Môn học: Thực tập cơ sở

Cho sinh viên ngành ATTT

I. Giới thiệu

Môn học **Thực tập cơ sở** có mục tiêu phát huy khả năng tổng hợp và ứng dụng các kiến thức trong Khối kiến thức Cơ sở ngành đã học của sinh viên ngành ATTT, từ đó vận dụng giải quyết một số bài toán thực tế, thông qua hình thức thực hiện các bài thí nghiệm thực hành. Qua đó, môn học cung cấp một số kinh nghiệm làm việc cơ bản của một chuyên viên quản trị hệ thống, đảm bảo an toàn cho hệ thống thông tin doanh nghiệp, giảm thiểu các mối đe dọa trong thế giới thực.

Nội dung thực tập bao gồm thực hành triển khai môi trường làm việc cho người dùng doanh nghiệp, khắc phục các sự cố thường gặp; triển khai các hệ thống và dịch vụ cho máy chủ, cấu hình an toàn cho máy chủ; triển khai các phần mềm đảm bảo an toàn hệ thống, rà quét phát hiện và xử lý một số mối đe dọa an ninh cơ bản.

Cụ thể, môn học này sẽ giúp sinh viên đạt được các kết quả sau:

- Rèn luyện kỹ năng quản trị hệ thống

- Rèn luyện kỹ năng cài đặt triển khai các công nghệ/kỹ thuật an toàn phổ biến

- Rèn luyện kỹ năng khắc phục sự cố, rà quét phát hiện lỗ hổng.

II. Mục tiêu và nội dung chi tiết

1. Rèn luyện kỹ năng quản trị hệ thống

1.1 Mục đích, yêu cầu

- Thành thạo việc cài đặt và quản trị hệ điều hành và các dịch vụ cơ bản của hệ điều hành (Windows/Linux)

1.2 Nội dung

- Cài đặt, cấu hình Windows 8, Windows 10, 11
- Cài đặt, cấu hình Windows Server 2012/2019 (kèm các dịch vụ)
- Cài đặt, cấu hình Ubuntu desktop, Ubuntu server, CentOS server (kèm các dịch vụ)

2. Rèn luyện kỹ năng cài đặt triển khai các công nghệ/kỹ thuật An toàn phổ biến

2.1 Mục đích, yêu cầu

- Thành thạo việc cài đặt và triển khai ứng dụng các công nghệ An toàn thông tin phổ biến

2.2 Nội dung

- Cài đặt, cấu hình Firewall
- Cài đặt, triển khai IDS (host-based và network-based)
- Cài đặt, cấu hình VPN
- Cài đặt, cấu hình Honeynet/honeypot

- Cài đặt cấu hình an toàn cho hệ điều hành: SSH, Fail2Ban, kiểm soát truy cập (SELinux / windows policy), phần mềm diệt virus/malware, …
- Cài đặt, triển khai các công cụ mã hóa để đảm bảo an toàn dữ liệu

3. Rèn luyện kỹ năng nâng cao: khắc phục sự cố, rà quét phát hiện lỗ hổng

3.1 Mục đích, yêu cầu

- Sử dụng thành thạo một số công cụ cơ bản khắc phục sự cố
- Biết cách sử dụng một số công cụ cho rà quét, phân tích điểm yếu, lỗ hổng,

3.2 Nội dung

- Tạo và sử dụng đĩa/usb khởi động cho khắc phục lỗi và rà quét mã độc
- Khắc phục sự cố (không khởi động được, xử lý khi máy bị nhiễm virus)
- Cài đặt và cấu hình các công cụ rà quét mã độc
- Rà quét hệ thống tìm thông tin và lỗ hổng sử dụng các công cụ (nmap, nessus,...)
- Cài đặt lab cho thử nghiệm thực hành ATTT: cấu hình mạng doanh nghiệp (mô phỏng với các vùng LAN. WAN, DMZ) dựa trên VMware hay docker, cấu hình hệ thống tường lửa cho mạng, hoặc IDS cho mạng, có các server DNS, DHCP, FTP, máy tính bảo mật kém, ứng dụng web có lỗi bảo mật.
- Sử dụng wireshark để bắt và phân tích gói tin (đơn giản)
- Phân tích Syslog, Web log, ...
- Phân tích tấn công dùng wireshark

4. Rèn luyện kỹ năng lập trình

3.1 Mục đích, yêu cầu

- Sử dụng thành thạo các kỹ thuật lập trình để giải quyết các bài toán cụ thể
- Các nền tảng ngôn ngữ lập trình gồm: C/C++, Java, Python

3.2 Nội dung

- Lập trình client/ server để trao đổi thông điệp
- Lập trình client/server để trao đổi khóa đơn giản
- Lập trình 1 thuật toán mật mã như SHA2, AES, hoặc RSA (với số lớn)

III. Chi tiết các bài thực hành

1. Yêu cầu chung:

- Để đủ điều kiện đạt cho môn học, sinh viên cần làm >= 50% số bài trong mỗi nhóm kỹ năng, và tổng số bài >=10 (bài).
- Giảng viên mỗi đầu tuần cung cấp bài, cuối tuần kiểm tra
- Để dễ kiểm tra kết quả đạt được, các bài đều nên có phần cá nhân hóa (tên máy, tên user, tên dịch vụ,...) có liên quan đến tên sinh viên, mã sinh viên.

2. Mô tả các bài thực hành

Dưới đây mô tả 1 số bài thực hành, cần triển khai chi tiết hơn về nội dung thực hành. Cách mô tả chi tiết các bài thực hành có thể xem theo mẫu trong phần phụ lục.

