

# Hacking: Footprinting Tools and Techniques

Ghodrat Moghadampour, PhD  
mg@puv.fi  
Principal Lecturer  
Vaasa University of Applied Sciences  
Vaasa  
Finland

# Outline

- ▶ Crackers vs. Hackers
- ▶ Hacking history
- ▶ Hacking Methodology
- ▶ Footprinting
  - Tools & techniques

# Crackers vs. Hackers

- ▶ People who break the law or break into systems without authorization are more correctly known as **crackers**.
- ▶ But, there are many experienced hackers, who never break the law, and who define hacking as producing an outcome the system designer never anticipated.



# Hacking History

- ▶ **1960 hackers:**
  - First generation of hackers, technology enthusiasts, “geeks”
  - Hacking was motivated by intellectual curiosity; causing damage or stealing information was “against the rules” for this small number of people.
- ▶ **1980 hackers:**
  - Hackers started gaining more of the negative connotations. Media attention started altering the image of a hacker from a technology enthusiast to a computer criminal.

# Hacking History

- During this time period, hackers engaged in activities such as theft of service by breaking into phone systems to make free phone calls.
- ▶ Current hackers can be categorized into several groups:
  - **Script kiddies:** beginners and may or may not understand the impact of their actions in the larger scheme of things. They typically possess very basic skills and rely upon existing tools that they can locate on the Internet.

