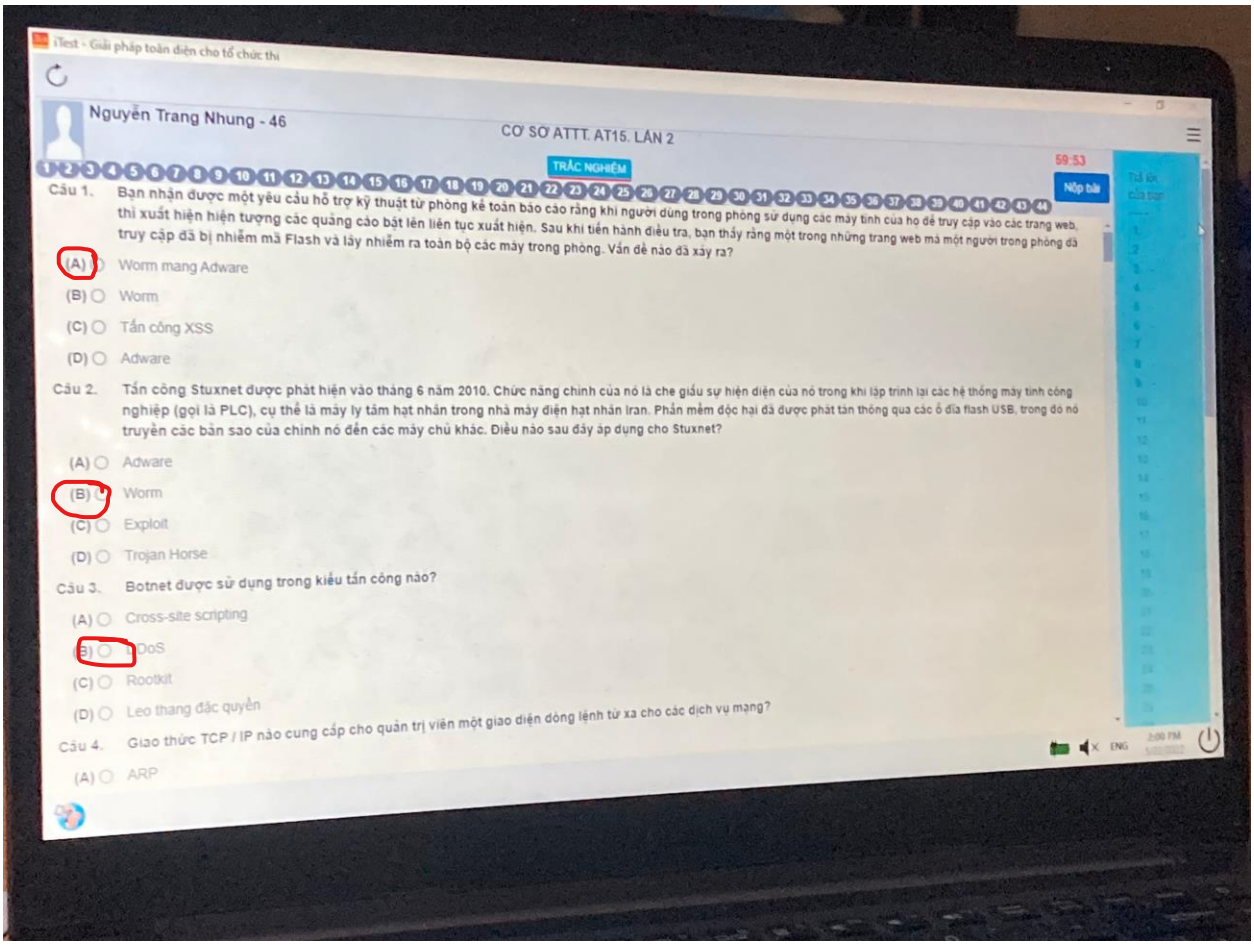
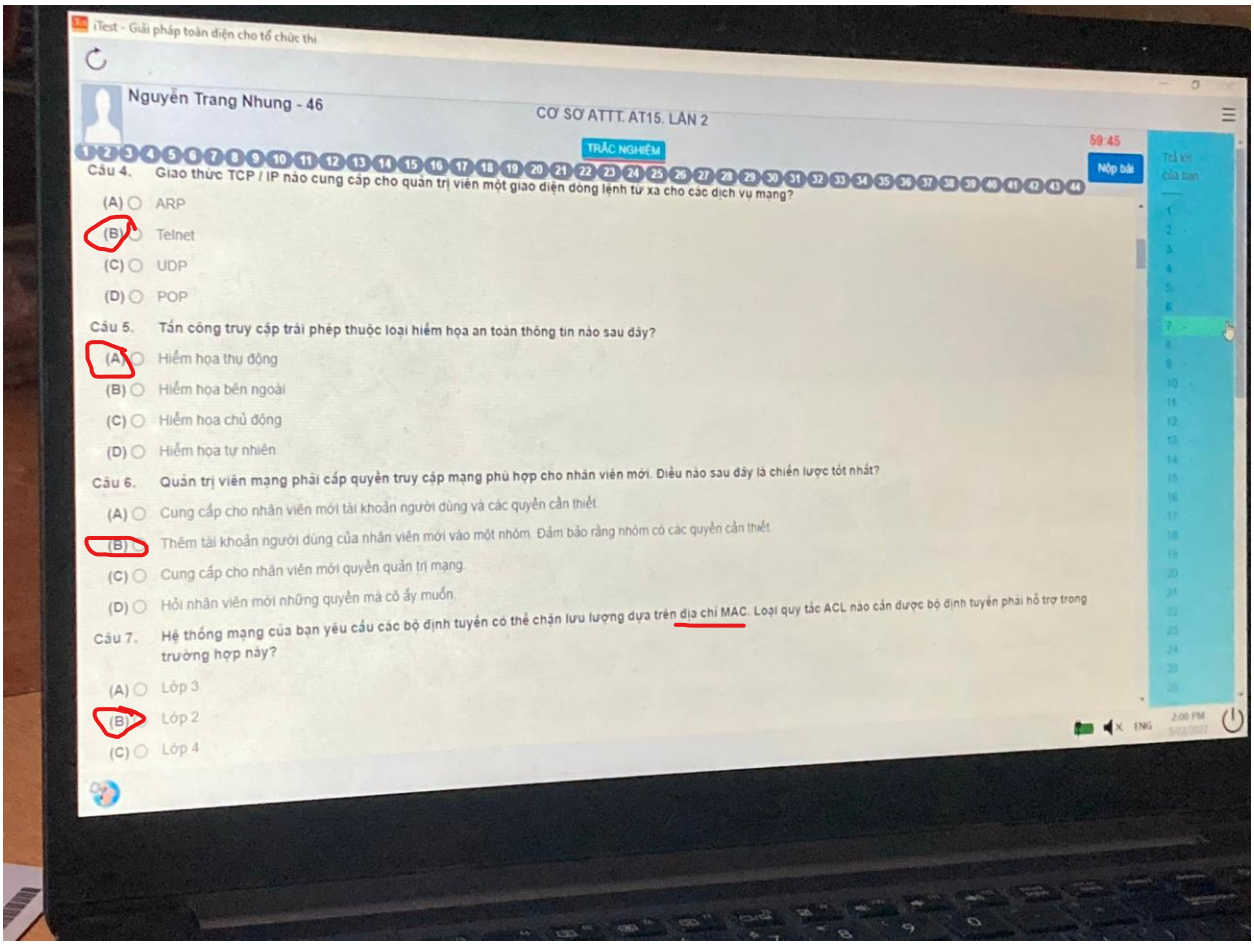
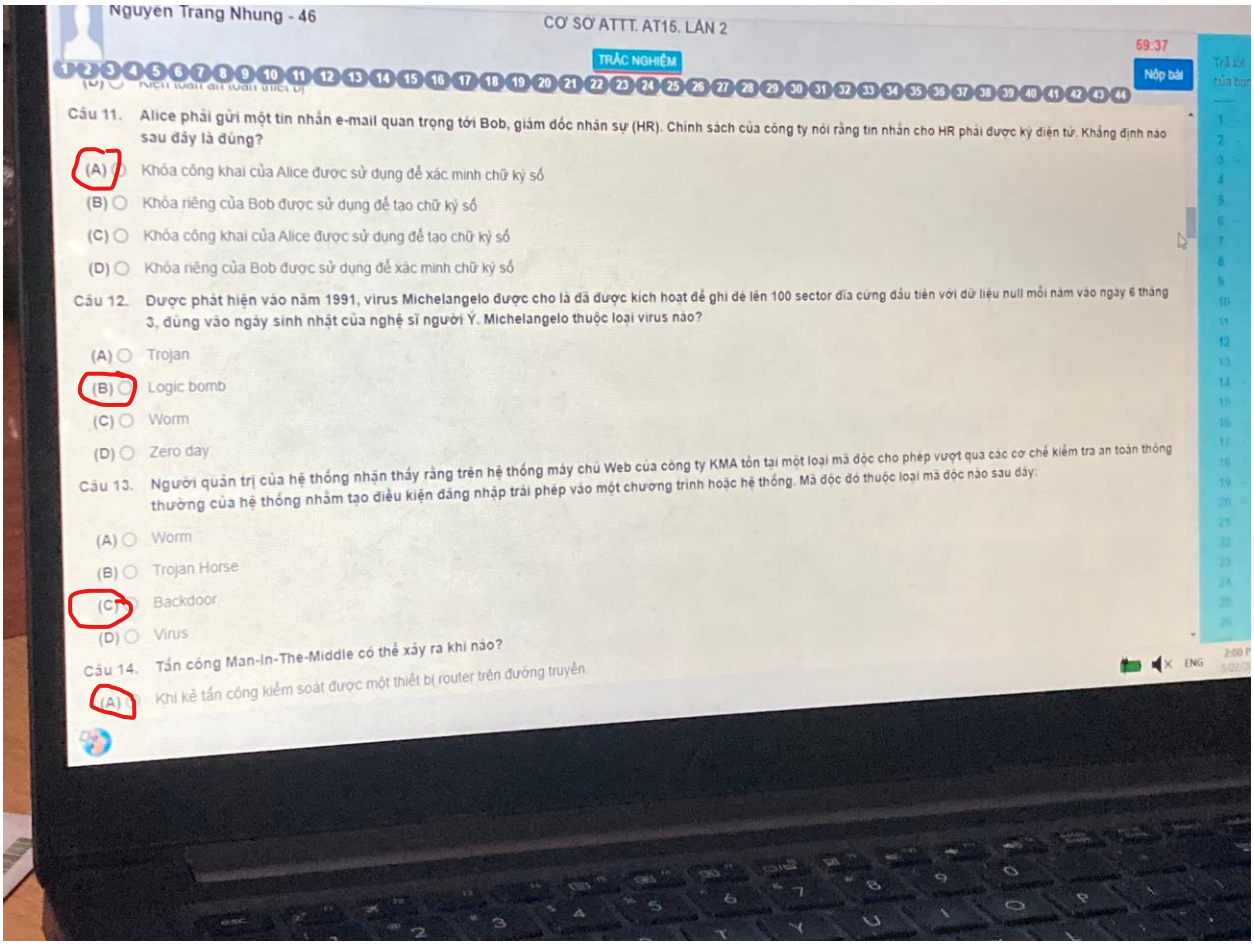
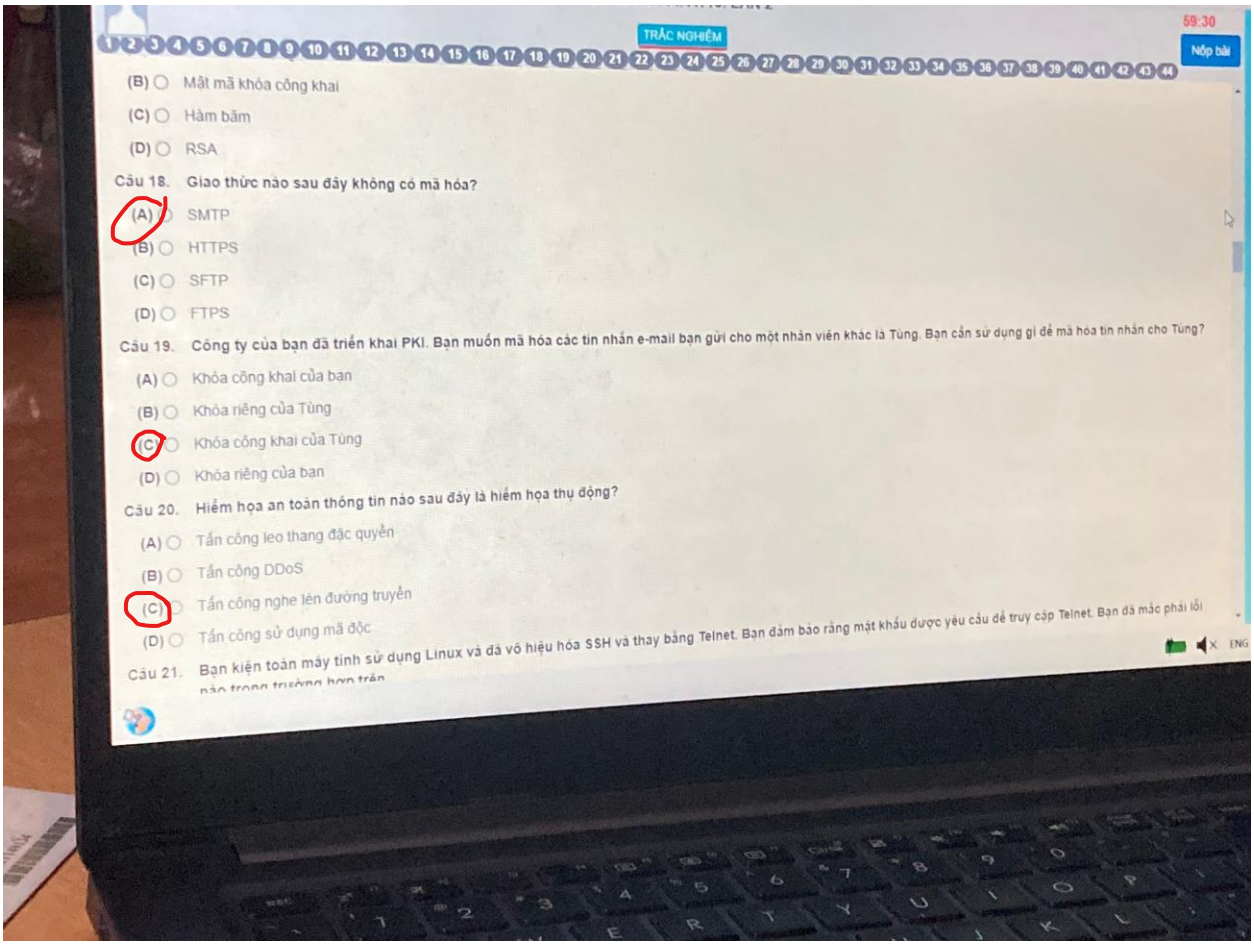
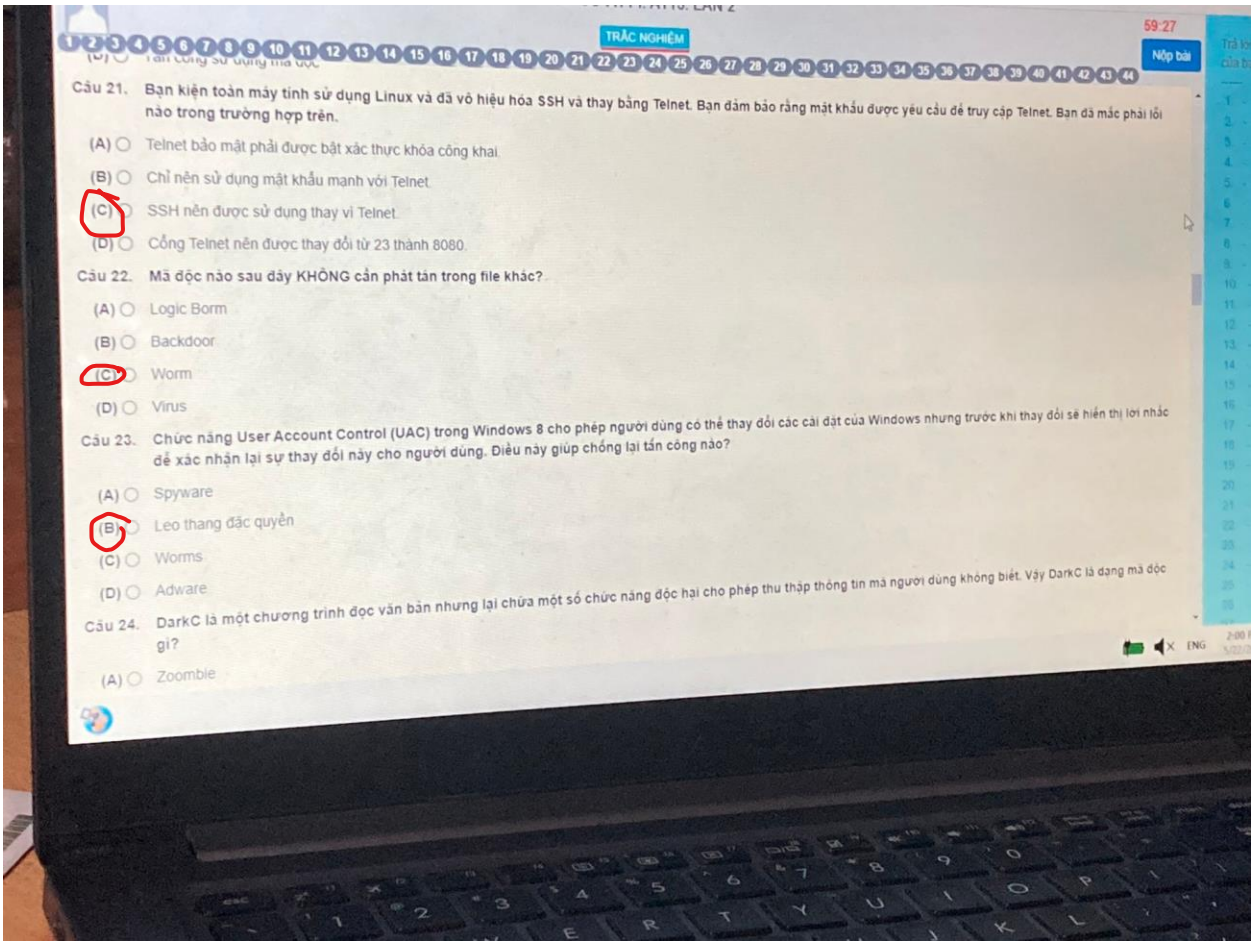
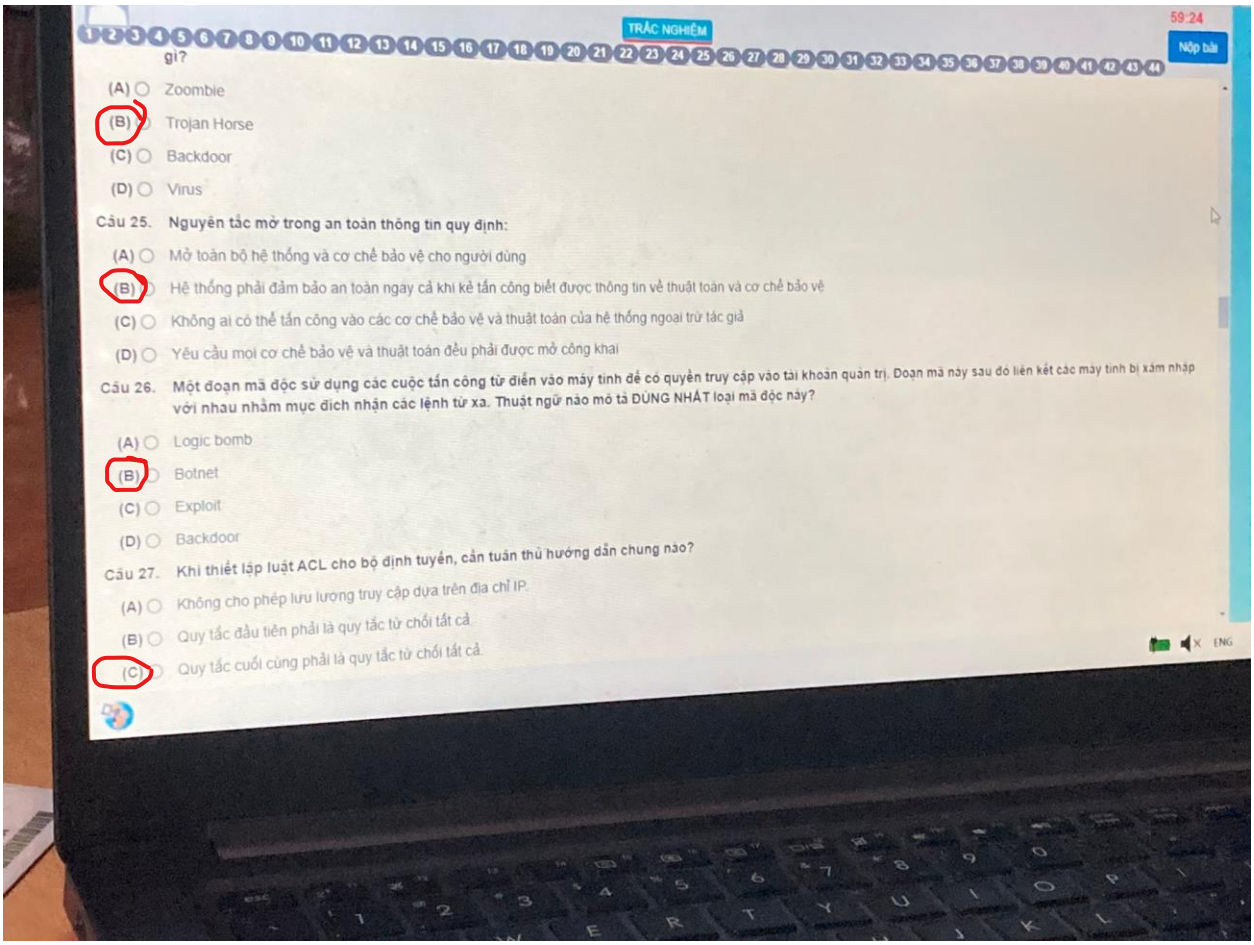

