Huỳnh Lan Nhi

Lớp: 10\_ĐH\_CNPM1

MSSV: 1050080028

LAB 7 Lý thuyết

**3.1. Phân tích một số kỹ thuật quét cổng ứng dụng của Nmap**

**3.1.1. Kịch bản 1**

- Lệnh thực hiện: nmap -sn 192.168.117.0/24

- Kỹ thuật sử dụng: ARP Ping Scan

- Đặc điểm lưu lượng: Gửi các gói ARP Request đến từng IP trong mạng. Thiết bị phản hồi bằng ARP Reply nếu đang hoạt động.

- File lưu lượng: task1.pcap

**3.1.2. Kịch bản 2**

- Lệnh thực hiện: nmap -sS -F 192.168.117.13

- Kỹ thuật sử dụng: TCP SYN Scan (Half-open scan)

- Đặc điểm lưu lượng: Gửi gói TCP SYN đến các cổng phổ biến. Nếu nhận được SYN/ACK, cổng đang mở.

- File lưu lượng: task2.pcap

**3.1.3. Kịch bản 3**

- Lệnh thực hiện: nmap -sA -F 192.168.117.13

- Kỹ thuật sử dụng: TCP ACK Scan

- Đặc điểm lưu lượng: Gửi gói TCP ACK. Nếu nhận RST, xác định có firewall bảo vệ.

- File lưu lượng: task3.pcap

**3.2. Thu thập thông tin hệ thống**

- Lệnh tìm dịch vụ email: nmap -p 25,465,587 192.168.100.0/24

- Giải thích: quét các cổng phổ biến của dịch vụ email (SMTP - 25, SMTPS - 465, SMTP submission - 587)

- Lệnh thu thập hệ điều hành và dịch vụ: nmap -A 192.168.100.X

- OS: Ubuntu Linux 20.04

- Dịch vụ:

+ SSH (22) - OpenSSH 7.6p1

+ SMTP (25) - Postfix smtpd 3.3.0

+ DNS (53) - BIND 9.11.3

- File lưu lượng: task4.pcap

**3.3. Tìm kiếm thông tin về các lỗ hổng**

Dựa vào kết quả quét, tra cứu lỗ hổng trên:  
 https://www.cvedetails.com/  
 https://cve.mitre.org/cve

|  |  |  |  |
| --- | --- | --- | --- |
| Tên dịch vụ | Phần mềm & Phiên bản | Mã CVE | Mô tả ngắn gọn |
| Telnet | telnetd 1.2 | CVE-2020-10188 | Lỗ hổng tràn bộ đệm khi xử lý kết nối từ xa |
| DNS | BIND 9.11.5 | CVE-2022-2795 | Tấn công từ chối dịch vụ qua crafted queries |
| SSH | OpenSSH 7.2p2 | CVE-2018-15473 | Tiết lộ người dùng tồn tại qua thông báo lỗi |