VPN sử dụng các giải pháp an toàn nào để đảm bảo an toàn cho dữ liệu truyền qua mạng?	Tunnerling	Mã hóa	Ủy quyền	Xác thực
Giao thức nào sử dụng trong công nghệ VPN?	Ipsec	PPTP	L2TP	Cả 3 đáp án trên.
Những mô tả nào dưới đây được xem là ưu điểm của VPN?	Chi phí triển khai thấp	Tính bảo mật cao	Cải thiện băng thông	Có thể nâng cấp dễ dàng
VPN được phân loại thành nhóm:	Remote Access VPN	Intranet	Extranet	Cả 3 đáp án trên.
Intranet VPN được sử dụng cho kết nối nào sau đây?	Các văn phòng, chi nhánh của tổ chức với mạng Intranet trung tâm	Các văn phòng chi nhánh với nhau.	Chỉ trong một chi nhánh.	Cả 3 đáp án trên.
Đâu là ưu điểm của Intranet VPN?	Chống được tấn công DDoS	Cải thiện được tốc độ truyền tải dữ liệu.	Chất lượng QoS ổn định	Dễ dàng thiết lập các kết nối Peer-to-peer mới.
Ưu điểm chính của Extranet VPN là gì?	Chống được tấn công DDoS	Giảm được xâm nhập vào mạng Internet của tổ chức.	Đảm bảo tốt dịch vụ Qos	Giảm chi phí nhiều so với phương pháp truyền thống.
Nhược điểm của Extranet VPN là gì?	Kinh phí tăng lên rất nhiều so với phương pháp truyền thống	Tăng rủi ro cho sự xâm nhập vào mạng Internet nội bộ	Khó khăn cho việc cài đặt, bảo trì, chỉnh sửa các thiết lập sẵn có	Do sử dụng đường truyền internet, chúng ta không có nhiều sự lựa chọn dịch vụ phù hợp giải pháp tailoring phù hợp với nhu cầu tổ chức.
Chức năng chính của các VPN Server	Lắng nghe các yêu cầu kết nối cho VPN	Dàn xếp các yêu cầu và thông số kết nối như là kỹ thuật mật mã, kỹ thuật xác thực.	Sự xác thực và sự cấp phép cho khách hàng VPN	Các người giao tiếp từ xa sử dụng internet hoặc mạng công khai để kết nối tới nguồn tài nguyên của tổ chức từ nhà.
Các mô tả nào dưới đây là tiêu biểu của một VPN client?	Các giao tiếp từ xa sử dụng mạng intermet hoặc mạng công khai để kết nối tới nguồn tài nguyên của tổ chức từ nhà.	Dàn xếp các yêu cầu và thông số kết nối như là kỹ thuật mật mã, kỹ thuật xác thực.	Xác thực và cấp phép cho khách hàng VPN	Những người sử dụng Laptop, notebook, mạng công cộng kết nối với mạng nội bộ của tổ chức để truy cập các tài nguyên nội bộ.
Hệ thống phát hiện xâm nhập được cài đặt như một tác nhân trên máy chủ. Hệ thống phát hiện xâm nhập này có thể xem các tập tin log của các trình ứng dụng hoặc của hệ thống để phát hiện xâm nhập được gọi là:	Network IDS hoặc NIDS	Host IDS hoặc HIDS		
Các thiết bị bảo mật nào dưới đây không phải IDS	Hệ thống đăng nhập mạng được sử dụng để phát hiện lỗ hổng đối với DoS trên một mạng nào đó.	Các công cụ đánh giá lỗ hổng kiểm tra lỗi và lỗ hổng trong hệ điều hành, dịch vụ mạng (Các bộ quét bảo mật)	Các sản phẩm chống virus được thiết kế để phát hiện các phần mềm nguy hiểm như: virus, trojan…	Cả 3 đáp án trên.

Các chức năng quan trọng nhất của IDS	Giám sát	Cảnh báo	Bảo vệ	Cả 3 đáp án trên.
