

Đánh giá & Kiểm định an toàn hệ thống thông tin

Module 2. Open-Source Intelligence
(OSINT) Methodology

1

Tổng quan

2

Phương pháp luận

3

Công cụ

1

Tổng quan

2

Phương pháp luận

3

Công cụ

OSINT

- ❑ **OSINT** – Việc thu thập dữ liệu hoặc thông tin cá nhân/ tổ chức từ các nguồn mở trên mạng internet
- ❑ **Footprinting** (In dấu ấn) là quá trình thu thập thông tin về đối tượng, tổ chức nhằm:
 - Xác định thông tin về kiến trúc bảo mật, hạ tầng mạng
 - Giảm thiểu bề mặt tấn công
 - Xác định lỗ hổng bảo mật
 - Footprinting pentesting được sử dụng để tìm kiếm các thông tin của công ty tổ chức

Footprinting pentesting

❑ **Footprinting pentesting** – quá trình thu thập thông tin nhiều nhất có thể về cơ quan/ tổ chức từ các nguồn tài nguyên công cộng (vd: trên mạng Internet)

Footprinting pentesting giúp cơ quan/ tổ chức:

- Ngăn ngừa rò rỉ thông tin cá nhân, tổ chức
- Ngăn ngừa các nỗ lực tấn công kỹ nghệ xã hội
- Ngăn chặn rò rỉ các thông tin bản ghi DNS

Footprinting

❑ Các thông tin thu thập:

- Thông tin về cá nhân, tổ chức (thông tin cá nhân, số điện thoại, địa chỉ,...)
- Thông tin về hệ thống mạng (Domain, subdomain, địa chỉ IP,...)
- Thông tin về hệ thống (OS, username, password...)

❑ Phân loại:

- ***Passive Footprinting***: Không tương tác trực tiếp với đối tượng trong quá trình thu thập thông tin
- ***Active Footprinting***: Có sự tương tác trực tiếp

1

Tổng quan

2

Phương pháp luận

3

Công cụ

Footprinting techniques

- Search engines
- Web services
- Social networking sites
- Website, Email, DNS, Whois footprinting
- Social engineering
- Competitive intelligence
- ...

Search Engines

- ❑ Pentester có thể sử dụng search engines để tìm kiếm thông tin như công nghệ được sử dụng, thông tin cá nhân, trang đăng nhập...
- ❑ Một số search engines phổ biến: Google, Bing, Yahoo, Ask.com, AOL.com, Baidu, DuckDuckGo...

The Google logo, featuring the word "Google" in its characteristic multi-colored font.The Yahoo! logo, featuring the word "YAHOO!" in a purple, stylized font.The Baidu logo, featuring the word "Baidu" in red and blue, with a blue paw print icon and the Chinese characters "百度" to the right.

Advanced Google Hacking Search

❑ Sử dụng "Google dork" để tăng hiệu quả tìm kiếm thông tin:

❑ [**cache:**] - Google sẽ trả lại kết quả của trang web được google lưu lại trước đó.

cache:hocvienact.edu.vn

❑ [**link:**] - liệt kê những trang web mà có các liên kết đến đến những trang web chỉ định.

link:hocvienact.edu.vn

❑ [**related:**] - liệt kê các trang Web "tương tự" với trang Web chỉ định.

related:hocvienact.edu.vn

Advanced Google Hacking Search

- ❑ [**site:**] - giới hạn Google chỉ truy vấn những từ khóa xác định trong một site hoặc tên miền riêng biệt.

ceh site:www.hocvienact.edu.vn

- ❑ [**intitle:**] - tìm kiếm những trang có chứa từ khóa trong tiêu đề.

intitle:admin

- ❑ [**allintitle:**] - Tìm kiếm nhiều hơn 1 từ khóa trong tiêu đề.

intitle:admin intitle:login

allintitle:admin login

Advanced Google Hacking Search

- ❑ [**intext:**] - Tìm kiếm từ khóa có trong phần nội dung của trang web và bỏ qua phần URL hoặc tiêu đề của trang web.

intext:exploitation

- ❑ [**inurl:**]- Google tập trung tìm kiếm từ khóa có trong URL của trang web.

inurl:admin

- ❑ [**allinurl:**] - Tương tự cú pháp [**intitle:**]

allinurl: admin php

- ❑ [**filetype:**] - Chỉ tìm kiếm những files trên internet có phần mở rộng riêng biệt

filetype:pdf cehv9

Advanced Google Hacking Search

□[" "] – (Dấu ngoặc kép) tìm kiếm chính xác thông tin nằm trong dấu ngoặc kép.

"windows explotation"

□[–] – (Dấu trừ) loại bỏ từ khóa không muốn Google tìm kiếm trong một trang web.

windows –explotation

□[**index of**] - tìm kiếm những website cho phép duyệt theo cây thư mục.

Index of /admin

Index of /password



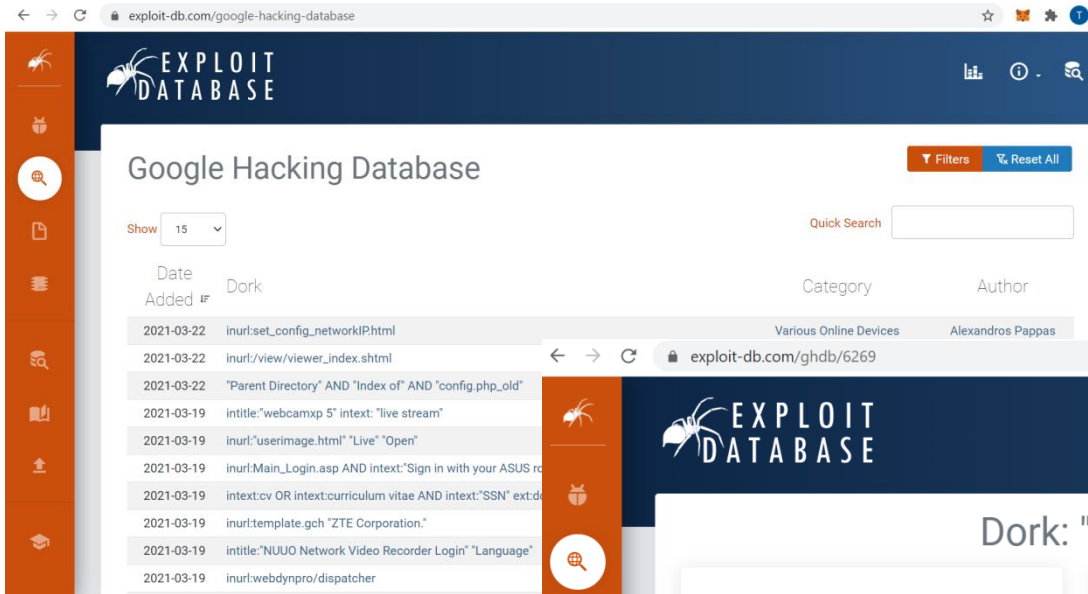
The screenshot shows a web browser window with the address bar displaying 'aspirt.ie/admin/'. Below the address bar, the title is 'Index of /admin'. The main content is a table listing files and directories in the /admin directory. The table has four columns: Name, Last modified, Size, and Description. The files listed include 'Parent Directory', 'assets', 'banner_del.php', 'banner_edit.php', 'banner_in.php', 'banner_pics.php', 'banner_view.php', 'blog.php', 'blog_delete.php', 'blog_edit.php', 'blog_insert.php', 'ce.js', 'change-log-in.php', 'content.php', 'create-gall-del.php', 'create-gall-edit.php', 'create-gall-in.php', 'create_gallery_view.php', 'cus-e.php', 'cus-i.php', 'cus-v.php', and 'cus-d.php'.

Name	Last modified	Size	Description
Parent Directory		-	
assets/	2016-04-12 15:19	-	
banner_del.php	2016-07-29 11:08	8.6K	
banner_edit.php	2016-07-29 11:08	11K	
banner_in.php	2016-07-29 11:08	10K	
banner_pics.php	2016-07-29 11:08	6.3K	
banner_view.php	2016-07-29 11:08	5.0K	
blog.php	2016-07-29 11:28	4.8K	
blog_delete.php	2016-07-29 11:08	13K	
blog_edit.php	2016-07-29 11:08	14K	
blog_insert.php	2016-07-29 11:08	14K	
ce.js	2016-07-29 11:08	450K	
change-log-in.php	2016-07-29 11:08	6.4K	
content.php	2016-07-29 11:08	6.0K	
create-gall-del.php	2016-07-29 11:08	5.8K	
create-gall-edit.php	2016-07-29 11:08	10K	
create-gall-in.php	2016-07-29 11:08	10K	
create_gallery_view.php	2016-07-29 11:08	4.8K	
cus-e.php	2019-01-18 17:38	12K	
cus-i.php	2016-07-29 11:08	11K	
cus-v.php	2016-07-29 11:08	6.1K	
cus-d.php	2016-07-29 11:08	12K	

Advanced Google Hacking Search

❑ Google Dork hacking database

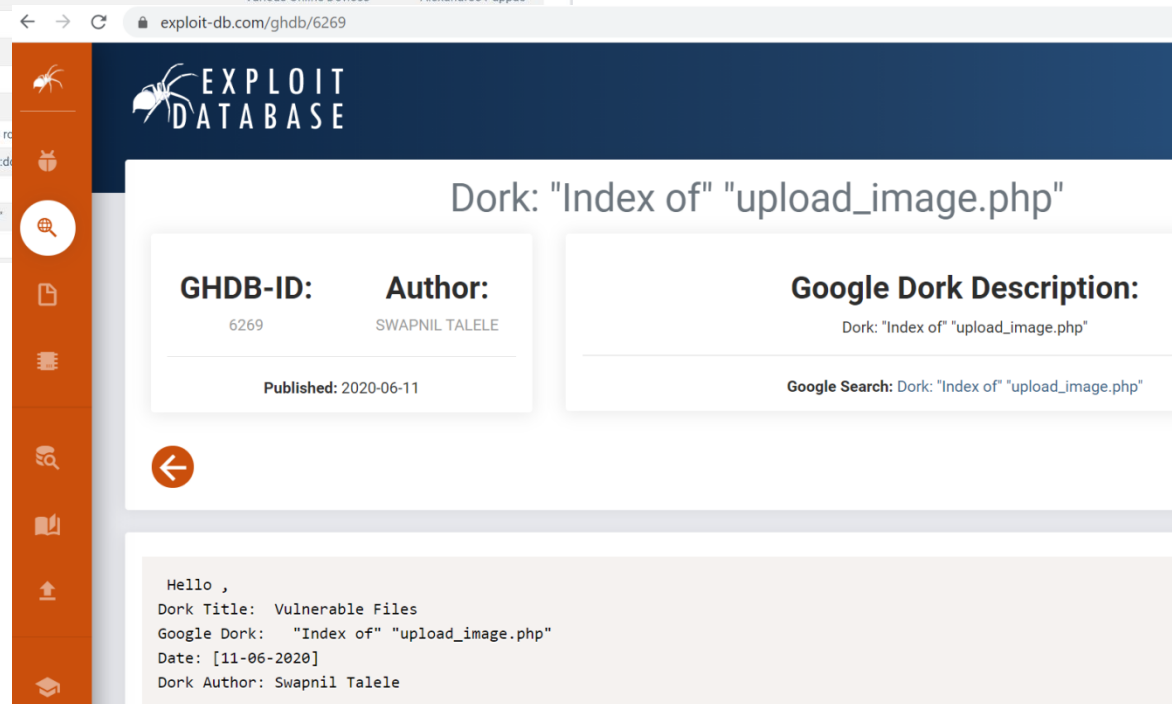
<https://www.exploit-db.com/google-hacking-database>



The screenshot shows the 'Google Hacking Database' page on exploit-db.com. It features a sidebar with navigation icons, a search bar, and a list of search results. The results are sorted by 'Date Added' and include columns for 'Dork', 'Category', and 'Author'. A large orange spider logo is visible in the bottom left corner of the image.

Date Added	Dork	Category	Author
2021-03-22	inurl:set_config_networkIPhtml	Various Online Devices	Alexandros Pappas
2021-03-22	inurl:/view/viewer_index.shtml		
2021-03-22	"Parent Directory" AND "Index of" AND "config.php_old"		
2021-03-19	intitle:"webcamxp 5" intext:"live stream"		
2021-03-19	inurl:"userimage.html" "Live" "Open"		
2021-03-19	inurl:Main_Login.asp AND intext:"Sign in with your ASUS re		
2021-03-19	intext:cv OR intext:curriculum vitae AND intext:"SSN" ext:d		
2021-03-19	inurl:template.gch "ZTE Corporation"		
2021-03-19	intitle:"NUUO Network Video Recorder Login" "Language"		
2021-03-19	inurl:webdynpro/dispatcher		

GOOGLE
HACKING-DATABASE



The screenshot shows the detailed view of a Google Hacking Database (GHDB) entry. The entry is titled 'Dork: "Index of" "upload_image.php"'. It includes the GHDB-ID (6269), the Author (SWAPNIL TALELE), and the Published date (2020-06-11). The Google Dork Description is 'Dork: "Index of" "upload_image.php"'. The Google Search result is 'Dork: "Index of" "upload_image.php"'. The entry content is 'Hello ,
Dork Title: Vulnerable Files
Google Dork: "Index of" "upload_image.php"
Date: [11-06-2020]
Dork Author: Swapnil Talele'.

Dork: "Index of" "upload_image.php"

GHDB-ID: 6269 **Author:** SWAPNIL TALELE

Published: 2020-06-11

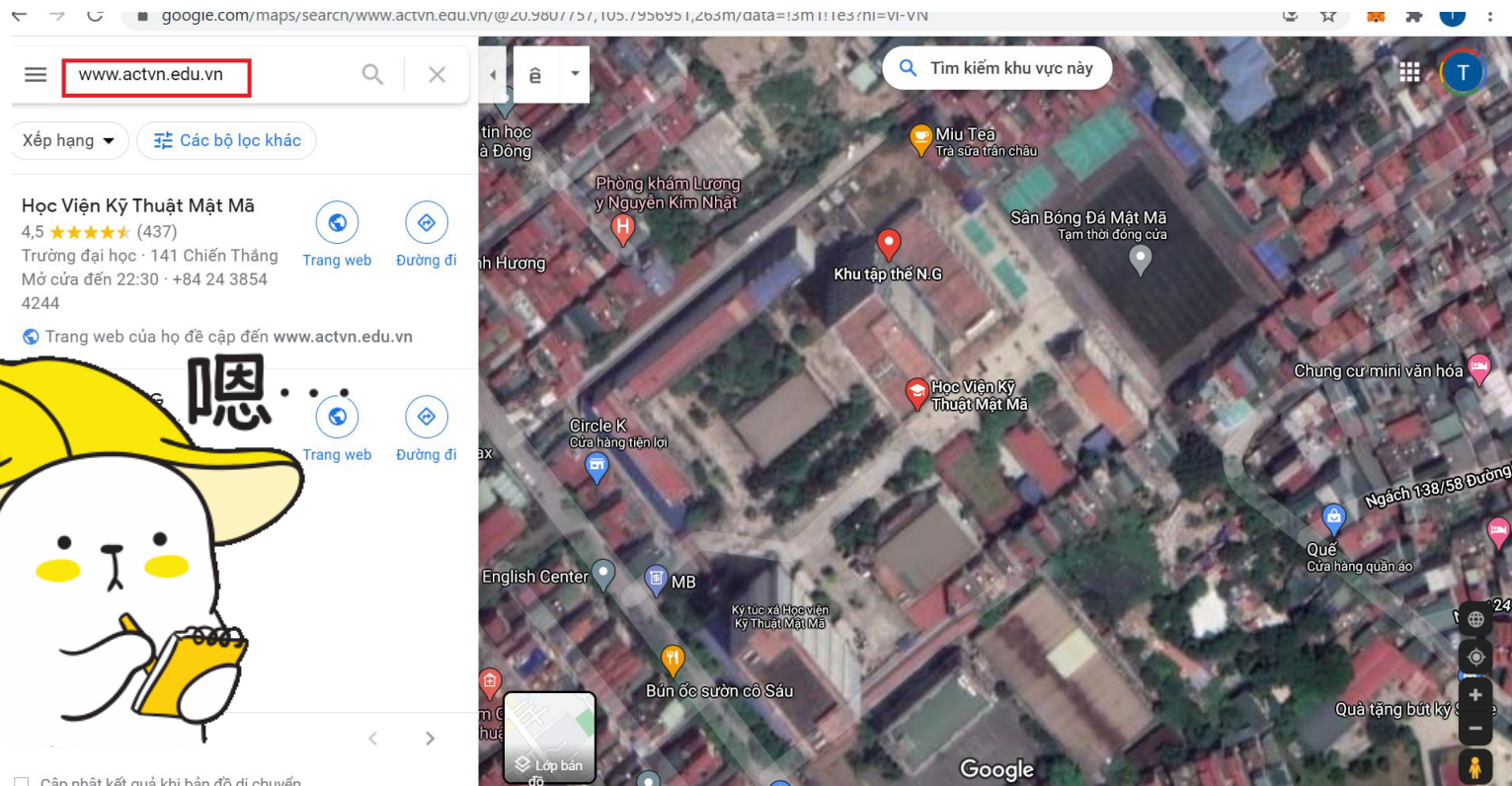
Google Dork Description:
Dork: "Index of" "upload_image.php"

Google Search: Dork: "Index of" "upload_image.php"

Hello ,
Dork Title: Vulnerable Files
Google Dork: "Index of" "upload_image.php"
Date: [11-06-2020]
Dork Author: Swapnil Talele

Tìm kiếm vị trí địa lý của tổ chức

- ❑ Sử dụng Google Maps hoặc Google Earth để tìm kiếm vị trí của cơ quan/tổ chức
- ❑ Tìm hiểu tình trạng giao thông quanh cơ quan/tổ chức
- ❑ Ngoài ra có thể sử dụng các dịch vụ khác như:
 - ❑ <http://www.wikimapia.org>
 - ❑ <https://www.mapquest.com>
 - ❑ <https://www.waze.com/en-GB/livemap>
 - ❑ <https://www.bing.com/maps>



Shodan

- ❑ Shodan tìm kiếm thông tin về OS, port, services, banners... của các thiết bị như Servers, Routers, Switches... sau đó index vào Database của SHODAN chứ không phục vụ cho mục đích search nội dung của website
- ❑ <https://www.shodan.io>
- ❑ Các từ khóa:
 - ❑ **title**: Tìm kiếm theo tiêu đề.
 - ❑ **country**: tìm kiếm theo quốc gia.
 - ❑ **city**: tìm kiếm theo thành phố.
 - ❑ **net**: tìm kiếm theo địa chỉ IP hoặc dãy IP.
 - ❑ **hostname**: tìm kiếm theo tên máy.
 - ❑ **org**: tìm kiếm theo tổ chức.
 - ❑ **port**: tìm kiếm theo port.
 - ❑ **os**: tìm kiếm theo hệ điều hành.

Shodan

- ❑ Tìm các webserver chạy Apache ở Việt Nam:
apache 2.2.3 country:VN
- ❑ Tìm các thiết bị cisco banner là 200 ở CN:
cisco 200 OK country:CN
- ❑ Tìm các Webcam có banner là 200 ở VN:
Webcam 200 country:VN

Shodan search results for query: `apache 2.2.3 country:VN`. The interface shows 273 total results. A red box highlights the search bar and the 'TOTAL RESULTS' count. Another red box highlights the 'TOP CITIES' table, and a third red box highlights the 'TOP SERVICES' table.

TOP CITIES	Count
Hanoi	119
Ho Chi Minh City	80
Hoi An	7
Haiphong	5
Tuy Hoa	5

TOP SERVICES	Count
HTTP	136
HTTPS	84
HTTP (8080)	16
Qconm	6
8081	5

SSL Certificate details for `student.mail.vnu.edu.vn`:

- Issued By: student.mail.vnu.edu.vn
- Issued To: student.mail.vnu.edu.vn
- Supported SSL Versions: SSLv3, TLSv1
- Diffie-Hellman Parameters: mod_ssl, 2.2.x:Hardcoded 1024-bit prime

HTTP/1.1 200 OK
Date: Wed, 24 Mar 2021 18:25:10 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Set-Cookie: SQMSESSID=j3ugkp36spr94j1kgaJ17fBr90; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no...

Shodan search results for query: `port:3389 country:VN`. The interface shows 34,618 total results. A red box highlights the search bar and the 'TOTAL RESULTS' count. Another red box highlights the 'TOP CITIES' table, and a third red box highlights the 'TOP ORGANIZATIONS' table.

