Hacking Techniques &
Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail
All materials is licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0/

You are free:

- to Share — to copy, distribute and transmit the work
- to Remix — to adapt the work

Under the following conditions:

- Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.
# whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests
Reconnaissance
(RECON)

With great knowledge, comes successful attacks!
Outline - Reconnaissance

• Intelligence Gathering
• Target Selection
• Open Source Intelligence (OSINT)
• Covert Gathering
• Footprinting
Intelligence Gathering

- What is it
- Why do it
- What is it not

- Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence.
Target Selection

- Identification and Naming of Target
- Consider any Rules of Engagement limitations
- Consider time length for test
- Consider end goal of the test
Open Source Intelligence (OSINT)

• Simply, it’s locating, and analyzing publically (open) available sources of information.

• Intelligence gathering process has a goal of producing current and relevant information that is valuable to either an attacker or competitor.

- OSINT is not only web searching!
Open Source Intelligence (OSINT)

Takes three forms:
• Passive Information Gathering
• Semi-passive Information Gathering
• Active Information Gathering

Used for:
• Corporate
• Individuals
Corporate - Physical

• Locations
  – Public sites can often be located by using search engines such as:
    – Google, Yahoo, Bing, Ask.com, Baidu, Yandex, Guruji, etc

• Relationships
Corporate - Logical

- Business Partners
- Business Clients
- Competitors
- Product line
- Market Vertical
- Marketing accounts
- Meetings
- Significant company dates
- Job openings
- Charity affiliations
- Court records
- Political donations
- Professional licenses or registries
Job Openings Websites

- Bayt, http://bayt.com
- Monster, http://www.monster.com
- CareerBuilder, http://www.careerbuilder.com
- Indeed, LinkedIn, etc
Corporate – Org. Chart

- Position identification
- Transactions
- Affiliates
Corporate – Electronic

- Document Metadata
- Marketing Communications
Corporate – Infrastructure Assets

- Network blocks owned
- Email addresses
- External infrastructure profile
- Technologies used
- Purchase agreements
- Remote access
- Application usage
- Defense technologies
- Human capability
Corporate – Financial

- Reporting
- Market analysis
- Trade capital
- Value history
Individual - History

- Court Records
- Political Donations
- Professional licenses or registries
Individual - Social Network (SocNet) Profile

- Metadata Leakage
- Tone
- Frequency
- Location awareness
- Social Media Presence
Location Awareness - Cree.py

• Cree.py is an open source intelligence gathering application.
• Can gather from Twitter.
Searching for locations .. Be patient, I am doing my best.
This can take a while, please hold ...
Individual - Internet Presence

- Email Address
- Personal Handles/Nicknames
- Personal Domain Names registered
- Assigned Static IPs/Netblocks
Paterva Maltego is a data mining and information-gathering tool that maps the information gathered into a format that is easily understood and manipulated.

It saves you time by automating tasks such as email harvesting and mapping subdomains.
NetGlub

• NetGlub is an open source data mining and information-gathering tool that presents the information gathered in a format that is easily understood, (Similar to Maltego).

• Consists of: Master, Slave, and GUI
<table>
<thead>
<tr>
<th>Transform Name</th>
<th>Input Entity</th>
<th>Output Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Dns Name [SE]</td>
<td>Domain Name</td>
<td>Dns Name</td>
</tr>
<tr>
<td>To Dns Name [Brute Force]</td>
<td>Domain Name</td>
<td>Dns Name</td>
</tr>
<tr>
<td>To Ip Adress [Dig]</td>
<td>Website</td>
<td>Ip Address</td>
</tr>
<tr>
<td>To Email [Mirror]</td>
<td>Website</td>
<td>Email Address</td>
</tr>
<tr>
<td>To Entities [NER]</td>
<td>URL</td>
<td>Person, Ph</td>
</tr>
<tr>
<td>To Url [SE]</td>
<td>Phrase</td>
<td>URL</td>
</tr>
<tr>
<td>To Domain [parse]</td>
<td>Dns Name, Website, Message Exchanger record, Name Server Record Domain Name</td>
<td></td>
</tr>
<tr>
<td>To Websites [Backlinks]</td>
<td>Website</td>
<td>Website</td>
</tr>
<tr>
<td>To Location</td>
<td>Ip Address</td>
<td>Location</td>
</tr>
<tr>
<td>To AS Number [Whois]</td>
<td>Ip Address</td>
<td>Autonomom</td>
</tr>
<tr>
<td>To Website [Dump]</td>
<td>Dns Name</td>
<td>Website</td>
</tr>
<tr>
<td>To Dns Name [Zone Transfert]</td>
<td>Domain Name</td>
<td>Dns Name</td>
</tr>
<tr>
<td>To Website [Mirror]</td>
<td>Website</td>
<td>Website</td>
</tr>
<tr>
<td>To MX [Dig]</td>
<td>Domain Name</td>
<td>Message Exchanger</td>
</tr>
<tr>
<td>To Wiki diff[Shared Ip Address]</td>
<td>Ip Address</td>
<td>URL</td>
</tr>
<tr>
<td>To Location [Whois]</td>
<td>Domain Name</td>
<td>Location</td>
</tr>
<tr>
<td>To Url [Parse]</td>
<td>URL, Operating System</td>
<td>URL</td>
</tr>
<tr>
<td>To Website [<a href="http://www">www</a>.]</td>
<td>Domain Name</td>
<td>Website</td>
</tr>
<tr>
<td>To Ip [Nmap]</td>
<td>Ip Subnetwork</td>
<td>Ip Address</td>
</tr>
<tr>
<td>To Ip Block [Cuts]</td>
<td>Ip Address</td>
<td>Ip Subnetwork</td>
</tr>
<tr>
<td>To Url [Backlinks]</td>
<td>URL</td>
<td>URL</td>
</tr>
<tr>
<td>To NS [Dig]</td>
<td>Domain Name</td>
<td>Name Server</td>
</tr>
<tr>
<td>To Domain [TLD]</td>
<td>Domain Name</td>
<td>Domain Name</td>
</tr>
<tr>
<td>To Websites [Parse]</td>
<td>URL</td>
<td>Website</td>
</tr>
<tr>
<td>To Email [Whois]</td>
<td>Domain Name, Ip Address</td>
<td>Email Address</td>
</tr>
<tr>
<td>To Url [Mirror]</td>
<td>Website</td>
<td>Email Address</td>
</tr>
<tr>
<td>To Domain [Top Level]</td>
<td>Domain Name</td>
<td>Domain Name</td>
</tr>
<tr>
<td>To Ip Address [dig]</td>
<td>Dns Name, Message Exchanger record, Name Server Record</td>
<td>Ip Address</td>
</tr>
</tbody>
</table>
TheHarvester

- TheHarvester is a tool, written by Christian Martorella, that can be used to gather e-mail accounts and subdomain names from different public sources (search engines, pgp key servers).

DEMO:
- .\theHarvester.py -d linuxac.org -l 500 -b google
Social Networks

• Check Usernames - Useful for checking the existence of a given username across 160 Social Networks.
• http://checkusernames.com/
Social Networks

Newsgroups

• Google - http://www.google.com
• Yahoo Groups - http://groups.yahoo.com

Mail Lists

• The Mail Archive - http://www.mail-archive.com
Audio / Video

Audio
• Podcast.com, http://podcast.com
• Podcast Directory, http://www.podcastdirectory.com

Video
• YouTube, http://youtube.com
• Yahoo Video, http://video.search.yahoo.com
• Bing Video, http://www.bing.com/
• Vemo, http://vemo.com
Archived Information

• There are times when we will be unable to access web site information due to the fact that the content may no longer be available from the original source.

• Being able to access archived copies of this information allows access to past information.

• Perform Google searches using specially targeted search strings: cache:<site.com>

• Use the archived information from the Wayback Machine (http://www.archive.org).
The goal is to identify data that is relevant to the target corporation.

It may be possible to identify locations, hardware, software and other relevant data from Social Networking posts.

Examples:
- ixquick - http://ixquick.com
- MetaCrawler - http://metacrawler.com
- Dogpile - http://www.dogpile.com
- Search.com - http://www.search.com
- Jeffery's Exif Viewer - http://regex.info/exif.cgi
Metadata leakage - FOCA

- FOCA is a tool that reads metadata from a wide range of document and media formats.
- FOCA pulls the relevant usernames, paths, software versions, printer details, and email addresses.