iTest - Giải pháp toàn diện cho tổ chức thi
Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
59:53
Nộp bài
Câu 1. Bạn nhận được một yêu cầu hỗ trợ kỹ thuật từ phòng kế toán báo cáo rằng khi người dùng trong phòng sử dụng các máy tính của họ để truy cập vào các trang web, thì xuất hiện hiện tượng các quảng cáo bật lên liên tục xuất hiện. Sau khi tiến hành điều tra, bạn thấy rằng một trong những trang web mà một người trong phòng đã truy cập đã bị nhiễm mã Flash và lây nhiễm ra toàn bộ các máy trong phòng. Vấn đề nào đã xảy ra?
(A) Worm mang Adware
(B) Worm
(C) Tấn công XSS
(D) Adware
Câu 2. Tấn công Stuxnet được phát hiện vào tháng 6 năm 2010. Chức năng chính của nó là che giấu sự hiện diện của nó trong khi lập trình lại các hệ thống máy tính công nghiệp (gọi là PLC), cụ thể là máy ly tâm hạt nhân trong nhà máy điện hạt nhân Iran. Phần mềm độc hại đã được phát tán thông qua các ổ đĩa flash USB, trong đó nó truyền các bản sao của chính nó đến các máy chủ khác. Điều nào sau đây áp dụng cho Stuxnet?
(A) Adware
(B) Worm
(C) Exploit
(D) Trojan Horse
Câu 3. Botnet được sử dụng trong kiểu tấn công nào?
(A) Cross-site scripting
(B) DoS
(C) Rootkit
(D) Leo thang đặc quyền
Câu 4. Giao thức TCP / IP nào cung cấp cho quản trị viên một giao diện dòng lệnh từ xa cho các dịch vụ mạng?
(A) ARP
ENG

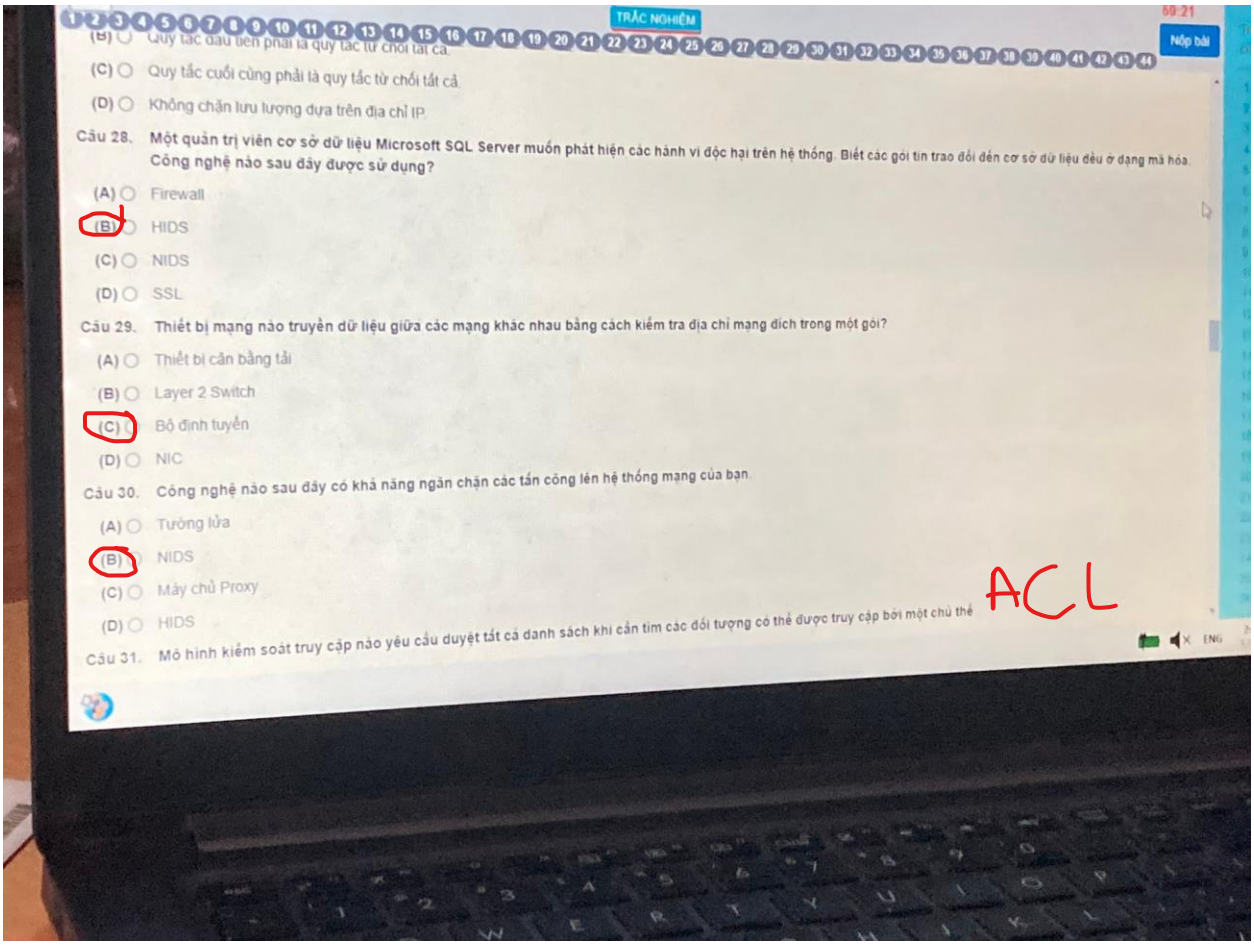

iTest - Giải pháp toàn diện cho tổ chức thi
Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
59:45
Nộp bài
Câu 4. Giao thức TCP / IP nào cung cấp cho quản trị viên một giao diện dòng lệnh từ xa cho các dịch vụ mạng?
(A) ARP
(B) Telnet
(C) UDP
(D) POP
Câu 5. Tấn công truy cập trái phép thuộc loại hiểm họa an toàn thông tin nào sau đây?
(A) Hiểm họa thụ động
(B) Hiểm họa bên ngoài
(C) Hiểm họa chủ động
(D) Hiểm họa tự nhiên
Câu 6. Quản trị viên mạng phải cấp quyền truy cập mạng phù hợp cho nhân viên mới. Điều nào sau đây là chiến lược tốt nhất?
(A) Cung cấp cho nhân viên mới tài khoản người dùng và các quyền cần thiết.
(B) Thêm tài khoản người dùng của nhân viên mới vào một nhóm. Đảm bảo rằng nhóm có các quyền cần thiết.
(C) Cung cấp cho nhân viên mới quyền quản trị mạng.
(D) Hỏi nhân viên mới những quyền mà cô ấy muốn.
Câu 7. Hệ thống mạng của bạn yêu cầu các bộ định tuyến có thể chặn lưu lượng dựa trên địa chỉ MAC. Loại quy tắc ACL nào cần được bộ định tuyến phải hỗ trợ trong trường hợp này?
(A) Lớp 3
(B) Lớp 2
(C) Lớp 4