Các mô tả nào dưới đây là ưu điểm của NIDS?	Quản lý được cả một network segment (Gồm nhiều host)	Có thể phân tích được các lưu lượng đã được mã hóa (SSL, SSH, Ipsec..)	Trong suốt với người dùng và kẻ tấn công	Cho biết tấn công có thành công hay không
Các mô tả nào dưới đây là ưu điểm của HIDS?	Chỉ giám sát hoạt động trên một máy tính	Thường được đặt trên các host xung yếu của tổ chức và các máy chủ trong vùng DMZ	Trong suốt với người dùng và kẻ tấn công	Cả 3 đáp án trên đều sai
Những mô tả nào dưới đây được xem là ưu điểm của Honeypot?	Honeypot có thể thu thập một vài thông tin chi tiết	Honeypot là công nghệ đơn giản, ít lỗi và ít cấu hình sai	Honeypot nắm được các cuộc tấn công chống lại các hệ thống khác.	Honeypot làm việc tốt trong môi trường mã hóa hay Ipv6
Để kiểm soát các luồng dữ liệu cũng như thu thập các dấu hiệu tấn công và ngăn chặn tấn công của các tin tặc thì honeywall phải sử dụng các công cụ chính sau:	IDS snort	Firewall Iptables	Honeyd	Specter
Iptables cung cấp các tính năng nào sau đây:	Tích hợp tốt với Kernel (nhân) của Linux	Có khả năng phân tích gói tin hiệu quả	Lọc gói tin dựa vào địa chỉ MAC và một số cờ hiệu trong TCP header	Cả 3 đáp án trên.
Vai trò của tường lửa là gì?	Giám sát lưu lượng mạng	Điều khiển lưu lượng mạng	Phát hiện xâm nhập mạng	Cả 3 đáp án trên.
Phân loại tường lửa theo chức năng thì có những loại nào sau đây?	Tường lửa lọc gói tin	Tường lửa chống chuyển mạch	Tường lửa ứng dụng	Cả 3 đáp án trên.
Tường lửa ứng dụng hoạt động như thế nào?	Kiểm tra địa chỉ IP của gói tin	Kiểm tra nguồn và đích gói tin	Kiểm tra nội dung gói tin	Kiểm tra giao thức tầng ứng dụng của gói tin
Tường lửa ứng dụng hoạt động ở tầng nào?	2 và 3	3 và 6	4, 5 và 7	3,4,5,7
Tường lửa cổng chuyển mạch hoạt động theo quy tắc nào?	Kiểm tra phiên kết nối	Kiểm tra nội dung gói tin	Kiểm tra cổng nguồn và đích	Cả 3 đáp án trên
Tường lửa lọc gói kiểm tra thông tin gì của gói tin?	Nội dung	Phiên kết nối	Cổng nguồn và đích	Địa chỉ IP Nguồn và đích
Tường lửa cứng có các đặc điểm nào sau đây?	Phải mua HDH	Được cài đặt trên máy chủ thông thường	Là thiết bị tường lửa chuyên dụng	Tường lửa cài đặt trên máy tính cá nhân
Tường lửa nào sau đây không phải là tường lửa thương mai	Cisco	Juniper	Checkpoint	Iptables
Tường lửa không làm những việc nào sau đây?	Kiểm tra cổng nguồn - đích gói tin	Phát hiện mã độc	Kiểm tra phiên kết nối	Định danh người dùng
WEP sử dụng chuẩn mã hóa nào sau đây?	AES	ECC	RC4	DES

Phương tiện liên lạc trong hệ thống mạng không dây là?	Dây cáp	Access point	Ăng ten	Sóng điện từ
Thiết bị không dây truyền thông trực tiếp với nhau thông qua AP hoạt động trong chế độ nào sau đây?	Peer to client mode	Adhoc mode	Independent hoc mode	Infrastructure mode
Loại nào sau đây không phải là lớp hợp lệ cho Bluetooth	Class 0	Class 1	Class 2	Class 3
Tiến hành khảo sát vị trí làm việc của công ty	Phân phối khóa mạng WEP/WPA	Tìm hiểu và gỡ bỏ các truy cập không mong muốn	Lập kế hoạch và thiết kế mô hình mạng dây	Ghi lại các tín hiệu mạng không dây và gợi ý nâng cấp.