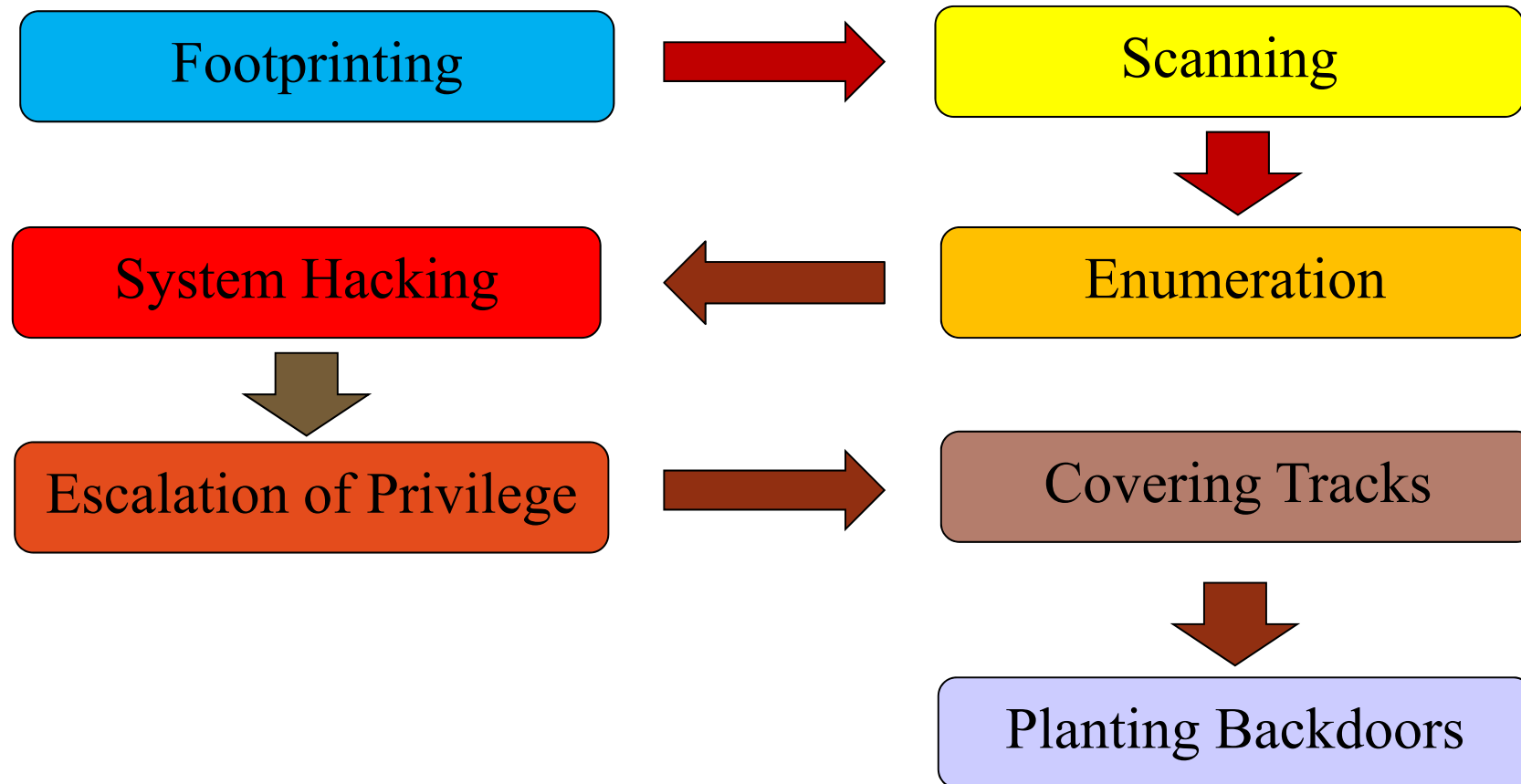
# Hacking History

- **White-hat hackers (ethical hackers):** know how hacking works and the danger it poses, but use their skills for good. They adhere the ethic of “do not harm” .
- **Gray-hat hackers:** rehabilitated hackers; those who once were on the dark side, but are now reformed.
- **Black-hat hacker:** have intent to break the law, disrupt systems or businesses or generate illegal financial return.

# Hacking History

- ▶ **Suicide hackers:** perform their activities with little regard for the law or staying undetected. They seek to accomplish their goal at all costs and do not worry if they are caught.

# Hacking Methodology





# Hacking Methodology

- ▶ Hacking methodology generally includes the following steps:
  - **Footprinting**: the attacker passively acquires information about intended victim's systems. In this context, passive information gathering means that no active interaction occurs between the attacker and the victim, like conducting a *whois* query.

# Hacking Methodology

- **Scanning**: the attacker takes the information obtained during the footprinting phase and uses it to actively acquire more detailed information about a victim, like conducting a *ping sweep* of all the victim's known IP addresses to see which machines respond.
- **Enumeration**: the attacker extracts more-detailed and useful information from a victim's system. Results of this step includes a list of usernames, groups, applications, banner settings, auditing information and so on.

# Hacking Methodology

- **System hacking**: the attacker actively attacks a systems using a method the attacker deems useful.
- **Escalation of privilege**: if successful, the attacker obtains privileges on a given system higher than should be permissible. Under the right condition, the attacker can use privilege escalation to move from a low-level account such as a guest account all the way up to administrator or system level access.
- **Covering tracks**: the attacker tries to avoid detection and covers his or her tracks by purging information from the system.

# Hacking Methodology

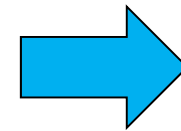
- **Planting backdoors**: the attacker may leave behind a backdoor on the system for later use. Backdoors can be used to regain access, as well as allow any number of different scenarios to take place, such as privilege escalations or remotely controlling a system.

# Hacking Overview

- ▶ The steps of the information-gathering process include:

1. Gathering information

2. Determining the network range



Footprinting

3. Identifying active machines

4. Finding open ports and access points

5. Detecting operating systems

6. Using fingerprinting services

7. Mapping the network

# Footprinting

- ▶ Information obtainable during footprinting phase is:
  - network range
  - equipment/technologies in use
  - financial information
  - locations
  - physical assets
  - employee names and titles

# Footprinting

- ▶ Some of the activities an attacker can perform when footprinting an organization:
  - Examining the company's web site
  - Identifying key employees
  - Analyzing open position and job requests
  - Assessing affiliate, parent or sister companies
  - Finding technologies and software used by the organization
  - Determining network address and range

# Footprinting

- Reviewing network range to determine whether the organization is the owner or if the systems are hosted by someone else
- Looking for employee postings, blogs and other leaked information
- Reviewing collected data



# The information on a company web site

- ▶ Web sites offer various amount of information about an organization because the web site has been published to tell customers about the organization.
- ▶ It is not uncommon to come across web sites that contain e-mail addresses, employee names, branch office locations and technologies the organization uses.