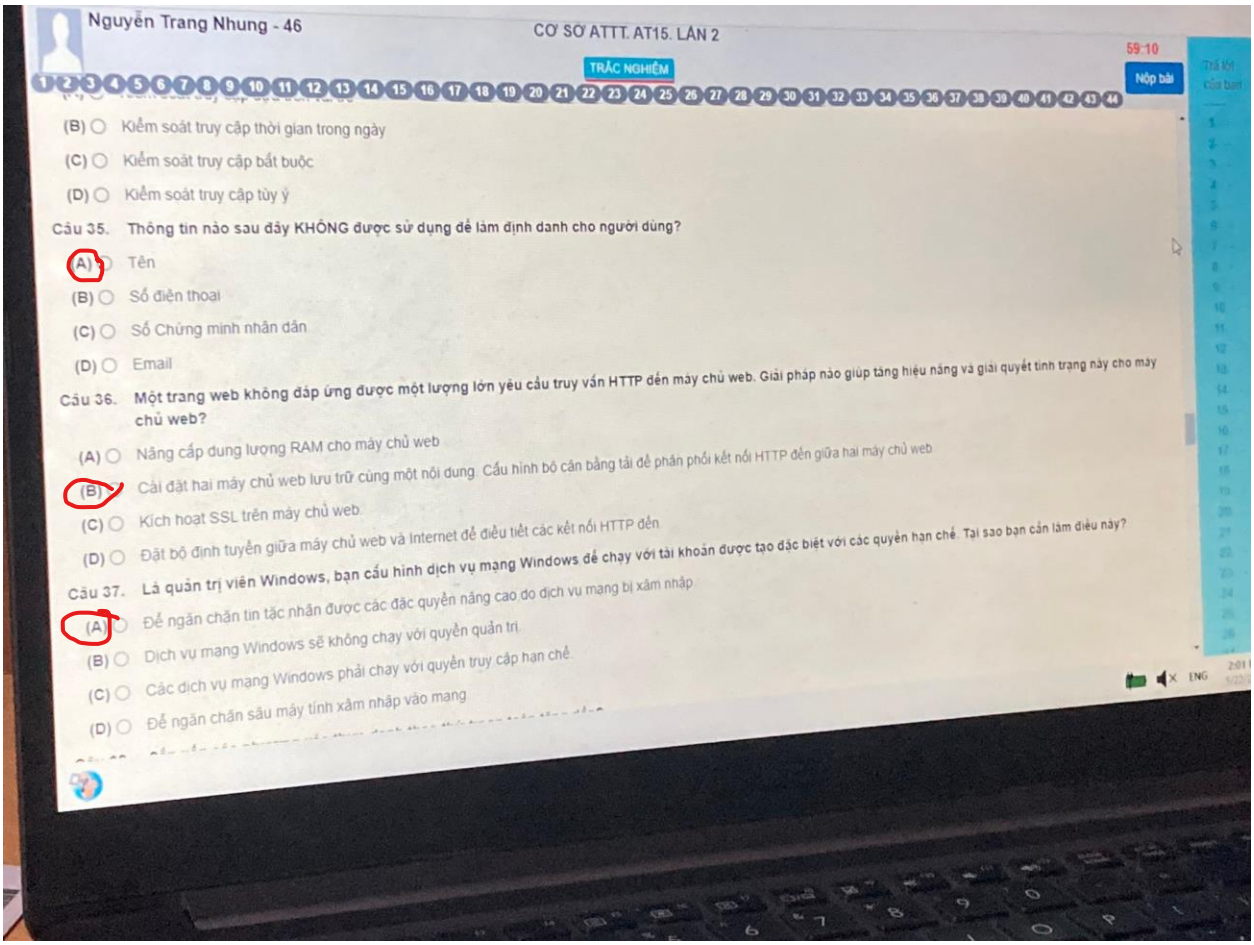

Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
59:37
Nộp bài
Câu 11. Alice phải gửi một tin nhắn e-mail quan trọng tới Bob, giám đốc nhân sự (HR). Chính sách của công ty nói rằng tin nhắn cho HR phải được ký điện tử. Khẳng định nào sau đây là đúng?
(A) Khóa công khai của Alice được sử dụng để xác minh chữ ký số
(B) Khóa riêng của Bob được sử dụng để tạo chữ ký số
(C) Khóa công khai của Alice được sử dụng để tạo chữ ký số
(D) Khóa riêng của Bob được sử dụng để xác minh chữ ký số
Câu 12. Được phát hiện vào năm 1991, virus Michelangelo được cho là đã được kích hoạt để ghi đè lên 100 sector đĩa cứng đầu tiên với dữ liệu null mỗi năm vào ngày 6 tháng 3, đúng vào ngày sinh nhật của nghệ sĩ người Ý. Michelangelo thuộc loại virus nào?
(A) Trojan
(B) Logic bomb
(C) Worm
(D) Zero day
Câu 13. Người quản trị của hệ thống nhận thấy rằng trên hệ thống máy chủ Web của công ty KMA tồn tại một loại mã độc cho phép vượt qua các cơ chế kiểm tra an toàn thông thường của hệ thống nhằm tạo điều kiện đăng nhập trái phép vào một chương trình hoặc hệ thống. Mã độc đó thuộc loại mã độc nào sau đây:
(A) Worm
(B) Trojan Horse
(C) Backdoor
(D) Virus
Câu 14. Tấn công Man-In-The-Middle có thể xảy ra khi nào?
(A) Khi kẻ tấn công kiểm soát được một thiết bị router trên đường truyền
ENG

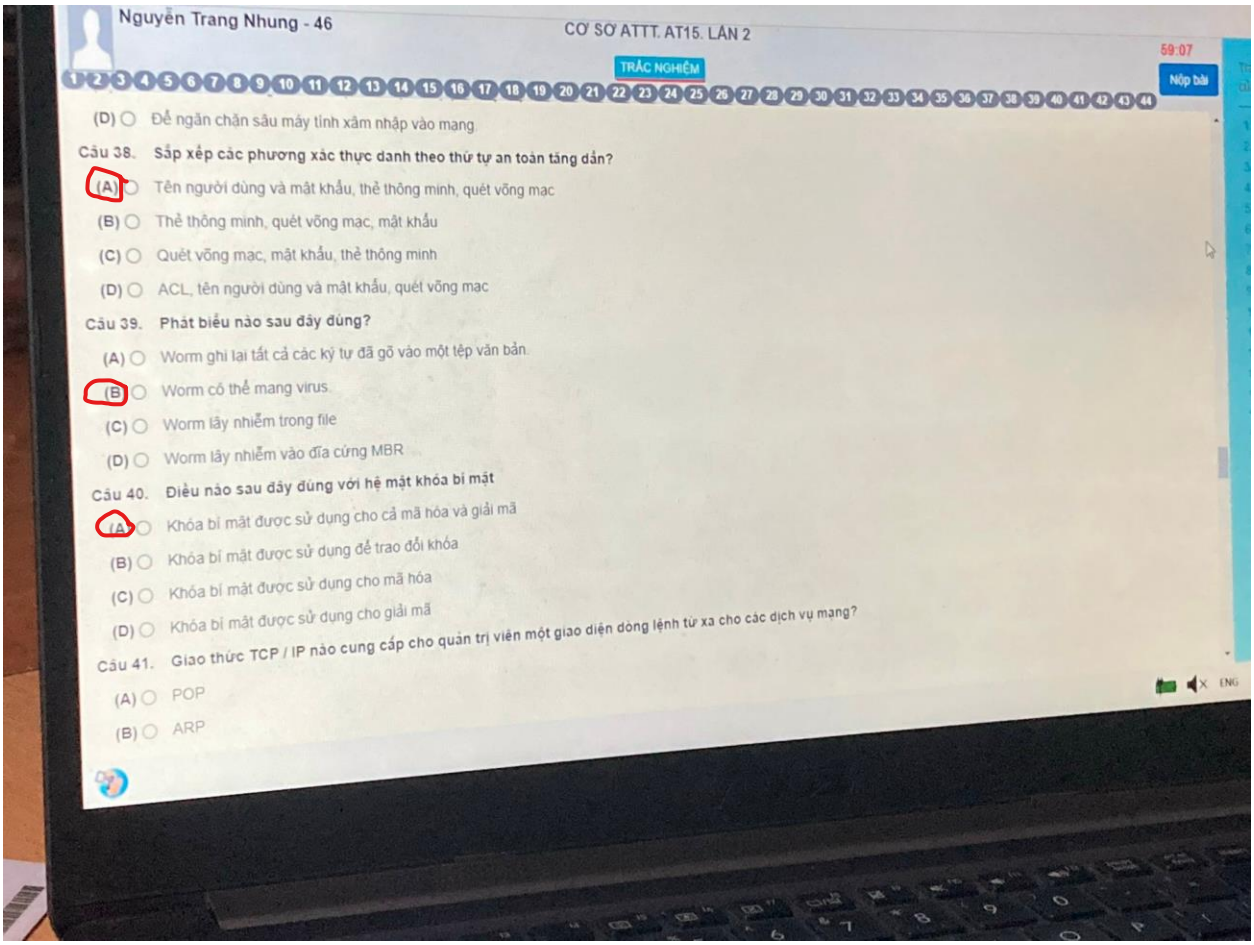

TRẮC NGHIỆM
59:30
Nộp bài
(B) Mật mã khóa công khai
(C) Hàm băm
(D) RSA
Câu 18. Giao thức nào sau đây không có mã hóa?
(A) SMTP
(B) HTTPS
(C) SFTP
(D) FTPS
Câu 19. Công ty của bạn đã triển khai PKI. Bạn muốn mã hóa các tin nhắn e-mail bạn gửi cho một nhân viên khác là Tùng. Bạn cần sử dụng gì để mã hóa tin nhắn cho Tùng?
(A) Khóa công khai của bạn
(B) Khóa riêng của Tùng
(C) Khóa công khai của Tùng
(D) Khóa riêng của bạn
Câu 20. Hiểm họa an toàn thông tin nào sau đây là hiểm họa thụ động?
(A) Tấn công leo thang đặc quyền
(B) Tấn công DDoS
(C) Tấn công nghe lén đường truyền
(D) Tấn công sử dụng mã độc
Câu 21. Bạn kiện toàn máy tính sử dụng Linux và đã vô hiệu hóa SSH và thay bằng Telnet. Bạn đảm bảo rằng mật khẩu được yêu cầu để truy cập Telnet. Bạn đã mắc phải lỗi
ENG

