Câu 1: Kỹ thuật đánh cắp tài khoản bằng Keylog thường được các newbie Hacker ưa thích sử dụng là do:
a. Keylog rất mạnh trong việc nhận dạng user/password trong các gói tin gởi ra ngoài
b. Keylog rất mạnh trong việc dò tìm mật khẩu đã bị mã hóa (encrypt) hoặc bị băm (Hash)
c. Do đa phần người dùng không quan tâm đến vấn đề bảo mật và Anti Virus
d. Khó bị các chương trình Anti Virus phát hiện

Câu 2. Để thực hiện cuộc tấn công Trojan-Backdoor. Hacker sẽ thực hiện:
a. Trojan Server được cài trên máy nạn nhân – Hacker điều khiển bằng Trojan Client
b. Hacker dùng Trojan Client, tấn công vào máy nạn nhân qua các port nhận đươc từ kỹ thuật Scanning.
c. Hacker dùng Trojan Server, tấn công vào máy nạn nhân qua các port nhận đươc từ kỹ thuật Scanning.
d. Trojan Client được cài trên máy nạn nhân – Hacker điều khiển bằng Trojan Server

Câu 3. Trojan là một phương thức tấn công kiểu:
a. Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng
b. Đánh cắp dữ liệu của nạn nhân truyền trên mạng
c. Tấn công làm tê liệt hệ thống mạng của nạn nhân
d. Điều khiển máy tính nạn nhân từ xa thông qua phần mềm cài sẵn trong máy nạn nhân

Câu 4: Metasploit Framework là công cụ tấn công khai thác lỗ hổng để lấy Shell của máy nạn nhân. Ngay sau khi cài đặt, chạy công cụ này thì gặp sự cố: tất cả các lệnh gõ trên Metasploit không được thi hành. Nguyên nhân là do:
a. Do không kết nối được tới máy nạn nhân.
b. Do không cài đặt công cụ Metasploit vào ổ C:
c. Do máy nạn nhân không cho phép tấn công.
d. Do Phần mềm Anti Virus trên máy tấn công đã khóa (blocked) không cho thi hành.

Câu 5: System Hacking là một phương thức tấn công kiểu:
a. Điều khiển máy tính nạn nhân từ xa
b. Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng
c. Tấn công làm tê liệt hệ thống mạng của nạn nhân
d. Đánh cắp dữ liệu của nạn nhân truyền trên mạng

Câu 6: Sniffing là một phương thức tấn công kiểu:
a. Điều khiển máy tính nạn nhân từ xa
b. Đánh cắp dữ liệu của nạn nhân truyền trên mạng
c. Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng
d. Tấn công làm tê liệt hệ thống mạng của nạn nhân

Câu 7: RFID - Radio Frequency Identification là kỹ thuật nhận dạng nào?
a. Nhận dạng sinh trắc học
b. Nhận dạng qua tín hiệu RF với thông tin cần xác định
c. Nhận dạng hình ảnh
d. Không phải các dạng nói trên

Câu 8: Phương thức thông dụng để chia sẻ một kết nối internet cho nhiều máy khác trong mạng là:
a. NAT (Network Address Translation)
b. ROUTE (Routing Service)
c. RAS (Remote Access Service)
d. ICS (Internet Connection Sharring)

Câu 9: Máy Windows Server 2003 có 2 thiết bị giao tiếp mạng: một giao tiếp Internet và một giao tiếp với các Client. Người quản trị triển khai NAT trên Windows Server này để chia sẻ kết nối internet. Sau khi triển khai xong thì Server giao tiếp internet tốt, còn các Client thì không giao tiếp được mặc dùng đã khai báo đúng và đủ các thông số IP cho Clients. Nguyên nhân dẫn đến tình trạng trên:
a. Do Hệ Điều hành trên Client không hỗ trợ giao tiếp internet qua NAT Server
b. Do Windows Server dùng phiên bản Standard, không hỗ trợ SecureNAT
c. Do dịch vụ "Basic Firewall" ngăn không cho các Client giao tiếp internet
d. Khi triển khai NAT, người quản trị đã chọn sai thiết bị giao tiếp internet.

Câu 10. Một máy Windows Server 2003 tên SERVER1 trước đây được xây dựng thành một FTP Server cung cấp Files cho người dùng nội bộ và người dùng các chi nhánh của Doanh nghiệp. Doanh nghiệp dùng SERVER1 để chia sẻ kết nối internet kiểu SecureNAT cho các máy khác. Khi người Quản trị thực hiện SecureNAT bằng Wizard của RRAS. Anh ta chọn "Network Address Translation (NAT)" và click "Next" cho đến khi "Finish". Kết quả:
a. Người dùng tại các chi nhánh sẽ không truy cập dữ liệu trong FTP được vì khi đăng nhập vào FTP Server, các Username/Password đều bị Server từ chối.
b. Người dùng bên trong mạng của SERVER1 sẽ truy cập FTP bình thường nhưng không giao tiếp được internet.
c. Người dùng tại các chi nhánh vẫn truy xuất dữ liệu trên FTP Server như bình thường.

d. Người dùng tại các chi nhánh sẽ không truy cập dữ liệu trong FTP trên SERVER1 được.

