

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Quét lỗ hổng bảo mật

GV: Trần Nguyễn Đức Huy

Ngày báo cáo: 24/11/2022

Nhóm: 05

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N12.ATCL.1

STT	Họ và tên	MSSV	Email
1	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
2	Nguyễn Hùng Thịnh	20521963	20521963@gm.uit.edu.vn
3	Dương Đỗ Khoa	20521465	20521465@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Câu 11	60%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

MỤC LỤC

A.	BÁO CÁO CHI TIẾT	2
	Câu 1:	2
	Câu 2:	2
	Câu 3:	2
	Câu 4:	2
	Câu 5:	2
	Câu 6:	2
	Câu 7:	2
	Câu 8:	2
	Câu 9:	2
	Câu 10:	2
	Câu 11:	2
B.	TÀI LIỆU THAM KHẢO.....	5
	YÊU CẦU CHUNG	6

A. BÁO CÁO CHI TIẾT

Câu 1:

Câu 2:

Câu 3:

Câu 4:

Câu 5:

Câu 6:

Câu 7:

Câu 8:

Câu 9:

Câu 10:

Câu 11:

Câu hỏi:

Sinh viên/nhóm sinh viên tìm hiểu 1 trong các công cụ quét lỗ hổng tự động sau đây, và viết báo cáo kết quả theo như các phần đã chia ở bài tập 1:

OpenVAS (<https://www.openvas.org/>)

- Tsunami (<https://github.com/google/tsunami-security-scanner>)
- Rapid7 Nexpose (<https://www.rapid7.com/try/nexpose/>)
- Qualys Community Edition (<https://www.qualys.com/community-edition/>)
- Arachni (<https://www.arachni-scanner.com/>)
- Sn1per (<https://github.com/1N3/Sn1per>)
- Trivy (<https://github.com/aquasecurity/trivy>)
- Jok3r (<https://github.com/koutto/jok3r>)

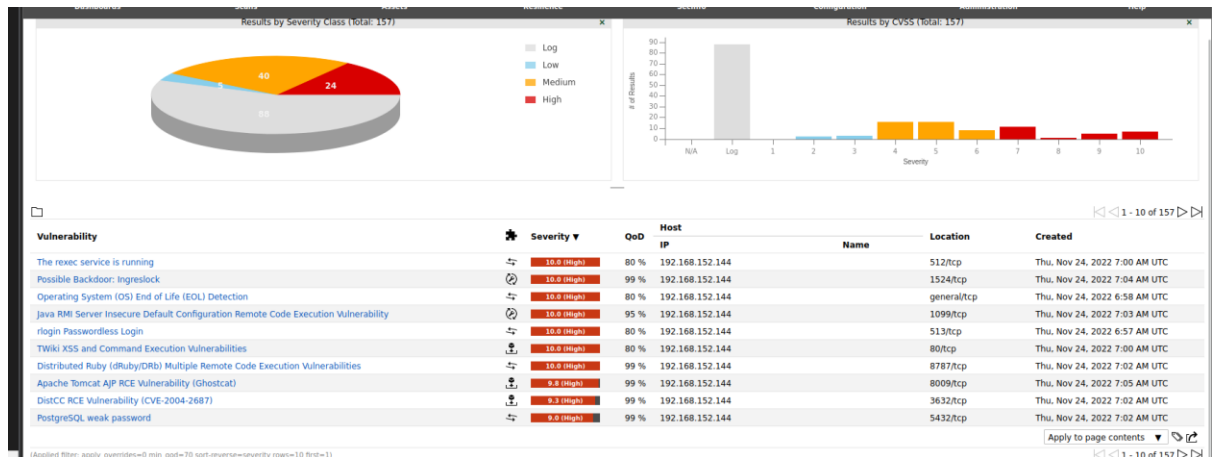
Trả lời:

Sử dụng công cụ OpenVAS:

Câu 11.1: Scan không sử dụng tài khoản chứng thực

- Đặt tên cho target và địa chỉ ip là của máy target

- Auto Delete Reports: ☒ Do not automatically delete reports, ☐ Automatically delete oldest reports but always keep newest 5 reports
- Scanner: OpenVAS Default
- Scan Config: Full and fast
- Order for target hosts: Sequential
- Maximum concurrently executed NVTs per host: 4
- Maximum concurrently scanned hosts: 20
- Sau đó lưu lại



- Kết quả khi quét có khá nhiều lỗ hổng ở mức high

Câu 11.4: Scan sử dụng tài khoản chứng thực

The screenshot shows the 'Edit Credential MyCredential' window in Metasploit. The fields are as follows:

- Name:** MyCredential
- Comment:** (empty)
- Type:** Username + Password
- Allow insecure use:** ☐ Yes ☒ No
- Username:** msfadmin
- Password:** ☐ Replace existing password with

Buttons: Cancel, Save

- Trong tab configure chọn Credential
- Tạo mới credential đặt tên
- Chọn type là username+password
- Điền username và password của máy metasploit

The screenshot shows the 'New Target' window in Metasploit. The fields are as follows:

- Simultaneous scanning via multiple IPs:** ☒ Yes ☐ No
- Port List:** All IANA assigned TCP
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:**
 - SSH:** MyCredential on port 22
 - Elevate privileges:** --
 - SMB:** --
 - ESXi:** --

- Trong phần task scan ở phần new target

- | Dashboards | Scans | Assets | Rescino | Sinfo | Configuration | Administration | Help | | | |
|---|------------------------|-------------------|---------------------|----------------------------|-------------------------------|-------------------------------|-------------------------|------------------------------|----------------------------|------------------|
| Information | Results
(65 of 559) | Hosts
(1 of 1) | Ports
(18 of 23) | Applications
(14 of 14) | Operating Systems
(1 of 1) | CVEs
(30 of 30) | Closed CVEs
(0 of 0) | TLS Certificates
(2 of 2) | Error Messages
(0 of 0) | User Tags
(0) |
| | | | | | | | | | | |
| Vulnerability | Severity ▼ | QoD | Host IP | Name | Location | Created | | | | |
| rlogin Passwordless Login | 🚩 10.0 (High) | 80 % | 192.168.152.144 | | 513/tcp | Thu, Nov 24, 2022 7:40 AM UTC | | | | |
| Possible Backdoor: Ingreslock | 🚩 10.0 (High) | 99 % | 192.168.152.144 | | 1524/tcp | Thu, Nov 24, 2022 7:50 AM UTC | | | | |
| Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability | 🚩 10.0 (High) | 95 % | 192.168.152.144 | | 1099/tcp | Thu, Nov 24, 2022 7:49 AM UTC | | | | |
| Distributed Ruby (dRubyDb) Multiple Remote Code Execution Vulnerabilities | 🚩 10.0 (High) | 99 % | 192.168.152.144 | | 6787/tcp | Thu, Nov 24, 2022 7:48 AM UTC | | | | |
| The nexex service is running | 🚩 10.0 (High) | 80 % | 192.168.152.144 | | 512/tcp | Thu, Nov 24, 2022 7:45 AM UTC | | | | |
| Twiki XSS and Command Execution Vulnerabilities | 🚩 10.0 (High) | 80 % | 192.168.152.144 | | 80/tcp | Thu, Nov 24, 2022 7:46 AM UTC | | | | |
| Operating System (OS) End of Life (EOL) Detection | 🚩 10.0 (High) | 80 % | 192.168.152.144 | | general/tcp | Thu, Nov 24, 2022 7:44 AM UTC | | | | |
| Apache Tomcat AJP RCE Vulnerability (jshostcat) | 🚩 9.8 (High) | 99 % | 192.168.152.144 | | 8009/tcp | Thu, Nov 24, 2022 7:51 AM UTC | | | | |
| DisTCC RCE Vulnerability (CVE-2004-2487) | 🚩 9.3 (High) | 99 % | 192.168.152.144 | | 3632/tcp | Thu, Nov 24, 2022 7:48 AM UTC | | | | |
| MySQL / MariaDB weak password | 🚩 9.0 (High) | 95 % | 192.168.152.144 | | 3306/tcp | Thu, Nov 24, 2022 7:48 AM UTC | | | | |
| VNC Brute Force Login | 🚩 9.0 (High) | 95 % | 192.168.152.144 | | 5900/tcp | Thu, Nov 24, 2022 7:47 AM UTC | | | | |
| PostgreSQL weak password | 🚩 9.0 (High) | 99 % | 192.168.152.144 | | 5432/tcp | Thu, Nov 24, 2022 7:48 AM UTC | | | | |
| phpinfo() output Reporting | 🚩 7.5 (High) | 80 % | 192.168.152.144 | | 80/tcp | Thu, Nov 24, 2022 7:46 AM UTC | | | | |
| PHP-CGI-based setups vulnerability when parsing query string parameters from php files. | 🚩 7.5 (High) | 95 % | 192.168.152.144 | | 80/tcp | Thu, Nov 24, 2022 7:53 AM UTC | | | | |
| Test HTTP dangerous methods | 🚩 7.5 (High) | 99 % | 192.168.152.144 | | 80/tcp | Thu, Nov 24, 2022 7:55 AM UTC | | | | |
| FTP Brute Force Logins Reporting | 🚩 7.5 (High) | 95 % | 192.168.152.144 | | 21/tcp | Thu, Nov 24, 2022 7:48 AM UTC | | | | |
| rsh Unencrypted Cleartext Login | 🚩 7.5 (High) | 80 % | 192.168.152.144 | | 514/tcp | Thu, Nov 24, 2022 7:45 AM UTC | | | | |
| The rlogin service is running | 🚩 7.5 (High) | 80 % | 192.168.152.144 | | 513/tcp | Thu, Nov 24, 2022 7:45 AM UTC | | | | |
| FTP Brute Force Logins Reporting | 🚩 7.5 (High) | 95 % | 192.168.152.144 | | 2121/tcp | Thu, Nov 24, 2022 7:48 AM UTC | | | | |
| SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 🚩 7.4 (High) | 70 % | 192.168.152.144 | | 5432/tcp | Thu, Nov 24, 2022 7:51 AM UTC | | | | |

- ## B. TÀI LIỆU THAM KHẢO

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).
Ví dụ: [NT101.K11.ANTT]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT