Reconnaissance

Kimmo Saurén

Helsinki Metropolia University of Applied Sciences

Course notice

Warning!!!

- Don't use any of these techniques on public networks
- You could get into lot of trouble
- Teacher is not responsible what you do
- Don't drink and ~~Drive~~ hack

Lecture topics

- Information gathering
  - Google hacking
  - DNS information
  - Domain searches
- Scanning activities
  - IP & port scanning
  - TCP/IP stack fingerprinting (OS detection)
  - Service identification

What is important information?
What information is valuable and to whom?

I would like to take this time to welcome you to our hiring process and give you a brief synopsis of the position's benefits and requirements.

If you are taking a career break, are on a maternity leave, recently retired or simply looking for some part-time job, this position is for you.

Occupation: Flexible schedule 2 to 8 hours per day. We can guarantee a minimum 20 hrs/week occupation
Salary: Starting salary is 2000 EUR per month plus commission, paid every month.
Business hours: 9:00 AM to 5:00 PM, MON-FRI, 9:00 AM to 1:00 PM SAT or part time (Europe time).

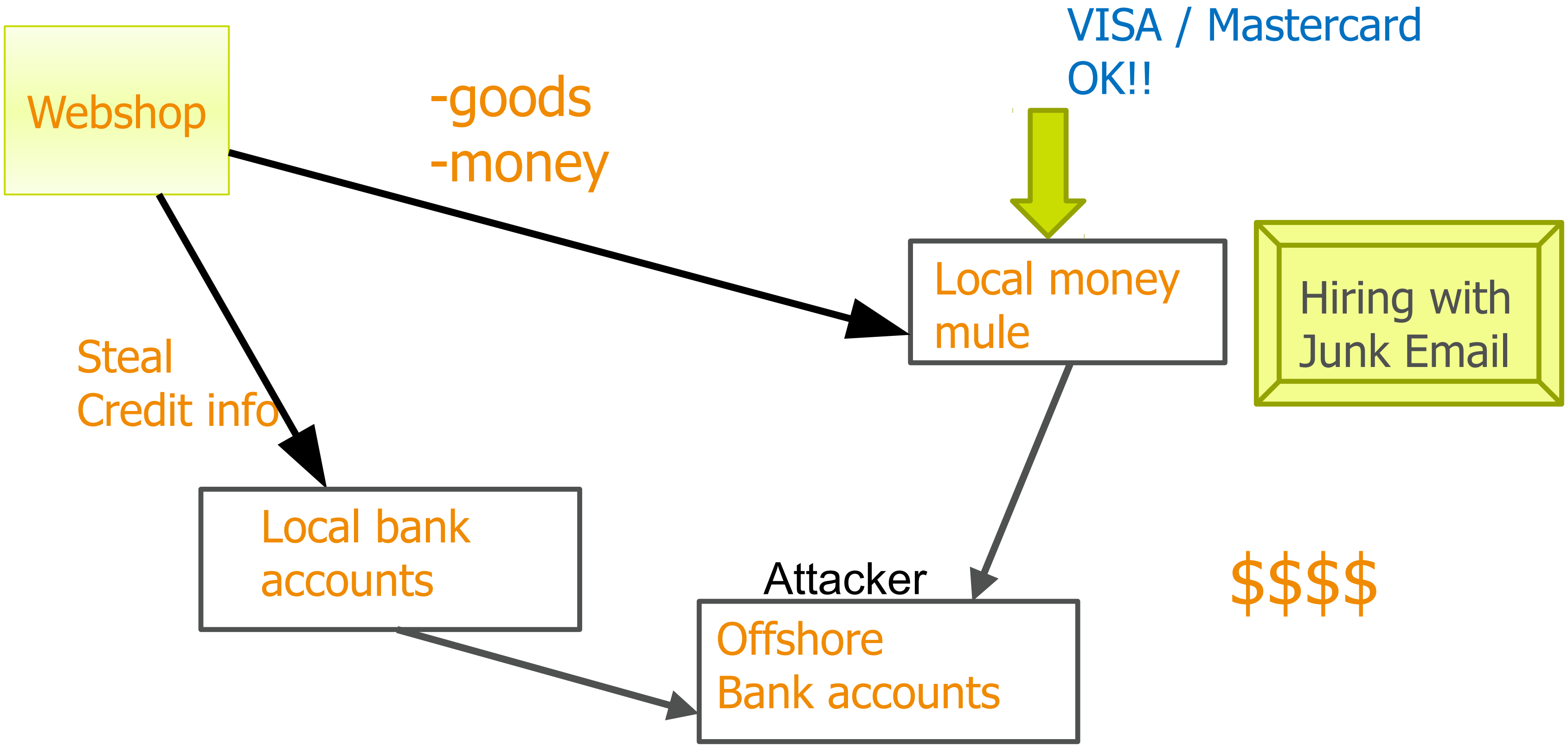
Region: Europe.