Câu 11: Một máy tính kết nối internet bằng công nghệ ADSL. Khi kết nối internet thành công, ISP sẽ cấp một địa chỉ IP. Trong trường hợp không có một sự can thiệp nào khác, hãy chọn phát biểu chính xác:
a. Địa chỉ IP đó được cấp cho thiết bị mạng cổng RJ-45 trên ADSL modem
b. Địa chỉ IP đó được cấp cho card mạng giao tiếp intenet trên máy người dùng.
c. Địa chỉ IP đó được cấp cho thiết bị mạng cổng RJ-11 trên ADSL modem
d. Địa chỉ IP đó được cấp cho máy tính của người dùng

Câu 12: Trước đây, phòng Kỹ thuật của một Doanh nghiệp chỉ có một máy tính chạy Windows Server 2003 tên SERVER1. Người quản trị thường sử dụng Remote Desktop để điều hành máy này từ nhà anh ta. Doanh nghiệp trang bị thêm cho Phòng Kỹ thuật 10 máy tính và dùng máy SERVER1 chia sẻ kết nối internet bằng SecureNAT. Sau khi chia sẻ kết nối internet thành công, người quản trị không còn sử dụng Remote Desktop để điều hành máy SERVER1 từ nhà được nữa. Giải pháp tối ưu nhất để khắc phục vấn đề này:
a. Thay đổi tài khoản được quyền Remote Desktop máy SERVER1
b. Tắt Basic Firewall trên máy SERVER1
c. Tắt dịch vụ Remote Desktop trên SERVER1 rồi khởi tạo lại dịch vụ này
d. Trên Basic Firewall của máy SERVER1: mở port 3389 chuyển về IP address của chính máy SERVER1.

Câu 13: Trường Đào tạo CNTT có nhiều chi nhánh. Các nhân viên kế toán ở các Chi nhánh muốn chia sẻ những thông tin kế toán với nhau. Giải pháp nào sau đây là khả thi hiện nay?
a. Với đường truyền Internet có sẵn, triển khai hệ thống VPN cho các Chi nhánh.
b. Sử dụng Remote Dial-up để quay số nối mạng từ Chi nhánh A qua B mỗi khi có nhu cầu truy cập thông tin chia sẻ.
c. Mỗi Chi nhánh thuê bao một Leased Line riêng. Routing các Leased Line lại với nhau.
d. Sử dụng dây mạng để nối tất cả các Chi nhánh lại với nhau.

Câu 14: Một gói tin có hỗ trợ IPSec được mã hóa cả Header và Content. Phương thức mã hóa này có tên gọi:
a. ESP
b. AH
c. SSL
d. EFS

Câu 15: Trường Đào tạo CNTT dự tính triển khai kết nối VPN Site-to-Site giữa các Chi nhánh nhưng vẫn còn lo ngại về độ an toàn của dữ liệu khi truyền trên hạ tầng internet. Là người quản trị mạng tại trường, bạn chọn giải pháp nào dưới đây để khắc phục khó khăn trên?
a. Sử dụng IPSec kết hợp với giao thức L2TP.
b. Yêu cầu nhà cung cấp dịch vụ internet (ISP) mã hóa các dữ liệu truyền bằng VPN từ ra ngoài internet.
c. Sử dụng hệ thống mã hóa tập tin (Encrypt File System - EFS) có sẵn trong Windows đê mã hóa các tập tin trước khi chia sẻ qua VPN.
d. Đặt mật khẩu có độ phức tạp cao cho các Dial-In User

Câu 16: Trường Đào tạo CNTT có nhiều chi nhánh. Các nhân viên thuộc Chi nhánh Biên Hòa có nhu cầu truy cập dữ liệu trên các máy tính trong phòng Kế toán của Chi nhánh Phú Nhuận. Là một người quản trị mạng tại , bạn chọn giải pháp nào là tối ưu nhất:
a. Thiết lập VPN kiểu Site-to-Site giữa 2 chi nhánh
b. Thiết lập VPN kiểu Remote-asccess và cấp cho những nhân viên tại Chi nhánh Biên Hòa tài khoản truy cập vào Chi nhánh Phú nhuận
c. Thiết lập một FTP Server tại chi nhánh Phú nhuận. Các dữ liệu Kế toán sẽ được đưa vào FTP Site để nhân viên CN Biên hòa truy xuất
d. Những dữ liệu cần truy xuất sẽ được nhân viên phòng Kế toán gởi mail cho các nhân viên Chi nhánh Biên Hòa.

Câu 17: Khi xây dựng kết nối VPN kiểu Remote-Access, người dùng A không thể dial vào VPN Server mặc dù đã thiết lập đúng các thông số cho VPN Connection và khai báo chính xác Username và password. Các người dùng khác vẫn kết nối VPN từ nhà vào Văn phòng Công ty được bình thường. Nguyên nhân lỗi có thể là:
a. Tài khoản của người dùng A không được cấp phép đăng nhập từ xa
b. IP address trên máy người dùng A không cùng Net.ID với IP address trong Văn phòng Công ty
c. Hệ Điều hành trên máy người dùng A và Hệ Điều hành trên máy VPN Server không tương thích nhau.
d. Hệ Điều hành trên máy người dùng A không hỗ trợ kết nối VPN

Câu 18: Áp dụng IPSec vào hệ thống VPN, phương thức chứng thực được hỗ trợ sẵn trong dịch vụ RRAS của Windows là:
a. Encapsulating Security Payload (ESP)
b. Internet Key Exchange (IKE)
c. Certified Authentication (CA)

d. Kerberos

Câu 19: IP Security Policy được Windows cấu hình với 3 Policies mặc định. Trong đó Policy có tên "Secure Server (Request Security)" mang ý nghĩa:
a. Máy tính cũng gởi yêu cầu sử dụng IPSec. Nếu máy kia không đáp ứng thì vẫn có thể giao tiếp bình thường (không có IPSec).
b. Nếu một máy khác yêu cầu dùng IPSec để giao tiếp, máy sẽ từ chối - không giao tiếp.
c. Máy tính cũng gởi yêu cầu sử dụng IPSec. Nếu máy kia không đáp ứng thì kết thúc phiên giao tiếp.
d. Nếu một máy khác yêu cầu dùng IPSec để giao tiếp, máy tính sẽ tự kích hoạt IPSec.

Câu 20. Khi xây dựng VPN Server bằng dịch vụ RRAS trên Windows Server 2003, người quản trị của một Doanh nghiệp cần phải xác định trước dãy IP address sẽ cấp phép cho các máy VPN Client đăng nhập vào hệ thống. Dãy IP này phải là:
a. Dãy IP address bất kỳ, nhưng phải bằng hoặc lớn hơn số lượng client đăng nhập vào hệ thống mạng qua VPN.
b. Dãy IP address cùng Net.ID với các mạng bên trong VPN Server của Doanh nghiệp. Đồng thời, không cùng Net.ID với mạng nội bộ nơiVPN Client là thành viên.
c. Dãy IP address này phải cùng Net.ID với mạng nội bộ của VPN Client.
d. Dãy IP address này là đoạn "Exclusive IP addresses" của Scope trên DHCP Server của mạng Doanh nghiệp.

Câu 21: Bạn là người quản trị mạng tại trung tâm. Máy Server ISA1 đặt tại CN Phú Nhuận, máy ISA2 đặt tại CN Biên Hòa. Bạn đang triển khai kết nối VPN kiểu Site-to-Site giữa 2 Chi nhánh với giao thức L2TP/IPSec và dùng phương thức chứng thực Pre-shared Key. Bạn mở "Routing and Remote Access" và nhập Pre-shared Key vào trong hộp thoại Properties của RRAS Server. Kết nối Site-to-Site thành công. Bạn khởi động lại ISA Server và thử kết nối lại thì thất bại. Bạn sẽ giải quyết vấn đề này bằng cách:
a. Nhập lại Pre-shared Key trên cả 2 ISA Server tại 2 Chi nhánh. Đảm bảo đúng từng ký tự, con số…
b. Gở bỏ tất cả các Certificates trên ISA Server ở cả 2 Chi nhánh
c. Cài đặt lại các Certificates trên ISA Server ở cả 2 Chi nhánh. Đồng thoại kích hoạt phương thức chứng thực EAP trên hộp thoại "Authenticaties" trong "ISA Management Console".
d. Trên ISA Server ở cả 2 Chi nhánh: xóa bỏ Pre-shared Key trong "Routing and Remote Access" và nhập lại Pre-shared Key trong hộp thoại "VPN Properties" trong "ISA Management Console"

Câu 22: Bạn là người quản trị mạng tại trung tâm. Máy Server ISA1 cung cấp truy cập Internet cho tất cả máy trong mạng. Để phòng tránh người dùng vô tình tải và thực thi các tập tin virus (dạng *.exe, *.com, *.dll,…). Bạn chọn giải pháp nào sau đây?

a. Lập một Access Rule cấm người dùng truy cập HTTP.
b. Lập một Access Rule cho phép truy cập HTTP. Trong hộp thoại "Content Type" của Access Rule này: bỏ chọn "Application"
c. Tạo một "Content Type" trong đó chứa danh sách tập tin Virus. Tạo Access Rule cấm người dùng truy cập HTTP trên Content này.
d. Lập một Access Rule cấm truy cập HTTP vào các Web Site phát tán Virus

Câu 23: Bạn là người quản trị mạng tại trung tâm. Máy Server ISA1 cung cấp giao tiếp Internet cho tất cả máy trong mạng. Để đảm bảo an toàn cho tất cả Client, Bạn quyết định triển khai giao tiếp internet cho Client kiểu Web Client Proxy. Triển khai vấn đề này, ISA1 phải được cấu hình như là một Proxy Server, bằng cách:
a. Trên máy ISA1, trong nhánh "Networks": Properties cho "Internal" vào tab "Web Proxy" và chọn "Enable Web Proxy Client".
b. Trên máy ISA1, trong nhánh "Networks": Properties cho "External" vào tab "Web Proxy" và chọn "Enable Proxy".
c. Trên máy ISA1, trong "Internet Options" vào tab "Connection" chọn nút "LAN Settings" và chọn "Use a Proxy Server".
d. Trên máy ISA1, trong nhánh "Networks": Properties chọn "Local Host" vào tab "Web Proxy" và chọn "Enable Proxy".

Câu 24: Bạn là người quản trị mạng tại trung tâm. Trung tâm gồm một văn phòng chính và một văn phòng chi nhánh. Mạng của trung tâm gồm có 2 máy tính ISA Server 2006 tên là _ISA1 và _ISA2. _ISA1 đặt tại văn phòng chính, _ISA2 đặt tại văn phòng chi nhánh.
Hai văn phòng này kết nối lại với nhau bằng VPN site-to-site thông qua IPSec. Các user ở văn phòng chi nhánh thì báo cáo rằng họ có thể truy cập dữ liệu share ở văn phòng chính nhưng không thể truy cập Microsoft Outlook Web Access Web site. Bạn nên làm gì để cho các user ở văn phòng chi nhánh có thể truy cập được Microsoft Outlook Web Access Web site?
a. Tạo một access rule để cho phép TCP port 80 outbound.
b. Sử dụng NAT giữa hai văn phòng.
c. Add một đia chỉ IP cho card mạng external trên _ISA2.
d. Thay đổi cấu hình IPSec trên _ISA1 và _ISA2 để sử dụng thuật toán MD5.

Câu 25: Máy ISA Server có 2 card giao tiếp mạng

- External Adapter có IP address: 192.168.1.2 và Defautl Gateway là: 192.168.1.1
- Internal Adapter có IP address: 172.16.1.2 và Defautl Gateway là: 172.16.1.1

Sau khi cài đặt ISA Server thì người dùng báo rằng họ không thể truy cập các Web site trên internet mặc dù bạn đã lập một Access Rule cho phép Internal truy cập internet. Bạn làm thế nào để giải quyết sự cố trên:
a. Bỏ trống Default Gateway trên Internal Adapter
b. Cấu hình lại Default Gateway của 2 card Internal và External là 192.168.1.1

c. Bổ sung thêm một Access rule cho phép HTTP trafic đi từ Internal đến External
d. Tạo Network Set cho mỗi Sub net của 2 giao tiếp mạng trên

Câu 26: Trường đào tạo CNTT có nhu cầu triển khai hệ thống Firewall bằng ISA Server 2004/2006. Hiện có một hệ thống mạng Active Directory với một DC và một File Server cùng với 50 máy Client. Ngoài ra, còn có 2 Web Server và 1 Mail Server (dùng Public IP) phục vụ người dùng internet. Là người quản trị mạng tại , bạn chọn giải pháp nào?
a. Xây dựng hệ thống Firewall kiểu Back-End Firewall, đưa máy Web Server, Mail Server, DC, FS vào DMZ Network
b. Xây dựng hệ thống Firewall kiểu Back-End Firewall, đưa máy Web Server và Mail Server vào DMZ Network; máy DC, FS và các Client vào Internal network
c. Xây dựng hệ thống Firewall kiểu Three-Leg (Three-Homed), đưa máy Client vào DMZ Network. Tất cả các Server và DC vào Internal Network
d. Xây dựng hệ thống Firewall kiểu Three-Leg (Three-Homed), đưa máy DC và FS vào DMZ Network

Câu 27: Bạn là người quản trị mạng tại trung tâm. Máy ISA1 được cài đặt ISA Server 2004. Bạn đã tạo một network Rule định nghĩa mối quan hệ NAT giữa Internal và External. bên trong Internal có một máy Windows Server 2003 trên SERVER1. Bạn cần điều khiển máy SERVER1 từ xa bằng Remote Desktop (RDP). Đồng thời, cũng cho phép một số người dùng Remote Desktop máy SERVER1 qua một port không theo chuẩn: 12345. Bạn phải làm thế nào trên ISA1? (chọn 2 hành động đáp ứng được yêu cầu).
a. Định nghĩa một Protocol mới có tên RDP-x, sử dụng TCP port 12345 làm inbound
b. Định nghĩa một Protocol mới có tên RDP-x, sử dụng TCP port 12345 làm outbound
c. Tạo một Access Rule sử dụng RDP-x Protocol
d. Tạo một Server publishing rule sử dụng RDP-x Protocol

Câu 28: Bạn là người quản trị mạng tại trung tâm. Máy Server ISA1 cung cấp giao tiếp Internet cho tất cả máy trong mạng. Máy MAIL1 là một Exchange Mail Server cung cấp truy xuất mail bằng cả 2 hình thức: Mail Client Access và Web Client Access. Khi Bạn Publishing máy MAIL1, bạn chọn kiểu "Client Access: RPC, POP3, IMAP, SMTP". Người dùng báo rằng họ truy xuất mail bằng "Outlook Express" thì được, nhưng truy xuất mail bằng "Internet Explorer" thì không được. Bạn sẽ giải quyết:
a. Trên ISA1, thêm một Access Rule cho phép truy cập HTTP từ External vào Internal.
b. Trên MAIL1: gở bỏ Exchange Mail Server rồi cài đặt lại.
c. Chỉnh sửa lại "Internet Options" trên máy người dùng để có thể truy xuất mail.
d. Publishing máy MAIL1 thêm một lần nữa với kiểu "Web Client Access".

Câu 29: Cache là một vùng đĩa cứng dùng lưu trữ các dữ liệu đi ngang qua ISA Server. Sau khi cài đặt

ISA Server 2006, nó sẽ:
a. Tự động cache tất cả dữ liệu đi ngang qua nó ngay sau khi cài đặt ISA
b. Chỉ tự động cache sau khi người dùng định nghĩa và Enable Cache trên ISA Server
c. Chỉ tự động cache sau khi người dùng Enable Cache trên ISA Server
d. Chỉ tự động cache sau khi người dùng định nghĩa Cache trên ISA Server (Define cache)

Câu 30. Trường đào tạo CNTT hiện có một hệ thống Firewall kiểu Three-Homed với Firewall Server là máy ISA1. Máy Web Server được đặt trong DMZ Network và đã được Publishing cho người dùng internet truy cập. Các người dùng nội bộ báo lại rằng: họ không truy cập được trang Web của trong khi các trang Web khác họ vẫn truy cập tốt. Là người quản trị mạng, Bạn sẽ giải quyết vấn đề này bằng cách:
a. Tạo mới một Network Rule với quan hệ giữa Internal và DMZ kiểu NAT.
b. Khai báo trên các Client: Default Gateway là IP address của Web Server
c. Tạo mới một Network Rule với quan hệ giữa Internal và DMZ kiểu ROUTE.
d. Tạo mới một Network Rule với quan hệ giữa DMZ và External kiểu ROUTE

Câu 31: Sâu máy tính và các virus khác phát tán như thế nào?
a. Tự động lan và lây nhiễm giữa các hệ thống.
b. Phát tán qua các phần đính kèm với thư điện tử
c. Gần như không thể phát tán trừ khi bạn mở hoặc chạy một chương trình bị nhiễm.
d. Phát tán qua nội dung thư điện tử

Câu 32: Các bước tiến hành nhằm giảm sự rủi ro vì virus:

a. Bằng phần mềm diệt virus
b. Giữ cho chương trình diệt virus được cập nhật
c. Chọn phần mềm diệt virus thích hợp
d. Tất cả các giải pháp trên

Câu 33: Denial Of Service (DoS) là:

a. Một dịch vụ mạng
b. Một kiểu kết nối mạng
c. Một phương thức liên kết mạng

d. Phương thức tấn công từ chối dịch vụ

Câu 34: Sau khi dùng Sniffing software để bắt thông tin phân tích gói thông tin gửi đi từ host, có dạng: Protocol :TCP; Destination Port: 80; Source IP 192.168.3.8; Destination IP 203. 162.4.132; SYN=1, ACK=0. Cho biết host trên đang làm gì?

a. Máy 203. 162.4.132 đang yêu cầu kết nối với FTP server tại 192.168.3.8
b. Máy 192.168.3.8 đang yêu cầu kết nối với Mail server tại 203. 162.4.132
c. Máy 192.168.3.8 đang yêu cầu kết nối với server tại 203. 162.4.132
d. Máy 192.168.3.8 đang yêu cầu kết nối với Web server tại 203. 162.4.132

Câu 35: Bạn cần cấm việc dò quét từ mạng khác theo giao thức ICMP. Bạn phải set lệnh deny ICMP với tham số nào?

a. Type = 3, Code = 1
b. Type = 3, Code = 6
c. Type = 3, Code = 7
d. Type = 3, Code = 0

Câu 36: Cho bảng số liệu các luật lọc gói tin không trạng thái (Stateless packet-filter rules) sau:

Rule	Source IP	Source Port	Destination IP	Destination Port	Action
1	Any	Any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	Any	Any	Any	Deny

Hỏi máy ở địa chỉ 192.168.120.1 có thể ping được đến những máy nào?
a. 192.168.120.x
b. 192.168.120.0
c. Tất cả các máy
d. Không có máy nào

Câu 37: Cho bảng số liệu các luật lọc gói tin không trạng thái (Stateless packet-filter rules) sau:

Rule	Source IP	Source Port	Destination IP	Destination Port	Action
1	Any	Any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	Any	Any	Any	Deny

Hỏi những máy nào có thể ping đến mạng có địa chỉ 192.168.120.0?

a. 192.168.120.x

b. 192.168.120.1

c. Tất cả các máy

d. Không có máy nào

Source IP	Source Port	Destination IP	Destination Port	Action
?	?	?	?	?