# Wayback Machine

- ▶ One of the tools that a security professional can use to gain information about a past version of a Web site is the Wayback machine; a Web application created by the Internet Archive that takes snapshots of a Web site at regular intervals and makes them available to anyone who looks.
- ▶ With the Wayback machine it is possible to recover information that was posted on a Web site sometime in the past.
  - <http://www.archive.org>

# Wayback Machine



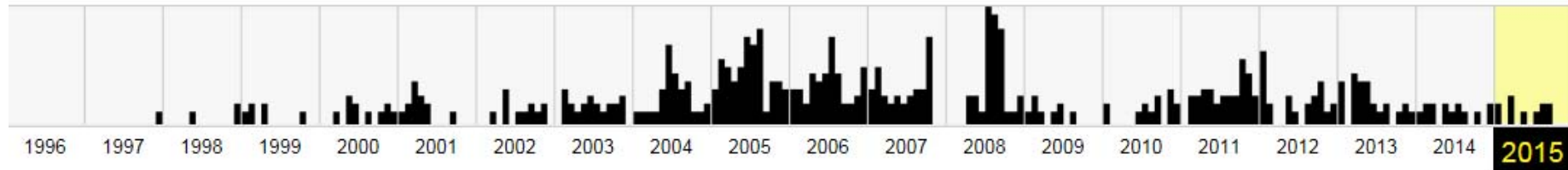
<http://www.fh-kiel.de/>

BROWSE HISTORY

<http://www.fh-kiel.de/>

Saved **508 times** between joulukuuta 10, 1997 and syyskuuta 10, 2015.

**PLEASE DONATE TODAY.** Your generosity preserves knowledge for future generations. Thank you.



TAMMI							HELMI							MAALIS							HUHTI						
			1	2	3		1	2	3	4	5	6	7					1	2	3	4						
4	5	6	7	8	9	10	8	9	10	11	12	13	14	8	9	10	11	12	13	14	5	6	7	8	9	10	11
11	12	13	14	15	16	17	15	16	17	18	19	20	21	15	16	17	18	19	20	21	12	13	14	15	16	17	18
18	19	20	21	22	23	24	22	23	24	25	26	27	28	22	23	24	25	26	27	28	19	20	21	22	23	24	25
25	26	27	28	29	30	31								29	30	31					26	27	28	29	30		

# Job Postings

- ▶ Job postings: another valuable source of information gleaning
- ▶ Job postings include the skills being requested.
- ▶ The information to could be used to fine-tune a later attack, doing some research and locating the vulnerabilities such as:
  - Vulnerabilities in the discovered products
  - Application-specific configuration issues
  - Product-specific defects

# Job Location

- ▶ The location information, browsed in conjunction with skills, can yield insight into potential activities are a location.
- ▶ The appearance of unusual skills at a specific location can be an indicator of activities such as those associated with research and development.
- ▶ An attacker could use the information to target specific locations that are more likely to contain assets of value.

# Discovering Financial Information

- ▶ Targets are footprinted prior to being attacked to determine whether a targeted company makes enough money to merit an attack.
- ▶ Financial records are accessible through the Securities and Exchange Commission (SEC) Web site at: <http://www.sec.gov>
- ▶ Electronic Data Gathering, Analysis and Retrieval (EDGAR) database contains all sorts of financial information.

# Discovering Financial Information

- ▶ These records indicate where the company is based, detailed financial information and the names of the principals.
- ▶ In addition to EDGAR the following sites provide the same type of information:
  - Hoover's: <http://www.hoovers.com>
  - Dun and Bradstreet: <http://www.dnb.com/>
  - Yahoo!Finance: <http://finance.yahoo.com>
  - Bloomberg: <http://www.bloomberg.com>

# Google Hacking

- ▶ Google contains tremendous amount of information of all type waiting to be searched and uncovered in Google hacking
- ▶ Google hacking is effective since Google indexes vast amounts of information in untold numbers of formats.
- ▶ Google indexes Web pages like any search engine, but it can also index images, videos, discussion group postings and all sorts of file types such as PDF, PPT and so on.



# Google Hacking

- ▶ Google Hacking Database (GHDB) is available at:
  - <http://www.hackersforcharity.org/ghdb>
  - <http://www.hackersonlineclub.com/google-hacking>
- ▶ This site offers insight into some of the ways an attacker can easily find exploitable targets and sensitive data by using Google's built-in functionality.

# Google Hacking



## Google queries for locating various Web servers

"Apache/1.3.28 Server at" intitle:index.of  
Apache 1.3.2  
"Apache/2.0 Server at" intitle:index.of  
Apache 2.0  
"Apache/\* Server at" intitle:index.of  
any version of Apache  
"Microsoft-IIS/4.0 Server at" intitle:index.of  
Microsoft Internet Information Services 4.0  
"Microsoft-IIS/5.0 Server at" intitle:index.of  
Microsoft Internet Information Services  
5.0  
"Microsoft-IIS/6.0 Server at" intitle:index.of  
Microsoft Internet Information Services 6.0  
"Microsoft-IIS/\* Server at" intitle:index.of  
any version of Microsoft Internet Information Services  
"Oracle HTTP Server/\* Server at" intitle:index.of  
any version of Oracle HTTP Server  
"IBM\_HTTP\_Server/\* \* Server at" intitle:index.of  
any version of IBM HTTP Server  
"Netscape/\* Server at" intitle:index.of  
any version of Netscape Server  
"Red Hat Secure/\*" intitle:index.of  
any version of the Red Hat Secure server  
"HP Apache-based Web Server/\*" intitle:index.of

## Update Imp. Dorks.

Dork : `"inurl:dettaglio.php?id="`

Exploit :  
`www.victim.com/sito/dettaglio.php?id=[SQL]`

Example :  
`http://www.cicloposse.com/dettaglio.php?id=61'`

Dork: `inurl:prodotto.php?id`

Exploit:  
`www.victim.com/prodotto.php?id=[SQL]`

Example:  
`http://www.poderimorini.com/en/prodotto.php?id=14'`

sql injection dorks  
`allinurl: \'index php go buy\'`



# Google Hacking

- ▶ Some of the items an attacker can find are available using the following techniques:
  - Advisories and server vulnerabilities
  - Error messages that contain too much information
  - Files containing passwords
  - Sensitive directories
  - Page containing logon portals
  - Pages containing network or vulnerability data

# Google Hacking

- ▶ What makes this possible is the way in which information is indexed by a search engine.
- ▶ Some common commands are:
  - **intitle**: "index of" finance.pdf (returns pages that contain files of the name finance.pdf)
  - **filetype:bak**  
url:"htaccess|passwd|shadow|htusers" (return files that have specific extensions)

# Google Hacking

- **inurl**: admin inurl:backup intitle:index.of  
(returns pages that include specific words or characters in the URL.)

# Exploring Domain Information Leakage

- ▶ A public company that wants to attract customers must walk a fine line because some information by necessity will have to be made public while other information can be kept secret.
- ▶ An example of information that should be kept secret by any company is domain information, or the information that is associated with the registration of an Internet domain.

# Exploring Domain Information Leakage

- ▶ Currently many tools are available that can be used for obtaining types of basic information, like:
  - **whois**
  - **nslookup**
  - **Internet Assigned Numbers Authority (IANA)** and **Regional Institute Registries (RIRS)** to find the range of Internet Protocol (IP) address
  - **traceroute** to determine the location of the network

# Root Zone Database

- ▶ To determine the network range manually, the best resource is the IANA Web site at the Root Zone Database page located at:
  - <http://www.iana.org/domains/root/db>
- ▶ The Root Zone Database represents the delegation details of top level domain (TLDS), including domains such as .com and country code TLDS such as .us.



