LAB 1

**TỔNG QUAN KALI LINUX**

BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Kỳ báo cáo: Buổi 02 (Session 02)**

**Tên chủ đề: Information Gathering**

*GVHD: Nghi Hoàng Khoa*

**Nhóm: 01 (ghi số thứ tự nhóm)**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT101.M11.ANTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Trần Hoàng Khang | 19521671 | 19521671@gm.uit.edu.vn |
| 2 | Nguyễn Đoàn Xuân Bình | 19521265 | 19521265@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 01 | 100% |
| 2 | Kịch bản 02 | 100% |
| 3 | Kịch bản 03 | 100% |
| 4 | Kịch bản 04 | 100% |
| 5 | Kịch bản 05 | 100% |

BÁO CÁO CHI TIẾT

*2. Hãy liệt kê những thành viên đang làm việc cho MegaCorp One và một vài thông tin về những thành viên đó (địa chỉ email, chức vụ, tài khoản mạng xã hội)?*

*A picture containing graphical user interface

Description automatically generated*

*3. Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra được điều gì?*

*Biết được tên máy chủ mail server, có mail để spam*

*4. Sử dụng công cụ whois để xác định các name server của MegaCorp One.*

*A screenshot of a computer

Description automatically generated with medium confidence  
5. Sử dụng công cụ whois để tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn) có được không? Giải thích?*

A screenshot of a computer

Description automatically generated with medium confidence

*Theo kết quả tìm kiếm trả về, ta thấy máy chủ tld của tên miền* ***uit.edu.vn*** *không có server của* ***whois***  *, tức là trong database của whois không tìm thấy nên không thể phân giải tên miền để tìm thông tin => Không*

*6. Thu thập thông tin về tên miền* ***uit.edu.vn*** *và hãy cho biết các thông tin như:  
a. Ngày đăng ký tên miền*

*  
b. Ngày hết hạn tên miền  
c. Chủ sở hữu tên miền (không rõ, chỉ tìm được owner của netblock)*

*  
d. Các name server của tên miền  
8. Bạn có thể tìm kiếm thêm các nhân viên khác của MegaCorp One mà không được liệt kê trên trang web www.megacorpone.com?  
9. Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)*

*From exploitdb with love*

intext: [intext:"index of/" "client-1.0-SNAPSHOT"](https://www.exploit-db.com/ghdb/7425)

intitle: [intitle:" index of "/Invoices\*"](https://www.exploit-db.com/ghdb/7414)

site: [site:"\*.com" inurl: admin/index.php](https://www.exploit-db.com/ghdb/7423)

inurl: [inurl:/wp-content/plugins/thecartpress/](https://www.exploit-db.com/ghdb/7419)

filetype: [filetype:log intext:("apache2" | "htdocs")](https://www.exploit-db.com/ghdb/7424)

*10. Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?*

*Payload:* **intext:"điểm rèn luyện" intext:"Nghi Hoàng Khoa " inurl: "uit. edu.vn "**

*Comment:* **Điểm ngày xưa nhìn lạ quá ~~**

Table

Description automatically generated

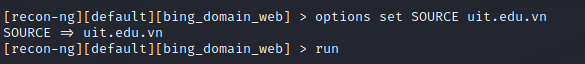
*12. Thực hiện sử dụng module có thể giúp phân giải tên miền ở Hình 20 thành địa chỉ IP tương ứng.*

*Chưa tìm được module nào. Sử dụng lệnh ping với từng trang web (cách thủ công, hoặc viết bash script với lệnh host để phân giải theo A record)  
13. Sử dụng một số module khác có trong recon-ng để thu thập thông tin về UIT nhiều nhất có thể.*

*Ví dụ tìm kiếm tên miền:*

*Một số gói hay:*

*Sử dụng gói “****bing\_domain\_web”***



Trả về 1 list khá đầy đủ: (Chụp không hết)

A picture containing text

Description automatically generated

Sử dụng gói “**brute hosts”**:

Tìm các sub domain theo một wordlist cho trước.

Text

Description automatically generated

*14. Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG*

Sử dụng **gitleaks:**

Lấy được những secret commit từ repo của một bạn làm đồ án bên trường Khoa học tự nhiên:

Github: <https://github.com/zricethezav/gitleaks.git>

Xem được những lần thay đổi commit trong repo, người thay đổi, …

Text

Description automatically generated

xem file my-report.json:

Text

Description automatically generated

*15. Thực hiện tìm kiếm các lệnh khác trên Shodan mà có thể tiết lộ thêm nhiều thông tin thú vị về một đối tượng bất kỳ.*

*Tìm một số máy chủ chạy dịch vụ torrent.*

*Graphical user interface

Description automatically generated*

*Truy vết về một số thông tin tổ chức và công nghệ được dùng:*

*Graphical user interface, table

Description automatically generated*

*Graphical user interface

Description automatically generated*

*Text, letter

Description automatically generated  
16. So sánh kết quả tìm kiếm trên Shodan so với các search engine khác như Google, Bing…*

*Shodan mang lại thông tin nhiều về công nghệ, chi tiết các tên tổ chức và dịch vụ được sử dụng, đồng thời có chỉ ra về những cảnh báo những lổ hổng có liên quan, cung cấp thông tin các opening port, hạ tầng kiến trúc, … Và nhiều thứ hay ho hơn nữa nếu đăng ký và mua gói dịch vụ*

*21. Ngoài các bản ghi kể trên, hãy liệt kê các bản ghi khác của DNS..*

*• Bản ghi AFSDB - Bản ghi này được sử dụng cho các khách hàng của Hệ thống tệp Andrew (AFS) do Carnegie Melon phát triển. Bản ghi AFSDB có chức năng tìm các ô AFS khác.*

*• Bản ghi APL - ‘danh sách tiền tố địa chỉ’ là bản ghi thử nghiệm chỉ định danh sách các dải địa chỉ.*

*• Bản ghi CAA - Đây là bản ghi ‘ủy quyền tổ chức chứng nhận’, nó cho phép chủ sở hữu miền nêu rõ tổ chức phát hành chứng chỉ nào có thể cấp chứng chỉ cho miền đó. Nếu không có bản ghi CAA nào tồn tại, thì bất kỳ ai cũng có thể cấp chứng chỉ cho miền. Các bản ghi này cũng được kế thừa bởi các miền phụ.*

*• Bản ghi DNSKEY - ‘Bản ghi khóa DNS’ chứa khóa công khai được sử dụng để xác minh chữ ký Tiện ích mở rộng bảo mật hệ thống tên miền (DNSSEC).*

*• Bản ghi CDNSKEY - Đây là bản sao con của bản ghi DNSKEY, có nghĩa là được chuyển cho cha mẹ.*

*22. Sử dụng lệnh* ***host*** *để tìm kiếm các bản ghi TXT, MX cho tên miền uit.edu.vn*

*A screenshot of a computer

Description automatically generated with medium confidence*

*23. Sử dụng lệnh* ***host*** *cho các hostname không tồn tại trong tên miền uit.edu.vn  
(idontexist, noexist, baithuchanhso2). Có nhận xét gì về kết quả trả về hay không? Giải thích?*

*Text

Description automatically generated*

*Những host này vẫn có địa chỉ IP, nhưng khi truy cập vào thì bên server không hoạt động và respose lại*

*Text

Description automatically generated with medium confidence*

*24. Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com*

*Bash script:*

**#! /bin/bash**

**for i in $(cat /usr/share/wordlists/rockyou.txt)**

**do**

**if host $i.megacorpone.com | grep "has address"**

**then**

**echo "True"**

**else**

**echo "False"**

**fi**

done

Kết quả :

