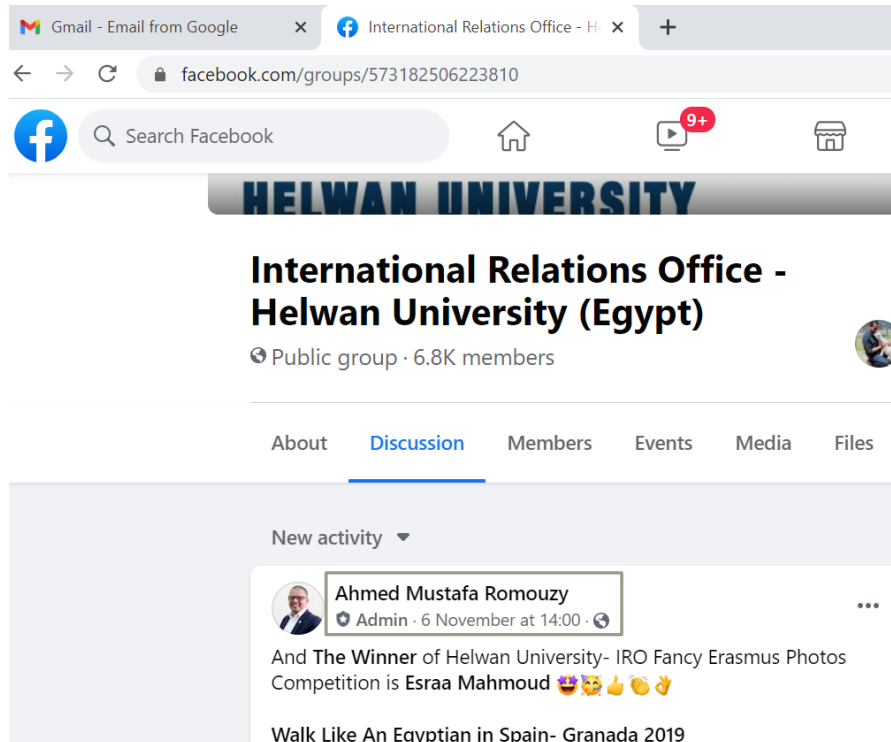
- Keypersons with contact details
- Important pages
- Services



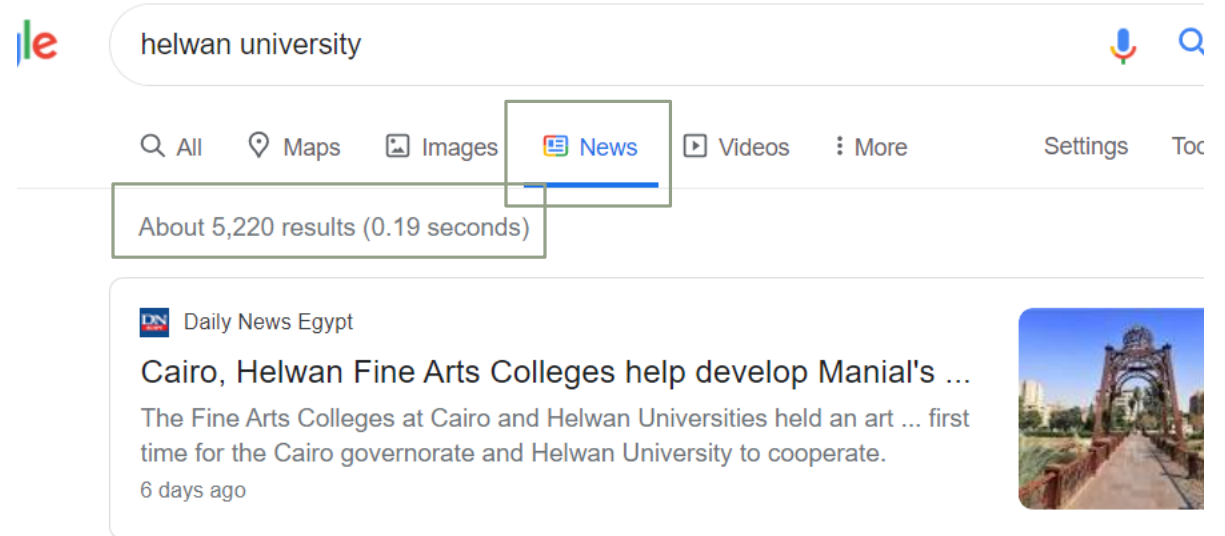
Simple Information Gathering using Google

□ Reading the news

□ Social Media info



The screenshot shows a web browser with two tabs: 'Gmail - Email from Google' and 'International Relations Office - Helwan University'. The address bar displays 'facebook.com/groups/573182506223810'. The Facebook page header includes the search bar, home icon, and a notification badge with '9+'. The page title is 'HELWAN UNIVERSITY' in a blue banner. Below this, the page name is 'International Relations Office - Helwan University (Egypt)', followed by 'Public group · 6.8K members'. Navigation tabs include 'About', 'Discussion' (which is selected), 'Members', 'Events', 'Media', and 'Files'. The 'New activity' section shows a post by 'Ahmed Mustafa Romouzy', an admin, dated '6 November at 14:00'. The post text reads: 'And The Winner of Helwan University- IRO Fancy Erasmus Photos Competition is Esraa Mahmoud 🎉👏👏👏👏'. Below the post, it says 'Walk Like An Egyptian in Spain- Granada 2019'.



The screenshot shows a Google search interface. The search bar contains the text 'helwan university'. Below the search bar, navigation links for 'All', 'Maps', 'Images', 'News', 'Videos', 'More', 'Settings', and 'Tools' are visible. The 'News' link is highlighted with a green box. Below the navigation links, a box indicates 'About 5,220 results (0.19 seconds)'. The first search result is from 'Daily News Egypt' and is titled 'Cairo, Helwan Fine Arts Colleges help develop Manial's ...'. The snippet below the title reads: 'The Fine Arts Colleges at Cairo and Helwan Universities held an art ... first time for the Cairo governorate and Helwan University to cooperate. 6 days ago'. To the right of the text is a small image of a bridge.

Pipl.com – Finding accounts

- ☐ Personal information
- ☐ Net catalogues
- ☐ Academic records
- ☐ Social accounts

The screenshot displays the Pipl.com search interface. At the top, the Pipl logo is on the left, and a search bar contains 'audun jøsang' and 'Oslo, Norway' with a search button. Below the search bar, the 'Search By' section shows 'First: Audun' and 'Last: Jøsang', with a '+ MORE OPTIONS' link and a search icon. A red box highlights a location filter menu on the left, which includes 'All Locations', 'Norway', 'Hvalstad', 'Oslo' (checked), 'Australia', 'State of Queensland', 'Brisbane', and 'South Brisbane'. The main results area shows 'No results found for Audun Jøsang, Oslo, Norway . Showing possibly related results'. The results list includes: 1. A purple icon with 'A' for 'Audun Jøsang' from Hvalstad, Norway. 2. A green icon with 'A' for 'Audun Jøsang' from Brisbane & South Brisbane, State of Queensland, known online as audunjosang. 3. A photo of a man for 'Audun Jøsang' with a Facebook link 'facebook.com/people/_/100000637206485' and 'Personal Web Profile - Facebook'. 4. Another photo of a man for 'Audun Josang'. 5. A briefcase icon for 'Audun Josang - Queensland University of Technology' with a ZoomInfo link and 'Web Extracted Biography - ZoomInfo'. 6. A person icon for 'Audun Josang, Australia' with an Amazon link and 'Customer Profile - Amazon.com'.

pipl

audun jøsang Oslo, Norway

Search By

First Audun

Last Jøsang

+ MORE OPTIONS

☐ All Locations

☐ Norway

☐ Hvalstad

☒ Oslo

☐ Australia

☐ State of Queensland

☐ Brisbane

☐ South Brisbane

No results found for **Audun Jøsang, Oslo, Norway** . Showing possibly related results

Audun Jøsang
Hvalstad, Norway

Audun Jøsang
Brisbane & South Brisbane, State of Queensland
Known online as audunjosang

Audun Jøsang
facebook.com/people/_/100000637206485
Personal Web Profile - Facebook

Audun Josang

Audun Josang - Queensland University of Technology
zoominfo.com/Search/PersonDetail.aspx?PersonID=978409446
Web Extracted Biography - ZoomInfo

Audun Josang, Australia
amazon.com/gp/pdp/profile/A3PVPT2Y5DD5QN/
Customer Profile - Amazon.com

Using social media to build personal profile

- ❑• Work and education
- ❑• Places of living
- ❑• Contact info
- ❑• Family relationships
- ❑• Details
- ❑• Life events
- ❑• Photos
- ❑• Favorites (music, sports, films, etc..)
- ❑• Friends
- ❑• Timeline data

Using social media to carry out social engineering attacks - examples

Social Engineering using private information:

Isak spent 5 days at the Scandic Hotel Kristiansand. He posted on Facebook (Checked in Scandic Kristiansand). 5 days later Isak receives an email from the "Hotel" (attacker). Dear guests! Our hotel would like to surprise all our guests between the age of 14 and 24 who visited us during the last month with a SuperMario Cart game as a summer holiday surprise. Please fill in the following form and provide your address: **link** We hope you enjoyed your stay at our hotel,etc..

