

IN5290 Ethical Hacking



Lecture 1: Introduction to Ethical Hacking, Information Gathering

Universitetet i Oslo
Laszlo Erdödi

Lecture Overview

- What is ethical hacking?
- Steps of penetration testing
- Information gathering techniques

Why ethical hacking is necessary at all?

- Computer systems have several security problems

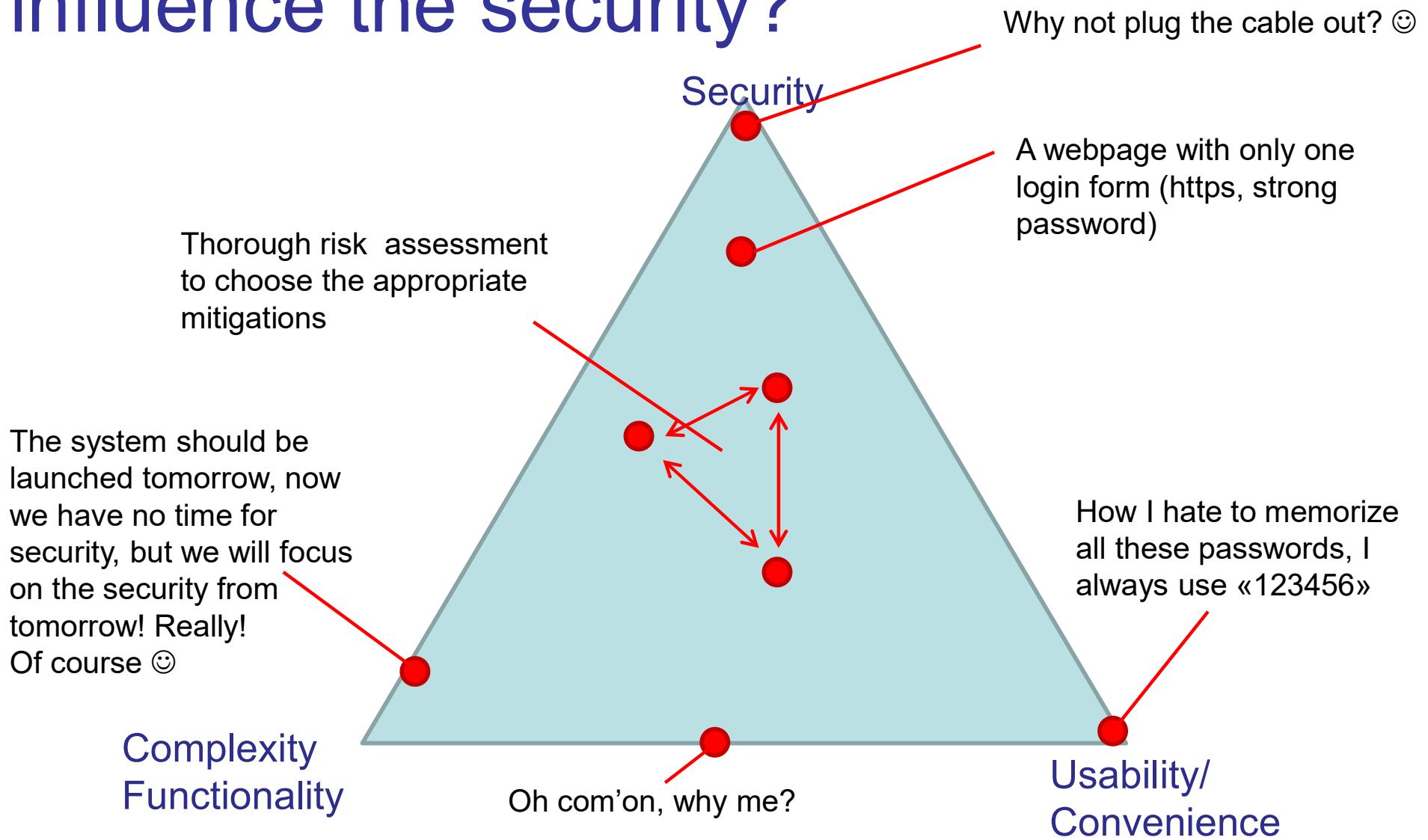
The image shows a collage of news snippets from various sources, each highlighting a different aspect of cybersecurity:

- Top Left Snippet:** "2 Million Passwords Reportedly Stolen" - Facebook, Other Social Media Sites Targeted. Published by Eric Chabrow (GovInfoSecurity) on December 5, 2013.
- Top Right Snippet:** "Default router password leads to spilled military secrets".
- Middle Left Snippet:** "Spectre, Meltdown Redux: Intel Chips Found Vulnerable to More Malware" - Published by Doug Black on August 14, 2018.
- Middle Right Snippet:** "The age of cyberwar is here. We can't keep citizens out of the debate" by David E Sanger, published in The Guardian on July 12, 2018.
- Bottom Left Snippet:** "Russian Hackers Penetrate US Electrical Grid – Report" - Published by Tom Jowitt on July 24, 2018.
- Bottom Right Snippet:** "Windows 3.1 Is Still Alive, And It Just Killed a French Airport" by Pierre Longeray, published on November 13, 2015.

What is the reason for having so many security issues?

- Lack of money
- Lack of time
- Lack of expertise
- Negligence
- Convenience
- Old systems
- Too complex systems
- 3rd party components
- And many others...

How does the usability and functionality influence the security?



Why ethical hacking is necessary at all?

- Checking the system from the attacker's perspective can reveal serious security deficiencies
- The «attacker» thinks like a real hacker (but not totally)
 - Do we use the same methodology as the real hackers?
 - Do we have the same goals?
 - Do we have to hide ourselves when ethically hacking?
 - What makes hacking ethical?
 - What is allowed and what is not?
- The system security cannot be guaranteed without deep and regular penetration testing
 - Can it be guaranteed with penetration testing? Unfortunately not always perfectly, the keyword is the appropriate mitigation

The motivation behind hacking – Why?

To understand the real hackers, first we have to understand the motivations:

- What a cool thing to be a hacker
- Because I can
- Money
- Revenge
- Annoyance
- Protesting against something
- Organized and well-paid professional groups (mafia and state sponsored groups)

The goal of hacking

- Break the information security triple (confidentiality, integrity, availability)
 - Steal confidential information
 - Modify data
 - Make services unavailable (Denial Of Service)
- To promote security? YES!

Type of hackers

- Black hat hackers: Hacking with malicious intent
- White hat hackers: Perform penetration testing to promote the security
- Script kiddies: amateurs (Usually young kids) using publicly available software tools to attack
- Protest hackers (Protest against something e.g. anonymous)
- Grey hat hackers: Usually white hat, but can be black hat
- Red hat hackers: Stopping black hat hackers by attacking them
- Blue hat hackers: Hacking in order to take revenge
- Green hat hackers: Beginners to hacking

Be ethical and legal, it's never worth doing anything against the law!!!

Hacker who helped end global cyberattack arrested in US

British researcher arrested for allegedly creating and distributing malware designed to collect bank-account passwords.

4 Aug 2017



Leader of Hacking Group Who Stole \$1 Billion From Banks Arrested In Spain

March 26, 2018 Wang Wei

Two Hackers Arrested for Hijacking Over 700,000 Online Accounts

By Catalin Cimpanu

June 27, 2018

09:40 AM

0



Skoleelev varslet om datahull i Bergen

Det var en elev ved en barneskole i Bergen som oppdaget sikkerhetshullet som gjorde at informasjon om tusenvis av elever og lærere kunne ha blitt spredt.

Av NTB

Oppdatert 17. august 2018

Differences between ethical and non-ethical hacking

- Task: Find the admin password of «*NonExistingBank*»
- How do I start? Which one of these will be used by the black hat and the white hat hackers?
 - Try with the websites, maybe there's a server side scripting flow?
 - Try to apply for an account to have access to password protected sites?
 - Try with low level exploitation against the server?
 - Try to access the DMZ through a less controlled service?
 - Try to sneak inside the building to have access to the internal network?
 - Try social engineering emails against the employees?
 - Try to make friendship with the system admin?

Differences between ethical and non-ethical hacking



- Legal (contract)
- Promote the security by showing the vulnerabilities
- Find all vulnerabilities
- Without causing harm
- Document all activities
- Final presentation and report
- Illegal
- Steal information, modify data, make service unavailable for own purpose
- Find the easiest way to reach the goal (weakest link)
- Do not care if the system destroys the system (but not too early)
- Without documentation
- Without report, delete all clues

Main steps of hacking

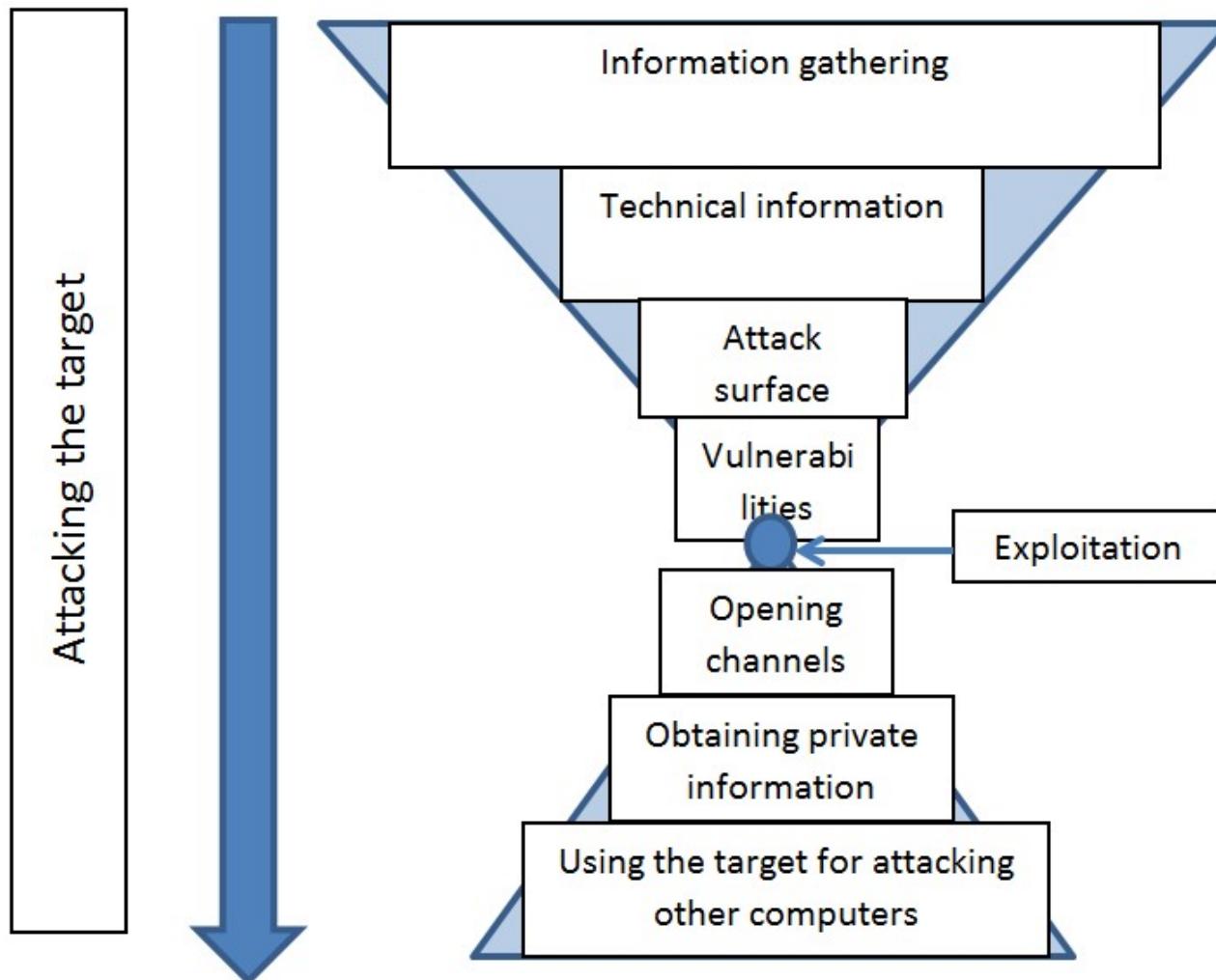
- Information gathering
- Identifying the target domain
- Finding vulnerabilities
- Exploiting the vulnerabilities
- Lateral movements
- Carry out the goal



Spectacular, but not real! 😊



Steps of an attack with available info as the hacking process proceeds



Detailed steps of hacking

1. General information gathering: collecting all available information from the target and systemize the information
2. Technical information gathering: collecting network and system specific information like target ip ranges
3. Identifying available hosts in the target network (which computer can be attacked)
4. Identifying available services in the target network (which service can be attacked)
5. Manual mapping of the services (to check how it looks like, the impressions, system reactions, mitigations, etc.)