Câu 38: Công ty ABC có máy chủ quản lý Website cung cấp thông tin trên Internet tại địa chỉ 203.162.4.115. Hãy cài đặt tập luật cho Server này:

a. 203.162.4.115 – 80 - Any – 80 - Allow

b. 203.162.4.115 – Any - 203.162.4.115 – 80 - Any

c. Any – Any - 203.162.4.115 – 80 - Allow

d. Any – Any - 203.162.4.115 – 80 - Deny

Source IP	Source Port	Destination IP	Destination Port	Action
?	?	?	?	?

Câu 39: Công ty ABC có Mail Server tại địa chỉ 203.162.4.116. Hãy cài đặt tập luật cho Server này:

a. 203.162.4.116 – 25 - Any – 80 - Allow

b. 203.162.4.116 – Any - 203.162.4.115 – 80 - Any

c. Any – Any - 203.162.4.116 – 25 - Allow

d. Any – Any - 203.162.4.115 – 25 - Deny

Câu 40. Các phương pháp chứng thực được sử dụng phổ biến hiện nay:

a. Password

b. e-Token

c. Fingerprint

d. Tất cả các phương pháp trên

[<g>] [</g>]

Hình sau được sử dụng cho các câu từ {<1>} đến {<5>}

Rule	Protocol	Transport Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
7	POP3 outbound	TCP	208.177.178.0/24	Any	Any	110	Allow
8	POP3/S outbound	TCP	208.177.178.0/24	Any	Any	995	Allow
9	POP inbound	TCP	Any	Any	208.177.178.0/24	110	Allow
10	POP3/S inbound	TCP	Any	Any	208.177.178.0/24	995	Allow
11	SMTP outbound	TCP	208.177.178.29	Any	Any	25	Allow
12	SMTP/S outbound	TCP	208.177.178.29	Any	Any	465	Allow
13	SMTP inbound	TCP	Any	Any	208.177.178.29	25	Allow
14	SMTP/S inbound	TCP	Any	Any	208.177.178.29	465	Allow

(<1>) Máy có địa chỉ IP 208.177.178.29 làm nhiệm vụ gì?

a. Web server
b. FTP server
c. Mail server
d. DNS server

(<2>) Mạng 208.177.178.0/24 có thể nhận các gói tin đến từ dịch vụ + cổng?

a. Web + 110
b. FTP + 110
c. Mail + 110
d. Mail + 25

(<3>) Máy có địa chỉ IP 208.177.178.29 có thể gửi gói tin của dịch vụ + qua cổng?

a. Web + 80
b. FTP + 21
c. Mail + 25
d. DNS + 53

(<4>) Máy có địa chỉ IP 208.177.178.29 có thể nhận gói tin của những máy tính + dịch vụ + qua cổng?

a. Bất kỳ + Mail + 465

b. IP 208.177.178.29 + Mail + 25
c. Bất kỳ + Mail + 25 hoặc 465
d. Bất kỳ + Mail + 25

(<5>) Các máy thuộc mạng 208.177.178.0/24 có thể nhận gói tin của những máy tính + dịch vụ + qua cổng?

a. Bất kỳ + Mail + 995
b. IP 208.177.178.29 + Mail + 25
c. Bất kỳ + Mail + 110 hoặc 995
d. Bất kỳ + Mail + 110

Câu 1. Cặp cổng: dịch vụ nào sau đây không đúng?

A. HTTP: 80

B. SSL: 25

C. DNS: 53

D. Telnet: 23

E. POP3: 110

Câu 2. MD5 có giá trị hàm băm dài?

A. 64 bit

B. 128 bit

C. 32 bit

D. 256 bit

E. 384 bit

Câu 3. DES có chiều dài khóa là?

A. 64 bit

B. 16 bit

C. 56 bit

D. 32 bit

E. Đáp án khác

Câu 4. Trong các giải thuật mã hóa sau, giải thuật nào không dùng trong SSH?

A. 3DES

B. IDEA

C. RSA

D. BlowFish

E. Đáp án khác

Câu 5. Giao thức IP Security (IPSec) được thực hiện tại lớp?

A. Application

B. Transport

C. Network (Internet)

D. Data link

E. Đáp án khác

Câu 6. Sử dụng phương pháp mã hóa Vigennère với chuỗi thông báo là ‘AN TOAN BAO MAT MANG” và khóa là “CITD” sẽ được chuỗi?

A. YF ALYF IXM EHQ KSUD

B. CV MRCU UDQ UTW OIGJ

C. CV MRCV UDQ UTW OIGJ

D. CV MRCU UDP UTW OIGJ

E. Đáp án khác

Câu 7. Tại tầng vận chuyển có thể triển khai giao thức bảo mật?

A. SSH

B. S/MIME

C. PGP

D. IPSec

E. SSL/TLS

Câu 8. Độ lớn của khóa đo bằng đơn vị?

A. Bit

B. Byte

C. KB

D. MB

E. Tất cả đều đúng

Câu 9. Điều nào dưới đây không phải là thành phần của an ninh mạng?