Công cụ Netstumber dùng để làm gì	Phát hiện xâm nhập mạng không dây	Khảo sát mạng	Nghe nén và giải mã từ công cụ CRT	Tấn công hệ thống mạng không dây
TEMPEST định nghĩa cho	Một phương pháp tấn công mạng có dây	Khái niệm tấn công mạng có dây	Công cụ nghe nén bị động	Công cụ thiết lập AP giả
Gửi thông điệp không được yêu cầu thông qua Bluetooth được gọi là	Bluecracking	Bluejacking	Karma	Bluesnifing
Bob đang lo lắng về an toàn của mạng không dây và anh ta đã vô hiệu hóa SSID. Bob bây giờ khẳng định mạng không dây của anh ấy không thể bị tấn công. Ban nên trả lời như thế nào?	Chặn bắt SSID là không thể vì nó đã bị vô hiệu hóa	Khi broadcast SSID đã bị vô hiệu hóa, nghe nén SSID chỉ có thể sử dụng thiết bị mở rộng đặc biệt	Bob chỉ đúng khi WEP 128bit được kích hoạt	Ngay cả khi tắt SSID thì vẫn có thể bị nghe nén qua mạng
Phát biểu nào sau đây về WPA2 là sai?	Sử dụng hệ mật RC4	Sử dụng hệ mật RSA	Sử dụng hệ mật AES	Sử dụng hệ mật TKIP
Kiểm soát an ninh vật lý và môi trường là một trong những biện pháp an toàn thông tin được đề cập trong ISO 17799-2005	Đúng	Sai		
Kiểm soát tính hoạt động liên tục là một trong những biện pháp quản lý ATTT được đề cập trong ISO 17799-2005	Đúng	Sai		
Theo tiêu chuẩn định nghĩa bởi Internet Engineering Task Force (IETE) VPN là sự kết nối các mạng WAN riêng sử dụng IP chia sẻ và công khai như mạng Internet hay IP backbones riêng	Đúng	Sai		

Thuật toán Diffe-Hellman, mỗi thực thể giao tiếp cần hai khóa một để phân phối cho các thực thể khác và một khóa là khóa riêng.	Đúng	Sai		
Thuật toán Diffe-Hellman thực hiện gồm 5 bước.	Đúng	Sai		
Trong lúc làm việc bạn phát hiện rằng ổ cứng của bạn hoạt động hết công suất mặc dù bạn không thực hiện bất kỳ thao tác nào trên máy tính. Bạn nghi ngờ điều gì?	Khả năng ổ đĩa ngừng hoạt động sắp xảy ra	Một virus đang phát tán rộng trong hệ thống	Hệ thống của bạn đang chịu một tác động từ tấn công DOS	Tấn công TCP/IP hijacking đang cố gắng thực hiện.
Bộ lọc gói thực hiện chức năng nào?	Cho phép tất cả các gói đi vào mạng	Cho phép tất cả các gói rời rạc	Ngăn chặn tất cả các gói trái phép đi từ bên ngoài	Loại trừ sự xung đột trong mạng
Thiết bị nào lưu trữ dữ liệu dẫn đường trong mạng	Hub	Modem	Firewall	Router
Giao thức nào được sử dụng rộng rãi hiện nay như một giao thức truyền tải đối với các kết nối sử dụng phương pháp quay số trên Internet	SLIP	PPP	PPTP	L2TP
Giao thức nào sau đây không phải là giao thức đường hầm nhưng lại sử dụng giao thức đường hầm để đảm bảo bảo mật trên mạng.	Ipsec	PPTP	L2TP	L2F
Một socket là sự kết hợp của những thành phần nào?	IP và sessionnumber	IP và portnumber	UDP và portnumber	TCP và portnumber
Thiết bị nào giám sát lưu lượng mạng một cách thụ động	IDS	Firewall	Sniffer	Web browser
Bạn nhận được một email từ microsoft trong đó có một file đính kèm trong thư nói rằng đã có một số lỗi được sửa, bạn phải chạy chương trình được đính kèm trong thư để sửa chữa các lỗi đó. Trong trường hợp này bạn sẽ làm gì để đảm bảo an toàn	Lưu chương trình đó lại và sử dụng chương trình diệt virus để quét, nếu không phát hiện thì mới chạy chương trình	Mở chương trình và chạy ngay, chương trình đó thực sự an toàn vì nó được gửi từ microsoft	Xóa email đó ngay, microsoft là nhà cung cấp không bao giờ gửi chương trình sửa lỗi qua mail.	Tất cả đều sai/
Hệ mật DES sử dụng khối khóa được tạo bởi	56 bit ngẫu nhiên	64 bit ngẫu nhiên	128 bit ngẫu nhiên	56 bit ngẫu nhiên và 8 bit kiểm tra "pairity"

Hệ mật DES xử lý từng khối Plain text có độ dài	56 bit	32 bit	64 bit	48 bit
Thuật toán SHA là gì?	Hàm băm một chiều	Dùng trong việc tạo chữ ký số	Cho giá trị băm 160 bit	Cả 3 đáp án trên
DSA là giải thuật gì?	Lấy dấu tay "Printing finger"	Tạo chữ ký số DS	Phân phối khóa	Bảo mật thông điệp
Thuật toán MD5 cho ra một giá trị băm có độ dài bao nhiêu	156 bit	128 bit	256 bit	512 bit
Trong các cặp khóa sau đây của hệ mật RSA p=5 q=7 cặp khóa nào có khả năng đúng nhất	c=12 d=11	c=4 d=11	e=7 d=23	e=3 d=18
Giải thuật Diffie-Hellman dùng để làm gì	Bảo mật thông điệp	Xác thực thông điệp	Phân phối khóa trước cho hệ mật đối xứng	Lấy chữ ký số
MAC là viết tắt của phương pháp bảo mật nào dưới đây	Mã xác thực thông báo (message authentication code)	Kiểm soát truy cập bắt buộc (mandatory accsess control)	Kiểm soát truy cập phương tiện (media access control)	Các ủy ban đa tư vấn (multiple advisory commites)
Phương pháp bảo mật nào sau đây không cần sử dụng mật mã	Bảo mật	Xác thực	Toàn vẹn	Điều khiển truy cập
Khái niệm nào sau đây được sử dụng để mô tả sự không thể chối bỏ của người gửi khi gửi thông điệp	Toàn vẹn	Tính không từ chối	Xác thực	Bảo mật
Quy trình mã hóa nào sử dụng cùng một khóa mã ở cả hai phía của một phiên làm việc	Symmetrical	Asymmetrical	PKCS	Split key
PKCS sử dụng cặp khóa nào để mã hóa	Symmetric	Private/public	Asymmetric/symmetric	Private/private
Vấn đề gì nảy sinh khi sử dụng quá trình sinh khóa mã tập trung	Bảo mật mạng	Truyền khóa	Thu hồi chứng chỉ	Bảo mật khóa cá nhân
Giao thức nào sau đây cung cấp dịch vụ bảo mật cho các phiên làm việc trên thiết bị đầu cuối của hệ thống UNIX từ xa?	SSL	TLS	SSH	PKI
Quá trình xác thực Typology của mạng được gọi là gì?	in dấu chân	Thiết bị làm nhiễu	Quét mạng	Liệt kê
Quá trình chiếm quyền truy cập đến tài nguyên mạng (Đặc biệt là các tập tin user và nhóm) được gọi là gì	in dấu chân	Quét	Thiết bị làm nhiễu	Liệt kê
Quá trình xác thực vị trí và thông tin mạng được gọi là gì	in dấu chân	Quét	Thiết bị làm nhiễu	Liệt kê
Đảm bảo an toàn thông tin có nghĩa là gì	Đảm bảo tính bí mật của thông tin	Đảm bảo tính toàn vẹn của thông tin	Đảm bảo tính sẵn sàng của thông tin	Cả 3 đáp án trên

Đảm bảo tính toàn vẹn của thông tin có nghĩa là gì	Giữ thông tin không bị sửa đổi trong khi chuyển đổi từ nơi phát đến nơi nhận vì bất kỳ lý do gì	Sử dụng những kênh liên lạc trực tiếp	Áp dụng các biện pháp mã hóa thông tin trên đường truyền	
Theo ISO 27001-2013 các yếu tố nào ảnh hưởng đến ATTT	Công nghệ, chính sách ATTT	Con người, công nghệ, chính sách ATTT	Con người, quy trình thủ tục, chính sách ATTT, công nghệ ATTT	
Rủi ro của hệ thống tỉ lệ thuận với	Nguy cơ mất ATTT của hệ thống	Điểm yếu của hệ thống	Cả 2 đáp án	
Muốn giảm nhẹ rủi ro cho HTTT chúng ta cần	Trang bị hệ thống tường lửa	Trang bị hệ thống chống virus	Loại trừ các điểm yếu bảo mật của hệ thống	