Please note that there are no startup fees or deposits to start working for us.

To request an application form, schedule your interview and receive more information about this position

- please reply to Sherman@eceuropaeu.com,with your personal identification number for this position IDNO: 9446

Internet crimes



Webshop

-goods
-money

VISA / Mastercard
OK!!

Local money mule

Hiring with Junk Email

Steal
Credit info

Local bank accounts

Attacker

Offshore
Bank accounts

$$$$

Internet crimes

Webshop

- Sell articles cheaply
- Create large customer database

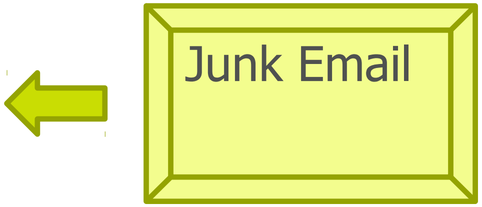
Junk Email

- Place an unresistable offer
- Collect orders with advance payouts

- Don’t deliver, close the shop and sell customer information
  - Email addresses to junk emailers
  - Account & credit card info to black market

Internet crimes

- Advance payment frauds
- Nigerian letters
  - Inheritance / business proposals
  - Re-victimization


Junk Email

- Basically many of crimes seen in the Internet are old fraud types just performed online

- If sounds too good to be true, it most likely is

Reconnaissance

- ***Reconnaissance*** *is the military term for exploring beyond the area occupied by friendly forces to gain information about enemy forces or features of the environment [Wikipedia]*
- Reconnaissace is very important step in the cyber warfare and system compromising
  - Makes it possible to find the weakest point of target system
  - Many occasions it is possible to gain first foothold with careful reconnaissance activities

Reconnaissance

- Passive reconnaissance
  - No connections directly to the target organization
  - Browsing web-pages
  - Searching information about the organization
    - Administrators, users, managers
    - DNS names
- Active reconnaissance
  - Scanning activities
  - Talking to people of the organization

Google hacking and social engineering

- Google hacking
  - Using Google to search information about target
  - Many organizations reveal more information than they realize
- Google hacking is a lot of FUN!
- Google hacking is information gathering therefore closely related to sosial engineering

Google hacking

- **Normal hacking procedure**
  - Select a site / organization that you want to break in
  - Investigate target system
  - Find vulnerable servers / software
  - Exploit and cover tracks
- **Google hacking procedure**
  - Select a vulnerability that you are going to use
  - Use Google to find a site vulnerable for that exploit
  - Expoit and see if you found anything interesting

Legality of Google hacking

- It is not a crime to use Google and search for information
- But if you do find something that could be exploited, it is not legal to use it

- So you can search and you can look at information, but you should not exploit weak points
- Also ethical hacker should notify responsible persons of the organization in case something is found

Google hacking basics

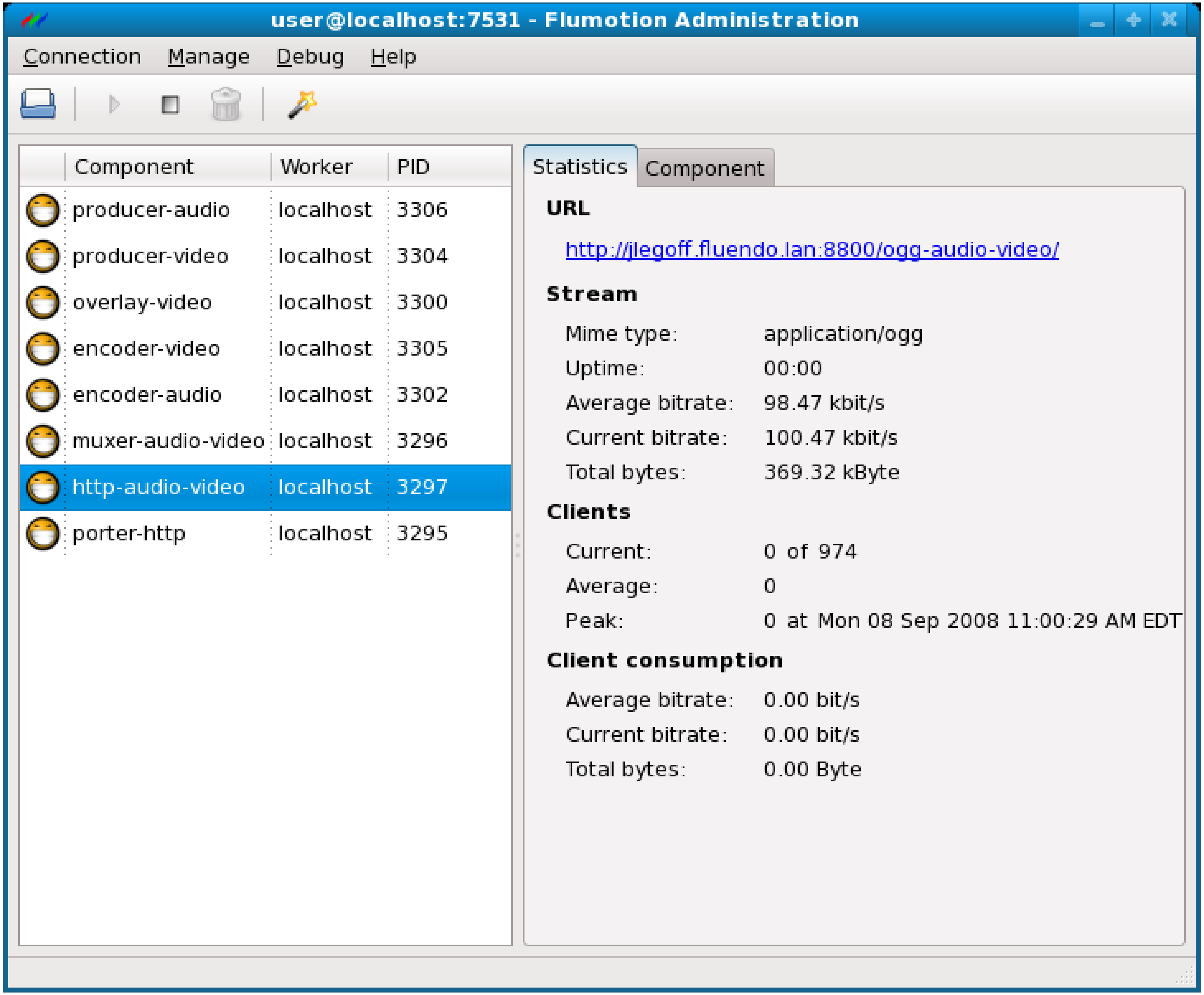
- Google does not support wildcards in a word
  - so 'hack*' does not work
- Google suppors automatic word stemming
  - so if you look for 'hack', you will get results for 'hackers', 'hacks' ,'hacking' and so on.
- Google suppors letter wild cards
  - 'r..ts' will find 'raats' 'riits' 'ruots' and so on
- Google supports word wildcards
  - So searching for 'project * was a succes' will work

Google hacking basics

- Basic search limitation methods:
  inurl:hacker -> in url part of the webpage
  intitle:secret -> in title part of the webpage
  +mp3 -> mp3 has to be in the results
  -boring -> exclude boring parts
  filetype:pdf -> find pdf filetypes
  site:www.metropolia.fi -> search only Metropolia
  link:www.metropolia.fi -> who links to Metropolia

Google hacking basics

- Holy grail of interesting information: Directory listings
  ”index of” site:www.metropolia.fi
  ”index of” site:metropolia.fi
  ”parent directory”
- Directory listings are information that is often shared to internet by accident
  - Web-server misconfigurations
  - Failure to restrict directory traversal
  - Copy paste mistakes
  - Using personal web-page directories as a personal storage place
- Use empty index.html in your web-directory if you don’t want this to happen



Component	Worker	PID
producer-audio	localhost	3306
producer-video	localhost	3304
overlay-video	localhost	3300
encoder-video	localhost	3305
encoder-audio	localhost	3302
muxer-audio-video	localhost	3296
http-audio-video	localhost	3297
porter-http	localhost	3295