# Automatic Registrar Query

- ▶ Numerous Web sites are dedicated to providing network range information automatically.
- ▶ Some of the more common search machines are:
  - <http://www.betterwhois.com>
  - <http://geektools.com>
  - <http://www.all-nettools.com>
  - <http://www.smartwhois.com>
  - <http://www.dnsstuff.com>
  - <http://whois.domaintools.com>

# Automatic Registrar Query

## Whois Record for fh-Kiel.de

Find out more about [Project Whois](#) and [DomainTools for Windows](#).

**DOMAINTOOLS** for Windows [Download Now](#)  
Access domain ownership records from your desktop

### Related Domains For Sale or At Auction

1 2 3 More >

[Zekiel.com](#) (\$2,695)

[YorkieLovers.com](#) (\$1,799)


[KielO.com](#) (\$5,500)

[LickieLick.com](#) (\$2,095)

[KielOnline.com](#) (\$1,995)

[Kiellan.com](#) (\$2,088)

### — Whois & Quick Stats

Email	christian.behn@fh-kiel.de is associated with ~14 domains	↷
Registrant Org	Christian Behn is associated with ~20 other domains	↷
Dates	Updated on 2010-07-15	↷
IP Address	149.222.20.63 - 10 other sites hosted on this server	↷
IP Location	 - Schleswig-holstein - Dietrichsdorf - Fachhochschule Kiel	

# Automatic Registrar Query

- ▶ The aim of using of these tools is to obtain registrar information. Underlying all these tools is is Whois tool, which is software designed to query the databases that hold registration information.
- ▶ **whois:**
  - primarily used to verify whether a domain name is available or whether it has been registered. The whois information contains the name, address and phone number of the administrative, billing and technical contacts of the domain name.

# Automatic Registrar Query

- ▶ **nslookup**: queries Internet domain name servers. If nslookup is given an IP address or a fully qualified domain name (FQDN), it will look up and show the corresponding IP address.
- ▶ nslookup can be used to do:
  - Find additional IP addresses if authoritative DNS is known from Whois
  - List the MX (mail) server for a specific range of IP addresses

# Automatic Registrar Query

## ▶ tracerout:

- shows the IP address, name, the time it took to reach each host and return a response, giving a clear picture of the path to connect to the remote host and the time to do so.

# Tracerout

```
/u/a/mg:traceroute fh-kiel.de
traceroute to fh-kiel.de (149.222.20.63), 30 hops max, 60 byte packets
 1  sw-c1.cc.puv.fi (193.166.140.1)  1.739 ms  1.700 ms  1.680 ms
 2  fw1.cc.puv.fi (195.148.171.9)   0.699 ms  0.697 ms  0.699 ms
 3  sw-c2.cc.puv.fi (195.148.171.17)  1.845 ms  1.842 ms  1.814 ms
 4  funet2.cc.puv.fi (195.148.171.2)  55.914 ms 55.906 ms 55.892 ms
 5  csc6-et-1-3-0-1-utu6.funet.fi (193.166.255.38)  8.197 ms  8.182 ms  8.
 6  se-fre.nordu.net (109.105.102.104)  13.938 ms 13.676 ms 13.729 ms
 7  dk-ore.nordu.net (109.105.97.130)  22.104 ms 22.208 ms 22.180 ms
 8  nl-sar.nordu.net (109.105.97.137) 32.648 ms 32.675 ms 32.650 ms
 9  nordunet-bckp2.mx1.ams.nl.geant.net (62.40.125.205) 32.608 ms 32.676
2.661 ms
10 ael.mx1.ham.de.geant.net (62.40.98.61) 39.077 ms 39.060
11 cr-tubl.x-win.dfn.de (62.40.112.146) 49.697 ms 49.776 m
12 cr-han1-hundredgige0-6-0-0-7.x-win.dfn.de (188.1.144.189)
ms 54.114 ms
13 xr-brel-te2-2.x-win.dfn.de (188.1.145.242) 63.857 ms 63
```

