Χηαπτερ 4

Information Gathering

(Foot Printing and Reconnaissance)

Mohd Zaki Mas’ud

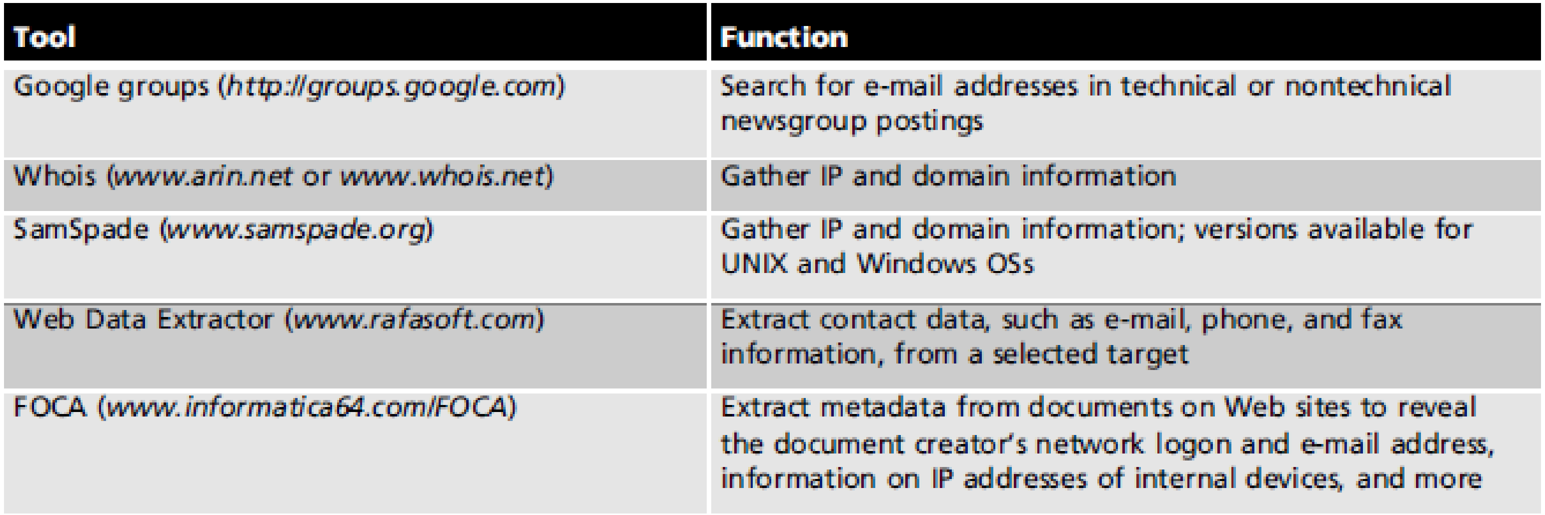
Content

- Introduction
- Goals of the Footprinting Process
- Terminology and Threat
- FootPrinting Process
- Social Engineering
- Reporting
- Summary

INTRODUCTION

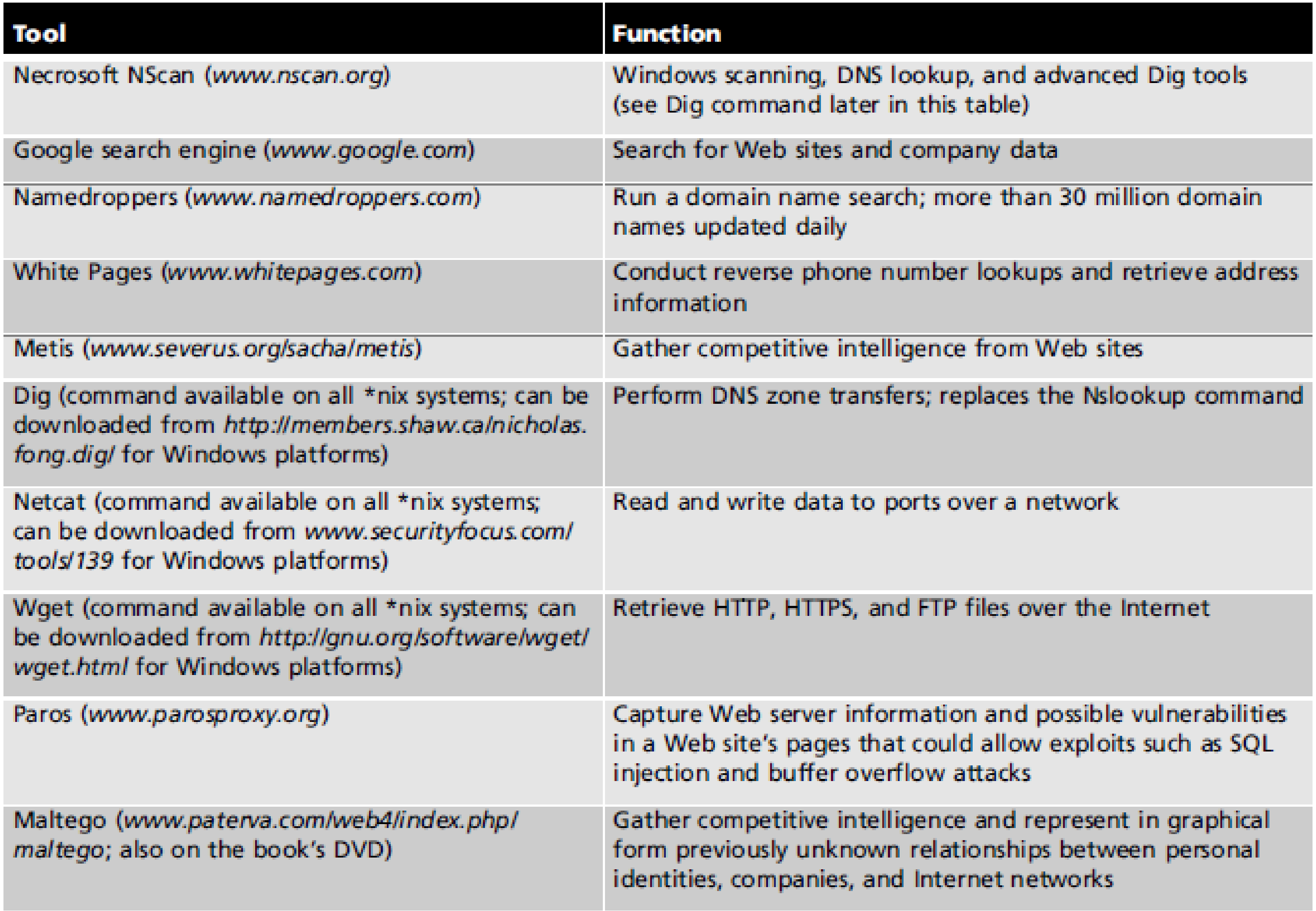
Introduction

- "Case the joint"
  - Look over the location
  - Find weakness in security systems
  - Types of locks, alarms
- In computer jargon, this is called footprinting
  - Discover information about
    - The organization
    - Its network
- The end result should be a profile of the target that is a rough picture but one that gives enough data to plan the next phase of scanning.
- Information that can be gathered during this phase includes:
    - IP address ranges
    - Namespaces
    - Employee information
    - Phone numbers
    - Facility information
    - Job information



Tool	Function
Google groups (*http://groups.google.com*)	Search for e-mail addresses in technical or nontechnical newsgroup postings
Whois (*www.arin.net* or *www.whois.net*)	Gather IP and domain information
SamSpade (*www.samspade.org*)	Gather IP and domain information; versions available for UNIX and Windows OSs
Web Data Extractor (*www.rafasoft.com*)	Extract contact data, such as e-mail, phone, and fax information, from a selected target
FOCA (*www.informatica64.com/FOCA*)	Extract metadata from documents on Web sites to reveal the document creator’s network logon and e-mail address, information on IP addresses of internal devices, and more

Table 4-1 Summary of Web tools



Tool	Function
Necrosoft NScan (*www.nscan.org*)	Windows scanning, DNS lookup, and advanced Dig tools (see Dig command later in this table)
Google search engine (*www.google.com*)	Search for Web sites and company data
Namedroppers (*www.namedroppers.com*)	Run a domain name search; more than 30 million domain names updated daily
White Pages (*www.whitepages.com*)	Conduct reverse phone number lookups and retrieve address information
Metis (*www.severus.org/sacha/metis*)	Gather competitive intelligence from Web sites
Dig (command available on all *nix systems; can be downloaded from *http://members.shaw.ca/nicholas.fong.dig/* for Windows platforms)	Perform DNS zone transfers; replaces the Nslookup command
Netcat (command available on all *nix systems; can be downloaded from *www.securityfocus.com/tools/139* for Windows platforms)	Read and write data to ports over a network
Wget (command available on all *nix systems; can be downloaded from *http://gnu.org/software/wget/wget.html* for Windows platforms)	Retrieve HTTP, HTTPS, and FTP files over the Internet
Paros (*www.parosproxy.org*)	Capture Web server information and possible vulnerabilities in a Web site's pages that could allow exploits such as SQL injection and buffer overflow attacks
Maltego (*www.paterva.com/web4/index.php/maltego*; also on the book's DVD)	Gather competitive intelligence and represent in graphical form previously unknown relationships between personal identities, companies, and Internet networks

Table 4-1 Summary of Web tools (cont’d.)

GOALS OF THE FOOTPRINTING PROCESS

Here’s what you should look for:

- Network information
- Operating system information
- Organization information, such as CEO and employee information, office information,
- and contact numbers and e-mail
- Network blocks
- Network services
- Application and web application data and configuration information
- System architecture
- Intrusion detection and prevention systems
- Employee names
- Work experience

In term Of Network Architecture

- Domain names the company uses to conduct business or other functions, including
- research and customer relations
- Internal domain name information
- IP addresses of available systems
- Rogue or unmonitored websites that are used for testing or other purposes
- Private websites
- TCP/UDP services that are running
- Access control mechanisms, including firewalls and ACLs
- Virtual private network (VPN) information
- Intrusion detection and prevention information as well as configuration data
- Telephone numbers, including analog and Voice over Internet Protocol (VoIP)
- Authentication mechanisms and systems

In term of Operating System Information

- User and group information and names
- Banner grabbing
- Routing tables
- SNMP
- System architecture
- Remote system data
- System names
- Passwords

In term of Organization Data

- Employee details
- Organization’s website
- Company directory
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles and press releases

TERMINOLOGY & THREATS

Terminology

- **Open Source and Passive Information Gathering**
  - obtaining information from those sources that are typically publicly available and out in the open.
  - Potential sources include newspapers, websites, discussion groups, press releases, television, social networking, blogs, and etc.
- **Active Information Gathering**
  - involves engagement with the target through techniques such as social engineering
- **Pseudonymous Footprinting**
  - gathering information from online sources that are posted by someone from the target but under a different name or in some cases a pen name.
  - In essence the information is not posted under a real name or anonymously
- **Internet Footprinting**
  - gaining information from the Internet (Google hacking)

Threats Introduced by Footprinting

- **Social Engineering** One of the easiest ways to gain information about a target or to get information in general is to just ask for it

- **Network and System Attacks** These are designed to gather information relating to an environment’s system configuration and operating systems.

- **Information Leakage** This one is far too common nowadays as organizations frequently have become victims of data and other company secrets slipping out the door and into the wrong hands.

- **Privacy Loss** Another one that is common is privacy loss. Attackers gaining access to a system can compromise not only the security of the system, but the privacy of the information stored on it as well.

- **Revenue Loss,** Loss of information and security related to online business, banking, and financial-related issues can easily lead to lack of trust in a business, which may even lead to closure of the business itself.

FOOTPRINTING PROCESS

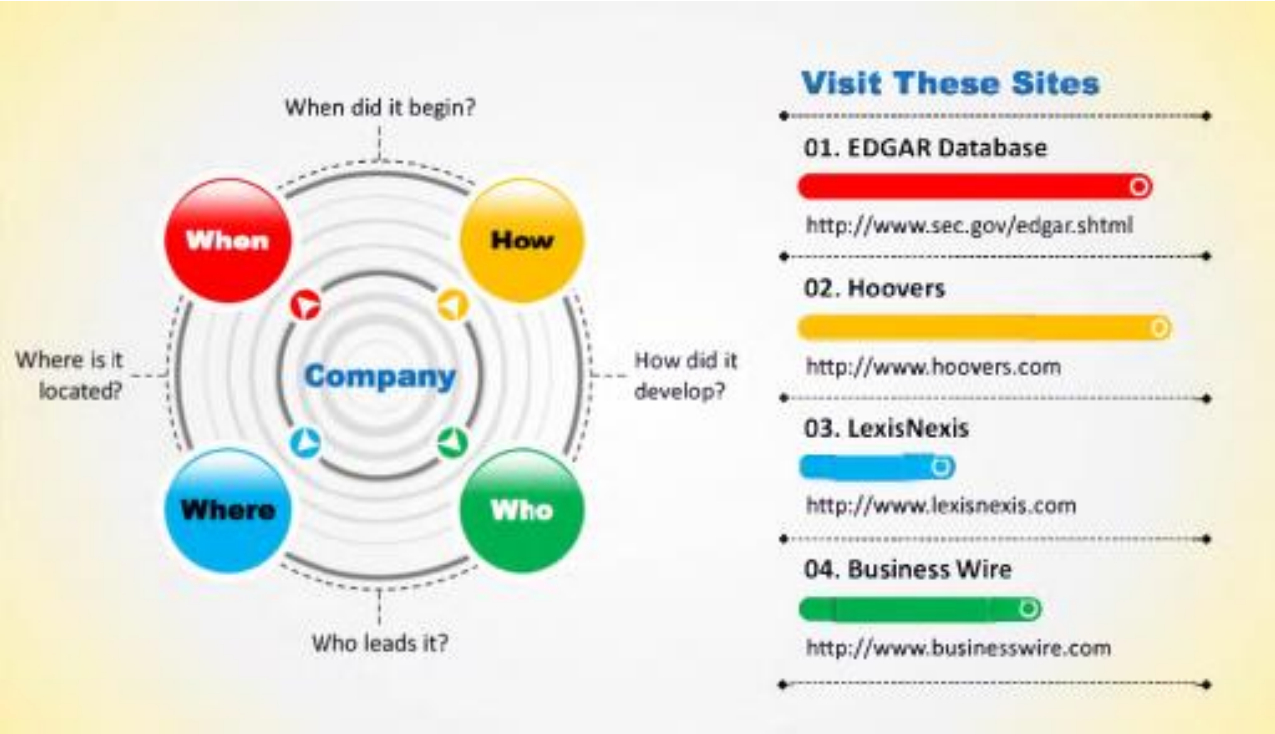
The Footprinting Process

- **Using Search Engines**
  - provide a wealth of information that the client may have wished to have kept hidden or may have just plain forgotten about it.
  - can find a lot of information, some of it completely unexpected or something a defender never considers, such as technology platforms, employee details, login pages, intranet portals, and so on
  - provide even more details such as names of security personnel, brand and type of firewall, and antivirus protection, and it is not unheard of to find network diagrams and other information
  - Related tool
    - **Netcraft** Actually a suite of related tools, you can use Netcraft to obtain web server version, IP address, subnet data, OS information, and subdomain information for any URL. Remember this tool—it will come in handy later.
    - **Link Extractor** This utility locates and extracts the internal and external URLs for a given location.

- **Public and Restricted Websites**
  - Websites that are intended *not* to be public but to be restricted to a few can provide you with valuable information

- **Location and Geography**
  - any information pertaining to the physical location of offices and personnel.
  - You should seek this information during the footprinting process because it can yield other key details that you may find useful in later stages, including physical penetrations
  - Among the tool available :-
    - **Google Earth**
    - **Google Maps**
    - **Webcams**
      - These are very common, and they can provide information on locations or people.
    - **People Search**
      - Many websites offer information of public record that can be easily
      - accessed by those willing to search for it. examples of people search utilities are Spokeo, ZabaSearch, Wink, and Intelius.

- Competitive analysis
  - Gathering competitor documents and records help simprove productivity and profitability and stimulate the growth.



01. EDGAR Database
http://www.sec.gov/edgar.shtml

02. Hoovers
http://www.hoovers.com

03. LexisNexis
http://www.lexisnexis.com

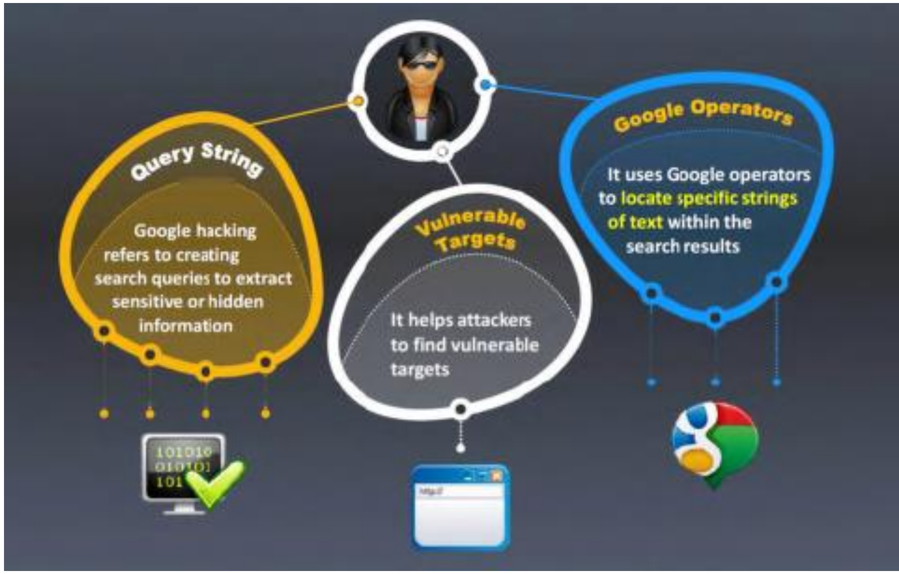
04. Business Wire
http://www.businesswire.com

- **Financial Services and Information Gathering**
  - Yahoo! Finance, Google Finance, and CNBC provide information that may not be available via other means. This data includes company officers, profiles, shares, competitor analysis, and many other pieces of data

- **The Value of Job Sites**
  - gathering information about a target is through job sites and job postings
  - Can find information such as infrastructure data, operating system information, and other useful data.
  - analyzing job postings, keep an eye out for information such as:
    - Job requirements and experience
    - Employer profile
    - Employee profile
    - Hardware information (this is incredibly common to see in profiles; look for labels such as Cisco, Microsoft, Juniper, Checkpoint, and others that may include model or version numbers)
    - Software information

