Câu hỏi ôn tập thực tập cơ sở:

Bài 1:

- cài đặt AVG để quét virus

- cài đặt skybot S&D là phần mềm chống gián điệp

- cài đặt Kaspaski: để làm ổ dự trữ.

Bài 2: hỏi về các câu lệnh thực hiện trong Ubuntu

Mkdir là gì

Man là gì

Mv là gì

Rmdir là gì

Pw là gì :

Cd là gì: move

Cp là gì: copy

Bài 3:

* Dịch vụ Web Server:

+) web server hay còn được gọi là cung cấp dữ liệu nội dung dưới dạng hình ảnh văn bản và video. ứng dụng(chương trình duyệt website.

+) ta nâng cấp win10 server thành DC rồi từ đó máy kết win10 kết nối với miền và truy cập webserver.

* FPT server:

+) là nơi lưu trữ các tệp tin và thư mục cho phép người dùng truy cập và tải chúng qua mạng internet

+) cổng giao tiếp là 21 vì nó là cổng TCP nó hoạt động với FTP.

* Remote server: thì là kết nối với remote kết nối máy chủ và nó chạy.
* kết nối thông qua ftp là cổng bao nhiêu? cổng 21
* Authentication: Anonymous (xác thực : vô danh) - ai cũng vào được
* Permissions: Read (Cấp phép : chỉ đọc) - chỉ cho phép đọc, không được sửa xóa

Bài 4:

* Thiếu SELinux
* Sử dụng sambashare để chia sẻ file trên samba.
* OpenSsh là dịch vụ kết nối dữa máy window và máy linux

BÀI 6: tấn công HIDS và NIDS

- hệ thống IDS là lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn

Có 4 hệ thống phát hiện:

- cảm biến: thu thập sự kiện.

- phân tích: phát hiện tấn công các hành vi dựa trên hệ thống cảm biến.

- không gian lưu trữ: lưu trữ các sự kiện và kết quả phân tích.

- Giao diện điều khiển: để cài đặt hệ thống IDS, cập nhật các trạng thái bảo mật.

1. đọc phần snort trong lý thuyết là một công cụ phân tích gói tin xâm nhập mã nguồn mở và được sử dụng để giám sát mạng máy tính.

- câu lệnh ipvar HOME\_NET <ip/24>: là để chỉ sử dụng xác định mạng nội bộ mà bạn muốn Snort gián sát và phân tích gói tin đó.

2. Tạo rule cho Snort để phát hiện 3 dạng tấn công Với

- "any" đầu tiên: bất kì ip nguồn nào

- "any" thứ hai: bất kì cổng nguồn nòa

- Count: số lượng sự kiện diễn ra

- Seconds: thời gian để n(trong count n) sự kiện diễn ra

3. trong bài snort để làm gì? - Snort phát hiện có các gói Ping gửi đến

- Snort phát hiện có các gói tin rà quét trên cổng 80 (cổng sử dụng giao thức truyền thông HTTP)

- Snort phát hiện đang bị tấn công TCP SYN Flood

* **hping3**: là tên của công cụ được sử dụng để tạo các gói tin mạng tùy chỉnh.
* **-c 15000**: gửi 15000 gói tin.
* **-d 120**: đặt kích thước dữ liệu của gói tin thành 120 byte.
* **-S**: thiết lập cờ SYN trong gói tin. Cờ SYN được sử dụng trong quá trình thiết lập kết nối TCP.
* **-w 64**: đặt cửa sổ TCP của gói tin thành 64.
* **-p 80**: đặt cổng đích của gói tin thành 80. Trong trường hợp này, cuộc tấn công nhắm vào cổng 80, là cổng tiêu chuẩn cho giao thức HTTP.
* **--flood**: tạo ra một lượng lớn gói tin một cách nhanh chóng và liên tục.
* **--rand-source**: đặt địa chỉ nguồn của gói tin là nguồn ngẫu nhiên. Điều này nhằm mục đích che giấu địa chỉ IP thật của nguồn tấn công.
* **<địa chỉ IP máy Snort>**: đây là địa chỉ IP của máy tính mục tiêu, máy chạy Snort (một hệ thống phát hiện xâm nhập và giám sát gói tin mạng).

4. TCP SYN FLOOD là gì? - SYN flood (half-open attack) là một dạng của tấn công từ chối dịch vụ phân tán (DDoS). Là mối đe dọa thường trực đối với hệ thống mạng và máy chủ dịch vụ của các cơ quan và tổ chức. Bằng việc gửi liên tục các packet tin yêu cầu kết nối ban đầu (SYN). Loại tấn công ngày thường gây cạn kiệt tài nguyên hệ thống hoặc ngập lụt đường truyền, làm ngắt quãng quá trình cung cấp dịch vụ cho người dùng hợp pháp, hoặc thậm chí khiến cả hệ thống ngừng hoạt động.