TOP CITIES	Count
Ho Chi Minh City	15,112
Hanoi	8,176
Da Nang	966
Vung Tau	549
Haiphong	276

TOP ORGANIZATIONS	Count
Viettel Group	4,706
Vietnam Posts and Telecom...	4,079
PPT Telecom Company	2,486
Vietnam Posts And Telecom...	1,702
VNPT	1,368

103.90.220.148
VNNETWORK Joint Stock Company
Added on 2021-03-25 03:39:29 GMT
Viet Nam, Ho Chi Minh City

self-signed

Administrator
phu.sienhu.ung

OSINT through Website analysis

❑ Thu thập thông tin về người dùng nhiều nhất có thể từ internet, website tổ chức, mạng xã hội (facebook, instagram, linkedin, twitter...), SE...

- Ví dụ jane có email công ty là jane@xcompany.com thì có thể jane có sử dụng các mail khác jane@yahoo.com, jane@gmail.com ...



```
root@packt:~# theharvester -d prakharprasad.com -b google
5.0.6_103037
*****
*                                     *
*  THE HARVESTER  *
*                                     *
* TheHarvester Ver. 2.6 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*****

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...

[+] Emails found:
-----
prakhar@prakharprasad.com

[+] Hosts found in search engines:
-----

[-] Resolving hostnames IPs...
104.25.230.16:www.prakharprasad.com
104.25.231.16:blog.prakharprasad.com
104.25.230.16:Blog.prakharprasad.com
104.25.231.16:sandbox.prakharprasad.com
```

OSINT through Website analysis

❑ Sử dụng <https://archive.org/> để tìm kiếm các thông tin được lưu trữ về website tổ chức.

web.archive.org/web/*/actvn.edu.vn

Calendar · Collections · Changes · Summary · Site Map

Saved 282 times between April 5, 2009 and March 16, 2021.

1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021

web.archive.org/web/20170603205820/http://actvn.edu.vn/

http://actvn.edu.vn/

282 captures
5 Apr 2009 - 16 Mar 2021

Go APR JUN JUL
2016 2017 2018

TRANG CHỦ GIỚI THIỆU ĐÀO TẠO KHOA HỌC CÔNG NGHỆ SINH VIÊN HỢP TÁC QUỐC TẾ LIÊN HỆ English

DÀNH CHO NGƯỜI HỌC

THÔNG TIN TUYỂN SINH

TUYỂN SINH SAU ĐẠI HỌC

THƯ VIỆN SỐ THƯ VIỆN ĐIỆN TỬ

DIỄN ĐÀN

CÁC KHOA

TIN TỨC & SỰ KIỆN

Học viện Kỹ thuật mật mã tham gia Ngày hội Tư vấn tuyển sinh - hướng nghiệp 2017
Ngày hội Tư vấn tuyển sinh - hướng nghiệp 2017 diễn ra tại Trường ĐH Bách Khoa TP.HCM ngày 15/1/2017 và tại Trường ĐH Bách khoa Hà Nội vào ngày 26/02/2017. Chương trình do Bộ GD-ĐT kết hợp với báo Tuổi Trẻ tổ chức

Lễ khánh thành và khai trương phòng Samsung Lab - ACT
Sáng ngày 14/12/2016, tại Học viện Kỹ thuật mật mã đã diễn ra Lễ ký kết bàn giao và Khai trương phòng thí nghiệm Samsung Lab - ACT do công ty Samsung Electronic Việt Nam (SVMC) tài trợ

Nguồn nhân lực quyết định an ninh thông tin thời đại mới
Hội thảo khoa học về An toàn, an ninh thông tin lần thứ nhất (SoIS 2016) do Bộ Thông tin & Truyền thông (TT&TT) phối hợp cùng Học viện Kỹ thuật mật mã tổ chức

THÔNG BÁO MỚI

- THÔNG BÁO: Về việc xác nhận thông tin cá nhân của các khóa AT10, AT11, AT12, AT13, CT1
- THÔNG BÁO: V/v tuyển chọn và đào tạo đội tuyển sinh viên tham dự cuộc thi "Sinh viên với an toàn thông tin năm 2017"
- THÔNG BÁO: V/v Báo cáo thực tập tốt nghiệp sinh viên AT9
- THÔNG BÁO: Về việc đóng học phí còn nợ đọng của sinh viên
- THÔNG BÁO: V/v triển khai mở lớp luyện thi TOEIC và cấp chứng chỉ Tiếng Anh cho học viên H23 và sinh viên AT10 theo chuẩn Tiếng Anh đầu ra
- THÔNG BÁO: V/v triển khai mở lớp học Bổ sung Tiếng Anh 6 tin chỉ cho sinh viên Hệ đào tạo đại học chuyên ngành AT&CT

Website Footprinting

- ❑ Website footprinting – thu thập và phân tích các thông tin về website của cá nhân/ tổ chức.
- ❑ Các thông tin có thể thu thập bao gồm:
 - Ứng dụng và phiên bản web được sử dụng
 - Hệ điều hành máy chủ web
 - Sub-directories/parameters
 - Filename, path, database
 - Thông tin (số điện thoại, email, địa chỉ) của người dùng
 - Địa chỉ IP, DNS record...

⇒ **Nội dung cụ thể:**

**Module 8. Web Application
Pentesting Methodology**



Website Footprinting

- ❑ Kiểm tra mã nguồn HTML, cookie
 - Tìm kiếm các thông tin như back-end technologies, external links, filesystem structure, scripts, comment...

```
bash-4.2$ cat page.php
cat page.php
<!doctype html>
<?php
session_start();
if (!isset ($_SESSION['username'])) header('Location: /');

$username1 = $_SESSION['username'];

$strErrorMsg="";
$cmdOutput=array();

$username = 'ldapuser';
$password = 'e398e27d5c4ad45086fe431120932a01';
```

```
$basedn = 'dc=ctf,dc=htb';
$usersdn =
```

```
// This co
<body>
    <h1> WARNING: <br> A BOMB IS GOING TO GO OFF <br> IN THIS HOUSEH
    <h2> ONLY YOU <br>CAN SAVE <br>US. </h2>
    <h3><a href="defuse.php"> CLICK HERE <br>TO DEFUSE<BR> THE BOMB.
</body>
</html>
```

Email Footprinting

- ❑ Thực hiện tìm kiếm các thông tin về máy chủ mail, địa chỉ ip máy chủ mail, địa chỉ email của các cá nhân trong cơ quan/ tổ chức, vị trí...