Phương án để giảm rủi ro ATTT bao gồm	Giảm nhẹ và loại trừ rủi ro	Chuyển giao rủi ro	Chấp nhập rủi ro	Cả 3 đáp án trên
"information security event" là thuật ngữ dùng để chỉ	Các hành động tấn công nhằm vào hệ thống	Các sự kiện vi phạm chính sách ANTT hay thất bại trong biện pháp bảo vệ tài sản thông tin xảy ra trong hệ thống dịch vụ hay mạng của tổ chức, hoặc một tình trạng hay sự việc xảy ra có liên quan đến ANTT	Một hay chuỗi các sự kiện ANTT không mong muốn hay bất ngờ xảy ra gây tổn hại nghiêm trọng đến hoạt động kinh doanh và đe dọa đến vấn đề ANTT	
"information security incident" là thuật ngữ dùng để chỉ	Các hành động tấn công mạng nhằm vào hệ thống	Các sự kiện vi phạm chính sách ANTT hay thất bại trong biện pháp bảo vệ tài sản thông tin xảy ra trong hệ thống dịch vụ hay mạng của tổ chức, hoặc một tình trạng hay sự việc xảy ra có liên quan đến ANTT	Một hay chuỗi các sự kiện ANTT không mong muốn hay bất ngờ xảy ra gây tổn hại nghiêm trọng đến hoạt động kinh doanh và đe dọa đến vấn đề ANTT	
Theo ISO 17799-2005 nhằm đảm bảo an toàn thông tin có bao nhiêu lĩnh vực cần kiểm soát	11 lĩnh vực	12 lĩnh vực	13 lĩnh vực	
Phần mềm quản lý, cập nhật bản vá Microsoft (windows server update services 3.0 - WSUS) có thể cập nhật những bản vá cho những hệ điều hành nào dưới đây (chọn tất cả các đáp án phù hợp)	Windows 95, 98 windows NT, windows ME	Microsoft windows server 2003	windows 2000, windows XP	windows vista

Câu trả lời nào dưới đây trả lời đúng chức năng của phần mềm quản lý cập nhật bản vá của micorsoft	Cập nhật bản vá cho tất cả các hdh	Cập nhật bản vá cho hdh windows	Cập nhật bản vá cho các phần mềm của microsoft	cả 3 đều sai
Phần mềm quản lý, cập nhật bản vá của microsoft (service 3.0) có thể cài đặt trên hdh nào	Windows 2000, service pack 4 trở lên	Windows server 2003	Windows server 2003, service pack 1	Windows XP service pack 2
Phần mềm quản lý cập nhật bản vá của microsoft có thể cập nhật những loại bản vá nào	Critical updates	security updates	Service packs	Cả 3 đáp án
Phần mềm quản lý cập nhật bản vá của microsoft (service 3.0) có thể cập nhật cho hệ điều hành 64 bit nào sau đây	Windows XP 64 bit edition	Windows 2003 datacenter edition	Windows Vista 64 Ultimate	Windows server 2008 64 bit
L2TP sử dụng phương thức xác thực nào để xác thực người dùng	PAP và SPAP	EAP	CHAP	MS-CHAP
Các mô tả nào dưới đây được coi là ưu điểm của phương pháp L2TP (Chọn 3)	Mất đáp án	Mất đáp án	Mất đáp án	Mất đáp án
Ipsec chạy ở lớp nào và sử dụng IKE để thiết lập SA giữa các đối tượng ngang hàng.	Lớp 1	Lớp 2	Lớp 4	Lớp 3
Những mô tả nào dưới đây được coi là ưu điểm của L2F	L2F kiểm soát bằng luồng	Độc lập với nền	Không cần phải đàm phán với ISP	Các giao dịch thực hiện trên đường hầm dựa trên L2F nhanh hơn khi so sánh với PPTP
PPTP đưa ra nhiều dịch vụ bảo mật xây dựng sẵn khác nhau cho PPTP server và client. Các dịch vụ bảo mật này bao gồm:	Mã hóa và nén dữ liệu	Xác thực	Kiểm soát truy cập và lọc gói tin	Cả 3 đáp an
PPP là giao thức truy cập vào internet và các mạng IP phổ biến hiện nay. Nó hoạt động ở lớp nào trong OSI	Tầng liên kết dữ liệu	Tầng mạng	Tầng giao vận	Tầng phiên
