

Kiểm thử & đánh giá 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

Motivation

- Recon giúp chúng ta đưa ra các quyết định tấn công “thông minh” hơn -> Cần phân bổ thời gian và nguồn lực cho Recon.
 - Thông tin người dùng/tổ chức giúp tăng khả năng SE thành công.
 - Định dạng tài khoản được sử dụng và danh sách người dùng giúp việc dự đoán hiệu quả hơn.
 - Hiểu biết về hardware và software được sử dụng giúp tiết kiệm thời gian và công sức.

```
graph LR; A[Recon] --> B[Footprinting & Scanning]; B --> C[Exploitation]; C --> D[Post-Exploitation]
```

Recon

Footprinting
& Scanning

Exploitation

Post-
Exploitation

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.

.com

Traffic

- Zero touch: Không có bất kỳ tương tác trực tiếp nào với mục tiêu (lý tưởng).
 - Thu thập thông tin từ 3-parties.
- Light touch: Nếu có tương tác trực tiếp với mục tiêu thì nên đảm bảo “traffic” giống như bình thường.
 - Duyệt web mục tiêu.
 - DNS lookups.
- Để việc kiểm thử đảm bảo “stealth” thì hạ tầng dùng để “recon” và “testing” nên được tách biệt.

Targets

- Organization.
 - Goals/Mergers and Acquisitions
 - Projects and Products
 - Recent news
- Infrastructure.
 - IP Addresses/Hostnames/Software & Hardware.
- Employees.
 - Usernames/Email addresses
 - Breached credentials
 - Roles

Information on the Organization

- ❑ Thông tin mức cao về “target”.
- ❑ Tìm kiếm thông tin liên quan đến tiểu sử, lịch sử...của target qua mạng internet.
- ❑ Danh sách domain, các công ty con, việc mua bán, kinh doanh.
- ❑ Sử dụng search engine, xác định các mục tiêu:
 - Công ty chính, dịch vụ và sản phẩm chính.
 - Nhân viên công ty và VIPs.
 - Đối thủ chính.
 - Vị trí vật lý...
- ❑ Các thông tin này có thể sử dụng để phishing.

Infrastructure

- Tìm kiếm thông tin liên quan đến hệ thống, bao gồm cả phần cứng và phần mềm:
 - Thu thập thông tin về địa chỉ IP và subnet.
 - DNS và host names.
 - Cổng và dịch vụ đang lắng nghe.
 - Software và hardware đang sử dụng.

gmail.com

Hostname Information

- Hostname thường phản ánh mục tiêu/nhiệm vụ của thiết bị.
- Tìm kiếm hostnames chứa các nội dung sau:
 - VPN sign-on portals: *vpn, access*.
 - Citrix StoreFront portals: *ctx, citrix, storefront*.
 - Online email: *email, autodiscover, owa*.
 - Hostnames chứa *login, portal, sso, adfs, remote*.

nguyenvan@gmail.com

DNSRecon

- ☐ Có thể tìm kiếm thủ công (vd sử dụng *dig*) hoặc sử dụng công cụ tự động.

- ☐ Multi-threaded DNS recon tool:

<https://github.com/darkoperator/dnsrecon>

- DNS record (default), reverse IP address lookup (rvl), zone transfer (axfr), DNSSEC zone walks (zonewalk), cache snooping (snoop)
- Dictionary-based subdomain brute forcing (brt)
- Output có thể ở định dạng XMP (--xml) hoặc SQLite database formats (--db)

```
dnsrecon -d domain.kma -t type
```

Example: dnsrecon -d [domain] -t axfr

DNSRecon Usage

```
sec560@slingshot:~$ dnsrecon -d sans.org -n 8.8.8.8
[*] Performing General Enumeration of Domain: sans.org
[-] DNSSEC is not configured for sans.org
[*]      SOA ns-1746.awsdns-26.co.uk 205.251.198.210
[*]      NS  ns-1270.awsdns-30.org 205.251.196.246
[*]      NS  ns-1270.awsdns-30.org 2600:9000:5304:f600::1
[*]      NS  ns-1746.awsdns-26.co.uk 205.251.198.210
[*]      NS  ns-1746.awsdns-26.co.uk 2600:9000:5306:d200::1
[*]      NS  ns-282.awsdns-35.com 205.251.193.26
[*]      NS  ns-282.awsdns-35.com 2600:9000:5301:1a00::1
[*]      NS  ns-749.awsdns-29.net 205.251.194.237
[*]      NS  ns-749.awsdns-29.net 2600:9000:5302:ed00::1
[*]      MX  mx-a-002c1802.gslb.pphosted.com 205.220.173.71
[*]      MX  mx-b-002c1802.gslb.pphosted.com 205.220.173.71
[*]      A   sans.org 45.60.31.34
[*]      A   sans.org 45.60.103.34
[*]      TXT sans.org MS=ms15381092
[*]      TXT sans.org
```

DNSDumpster

- Cung cấp thông tin “DNS A record” về tên miền.
 - Free version cung cấp tối 100 A records.
 - Paid version cung cấp “full” list cùng các dịch vụ bổ sung.
- Tìm kiếm Autonomous System Numbers (ASN) cùng với tên của đối tượng là dấu hiệu tốt về các máy chủ và địa chỉ IP bổ sung.
- Tìm tên miền phụ (subdomain), bản ghi MX, bản ghi TXT
- <https://dnsdumpster.com/>

DNSDumpster Usage (1/2)

MX Records ** This is where email for the domain goes...

10 mx^a-002c1802.gslb.phhosted.com.



205.220.161.71

mx0a-002c1802.phhosted.com

10 mx^b-002c1802.gslb.phhosted.com.



205.220.173.71

mx0b-002c1802.phhosted.com

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

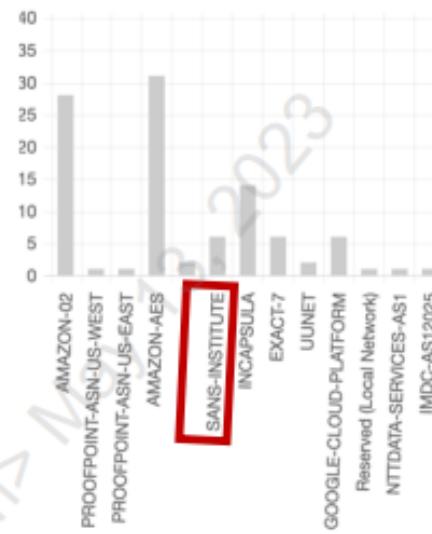
"MS=ms15381092"

"YOfxOkgh96cLKDUD0042Sx/iL9bDXs/ZIJ11T2OczGY4TajTWwW8RXLmRajj6sSrD+sNde1F3pXA0PPmx3cE5Q=="

"_globalsign-domain-verification=XbqPoFvyLnW1HWyrKazU_F9bRAXRI-_SoC2KhQHxT"

"_globalsign-domain-verification=Z0fOVJB0oLvstF1L9BBVBnLszC-egXTqDZTeNuNdCx"

Hosting (IP block owners)



Email filtering by ProofPoint

Block owner containing "SANS" (possible more targets)

DNSDumpster Usage (2/2)

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

Name

mylabs.odin.labs.sans.org	108.139.1.42 server-108-139-1-42.sfo5.r.cloudfront.net	AMAZON-02 United States
gw2-prod-aws.sans.org	34.192.32.13 gw2-prod-aws.sans.org	AMAZON-AES United States
api.odin.devlabs.sans.org	34.207.219.177 ec2-34-207-219-177.compute-1.amazonaws.com	AMAZON-AES United States
phish.sans.org	54.80.160.189 ec2-54-80-160-189.compute-1.amazonaws.com	AMAZON-AES United States
HTTP: Apache		
api.eu-central-1.develop.securityawareness.sans.org	18.66.248.76 server-18-66-248-76.dns51.r.cloudfront.net	AMAZON-02 United States
api.develop.securityawareness.sans.org	13.33.21.86 server-13-33-21-86.lax53.r.cloudfront.net	AMAZON-02 United States
api.eu-central-1.sandbox.securityawareness.sans.org	13.227.74.88 server-13-227-74-88.sfo20.r.cloudfront.net	United States
HTTP: CloudFront		
develop.devhq.sans.org	52.207.107.138 ec2-52-207-107-138.compute-1.amazonaws.com	AMAZON-AES United States
alerts.odin.labs.sans.org	52.91.129.229 ec2-52-91-129-229.compute-1.amazonaws.com	AMAZON-AES United States
lists-ng.sans.org	66.35.60.135 lists-ng.sans.org	SANS-INSTITUTE United States

IP Address

PTR

Header

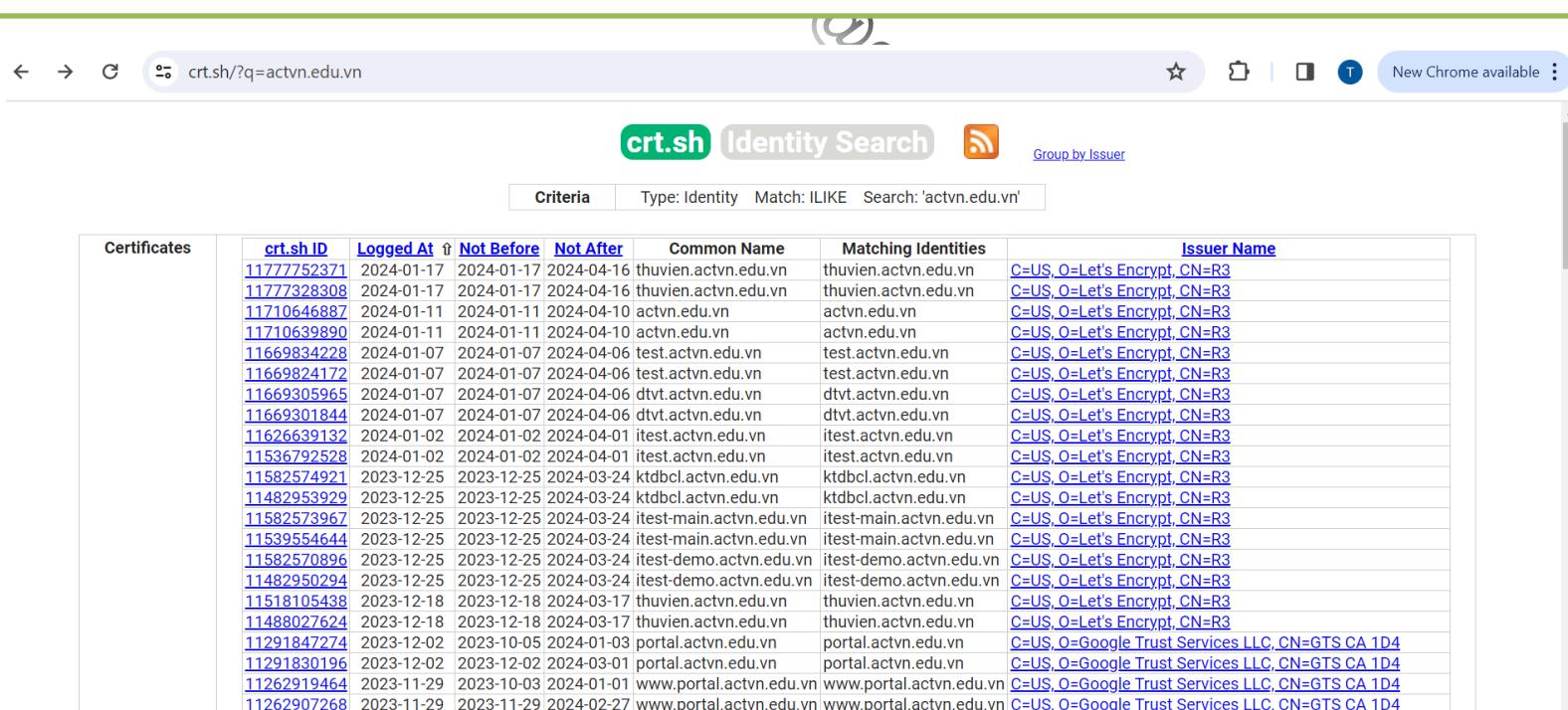
IP Block Owner

IP Address Assignment WHOIS Databases

- Cơ quan đăng ký internet khu vực (Regional Internet Registries – RIRs) cung cấp CSDL Whois có chứa thông tin về các khối địa chỉ IP.
 - Company/domain name/IPv4/IPv6/CIDR block.
 - Autonomous System (AS) number.
 - DNS information.
- Một vài tổ chức nhận địa chỉ từ ISP của họ.
- Khi tìm kiếm khối địa chỉ IP của một cơ quan tổ chức thì kết quả trả về có thể là:
 - Địa chỉ thực tế được gán.
 - Không có gì.
 - Một không gian lớn các địa chỉ.

