How to penetrate the company`s network?

Passive and active reconnaissance

A practical case about KEA

Please read the following example case scenario about KEA.

You will find the requirements for this assignment at the end of the document!

1.Introduction

Many times the security tester is given just a name of the company , who hired him to test the network security. Of course , he could be given a contract with permission to do that ,and let`s assume he already signed the documents for the job. So , he knows the company `s name , but nothing else. That is what is called the black box model. He doesn`t know how big is the company , what actually they possess ,for example – if they have a physical office or just an online one , if they are situated in Morocco or in the USA ,and so on and so on. Well ,it looks like he has a lot of things to find out. The most important in this case is for the tester to have a logical thinking , and also to have a notepad and to write every info he finds out inside.

2. Structure of the company`s network

In order for you to penetrate or test the company`s network you have to visualize it in your brain and make a structure of it (usually using diagrams). This will help you see better how it is organized , how big is it and will give you some clues on which way to go next.

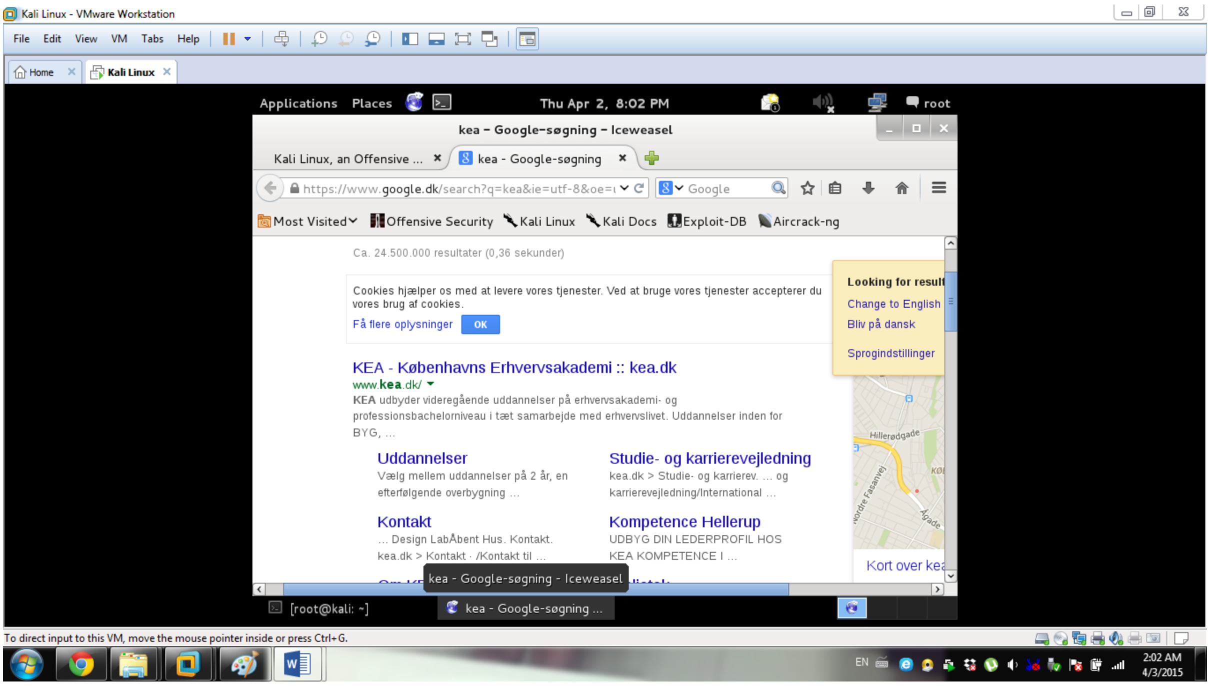
3.A practical case using passive and active recoinnnasance

Let`s assume you have been given just a name : KEA.

Ok , what is it? It should be some type of organization right? The first and the most important stage of a penetration test is gathering information about the target. We use passive and active techniques to do that ,depending on our scope. Since I do not have a permission to scan the company`s network or to exploit it (and you are not encouraged to do that either !!!) , I will just search for some information online about my target. Well everybody has done that before , wheather he has been stalking his girlfriend on the social websites , or internet forums , or just digging some information about a specific company online. Let`s begin.

4.Simple steps when gathering information

- The first logical thing to do is just to open up my web browser and type in KEA.



Ca. 24.500.000 resultater (0,36 sekunder)

Cookies hjælper os med at levere vores tjenester. Ved at bruge vores tjenester accepterer du vores brug af cookies.

Få flere oplysninger OK

KEA - Københavns Erhvervsakademi :: kea.dk
www.kea.dk/
KEA udbyder videregående uddannelser på erhvervsakademi- og professionsbachelorniveau i tæt samarbejde med erhvervslivet. Uddannelser inden for BYG, ...

Uddannelser
Vælg mellem uddannelser på 2 år, en efterfølgende overbygning ...

Studie- og karrierevejledning
kea.dk > Studie- og karrierev. ... og karrierevejledning/International ...

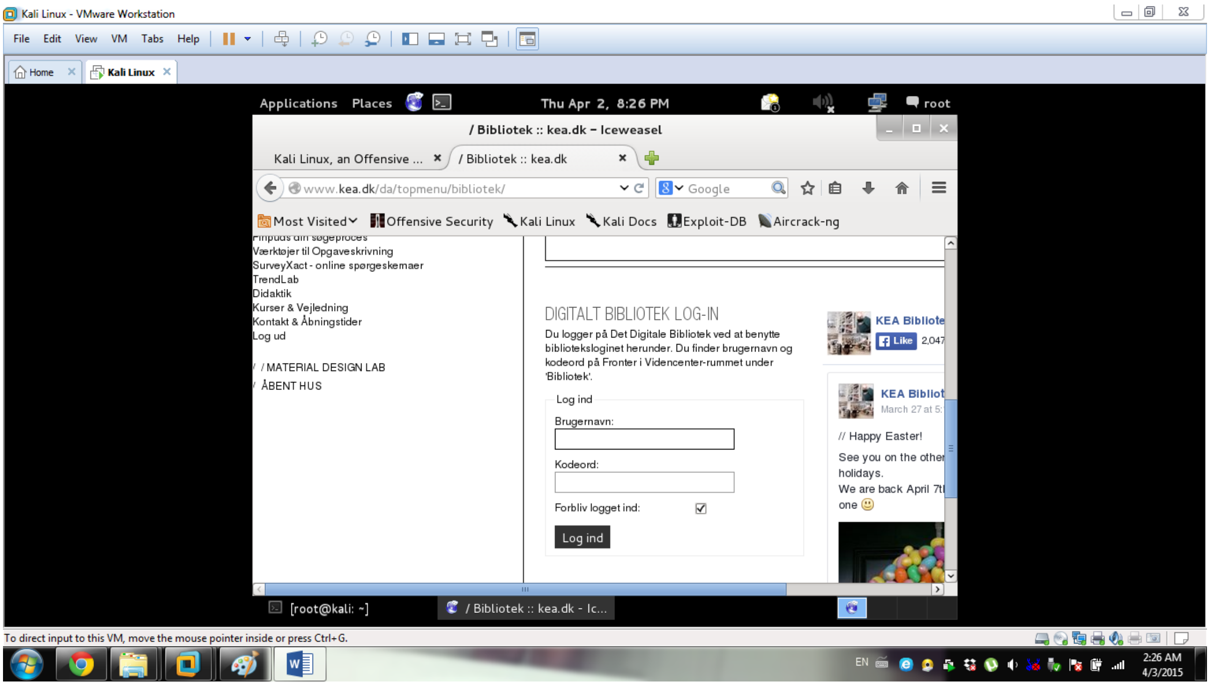
Kontakt
... Design LabÅbent Hus. Kontakt. kea.dk > Kontakt · /Kontakt til ...

Kompetence Hellerup
UDBYG DIN LEDERPROFIL HOS KEA KOMPETENCE I ...