Detailed steps of hacking

6. Automatic vulnerability scanning (intelligent tools with huge vulnerability database)
7. Manual verification of the findings (to check if the previous findings are real – true positive)
8. Exploitation
9. Lateral movements (to move through the network)
10. Ensure access until the end of the project
11. Collect info – achieve primary and secondary goals
12. Remove clues
13. Reporting and presentation
14. Removing the attacking files!!! (tools, data, script created temporarily during the pentest)

Type of ethical hacking projects

From the attacker's location point of view:

- External penetration testing
- Web hacking
- Internal penetration testing
- Wireless penetration testing
- Social Engineering

From the attacker's access (right) point of view:

- Black box testing
- Grey box testing
- White box testing

General 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 analyzed 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 to do information gathering

- 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

The screenshot shows a Google search results page for the query "university of oslo". The results include:

- Home - University of Oslo - UiO** (<https://www.uio.no/english/>)
Jul 27, 2018 - The University of Oslo is a leading European university and Norway's largest. UiO is home to outstanding research and offers a great variety in ...
Study programmes in English
Courses offered in English
Studies
More results from uio.no »
- University of Oslo - Wikipedia** (https://en.wikipedia.org/wiki/University_of_Oslo)
The University of Oslo (Norwegian: Universitetet i Oslo), until 1939 named the Royal Frederick University is the oldest university in Norway, located in the ...
Location: Oslo, Norway Administrative staff: 2,768 (2014)
Academic staff: 3,425 (2014) Students: 27,227 (2014)
History · Hierarchy · Faculties · Notable academics and ...

On the right side of the search results, there is a snippet for the University of Oslo, featuring its logo, a map of the campus area, and a "See photos" button.

- Default website (domain name), other sites
- History, several public data (faculties, number of staff members)

Simple information gathering using Google

- Keypersons with contact details
- Important pages
- Services

IT services

IT services at the Department

- Premissions on windows
- Permissions for files and folders
- Printing at IFI
- All services at the department
- Permissions on Mac
- Web publishing
- AV equipment at Ifi

IT services at the faculty

- Netbased application services in the faculty
- Technical support auditoriums teaching rooms
- AV-equipment at the faculty of natural sciences.
- All services at the faculty
- Laptop details
- Software for MN's computers
- E-academy

Need help?

Do you need help with the IT services?

Quicklinks (services in Norwegian)

- Fronter
- Studentweb
- Brukerinfo
- kiosk.uio.no
- Vortex
- Webmail and calendar
- Programvare-databasen

Service messages from Ifi (Norwegian)

- Nedetid på et knippe servere 7. juli

The University Leadership Team

Persons 1 - 6 of 6

Name	Phone	E-mail	Tags
 Gornitzka, Åse Vice-Rector	+47-22856036	ase.gornitzka @stv.uio.no	
 Karlsen, Tove Kristin Deputy University Director	+47-22856226 +47-92620646	t.k.karlsen @admin.uio.no	Deputy University Director
 Mo, Gro Bjørnerud Pro-Rector	+47-22854333 +47-40281612	prorektor @uio.no	

Collecting actual target related information

- Reading the news
- Social media info

Universitetet i Oslo (UiO)

Tweets 3,371 Following 2,175 Followers 21.8K Likes 672 Lists 5

Universitetet i Oslo (UiO) Yesterday at 10:45 AM

Takk for alt, Fronter ❤️ Møt vår nye flamme, Canvas 🔥

See Translation

UNIVERSITAS NO
Fronter erstattes med Canvas – dette må du vite
I mange år har Fronter skapt hodebry for studenter. Nå sier flere...

1 Comment 1 Share

Like Follow Share ...

university of oslo

All Images Maps News Videos More Settings Tools

About 121,000 results (0.35 seconds)

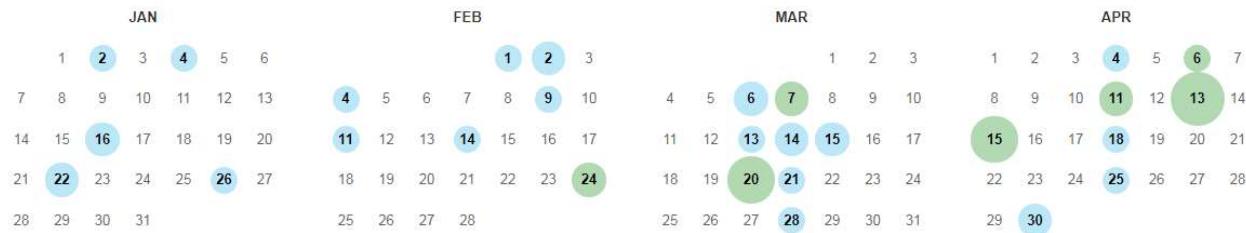
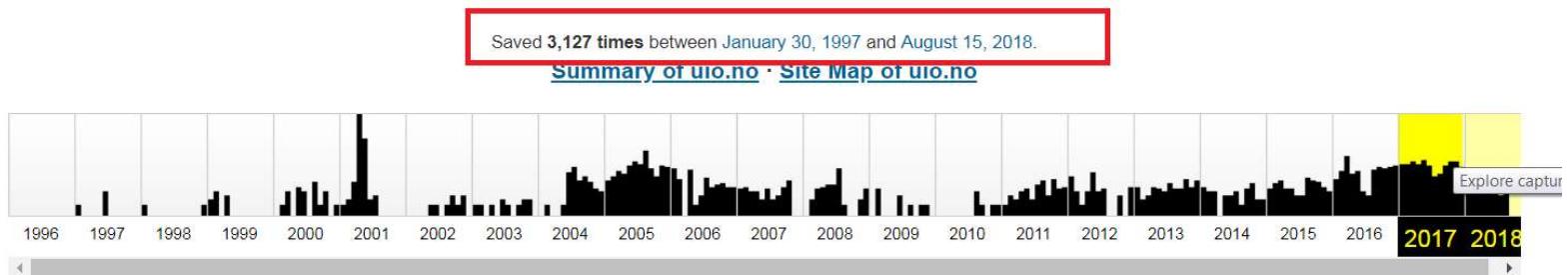
Bacteria: The new superheroes
ScienceNordic 11 hours ago
"We want to use bacteria to produce concrete," says Anja Røyne at the Department of Physics at the University of Oslo, lead researcher for ...

Universitetet i Oslo @UniOslo · Aug 16
Vi har forsket på @ArendalsUka. Er det sånn at de organisasjonene med mest ressurser føler de får mest ut av Arendalsuka? Kl 17:15 kan du høre om forskningen fra blant annet @ketilraknes på MS Sunnhordaland. @UniOsloHF @hkristiania @ISFnytt

Translate Tweet

Collecting cached information

- Archive.org wayback machine



- Google cached results

Home - University of Oslo - UiO
<https://www.uio.no/english/>

Jul 27, 2018 - The University of Oslo is a leading European university and Norway's largest. UiO is home to outstanding research, education and great variety in ...

You visited this page on Jul 17/18

Pipl.com – Finding accounts

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

The screenshot shows the Pipl.com search interface. In the top search bar, the query "audun jøsang" is entered, along with the location "Oslo, Norway". A search button is visible on the right. Below the search bar, there are input fields for "First" (Audun) and "Last" (jøsang), with a "Search By" dropdown menu above them. A "MORE OPTIONS" link and a search icon are also present. To the left, a sidebar lists location filters: "All Locations", "Norway", "Hvalstad", "Oslo" (which is checked), "Australia", "State of Queensland", "Brisbane", and "South Brisbane". The "Oslo" filter is highlighted with a red box. The main search results area displays five entries, each with a profile picture, name, location, and a brief description. The first result is for "Audun Jøsang" in Hvalstad, Norway. The second result is for "Audun Jøsang" in Brisbane & South Brisbane, State of Queensland. The third result is a Facebook profile for "Audun Jøsang". The fourth result is for "Audun Josang" at Queensland University of Technology. The fifth result is for "Audun Josang, Australia" on Amazon.com.

Result	Name	Location	Description
1	Audun Jøsang	Hvalstad, Norway	Known online as audunjosang
2	Audun Jøsang	Brisbane & South Brisbane, State of Queensland	Known online as audunjosang
3	Audun Jøsang		facebook.com/people/_/100000637206485 Personal Web Profile - Facebook
4	Audun Josang		
5	Audun Josang - Queensland University of Technology		zoominfo.com/Search/PersonDetail.aspx?PersonID=978409446 Web Extracted Biography - ZoomInfo
6	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..

Building personal profile using social media

Stine has a Facebook account where she listed all her favorites. One of her favorite 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!

OSINT tools

- Maltego (collecting information using various sources)
- Shodan (Finding IoTs, vulnerabilities in IoTs)
- Google dorks (special search engine expressions)
- Metagoofil (collecting metadata)
- Recon-ng (Modular information gathering tool)
- Checkusernames.com (search for users on social media)
- TinEye (reverse image search)
- Knowem.com (social media profiles)
- Darksearch.io
- Many others...

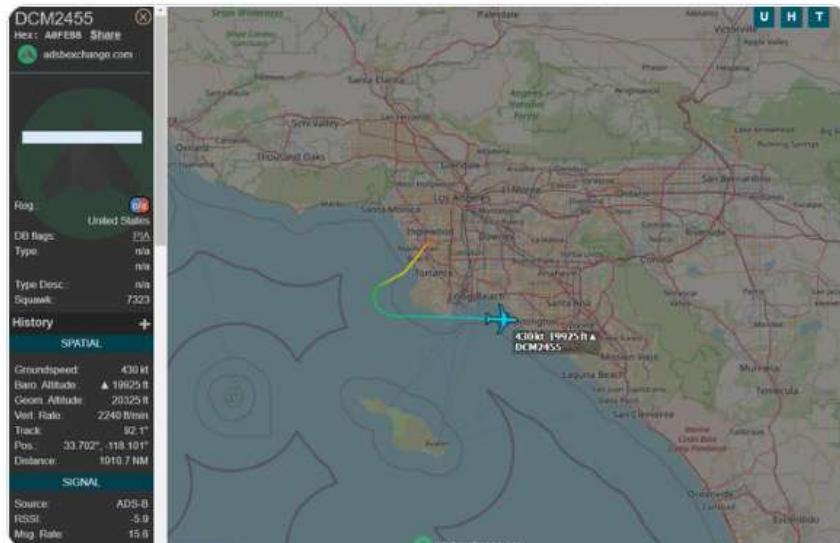
Twitter search 😊



Elon Musk's Jet @ElonJet
Automated



Took off from Hawthorne, Elon got PIA blocking program but already found the aircraft.



9:39 PM · Jan 26, 2022



WHEN YOU OFFER \$43B TO PREVENT PEOPLE FROM RETWEETING THIS PICTURE



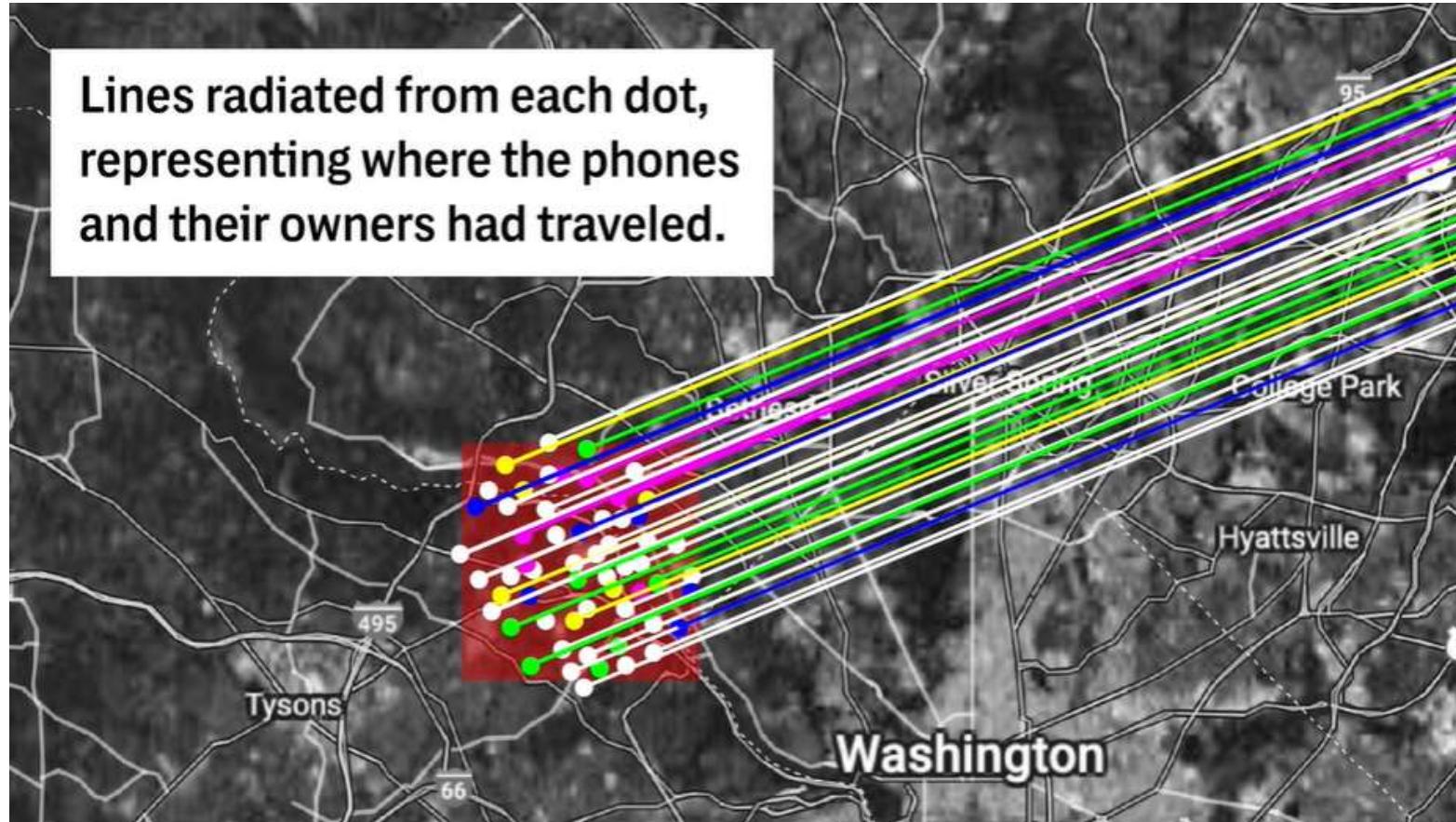
Elon: Can you take this down? It is a security risk.

Sweeney: Yes I can but it'll cost you a Model 3 only joking unless?

Elon: How about \$5k for this account and generally helping make it harder for crazy people to track me?

Sweeney: Sounds doable, account and all my help. Any chance to up that to \$50K?

Phone tracking allows to identify CIA and NSA workers? (Anomaly Six)

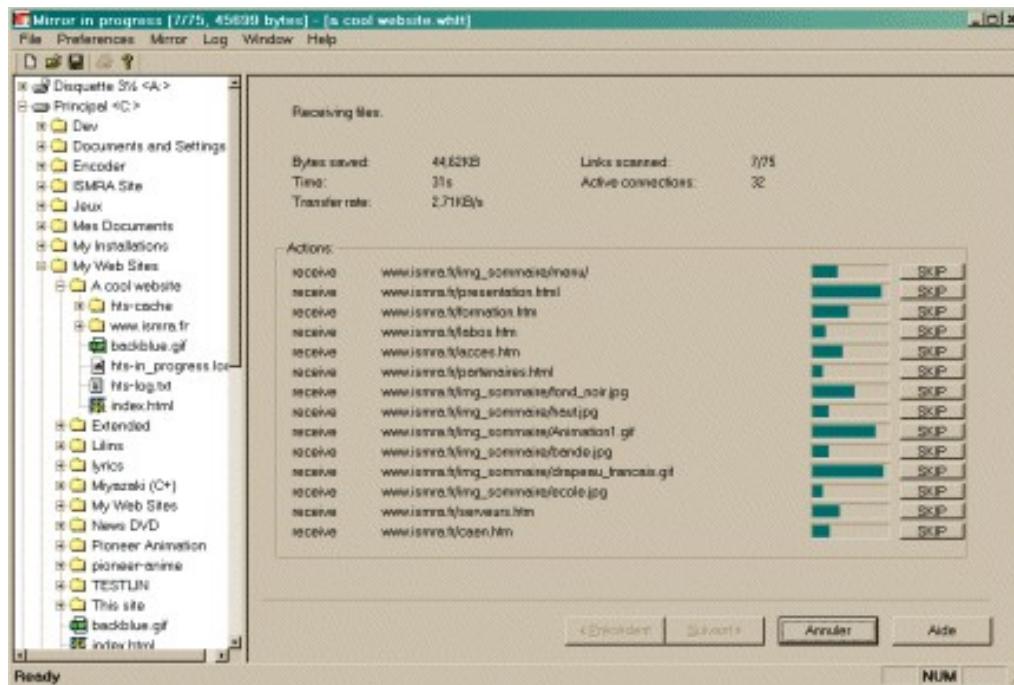


<https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/>

Collecting information from webpages

- All static information can be downloaded at once (noisy, but useful)
- Several tools exist like *wget* or *Httrack*

Httrack demo ...



