Bài tập tuần 1:

Câu 1. Lập bản các kỹ thuật tấn công cơ bản

*Lời giải:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | Tên | Hoạt động | Công cụ | Hacker đạt được | Biện pháp |
| 1 | Eavesdropping | Nghe trộm  Giám sát, bắt các gói tin đi qua | 1 thiết bị mạng và một chương trình ứng dụng | Thông tin | Mã hoá dữ liệu trước khi truyền |
| 2 | Cryptanalysis | Lấy thông tin từ dữ liệu đã mã hoá mà không cần khoá giải mã | Công cụ toán học và máy tính hiệu suất cao | Thông tin | Sử dụng giải thuật mã hoá không thể hiện cấu trúc thống kê trong chuỗi mật mã  Khoá có độ dài lớn |
| 3 | Password Pilfering | Thông qua password, username. |  | Đánh cắp thông tin | Secret passwords  Biometrics  Authenticating items  Lưu ý quy tắc bảo vệ mật khẩu |
| 4 | Identity Spoofing | Mạo nhận nạn nhân mà không cần sử dụng mật khẩu của nạn nhân |  |  |  |
| 5 | Buffer-Overflow Exploitations | Làm tràn bộ đệm |  |  |  |
| 6 | Repudiation |  |  |  | Sử dụng các thuật toán mã hoá và xác thực |
| 7 | Intrusion | Truy cập bất hợp pháp vào mạng | IP Scan và Port Scan | Đánh cắp thông tin, tài nguyên, băng thông |  |
| 8 | Denial of Service Attacks | Ngăn chặn người dùng hợp pháp sử dụng dịch vụ.  DoS hoặc DDoS | Jolt2, Bubonic.c, Targa,… |  |  |
| 9 | Malicious Software | Virus  Worms  Trojan horses  Logic bombs  Backdoors  Spywares |  |  |  |

Câu 2. Phân tích mô hình phòng thủ theo chiều sâu

*Lời giải:*



Ví dụ:

* Data: Digital Signature
* Application: Antivirus
* Host: phân quyền truy cập
* Internal Network: sử dụng phần mềm chống xâm nhập…
* Perimeter: firewall
* Physical: Lock, camera
* Policies, Procedures, and Awareness: quy tắc mật khẩu trên 8 chữ số,…