- **Working with E-mail**
  - contents of e-mail are staggering and can be extremely valuable to an attacker looking for more inside information
  - PoliteMail (*www.politemail.com*), which is designed to create and track e-mail communication from within Microsoft Outlook.
- **Google Hacking**
  - using advanced operators to fine-tune your results to get what you want instead of being left at the whim of the search engine.
  - With Google hacking it is possible to fine-tune results to obtain items such as passwords, certain file types, sensitive folders, logon portals, configuration data, and other data
  - www.exploit-db.com/google-dorks/

- Error messages that contain sensitive information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability dat a
- Advisories and server vulnerabilities


Query String
Google hacking refers to creating search queries to extract sensitive or hidden information
Vulnerable Targets
It helps attackers to find vulnerable targets
Google Operators
It uses Google operators to locate specific strings of text within the search results
101010
010101
101

- **cache** Displays the version of a web page that Google contains in its cache instead of displaying the current version.
  - Syntax: **cache:<website name>**

- **link** Lists any web pages that contain links to the page or site specified in the query.
  - Syntax: **link:<website name>**

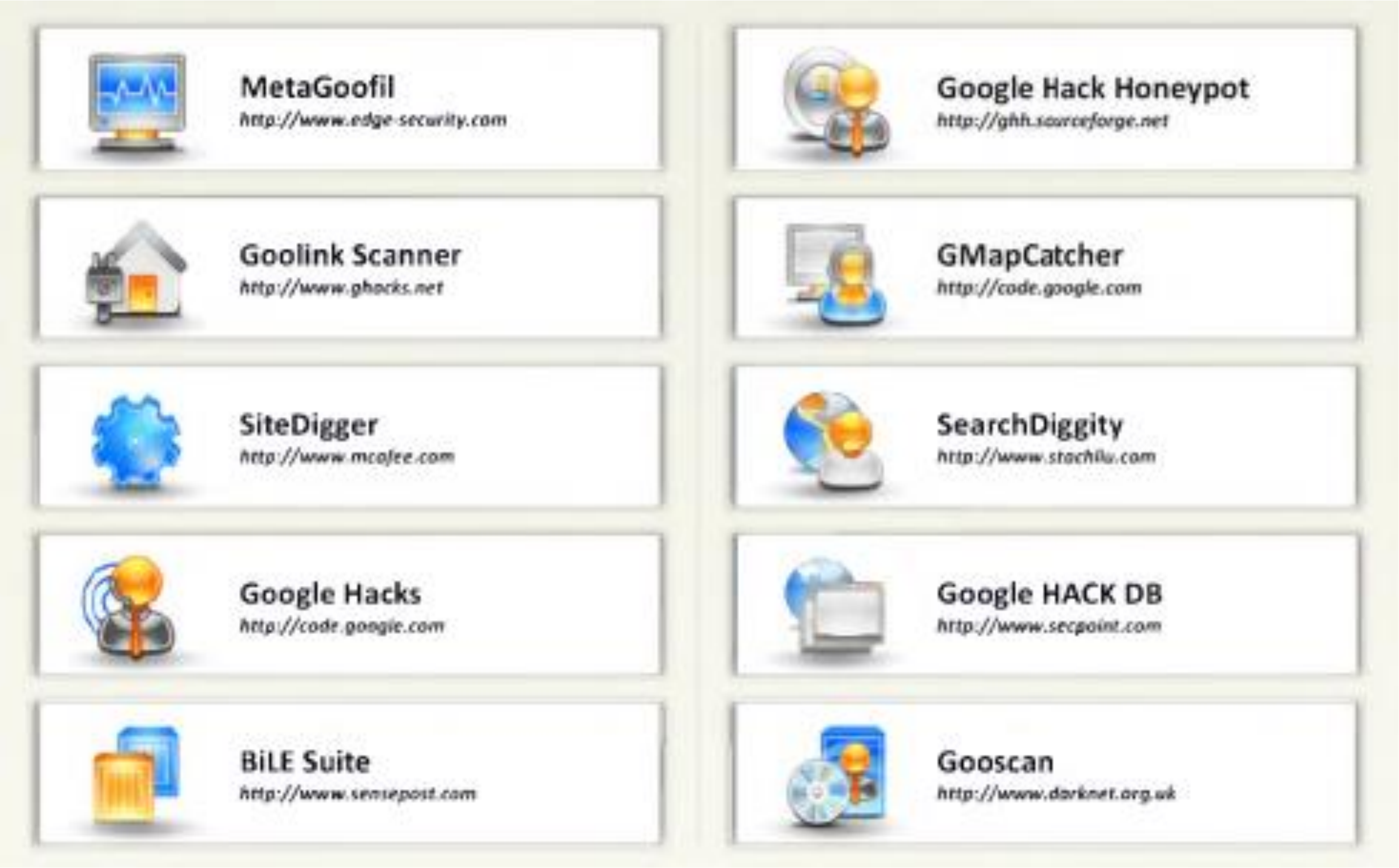
- **info** Presents information about the listed page.
  - Syntax: **info:<website name>**

- **site** Restricts the search to the location specified.
  - Syntax: **<keyword> site:<website name>**

- **allintitle** Returns pages with specified keywords in their title.
  - Syntax: **allintitle:<keywords>**

- **allinurl** Returns only results with the specific query in the URL.
  - Syntax: **allinurl:<keywords>**

Google hacking Tools



MetaGoofil
http://www.edge-security.com

Goolink Scanner
http://www.ghocks.net

SiteDigger
http://www.mcafee.com

Google Hacks
http://code.google.com

BiLE Suite
http://www.sensepost.com

Google Hack Honeypot
http://ghh.sourceforge.net

GMapCatcher
http://code.google.com

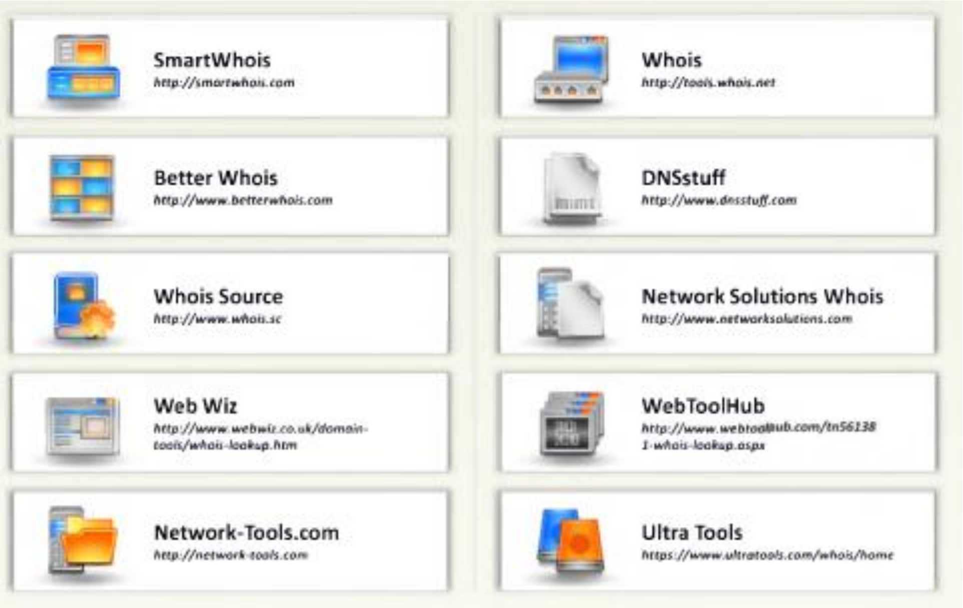
SearchDiggity
http://www.stachliu.com

Google HACK DB
http://www.secpoint.com

Gooscan
http://www.darknet.org.uk

- **Gaining Network Information**
  - gain information, where possible, about a target’s network
  - **Whois** This utility helps you gain information about a domain name, including ownership information, IP information, netblock data, and other information where available.
  - **Tracert** This utility is designed to follow the path of traffic from one point to another, including intermediate points in between.

Who is tools



SmartWhois
http://smartwhois.com

Better Whois
http://www.betterwhois.com

Whois Source
http://www.whois.sc

Web Wiz
http://www.webwiz.co.uk/domain-tools/whois-lookup.htm

Network-Tools.com
http://network-tools.com

Whois
http://tools.whois.net

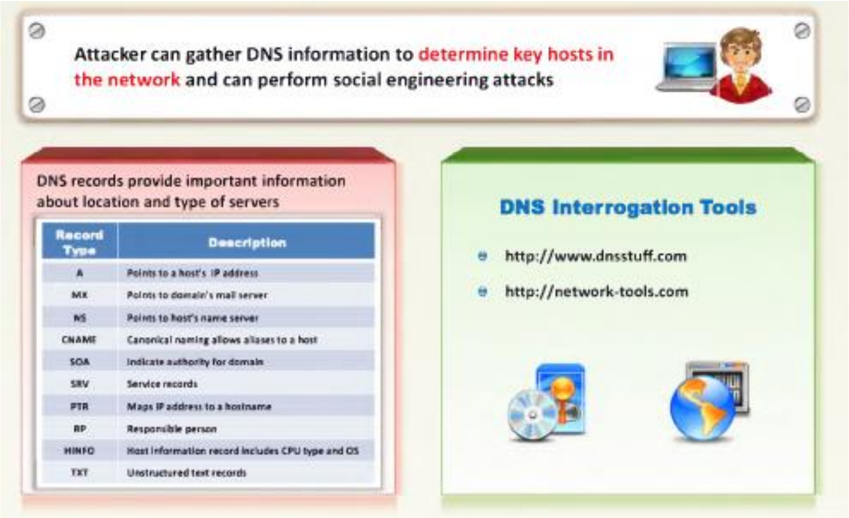
DNSstuff
http://www.dnsstuff.com

Network Solutions Whois
http://www.networksolutions.com

WebToolHub
http://www.webtoolhub.com/tn561381-whois-lookup.aspx

Ultra Tools
https://www.ultratools.com/whois/home

DNS Reconaissance



Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks

DNS records provide important information about location and type of servers

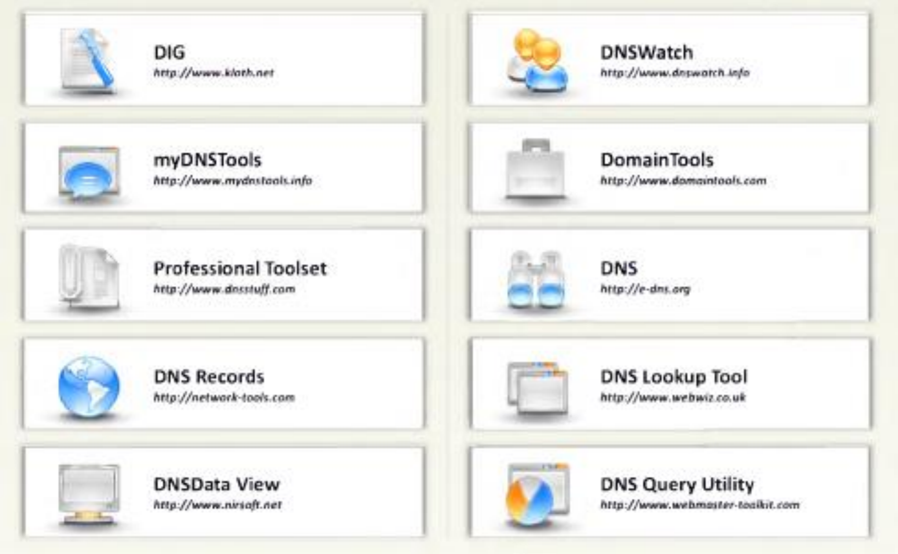
Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

DNS Interrogation Tools

- http://www.dnsstuff.com
- http://network-tools.com

- The attacker performs DNS foot printing on the target network in order to obtain the information about DNS.
- This info can be use to determine key hosts in the network and then performs social engineering attacks to gather more information.

- Once send the query using the DNS interrogation tool to the DNS server, the server will respond to you with a record structure that contains information about the target DNS .



DIG
http://www.kloth.net

myDNSTools
http://www.mydnstools.info

Professional Toolset
http://www.dnsstuff.com

DNS Records
http://network-tools.com

DNSData View
http://www.nirsoft.net

DNSWatch
http://www.dnswatch.info

DomainTools
http://www.domaintools.com

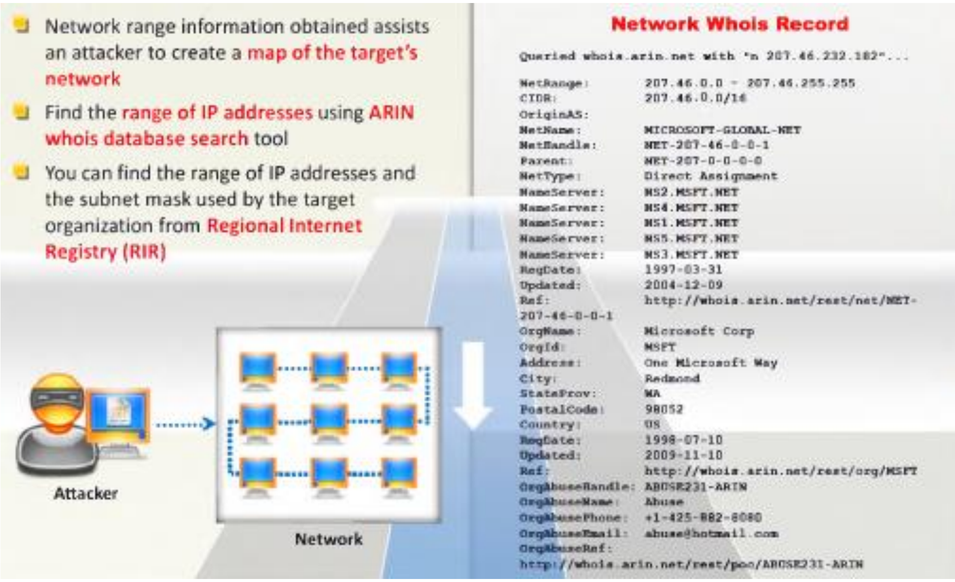
DNS
http://e-dns.org

DNS Lookup Tool
http://www.webwiz.co.uk

DNS Query Utility
http://www.webmaster-toolkit.com

- M- Points to domain's mail server
- NS- Points to host's name server
- CNAME - Canonical naming allows aliases to a host
- SOA - Indicate authority for domain
- SRV - Servicere cords
- PTR - Maps IP address to a host name
- RP - Responsible person
- HINFO – Host information recorcd includes CPU type and OS

Locate the Network Range



- Network range information obtained assists an attacker to create a map of the target's network
- Find the range of IP addresses using ARIN whois database search tool
- You can find the range of IP addresses and the subnet mask used by the target organization from Regional Internet Registry (RIR)