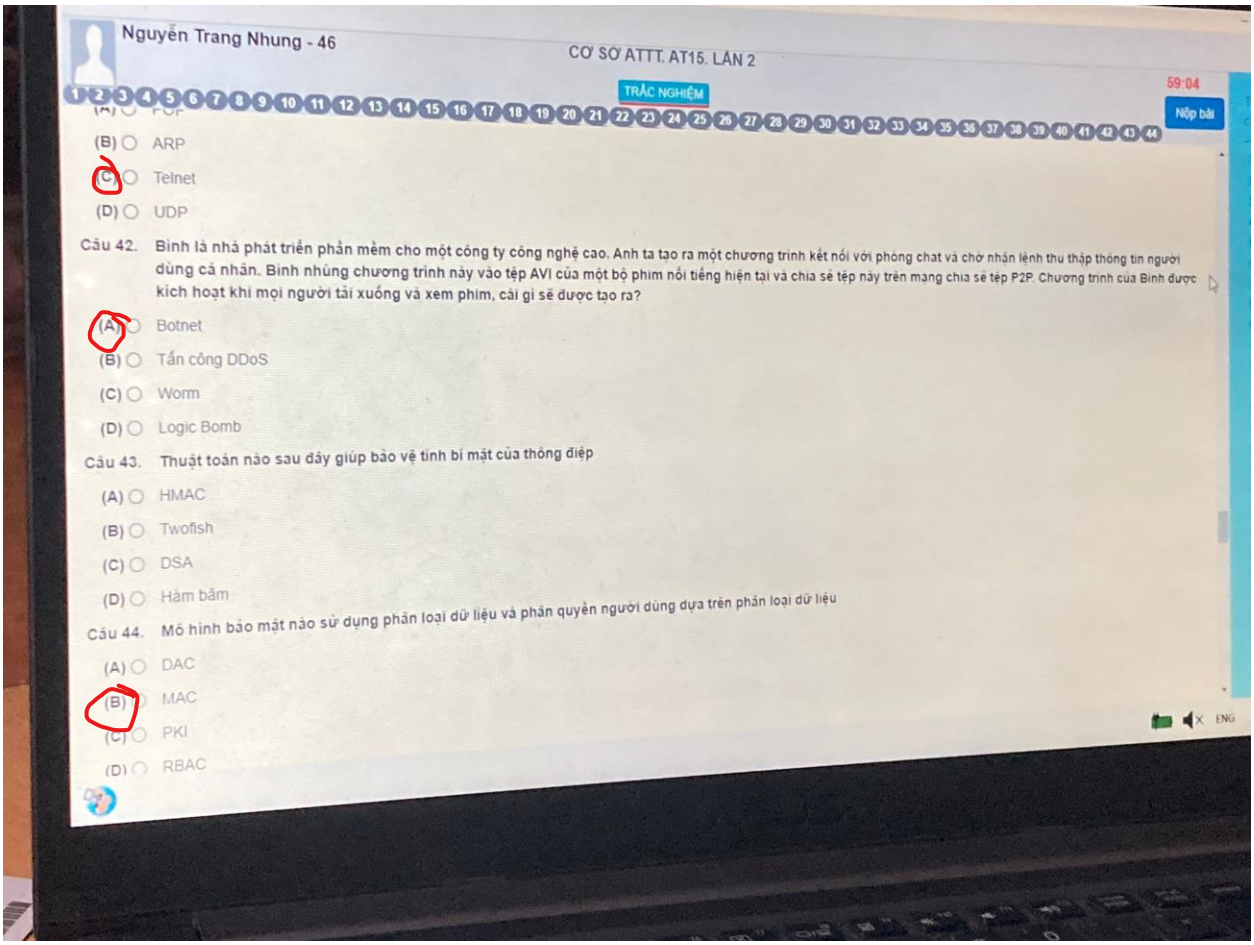

TRẮC NGHIỆM
59:27
Nộp bài
Câu 21. Bạn kiện toàn máy tính sử dụng Linux và đã vô hiệu hóa SSH và thay bằng Telnet. Bạn đảm bảo rằng mật khẩu được yêu cầu để truy cập Telnet. Bạn đã mắc phải lỗi nào trong trường hợp trên.
(A) Telnet bảo mật phải được bật xác thực khóa công khai.
(B) Chỉ nên sử dụng mật khẩu mạnh với Telnet.
(C) SSH nên được sử dụng thay vì Telnet.
(D) Cổng Telnet nên được thay đổi từ 23 thành 8080.
Câu 22. Mã độc nào sau đây KHÔNG cần phát tán trong file khác?
(A) Logic Borm
(B) Backdoor
(C) Worm
(D) Virus
Câu 23. Chức năng User Account Control (UAC) trong Windows 8 cho phép người dùng có thể thay đổi các cài đặt của Windows nhưng trước khi thay đổi sẽ hiển thị lời nhắc để xác nhận lại sự thay đổi này cho người dùng. Điều này giúp chống lại tấn công nào?
(A) Spyware
(B) Leo thang đặc quyền
(C) Worms
(D) Adware
Câu 24. DarkC là một chương trình đọc văn bản nhưng lại chứa một số chức năng độc hại cho phép thu thập thông tin mà người dùng không biết. Vậy DarkC là dạng mã độc gì?
(A) Zoombie
ENG