Text

Description automatically generated

*25. Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (hcmus.edu.vn, hcmussh.edu.vn, uit.edu.vn, hcmut.edu.vn, hcmiu.edu.vn, uel.edu.vn, hcmier.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.*

*Bash script:*

***#! /bin/bash***

***for i in $(cat /home/virus/Desktop/list)***

***do***

***a=$(host -t ns $i)***

***for j in $(echo $a | awk -F " " '{print $4}')***

***do***

***host -l $i $j***

***done***

***done***

*Kết quả trả về khá dài nên chỉ screenshot 1 phần*

A screenshot of a computer

Description automatically generated with medium confidence

*26. Viết Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn* ***-t***

*Nguồn kali****.****org/tools/dnsrecon*

Text

Description automatically generated*27. Cho một vài ví dụ sử dụng kết hợp các tùy chọn được DNSRecon hỗ trợ khác (ít nhất là 2 ví dụ)*

***-b: Perform Bing enumeration with standard enumeration.***

Text

Description automatically generated

***-y Perform Yandex enumeration with standard enumeration.***

Text

Description automatically generated

*28. So sánh 2 công cụ DNSEnum và DNSRecon? Công cụ nào dễ sử dụng hơn? Công cụ nào cho kết quả chính xác hơn? Công cụ nào hiển thị nhiều kết quả hơn?*

*Theo nhận xét cá nhân,* ***dnsenum*** *trả về kết quả chính xác hơn và có khả năng sàng lọc output và xử lý tên miền, thể hiện kết quả đẹp mắt hơn. Nhiều tiện ích hơn so với* ***dnsrecon****, theo description mô tả. Nhưng mặc định với nhiều option thực hiện cùng một lúc, dnsenum đưa ra output lâu hơn .*

*29. Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan sử dụng Nmap*

*Gửi gói SYN và nhận gói RST trên các port*

A picture containing text, phone, cellphone, stack

Description automatically generated

*30. Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.*

*Gửi SYN nhận SYN-ACK, gửi RST và ACK*

A picture containing calendar

Description automatically generated

*31. So sánh với sử dụng phương thức SYN Scan (số lượng gói tin được gửi, số lượng gói tin được nhận, thời gian quét, kết quả hiển thị…)*

*Thời gian quét thay đổi không đáng kể (nhanh quá)*

*Số lượng gói tin theo wireshark bắt được tăng lên*

*32. Thực hiện kiểm tra các host đang hoạt trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, …)*

***Sử dụng lớp socket***

***Nguồn : geeksforgeeks***

*import pyfiglet*

*import sys*

*import socket*

*from datetime import datetime*

*ascii\_banner = pyfiglet.figlet\_format("PORT SCANNER")*

*print(ascii\_banner)*

*# Defining a target*

*if len(sys.argv) == 2:*

*# translate hostname to IPv4*

*target = socket.gethostbyname(sys.argv[1])*

*else:*

*print("Invalid ammount of Argument")*

*# Add Banner*

*print("-" \* 50)*

*print("Scanning Target: " + target)*

*print("Scanning started at:" + str(datetime.now()))*

*print("-" \* 50)*

*try:*

*# will scan ports between 1 to 65,535*

*for port in range(1,65535):*

*s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)*

*socket.setdefaulttimeout(1)*

*# returns an error indicator*

*result = s.connect\_ex((target,port))*

*if result ==0:*

*print("Port {} is open".format(port))*

*s.close()*

*except KeyboardInterrupt:*

*print("\n Exitting Program !!!!")*

*sys.exit()*

*except socket.gaierror:*

*print("\n Hostname Could Not Be Resolved !!!!")*

*sys.exit()*

*except socket.error:*

*print("\ Server not responding !!!!")*

*sys.exit()*

*33. Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn* ***-sn***

*Không bắt được gói tin*

*34. Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP)*

Text

Description automatically generated

*35. Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)*

***xmpp-info.nse***

Text

Description automatically generated

**smb-protocols.nse**

Text

Description automatically generated