Ok. The first result is KEA – Kobenhavns Ehrversakademy and it gives me a website right : www.kea.dk

So they have a website . Websites usually are standing on webservers. If the company is rich they can afford to buy and to maintain a webserver themselves. If not , they just pay to a hosting company to use a space on their webserver . I can try to find the IP address of this webserver. I write it down in my notebook. Second thing to do is to open the website.Most of the recent websites nowadays are Not static ones. A static website means it is not changing ,it just shows the same thing every time you open it. Modern websites like amazon , facebook , google and so on are dynamic ones(they change dynamically and are constantly synchronizing with the backend applications).Usually a website like ebay for example has got an SQL backend ,which contains all the items with their prices and name ,number and so on. As soon as the price is changed in the backend ,the frontend syncronyzes and also changes the price that you see.A very famous attack on this is called an SQL injection – you are attacking the backend SQL ,changing something ,without the rights to do that.(for example if you can do a successful SQL injection attack you can manipulate the oroginal price of an item on ebay and buy it for cents)

Another very important feature of the modern websites is that some of them are also applications.It means that you are presented with a field to log in with username and password . Since websites are representing the company itself , they are giving information and so on to the people ,they have to be exposed to the public, so that everybody can be able to open them. Many of them suffer from a vulnerability called XSS cross site scripting or Code injection attacks. I found the following:



Værktøjer til Opgaveskrivning
SurveyXact - online spørgeskemaer
TrendLab
Didaktik
Kurser & Vejledning
Kontakt & Åbningstider
Log ud

/ MATERIAL DESIGN LAB
ÅBENT HUS

DIGITALT BIBLIOTEK LOG-IN

Du logger på Det Digitale Bibliotek ved at benytte biblioteksloginet herunder. Du finder brugernavn og kodeord på Fronter i Videncenter-rummet under 'Bibliotek'.

Log ind

Brugernavn:

Kodeord:

Forbliv logget ind: ☑

Log ind

KEA Bibliote
Like 2,047

KEA Bibliot
March 27 at 5:

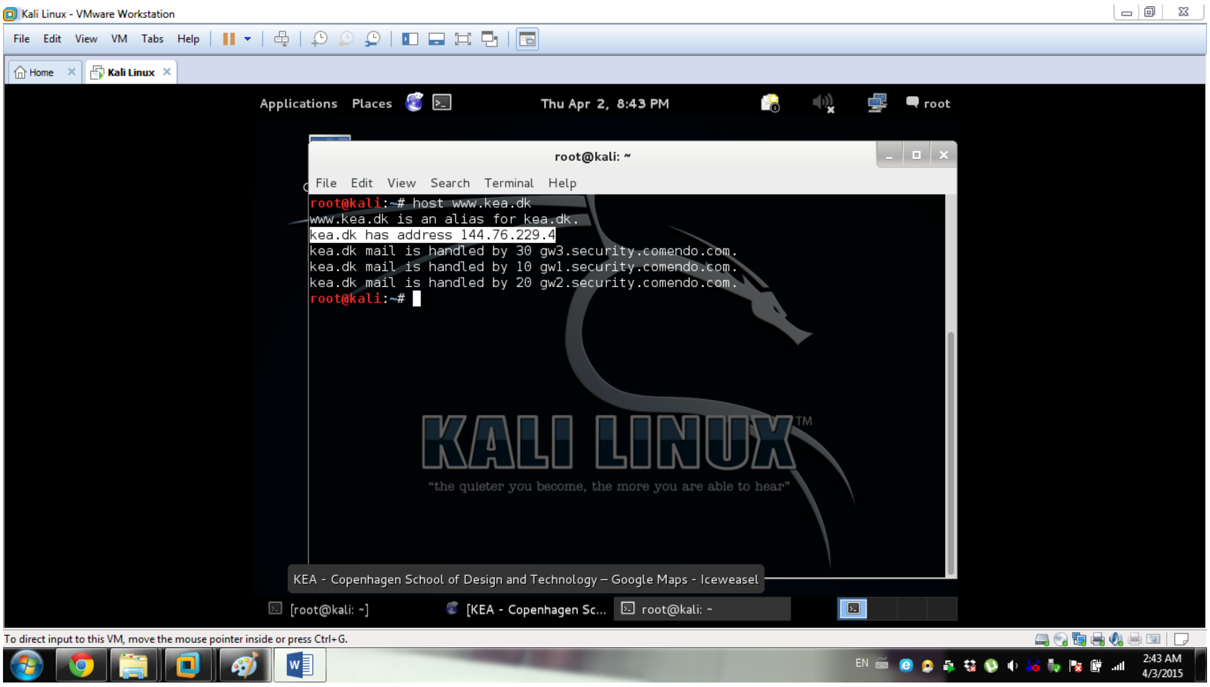
// Happy Easter!

See you on the other holidays.
We are back April 7t one 🙂

[root@kali: ~]
/ Bibliotek :: kea.dk - Ic...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
EN
2:26 AM
4/3/2015

It is a form I can put my username and pasword. If I can ,by any chance ,to log in as administrator ,then I can borrow books from the library or do other types of damage to the organization.I can run vulnerability scanners against the website ,which are called web spiders or crawlers , which can find something. I write it down in my notebook.

- The next thing I need to know is IP adresses. In order to run tests , you need to know the exact IP adresses ,computers find each other with IP adresses. I am using the command host.Here:



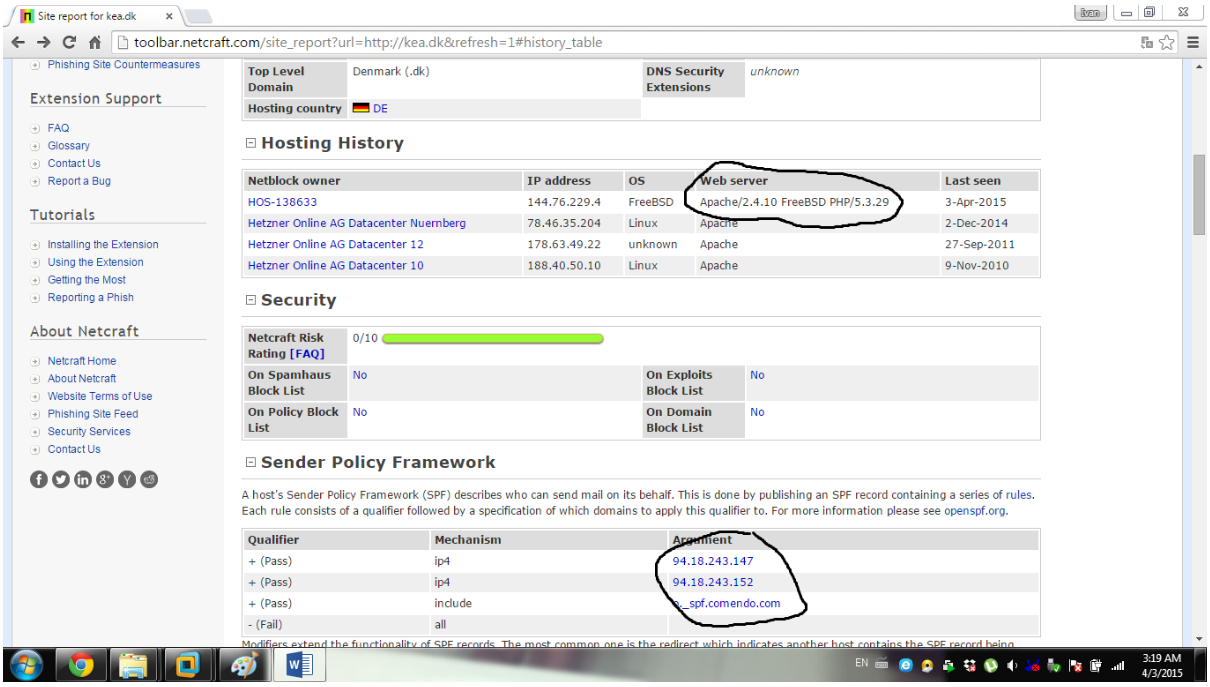
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
Applications Places
Thu Apr 2, 8:43 PM
root
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# host www.kea.dk
www.kea.dk is an alias for kea.dk.
kea.dk has address 144.76.229.4
kea.dk mail is handled by 30 gw3.security.comendo.com.
kea.dk mail is handled by 10 gw1.security.comendo.com.
kea.dk mail is handled by 20 gw2.security.comendo.com.
root@kali:~# 
```

KALI LINUX™
"the quieter you become, the more you are able to hear"
KEA - Copenhagen School of Design and Technology – Google Maps - Iceweasel
[root@kali: ~]
[KEA - Copenhagen Sc...
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
EN
2:43 AM
4/3/2015

Ok ,I see that the webserver ,running KEA`s website has got IP address. I can see that they also have a mail server. Unfortunately it is managed by another company and I cannot see its IP adress. Now that I know the IP of the webserver I can do port scanning and see what services he is running – what ports he got open.If he is behind a firewall ,my scan will show that all ports are closed or filtered. Well this will not be true , since we know what the webserver is actually doing: he receives requests from the clients` browsers and replies back to them. I assume ,even without scanning ,that he will have ports 80 (HHTP) and port 443 (HTTPS) open. I can try to get inside through there .Of course that is not so easy as it sounds,cause more likely they will be filtered by a firewall.Usually you need to have a permission to scan company`s servers , since your scan can trigger some alarms or crash a service on the target.

- I need more IP addresses .I am gonna use a website that is called Netcraft.Here are theresults:



Top Level Domain	Denmark (.dk)	DNS Security Extensions	unknown
Hosting country	DE		

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen
HOS-138633	144.76.229.4	FreeBSD	Apache/2.4.10 FreeBSD PHP/5.3.29	3-Apr-2015
Hetzner Online AG Datacenter Nuernberg	78.46.35.204	Linux	Apache	2-Dec-2014
Hetzner Online AG Datacenter 12	178.63.49.22	unknown	Apache	27-Sep-2011
Hetzner Online AG Datacenter 10	188.40.50.10	Linux	Apache	9-Nov-2010

⊟ Security

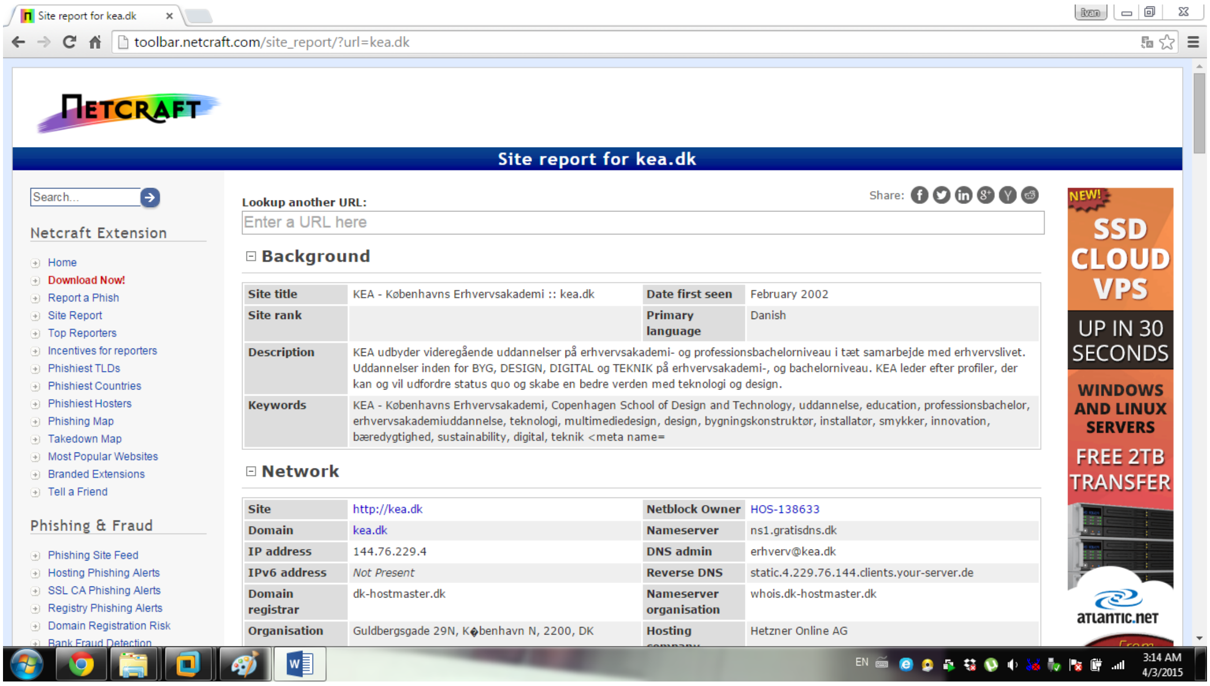
Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

⊟ Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Qualifier	Mechanism	Argument
+ (Pass)	ip4	94.18.243.147
+ (Pass)	ip4	94.18.243.152
+ (Pass)	include	o._spf.comendo.com
- (Fail)	all	

Modifiers extend the functionality of SPF records. The most common one is the redirect which indicates another host contains the SPF record being



Site report for kea.dk

Lookup another URL:

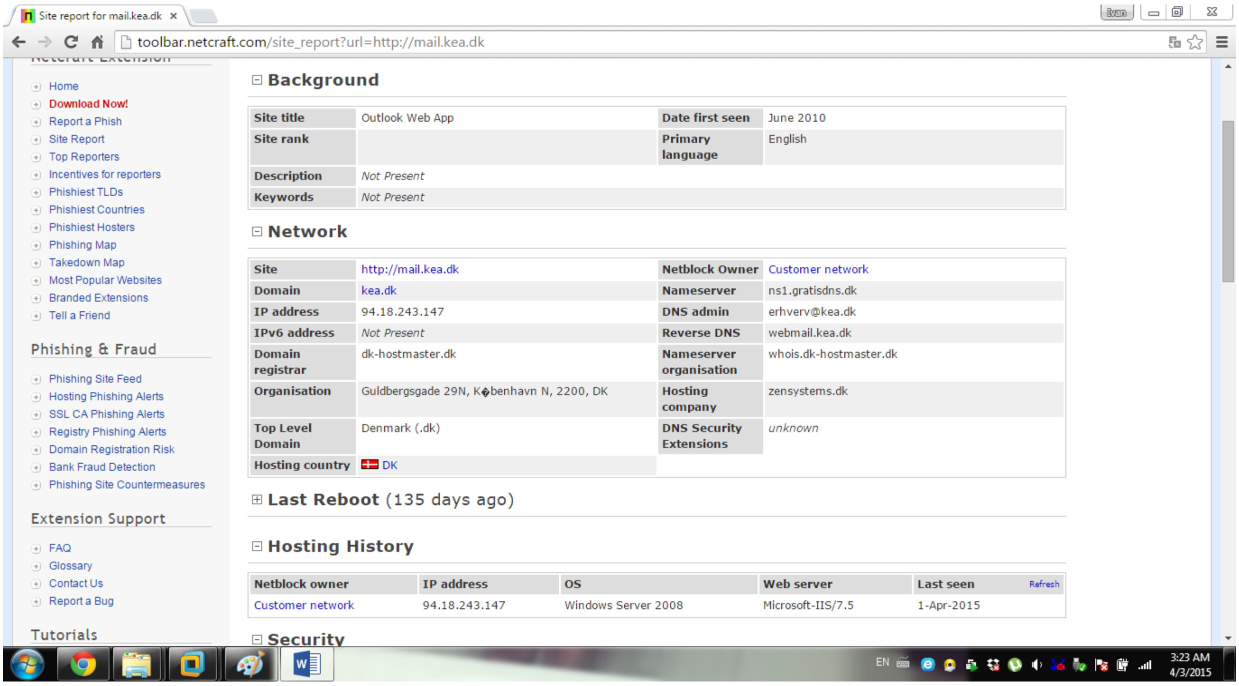
Enter a URL here