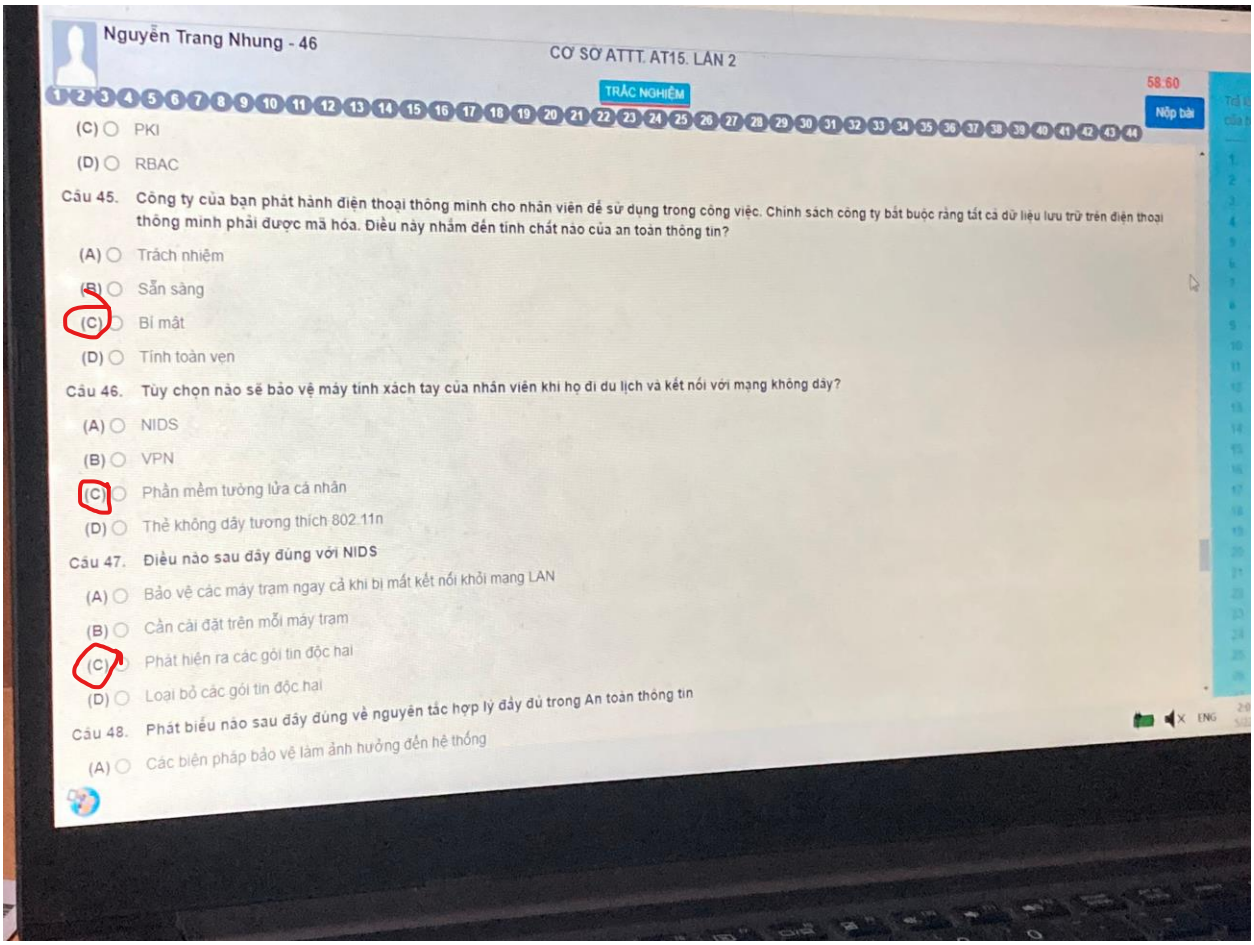

TRẮC NGHIỆM
59:24
Nộp bài
gì?
(A) Zoombie
(B) Trojan Horse
(C) Backdoor
(D) Virus
Câu 25. Nguyên tắc mở trong an toàn thông tin quy định:
(A) Mở toàn bộ hệ thống và cơ chế bảo vệ cho người dùng
(B) Hệ thống phải đảm bảo an toàn ngay cả khi kẻ tấn công biết được thông tin về thuật toán và cơ chế bảo vệ
(C) Không ai có thể tấn công vào các cơ chế bảo vệ và thuật toán của hệ thống ngoại trừ tác giả
(D) Yêu cầu mọi cơ chế bảo vệ và thuật toán đều phải được mở công khai
Câu 26. Một đoạn mã độc sử dụng các cuộc tấn công từ điển vào máy tính để có quyền truy cập vào tài khoản quản trị. Đoạn mã này sau đó liên kết các máy tính bị xâm nhập với nhau nhằm mục đích nhận các lệnh từ xa. Thuật ngữ nào mô tả ĐÚNG NHẤT loại mã độc này?
(A) Logic bomb
(B) Botnet
(C) Exploit
(D) Backdoor
Câu 27. Khi thiết lập luật ACL cho bộ định tuyến, cần tuân thủ hướng dẫn chung nào?
(A) Không cho phép lưu lượng truy cập dựa trên địa chỉ IP.
(B) Quy tắc đầu tiên phải là quy tắc từ chối tất cả.
(C) Quy tắc cuối cùng phải là quy tắc từ chối tất cả.
ENG

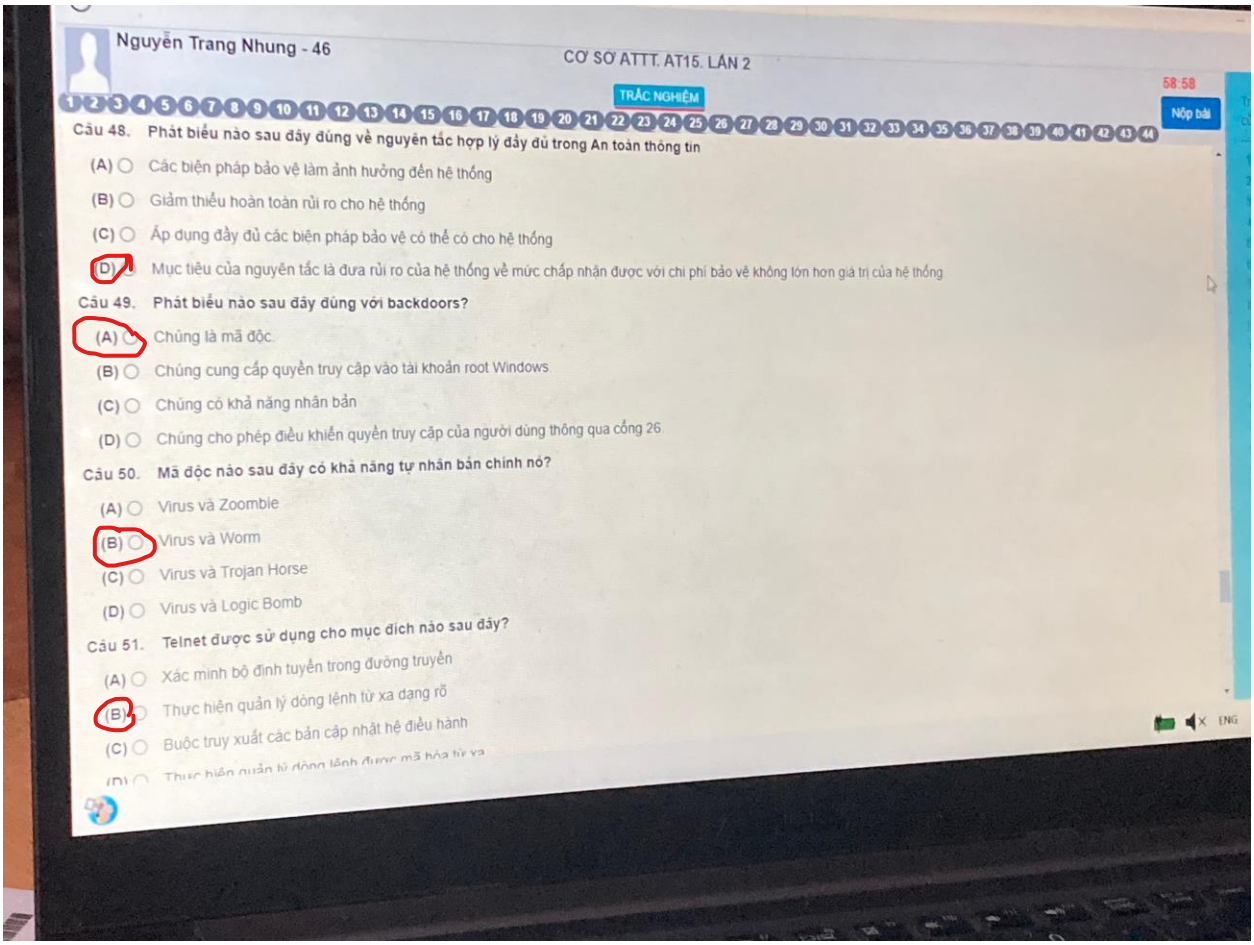

TRẮC NGHIỆM
Nộp bài
(C) Quy tắc cuối cùng phải là quy tắc từ chối tất cả.
(D) Không chặn lưu lượng dựa trên địa chỉ IP.
Câu 28. Một quản trị viên cơ sở dữ liệu Microsoft SQL Server muốn phát hiện các hành vi độc hại trên hệ thống. Biết các gói tin trao đổi đến cơ sở dữ liệu đều ở dạng mã hóa. Công nghệ nào sau đây được sử dụng?
(A) Firewall
(B) HIDS
(C) NIDS
(D) SSL
Câu 29. Thiết bị mạng nào truyền dữ liệu giữa các mạng khác nhau bằng cách kiểm tra địa chỉ mạng đích trong một gói?
(A) Thiết bị cân bằng tải
(B) Layer 2 Switch
(C) Bộ định tuyến
(D) NIC
Câu 30. Công nghệ nào sau đây có khả năng ngăn chặn các tấn công lên hệ thống mạng của bạn.
(A) Tường lửa
(B) NIDS
(C) Máy chủ Proxy
(D) HIDS
Câu 31. Mô hình kiểm soát truy cập nào yêu cầu duyệt tất cả danh sách khi cần tìm các đối tượng có thể được truy cập bởi một chủ thể
ACL

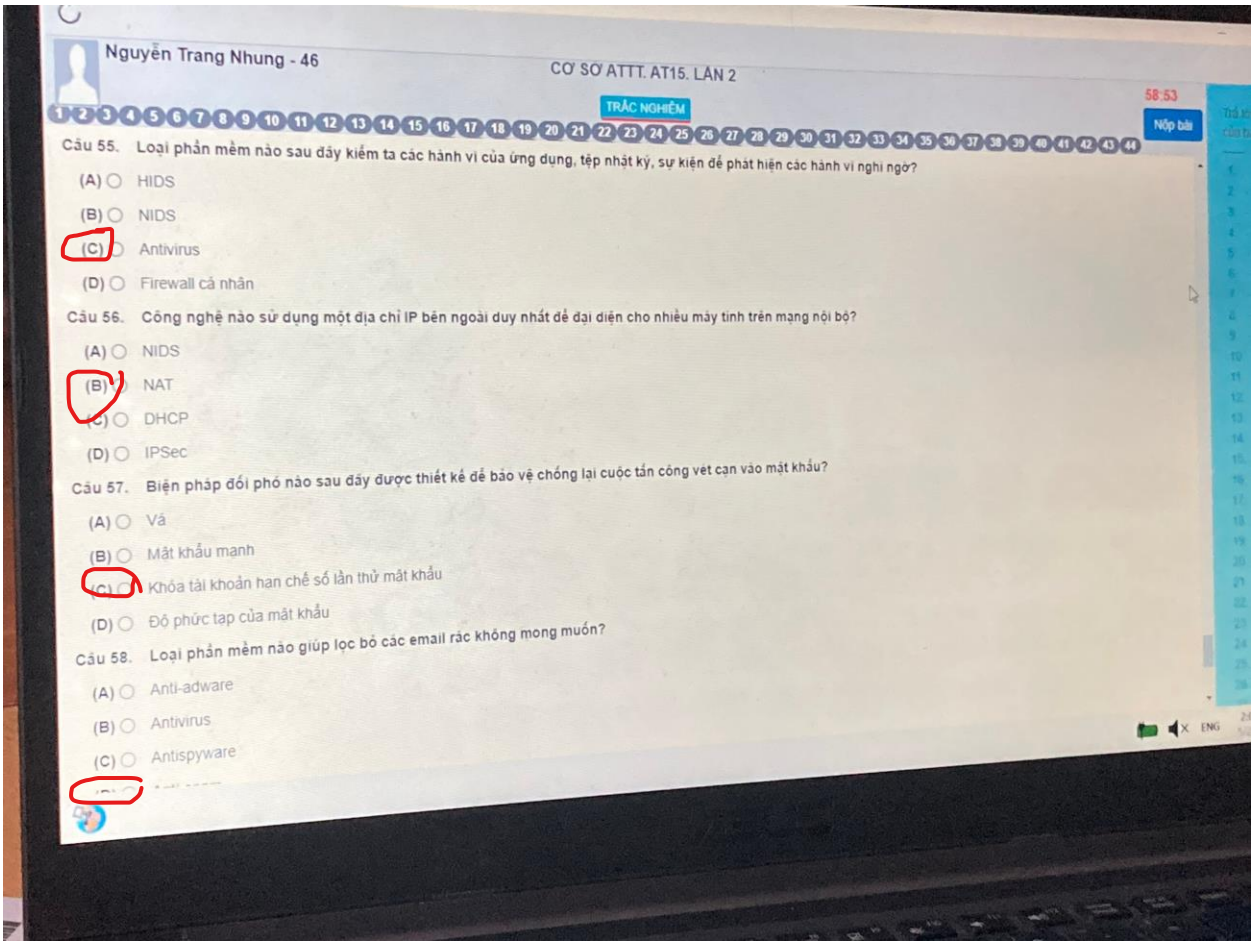

Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
59:10
TRẮC NGHIỆM
Nộp bài
(B) Kiểm soát truy cập thời gian trong ngày
(C) Kiểm soát truy cập bắt buộc
(D) Kiểm soát truy cập tùy ý
Câu 35. Thông tin nào sau đây KHÔNG được sử dụng để làm định danh cho người dùng?
(A) Tên
(B) Số điện thoại
(C) Số Chứng minh nhân dân
(D) Email
Câu 36. Một trang web không đáp ứng được một lượng lớn yêu cầu truy vấn HTTP đến máy chủ web. Giải pháp nào giúp tăng hiệu năng và giải quyết tình trạng này cho máy chủ web?
(A) Nâng cấp dung lượng RAM cho máy chủ web
(B) Cài đặt hai máy chủ web lưu trữ cùng một nội dung. Cấu hình bộ cân bằng tải để phân phối kết nối HTTP đến giữa hai máy chủ web
(C) Kích hoạt SSL trên máy chủ web.
(D) Đặt bộ định tuyến giữa máy chủ web và Internet để điều tiết các kết nối HTTP đến
Câu 37. Là quản trị viên Windows, bạn cấu hình dịch vụ mạng Windows để chạy với tài khoản được tạo đặc biệt với các quyền hạn chế. Tại sao bạn cần làm điều này?
(A) Để ngăn chặn tin tặc nhận được các đặc quyền nâng cao do dịch vụ mạng bị xâm nhập
(B) Dịch vụ mạng Windows sẽ không chạy với quyền quản trị
(C) Các dịch vụ mạng Windows phải chạy với quyền truy cập hạn chế
(D) Để ngăn chặn sâu máy tính xâm nhập vào mạng
ENG

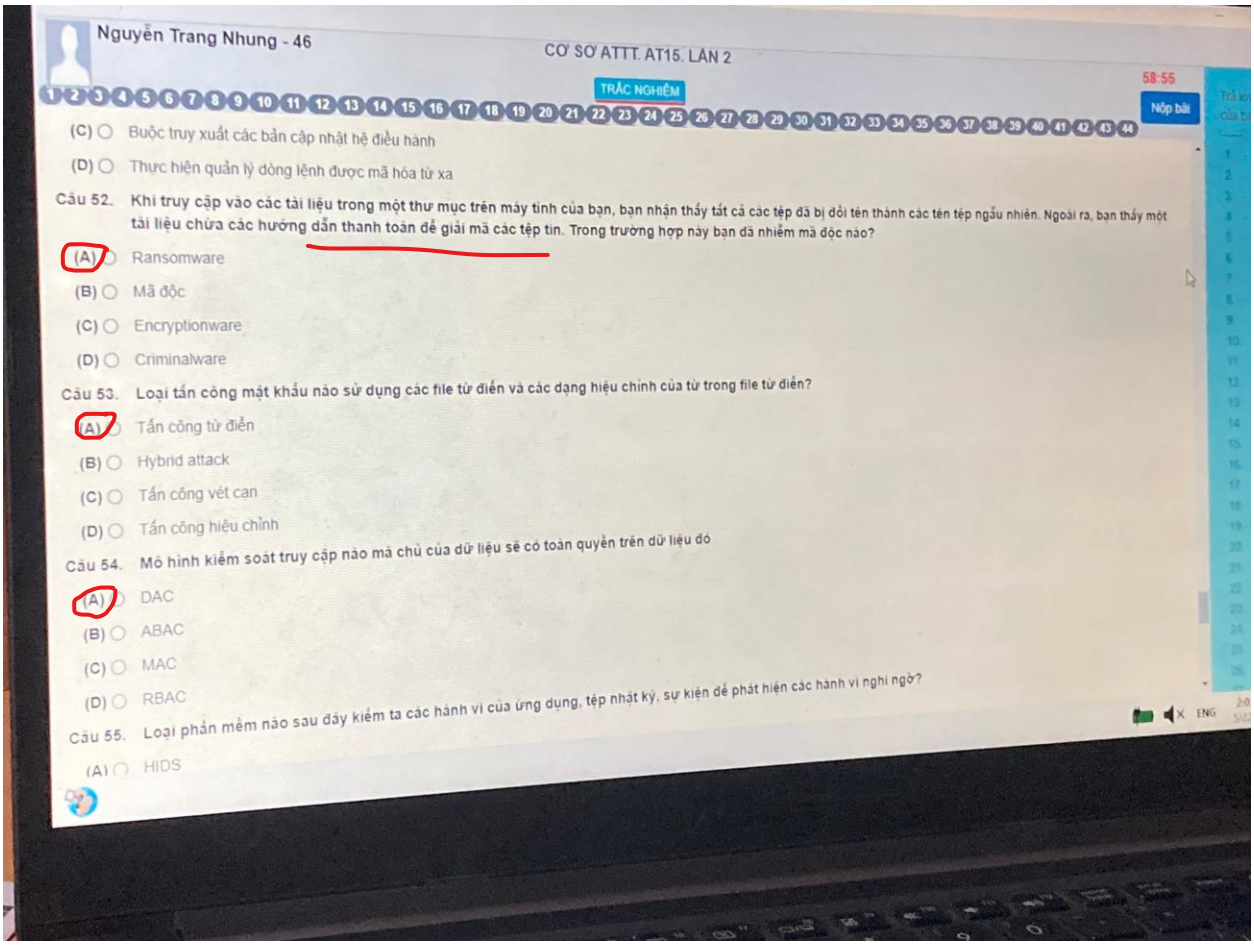

Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
59:07
Nộp bài
(D) Để ngăn chặn sâu máy tính xâm nhập vào mạng
Câu 38. Sắp xếp các phương xác thực danh theo thứ tự an toàn tăng dần?
(A) Tên người dùng và mật khẩu, thẻ thông minh, quét võng mạc
(B) Thẻ thông minh, quét võng mạc, mật khẩu
(C) Quét võng mạc, mật khẩu, thẻ thông minh
(D) ACL, tên người dùng và mật khẩu, quét võng mạc
Câu 39. Phát biểu nào sau đây đúng?
(A) Worm ghi lại tất cả các ký tự đã gõ vào một tệp văn bản.
(B) Worm có thể mang virus.
(C) Worm lây nhiễm trong file
(D) Worm lây nhiễm vào đĩa cứng MBR
Câu 40. Điều nào sau đây đúng với hệ mật khóa bí mật
(A) Khóa bí mật được sử dụng cho cả mã hóa và giải mã
(B) Khóa bí mật được sử dụng để trao đổi khóa
(C) Khóa bí mật được sử dụng cho mã hóa
(D) Khóa bí mật được sử dụng cho giải mã
Câu 41. Giao thức TCP / IP nào cung cấp cho quản trị viên một giao diện dòng lệnh từ xa cho các dịch vụ mạng?
(A) POP
(B) ARP
ENG