STT	Tên bài	Mục đích	Nhóm kỹ năng	Kết quả cần đạt
Bài 1:	Cài đặt hệ điều hành máy trạm Windows	Rèn luyện kỹ năng cài đặt và quản trị HĐH máy trạm Windows cho người dùng với các dịch vụ cơ bản	1	1. Môi trường Windows desktop có tên người dùng riêng, có tường lửa và phần mềm diệt virus. 2. Tạo, sử dụng đĩa cứu hộ để xử lý hệ thống Windows lỗi/có virus
Bài 2:	Cài đặt hệ điều hành máy trạm Linux	Rèn luyện kỹ năng cài đặt và quản trị HĐH máy trạm Linux cho người dùng với các dịch vụ cơ bản	1	1. Môi trường Ubuntu có tên người dùng riêng, có tường lửa và phần mềm diệt virus 2. Thực hành được một số lệnh cơ bản trên Ubuntu. Ví dụ: sudo, pwd, ls, man, PS1, mkdir, cd, cp, mv, rm, rmdir, cat, more, head, tail, grep, wc, clear, echo, >, >> (append), cat, sort, uniq.
Bài 3:	Cài đặt, cấu hình Ubuntu Server	Rèn luyện kỹ năng cài đặt và quản trị HĐH máy chủ Linux server với các dịch vụ cơ bản	1	1. Môi trường Ubuntu Server đã cài đặt các dịch vụ tường lửa, SSH, có tài khoản người dùng quyền root. 2. Cài đặt và cấu hình Samba để chia sẻ file 3. Cài đặt cấu hình được SELinux
Bài 4:	Cài đặt, cấu hình Windows Server 2012/2019	Rèn luyện kỹ năng cài đặt và quản trị HĐH máy chủ Windows server	1	1. Môi trường Windows Server có tài khoản người dùng quyền domain/admin. 2. Cài đặt tường lửa 3. Cài đặt các dịch vụ Web server, FTP server

		với các dịch vụ cơ bản		4. Cấu hình Remote Desktop Users để truy cập từ xa qua giao diện đồ họa và truy nhập bằng dòng lệnh từ xa với psexec
Bài 5:	Cài đặt, cấu hình mạng doanh nghiệp với pfsense firewall	Cài đặt mô phỏng mạng doanh nghiệp với tường lửa để kiểm soát truy cập	2	1. Hiểu về Vmware/ Virtual box network 2. Hoàn thành thiết kế, cài đặt một mạng doanh nghiệp trong Vmware/Virtual box 3. Cài đặt cấu hình pfsense firewall trong mạng 4. Thử nghiệm cấu hình 1 số luật cho pfsense firewall
Bài 6:	Cài đặt cấu hình HIDS/NIDS	Triển khai hệ thống IDS trên server (OSSEC/Zeek/ Snort/Suricata)	2	1. Cài đặt được IDS trên server 2. Cấu hình được IDS
Bài 7:	Cài đặt cấu hình VPN server	Triển khai hệ thống VPN trên server	2	1. Cài đặt được VPN server 2. Cấu hình được VPN server
Bài 8:	Bắt dữ liệu mạng	Sử dụng các công cụ để bắt gói tin trên mạng	3	1. Sử dụng tcpdump để bắt gói tin mạng 2. Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP / TCP/IP) 3. Sử dụng Network Miner để bắt và phân tích gói tin mạng
Bài 9:	Phân tích log hệ thống	Nắm được các công cụ và cách phân tích log hệ thống	3	1. Phân tích log sử dụng grep/gawk trong Linux 2. Phân tích log sử dụng find trong Windows 3. Tìm hiểu về Windows Event Viewer và auditing

				4. Phân tích event log trong Windows
Bài 10:	Sao lưu hệ thống	Nắm được công cụ và cách thức sao lưu hệ thống	3	1. Sao lưu hệ thống tới ổ đĩa mạng 2. Sao lưu file lên FTP server 3. Sao lưu file sử dụng SCP
Bài 11:	Tìm kiếm và khai thác lỗ hổng	Hiểu được các mối đe dọa, lỗ hổng và biết cách sử dụng công cụ để phát hiện, khai thác chúng	3	1. Sử dụng nmap/zenmap để quét các cổng dịch vụ 2. Sử dụng nessus để quét các lỗ hổng 3. Thử nghiệm với Metasploit framework để khai thác lỗ hổng
Bài 12:	Crack mật khẩu	Hiểu được mối đe dọa về tấn công mật khẩu	3	1. Crack mật khẩu Linux 2. Crack mật khẩu Windows
Bài 13:	Đảm bảo an toàn với mã hóa	Biết sử dụng các công cụ mã hóa để đảm bảo an toàn dữ liệu	3	1. Cài đặt và sử dụng TrueCrypt 2. Mã hóa với hệ thống file mã hóa 3. Sao lưu khóa của hệ thống file mã hóa 4. Khôi phục hệ thống file mã hóa
Bài 14:	Phát hiện lỗ hổng với công cụ tìm kiếm	Hiểu được mối đe dọa đến từ các công cụ tìm kiếm	3	1. Tìm kiếm lỗ hổng sử dụng Shodan 2. Tìm kiếm lỗ hổng với Google Hacking
Bài 15:	Lập trình client/server để trao đổi thông tin an toàn	Sinh viên tự lập trình client/server dựa trên socket và trao đổi thông tin đảm bảo an toàn	4	1. Lập trình client/server dựa trên socket 2. Trao đổi thông điệp giữa client và server đảm bảo tính toàn vẹn

Bài 16:	Lập trình thuật toán mật mã học	Tự tìm hiểu và lập trình được một thuật toán mật mã cụ thể và chạy được số lớn	4	1. Lập trình chương trình mã hóa, giải mã