The address from which the message was sent

Sender's IP address

Sender's mail server

Date and time received by the originator's email servers

Authentication system used by sender's mail server

Date and time of message sent

Sender's full name

The Whois query

The Whois servers

The physical location for our target

Email Addresses

Telephone Numbers

Name Servers

```
Delivered-To: <[redacted]@gmail.com>
Received: by 10.112.39.167 with SMTP id q7c
Fri, 1 Jun 2012 21:24:01 -0700 (PDT)
Return-Path: <[redacted]@gmail.com>
Received-SPF: pass (google.com: domain of [redacted]
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf=
10.224.205.137 as permitted sender) smtp.mail=
header.id=[redacted]@gmail.com
Received: from mr.google.com ([10.224.205.137])
by 10.224.205.137 with SMTP id fq9mr8578570qab.39.13
Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:in-reply-to:refer
:content-type;
bh=TGEIPb4ti17gfQG+ghh7OkPjKx+Tt/iACl
b=Egu2LTLfg2+QZXzZKex1NnvRcnD/+P4Nk
b1PK3eJ3Uf/CsaBZNDIT0XLaK0A0.F0b0tS2McZTawUQ6uWd/AMALsukeUIEEeKGqOC
oa9hD59D3oXI8KAC7ZmkblGzXmV4D1WfCL894RaMBOUoMzRwOWNIib95a1I38cqt1FP
ZhrWFKh5xSnZx0E73xZPEYzp7yeeCeQuYHENGaiKxc07xQjeZuw+HWK/vR6xChDjapZ4
E52AFyZmkIkFX+VdLZqu7YGFzy6oHcuF16yS/C2fXHVdsuYamMT/yecvvhCv08Og7FKt6
/Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9mr8704ER6ash.72.1370611040318;
Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Fri, 1
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4ber2M
References: <CAOYWATT1zdDXE3o8D2rhiE4ber2M
Date: Sat, 2 Jun 2012 09:53:59 +0530
Message-ID: <CAM5V0XUQjnrwswdsqnnh0-EMJcgfgX+mUfjB_tt2ay2dXA@mail.gmail.co
Subject: [redacted] SOLUTIONS [redacted]
From: [redacted] Mirza <[redacted]@gmail.com>
To: [redacted]@gmail.com,
[redacted] <[redacted]@networksolutions.com>
```

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>whois cisco.com

Whois v1.01 - Domain information lookup utility
Sysinternals - www.sysinternals.com
Copyright (C) 2005 Mark Russinovich

Connecting to COM.whois-servers.net...
Connecting to whois.networksolutions.com...

Cisco Technology, Inc.
170 W. Tasman Drive
San Jose, CA 95134
US

Domain Name: CISCO.COM

Promote your business to millions of viewers for only $1 a month
Learn how you can get an Enhanced Business Listing here for your domain name.
Learn more at http://www.NetworkSolutions.com/

Administrative Contact:
InfoSec infosec@CISCO.COM
170 West Tasman Drive
San Jose, CA 95134
408-527-3842 fax: 408-526-4575

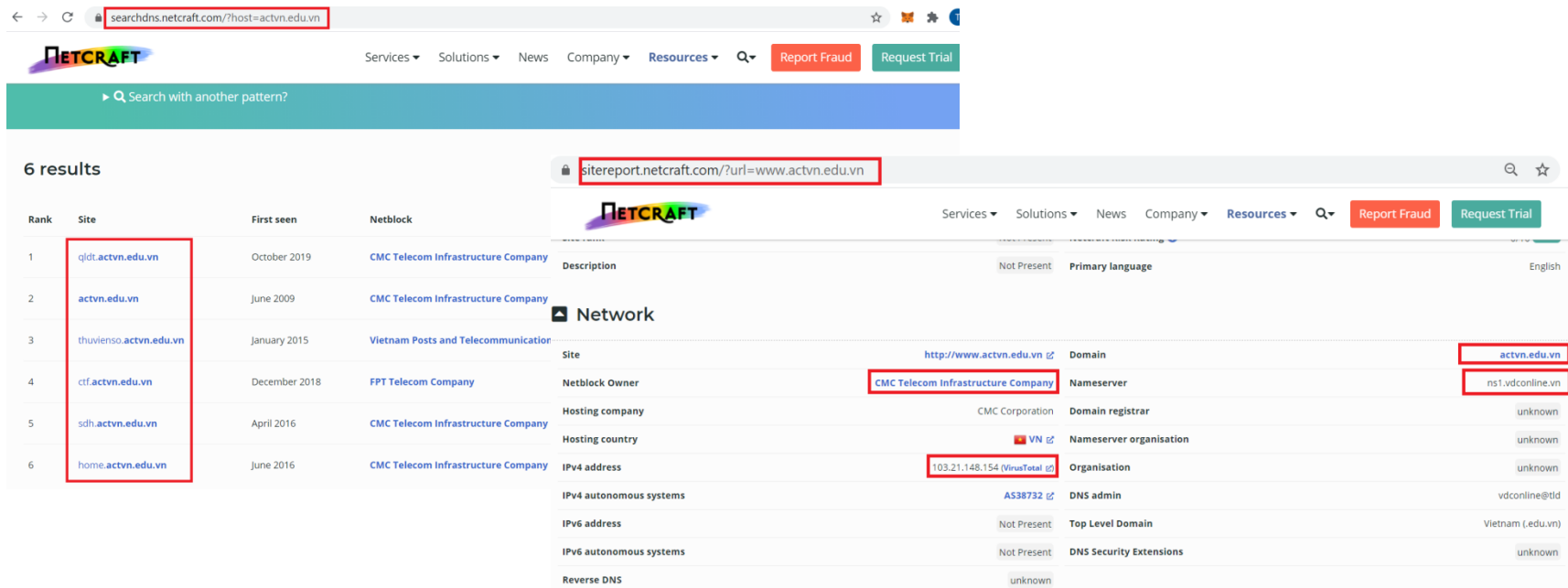
Technical Contact:
Network Services
170 W. Tasman Drive
San Jose, CA 95134
408-527-9223 fax: 408-526-7373

Record expires on 15-May-2009.
Record created on 14-May-1987.
Database last updated on 10-Jan-2008 02:19:40 EST.

Domain servers in listed order:
NS1.CISCO.COM 128.107.241.185
NS2.CISCO.COM 64.102.255.44
```


Tìm kiếm Domain & Subdomain

- ❑ Sử dụng các công cụ như Google, Bing... để tìm kiếm thông tin về URL
- ❑ Tìm kiếm các thông tin về Domain, Subdomain của tổ chức
- ❑ Công cụ: Netcraft, Sublist3r, dnsmap, whois nmap script...



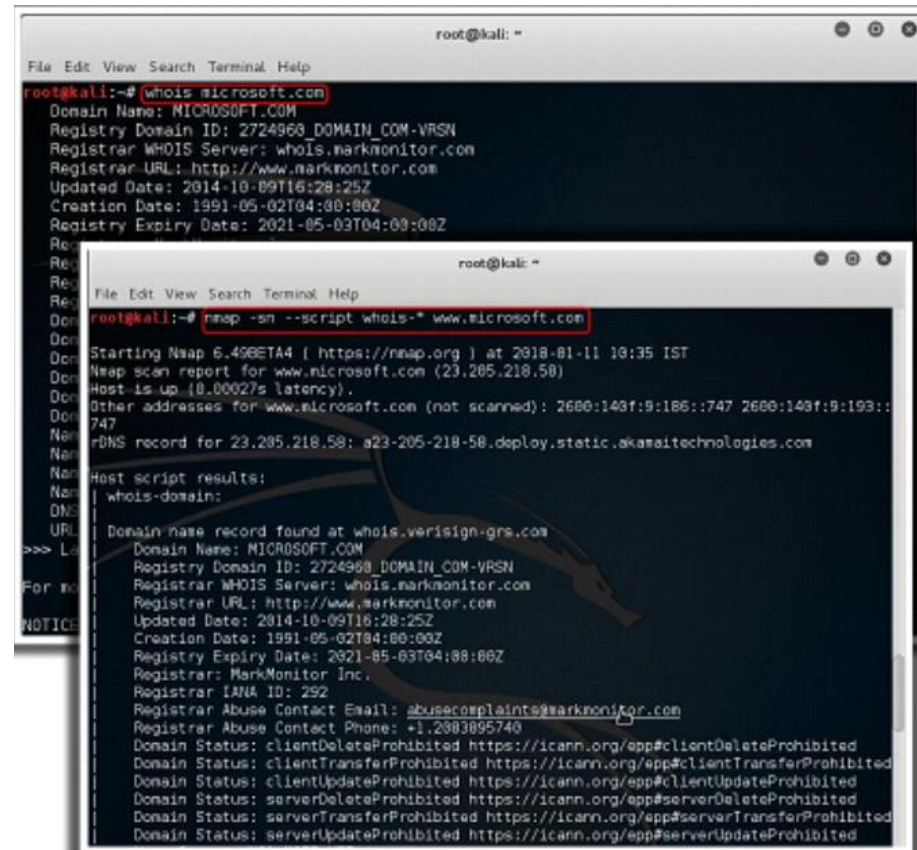
The screenshot shows the Netcraft website interface. The top navigation bar includes links for Services, Solutions, News, Company, Resources, and buttons for Report Fraud and Request Trial. A search bar at the top left contains the URL `searchdns.netcraft.com/?host=actvn.edu.vn`. Below the search bar, a table displays 6 results for the domain `actvn.edu.vn`. The table columns are Rank, Site, First seen, and Netblock. The results list various subdomains like `qjdt.actvn.edu.vn`, `actvn.edu.vn`, `thuvienso.actvn.edu.vn`, `ctf.actvn.edu.vn`, `sdh.actvn.edu.vn`, and `home.actvn.edu.vn`, all associated with CMC Telecom Infrastructure Company.

Rank	Site	First seen	Netblock
1	<code>qjdt.actvn.edu.vn</code>	October 2019	CMC Telecom Infrastructure Company
2	<code>actvn.edu.vn</code>	June 2009	CMC Telecom Infrastructure Company
3	<code>thuvienso.actvn.edu.vn</code>	January 2015	Vietnam Posts and Telecommunication
4	<code>ctf.actvn.edu.vn</code>	December 2018	FPT Telecom Company
5	<code>sdh.actvn.edu.vn</code>	April 2016	CMC Telecom Infrastructure Company
6	<code>home.actvn.edu.vn</code>	June 2016	CMC Telecom Infrastructure Company

Below the table, a detailed report for `actvn.edu.vn` is shown. The report includes a Network section with details such as Site (`http://www.actvn.edu.vn`), Domain (`actvn.edu.vn`), Nameserver (`ns1.vdconline.vn`), and IP address (`103.21.148.154`).

Tìm kiếm Domain & Subdomain

- ❑ Cơ sở dữ liệu Whois chứa các thông tin cá nhân về chủ sở hữu domain như
 - Thông tin chi tiết Domain name
 - Contact Domain owner
 - Domain name servers
 - IP address & NetRange
 - Ngày đăng ký & hết hạn
 - Vị trí vật lý
 - Phone number & email
 -



The image shows two overlapping terminal windows from a Kali Linux system. The top window displays the output of the `whois microsoft.com` command, showing domain registration details for MICROSOFT.COM. The bottom window displays the output of the `nmap -sn --script whois-* www.microsoft.com` command, showing a host script result for the domain.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# whois microsoft.com  
Domain Name: MICROSOFT.COM  
Registry Domain ID: 2724968_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2014-10-09T16:28:25Z  
Creation Date: 1991-05-02T04:00:00Z  
Registry Expiry Date: 2021-05-03T04:00:00Z  
Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
Registrar Abuse Contact Phone: +1.2083855740  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited  
NOTICE: For more information on this domain status, please go to the ICANN website at https://www.icann.org/epp  
root@kali:~# nmap -sn --script whois-* www.microsoft.com  
Starting Nmap 6.40BETA4 ( https://nmap.org ) at 2018-01-11 10:35 IST  
Nmap scan report for www.microsoft.com (23.205.218.50)  
Host is up (0.0002s latency).  
Other addresses for www.microsoft.com (not scanned): 2680:143f:9:185::747 2680:143f:9:193::747  
rDNS record for 23.205.218.50: a23-205-218-50.deploy.static.akamaitechnologies.com  
Host script results:  
| whois-domain:  
| Domain name record found at whois.verisign-grs.com  
| Domain Name: MICROSOFT.COM  
| Registry Domain ID: 2724968_DOMAIN_COM-VRSN  
| Registrar WHOIS Server: whois.markmonitor.com  
| Registrar URL: http://www.markmonitor.com  
| Updated Date: 2014-10-09T16:28:25Z  
| Creation Date: 1991-05-02T04:00:00Z  
| Registry Expiry Date: 2021-05-03T04:00:00Z  
| Registrar: MarkMonitor Inc.  
| Registrar IANA ID: 292  
| Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
| Registrar Abuse Contact Phone: +1.2083855740  
| Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
| Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
| Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
| Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
| Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
| Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
```


