Tổng hợp các câu hỏi kiểm tra thử An Toàn Mạng

# Giao thức nào dưới đây được sử dụng rộng rãi nhất để truy cập kiểu quay số (Dial Up) tới 1 máy chủ từ xa (Chọn >=1 đáp án):

## SLIP

## RAS

## **PPP**

## TELNET

# Virus Macro chỉ có khả năng tấn công vào:

## Outlook Mail

## Word, Outlook Mail

## **Exel, Word, Outlook Mail**

## Exel, Word

# Kĩ thuật nào sau đây được sử dụng để chia 1 mạng bên trong thành mạng logic nhỏ hơn, dễ sử dụng hơn và hiệu năng mạng tốt hơn:

## VPN

## Tunneling

## **VLAN**

## NAT

# Với 1 laptop bị thất lạc, cần phải làm gì trước đó nhằm phòng tránh việc dữ liệu trên đó bị đánh cắp:

## Khóa không cho sử dụng ổ CD/DVD

## Sao lưu dữ liệu định kỳ ra USB/CD

## **Mã hóa dữ liệu trên laptop**

## Bật chế độ bắt buộc đăng nhập vào OS

# Phương pháp nào tốt nhất để kết nối 2 mạng ở 2 khoảng cách địa lý cách xa nhau:

1. VLAN

## **VPN**

1. DMZ
2. Firewall

# Các chuẩn giao thức mạng không dây IEEE nào dưới đây được sử dụng phổ biến nhát (Chọn >=1 đáp án):

## **802.11a**

## **802.11b**

1. 802.11

## **802.11g**

# Các yếu tố ảnh hưởng đến quá trình mã hóa:

1. Xung đột
2. Thuật toán mã, giải mã và tính an toàn của kênh truyền
3. Chữ ký số
4. ACL (Danh sách điều khiển truy cập)

# Nếu muốn xem tài liệu bảo mật bất đối xứng, ta sử dụng:

## Khóa cá nhân của bạn

## Khóa công khai của bạn

## Tính không chối từ

## Tất cả đều đúng

# Hai giao thức sử dụng trong IPSEC gồm:

## IP Authentication Header, TCP/IP

## TCP/IP, IP Encapsulating Sercurity Payload

## **IP Authentication Header, IP Encapsulating Sercurity Payload**

## Tất cả đều đúng

# Trong các hệ thống mật mã, đặc tính nào sau đây không thuộc chức năng bảo mật thông tin:

## Tính toàn vẹn

## Tính bảo mật

## **Tính hiệu quả**

## Tính không thể chối bỏ

# Khi giá trị 2 hàm băm của 2 thông điệp khác nhau có giá trị tương tự nhau gọi là:

## Thám mã

## Bắt gói tin

## Symmetrical

## **Xung đột**

# 2 cơ chế chính của hệ thống IDS Trigger để phát hiện khi có tấn công:

## IP Authentication Header, IP Encapsulating Sercurity Payload

## Phát hiện thay đổi, sử dụng bất bình thường

## Symmetrical, Phân phối khóa

## VPN, lọc MAC

# LAC và LNS là các thành phần của giao thức đường hầm nào:

## PPTP

## **L2TP**

## PPP

## IPSec

# