

Did you want the world to know...?

An Hilven
ahilven@student.ecu.edu.au
School of Computer and Information Science
Edith Cowan University

Supervisor: Andrew Woodward

Abstract

Corporate websites, Google, forums, newsgroups ... All valuable sources of all kinds of information. Unfortunately, those that seek information from these sources are not always our customers, partners, or (potential) employees, but can also be people with less honest intentions. In order to research which sensitive information can be found freely available on the Internet, the author will put on a black hat and scour various online locations and use simple tools to get this information without breaking the law, and without crossing the line between ethical and non-ethical. Research includes locations where it is often already expected that an adversary will turn to for intelligence gathering, such as attempts to perform zone transfers. But also information that may not seem sensitive at first, such as corporate websites and even Google searches will be put under the loop. The conclusion of this research is that a lot of sensitive information is out there, and was put there by people either knowingly or unknowingly. It is about time that user education is taken more seriously, and turning the Internet inside out in search for sensitive information should become a very important part of audits and penetration testing.

Keywords

Passive reconnaissance, intelligence gathering, penetration testing

Introduction

In books covering hacking techniques, one of the first chapters will usually talk about passive reconnaissance, indicating that this is often the initial step a potential hacker would take in analyzing his or her target and preparing for a possible attack. The majority of books discussing information security, security auditing, and penetration testing, on the other hand, do not even touch on this topic and head straight to securing the network and its perimeter and scanning techniques.

Zalewski (2005), for example, describes various passive reconnaissance techniques in his book, such as how an attacker can deduct what his target is typing on the keyboard by analysing the timing patterns and sounds of different key presses, or that analysis of EMR emissions from typical CRT monitors can leak information. Or even analysis of LEDs on computer equipment. Long (2008) describes other techniques such as dumpster diving, shoulder surfing. And Mitnick (2002, 2006) goes more into the social engineering aspect in his books. Even though all very interesting attack vectors worthy of research, each of these techniques require either physical access or preliminary information to be known before one can start the “attack”.

After having attended Hacker techniques, exploits and incident handling by The SANS Institute (Triulzi, 2008) where various passive reconnaissance techniques were discussed not requiring physical access, the author started to wonder if there really is so much information out on the Internet as these books and courses try to warn everyone about. Armed with additional knowledge gained from Hands-on Penetration Testing with Backtrack 3 by Offensive Security (Aharoni, 2008), research started for this paper without having a need for physical access to the targeted organisations’ networks. This paper will research whether or not there is a need to include the evaluation of information out on the Internet into the process of security auditing and penetration testing, and thus expand the scope of these audits outside the network perimeter.

To get to this point, analysis will first be done on what is already known and published about passive reconnaissance, otherwise known as intelligence gathering. Thus, the research itself will be preceded by a discussion as to what passive reconnaissance is, how it can aid a potential attacker in finding information on the Internet about the organization he or she is targeting, and how the search for this information can be the interlude of a more serious threat. This discussion will then be followed by putting the theory into practice, and attempts will be made to find

and analyse real life examples of information that could be found by an adversary while using intelligence gathering techniques. This information can range from data of which the organization is not aware that it can be used in an abusive manner, up to sensitive or private data that is available and of which the organization does not even know that it can be publicly accessed.

What is passive reconnaissance?

Most organisations nowadays have technical security measures in place to protect their perimeter and the internal network from threats coming from the outside world. Many of these organisations also have a security policy instructing their employees how to treat information and information systems in order to maintain this security. But still, at some point, they become the victim of an attack, and then they wonder “Why? What is it that we forgot in our line of defense?”

To answer this question, there is a story that Mati Aharoni tells the students in his Offensive Security training classes (quoted with permission):

```
It was once engaged in a penetration test where my attack surface was limited and the few services that were present were well secured. After scouring Google for information about the company I was supposed to attack, I found a post, made by one of the company employees, in a stamp collecting forum. In this post, the employee was asking to buy or trade rare stamps from the 50's, and the post contained this employee's corporate e-mail address, and his cell phone number. This post was all I needed in order to launch a semi-sophisticated client side attack. I registered a domain, collected some stamp images from Google images, and embedded some code exploiting the latest Internet Explorer security hole at the time. I called the employee on his cellular phone, and explained I would be willing to trade several stamps, and directed him to my malicious website to see the stamps I had to offer. While browsing to my site, the exploit code was downloaded and executed Netcat on his local machine, sending me a reverse shell.
```

A post on a forum for stamp collecting was all that was needed to social-engineer through the organisation's defences and get a foothold on their internal network. That is exactly what passive reconnaissance is: simply searching the Internet and using publicly available services, and using information out there to penetrate the network without scanning it or launching brute-force attacks. And no firewall or IDS system will stop someone with malicious intent to do just that: use the Internet.

Information gathered by browsing the Internet

Corporate websites

Probably a page that each corporate website has is a section for careers and job opportunities. Although this is very useful both for the organisation and possible applicants, caution should be taken when writing job descriptions and which information is shared with the world when publishing these details online.

The organisation chosen to illustrate this example is Euroclear. According to the “about” page on their website, Euroclear is a provider of domestic and cross-border securities settlement and related services. The total value of securities transactions settled by this company is in excess of EUR 450 trillion per annum, while assets held for clients are valued at more than EUR 18 trillion.

This does appear to be an interesting company for an attacker to get access to. And a lot of information about their network is available on their own website. As a matter of fact, the only thing that appears to be missing is a network diagram.

From the job postings it was found that they use Cisco LAN & WAN technologies, Check Point firewalls running on Nokia hardware, they have Windows 2000 and UNIX servers of which the Windows servers are part of a Windows domain. Other hardware and applications that can be found on their network are reverse proxies, Clearcase servers, IBM Rational Buildforge, Totalnet Advanced Server, Documentum, SQL Server, Websphere, IBM DB2 data servers, Datastore, Sharepoint, SUN AIX, Tandem, Cisco IP telephony, NICE voice recording and Polycom video conferencing. It also appears that Euroclear develops applications in-house, and does so in Visual Basic, .net, Java and C++ using Eclipse, Jakarta ANT, Maven 2, Eclipse, SVN, J-Unit and CICSTransaction Gateway.

Of course this information alone will not give an adversary immediate access to the organisation's network, but it will help him greatly once he has gathered more information such as the IP addresses of the before mentioned Check Point firewalls. At that moment, the adversary will only need to focus on the Check Point product and Nokia platform, and any searches for vulnerabilities can be limited to just these products. Not knowing which type and brand of devices are in place will greatly limit the attacker's ability puncture through the perimeter, as he will first have to figure out which exact technologies before he can proceed. Other information, such as the applications used in the organization, could help him with this. Especially the applications that are network-aware will usually have default ports they known to listen on, and which by most organizations are not changed from the default. So even if the firewall itself is unknown, chances are that it will allow access to hosts behind it on those specific ports.

Admitted, in order to find the right candidate for the right job, the job description presented online will have to include at least some details if the organisation wants to avoid attracting less competent candidates. However, one should be careful with which information is included and how it can be abused by those that are not necessarily looking for a job. Therefore, it would be highly recommendable to ensure that a security officer evaluates this kind of information before it is published, and that during penetration tests and audits it is brought forward the organisation is reminded again what the consequences may be of sharing it.

Vendors' and Business Partners' websites

Vendors and business partners are often very keen on publishing testimonials on their websites or in press releases, sometimes even in return for discounts on the products or services they are offering. The organization's that agree with this type of publications, however, should seriously consider the information they are giving away by doing this. These organizations may share with the whole world which products they use:

NATO Deploys Guidance Software EnCase® Information Assurance for Forensic Approach to Computer Security Incident Response and Classified Spillage Auditing
Leading Technology Provides NATO with Accurate View of Incidents on Thousands of Systems within Seconds

Or even indicate that the security of information regarding elections is outsourced:

Telindus provides the ICT-support to the "Ministerie van de Vlaamse Gemeenschap" for the elections organisation
The latest Belgian elections were the first one to be organised by each regional government. The Flemish Government decided to make use, as much as possible, of the Information and Communication Technologies (ICT) to support the election process. They decided to work together with the EDS-Telindus Consortium. Concretely, they requested that all information related to the elections will be centralized on the Flemish government servers in Brussels and will be sent to the many different users from there.


The same warnings apply for this kind of information sharing as previously mentioned for job descriptions. But in case of testimonials with regards to services, an organisation should be extra careful in the sense of social engineering opportunities they open. Anyone could step up to the receptionist saying they are from support provider so-and-so, have noticed a problem with the server via remote monitoring, and have come onsite to have a closer look at the problem.

As with the publications discussed in the previous section, it might be a good idea to consult with the security officer before allowing publications of this kind. And again, during a penetration test or information security audit it could be a real eye-opener to confront the tested or targeted organisation with the information other organisations have published about them.

Social networking websites

Even if a company is very careful with the information they publish themselves, there may always be employees who post sensitive network information online, often unaware of the consequences this may have for their company. With their growing popularity over the last years, social networking websites are a very lucrative source that can be used to gather information. On most of these websites, employees can be found simply by searching for the name of the organisation. Often the employee's name may not be publicly available unless one is "connected" to them, but

details are available nevertheless.

System Engineer
Bull 

(Privately Held ; 10,001 or more employees ; Information Technology and Services industry)
July 2006 – Present (1 year 11 months)

sourced to Sibelga (manages the natural gas and electricity network in the Brussels region) as system engineer. (100+ server wintel and AIX environment)

key technologies: Cisco/Juniper , IBM Bladecenter/BULL(NEC), EMC/BULL, MX-ONE(traditional/IP), (Wintel/AIX, Citrix/VMWARE/Softgrid)

In the example above, a contractor reveals which technologies his employer uses, but it may as well have been a direct employee of this organisation. People are often proud of their knowledge, and want the world to know that they know this and that, and in itself there is nothing wrong with it, but once they start sharing sensitive network information this might be one step too far.

Organisations might try to stop this behaviour by including relevant clauses in the organisation’s security policy, or by forcing employees and contractors to sign a non-disclosure agreement. However, policies and agreements should also be enforced, and that is where it can go wrong. Similarly to revealing to an organisation which information is published about them by other organisations, it can be just as confronting to know that a penetration test was successful due to the information that was published on social networking sites by one of the organisations own employees.

Forums and news groups

Other locations for finding sensitive information about an organisation’s network are forums and news groups. One example is the story of the stamps collection quoted earlier, but quite often social engineering is not even required, and confidential network details are posted on technical forums and news groups.

Cisco Pix 515e ERROR: % Inval

- *This message:* [[Message body](#)] [[More options](#)]
- *Related messages:* [[Next message](#)] [[Previous message](#)]

From: Jesse DeGarmo <jdegarmo_at_kshs.org>
Date: Sun, 02 Dec 2007 21:51:36 -0600

I have a Cisco Pix 515e that when we upgraded the software from 6.3 to 7.0 we are getting (ERROR: % Invalid input detected at '^' marker) any

The fact that employee DeGarmo (above) is having problems with the firewall, and what the problem is is probably less interesting in this research, but DeGarmo also just shared with the world that his company has a Cisco PIX 515E running firmware 7.0. And although employee Driscoll (below) is aware of the “gaping security hole” 2nd Life will create in his firewall, he also just told everyone that management wants to use 2nd Life on the corporate network, together with a list of ports that are very likely to be opened on the firewall for this purpose.

2nd Life

Management is pushing pretty hard for this and they have persuaded our Risk Management group to move forward with a possible solution. So simply denying this is not an option.

```
Of course direct client access appears to be a gaping hole as second
life requires...
TCP/443
TCP/12043
UDP/12035-12036
UDP/13000-13050

Then depending on whether or not we are forced to allow voice traffic
through
TCP/80
TCP/443
TCP/21002
UDP/12000-13000
UDP/5060
UDP/5062
```

The posting of this information in itself may be harmless. But it becomes worrisome if the employee, very often a security administrator who is expected to be security aware, uses his or her real name and corporate (e-mail) address to sign the post.

```
Jesse G. DeGarmo
System Administrator
Kansas State Historical Society
6425 SW 6th Avenue
Topeka, KS 66615-1099
785-272-8681 x 242
785-272-8682 fax
jdegarmo_at_kshs.org
```

```
Robert Driscoll, CISSP
robdri_at_safeco.com
```

In the above examples, it is again the organisation's own employees that share sensitive information with the rest of the world. The difference, however, with social networking websites is that this is information which the organisation's management will seldom stumble upon, as the contents of these publications are considerably more technical, and thus the employee will rarely be told his mistakes as no one has noticed these mistakes. And yet again, this is the kind of information that can make a penetration test successful and a security policy audit fail.

Information gathered by browsing the Internet, for the slightly more tech savvy

Robots.txt

A few years ago, the website of the American anti-piracy organisation RIAA was found serving illegal MP3 music files (zone-h.org, 2002). How this could have happened has a fairly simple explanation: the administration module on this website was not properly secured.

The mistake the RIAA made back in 2002 was one that organisations still make today. They included in their robots.txt file that the /admin page of the website should not be crawled by search engine spiders. This in itself is not really a problem, besides the fact that now the world knows that a /admin page is likely to exist, but the problem lies in the fact that the RIAA appears to have assumed that this also means that the page is inaccessible, and thus decided not to protect it with a password.

"Oh no Dr. Watson! There was no sci-fi involved. Let me explain you. Do you know what robots.txt file is used for on websites?"

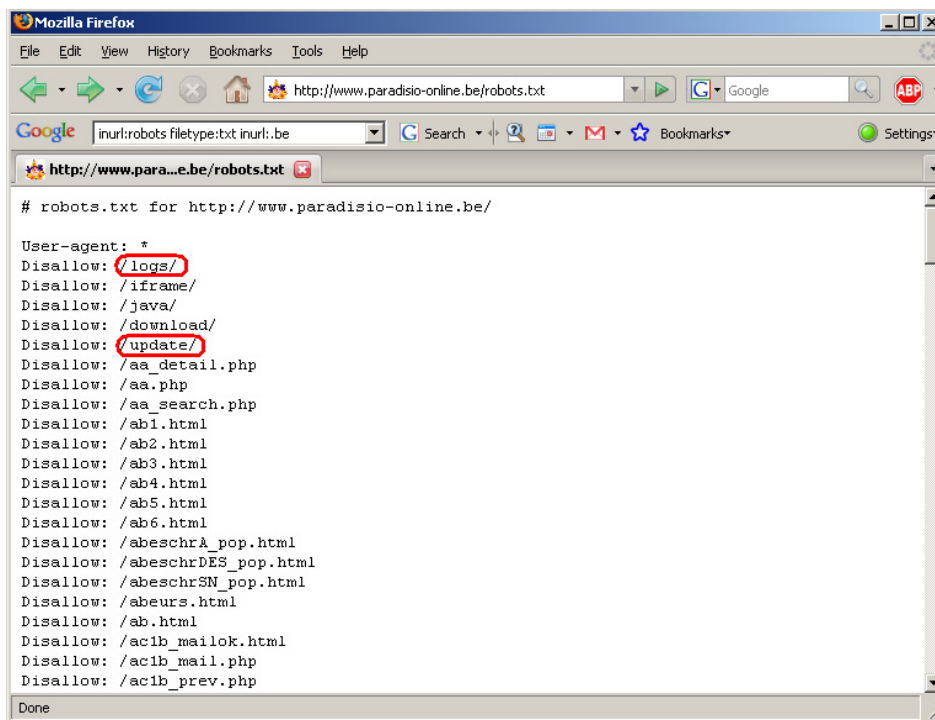
"Sure I know," proudly declared Watson "it is meant to keep web crawlers and spiders away from certain folders on the server."

"Yes indeed," Holmes continued, "but ID does not prevent the hackers from taking the peek at folders that the webmaster wanted to hide from spiders, folders like admin on that very website."

"And?" asked an even more curious Watson.

"This organization must be employing a blind webmaster if he did not figure out that this very passwordless admin module at www.that-site.org/admin was used to deface the website. There was also no filtering to prevent uploading mp3 files through the PDF upload section. That would also explain how illegal mp3 music files appeared on this anti-piracy site," explained Holmes smugly.