Certificate Transparency Logs (CTL)

- CTL chứa danh sách các tên hiện tại và tên cũ được sử dụng trên certificates.
 - Tìm kiếm hostnames được sử dụng bởi nhiều dịch vụ khác nhau.
 - Kiểm tra logs trên <https://crt.sh/> (ID, Logged Date, Expiry, Common Name, Matching Identities, Issuer).



The screenshot shows a browser window displaying the crt.sh Identity Search results for the domain actvn.edu.vn. The search bar at the top contains the query "actvn.edu.vn". Below the search bar, there are tabs for "Criteria", "Type: Identity", "Match: ILIKE", and "Search: 'actvn.edu.vn'". The main content area is a table titled "Certificates" with columns: crt.sh.ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The table lists numerous entries, each corresponding to a certificate issued to actvn.edu.vn or its subdomains, such as thuvien.actvn.edu.vn, test.actvn.edu.vn, and portal.actvn.edu.vn. The Issuer Name column consistently shows "C=US, O=Let's Encrypt, CN=R3" for most entries, indicating they were issued by the Let's Encrypt certificate authority.

Certificates	crt.sh.ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	1177752371	2024-01-17	2024-01-17	2024-04-16	thuvien.actvn.edu.vn	thuvien.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11777328308	2024-01-17	2024-01-17	2024-04-16	thuvien.actvn.edu.vn	thuvien.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11710646887	2024-01-11	2024-01-11	2024-04-10	actvn.edu.vn	actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11710639890	2024-01-11	2024-01-11	2024-04-10	actvn.edu.vn	actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11669834228	2024-01-07	2024-01-07	2024-04-06	test.actvn.edu.vn	test.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11669824172	2024-01-07	2024-01-07	2024-04-06	test.actvn.edu.vn	test.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11669305965	2024-01-07	2024-01-07	2024-04-06	dtvt.actvn.edu.vn	dtvt.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11669301844	2024-01-07	2024-01-07	2024-04-06	dtvt.actvn.edu.vn	dtvt.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11626639132	2024-01-02	2024-01-02	2024-04-01	itest.actvn.edu.vn	itest.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11536792528	2024-01-02	2024-01-02	2024-04-01	itest.actvn.edu.vn	itest.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11582574921	2023-12-25	2023-12-25	2024-03-24	ktdbcl.actvn.edu.vn	ktdbcl.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11482953929	2023-12-25	2023-12-25	2024-03-24	ktdbcl.actvn.edu.vn	ktdbcl.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11582573967	2023-12-25	2023-12-25	2024-03-24	itest-main.actvn.edu.vn	itest-main.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11539554644	2023-12-25	2023-12-25	2024-03-24	itest-main.actvn.edu.vn	itest-main.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11582570896	2023-12-25	2023-12-25	2024-03-24	itest-demo.actvn.edu.vn	itest-demo.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11482950294	2023-12-25	2023-12-25	2024-03-24	itest-demo.actvn.edu.vn	itest-demo.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11518105438	2023-12-18	2023-12-18	2024-03-17	thuvien.actvn.edu.vn	thuvien.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11488027624	2023-12-18	2023-12-18	2024-03-17	thuvien.actvn.edu.vn	thuvien.actvn.edu.vn	C=US, O=Let's Encrypt, CN=R3
	11291847274	2023-12-02	2023-10-05	2024-01-03	portal.actvn.edu.vn	portal.actvn.edu.vn	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
	11291830196	2023-12-02	2023-12-02	2024-03-01	portal.actvn.edu.vn	portal.actvn.edu.vn	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
	11262919464	2023-11-29	2023-10-03	2024-01-01	www.portal.actvn.edu.vn	www.portal.actvn.edu.vn	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
	11262907268	2023-11-29	2023-11-29	2024-02-27	www.portal.actvn.edu.vn	www.portal.actvn.edu.vn	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4

Shodan

- Shodan tìm kiếm thông tin về OS, port, services, banners... của các thiết bị như Servers, Routers, Switches... kết nối vào mạng internet (<https://www.shodan.io>).
- Thông tin về SSL Certificate.
 - SSL Certificate có thể tiết lộ subdomains
- IP Address Geolocation.
- Toán tử tìm kiếm:
 - Title; country; city; net; hostname; org; port; os

Shodan Search (1/2)

- 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

The screenshot shows the Shodan search interface with the query 'apache 2.2.3 country:VN' entered. The results page displays a map of the world with red dots indicating found locations. A sidebar on the left lists 'TOP COUNTRIES' and 'TOP SERVICES'. The main content area shows detailed information for a service from 'Information Technology Institute JSC Hanoi National University' located in 'Viet Nam, Hanoi'. It includes an SSL certificate, supported SSL versions (SSLv3, TLSv1), and Diffie-Hellman parameters. A red box highlights the banner information at the bottom:

```
HTTP/1.1 200 OK
Date: Wed, 24 Mar 2021 18:25:18 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Set-Cookie: SQSESSID=j3ugkp36spr94jlkga1fbr90; 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...
```