⊟ Background

Site title	KEA - Københavns Erhvervsakademi :: kea.dk	**Date first seen**	February 2002
Site rank		**Primary language**	Danish
Description	KEA udbyder videregående uddannelser på erhvervsakademi- og professionsbachelorniveau i tæt samarbejde med erhvervslivet. Uddannelser inden for BYG, DESIGN, DIGITAL og TEKNIK på erhvervsakademi-, og bachelorniveau. KEA leder efter profiler, der kan og vil udfordre status quo og skabe en bedre verden med teknologi og design.		
Keywords	KEA - Københavns Erhvervsakademi, Copenhagen School of Design and Technology, uddannelse, education, professionsbachelor, erhvervsakademiuddannelse, teknologi, multimediedesign, design, bygningskonstruktør, installatør, smykker, innovation, bæredygtighed, sustainability, digital, teknik <meta name=		

⊟ Network

Site	http://kea.dk	**Netblock Owner**	HOS-138633
Domain	kea.dk	**Nameserver**	ns1.gratisdns.dk
IP address	144.76.229.4	**DNS admin**	erhverv@kea.dk
IPv6 address	*Not Present*	**Reverse DNS**	static.4.229.76.144.clients.your-server.de
Domain registrar	dk-hostmaster.dk	**Nameserver organisation**	whois.dk-hostmaster.dk
Organisation	Guldbergsgade 29N, K�benhavn N, 2200, DK	**Hosting**	Hetzner Online AG



⊟ Background

Site title	Outlook Web App	**Date first seen**	June 2010
Site rank		**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

⊟ Network

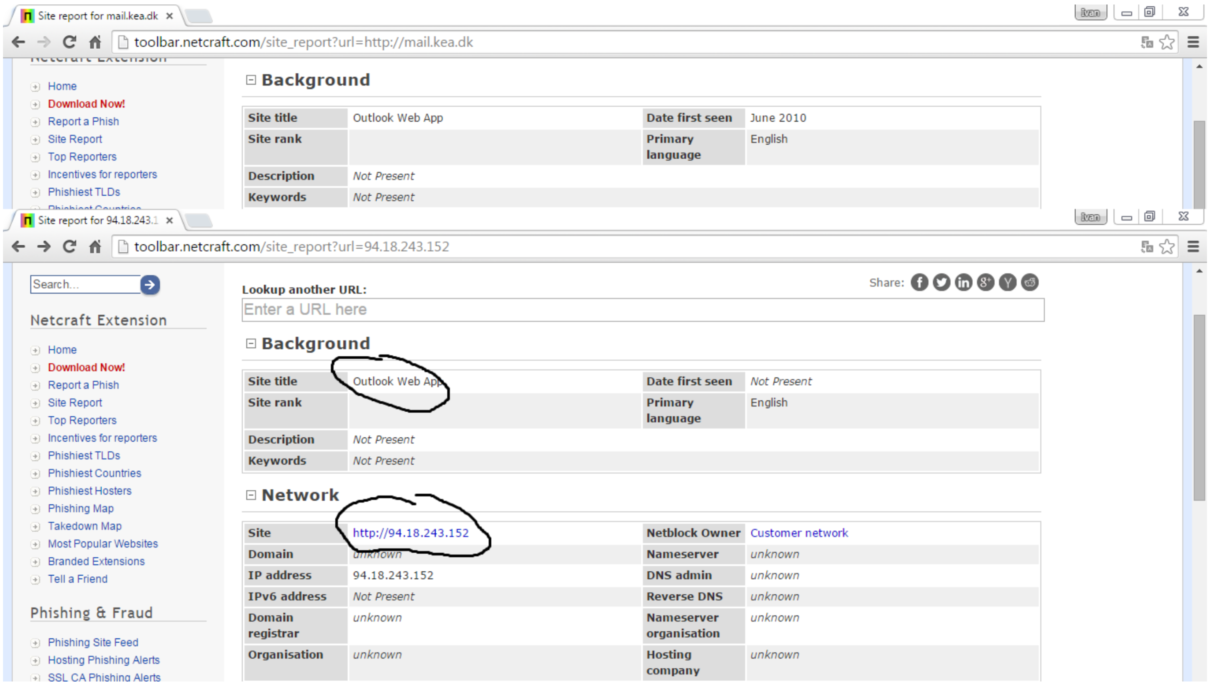
Site	http://mail.kea.dk	**Netblock Owner**	Customer network
Domain	kea.dk	**Nameserver**	ns1.gratisdns.dk
IP address	94.18.243.147	**DNS admin**	erhverv@kea.dk
IPv6 address	*Not Present*	**Reverse DNS**	webmail.kea.dk
Domain registrar	dk-hostmaster.dk	**Nameserver organisation**	whois.dk-hostmaster.dk
Organisation	Guldbergsgade 29N, K�benhavn N, 2200, DK	**Hosting company**	zensystems.dk
Top Level Domain	Denmark (.dk)	**DNS Security Extensions**	*unknown*
Hosting country	DK		

⊞ Last Reboot (135 days ago)

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Customer network	94.18.243.147	Windows Server 2008	Microsoft-IIS/7.5	1-Apr-2015

⊟ Security



toolbar.netcraft.com/site_report?url=http://mail.kea.dk

Background

Site title	Outlook Web App	Date first seen	June 2010
Site rank		Primary language	English
Description	Not Present		
Keywords	Not Present		

toolbar.netcraft.com/site_report?url=94.18.243.152

Lookup another URL:

Background

Site title	Outlook Web App	Date first seen	Not Present
Site rank		Primary language	English
Description	Not Present		
Keywords	Not Present		

Network

Site	http://94.18.243.152	Netblock Owner	Customer network
Domain	unknown	Nameserver	unknown
IP address	94.18.243.152	DNS admin	unknown
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	unknown

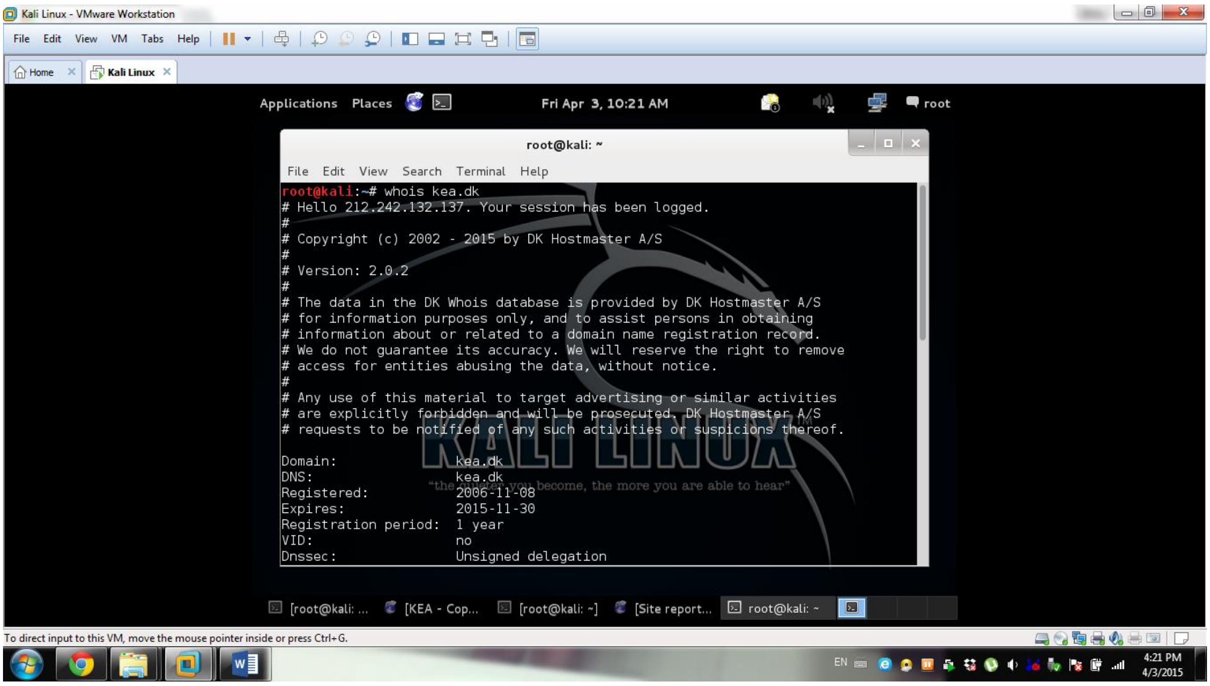
Ok to summarize our findings up to here:

1.We can see that the webserver is hosted by a german company in Nurnberg. Also the DNS server `s hosting company.It is very important to know the DNS`s server IP. I can try to do zone transfer , this means to copy all the IP addresses that this DNS server knows .This is very important information.Another thing I can do is , if I can masquarade as this DNS server , all the requests will come to my machine. I can send them to anywhere they want – fishy websites ,and so on.

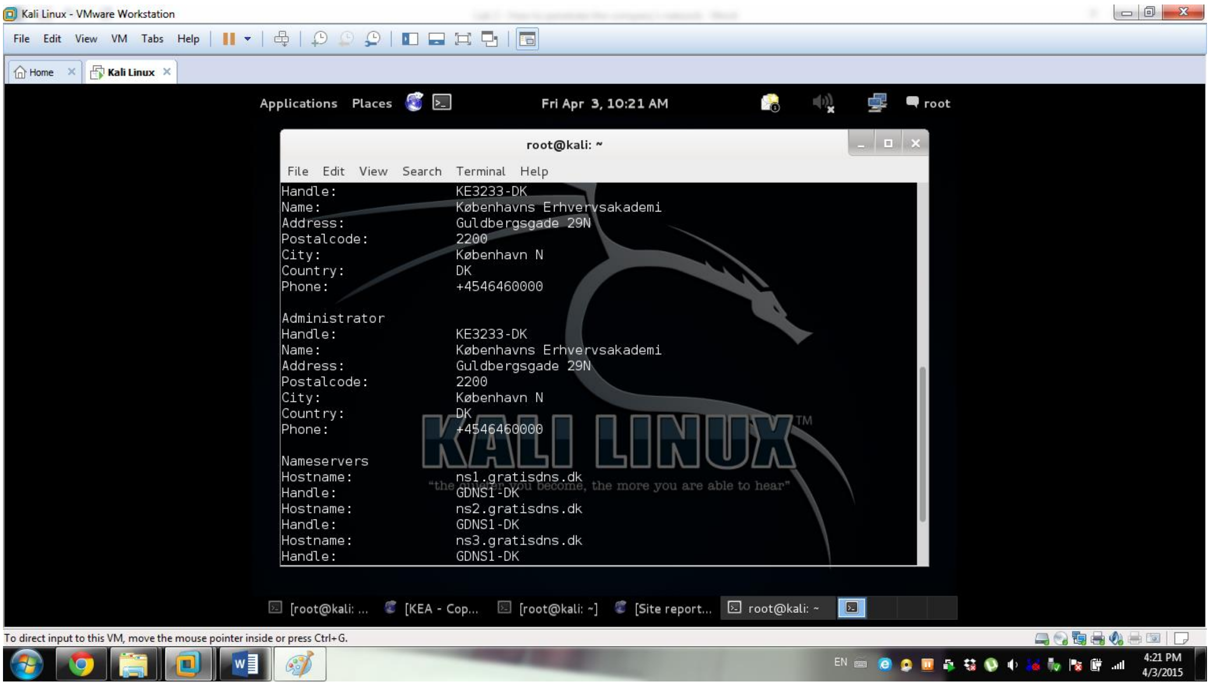
2.The version of software ,running on the webserver.The IP of the mail server of KEA + the version its running.If I know the version I am checking for vulnerabilities online.The server is running Apache version 2.4.10 , which I think is outdated and should be patched to the latest one. A quick google search tells me that the latest version now is 2.4.12.

3.The physical address of KEA. Using google maps we can see that is building. Well if they have an office,they have also people working in it. All of these people have computers,which are running on an internal network.If they have an internal network , they have routers ,switches and so on. We can try attacking the routers directly.Or we can use social engineering. Once you get on the internal network , you can try to navigate through different machines , until you find what you are looking for. In order to try some attacks on the company`s routers you need to be in close range, for example inside the building , or in a car , parked near by.

- Next I will use a tool called whois to understand the DNS servers , responsible for kea.dk.Simly type in:


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
Applications Places
Fri Apr 3, 10:21 AM
root
root@kali: ~
File Edit View Search Terminal Help
[root@kali: ... [KEA - Cop... [root@kali: ~] [Site report... root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
EN
4:21 PM
4/3/2015

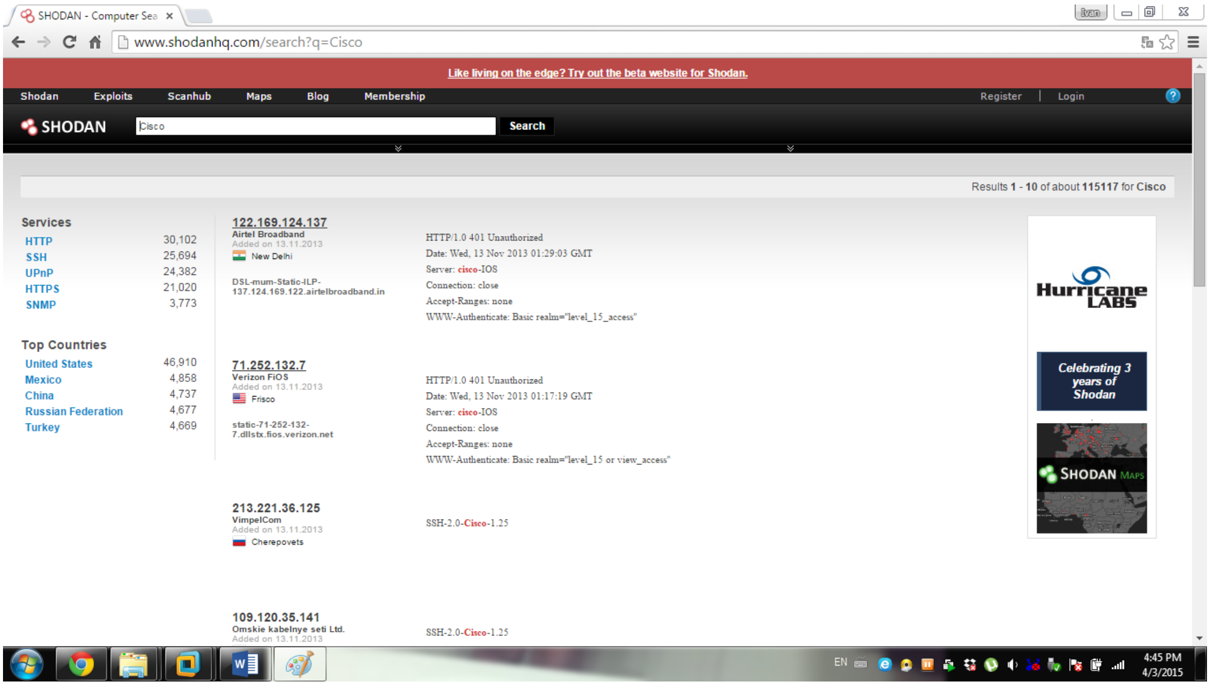
```
root@kali:~# whois kea.dk
# Hello 212.242.132.137. Your session has been logged.
#
# Copyright (c) 2002 - 2015 by DK Hostmaster A/S
#
# Version: 2.0.2
#
# The data in the DK Whois database is provided by DK Hostmaster A/S
# for information purposes only, and to assist persons in obtaining
# information about or related to a domain name registration record.
# We do not guarantee its accuracy. We will reserve the right to remove
# access for entities abusing the data, without notice.
#
# Any use of this material to target advertising or similar activities
# are explicitly forbidden and will be prosecuted. DK Hostmaster A/S
# requests to be notified of any such activities or suspicions thereof.

Domain:               kea.dk
DNS:                  kea.dk
Registered:           2006-11-08
Expires:              2015-11-30
Registration period:  1 year
VID:                  no
Dnssec:               Unsigned delegation
```


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
Applications Places
Fri Apr 3, 10:21 AM
root
root@kali: ~
File Edit View Search Terminal Help
[root@kali: ... [KEA - Cop... [root@kali: ~] [Site report... root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
EN
4:21 PM
4/3/2015

```
Handle:               KE3233-DK
Name:                 Københavns Erhvervsakademi
Address:              Guldbergsgade 29N
Postalcode:           2200
City:                 København N
Country:              DK
Phone:                +4546460000

Administrator
Handle:               KE3233-DK
Name:                 Københavns Erhvervsakademi
Address:              Guldbergsgade 29N
Postalcode:           2200
City:                 København N
Country:              DK
Phone:                +4546460000

Nameservers
Hostname:             ns1.gratisdns.dk
Handle:               GDNS1-DK
Hostname:             ns2.gratisdns.dk
Handle:               GDNS1-DK
Hostname:             ns3.gratisdns.dk
Handle:               GDNS1-DK
```

As you can see , the hosting company is not very happy when somebody is digging info about their servers ☺ So they will log my session and my IP. Well , I can evade this , if I use a VPN connection and change my IP to Nigeria for example ☺ The most important here is that I can see the DNS servers. I can use different tools, which are built into Kali , in order to try to do a zone transfer from them. Tools for this are nslookup ,dig and fierce.You have to be very careful when using them.Fierce is actually an interrogation tool , which will try to bruteforce his way through the DNS server to get into it. You are not advised to do that ,without any special permission from the company though !!!!!

- For my next exercise I will use a website called Shodan. It is usually called the Hacker`s Google.It allows you to search for computers on the web ,in the entire world by putting a keyword. All kinds of machines could be found here.From routers to smartphones , servers , desktops , even security cameras ,elevators,embedded systems and all kind of devices which are run by an operating system. Simply type in :Shodanhq.com:



Results 1 - 10 of about 115117 for Cisco

Services

HTTP	30,102
SSH	25,694
UPnP	24,382
HTTPS	21,020
SNMP	3,773

Top Countries

United States	46,910
Mexico	4,858
China	4,737
Russian Federation	4,677
Turkey	4,669

122.169.124.137
Airtel Broadband
Added on 13.11.2013
New Delhi
DSL-mum-Static-ILP-137.124.169.122.airtelbroadband.in

```
HTTP/1.0 401 Unauthorized
Date: Wed, 13 Nov 2013 01:29:03 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15_access"
```

71.252.132.7
Verizon FiOS
Added on 13.11.2013
Frisco
static-71-252-132-7.dllstx.fios.verizon.net

```
HTTP/1.0 401 Unauthorized
Date: Wed, 13 Nov 2013 01:17:19 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15 or view_access"
```

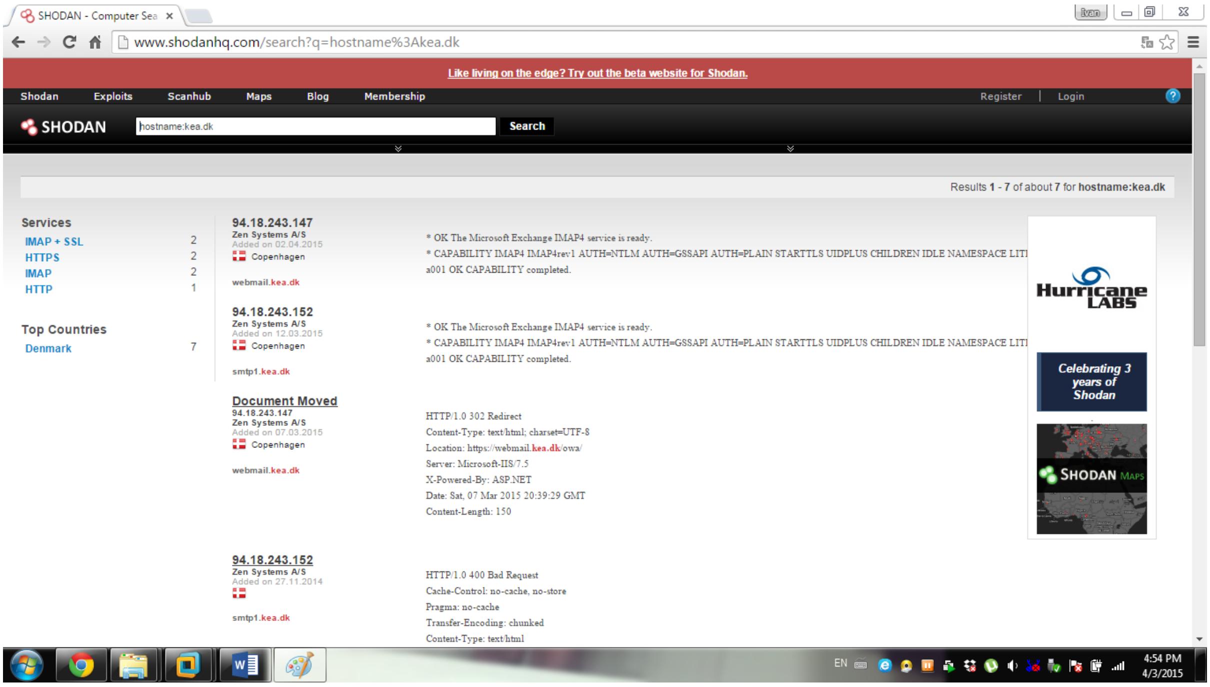
213.221.36.125
VimpelCom
Added on 13.11.2013
Cherepovets

```
SSH-2.0-Cisco-1.25
```

109.120.35.141
Omskie kabelnye seti Ltd.
Added on 13.11.2013

```
SSH-2.0-Cisco-1.25
```

If I simply type in :Cisco in the search bar , the site presents me with thousands of devices worldwide.If I type in hostname:kea.dk



Results 1 - 7 of about 7 for hostname:kea.dk

Services

IMAP + SSL	2
HTTPS	2
IMAP	2
HTTP	1

Top Countries

Denmark	7

94.18.243.147
Zen Systems A/S
Added on 02.04.2015
Copenhagen
webmail.kea.dk

```
* OK The Microsoft Exchange IMAP4 service is ready.
* CAPABILITY IMAP4 IMAP4rev1 AUTH=NTLM AUTH=GSSAPI AUTH=PLAIN STARTTLS UIDPLUS CHILDREN IDLE NAMESPACE LITI
a001 OK CAPABILITY completed.
```

94.18.243.152
Zen Systems A/S
Added on 12.03.2015
Copenhagen
smtp1.kea.dk

```
* OK The Microsoft Exchange IMAP4 service is ready.
* CAPABILITY IMAP4 IMAP4rev1 AUTH=NTLM AUTH=GSSAPI AUTH=PLAIN STARTTLS UIDPLUS CHILDREN IDLE NAMESPACE LITI
a001 OK CAPABILITY completed.
```

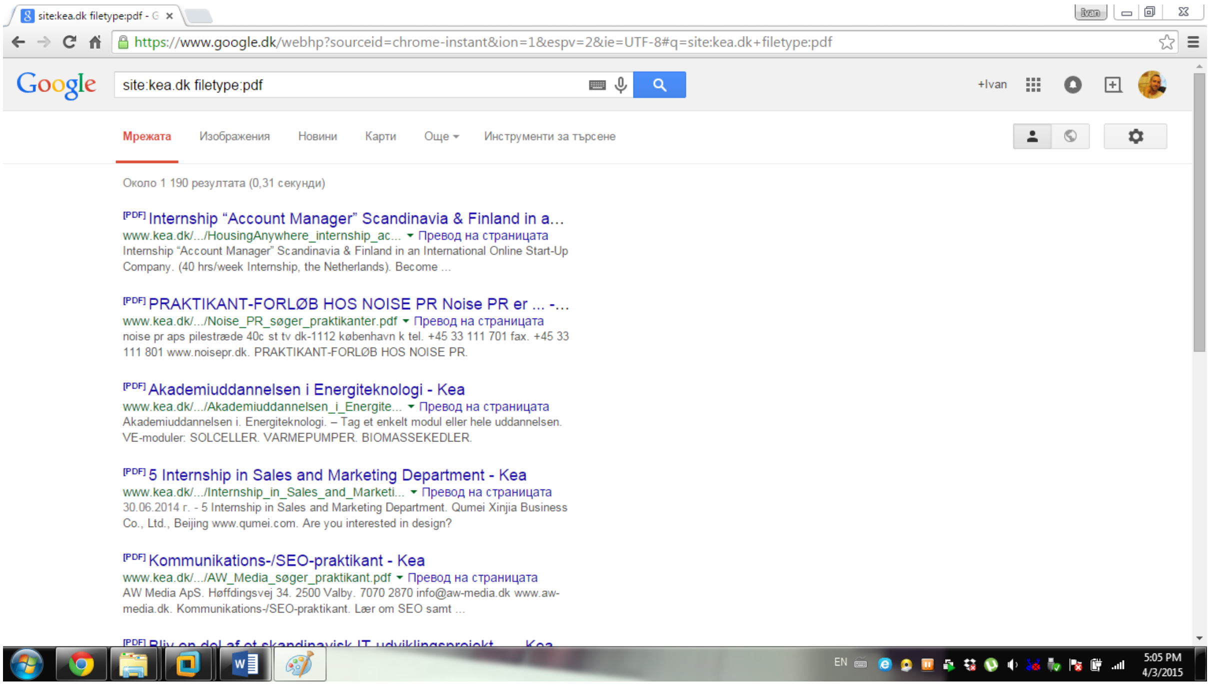
Document Moved
94.18.243.147
Zen Systems A/S
Added on 07.03.2015
Copenhagen
webmail.kea.dk