Bài 7: (chưa ổn)

* Vpn Dùng để làm gì: VPN là virtual private network: là cài đặt mạng ảo cá nhân, dùng để thiết lập mạng ảo riêng khác với một mạng khác trên internet. VPN có thể tránh sự tò mò và thiết lập cơ chế an toàn chỉ những người có tài khoản và mật khẩu thì mới có thể vào.
* Các loại cơ bản trong VPN là: site –to –site và remote access VPN  
  site to side là gì nó tương tự như
* Sử dụng softEther VPN để thêm người đó vào mạng

Bài 8: bắt gói tin bằng Tcpdump và wireshark.

* 192.168.100 là mạng trong.
* 10.10.19 là mạng ngoài.
* Linux sniffer để bắt các gói tin mạng trong và ngoài
* tcpdump để làm gì? - Sử dụng tcpdump để bắt gói tin mạng. chỉ bắt được gói tin dạng pcap
* wireshark dùng để làm gì? – sử dụng được wireshark để bắt và phân tích gói tin mạng (HTTP/ HTTPS/FTP/TCP/IP).

Bài 9: Phân tích về file log hệ thống.

* Tìm hiểu về grep: phân tích log lệnh grep thường được sử dụng để tìm kiếm và lọc các dòng trong tệp dựa trên mẫu cụ thể.
* Gawk: là một công cụ mạnh mẽ được sử dụng trong phân tích và xử lý văn bản dựa trên quy tắc được xác định trước.
* Find: là thuật ngữ được sử dụng để chỉ việc tìm kiếm phân tích log hoặc mẫu cụ thể.
* xhydra: là công cụ trong lĩnh vực phân tích log và kiểm tra độ mạnh của hệ thống mật khẩu.

Bài 10: sao lưu hệ thống.

* SCP – Secure copy (SCP) là một phương tiện truyền tệp một cách an toàn giữa một máy chủ cục bộ và một máy chủ từ xa hoặc giữa hai máy chủ từ xa, dựa trên giao thức Secure Shell (SSH). Các tệp có thể được tải lên bằng giao thức SSH với SCP. Các tệp sẽ được mã hóa khi gửi qua mạng.
* FTP - Giao thức truyền tệp hay FTP cho phép người dùng truyền tệp từ máy này sang máy khác từ xa. Hạn chế của việc sử dụng FTP là dữ liệu được gửi dưới dạng văn bản không được mã hóa.
* Ổ đĩa mạng - Ổ đĩa mạng là bộ nhớ trên máy tính khác được gán ký tự ổ đĩa. Trong một số trường hợp, người dùng sẽ chỉ có quyền truy cập đọc vào ổ đĩa mạng, vì vậy họ sẽ không thể lưu trữ bất kỳ tệp nào. Nếu quyền ghi tồn tại, người dùng có thể lưu trữ tệp.
* Sao lưu hệ thống: sử dụng backup trên window server để thực hiện backup.

1. Sao lưu trên ổ đĩa mạng:

+) window server trở thành DC và máy attack kết nối đến và sử đụng để chia sẻ file.

+) thì ta sử dụng chia sẻ trong mạng nội bộ.

+) cài đặt ntbackup trong window server và

+) rồi ta chia sẻ và sao lưu lại

1. Sao lưu trên FTP thì ta share trong với cổng 21.

+) ban đầu cài trong mạng nội bộ thì máy window là client còn linux là server

+) sao lưu trên cổng 21

1. Sao lưu trên SCP:

+) ta sử dụng và sao lưu sử dụng openssh.

+) sử dụng trong

Bài 11: tìm kiếm và khai thác lỗ hoognr.

* Nmap/zenmap: Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Quét 135,139,445 tìm hiểu.
* Nessus: quét cổng 49153 và cổng 5355
* Dùng metasploit: quét cổng:

Bài 12: crack mật khẩu:

* Ta sử dụng join cho tài khoản bên linux
* Crack mật khẩu trên window thì ta sử dụng mimikatz và john the ripper để crack bên window.

Bài 13: đảm bảo an toàn mã hóa.à va

* TrueCrypt:
* là phần mềm mã hóa ở đĩa mã nguồn mở được sử dụng để bảo vệ dữ liệu trên ổ điĩa và thư muc trên máy tính.
* Cho phép mã hóa và phân vùng trên máy.
* Ta sao lưu khóa và sử dụng để giải mãi nó.

Bài 15:kết nối clienserver

Thuật toán kết nối client server:

Bài 16 code thuật toán RSA và thuật toán AES.