The screenshot shows the Shodan search interface with the query 'port:3389 country:VN' entered. The results page displays a map of the world with red dots indicating found locations. A sidebar on the left lists 'TOP CITIES' and 'TOP ORGANIZATIONS'. The main content area shows detailed information for a service from 'VNENETWORK Joint Stock Company' located in 'Viet Nam, Ho Chi Minh City'. It includes a self-signed SSL certificate. A red box highlights the banner information at the bottom:

```
HTTP/1.1 200 OK
Date: Wed, 24 Mar 2021 18:25:18 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Set-Cookie: SQSESSID=j3ugkp36spr94jlkga1fbr90; 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 (2/2)

IP Address

204.51.94.153 [View Raw Data](#)

starttls

Org

Country United States

Organization Sans Institute

ISP Verizon Business

Scan Time

Last Update 2020-08-06T16:31:59.872226

ASN AS62669

Web Tech

Web Technologies

Bootstrap

Font Awesome

jQuery

YouTube

Ports

25

80

443

587

Services

25

tcp

smtp

Postfix smtpd

220 isc.sans.org ESMTP Postfix

250-isc.sans.org

250-PIPELINING

250-SIZE 20240000

250-VRFY

250-ETRN

250-STARTTLS

250-ENHANCEDSTATUSCODES

250-8BITMIME

250 DSN

Hunter.io

- ❑ Thường xuyên thực hiện OSINT và tổng hợp danh sách dữ liệu tổ chức.
 - Contact name, email address
 - Phone number, job title
- ❑ Cung cấp định dạng email phổ biến
 - ❑ {f}{last}
 - ❑ {first}{last}
 - ❑ {first}{l}

Domain Search ?

sans.org

Email Address Format

All Personal Generic

216 results Export in CSV

Most common pattern: {f}{last}@sans.org

Find someone...

Communication (13) Support (12) IT / Engineering (5) ...

Georgina Davies Chief Information Security +44 78 8293 1829
gdavies@sans.org • ✓

Employee Info

Phonebook.cz

- phonebook.cz liệt kê “tất cả domain, địa chỉ email, URLs” về tên miền.

Phonebook.cz

Phonebook lists all domains, email addresses, or URLs for the given input domain.
You are searching 34 billion records.

 Submit

Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [*.nu](#), [*.gov.uk](#), [solarwinds.com](#)

- Domains
- Email Addresses
- URLs

mbrown@sans.org
spa@sans.org
paller@sans.org
snmpool@sans.org
jullrich@sans.org
critical-controls@sans.org
info@sans.org
cyber-defense@sans.org

Public Breach Data of Credentials

- Tìm kiếm các thông tin bị rò rỉ trên các dịch vụ công cộng
- Dữ liệu được bán trên chợ đen (dark web, forum)
 - SSL Certificate có thể tiết lộ subdomains
- Người dùng hay sử dụng mật khẩu tương tự các mật khẩu cũ, thậm chí nếu các mật khẩu đã bị thay đổi thì vẫn có thể sử dụng thông tin về địa chỉ email thu được
- Một số site:
 - <https://haveibeenpwned.com/>
 - <https://www.dehashed.com/>
 - <https://intelx.io/>
 - Public data dump forum
 - Torrents

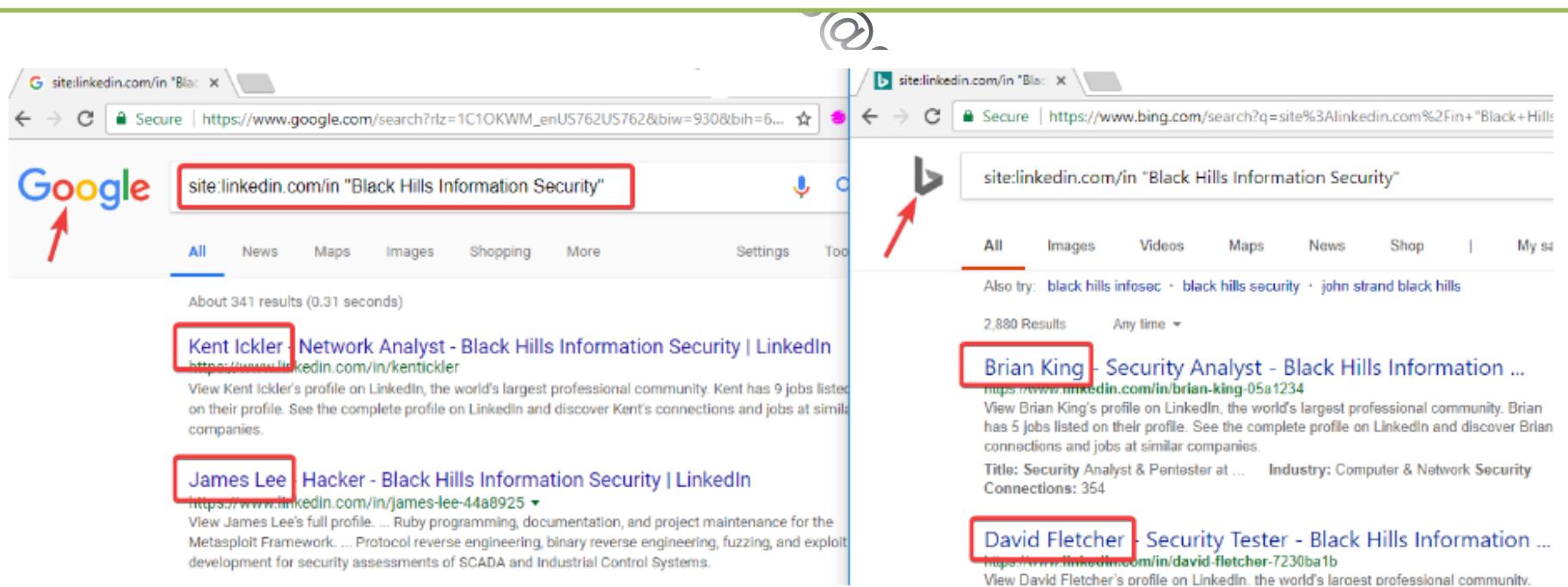
Employee Roles

- LinkedIn cung cấp thông tin về người lao động.
 - Employee names
 - Position/Titles
 - Email Addresses
- Thông tin trên các sites khác như Twitter, Facebook, Instagram, Tiktok...

nhail.com

GatherContacts

- GatherContacts là một extension của Burp Suite, cho phép thu thập “employee names, job titles” từ kết quả tìm kiếm trên LinkedIn của Google, Bing.
- <https://github.com/clr2of8/GatherContacts>
- Yêu cầu tìm kiếm thủ công: site: linkedin.com/in [target]



GatherContacts Results

site:linkedin.com/in "SANS Institute"

Page 2 of about 28,700 results (0.31 seconds)

www.linkedin.com › johnlhubbard

[John Hubbard - SANS Institute - LinkedIn](#)

John Hubbard. Certified Instructor and Author @ SANS Institute | On a mission to spread security knowledge and expertise. Teams everywhere! SANS InstitutePurdue University.

Philadelphia, Pennsylvania - Certified Instructor / Course Author - SANS Institute

www.linkedin.com › wanicha-owen-gisf-43693050

[Wanicha Owen, GISF - SANS Institute - LinkedIn](#)

SANS is a leading organization in information security training, the SANS Institute provides intensive, immersion training designed to help you and your organization stay ahead. Denver, Colorado - Inside Account Manager, GISF - SANS Institute

B	C	D	E
Column2	Column3	Column6	Column7
Name 1	Name 2	Description 1	Description 2
Johannes	Ullrich	Fellow	SANS Institute
John	Nix	Director, Federal	SANS Institute
Rob	Lee	SANS Institute	LinkedIn www.linkedin.com/in/johnlhubbard
Ray	Hawkins	Director	The SANS Institute / Global
Jay	Armstrong	Director, SLED Partnerships	The SANS ... www.linkedin.com/in/jayarmstrong
Tim	Conway	ICS	SANS Institute
Brian	Ventura	Certified Instructor	SANS Institute
Benjamin	Wright	SANS Institute	LinkedIn www.linkedin.com/in/benwright
Frank	Kim	Fellow	SANS Institute
Scott	Cassity	Managing Director	SANS Institute
Steve	Penny	Director	SANS Institute
Howard	Cribbs	CIO	SANS Institute
Wanicha	Owen	SANS Institute	LinkedIn www.linkedin.com/in/wanicha-owen-gisf-43693050
John	Hubbard	SANS Institute	LinkedIn www.linkedin.com/in/johnlhubbard

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
- ...

.com

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...

Google



gmail.com



DuckDuckGo

YAHOO!



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 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 từ khóa chỉ được trong một site hoặc tên miền cụ thể.

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 được chỉ định.

filetype:pdf cehv12

Advanced Google Hacking Search

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

“windows exploitation”

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

windows –exploitation

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

Index of /admin

Index of /password

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	
cuv-d.php	2016-07-29 11:08	17K	

Advanced Google Hacking Search

□ Google Dork hacking database

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

The image shows two screenshots of the Exploit Database Google Hacking Database. The top screenshot displays a list of search queries (Dorks) added on March 22, 2021. The bottom screenshot shows a detailed view of a specific dork entry with ID 6269, published by Swapnil Talele on June 11, 2020.

Google Hacking Database

Added: Dork

2021-03-22 inurl:set_config_networkP.html
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 ro...
2021-03-19 intext:cov OR intext:curriculum vitae AND intext:"SSN" ext:do...
2021-03-19 inurl:template.gch "ZTE Corporation."
2021-03-19 intitle:"NUUO Network Video Recorder Login" "Language"
2021-03-19 inurl:webdynpro/dispatcher

Dork: "Index of" "upload_image.php"

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

Published: 2020-06-11

Google Dork Description:

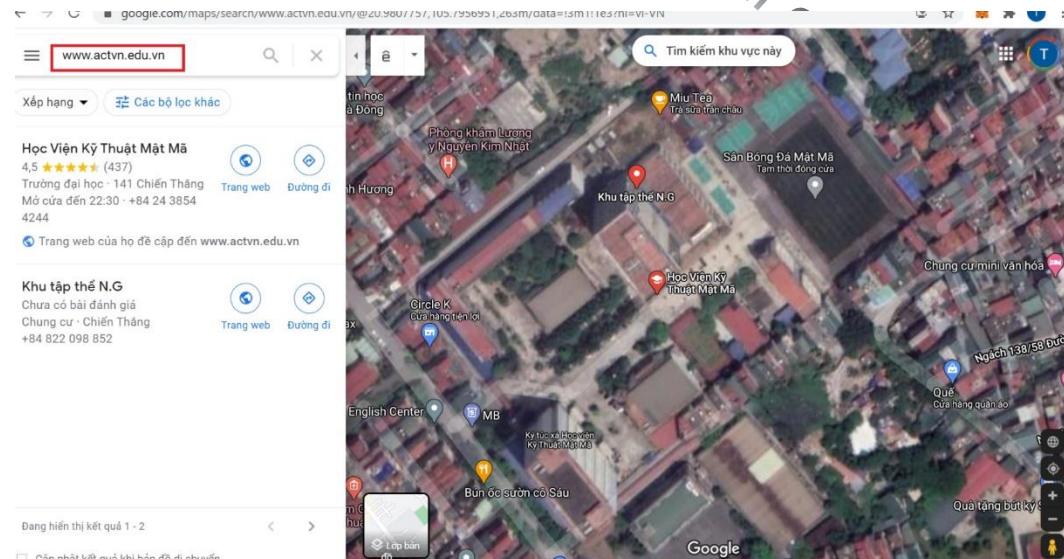
Dork: "Index of" "upload_image.php"

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.bing.com/maps>



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
*****
* 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.

The screenshot shows the Wayback Machine interface. At the top, a search bar contains the URL web.archive.org/web/*/actvn.edu.vn. Below the search bar is a navigation bar with links to Calendar, Collections, Changes, Summary, and Site Map. A message indicates "Saved 282 times between April 5, 2009 and March 16, 2021." The main area features a timeline graph showing the frequency of captures over time, with a red box highlighting the year 2017. On the left, a detailed view of a specific capture from April 3, 2017, is shown. This view includes a header menu with links to TRANG CHỦ, GIỚI THIỆU, ĐÀO TẠO, KHOA HỌC CÔNG NGHỆ, SINH VIÊN, HỢP TÁC QUỐC TẾ, LIÊN HỆ, and English. Below the menu is a sidebar with categories: DÀNH CHO NGƯỜI HỌC, THÔNG TIN TUYỂN SINH, TUYỂN SINH SAU ĐẠI HỌC, THƯ VIỆN SỐ, THƯ VIỆN ĐIỆN TỬ, DIỄN ĐÀN, and CÁC KHOA. The main content area displays news items under the heading TIN TỨC & SỰ KIỆN, including articles about the university's participation in the 2017 job fair and the opening of the Samsung Lab. The right side of the interface features a large calendar grid for the years 2009 to 2021, with a red box highlighting the date April 16, 2016.

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

282 captures

5 Apr 2009 - 16 Mar 2021

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 m特 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 m特 đã diễn ra Lễ ký kết bàn giao và Khai trương phòng thí nghiệm Samsung Lab - ACT do công ty Samsung Electronic Việt Nam (SMVC) 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) và Học viện Công nghệ Bách Khoa TP.HCM (HKTU) phối hợp tổ chức

Calendar · Collections · Changes · Summary · Site Map

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

2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021

FEB MAR APR

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

JUN JUL AUG

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

38

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...



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'];

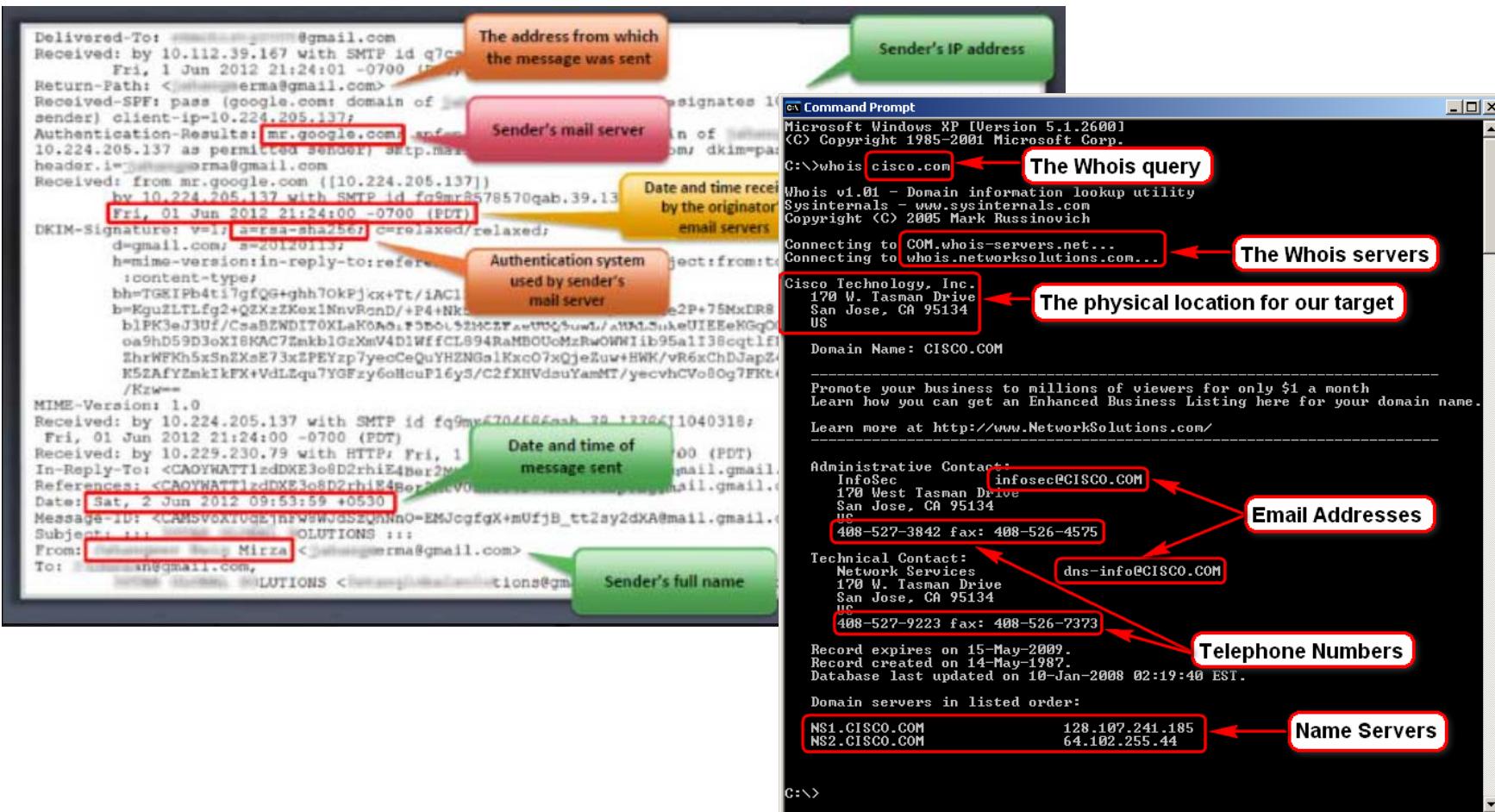
$strErrorMsg="";
$cmdOutput=array();

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

$basedn = 'dc=ctf.dc=htb';
$usersdn =
<body>
// This co
    <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...



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 a search results page from Netcraft. The URL in the address bar is `searchdns.netcraft.com/?host=actvn.edu.vn`. The results table has columns for Rank, Site, First seen, and Netblock. The first result is `qldt.actvn.edu.vn`, which is highlighted with a red box. The second result is `actvn.edu.vn`. The third result is `thuviensao.actvn.edu.vn`. The fourth result is `ctf.actvn.edu.vn`. The fifth result is `sdh.actvn.edu.vn`. The sixth result is `home.actvn.edu.vn`.

Below the table, there is a detailed network report for `http://www.actvn.edu.vn`. The report includes fields for Description, Primary language (English), Network, Site, Domain, Nameserver, Domain registrar, Nameserver organisation, Organisation, DNS admin, Top Level Domain, and DNS Security Extensions. The IP address `103.21.148.154` is linked to VirusTotal. The report also lists Netblock Owner, Hosting company, Hosting country, IPv4 address, IPv4 autonomous systems, IPv6 address, IPv6 autonomous systems, and Reverse DNS.

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
 - ...

1

Tổng quan

2

Phương pháp luận

3

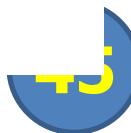
Công cụ

Cyber Detective's OSIN collection

- ❑ <https://github.com/cipher387/osint stuff tool collection?tab=readme-ov-file>

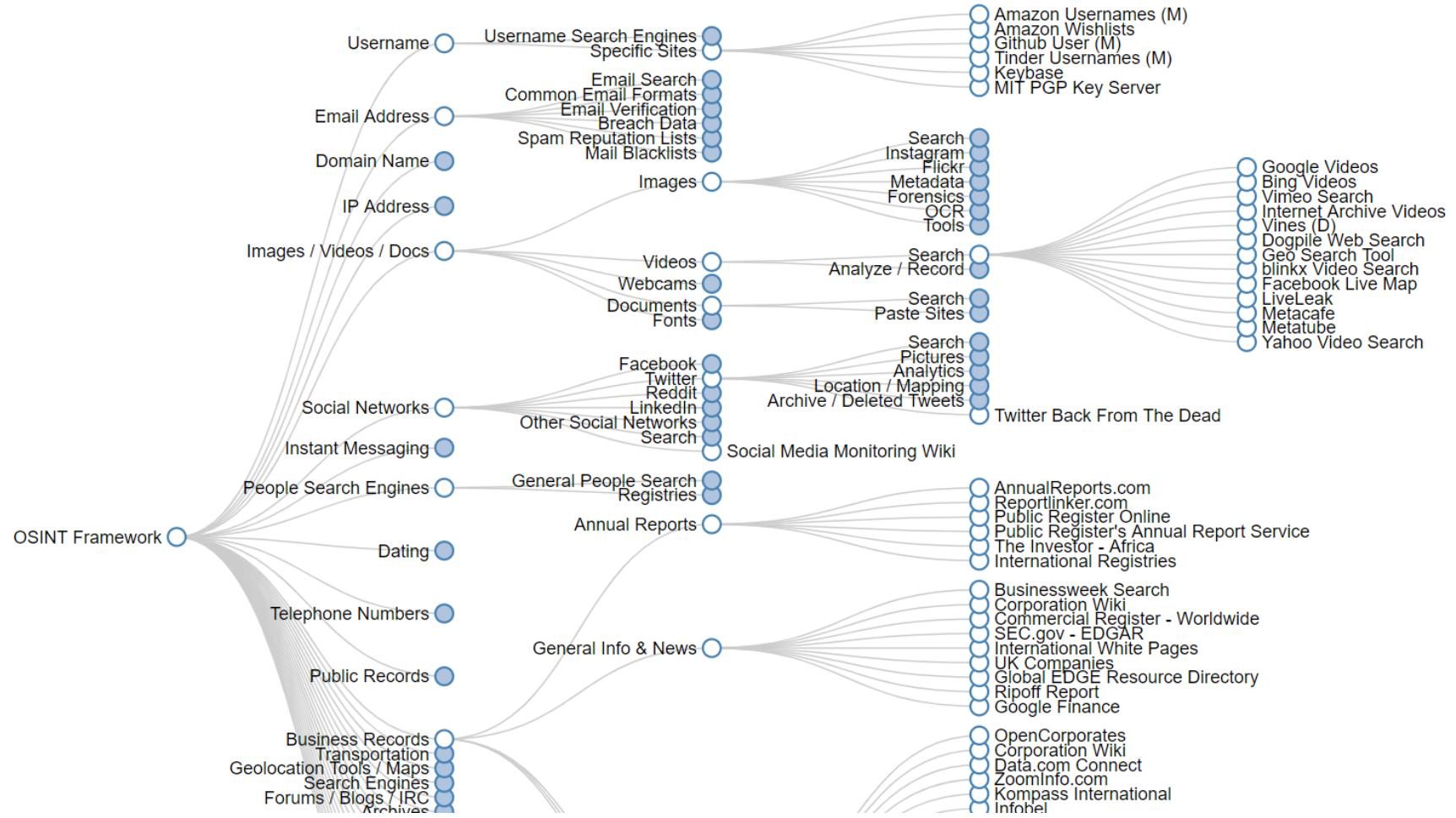
Cyber Detective OSINT Tools Collection

- Maps, Geolocation and Transport
 - Social media and photos
 - Nature
 - Aviation
 - Maritime
 - Railway
 - Routes
 - Politics, conflicts and crisis
 - Urban and industrial infrastructure
 - Culture
 - Worldwide street webcams
 - Tools
 - Transport
 - Communications, Internet, Technologies
 - Anomalies and Lost Places
 - Street View
 - Satellite/aerial imagery
 - Military tracking
 - Military visualisation
 - Other
- Social Media
 - Twitter
 - YouTube
 - TikTok
 - Protonmail
 - Facebook
 - Clubhouse
 - LinkedIn
 - Xing
 - Reddit
 - Onlyfans
 - Snapchat
- Twitch
- Fidonet
- Usenet
- Tumblr
- Flickr
- Spotify
- Discord
- Mastodon
- Yandex
- Instagram
- Google
- Patreon
- Github
- Wikipedia
- Parler
- Pornhub
- Steam
- Minecraft
- Xbox
- VK
- Office365
- OneDrive
- Udemy
- Duolingo
- Universal
- Downloaders
- Domain/IP/Links
- Dorks/Pentest/Vulnerabilities
- Searchers, scrapers, extractors, parsers
- Redirect lookup
- Cookies analyze
- Website's files metadata analyze and files downloads
- Backlinks analyze
- Website analyze
- Domain/IP investigation
- Subdomains scan/brute
- Cloudflare
- Databases of domains
- Website traffic look up
- Website technology look up
- Source Code Analyzes
- Broken Links Checkers
- URL unshorteners
- Text Analyze
- Sound indefication and analyze
- Sound search and analyze
- Video editing and analyze
- Image Search and Identification
 - Reverse Image Search Engines and automation tools
 - Image editing tools
 - Other Image Search Engines
 - Image Analyze
 - Exif Analyze and editing
 - Face recognition and search
 - Font Indenification
- Cryptocurrencies
- Messengers
 - Telegram
 - WhatsApp
 - Kik
 - Slack
 - Skype
- Code
- Search engines
 - Universal search tools
 - Darknet/deepweb search tools
 - Public buckets search tools
 - Bugbounty/vulnerabilities search tools
 - Filesharing Search Engines
 - Tools for DuckDuckGo
 - Tools for Google
- IOT
- Archives
 - Tools for working with web archives
 - Archives of documents/newspapers
 - Tools for working with WARC (WebARChive) files
- Datasets
- Science
- Passwords
- Emails
- Nicknames
- Phone numbers
- Universal Contact Search and Leaks Search
- Sock Puppets
- NOOSINT tools
- Visualization tools
- Routine/Data Extraction Automation
- Browser analyze
- Files
- IMEI and serial numbers
- NFT
- Keywords, trends, news analytics
- Apps and programs
- Company information search
- Bank information search



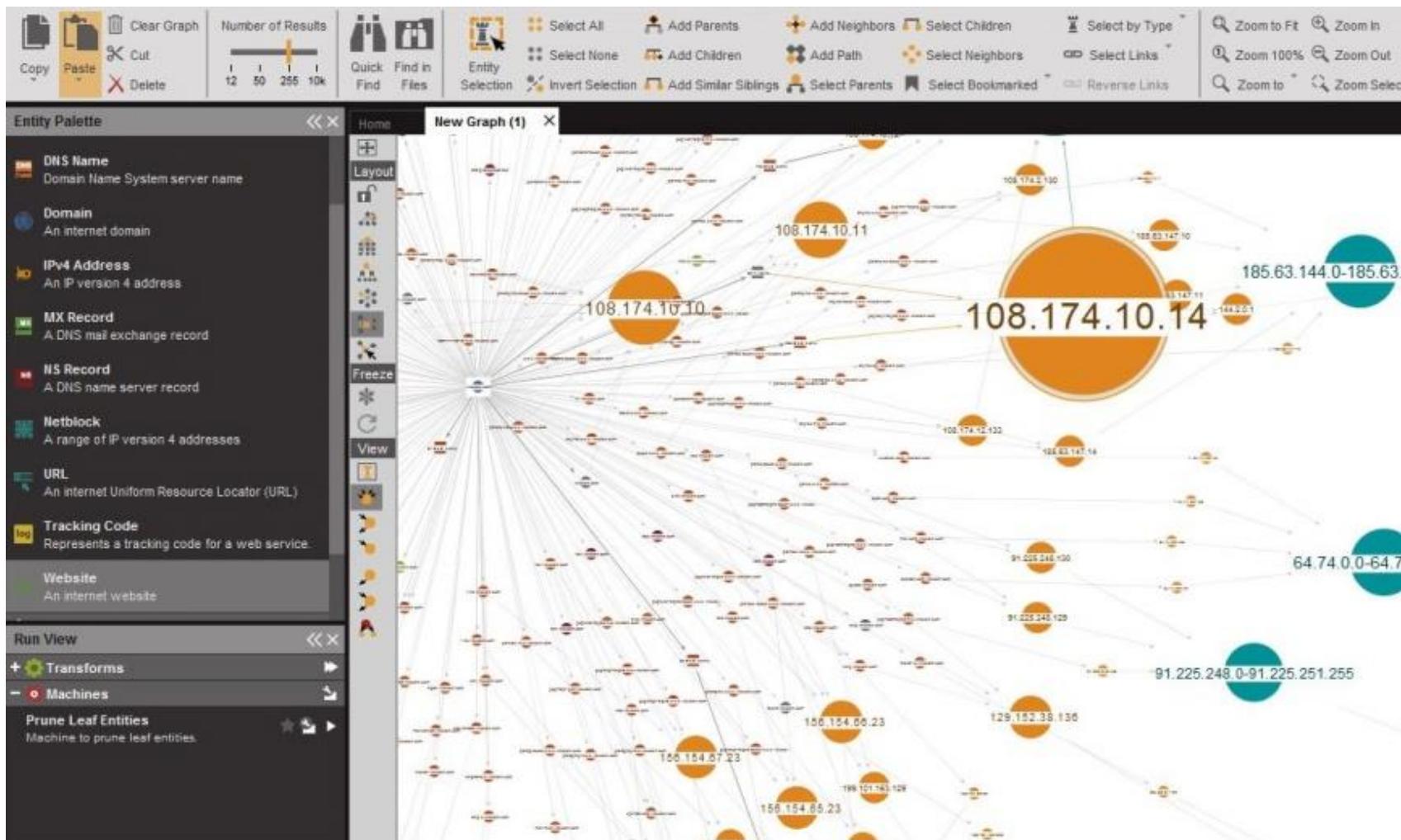
OSINT Framework

- ❑ <https://osintframework.com/>
- ❑ <https://github.com/lockfale/OSINT-Framework>



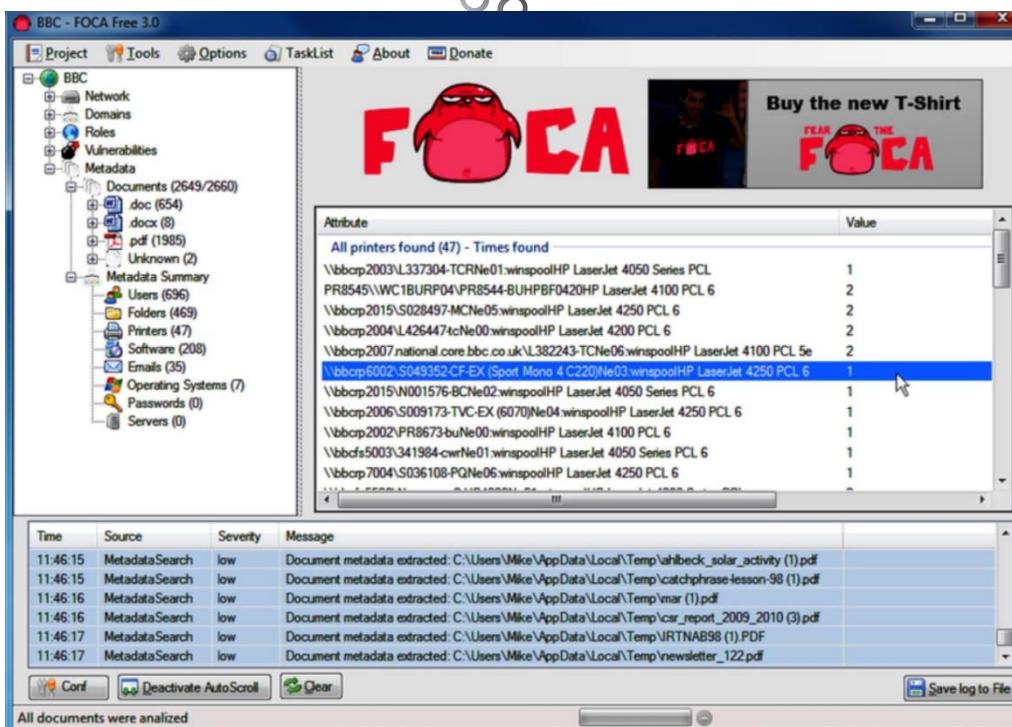
Maltego

- 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'
88000 `8bo. 88 88 8P 88 8800000 88 `8bd8'
88 `Y8b. 88 88 8b 88 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}--XSSStrike
{7}--Doork
{8}--Crips

{99}-Back To Main Menu

fsociety ~# 2
```

www.hackingblogs.com

PENTMENU

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

```
ddos@DESKTOP-740A66K: ~
```



```
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:
 - CheckUserNames (<https://checkusernames.com/>)
 - HaveIbeenPwned (<https://haveibeenpwned.com/About>)
 - BuildWith (<https://builtwith.com/>)
 - Google Dorks / Shodan
 - Jigsaw (<https://www.jigsawsecurityenterprise.com/>)
 - Recon-ng
 - TheHavester
 - Metagoofil/exiftool
 - SpiderFoot
 - ...

Lập báo cáo

- Lập báo cáo về các thông tin thu được sau quá trình OSINT.
- Có 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.

Thảo luận

Footprinting
countermeasures?

Imtuan1980@gmail.com