Although over the last years organisations have become more security aware, and are at least password-protecting their administration modules, caution should still be taken when creating a robots.txt file simply because it reveals which otherwise hidden or unknown pages may exist on the website:



```
# robots.txt for http://www.paradisio-online.be/

User-agent: *
Disallow: /logs/
Disallow: /iframe/
Disallow: /java/
Disallow: /download/
Disallow: /update/
Disallow: /aa_detail.php
Disallow: /aa.php
Disallow: /aa_search.php
Disallow: /ab1.html
Disallow: /ab2.html
Disallow: /ab3.html
Disallow: /ab4.html
Disallow: /ab5.html
Disallow: /ab6.html
Disallow: /abeschrA_pop.html
Disallow: /abeschrDES_pop.html
Disallow: /abeschrSN_pop.html
Disallow: /abeurs.html
Disallow: /ab.html
Disallow: /ac1b_mailok.html
Disallow: /ac1b_mail.php
Disallow: /ac1b_prev.php
```

Attempting to access all hidden pages on a website is a technique that can be used by attackers in order to gain unauthorized access to the web server itself, as proven with the RIAA example above. So if hackers use this technique, it could easily be included in penetration testing as well as security auditing, as it is a quick and simple technique to discover major security holes in the network.

Google hacking

Google hacking was first introduced by Johnny "I Hack Stuff" Long on his personal website, and later in his book Google Hacking for Penetration Testers volume 1 (Long, 2005) and volume 2 (Long, 2008). It is the practise of using cleverly crafted Google searches in order to find servers vulnerable to a certain exploit or confidential documents that would otherwise be hidden.

One example that could be very interesting to find during reconnaissance is automatic configuration scripts such as `kickstart.cfg` and `winnt.sif`. Luckily, no `winnt.sif` files were found during this research, but imagine the information

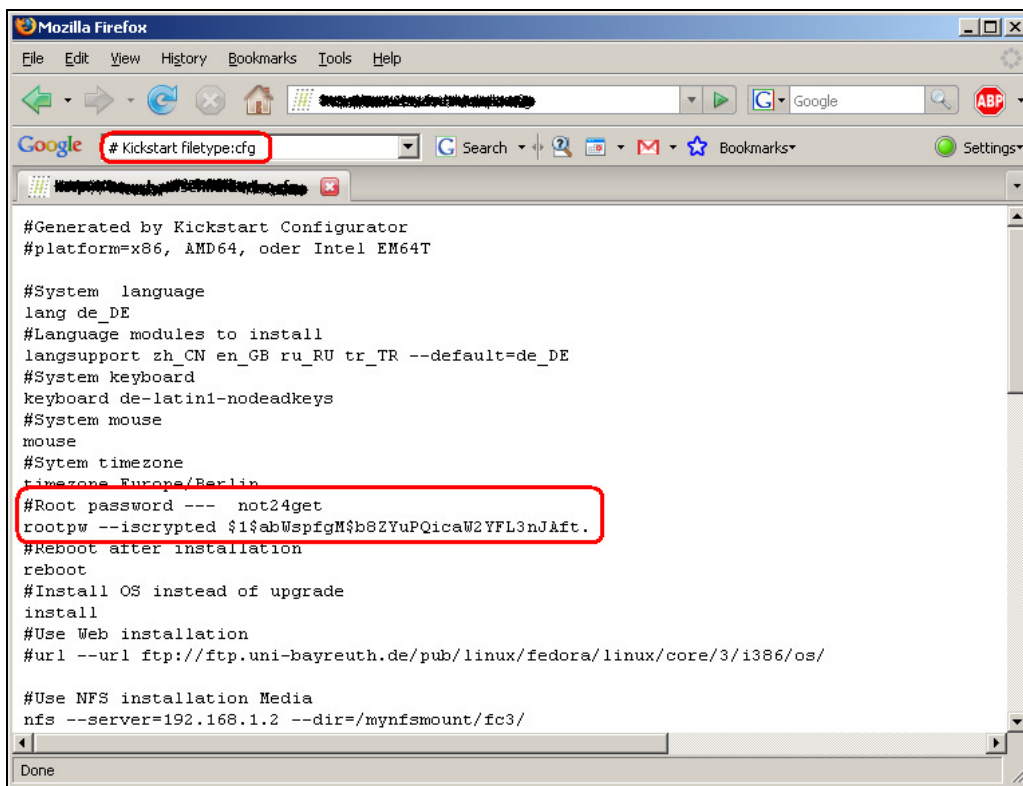
that would be shared with the world:

```
[GuiUnattended]
  AdminPassword=your-password

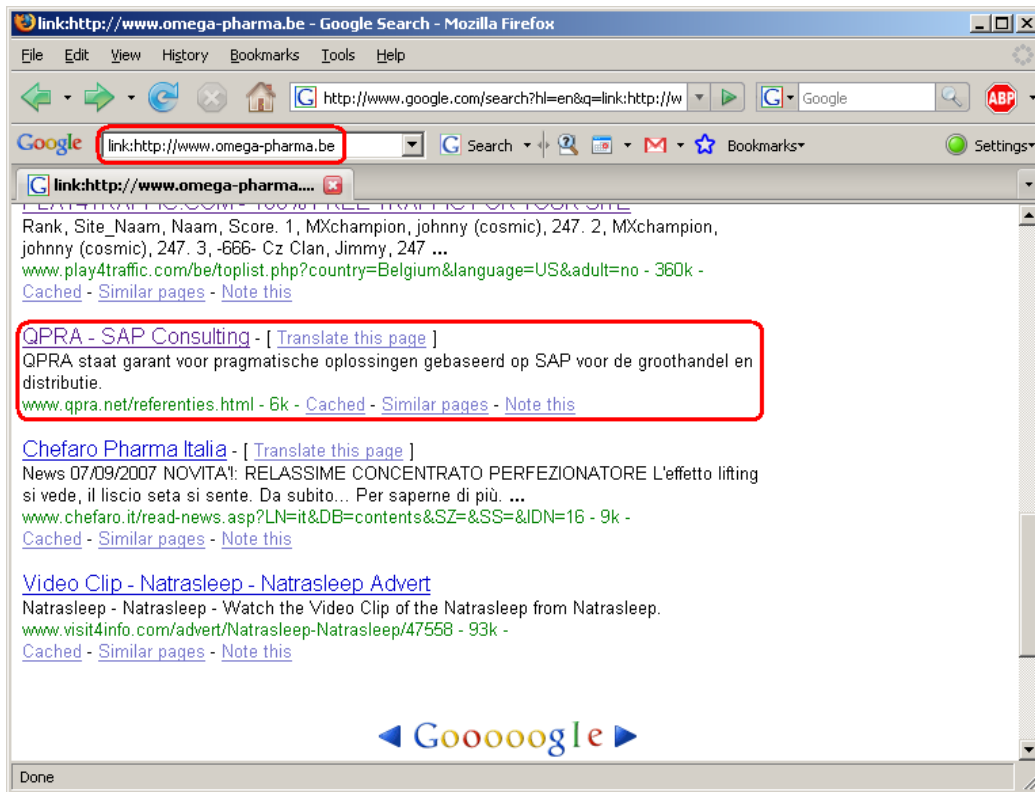
[UserData]
;   ProductId="VVVVV-WWWW-XXXX-YYYY-ZZZZ"

[Identification]
;   JoinDomain=organisation-name
;   DomainAdmin=root
;   DomainAdminPassword=*****
```

Kickstart.cfg files, on the other hand, can be found by the dozens. Not only do these files reveal the packages that are installed on devices configured by them, they also show various IP addresses where information is downloaded from, revealing part of the internal IP addressing structure. And not to forget, administrators might be afraid they forget their root password, and put it in a comment unencrypted:



These searches can also have a more general use, for example one could search which websites are serving a link to the organisation which is the victim of passive reconnaissance, again revealing which products and/or services this organisation uses, and possible business partners they might have:



As if all of this was not enough, Johnny created and maintains a freely accessible database of “interesting” Google searches (Long, n.d.). The people over at GNUCITIZEN even decided to give the database some better usability, and designed an interface for it (Petkov, 2007).

Some information found through Google hacking is more sensitive than others, i.e. there is a big difference between discovering business partners and getting ones hands on a kickstart.cfg file. However, it should be clear by now that even the smallest amount of seemingly irrelevant information can make the difference between a successful and failed penetration test. Unfortunately this attack vector is much more difficult to be used in security auditing, as it is more often used to find vulnerable systems and then attack those systems, as opposed to finding vulnerabilities within one specific targeted organisation. Nevertheless, searches for other websites that are linked to the organisation’s website, or a listing of all documents publicly available on the web server can still help the auditor.

Information gathered by using third-party products and services

Netcraft

Netcraft provides a service online through which anyone can find out information about many public web servers. The only information one has to enter is the domain name, and the service will do all the work. In the example below, it was found that the website cisco.be used to run on Windows NT and 2000 with IIS4 and 5, but was migrated to Solaris and later to Linux with Apache 2. It also appears that this organisation changed hosting providers several times before deciding to host their website in-house.

OS, Web Server and Hosting History for www.cisco.be				
http://www.cisco.be was running Apache on Linux when last queried at 25-May-2008 16:43:32 GMT - refresh now Site Report FAQ Try out the Netcraft Toolbar!				
OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache/2.0	25-May-2008	198.133.219.23	Cisco Systems, Inc.
Linux	Apache/2.0	14-Sep-2006	198.133.219.23	Cisco Systems, Inc.
Solaris	CCO/1.0 (Unix)	31-Aug-2006	198.133.219.23	Cisco Systems, Inc.
Solaris	CCO/1.0 (Unix)	18-Sep-2005	198.133.219.23	Cisco Systems, Inc.
Windows 2000	Microsoft-IIS/5.0	6-May-2003	212.3.250.180	Equinox
NT4/Windows 98	Microsoft-IIS/4.0	20-May-2002	212.3.250.180	Equinox
NT4/Windows 98	Microsoft-IIS/4.0	17-Dec-2001	213.193.160.139	Easynet Belgium
NT4/Windows 98	Microsoft-IIS/4.0	23-Nov-2000	212.68.209.137	IP Network of UCHRONY
NT4/Windows 98	Microsoft-IIS/4.0	23-Nov-2000	212.68.209.137	IP Network of UCHRONY

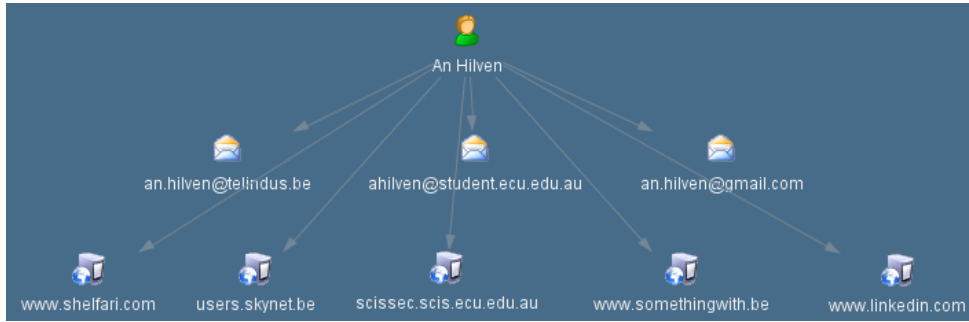
The ease of use of this service is almost scary. Within seconds, anyone knows the history of a web server, its IP address and its operating system and server platform. An adversary can immediately limit his attack paths and use only relevant attacks straight from the beginning, without the need of performing any scans or sweeps. This same information can be used for the same purposes during penetration testing, limiting the scans required to retrieve information, and thus limiting the risk of being seen by the intrusion detection team. Again a mind boggling result that looks good in a penetration testing report.

Also during security audits this information can be used, namely recommendations could be made that servers should return incorrect or inconsistent fingerprints, such as can be seen in the example below. Although these results could also indicate a misconfiguration, a potential adversary may turn to an easier identifiable server or will have to do additional testing before being able to gain access, potentially revealing his presence in the network. Admitted, this is mere security through obscurity, but it does add an additional layer of abstraction the adversary has to pass through.

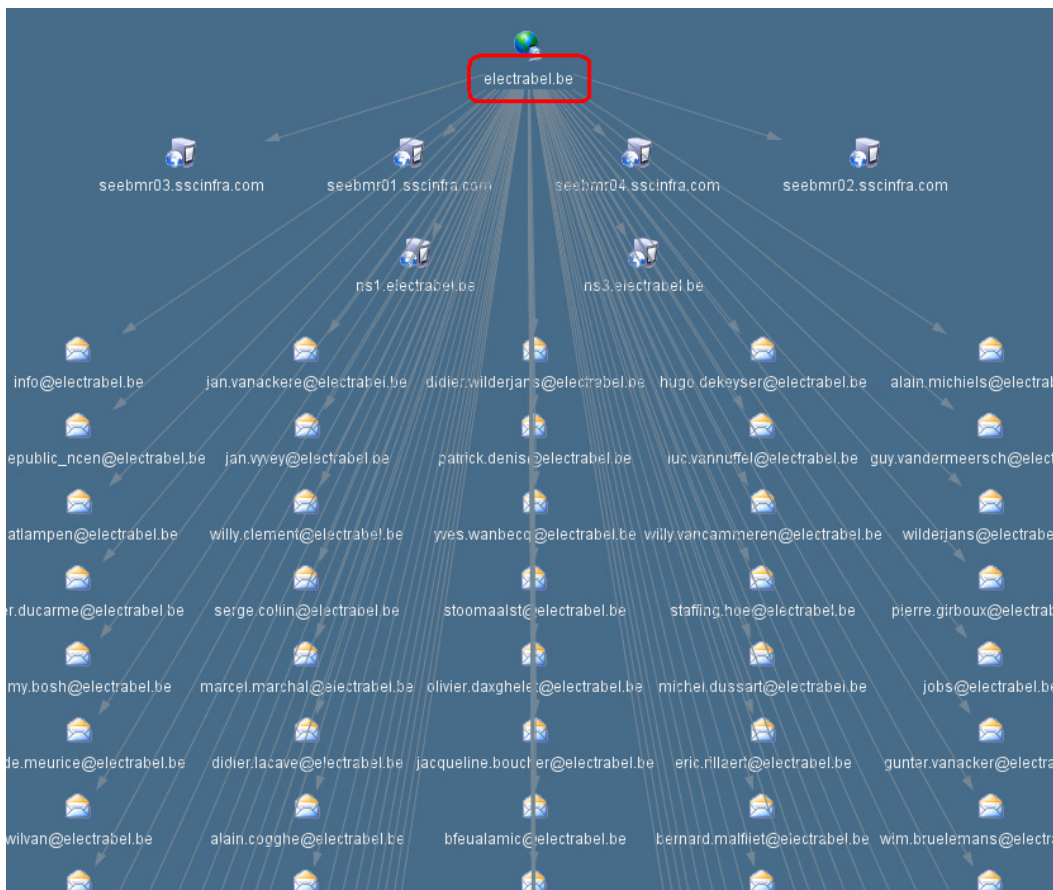
OS, Web Server and Hosting History for www.uzleuven.be				
http://www.uzleuven.be was running Microsoft-IIS on unknown when last queried at 28-May-2008 12:48:25 GMT - refresh now Site Report FAQ Try out the Netcraft Toolbar!				
OS	Server	Last changed	IP address	Netblock Owner
unknown	Microsoft-IIS/4.0	28-May-2008	134.58.179.15	Katholieke Universiteit Leuven
unknown	Microsoft-IIS/4.0	20-Apr-2007	134.58.179.2	Katholieke Universiteit Leuven
Linux	Microsoft-IIS/4.0	19-Apr-2007	134.58.179.2	Katholieke Universiteit Leuven
unknown	Microsoft-IIS/4.0	18-Apr-2007	134.58.179.2	Katholieke Universiteit Leuven
unknown	Microsoft-IIS/4.0	14-Apr-2007	134.58.179.2	Katholieke Universiteit Leuven
Linux	Microsoft-IIS/4.0	13-Apr-2007	134.58.179.2	Katholieke Universiteit Leuven
unknown	Microsoft-IIS/4.0	10-Apr-2007	134.58.179.2	Katholieke Universiteit Leuven
Linux	Microsoft-IIS/4.0	7-Apr-2007	134.58.179.2	Katholieke Universiteit Leuven
unknown	Microsoft-IIS/4.0	15-Jan-2007	134.58.179.2	Katholieke Universiteit Leuven
Linux	Microsoft-IIS/4.0	14-Jan-2007	134.58.179.2	Katholieke Universiteit Leuven

Maltego

Everyone has done it at least once: Google their own name or the name of someone they have just met and see what comes up. But in fact, there is a lot more information to find than what Google shows. By using Maltego to search someone's name, one might find their e-mail addresses, websites and even phone numbers.