A. Authentication

B. Auditing

C. Strong Encryption

D. Security Policies

E. Tất cả đều sai

Câu 10. Thuật toán AES công bố năm 2001 có chiều dài khóa?

A. 2048 bit

B. 1024 bit

C. 512 bit

D. 128 - 256 bit

E. 256 bit

Câu 11. Trường có công dụng kiểm tra sự toàn vẹn của gói tin (TCP, UDP, ICMP) là?

A. Flags

B. Checksum

C. Options

D. TTL

E. Protocol

Câu 12. Lớp nào không thể thực hiện mã hóa bởi phần cứng?

A. Application

B. Transport

C. Network

D. Data link

E. Physical

Câu 13. Hệ thống PKI uy tín nhất thế giới hiện nay là?

A. VerySign

B. OpenCA

C. Microsoft

D. GeoTrust

E. EnTrust

Câu 14. Tường lửa (firewall) không có tác dụng với?

A. Social Engineering

B. Bảo vệ các lớp bên trong

C. Cấm hoặc cho phép gói tin

D. Kiểm soát luồng dữ liệu đi qua

E. Virus

Câu 15. Ứng dụng nào thường dùng để đính kèm Trojan với một tập tin khác?

A. File EXE maker

B. Insider

C. FPort

D. What is running

E. Make on

Câu 16. Thiết lập quyền điều khiển từ xa của hacker đến máy nạn nhân là tác động hay gặp nhất của?

A. Trojan

B. Keylogger

C. RAT

D. Virus

E. Câu trả lời khác

Câu 17. Điều gì là sai khi nói về Trojan?

A. Thường dùng để đánh cắp thông tin

B. Làm chậm tốc độ máy tính

C. Cấm chỉnh sửa Registry

D. Có khả năng tự nhân bản

E. Kích thước nhỏ

Câu 18. Trojan không thâm nhập máy tính bằng?

A. Truy cập vật lý

B. Chia sẻ file

C. Duyệt web

D. Mở file đính kèm

E. Câu trả lời khác

Câu 19. Điều gì không phải là đặc tính của chữ ký số?

A. Secrecy

B. Privacy

C. Integrity

D. Non-repudiation

E. Authentication

Câu 20. Các quy tắc (rule) của firewall được xác định bởi?

A. Tên rule

B. Hành động

C. Giao thức

D. Điều kiện

E. Tất cả đều đúng

Câu 21. Có thể kiểm tra các port đang mở với?

A. MSConfig

B. Tracert

C. WhiteShark

D. ipconfig

E. Netstat

Câu 22. Điều nào dưới đây là thành phần cơ bản của X.509 (PKIX)?

A. Version

B. Certificate Serial Number

C. Signature Algorithm ID

D. Validity Period

E. Tất cả các đáp án trên

Câu 23. Có khả năng lan truyền độc lập mà không cần lan truyền qua file là?

A. Worm

B. Zombie

C. Virus

D. Trojan

E. Spyware

Câu 24. PGP có thể được dùng để?

A. Chứng thực

B. Mã hóa

C. Nén

D. Chứng thực - Mã hóa

E. Đáp án khác

Câu 25. Kỹ thuật sử dụng các gói tin giả mạo chiếm đoạt kết nối giữa máy tính nạn nhân với máy đích?

A. TCP Hijacking

B. Eavesdropping

C. SYN Flooding

D. Message replays

E. Đáp án khác

Câu 26. Mã hóa chuỗi "AN TOAN BAO MAT MANG" bằng phương pháp Permutation thu được chuỗi "NATO NABA OATMM NGA". Khóa h sẽ là?

A. 12345

B. 21435

C. 54321

D. 21453

E. Đáp án khác

Câu 27. Kỹ thuật nào không phải là cơ bản của virus?

A. Phá hoại

B. Lây nhiễm

C. Thường trú

D. Mã hóa

E. Đa hình

Câu 28. SSH dùng cổng?

A. 25

B. 23

C. 22

D. 21e

E. 20

Câu 29. Mật khẩu nào dưới đây không thuộc nhóm 5 mật khẩu phổ biến nhất trên Internet (theo tạp chí PC Magazine)?

A. zxcv

B. qwerty

C. abc123

D. 123456

E. Password

Câu 30. Kỹ thuật nhằm tăng tốc độ thực thi và giảm kích thước chương trình virus được gọi là?

A. Biến hình

B. Chống bẫy

C. Tối ưu

D. Ngụy trang

E. Mã hóa

Câu 31. Chương trình nào không phải là chương trình chống virus?

A. AVG

B. BitDefender

C. IDA Pro Tool

D. Kaspersky

E. McAfee

Câu 32. Giao thức nào không dùng tại tầng ứng dụng?

A. SSL

B. PGP

C. S/MIME

D. SSH

E. Kerberos

Câu 33. Chọn thứ tự thực hiện đúng với giao thức Kerberos? Với thứ tự quy định như sau:

1. User thực hiện giao dịch với server

2. User yêu cầu 1 server ticket

3. User yêu cầu 1 TGT = Ticket Granting Ticket

4. User trình server ticket

A. 1234

B. 3241

C. 1243

D. 2143

E. 3214

Câu 34. Hình thức nào sau đây không phải là hình thức tấn công DoS?

A. Teardrop

B. SYN attack

C. Smurf

D. ARP spoofing

E. Ping of death

Câu 35. Loại nào sau đây được xem như là một tường lửa lai?

A. Dynamic packet filter

B. Packet filter

C. Circuit gateway

D. Application gateway

E. C, D đúng

Câu 36. Máy chủ cấp vé trong giao thức Kerberos là?

A. TSS

B. AS

C. SS

D. TGS

E. Đáp án khác

Câu 37. Việc sử dụng đội quân zombie tấn công trên mạng là hình thức?

A. DDoS

B. Repudiation

C. Instruction

D. Buffer Overlow

E. DoS

Câu 38. Giao thức dùng để xác thực trên các mạng không an toàn là?

A. SSL

B. PGP

C. S/MIME

D. SSH

E. Kerberos

Câu 39. Giao thức SSL/TLS được phát triển bởi?

A. Netscape

B. Microsoft

C. Norton Corp.

D. BKIS

E. AVG

Câu 40. Loại virus có thể thay đổi đặc điểm của nó sau mỗi lần nhiễm là?

A. Polymorphic

B. Stealth

C. Camoulage

D. Cavity

E. Tunneling

Câu 41. Version của chứng chỉ X.509 dùng phổ biến nhất hiện nay?

A. 4

B. 3

C. 2

D. 1

E. Đáp án khác

Câu 42. Các kỹ thuật nào không phải là cơ bản của virus máy tính?

A. Đa hình

B. Lây nhiễm

C. Thường trú

D. Mã hóa

E. Tối ưu

Câu 43. Phương pháp Substitution Cipher dùng bảng chữ cái tiếng Anh (26 ký tự) sẽ có số khả năng biểu diễn mã?

A. 2^{26}

B. 26^2

C. 26^{26}

D. 26!

E. Đáp án khác

Câu 44. Phương pháp mã hóa DES sẽ tạo ra số lượng subkey là?

A. 4

B. 16

C. 2

D. 8

E. 56

Câu 45. A muốn mã hóa thông điệp M trước khi gửi cho B và đảm bảo chỉ B mới có thể đọc được thì A sẽ dùng khóa?

A. PU_B

B. PR_B

C. PU_A

D. PR_A

E. Đáp án khác

Câu 46. Phương pháp tấn công DoS có các gói tin gửi từ attacker có các thông số rất khó hiểu để chia ra các phần (fragment) là?

A. Smurf

B. ARP spoofing

C. Ping of death

D. Teardrop

E. SYN attack

Câu 47. Giao thức thường được sử dụng với mạng riêng ảo (VPN)?

A. IPSec

B. SSH

C. SSL/TLS

D. Kerberos

E. PGP

Câu 48. A muốn khẳng định với B rằng thông điệp M do chính A gửi đi, A sẽ mã hóa với khóa?

A. PU_B

B. PR_B

C. PU_A

D. PR_A

E. Đáp án khác

Câu 49. Thông tin đi kèm theo dữ liệu nhằm mục đích xác nhận người chủ của dữ liệu đó gọi là?

A. Secure mail

B. Biometric

C. Digital Certificate

D. Digital Signature

E. Đáp án khác

Câu 50. Tường lửa loại Packet Filter được đặt tại lớp?

A. Physical

B. Data link

C. Transport

D. Network

E. Application

Câu 51. Các server như: Web, Mail thường được đặt trong vùng nào dưới đây?

A. Single-Homed Bastion Host System

B. Dual-Homed Bastion Host System

C. Screened Subnets

D. Demilitarized Zones (DMZ)

E. PGP

Câu 52. Lớp (layer) nào dưới đây không thuộc SSH?

A. Connection

B. User Authentication

C. Transport

D. Data Link

E. Đáp án khác

Câu 53. Xem hình dưới đây và cho biết quá trình diễn ra tại source A là?

A. Bảo mật

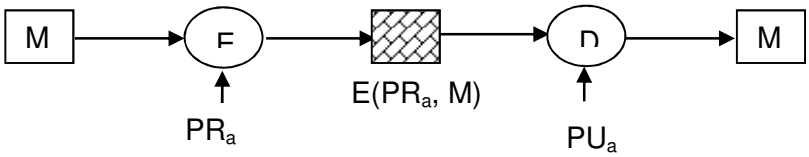
B. Chứng thực

C. Chứng thực – Bảo mật

D. Bảo mật - Chứng thực

E. Đáp án khác

Câu 54. Xem hình dưới đây và cho biết quá trình là?



A. Symmetric encryption: confidentiality and authentication

B. Public key encryption: confidentiality

C. Public key encryption: authentication and signature

D. Public key encryption: confidentiality, authentication and signature

E. Đáp án khác