1

Tổng quan

2

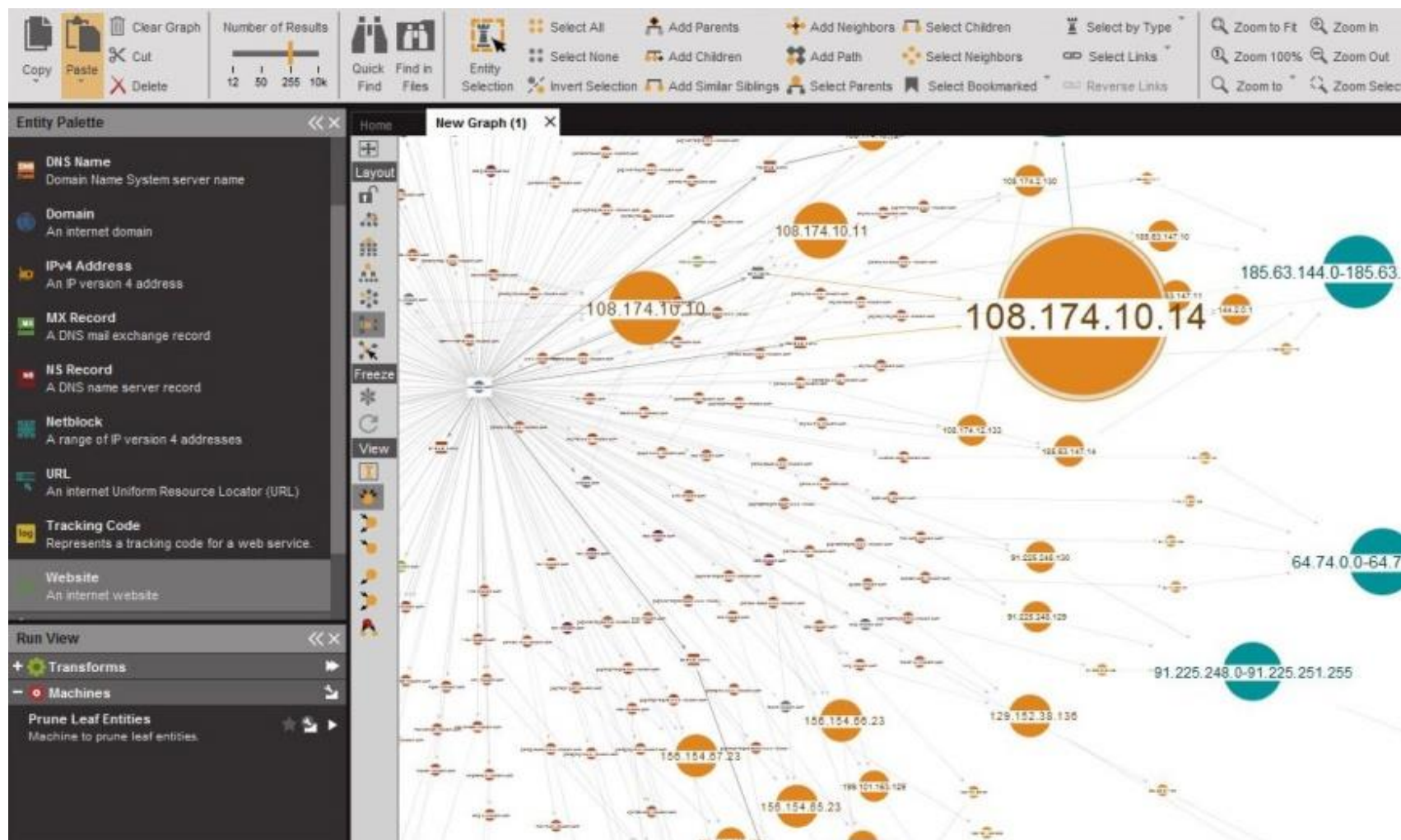
Phương pháp luận

3

Công cụ

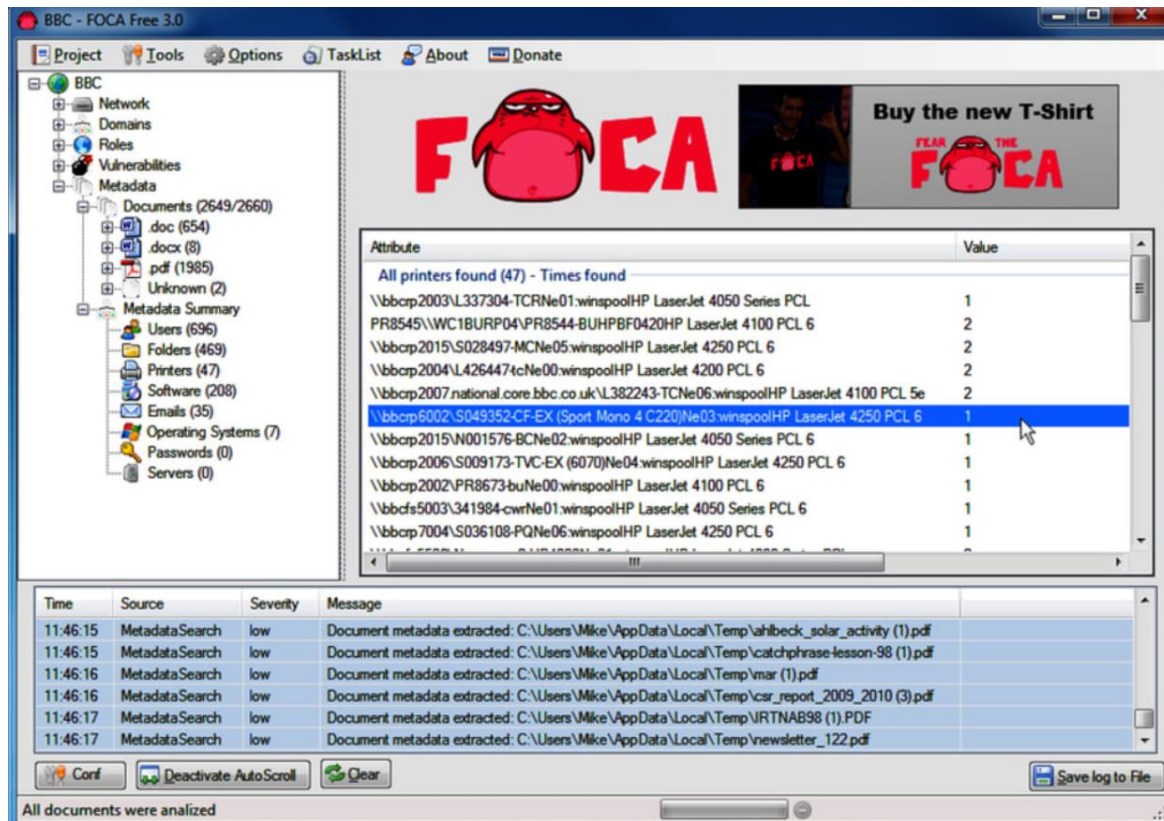
Maltego

❑ Sử dụng **Maltego** để xây dựng mối quan hệ thực tế giữa người, nhóm người, công ty, tổ chức, website, tài liệu...



FOCA

- ❑ Sử dụng **FOCA** để thu thập metadata và các thông tin ẩn trong tệp tin, tài liệu mà nó scan
- ❑ FOCA cho phép thực hiện các kỹ thuật phân tích như metadata extraction, network analysis, DNS snooping, proxies search, fingerprinting...