But Maltego can do more than that. Simply entering a domain name and running all possible searches or “transforms” can provide mind boggling results. In the example below, a search was done for Electrabel, one of the largest electricity providers in Belgium. Not only are their mail and name servers revealed within seconds, but after waiting a little longer it shows a large number of e-mail addresses related to this organisation. Each of which can then again be used in social engineering and other attacks.



whois

When registering a domain name, an organisation has to provide contact details for the person within the organisation that will be responsible for the domain. Most organisations nowadays do appear clever enough not to sign up with names of people but names of teams, because this information is freely available to anyone that can perform whois lookups. Those organisations that decide to include a person’s name in the registration might get a phone call one day from someone claiming to be that person, explaining that they are currently at the airport and need to access the corporate network but forgot their password and need it reset. Yet again, a successful penetration

test. Exactly because this information is publicly available, and little or nothing can be done to prevent it from being public information, it is very important that during security audits this information is verified to ensure that no direct e-mail addresses, phone numbers and names of employees are disclosed.

```
Agent Technical Contacts:
First Name:  DNS
Last Name:   Master
Company Name: Mobistar
Language:    en
Street:      rue Colonel Bourg, 149
Location:    1140 Evere
Country:     BE
Phone:       +32.27459207
Fax:         +32.27459461
Email:       dnsmaster@mail.mobistar.be

First Name:  Dirk
Last Name:   Haegemans
Company Name: Mobistar
Language:    en
Street:      Rue Colonelbourgstraat 149
Location:    Brussels 1040 Evere
Country:     BE
Phone:       +32.27457917
Fax:         +32.27458890
Email:       dhaegema@mail.mobistar.be

Agent:
Name:        MOBISTAR SA
Website:     http://www.mobistar.be

Nameservers:
ns1.mobistar.be (212.65.63.217)
ns2.mobistar.be (212.224.255.252)

bt ~ #
```

nslookup

It is generally known that the nslookup utility is often used simply for finding the IP address of a known website. But that is not the only use of nslookup. It can also be used to find an organisation's mail server and DNS server, respectively their name and IP address.

```
bt ~ # nslookup
> www.mobistar.be
Server:          192.168.1.1
Address:         192.168.1.1#53

Name:   www.mobistar.be
Address: 212.65.63.184
> set type=mx
> mobistar.be
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
mobistar.be mail exchanger = 10 smtp-mx.mobistar.be.

Authoritative answers can be found from:
smtp-mx.mobistar.be internet address = 80.12.204.210
> set type=ns
> mobistar.be
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
mobistar.be nameserver = ns1.mobistar.be.
mobistar.be nameserver = ns2.mobistar.be.

Authoritative answers can be found from:
ns2.mobistar.be internet address = 212.224.255.252
ns1.mobistar.be internet address = 212.65.63.217
>
```

Other uses of nslookup can be to find if certain often-used hostnames exist on the organisation's (public) network,

```
bt ~ # nslookup www.mobistar.be
Server:      192.168.1.1
Address:     192.168.1.1#53

Name:   www.mobistar.be
Address: 212.65.63.184

bt ~ # nslookup proxy.mobistar.be
Server:      192.168.1.1
Address:     192.168.1.1#53

** server can't find proxy.mobistar.be: NXDOMAIN
```

of which the results can in turn be used to reveal the complete IP address block that is assigned to this organisation.

```
bt ~ # whois 212.65.63.184
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html
%
% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.
% Information related to '212.65.63.0 - 212.65.63.255'
inetnum:      212.65.63.0 - 212.65.63.255
netname:      MOBISTAR-ISD
descr:        be.mobistar
country:      BE
```

Once the IP address block is known, one can start from the beginning and begin doing nslookups for each IP address in the range, revealing more hostnames. Because quite often hostnames of servers are indicative of what they are used for, this can be very useful information to be found in reconnaissance. Due to the very nature of DNS, little can, and should, be done about the disclosure and availability of this information. However, organisations should be aware that this information is out there.

```
bt ~ # nslookup 212.65.63.184
Server:      192.168.1.1
Address:     192.168.1.1#53

184.63.65.212.in-addr.arpa    name = www.mobistar.be.

bt ~ # nslookup 212.65.63.55
Server:      192.168.1.1
Address:     192.168.1.1#53

** server can't find 55.63.65.212.in-addr.arpa: NXDOMAIN
```

Information gathered by interacting with public services on the corporate network

Zone transfers

Although DNS zone transfers are under normal circumstances only to be used by DNS server administrators, some of these servers are incorrectly configured and allow zone transfers to be executed by anyone. Most DNS servers, however, do appear to be protected against unauthorized transfers of information.

```
bt ~ # host -t ns mobistar.be
mobistar.be name server ns1.mobistar.be.
mobistar.be name server ns2.mobistar.be.
bt ~ # host -l mobistar.be ns1.mobistar.be
; Transfer failed.
Using domain server:
Name: ns1.mobistar.be
Address: 212.65.63.217#53
Aliases:

Host mobistar.be not found: 5(REFUSED)
; Transfer failed.
```