Specific information search

- We can look for specific info such as email addresses, phone numbers, meta data, etc.

Web Data Extractor demo ...

The screenshot shows the 'Web Data Extractor 8.3' application window. The interface includes a toolbar with icons for New, Edit, Open, Start, and Stop, and a status bar showing 'Jobs 15 / 15', 'Cur. speed 4.00 kbps', and 'Avg. speed 5.73 kbps'. Below the toolbar is a menu bar with File, View, and Help. A tab bar at the top of the main area includes Session, Meta tags, Emails (16), Phones (71) (which is selected), Faxes (70), Merged list, URLs, and Inactive sites (59). The main content area is a grid table with columns: Phone, Source, Tag, URL, and Title. The table lists various phone numbers and their associated sources and titles from different websites.

Phone	Source	Tag	URL	Title
08444122127	0844 4122127		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance Budget Ins
08444122128	0844 4122128		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance Budget Ins
08444122129	0844 4122129		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance Budget Ins
08446710099	0844 8710099		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance Budget Ins
18005254784	1-800-525-4784		http://www.campmor.com	Camping Gear & Outdoor Gear - Outerwear & Outd
18882267667	1-888-226-7667	phone	http://www.campmor.com	Camping Gear & Outdoor Gear - Outerwear & Outd
952011	95 2011		http://www.campmor.com	Camping Gear & Outdoor Gear - Outerwear & Outd
50222326178	+502-2232-6178		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
13056772280	1 (305)677-2280	Ph	http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
13023619942	1(302) 361-9942		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
18668648283	1-866-864-8283		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
533244	53-3244		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
05151210	05-15-12 10		http://photo.net/	Photography community, including forums, reviews
05151218	05-15-12 18		http://photo.net/	Photography community, including forums, reviews
05161200	05-16-12 00		http://photo.net/	Photography community, including forums, reviews
120300	120-300		http://photo.net/	Photography community, including forums, reviews
220120511	2 2012-05-11		http://photo.net/	Photography community, including forums, reviews
2026475225	202-647-5225		http://www.state.gov/travel/	Travel
1503528	+1 503-528		http://www.bootsnall.com/	Around the World Travel Community for Indie Trav
5011000	501-1000		http://www.statravel.com/	Book cheap student and teacher flights, hotels and
9067745190	906-774-5190		http://www.uptravel.com/	Upper Peninsula Michigan, UP Michigan Travel &
8006823333	(800) 682-3333		http://www.gate1travel.com/	Tours, Vacation Packages, Escorted Tour, Travel

Specific information search

- Foca is able to find documents by extensions
- It also shows several technical information

The screenshot shows the FOCA Free 3.0 application window. On the left is a tree view of a network structure under 'italia'. The main area contains a search interface with a logo, search engines (Google, Bing, Exalead), and extension filters (doc, ppt, xls, etc.). A large table titled 'Custom search' lists 16 documents with columns for Id, Type, URL, Download Date, Size, Analyzed, and Modified Date. Below this is a log table with columns Time, Source, Severity, and Message, containing entries for metadata extraction. At the bottom are buttons for configuration, auto-scrolling, clearing logs, and saving logs to file.

Id	Type	URL	Downl...	Download Date	Size	Analyzed	Modified Date
1	doc	http://www.governo.it/Presidenza/DICA/2_CONCERTA...		16/07/2013 17.47.06	24 KB		05/01/2010 15.28.00
2	doc	http://www.governo.it/Presidenza/DICA/2_CONCERTA...		16/07/2013 17.47.06	20 KB		05/01/2010 15.29.00
3	doc	http://www.governo.it/Presidenza/controlli_strategico/...		16/07/2013 17.47.15	40,5 KB		30/05/2003 10.54.00
4	doc	http://www.governo.it/Presidenza/DICA/2_CONCERTA...		16/07/2013 17.47.24	29,5 KB		01/03/2012 13.36.00
5	doc	http://www.governo.it/Presidenza/DSCT/servizi_innova...		16/07/2013 17.47.24	111 KB		16/05/2011 11.59.00
6	doc	http://www.governo.it/Presidenza/USRI/nuova_normati...		16/07/2013 17.47.32	68,5 KB		10/03/2008 12.22.00
7	doc	http://www.governo.it/Presidenza/DSCT/servizi_innova...		16/07/2013 17.47.32	30 KB		16/05/2011 11.55.00
8	doc	http://www.governo.it/Presidenza/DICA/otopermille/no...		16/07/2013 17.47.41	20,5 KB		15/12/2005 10.05.00
9	doc	http://www.governo.it/DIE/attivita/modulistica_premi/m...		16/07/2013 17.47.41	19 KB		12/05/2010 13.08.00
10	doc	http://www.governo.it/Presidenza/DICA/2_modulistica_4...					17/09/2010 13.41.00
11	doc	http://www.governo.it/Presidenza/DICA/2_LUNCERTA...		16/07/2013 17.58.31	24,5 KB		27/11/2009 16.20.00
12	doc	http://www.governo.it/Presidenza/DICA/2_CONCERTA...	x		19,5 KB	x	
13	doc	http://www.governo.it/Presidenza/USRI/nuova_normati...	x		35 KB	x	
14	doc	http://www.governo.it/DIE/modulistica/rimborso_tariffari/...	x		36 KB	x	
15	doc	http://www.governo.it/Presidenza/DICA/otopermille/no...	x		21,5 KB	x	
16	doc	http://www.governo.it/Presidenza/DICA/4_ACCESSO/...	x		22 KB	x	

Time	Source	Severity	Message
17.58.38	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\enrico\Impostazioni locali\Temp\Domain...
17.58.38	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\enrico\Impostazioni locali\Temp\Virt.47...

Buttons at the bottom include: Conf, Deactivate AutoScroll, Clear, Save log to File, and a status bar showing 'start italia - FOCA Free 3.0' and system icons.

Information gathering with Google hacking

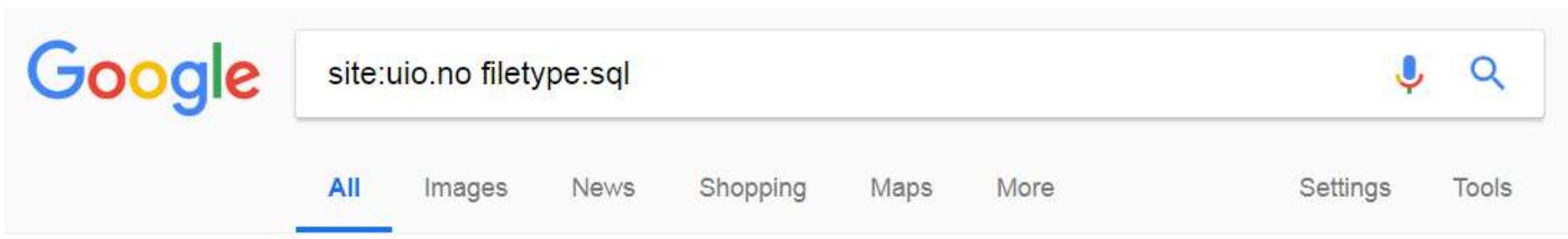
- Using specific Google queries we can use smart filtering or get «hidden» data
- Filter to domain: use the site keyword
- Negative filtering is also possible:

site:uio.no -www

A screenshot of a Google search results page. The search query in the bar is "site:uio.no". The results are filtered under the "All" tab. There are 1,260,000 results in 0.19 seconds. A tip at the top says "Tip: Search for English results only. You can specify your search language in Preferences". Below the tip, there's a "Google promotion" for "Try Google Search Console". The first result is "Forsiden Universitetet i Oslo" with a link to <https://www.uio.no/>. The second result is "Det matematisk-naturvitenskapelige fakultet: Forside" with a link to <https://www.mn.uio.no/>. The third result is "Kulturhistorisk museum: Forsiden" with a link to <https://www.khm.uio.no/>. The fourth result is "Det teologiske fakultet: Forside" with a link to <https://www.tf.uio.no/>. Each result has a "Translate this page" button next to it. Red boxes highlight the URLs and the "Translate this page" buttons for each result.

Information gathering with Google hacking

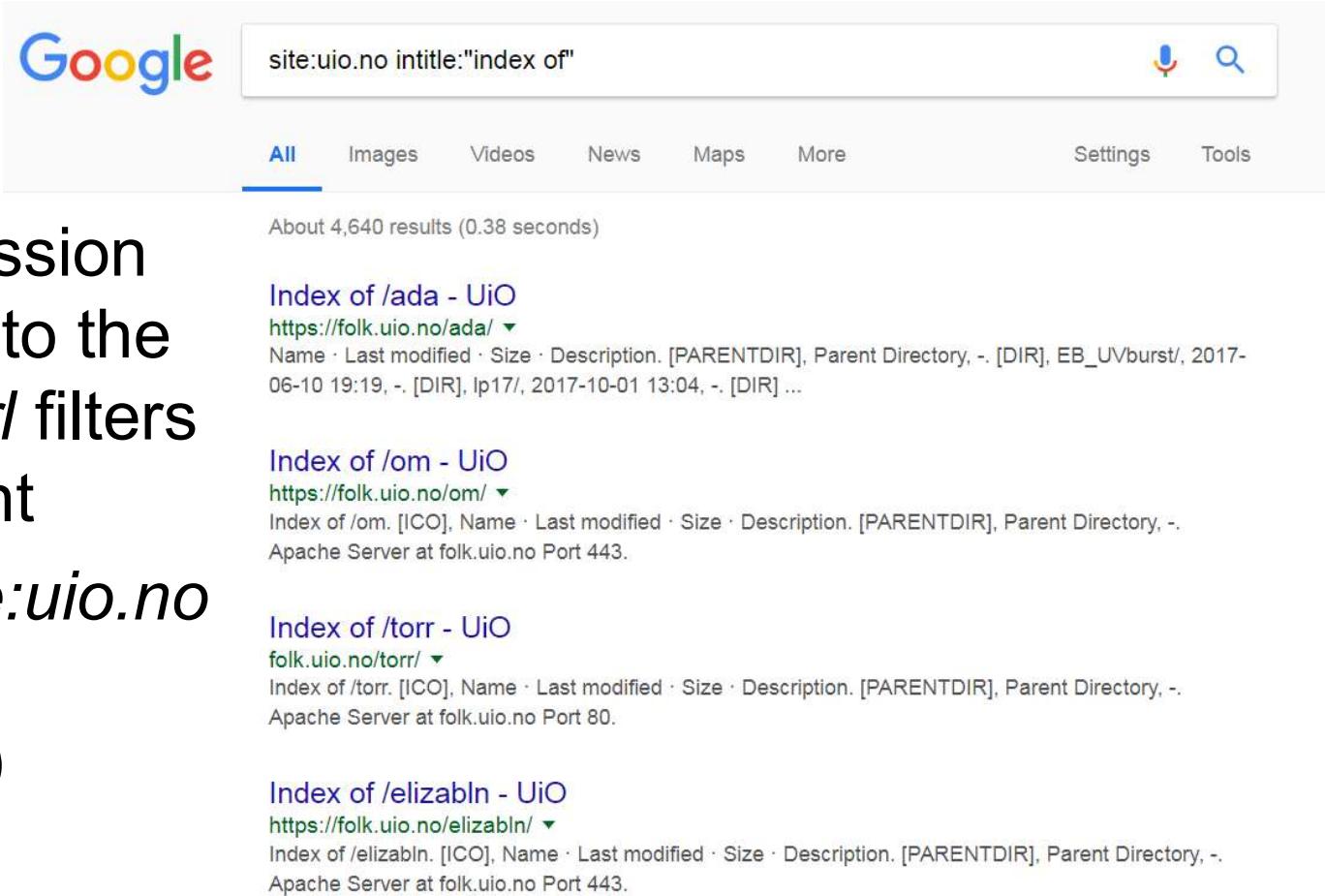
- Filter to file type with extension: use the type keyword
- Interesting file extensions: doc, xls, txt, conf, inc, sql, ...
- Expressions can be combined



A screenshot of a Google search results page. The search query in the bar is "site:ui.no filetype:sql". The results section shows one result found in 0.14 seconds. The result is a link titled "Create_Insert_1014.sql - UiO" with the URL "https://www.uio.no/studier/emner/matnat/.../Create_Insert_1014.sql". There are also links for "Translate this page" and "View page in Google Translate". The page includes standard Google navigation links like All, Images, News, Shopping, Maps, More, Settings, and Tools.