Network Whois Record

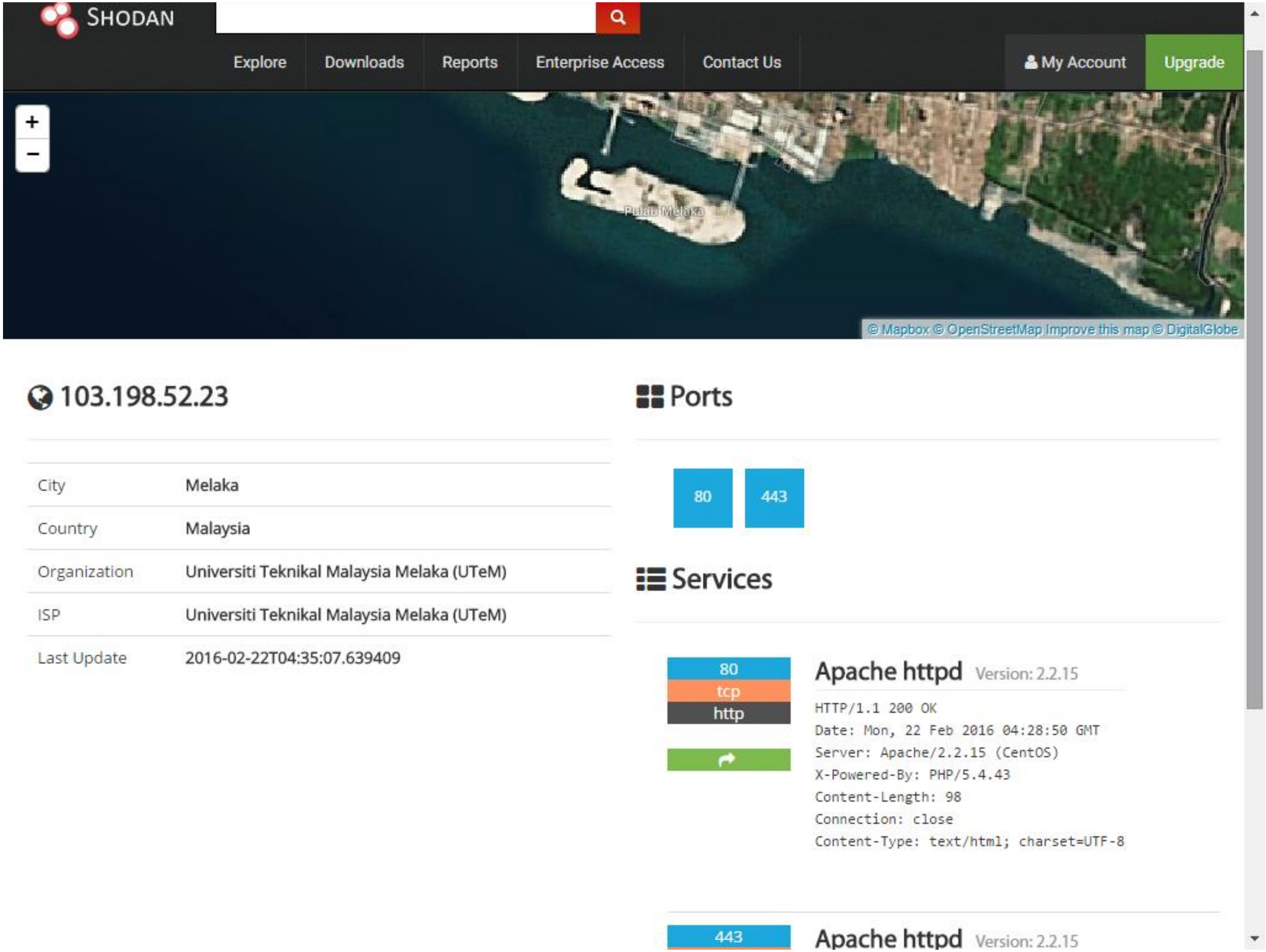
```
Queried whois.arin.net with "n 207.46.232.182"...

NetRange:       207.46.0.0 - 207.46.255.255
CIDR:           207.46.0.0/16
OriginAS:
NetName:        MICROSOFT-GLOBAL-NET
NetHandle:      NET-207-46-0-0-1
Parent:         NET-207-0-0-0-0
NetType:        Direct Assignment
NameServer:     NS2.MSFT.NET
NameServer:     NS4.MSFT.NET
NameServer:     NS1.MSFT.NET
NameServer:     NS5.MSFT.NET
NameServer:     NS3.MSFT.NET
RegDate:        1997-03-31
Updated:        2004-12-09
Ref:            http://whois.arin.net/rest/net/NET-
207-46-0-0-1
OrgName:        Microsoft Corp
OrgId:          MSFT
Address:        One Microsoft Way
City:           Redmond
StateProv:      WA
PostalCode:     98052
Country:        US
RegDate:        1998-07-10
Updated:        2009-11-10
Ref:            http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle: ABUSE231-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-425-882-8080
OrgAbuseEmail:  abuse@hotmail.com
OrgAbuseRef:
http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

- get more detailed in formation from the appropriate regional registry data base regarding IP allocation and the nature of the allocation .
- An attacker can also determine the subnet mask of the domain

OS fingerprinting

- findout the OS running on the target network.
- The Netcraft tool can be used to findout the OS running on the target network .

- Netcraf
- Shodan



103.198.52.23

City	Melaka
Country	Malaysia
Organization	Universiti Teknikal Malaysia Melaka (UTeM)
ISP	Universiti Teknikal Malaysia Melaka (UTeM)
Last Update	2016-02-22T04:35:07.639409

Ports

80 443

Services

80
tcp
http

Apache httpd Version: 2.2.15

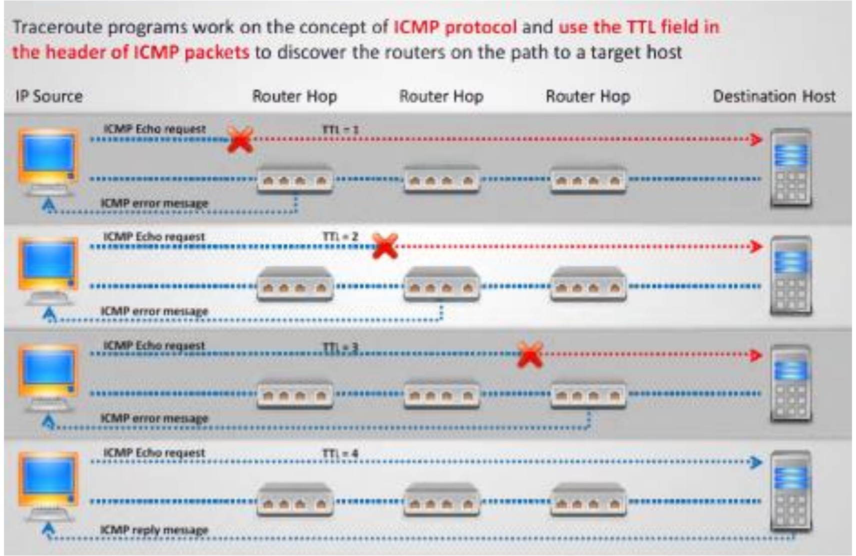
```
HTTP/1.1 200 OK
Date: Mon, 22 Feb 2016 04:28:50 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.43
Content-Length: 98
Connection: close
Content-Type: text/html; charset=UTF-8
```

443

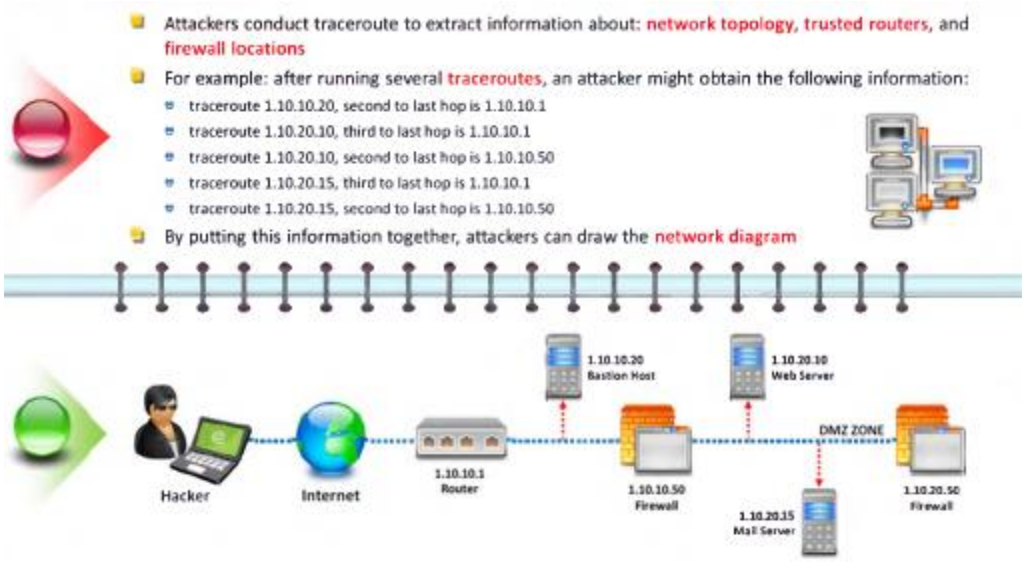
Apache httpd Version: 2.2.15

Traceroute

- It allows you to trace the path or route through which the target host packets travel in the network

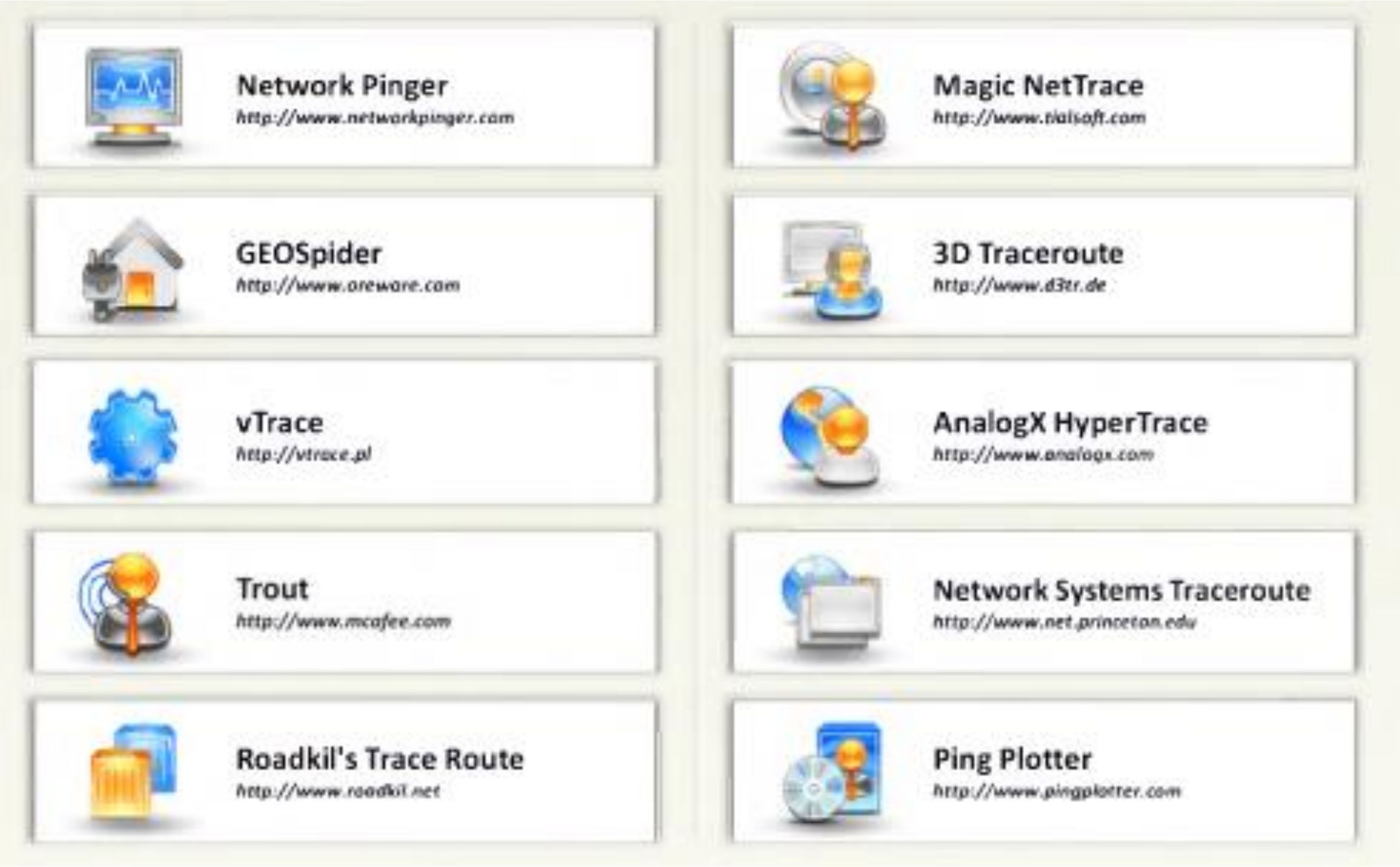


Traceroute programs work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover the routers on the path to a target host



- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations
- For example: after running several traceroutes, an attacker might obtain the following information:
  - traceroute 1.10.10.20, second to last hop is 1.10.10.1
  - traceroute 1.10.20.10, third to last hop is 1.10.10.1
  - traceroute 1.10.20.10, second to last hop is 1.10.10.50
  - traceroute 1.10.20.15, third to last hop is 1.10.10.1
  - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By putting this information together, attackers can draw the network diagram

Traceroute tools



Network Pinger
http://www.networkpinger.com

GEOSpider
http://www.oreware.com

vTrace
http://vtrace.pl

Trout
http://www.mcafee.com

Roadkil's Trace Route
http://www.roadkil.net

Magic NetTrace
http://www.tialsoft.com

3D Traceroute
http://www.d3tr.de

AnalogX HyperTrace
http://www.analogx.com

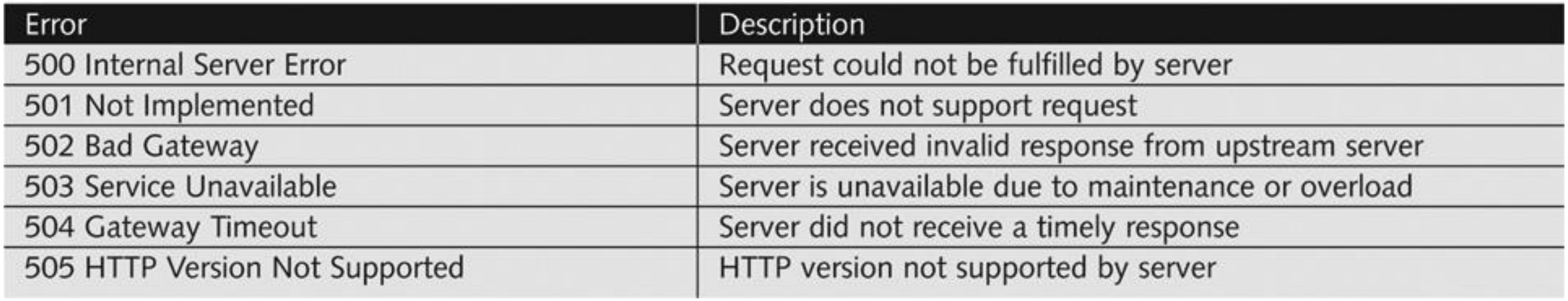
Network Systems Traceroute
http://www.net.princeton.edu

Ping Plotter
http://www.pingplotter.com

Table 4-2 HTTP client errors

Error	Description
400 Bad Request	Request not understood by server
401 Unauthorized	Request requires authentication
402 Payment Required	Reserved for future use
403 Forbidden	Server understands request but refuses to comply
404 Not Found	Unable to match request
405 Method Not Allowed (methods are covered later in this section)	Request not allowed for the resource
406 Not Acceptable	Resource does not accept your request
407 Proxy Authentication Required	Client must authenticate with proxy
408 Request Timeout	Request not made by client in allotted time
409 Conflict	Request could not be completed due to an inconsistency
410 Gone	Resource is no longer available
411 Length Required	Content length not defined
412 Precondition Failed	Request header fields evaluated as false
413 Request Entity Too Large	Request larger than server is able to process
414 Request-URI (Uniform Resource Identifier) Too Long	Request-URI is longer than the server is willing to accept

Table 4-3 HTTP server errors



Error	Description
500 Internal Server Error	Request could not be fulfilled by server
501 Not Implemented	Server does not support request
502 Bad Gateway	Server received invalid response from upstream server
503 Service Unavailable	Server is unavailable due to maintenance or overload
504 Gateway Timeout	Server did not receive a timely response
505 HTTP Version Not Supported	HTTP version not supported by server

SOCIAL ENGINEERING

Social Engineering:
The Art of Hacking Humans

- Older than computers
- Targets the human component of a network
- Goals
  - Obtain confidential information (passwords)
  - Obtain personal information

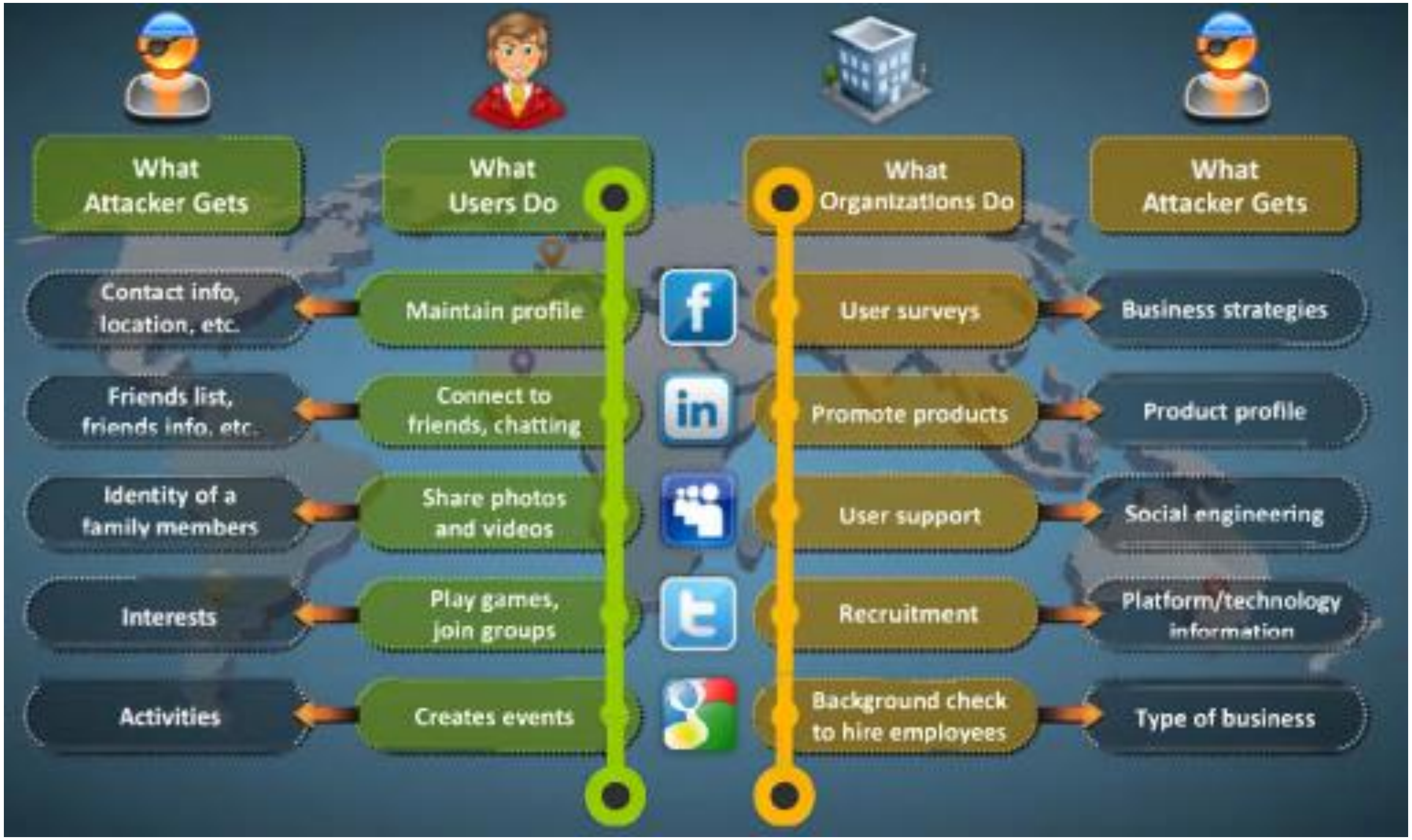
“Manipulate people into doing something, rather than by breaking in using technical means”

SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

SE Movie to watch

How Information on SM can be manipulated



What Attacker Gets

What Users Do

What Organizations Do

What Attacker Gets

Contact info, location, etc. ← Maintain profile | User surveys → Business strategies

Friends list, friends info, etc. ← Connect to friends, chatting | Promote products → Product profile

Identity of a family members ← Share photos and videos | User support → Social engineering

Interests ← Play games, join groups | Recruitment → Platform/technology information

Activities ← Creates events | Background check to hire employees → Type of business

Types of Social Engineering

- **Quid Pro Quo**
  - Something for something
- **Phishing**
  - Fraudulently obtaining private information
- **Baiting**
  - Real world trojan horse
- **Pretexting**
  - Invented Scenario
- **Diversion Theft**
  - A con

Quid Pro Quo

- **Something for Something**
  - **Call random numbers** at a company, claiming to be from technical support.
  - Eventually, you will reach someone with a **legitamite problem**
  - Grateful you called them back, they will **follow your instructions**
  - The attacker will "help" the user, but will really have the victim type commands that will allow the attacker to **install malware**

Phishing

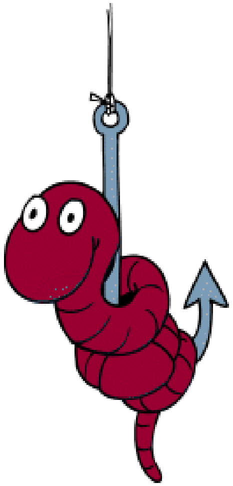
- **Fraudulently obtaining private information**
  - **Send an email** that looks like it came from a legitimate business
  - **Request verification** of information and warn of some consequence if not provided
  - Usually contains link to a **fraudulent web page** that looks legitimate
  - User gives information to the social engineer
    - **Ex**: Ebay Scam

Phishing continued

- Spear Fishing
  - **Specific phishing**
    - **Ex**: email that makes claims using your name

- Vishing
  - **Phone phishing**
  - Rogue interactive voice system
    - **Ex**:call bank to verify information

Baiting



- **Real world Trojan horse**
  - **Uses physical media**

  - Relies on **greed/curiosity of victim**

  - Attacker leaves a **malware infected cd or usb drive** in a location sure to be found

  - Attacker puts a **legitimate or curious lable** to gain interest

  - **Ex**: "Company Earnings 2009" left at company elevator
    - **Curious employee/Good samaritan uses**