- DEMO (WinXP VM_Box)
Metadata leakage - Foundstone SiteDigger

- Foundstone has a tool, named SiteDigger, which allows us to search a domain using specially strings from both the Google Hacking Database (GHDB) and Foundstone Database (FSDB).
### Domain to search

**Site/Domain:** [Optional]

### Search Queries

#### Queries Scanned:

1. "Index of /backup" F142
2. intitle:"Index of" ".htpasswd" htpasswd.bak F31
3. intitle:"Index of" index.html.bak F1
4. intitle:"Index of" index.html.bak F176
5. intitle:"Index of" index.html" F178
6. intitle:"Index of" index.jsp.bak F3
7. intitle:"Index of" index.php.bak F2
8. intitle:"Index of" index.php.bak F177
9. intitle:"Index of" index.php" F179
10. intitle:index.of ".bash_history" F19
11. intitle:index.of ".sh_history" F20
12. iniutl:backup intitle:index.of iniutl:admin F141

### Search Results

<table>
<thead>
<tr>
<th>URL</th>
<th>Query</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>i_index.shtml &quot;Ready&quot;</td>
<td>i_index.shtml &quot;Ready&quot;</td>
<td>Configuration...</td>
</tr>
<tr>
<td>i_index.shtml &quot;Ready&quot;</td>
<td>i_index.shtml &quot;Ready&quot;</td>
<td>Configuration...</td>
</tr>
<tr>
<td>i_index.shtml &quot;Ready&quot;</td>
<td>i_index.shtml &quot;Ready&quot;</td>
<td>Configuration...</td>
</tr>
<tr>
<td>&quot;Incorrect syntax ne...&quot;</td>
<td>&quot;Incorrect syntax ne...&quot;</td>
<td>Error Messa...</td>
</tr>
<tr>
<td>&quot;Incorrect syntax ne...&quot;</td>
<td>&quot;Incorrect syntax ne...&quot;</td>
<td>Error Messa...</td>
</tr>
<tr>
<td>&quot;http://&quot;:@www&quot; b...</td>
<td>index.of.etc</td>
<td>Files contain...</td>
</tr>
<tr>
<td>index.of.etc</td>
<td>index.of.etc</td>
<td>Files contain...</td>
</tr>
<tr>
<td>index.of.etc</td>
<td>index.of.etc</td>
<td>Files contain...</td>
</tr>
<tr>
<td>index.of.etc</td>
<td>index.of.etc</td>
<td>Files contain...</td>
</tr>
</tbody>
</table>
Metadata leakage - Metagoofil

- Metagoofil is a Linux based information gathering tool designed for extracting metadata of public documents (.pdf, .doc, .xls, .ppt, .odp, .ods) available on the client's websites.

- Metagoofil generates an html results page with the results of the metadata extracted, plus a list of potential usernames that could prove useful for brute force attacks. It also extracts paths and MAC address information from the metadata.
Individual - Physical Location

• Physical Location
Individual - Mobile Footprint

- Phone #
- Device type
- Installed applications
Covert Gathering - Corporate

On-Location Gathering
• Physical security inspections
• Wireless scanning / RF frequency scanning
• Employee behavior training inspection
• Accessible/adjacent facilities (shared spaces)
• Dumpster diving
• Types of equipment in use

Offsite Gathering
• Data center locations
• Network provisioning/provider
Other Gathering Forms

Human Intelligence (HUMINT)

• Methodology always involves direct interaction - whether physical, or verbal.

• Gathering should be done under an assumed identity (remember pretexting?).
  – Key Employees
  – Partners/Suppliers
Other Gathering Forms

Signals Intelligence (SIGINT):

- Intelligence gathered through the use of interception or listening technologies.

- Example:
  - Wired/Wireless Sniffer
  - TAP devices
Other Gathering Forms

Imagery Intelligence (IMINT):

- Intelligence gathered through recorded imagery, i.e. photography.
- IMINT can also refer to satellite intelligence, (cross over between IMINT and OSINT if it extends to Google Earth and its equivalents).