Information gathering with Google hacking

- The *intitle* expression filters according to the site title, the *inurl* filters for the url content
- Try this one: *site:uio.no intitle:"index of"* (directory listing)



A screenshot of a Google search results page. The search query in the bar is "site:uio.no intitle:'index of'". The results show several directory listings from the University of Oslo (UiO) website, including "Index of /ada - UiO", "Index of /om - UiO", "Index of /torr - UiO", and "Index of /elizabln - UiO". Each result includes a link to the directory, file type (ICO), name, last modified, size, and description, indicating they are Parent Directories.

site:uio.no intitle:"index of"

All Images Videos News Maps More Settings Tools

About 4,640 results (0.38 seconds)

Index of /ada - UiO
<https://folk.uio.no/ada/> ▾
Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], EB_UVburst/, 2017-06-10 19:19, -. [DIR], lp17/, 2017-10-01 13:04, -. [DIR] ...

Index of /om - UiO
<https://folk.uio.no/om/> ▾
Index of /om. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. Apache Server at folk.uio.no Port 443.

Index of /torr - UiO
folk.uio.no/torr/ ▾
Index of /torr. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. Apache Server at folk.uio.no Port 80.

Index of /elizabln - UiO
<https://folk.uio.no/elizabln/> ▾
Index of /elizabln. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. Apache Server at folk.uio.no Port 443.

Information gathering with Google hacking

There is a database (google hack database – ghdb) that contains up-to-date google hack expressions (check the exploit-db website)

Google Hacking Database (GHDB)
Search the Google Hacking Database or browse GHDB categories

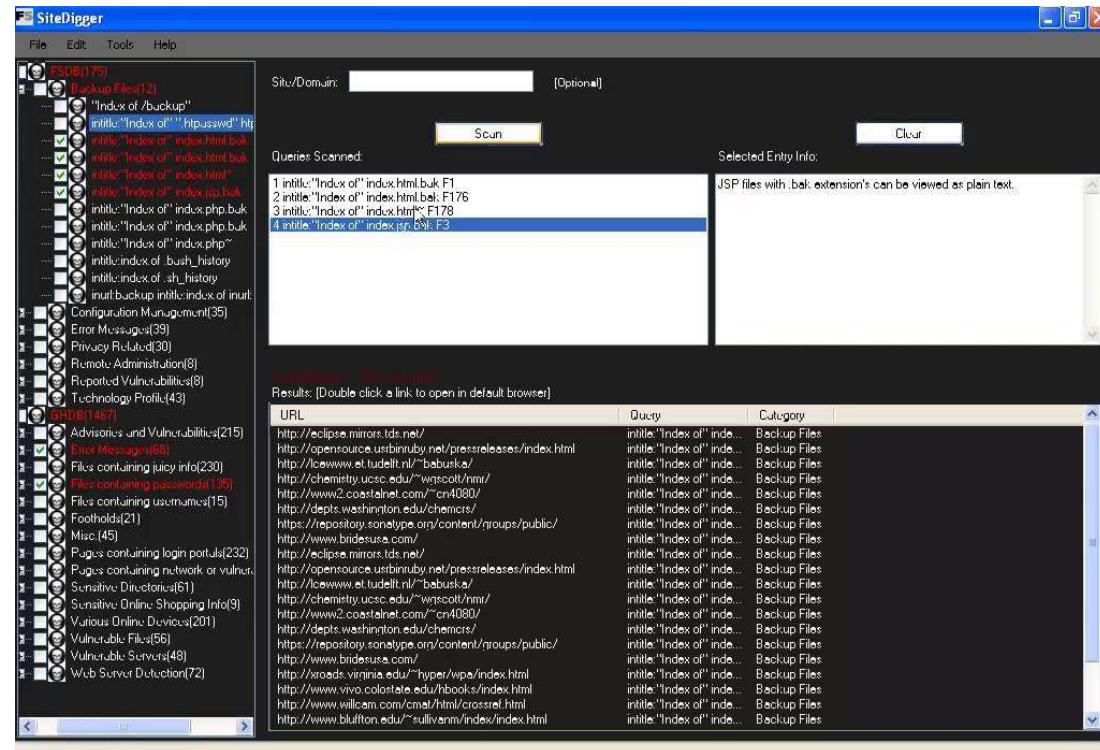
Date	Title	Category
2018-08-17	inurl:wp-config.bak	Files Containing Passwords
2018-08-17	inurl: "Mister Spy" intext:"Mister Spy & Souheyl Bypass Shell"	Footholds
2018-08-15	intext:"Thank you for using BIG-IP."	Pages Containing Login Portals
2018-08-15	inurl:login.php.bak	Files Containing Juicy Info
2018-08-14	intitle:"index of" ".travis.yml" ".travis.xml"	Files Containing Juicy Info

Tools supporting automatic Google hacking

SiteDigger (by FoundStone) is an old tool that carries out google hacking using its own database

Wikto is also capable using Google API key (1000 requests/day)

SiteDigger demo ...



What is needed for the lectures and workshops throughout the semester?

Kali Linux (<http://kali.org>)

- Debian based Linux distribution with hundreds of preinstalled hacking tools
- Easy to use, tools are classified according to the hacking tasks and steps (info gathering, forensics, vulnerability assessment, etc.)
- Easy to install (ready and up-to-date Vmware and Virtualbox images)



End of lecture