A successful zone transfer can reveal a whole internal network structure of existing IP addresses, as well as the hostnames they are mapped to. As discussed earlier, hostnames are often indicative of the purpose that particular host is used for. In the example below, a successful zone transfer resulted in over 130 hosts and their IP addresses revealed. It does not require a genius to guess what servers with names such as “juniper”, “videoconf”, “demo”, “testjabber”, “wepl”, “firewall” or “backup” are used for.

```
bt ~ # host -l belnet.be dns1.kulnet.kuleuven.ac.be
Using domain server:
Name: dns1.kulnet.kuleuven.ac.be
Address: 134.58.127.1#53
Aliases:

belnet.be name server ns1.belnet.be.
belnet.be name server ns2.belnet.be.
belnet.be name server dns1.kulnet.kuleuven.ac.be.
belnet.be has address 193.190.198.53
argos.belnet.be has address 193.190.198.45
smtp.belnet.be has address 193.190.198.9
smtp.belnet.be has address 193.190.198.13
romulus.belnet.be has IPv6 address 2001:6a8:3c80::14
romulus.belnet.be has address 193.190.198.14
mx1-out.belnet.be has address 193.190.198.18
demo.belnet.be name server ns.belnet.be.
noc.belnet.be has address 135.109.24.126
loba.belnet.be has address 193.190.198.53
palm.belnet.be has address 193.190.198.59
juniper.belnet.be has address 193.190.198.16
BELNET.belnet.be has address 193.190.0.0
```

In the example above, by the way, this organisation has a total of three DNS servers. Looking at their names, it appears that two of these are maintained by the organisation itself, and the third one by a local university. The servers maintained by the organisation itself are not susceptible to unauthorized zone transfers. This is to indicate that however secure an organisation may be, third parties should be secure and audited as well in order to reveal and solve this type of security holes in the network.

Recommendations and auditor could make in this field are many. First of all, third parties should be audited, especially if they have this level of access to the organisation’s network. Next, drop those 53/TCP connections from the Internet on the perimeter firewall. A normal Internet user will only need to do DNS lookups, not zone transfers. And last, use a consistent naming convention for networked hosts, yet not revealing the purpose of the host itself.

For a penetration tester, the discovery of zone transfers that are allowed on the DNS servers is very good news, and results in full compromise of the internal network.

SNMP enumeration

Even though SNMP is usually not allowed from outside the local network, many organizations outsource the monitoring of availability of their servers and are required to allow SNMP through the firewall. A small misconfiguration of the source address can have catastrophic results. Once interesting IP addresses within an organization have been identified, various SNMP lookup tools can then be used to disclose even more information such as hardware, operating system, user accounts, running processes, and etcetera. Although all of this information can be found using the public community string, which in its nature is publicly available and often consists of the string “public”, putting this into practice would be balancing on the line between ethical and non-ethical.

Conclusion

Did the organizations used as examples in this paper want the world to know all these details about their network? Probably not, but most likely they are either not aware of the risks, or have chosen to accept them.

This paper has shown that even organisations with the best perimeter and local network defences to secure themselves against all possible threats from the outside world they are so scared of, are still very vulnerable in the information they often inadvertently have available to this same outside world. Quite a few of the topics discussed here relatively easy to avoid from happening. The main key in doing so is not to buy more, better, newer, or more expensive technical defences, but to conduct a thorough risk assessment, ensure a good security policy is in place, and most importantly is adhered to. Simple security awareness trainings explaining how long a password should be are no longer sufficient, and audits and penetration tests are a must if only to be an eye-opener to everyone in the organisation, from employee to corporate management.

So to come back to the question it all started with: Is there a need to include the evaluation of information out on the Internet into the process of security auditing and penetration testing, and thus expand the scope of these audits outside the network perimeter? The answer is yes. Passive reconnaissance or intelligence gathering is very often overlooked. Therefore it is of utmost importance that this phase is included in penetration testing. The target organisation will be baffled with the results of the penetration test if their IDS system did not even notice aggressive scanning activity, and even more so if they are told that all information that was needed to assess and penetrate their defences was an administrator that forgot to password-protect the corporate website's administration module...

References

Books

- Aharoni, M. (2008). Penetration Testing with Backtrack 3. Offensive Security 101. Lab Guide v. 2.0. Offensive Security.
- Long, J., Skoudis, E., van Eijkelenborg, A. (2005). Google Hacking for Penetration Testers, Volume 1. Syngress.
- Long, J. (2008). Google Hacking for Penetration Testers, Volume 2. Syngress.
- Long, J. (2008). No Tech Hacking. Syngress.
- McClure, S., Scambray, J., & George Kurtz, G. (2005). Hacking Exposed: Network Security Secrets & Solutions. McGraw-Hill/Osborne Media.
- Mitnick, K. D., Simon, W. L. (2002) The art of deception. Wiley Publishing Inc.
- Mitnick, K. D., Simon, W. L. (2006) The art of intrusion. Wiley Publishing Inc.
- SANS Institute & Skoudis, E. (2007). SANS Security 504: Hacker techniques, exploits and incident handling. SANS Institute.
- Skoudis, E. (2001). Counter Hack: A step-by-step guide to computer attacks and effective defenses. Prentice Hall PTR.
- Zalewski, M. (2005). Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. No Starch Press.

Classroom Training

- Aharoni, M. (2008). Hands-on Penetration Testing with Backtrack 3. Offensive Security.
- Triulzi, A. (2008). SANS Security 504: Hacker techniques, exploits and incident handling. SANS Institute.

Computer Based Training

Conrad, J. I. (Instructor). Certified Ethical Hacker Series [video]. CBT Nuggets.

Internet Resources

Long, J. (n.d.). Google Hacking Database. Retrieved March 12, 2008, from <http://johnny.ihackstuff.com/ghdb.php>

Petkov, P. (May 21, 2007). GHDB. Retrieved March 12, 2008, from <http://www.gnucitizen.org/blog/the-extreme-web-based-google-hacking-tool>

Zone-h.org (September 21, 2002). Want to know how RIAA.org was hacked? Retrieved March 18, 2008, from http://www.theregister.co.uk/2002/09/21/want_to_know_how_riaa/