    - User inserts media and **unknowingly installs malware**

Pretexting

- **Invented Scenario**
  - **Prior Research/Setup** used to establish legitimacy
    - **Give** information that a user would normally not divulge

  - This technique is **used to impersonate**
    - **Authority** ect
      - Using **prepared answers** to victims questions
      - **Other gathered information**

  - **Ex**: Law Enforcement
    - **Threat of alleged infraction** to detain suspect and hold for questioning

Pretexting Real Example:

- **Signed up for Free Credit Report**

- Saw **Unauthorized charge** from another credit company

    - Called to **dispute charged** and was **asked for Credit Card Number**

        - They **insisted it was useless** without the security code

    - Asked for **Social Security number**

- Talked to **Fraud Department** at my bank

Diversion Theft

- **A Con**
  - Persuade deliver person that **delivery is requested elsewhere** - "*Round the Corner*"
  - When deliver is redirected, attacker pursuades delivery driver to **unload delivery near address**
  - **Ex**: Attacker parks **security van outside a bank**. **Victims going to deposit money** into a night safe are told that the **night safe is out of order**. **Victims then give money to attacker** to put in the fake security van
  - Most companies do not prepare employees for this type of attack

The Art of Shoulder Surfing

- Shoulder surfer
  - Reads what users enter on keyboards
    - Logon names
    - Passwords
    - PINs

Tools for Shoulder Surfing

- Binoculars or telescopes or cameras in cell phones
- Knowledge of key positions and typing techniques
- Knowledge of popular letter substitutions
  - s equals $, a equals @

The Art of Shoulder Surfing (continued)

- Prevention
  - Avoid typing when someone is nearby
  - Avoid typing when someone nearby is talking on cell phone
  - Computer monitors should face away from door or cubicle entryway
  - Immediately change password if you suspect someone is observing you

Dumpster Diving

- Attacker finds information in victim’s trash
  - Discarded computer manuals
    - Notes or passwords written in them
  - Telephone directories
  - Calendars with schedules
  - Financial reports
  - Interoffice memos
  - Company policy
  - Utility bills
  - Resumes of employees

The Art of Dumpster Diving (continued)

- Prevention
  - Educate your users about dumpster diving
  - Proper trash disposal
  - Use “disk shredder” software to erase disks before discarding them
    - Software writes random bits
    - Done at least seven times
  - Discard computer manuals offsite
  - Shred documents before disposal

Piggybacking

- Trailing closely behind an employee cleared to enter restricted areas
- How it works:
  - Watch authorized personnel enter an area
  - Quickly join them at security entrance
  - Exploit the desire of other to be polite and helpful
  - Attacker wears a fake badge or security card

Piggybacking Prevention

- – Use turnstiles
- – Train personnel to notify the presence of strangers
- – Do not hold secured doors for anyone
  - Even for people you know
- – All employees must use secure cards

Weakest Link?

- No matter how strong your:
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software

- You are the weakest link in computer security!
  - People are more vulnerable than computers

- "*The weakest link in the security chain is the human element*" -Kevin Mitnick

Ways to Prevent Social Engineering

Training

- User Awareness
  - User knows that **giving out certain information is bad**

- **Military** requires Cyber Transportation to hold
  - **Top Secret Security Clearance**
  - **Security Plus Certification**

- **Policies**
  - Employees are **not allowed to divulge private information**
  - **Prevents employees from being socially pressured or tricked**

Ways to Prevent Social Engineering Cont..

- 3rd Party test - **Ethical Hacker**
  - Have a third party come to your company and attempted to **hack into your network**
  - 3rd party will attempt to **glean information from employees using social engineering**
  - Helps **detect problems people have with security**

- **Be suspicious** of unsolicited phone calls, visits, or email messages from individuals asking about internal information

- **Do not provide personal information**, information about the company(such as internal network) unless authority of person is verified

General Saftey

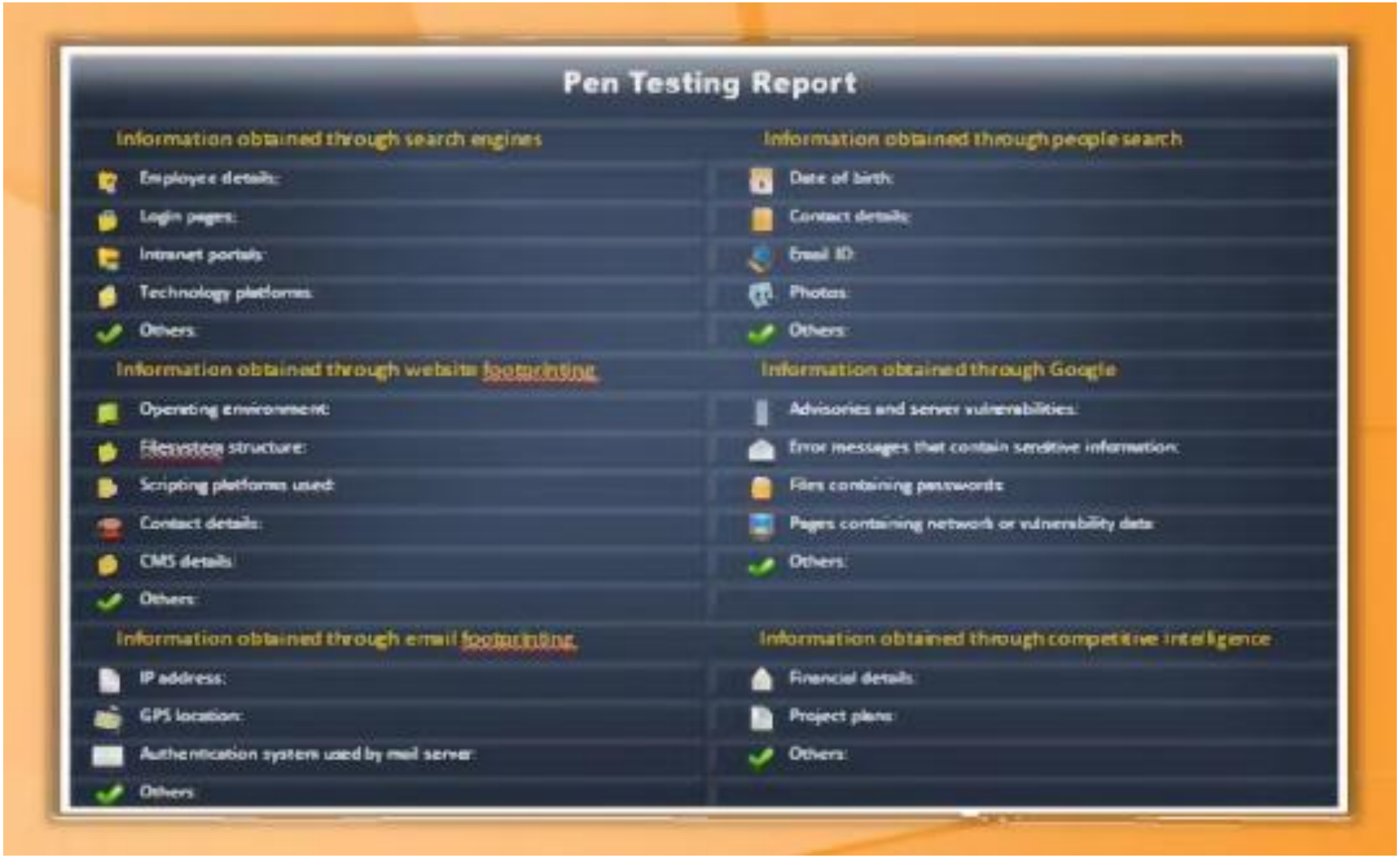
- Before transmitting personal information over the internet, check the **connection is secure** and check the **url is correct**

- If unsure if an email message is legitimate, **contact the person or company by another means** to verify

- Be **paranoid and aware** when interacting with anything that needs protected
    - The smallest information could compromise what you're protecting

REPORTING

FootPrinting and Reconnaissance PT Report



Pen Testing Report

Information obtained through search engines

- Employee details:
- Login pages:
- Intranet portals:
- Technology platforms:
- ✓ Others:

Information obtained through website footprinting

- Operating environment:
- Filesystem structure:
- Scripting platforms used:
- Contact details:
- CMS details:
- ✓ Others:

Information obtained through email footprinting

- IP address:
- GPS location:
- Authentication system used by mail server:
- ✓ Others:

Information obtained through people search

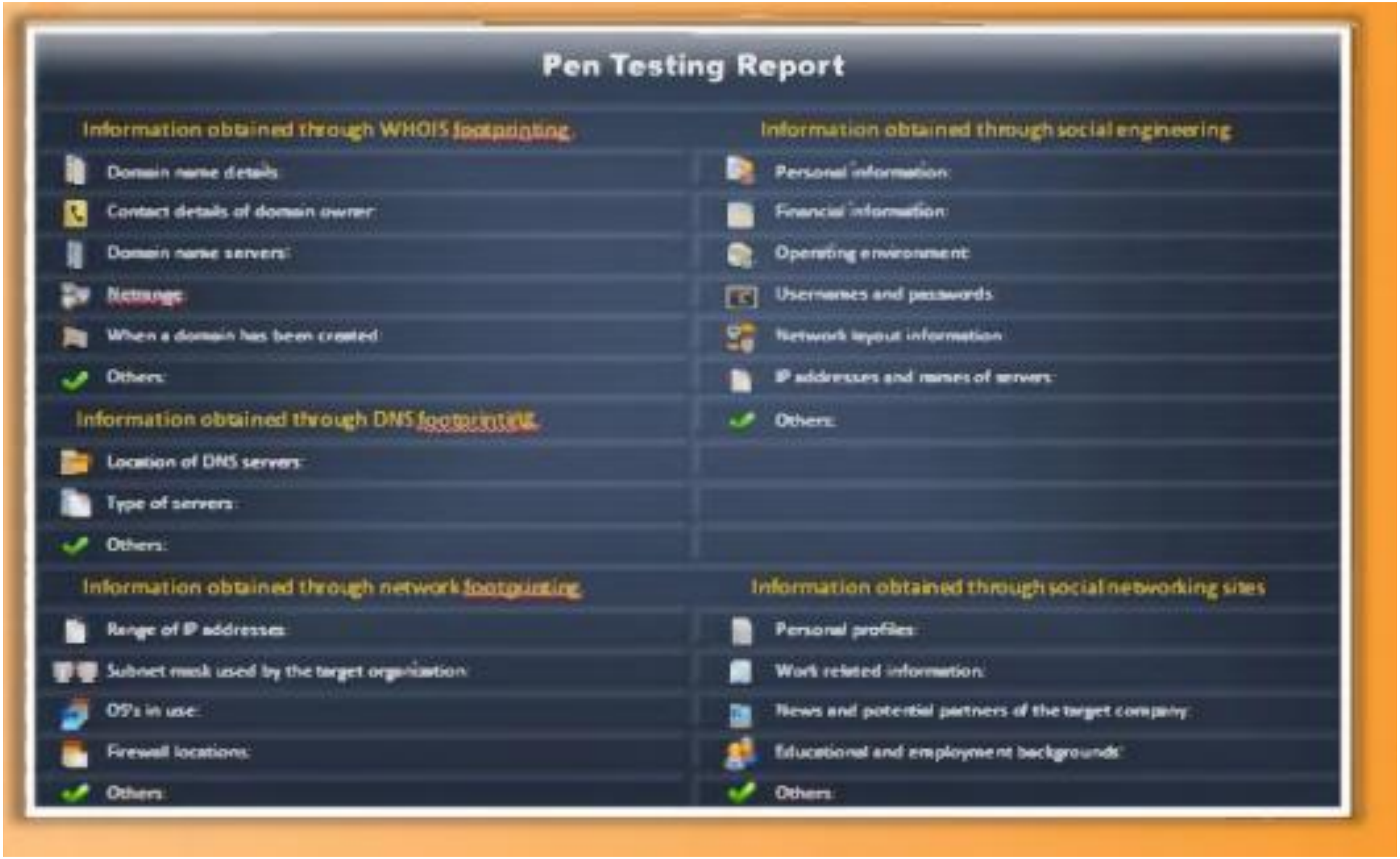
- Date of birth:
- Contact details:
- Email ID:
- Photos:
- ✓ Others:

Information obtained through Google

- Advisories and server vulnerabilities:
- Error messages that contain sensitive information:
- Files containing passwords:
- Pages containing network or vulnerability data:
- ✓ Others:

Information obtained through competitive intelligence

- Financial details:
- Project plans:
- ✓ Others:



Pen Testing Report

Information obtained through WHOIS footprinting

- Domain name details:
- Contact details of domain owner:
- Domain name servers:
- Netrange:
- When a domain has been created:
- ✓ Others:

Information obtained through DNS footprinting

- Location of DNS servers:
- Type of servers:
- ✓ Others:

Information obtained through network footprinting

- Range of IP addresses:
- Subnet mask used by the target organization:
- OS's in use:
- Firewall locations:
- ✓ Others:

Information obtained through social engineering

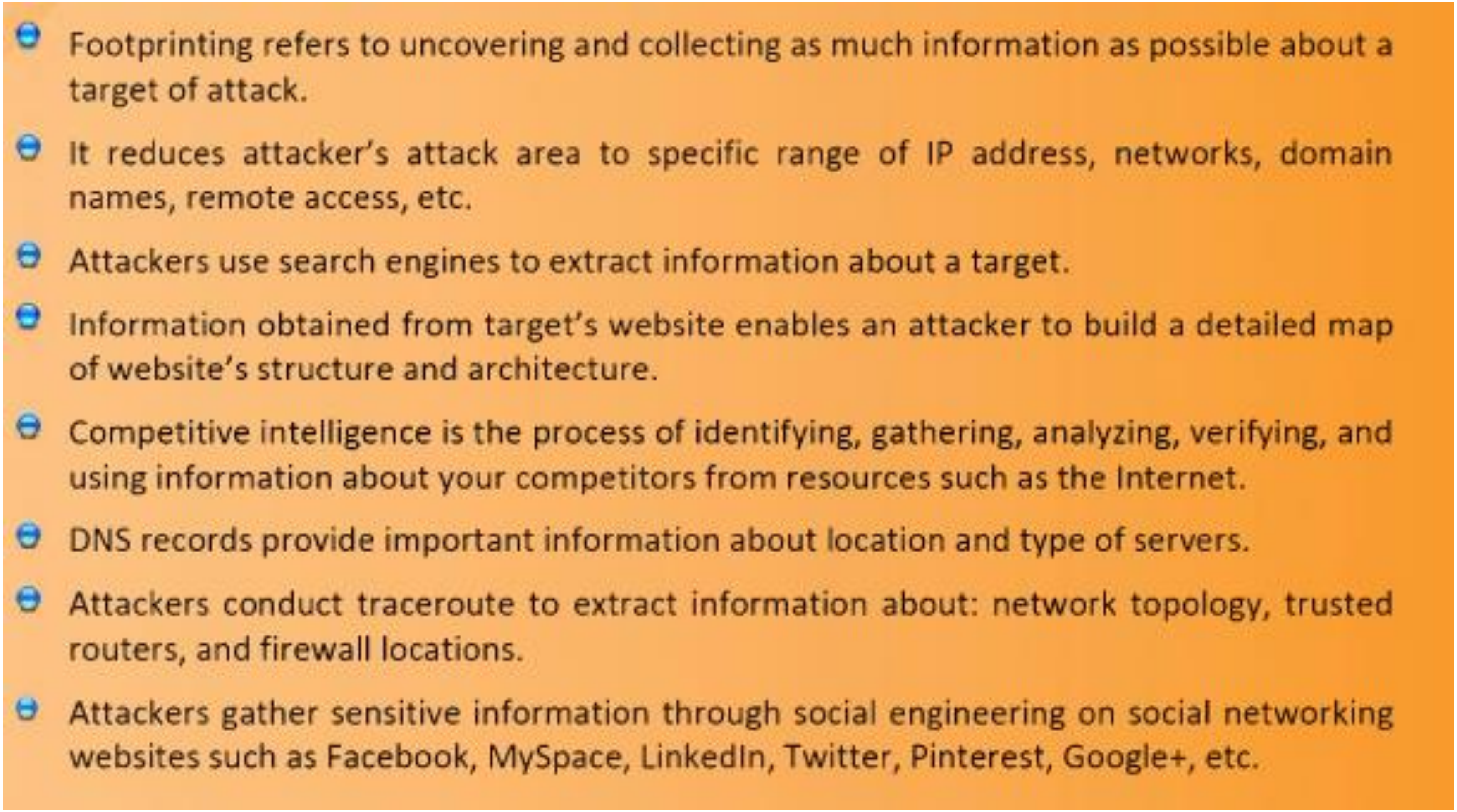
- Personal information:
- Financial information:
- Operating environment:
- Usernames and passwords:
- Network layout information:
- IP addresses and names of servers:
- ✓ Others:

Information obtained through social networking sites

- Personal profiles:
- Work related information:
- News and potential partners of the target company:
- Educational and employment backgrounds:
- ✓ Others:

SUMMARY

Summary



- Footprinting refers to uncovering and collecting as much information as possible about a target of attack.
- It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- Attackers use search engines to extract information about a target.
- Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture.
- Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet.
- DNS records provide important information about location and type of servers.
- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations.
- Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.