(He can get hacked easily by clicking on the link, he also can provide his address so easily)

Using social media to carry out social engineering attacks - examples

Building personal profile using social media

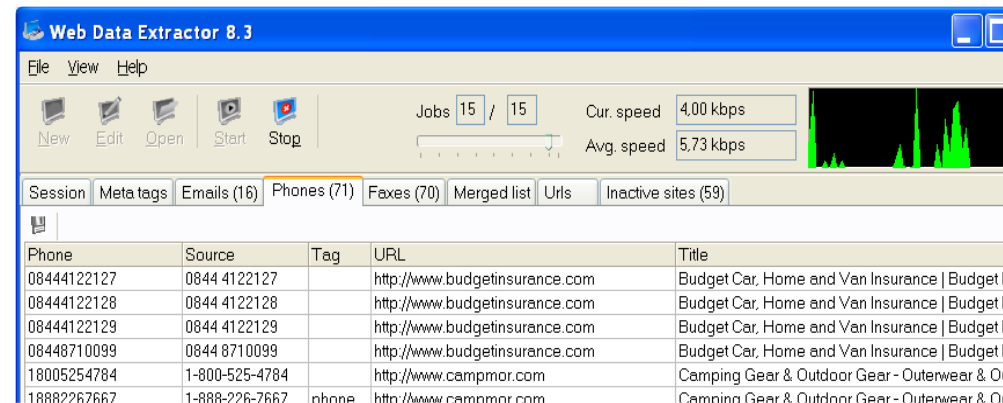
Stine has a Facebook account where she listed all her favourites. One of her favourite singer is Rihanna. The attacker brute-forces Stina's password and finds out that one of her passwords is Diamonds2012. The attacker logs in to Stine's Facebook account and steals private photos, writes weird messages to her friends, etc.

Everyone can be misled, it's just a question of timing and story!

Every information can be important, hackers collect all available information and systemize them before planning the attack!

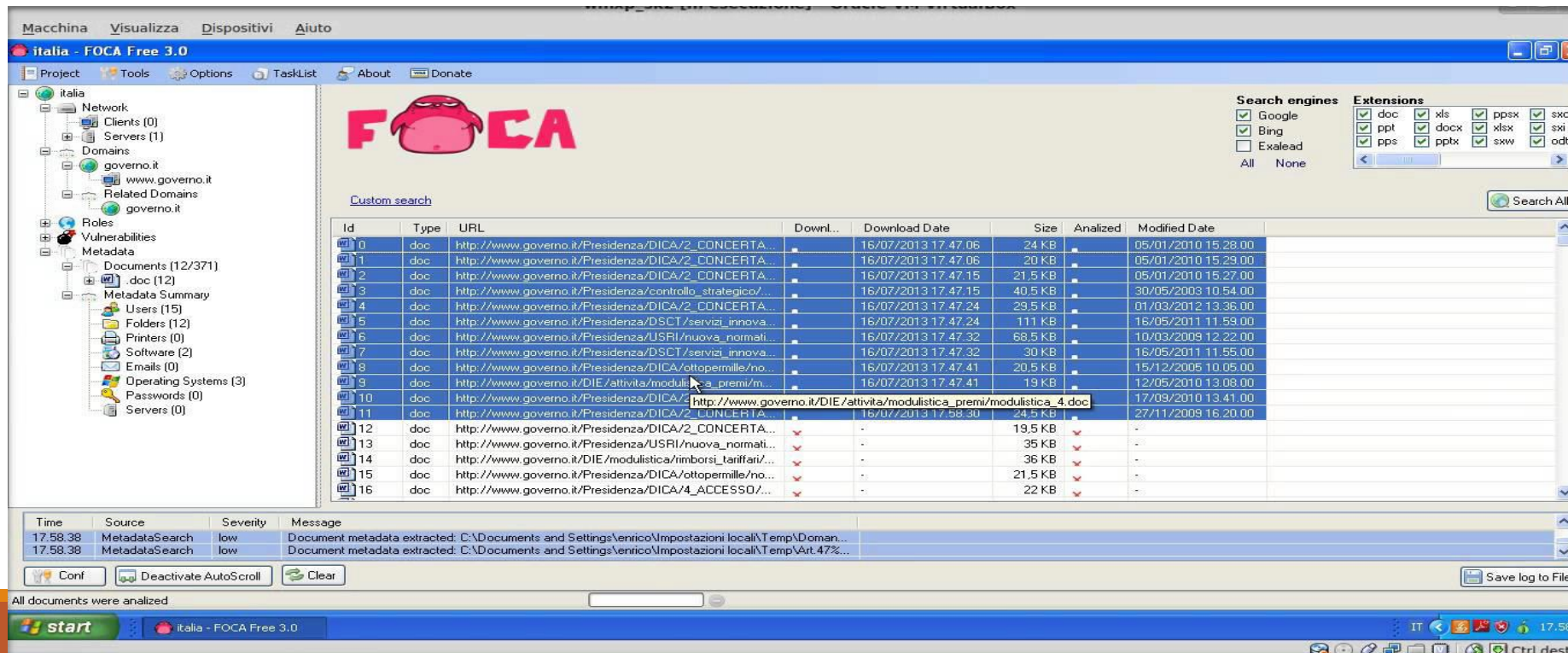
Collecting information from webpages

- ❑ All static information can be downloaded at once (noisy, but useful)
- ❑ Several tools exist like *wget* or *Httrack*
- ❑ We can look for specific info such as email addresses, phone numbers, meta data, etc. using web data extractor.



Specific information search

- *Foca* is able to find documents by extensions: it is a tool used mainly to find metadata and hidden information in the documents its scans. These documents may be on web pages and can be downloaded and analyzed with FOCA.
- It also shows several technical information



Google hacking

Each of the operators mentioned here is entered directly into the search box on the [Google.com](https://www.google.com) home page. You don't have to go to a special page to use these commands.

cache Displays the version of a web page that Google contains in its cache instead of displaying the current version. Syntax: **cache:<website name>**

link Lists any web pages that contain links to the page or site specified in the query. Syntax: **link:<website name>**

info Presents information about the listed page. Syntax: **info:<website name>**

site Restricts the search to the location specified. Syntax: **<keyword> site:<website name>**

allintitle Returns pages with specified keywords in their title. Syntax: **allintitle: <keywords>**

allinurl Returns only results with the specific query in the URL. Syntax: **allinurl: <keywords>**

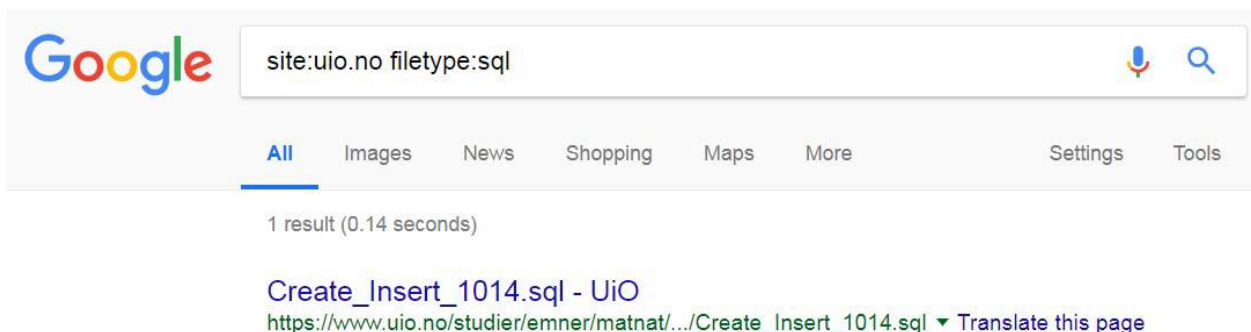
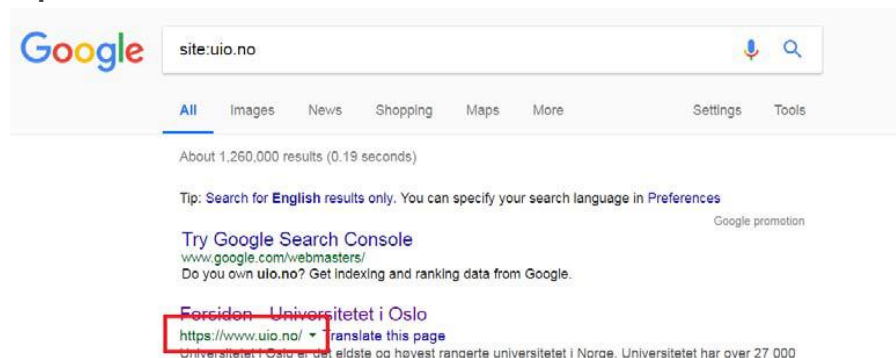
Information gathering with Google hacking

Using specific Google queries we can use smart filtering or get «hidden» data

- Filter to domain: use the **site** keyword

Filter to file type with extension: use the type keyword

- Interesting file extensions: doc, xls, txt, conf, inc, sql, ...
- Expressions can be combined



Exercise using google hacking

This exercise demonstrates how to use Google hacking to uncover information about a target. To do this exercise, you can use any browser and just go to www.google.com.

1. In the search box enter the phrase **Site:**www.wiley.com **Oriyano**. This will search the Wiley website and return any references that include the name Oriyano.
2. In the search box enter the phrase **Allinurl: network camera**. This will return a list of web-enabled cameras that are attached to the Internet.
3. In the search box enter the phrase **Link: itpro.tv**. This will return a list of websites that link to the website itpro.tv.

This is just an example of three operators available to you for Google hacking. To gain information about your target, replace the website and keywords with your target. Experiment with different combinations and phrases to extract information regarding your target

Thank you 😊