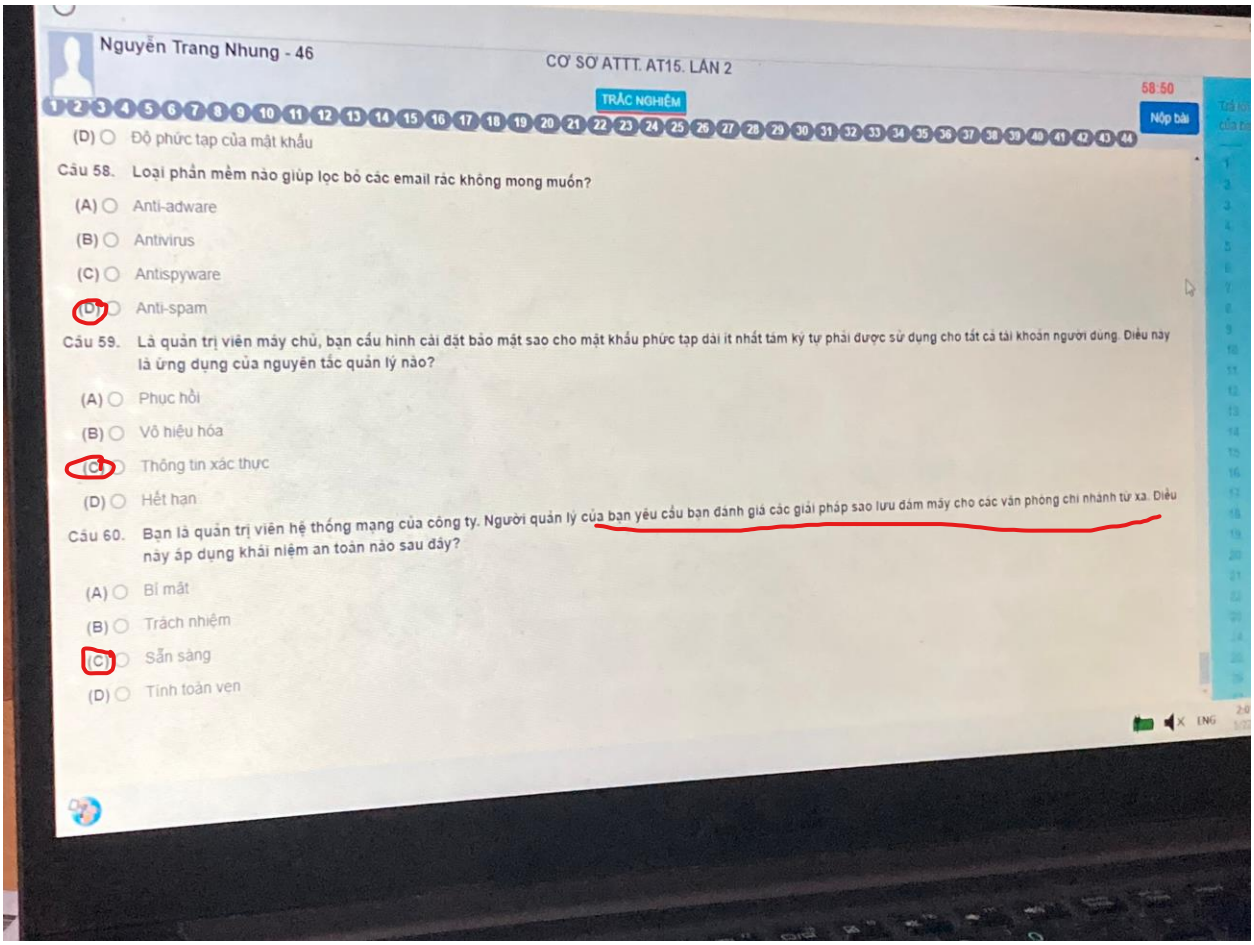

Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
59:04
Nộp bài
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44
(B) ARP
(C) Telnet
(D) UDP
Câu 42. Bình là nhà phát triển phần mềm cho một công ty công nghệ cao. Anh ta tạo ra một chương trình kết nối với phòng chat và chờ nhận lệnh thu thập thông tin người dùng cá nhân. Bình nhúng chương trình này vào tệp AVI của một bộ phim nổi tiếng hiện tại và chia sẻ tệp này trên mạng chia sẻ tệp P2P. Chương trình của Bình được kích hoạt khi mọi người tải xuống và xem phim, cái gì sẽ được tạo ra?
(A) Botnet
(B) Tấn công DDoS
(C) Worm
(D) Logic Bomb
Câu 43. Thuật toán nào sau đây giúp bảo vệ tính bí mật của thông điệp
(A) HMAC
(B) Twofish
(C) DSA
(D) Hàm băm
Câu 44. Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu
(A) DAC
(B) MAC
(C) PKI
(D) RBAC
ENG


Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
58:60
Nộp bài
(C) PKI
(D) RBAC
Câu 45. Công ty của bạn phát hành điện thoại thông minh cho nhân viên để sử dụng trong công việc. Chính sách công ty bắt buộc rằng tất cả dữ liệu lưu trữ trên điện thoại thông minh phải được mã hóa. Điều này nhằm đến tính chất nào của an toàn thông tin?
(A) Trách nhiệm
(B) Sẵn sàng
(C) Bí mật
(D) Tính toàn vẹn
Câu 46. Tùy chọn nào sẽ bảo vệ máy tính xách tay của nhân viên khi họ đi du lịch và kết nối với mạng không dây?
(A) NIDS
(B) VPN
(C) Phần mềm tường lửa cá nhân
(D) Thẻ không dây tương thích 802.11n
Câu 47. Điều nào sau đây đúng với NIDS
(A) Bảo vệ các máy trạm ngay cả khi bị mất kết nối khỏi mạng LAN
(B) Cần cài đặt trên mỗi máy trạm
(C) Phát hiện ra các gói tin độc hại
(D) Loại bỏ các gói tin độc hại
Câu 48. Phát biểu nào sau đây đúng về nguyên tắc hợp lý đầy đủ trong An toàn thông tin
(A) Các biện pháp bảo vệ làm ảnh hưởng đến hệ thống
ENG


Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
58:58
Nộp bài
Câu 48. Phát biểu nào sau đây đúng về nguyên tắc hợp lý đầy đủ trong An toàn thông tin
(A) Các biện pháp bảo vệ làm ảnh hưởng đến hệ thống
(B) Giảm thiểu hoàn toàn rủi ro cho hệ thống
(C) Áp dụng đầy đủ các biện pháp bảo vệ có thể có cho hệ thống
(D) Mục tiêu của nguyên tắc là đưa rủi ro của hệ thống về mức chấp nhận được với chi phí bảo vệ không lớn hơn giá trị của hệ thống
Câu 49. Phát biểu nào sau đây đúng với backdoors?
(A) Chúng là mã độc
(B) Chúng cung cấp quyền truy cập vào tài khoản root Windows
(C) Chúng có khả năng nhân bản
(D) Chúng cho phép điều khiển quyền truy cập của người dùng thông qua cổng 26
Câu 50. Mã độc nào sau đây có khả năng tự nhân bản chính nó?
(A) Virus và Zoombie
(B) Virus và Worm
(C) Virus và Trojan Horse
(D) Virus và Logic Bomb
Câu 51. Telnet được sử dụng cho mục đích nào sau đây?
(A) Xác minh bộ định tuyến trong đường truyền
(B) Thực hiện quản lý dòng lệnh từ xa dạng rõ
(C) Buộc truy xuất các bản cập nhật hệ điều hành
ENG


Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
58:53
Nộp bài
Câu 55. Loại phần mềm nào sau đây kiểm ta các hành vi của ứng dụng, tệp nhật ký, sự kiện để phát hiện các hành vi nghi ngờ?
(A) HIDS
(B) NIDS
(C) Antivirus
(D) Firewall cá nhân
Câu 56. Công nghệ nào sử dụng một địa chỉ IP bên ngoài duy nhất để đại diện cho nhiều máy tính trên mạng nội bộ?
(A) NIDS
(B) NAT
(C) DHCP
(D) IPSec
Câu 57. Biện pháp đối phó nào sau đây được thiết kế để bảo vệ chống lại cuộc tấn công vét cạn vào mật khẩu?
(A) Vá
(B) Mật khẩu mạnh
(C) Khóa tài khoản hạn chế số lần thử mật khẩu
(D) Độ phức tạp của mật khẩu
Câu 58. Loại phần mềm nào giúp lọc bỏ các email rác không mong muốn?
(A) Anti-adware
(B) Antivirus
(C) Antispyware
ENG


Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
58:55
Nộp bài
(C) Buộc truy xuất các bản cập nhật hệ điều hành
(D) Thực hiện quản lý dòng lệnh được mã hóa từ xa
Câu 52. Khi truy cập vào các tài liệu trong một thư mục trên máy tính của bạn, bạn nhận thấy tất cả các tệp đã bị đổi tên thành các tên tệp ngẫu nhiên. Ngoài ra, bạn thấy một tài liệu chứa các hướng dẫn thanh toán để giải mã các tệp tin. Trong trường hợp này bạn đã nhiễm mã độc nào?
(A) Ransomware
(B) Mã độc
(C) Encryptionware
(D) Criminalware
Câu 53. Loại tấn công mật khẩu nào sử dụng các file từ điển và các dạng hiệu chỉnh của từ trong file từ điển?
(A) Tấn công từ điển
(B) Hybrid attack
(C) Tấn công vét cạn
(D) Tấn công hiệu chỉnh
Câu 54. Mô hình kiểm soát truy cập nào mà chủ của dữ liệu sẽ có toàn quyền trên dữ liệu đó
(A) DAC
(B) ABAC
(C) MAC
(D) RBAC
Câu 55. Loại phần mềm nào sau đây kiểm ta các hành vi của ứng dụng, tệp nhật ký, sự kiện để phát hiện các hành vi nghi ngờ?
(A) HIDS
ENG


Nguyễn Trang Nhung - 46
CƠ SỞ ATTT. AT15. LẦN 2
TRẮC NGHIỆM
58:50
Nộp bài
(D) Độ phức tạp của mật khẩu
Câu 58. Loại phần mềm nào giúp lọc bỏ các email rác không mong muốn?
(A) Anti-adware
(B) Antivirus
(C) Antispyware
(D) Anti-spam
Câu 59. Là quản trị viên máy chủ, bạn cấu hình cài đặt bảo mật sao cho mật khẩu phức tạp dài ít nhất tám ký tự phải được sử dụng cho tất cả tài khoản người dùng. Điều này là ứng dụng của nguyên tắc quản lý nào?
(A) Phục hồi
(B) Vô hiệu hóa
(C) Thông tin xác thực
(D) Hết hạn
Câu 60. Bạn là quản trị viên hệ thống mạng của công ty. Người quản lý của bạn yêu cầu bạn đánh giá các giải pháp sao lưu đám mây cho các văn phòng chi nhánh từ xa. Điều này áp dụng khái niệm an toàn nào sau đây?
(A) Bí mật
(B) Trách nhiệm
(C) Sẵn sàng
(D) Tính toàn vẹn
ENG