Fsociety

- ❑ Fsociety – pentesting framework chứa rất nhiều các công cụ thường được sử dụng để pentest

```
File Edit View Search Terminal Help
d88888b .d8888. .d88b. .o88b. d888888b d88888b d888888b db db
88' 88' YP .8P Y8. d8P Y8 `88' 88 88 `8b d8'
88ooo `8bo. 88 88 8P 88 88oooo 88 `8bd8'
88 `Y8b. 88 88 8b 88 88 88 88
88 db 8D `8b d8' Y8b d8 .88. 88. 88 88
YP `8888Y' `Y88P' `Y88P' Y888888P Y888888P YP YP

}-----{+} Coded By Manisso {+}-----{
}-----{+} GitHub.com/Manisso/fsociety {+}-----{

{1}--Information Gathering
{2}--Password Attacks
{3}--Wireless Testing
{4}--Exploitation Tools
{5}--Sniffing & Spoofing
{6}--Web Hacking
{7}--Private Web Hacking
{8}--Post Exploitation
{0}--INSTALL & UPDATE
{11}-CONTRIBUTORS
{99}-EXIT

fsociety ~# 1
```

```
88 88b 88 888888 dP"Yb
88 88Yb88 88 dP Yb
88 88 Y88 88"" Yb dP
88 88 Y8 88 YbodP

{1}--Nmap - Network Mapper
{2}--Setoolkit
{3}--Host To IP
{4}--WPScan
{5}--CMSmap
{6}--XSStrike
{7}--Doork
{8}--Crips

{99}-Back To Main Menu

fsociety ~# 2
```

PENTMENU

- ❑ Fociety – bash scripts, được sử dụng để kiểm thử xâm nhập mạng

```
ddos@DESKTOP-740A66K: ~  
  
PENTMENU  
  
Welcome to pentmenu!  
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues  
This software is only for responsible, authorised use.  
YOU are responsible for your own actions!  
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding  
  
1) Recon  
2) DOS  
3) Extraction  
4) View Readme  
5) Quit  
Pentmenu>2  
1) ICMP Echo Flood      6) TCP XMAS Flood      11) Distraction Scan  
2) ICMP Blacknurse      7) UDP Flood           12) DNS NXDOMAIN Flood  
3) TCP SYN Flood        8) SSL DOS             13) Go back  
4) TCP ACK Flood        9) Slowloris  
5) TCP RST Flood        10) IPsec DOS  
Pentmenu>
```

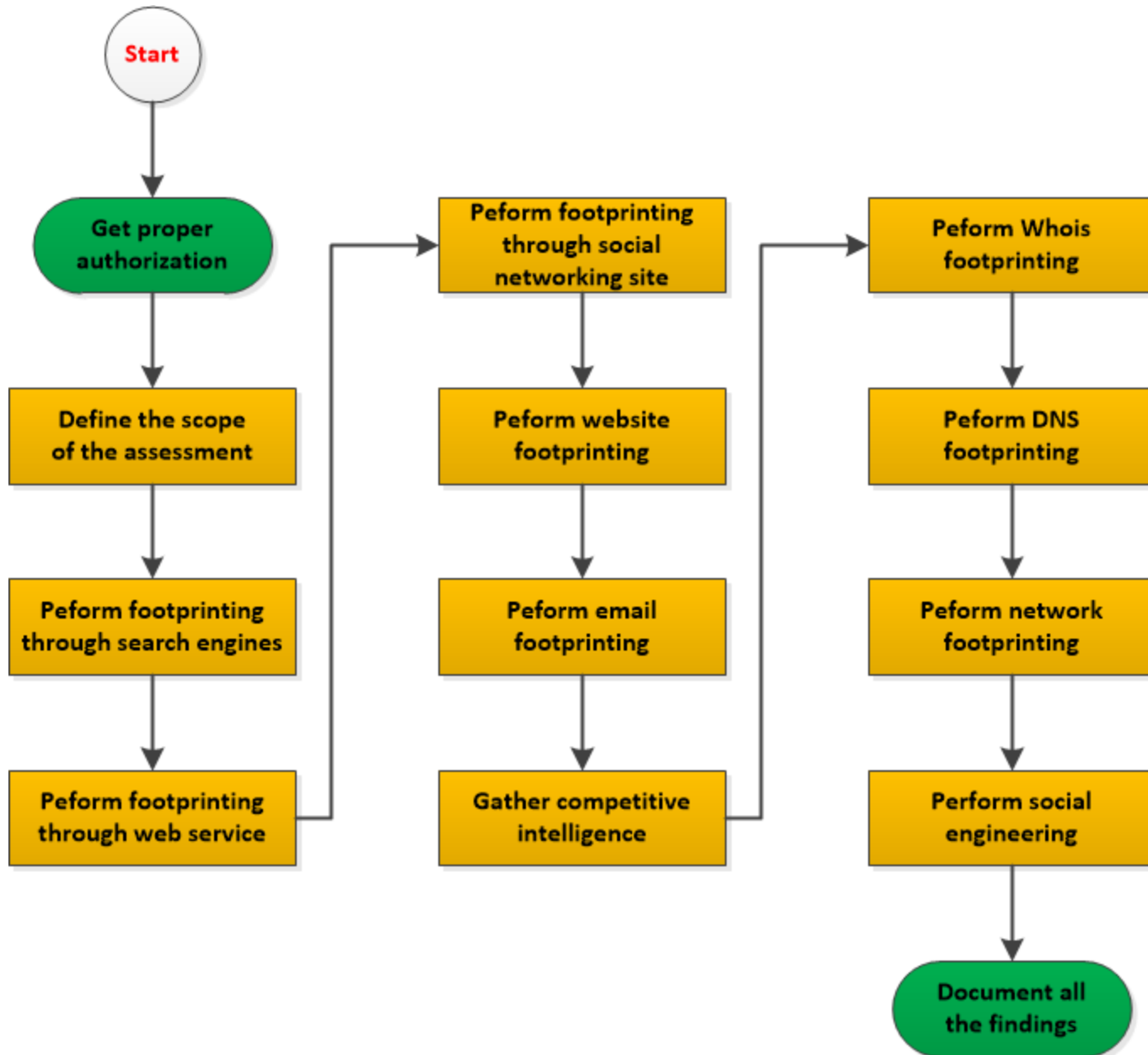
Automating Tools/Frameworks/Scripts

- ❑ Ngoài ra còn có rất nhiều các tools/frameworks/scripts như:
 - OSINT Framework (<https://osintframework.com/>)
 - CheckUserNames (<https://checkusernames.com/>)
 - HaveIbeenPwned (<https://haveibeenpwned.com/About>)
 - BuildWith (<https://builtwith.com/>)
 - Google Dorks / Shodan
 - Nmap
 - Jigsaw (<https://www.jigsawsecurityenterprise.com/>)
 - Recon-ng
 - TheHarvester
 - Metagoofil/exiftool
 - ZoomEye (<https://www.zoomeye.org/>)
 - SpiderFoot
 - ...

Lập báo cáo

- ❑ Lập báo cáo về các thông tin thu được sau quá trình OSINT
- ❑ Pentester có thể tìm được các thông tin quan trọng sau:
 - Domain & sub-domains
 - Vị trí vật lý
 - Thông tin cá nhân trong tổ chức
 - Số điện thoại & địa chỉ liên lạc
 - Sản phẩm/Dịch vụ
 - Thiết bị mạng
 - Cấu trúc website, công nghệ, link liên kết
 - DNS record
 - Public IP

Footprinting Pentesting Steps



Thảo luận

Footprinting
countermeasures?



Thank you & Any questions?