URL

http://jlegoff.fluendo.lan:8800/ogg-audio-video/

Stream

Mime type:	application/ogg
Uptime:	00:00
Average bitrate:	98.47 kbit/s
Current bitrate:	100.47 kbit/s
Total bytes:	369.32 kByte

Clients

Current:	0 of 974
Average:	0
Peak:	0 at Mon 08 Sep 2008 11:00:29 AM EDT

Client consumption

Average bitrate:	0.00 bit/s
Current bitrate:	0.00 bit/s
Total bytes:	0.00 Byte

Why Google hacking is so effective?

- Find out how does the admin page look like
- Find out the default url

- And search for those in Google
  - You will be supriced what you can find

- Think and try to guess following also
  - Page titles
  - Directory names (URLs)
  - Page information

- And now let’s see what we can find!

Problems with Google hacking

- Google has taken actions against automated Google hacking
  - If you generate a lot of Google hacking queries, Google starts to limit your searching
    - CAPTCHA testing and temporally limiting access to Google
- You can evade this by using web proxies
  - There are a lot of free web proxies available
  - Use one of those and your organization does not get banned for using Google

Social engineering

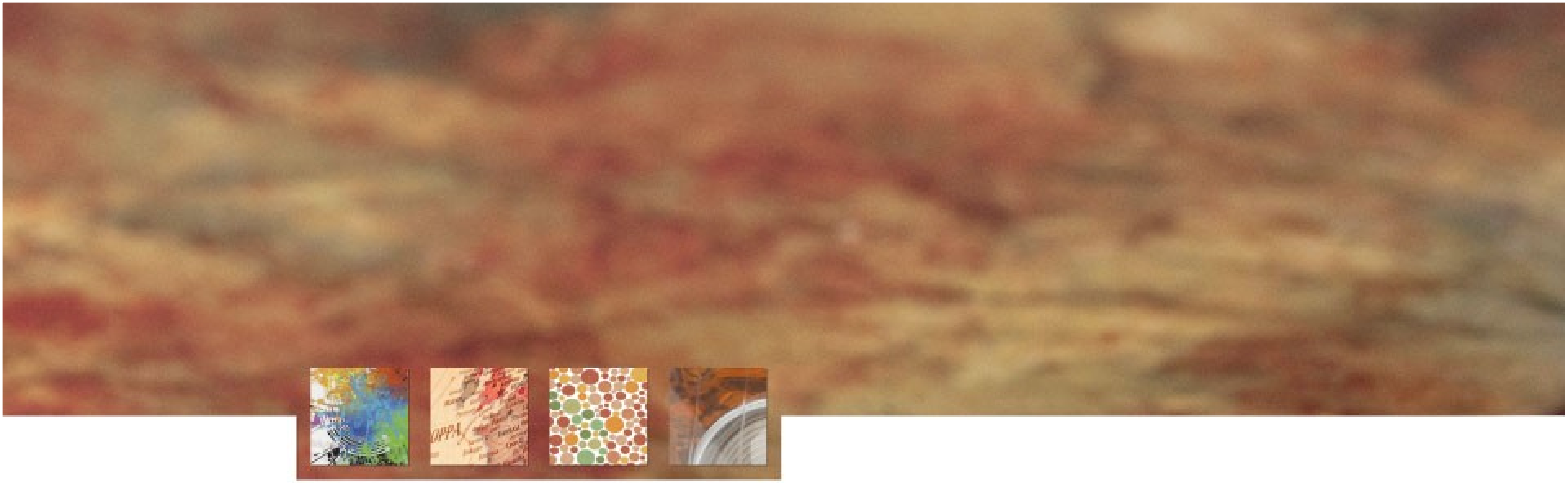
- Is extremely effective method to do reconnaissance

- Combined with simple email / web-site / DNS forgery you can easily get peoples password and login information
  - Actually it is so effective that we banned the usage of these methods in finnish practical attack & defence course
- Social media makes social engineering a lot easier

Google hacking database

- Google hacking is art and skill

- To learn more
  - http://www.hackersforcharity.org/ghdb/
  - http://www.exploit-db.com/google-dorks/



www.metropolia.fi/en
kimmo.sauren@metropolia.fi

Helsinki
Metropolia
University of Applied Sciences