```
HTTP/1.0 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: https://webmail.kea.dk/owa/
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sat, 07 Mar 2015 20:39:29 GMT
Content-Length: 150
```

94.18.243.152
Zen Systems A/S
Added on 27.11.2014
smtp1.kea.dk

```
HTTP/1.0 400 Bad Request
Cache-Control: no-cache, no-store
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html
```

- Another great technique is called Google hacking. There is a whole book ,dedicated only on this. If you know what keywords to put into your web browser , you can narrow your search results and find out a lot of interesting things about a target.If you want to pull results only from the target`s website, the command is site:website.For example if I want to search for PDF documents only on the kea website I put :



https://www.google.dk/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=site:kea.dk+filetype:pdf

site:kea.dk filetype:pdf

Около 1 190 резултата (0,31 секунди)

[PDF] Internship “Account Manager” Scandinavia & Finland in a...
www.kea.dk/.../HousingAnywhere_internship_ac... ▾ Превод на страницата
Internship “Account Manager” Scandinavia & Finland in an International Online Start-Up Company. (40 hrs/week Internship, the Netherlands). Become ...

[PDF] PRAKTIKANT-FORLØB HOS NOISE PR Noise PR er ... -...
www.kea.dk/.../Noise_PR_søger_praktikanter.pdf ▾ Превод на страницата
noise pr aps pilestræde 40c st tv dk-1112 københavn k tel. +45 33 111 701 fax. +45 33 111 801 www.noisepr.dk. PRAKTIKANT-FORLØB HOS NOISE PR.

[PDF] Akademiuddannelsen i Energiteknologi - Kea
www.kea.dk/.../Akademiuddannelsen_i_Energite... ▾ Превод на страницата
Akademiuddannelsen i. Energiteknologi. – Tag et enkelt modul eller hele uddannelsen. VE-moduler: SOLCELLER. VARMEPUMPER. BIOMASSEKEDLER.

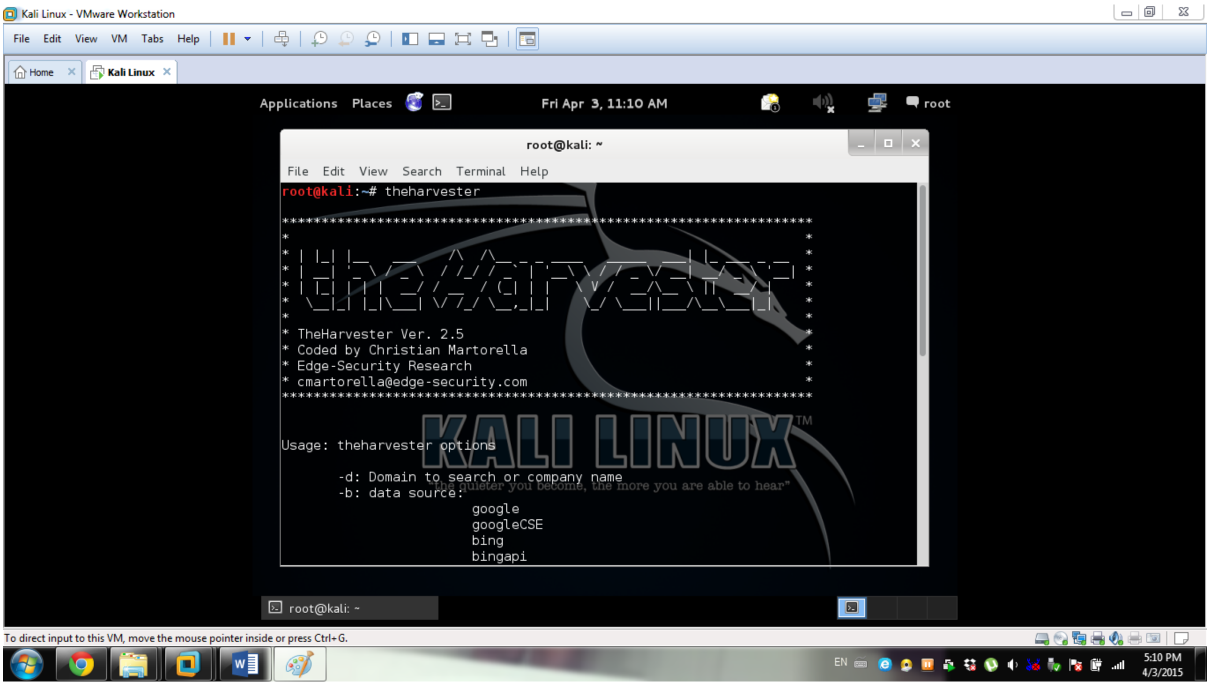
[PDF] 5 Internship in Sales and Marketing Department - Kea
www.kea.dk/.../Internship_in_Sales_and_Marketi... ▾ Превод на страницата
30.06.2014 г. - 5 Internship in Sales and Marketing Department. Qumei Xinjia Business Co., Ltd., Beijing www.qumei.com. Are you interested in design?

[PDF] Kommunikations-/SEO-praktikant - Kea
www.kea.dk/.../AW_Media_søger_praktikant.pdf ▾ Превод на страницата
AW Media ApS. Høffdingsvej 34. 2500 Valby. 7070 2870 info@aw-media.dk www.aw-media.dk. Kommunikations-/SEO-praktikant. Lær om SEO samt ...

[PDF] Bliv en del af et skandinavisk IT udviklingsprojekt ... - Kea

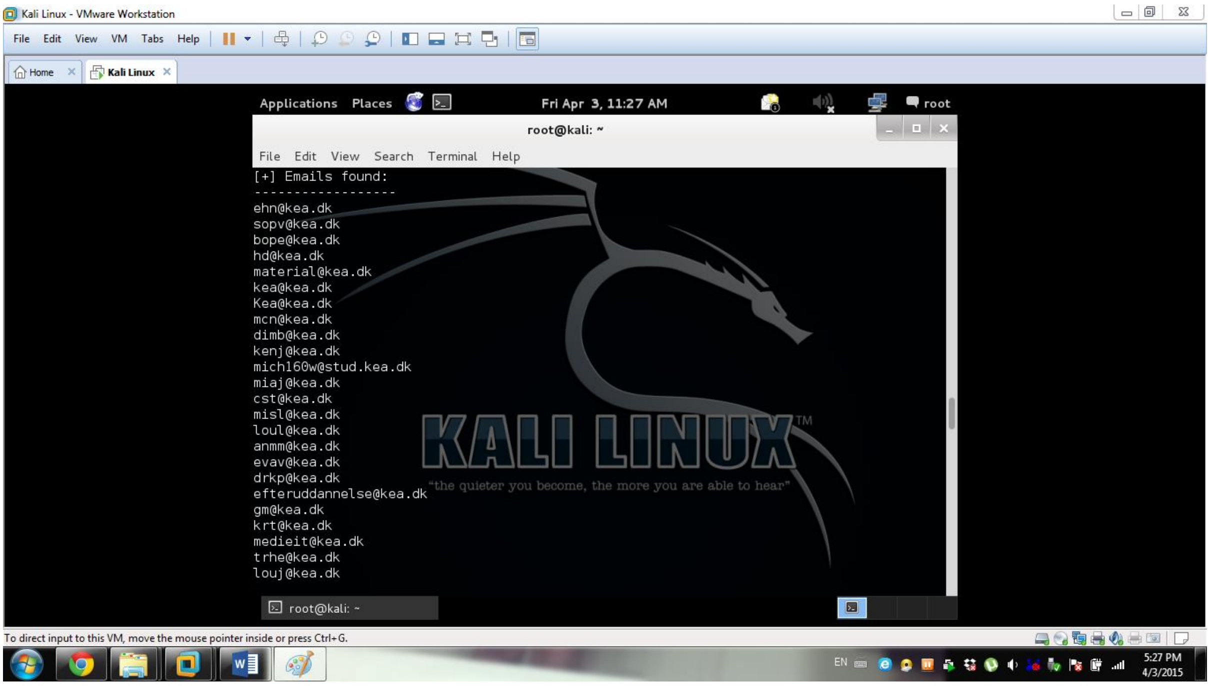
If you want to pull information about specific person only from the website , the command is :site:kea.dk *name of the person* . You can try this one and see what you will find.

- I would like to know some emails of people ,working for KEA.dk.I will use a tool called The harvester , built into Kali.Type in :theharvester in the console:


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
Applications Places
Fri Apr 3, 11:10 AM
root
root@kali: ~
File Edit View Search Terminal Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
5:10 PM
4/3/2015

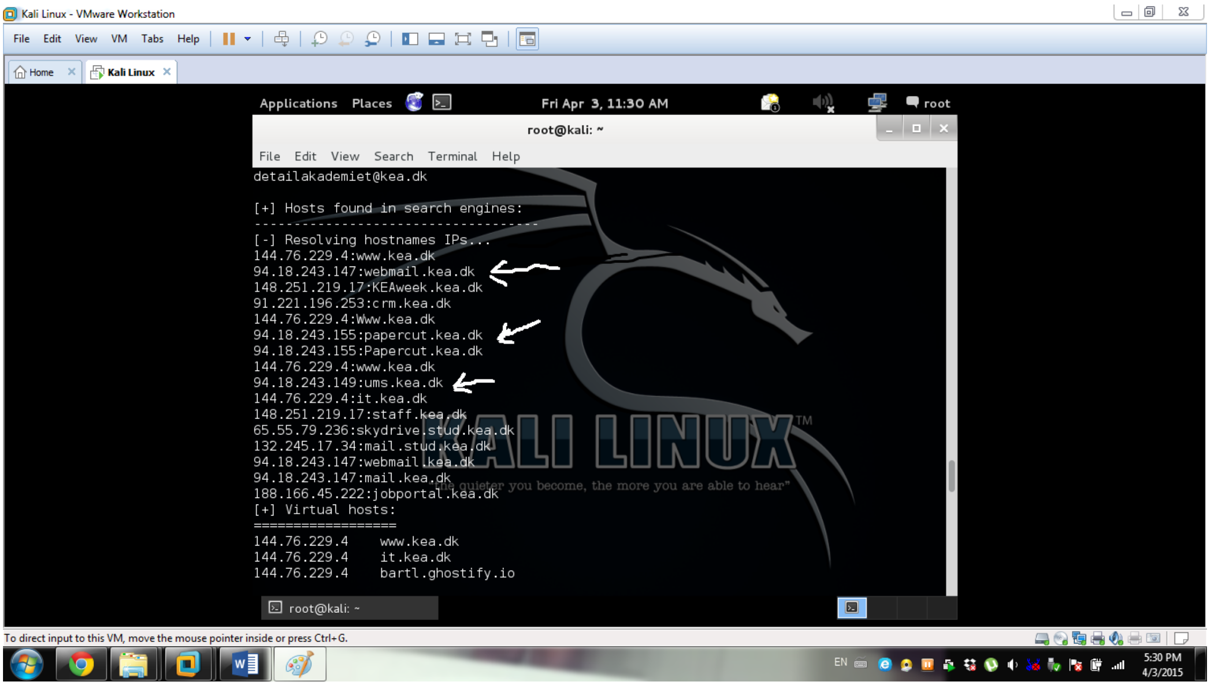
```
root@kali:~# theharvester

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.5                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source:
                        google
                        googleCSE
                        bing
                        bingapi
```

The tool produced the following results:


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
Applications Places
Fri Apr 3, 11:27 AM
root
root@kali: ~
File Edit View Search Terminal Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
5:27 PM
4/3/2015

```
[+] Emails found:
------------------
ehn@kea.dk
sopv@kea.dk
bope@kea.dk
hd@kea.dk
material@kea.dk
kea@kea.dk
Kea@kea.dk
mcn@kea.dk
dimb@kea.dk
kenj@kea.dk
mich160w@stud.kea.dk
miaj@kea.dk
cst@kea.dk
misl@kea.dk
loul@kea.dk
anmm@kea.dk
evav@kea.dk
drkp@kea.dk
efteruddannelse@kea.dk
gm@kea.dk
krt@kea.dk
medieit@kea.dk
trhe@kea.dk
louj@kea.dk
```

Here are emails of the employees(I suppose) One smart thing they did is they use only ititials in the emails , so you don`t know the full name of the person.Well of course you can dig some more about it ☺



Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
Applications Places
Fri Apr 3, 11:30 AM
root
root@kali: ~
File Edit View Search Terminal Help
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
EN
5:30 PM
4/3/2015

```
detailakademiet@kea.dk

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
144.76.229.4:www.kea.dk
94.18.243.147:webmail.kea.dk
148.251.219.17:KEAweek.kea.dk
91.221.196.253:crm.kea.dk
144.76.229.4:Www.kea.dk
94.18.243.155:papercut.kea.dk
94.18.243.155:Papercut.kea.dk
144.76.229.4:www.kea.dk
94.18.243.149:ums.kea.dk
144.76.229.4:it.kea.dk
148.251.219.17:staff.kea.dk
65.55.79.236:skydrive.stud.kea.dk
132.245.17.34:mail.stud.kea.dk
94.18.243.147:webmail.kea.dk
94.18.243.147:mail.kea.dk
188.166.45.222:jobportal.kea.dk
[+] Virtual hosts:
==================
144.76.229.4    www.kea.dk
144.76.229.4    it.kea.dk
144.76.229.4    bartl.ghostify.io
```

I found some more interesting IP addresses also. Actually a list of IP addresses ,which I can check.This search gives me more knowledge about their network.

CONCLUSION

It is very important to notice that in this lab I am not directly interacting with the company`s servers or resources. They do not know that I am actually looking at all this information. You can see that only from one single name ,Now I have a full list of targets ,which can give me some ideas on how to proceed.

ASSIGNMENT

1. Choose a random company ,and using PASSIVE Information Gathering ,find as much information about it and the resources it has (employees ,emails ,ip adrresses ,websites ,subdomains and so on.) Avoid huge corporations (amazon , facebook and so on ,simply because you will not find much ☺
2. Describe all your findings and include them into a logbook.(It should be a word document , with some explanations and screenshots)

3. Please do not use Port scanning or DNS interrogation tools against the company ,since your session could be logged and you could be considered an intruder! Your purpose is to remain undetected ,not to trigger some alarms !

HOW TO DO IT

1.Open up the website of the company and try to find any usable information.Tip: you can use a web site crawler to mirror the company`s website and get familiar with it.

2.Use google hacking. Try to find any info on google using the commands.

3.Use commands like : host , netcraft ,or any websites to find ip addresses,belonging to the company.

4.Use Shodan and try to find some juicy info about the company.

5.In your Kali Linux machine >Applications >Information Gathering > here are listed tools for information gathering.Please run and study some of them.Help regarding each tool usage is provided in Kali tools section in your web browser menu.

6.Include all your findings in a log book -report