PPTP sử dụng PPP để thực hiện các chức năng thiết lập và kết thúc kết nối vật lý, xác định người dùng và tạo các gói dữ liệu PPP	Đúng	Sai		
Cơ chế xác thực nào dưới đây được sử dụng bởi giao thức PPP	Giao thức xác thực mở rộng EAP	Giao thức xác thực có thử thách bắt tay CHAP	Giao thức xác định mật khẩu PAP	Cả 3 đáp án

Các thiết bị bảo mật nào dưới đây không phải IDS	Giống câu 12	Giống câu 12	Giống câu 12	Giống câu 12
Chức năng quan trọng nhất của IDS là	Giám sát	Cảnh báo	Bảo vệ	Cả 3 đáp án
Giống câu 15	Giống câu 15	Giống câu 15	Giống câu 15	Giống câu 15
Như trên				
Những mô tả nào dưới đây được xem là nhược điểm của HIDS	Không có khả năng xác định người dùng liên quan đến một sự kiện	HIDS không có khả năng phát hiện các cuộc tấn công diễn ra trên một máy NIDS không có khả năng này	Không thể phân tích các dữ liệu mã hóa	HIDS phải được thiết lập trên từng host cần giám sát
Câu 23	**Câu 23**	**Câu 23**	**Câu 23**	**Câu 23**
Câu 24	**Câu 24**	**Câu 24**	**Câu 24**	**Câu 24**
Câu 25	**Câu 25**	**Câu 25**	**Câu 25**	**Câu 25**
Câu 26	**Câu 26**	**Câu 26**	**Câu 26**	**Câu 26**
Câu 27	**Câu 27**	**Câu 27**	**Câu 27**	**Câu 27**
Tường lửa cá nhân không làm những việc nào sau đây	Ngăn chặn một kết nối đã biết	Ngăn chặn một ứng dụng đã biết	Kiểm soát luồng dữ liệu cho một dải mạng	Giám sát lưu lượng mạng vào ra của máy tính
Công nghệ nào được sử dụng để chia một mạng bên trong thành mạng logic nhỏ hơn, dễ sử dụng hơn?	NAT	Tunneling	VPN	VLAN
Không sử dụng một liên kết chuyên dụng, phương pháp nào tốt nhất để nối hai mạng có khoảng cách địa lý các xa nhau để đảm bảo an toàn là gì?	VLAN	Tường lửa	DMZ	VPN
Sau khi cố gắng đăng nhập đến một máy tính trong ba lần, một người dùng thấy đã bị khóa tài khoản không cho phép truy cập vào hệ thống. Vấn đề này phù hợp nhất với điều gì dưới đây?	Tường lửa đã chặn truy cập đến máy tính	Tài khoản đã bị vô hiệu hóa bởi người quản trị	Hệ thống phát hiện xâm nhập đã vô hiệu hóa tài khoản của người dùng đó	Cổng mạng bị vô hiệu hóa
Giải pháp nào giúp các thiết bị mạng như Router hay Switch, cho phép điều khiển dữ liệu truy cập trên mạng	Tường lửa	Danh sách điều khiển truy cập ACL	Cập nhật vi chương trình	Giao thức DNS
Phần nào của một thiết bị phần cứng có thể được nâng cấp khả năng bảo mật tốt hơn và đáng tin hơn	Phần sụn (firmware)	Tập tin cấu hình	Cả A và B đúng	Cả A và B sai

Giao thức nào sau đây cần xóa trên thiết bị mạng quan trọng như Router	TCP/IP	ICMP	IPX/SPX	RIP
Giao thức nào sau đây cần xóa trên máy chủ email để ngăn chặn một tài khoản trái phép khai thác các điểm yếu bảo mật từ phần mềm giám sát mạng?	IMAP	POP3	TCP/IP	SNMP
Giải pháp nào cần phải thực hiện với một email server để ngăn chặn user bên ngoài gửi email thông qua nó?	Cài đặt phần mềm antivirus và antispam	Hạn chế chuyển tiếp tín hiệu SMTP	Xóa quyền truy cập POP3 và IMAP	cả 3 đều sai
Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ thống mật mã?	Hiệu quả	Bảo mật	Toàn vẹn	Không chối từ
Hệ mật nào mà người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa và khi giải mã?	Không đối xứng	Đối xứng	RSA	Diffie-Hellman
Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một chuẩn mã hóa dữ liệu?	DSA	ECC	3DES	AES
Hệ mật nào dưới đây mà người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã	Đối xứng	Bất đối xứng	Blowfish	Skipjack
Các giao thức mã hóa và các thuật toán nào sau đây được sử dụng như là nền tảng của cơ sở hạ tầng khóa công khai?	MD4	SHA	Diffie-Hellman	Skipjack
Giá trị hàm băm của hai thông điệp khác nhau có giá trị tương tự nhau, ta gọi hiện tượng này là gì?	Tấn công vào ngày sinh	Xung đột	Chữ ký số	Khóa công khai
Thực thể nào sau đây cho phép phát hành, quản lý và phân phối các chứng thư số?	Quyền cấp chứng chỉ (Certificate Authority)	Quyền đăng ký (Registation Authority)	Chính phủ NSA	PKI
Các phương pháp sinh trắc học nào sau đây được coi là an toàn nhất?	Phân tích chữ ký	Quét tiếng	Lấy dấu vân tay	Không quan trọng

Một người dùng gọi điện đến cho chúng ta (Với tư cách là người quản lý) thông báo họ bị mất mật khẩu và cần truy cập ngay lập tức. Ta nên làm gì?	Cung cấp truy cập ngay lập tức, và sau đó kiểm tra chứng cứ của họ.	Tạo một Login và mật khẩu tạm thời để họ sử dụng	Xác minh định danh của họ trước khi cấp quyền truy cập	Cho họ một mật khẩu riêng tạm thời
Phương pháp xác thực nào sử dụng một KDC để thực hiện xác thực?	Kerberos	CHAP	Sinh trắc học	Thẻ thông minh
Phương pháp xác thực nào gửi trả lại một yêu cầu cho máy trạm và yêu cầu đó sẽ được mã hóa và gửi lại cho máy chủ	Kerberos	Các mã thông báo bảo mật	DAC	CHAP
Giao thức hay các dịch vụ nào sau đây nên loại bỏ trong mạng nếu có thể?	Email	Telnet	ICMP	WWW
Kỹ thuật cho phép tạo kết nối ảo giữa hai mạng sử dụng một giao thức bảo mật được gọi là gì?	Tunneling	VLAN	Internet	Extranet
Khi được cung cấp về các mối đe dọa cho công ty từ phía các tin tặc. Loại thông tin nào sau đây có thể giúp ích nhiều nhất?	Xác minh tài sản sở hữu	Đánh giá rủi ro	Nhận dạng các mối đe dọa	Các điểm yếu
Khi một người dùng báo cáo rằng hệ thống của anh ta đã phát hiện một virus mới. Điều gì sau đây cần làm như là một bước đầu để xử lý tình huống này?	Kiểm tra lại phần mềm diệt virus hiện hành	Định dạng lại đĩa cứng	Cài lại HDH	Disable tài khoản email của anh ta
Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị tấn công từ bên ngoài?	Các tập tin ghi lại quá trình đăng nhập hệ thống Systemlog	Phần mềm antivirus	Kerberos	
Khi muốn cài đặt một máy chủ cung cấp dịch vụ web đến các máy trạm thông qua internet. Ta không muốn để lộ mạng bên trong để tránh rủi ro. Phương pháp nào để thực hiện điều này?	Cài đặt máy chủ trong mạng Internet	Cài đặt máy chủ trong một DMZ	Cài đặt máy chủ trong một VLAN	Cài đặt máy chủ trong một mạng Extranet
Loại tấn công nào sau đây dẫn tới truy cập hợp pháp của user bị từ chối?	DoS	Sâu	Logic Bomb (Bomb ngập đường truyền)	Social Engineering (khai thác giao tiếp)

Loại tấn công nào sau đây sử dụng nhiều hơn một máy tính để tấn công máy nạn nhân?	DoS	DDoS	Sâu	Tấn công UDP
Một máy chủ trên mạng có một chương trình đang chạy vượt quá thẩm quyền cho phép, loại tấn công nào đã xảy ra?	DoS	DDoS	Backdoor	Social Engineering (khai thác giao tiếp)
Nỗ lực tấn công để can thiệp vào một phiên liên lạc bằng việc thêm vào một máy tính giữa hai hệ thống được gọi là dạng tấn công gì?	MITM	Backdoor	Sâu	TCP/IP hijacking