# Internet Assigned Numbers Authority (IANA)

- ▶ IANA is responsible for the global coordination of the DNS root, IP addressing and other Internet protocol resources.
- ▶ The Root Zone Database page lists all top-level domains, including .com, .edu, .org and so on.
- ▶ To get information on an .com domain site we could start at:
  - <http://www.iana.org/domains/root/db/org.html>

# Internet Assigned Numbers Authority (IANA)

- ▶ These results also include a physical address along with all the other domain information.
- ▶ It would be possible to take the physical address provided and enter it into any of the commonly available mapping tools and gain information on the proximity of this address to the actual company.
- ▶ After knowing the domain administrator the next logical step could be to determine a valid network range.



# Determining a Network Range

- ▶ One of the missions of the IANA is to delegate Internet resources to RIRs (Regional Internet Registers)
- ▶ The RIRs further delegate resources as needed to customers, who include Internet service providers (ISPs) and end-user organizations.
- ▶ The RIRs are organizations responsible for control of IPV4 and IPv6 addresses within specific regions of the world.

# Regional Internet Registers (RIRs)

- ▶ The five RIRs are as follows:
  - American Registry for Internet Numbers (ARIN): North America and parts of the Caribbean
  - RIPE Network Coordination Center (RIPE NCC): Europe, the Middle East and Central Asia
  - Asia-Pacific Network Information Center (APNIC): Asia and the Pacific region
  - Latin American and Caribbean Internet Address Registry (LACNIC): Latin America and parts of the Caribbean region

# Regional Internet Registers (RIRs)

- ▶ Per standards each RIR must maintain point-of-contact (POC) information and IP address assignment.
- ▶ Some other Web sites used to mine the same type of information are:
  - <http://www.all-nettools.com>
  - <http://www.smartwhois.com>
  - <http://www.dnsstuff.com>

# Tracking Employees

- ▶ The Web can be used to find a wealth of information about a particular organization that can be used to plan a later attack.
- ▶ Gathering information on human beings is something that until recently has not been easy.
- ▶ But now, with the ever-increasing amount of personal information that people put online themselves, the task has become easier.

# Tracking Employees

- ▶ Information that can be uncovered online can include the following:
  - Posted photographs or information
  - Posted content about drinking or drug usage
  - Posting derogatory information about previous employers, coworkers or clients
  - Discriminatory comments or fabricated qualifications

# Tracking Employees

- ▶ Other employees have been known to get upset and set up what is known as a “sucks” domain, in which varying degrees of derogatory information are posted.
- ▶ Some of the sites that hackers have been known to review to obtain more information about a target includes:
  - Blogs: personal pages on a Social networking site: Facebook, MySpace, LinkedIn, Plaxo, Twitter, sucks domain

# Tracking Employees

- ▶ Wading into the sea of blogs on the Internet is a challenge, but using a site such as <http://www.blogsearchengine.com> will allow for the searchers of many blogs quickly.
- ▶ In addition, sites such as <http://www.wink.com> and <http://www.spock.com> allows users to search personal pages, such as on Facebook.

# Exploiting Insecure Applications

- ▶ Many applications were built with security in mind. Insecure applications such as Telnet, File Transfer Protocol (FTP), the “r” commands, Post Office Protocol (POP), Hyper Transfer Protocol (HTTP) and Simple Network Management Protocol (SNMP) operate without encryption.
- ▶ What adds to the problem is that some organizations even inadvertently put this information on the Web.



# Exploiting Insecure Applications

- ▶ As an example, terminal service Web access TSWEB (another name for Remote Desktop) is designed to allow users to connect to a work or home computer and access file just as if physically sitting in front of the computer.
- ▶ The problem with locating this information online is that an attacker can use the information to get further details about the organization or even break in more quickly in some cases.

# Thank you!