Dạng tấn công sử dụng một chứng chỉ đã hết hạn hiệu lực vẫn đang được sử dụng nhiều lần để giành được quyền đăng nhập. Đây là loại tấn công nào?	MITM	Backdoor	Replay Attack	TCP/IP hijacking
Một máy chủ trên mạng không tiếp tục chấp nhận các kết nối TCP. Máy chủ thông báo rằng nó đã vượt quá giới hạn phiên làm việc. Loại tấn công nào có thể đang xảy ra?	Tấn công TCP ACK	Tấn công smurf	Tấn công Virus	TCP/IP hijacking
Tấn công smurf sử dụng giao thức nào để kiểm soát kết nối?	TCP	IP	UDP	ICMP
Dạng virus được đính kèm chính nó vào Boot sector của đĩa cứng và thông báo thông tin sai về kích thước các tệp tin được gọi là gì?	Trojan	Polimorphic Virus	Sâu	Stealth Virus
Một chương trình được ẩn trong một chương trình khác cài vào hệ thống nhằm mục đích không lành mạnh được gọi là gì?	Trojan	Polimorphic Virus	Sâu	Amored virus
Người dùng trong mạng nội bộ báo cáo hệ thống của họ bị lây nhiễm mã độc nhiều lần. Trong mọi trường hợp mã độc có vẻ là cùng một loại. Thủ phạm là?	Máy chủ có thể là vật nhiễm virus	Một máy trạm trong mạng nhiễm virus	Phần mềm antivirus hiện tại bị sự cố	Tấn công DoS

Các log files trên hệ thống của bạn ghi nhận một nỗ lực giành quyền truy cập đến một tài khoản đơn. Nỗ lực này không thành công vào thời điểm đó. Theo kinh nghiệm của bạn thì loại tấn công phù hợp nhất là gì?	Tấn công đoán mật khẩu	Backdoor	Sâu	TCP/IP hijacking
Một người dùng báo cáo anh ta đang nhận một lỗi chỉ ra rằng địa chỉ TCP/IP của anh ta đã bị sử dụng khi anh ta bật máy tính. Tấn công nào có thể đang thực hiện?	MITM	Backdoor	Sâu	TCP/IP hijacking
Bộ lọc gói thực hiện chức năng nào?	Cho phép tất cả các gói đi vào mạng	Cho phép tất cả các gói rời mạng	Ngăn chặn tất cả các gói trái phép đi từ bên ngoài	Loại trừ sự xung đột trong mạng
Các yêu cầu nào dưới đây dành cho VPN lớp 1?	Mã hóa dữ liệu dựa vào DES	Các cơ chế an toàn thêm vào như: AAA, RADIUS, TACACS, NAT hoặc tường lửa	Mã hóa dữ liệu dựa vào Ipsec và 3DES	Quản lý các khóa dựa vào IKE
Các yêu cầu nào dưới đây dành cho VPN lớp 2?	Mã hóa dữ liệu dựa vào Ipsec và 3DES	Một chính sách truy cập từ xa được định nghĩa rõ ràng	Quản lý các khóa dựa vào IKE	Phần mềm truy nhập quay số từ xa và khách hàng truy nhập từ xa
Các yêu cầu nào dưới đây dành cho VPN lớp 4?	Kết nối IPS với một SLA được định nghĩa rõ ràng	Dịch vụ thư mục tập trung nhưLDAP	MÃ hóa dữ liệu dựa vào DES	Các tùy chọn truy cập với tốc độ cao như ISDN và xDSL với T1 và T3
Cơ chế xác thực người sử dụng là khi người sử dụng ở các điểm VPN muốn truy xuất tài nguyên trong mạng thì phải được xác thực cho phép truy nhập bao gồm các thành phần sau?	ID và password	S/key password	A và B đúng	A và B sai
Mã hóa dữ liệu trong VPN có thể giúp ngăn chặn được tấn công gì sau đây?	Xem dữ liệu trái phép	Thay đổi dữ liệu	Dữ liệu giả	Bao gồm xem dữ liệu trái phép,thay đổi dữ liệu, dữ liệu giả
Những mô tả nào dưới đây đúng với phương pháp phát hiện tấn công dựa trên dấu hiệu?	Dễ phát hiện	Cho phản hồi chính xác về cảnh báo	Yêu cầu ít tài nguyên tính toán	Cả 3 đáp án
	Vì cậu đã kiên nhẫn xem được đến tận đây nên cậu xứng đáng qua môn này <3			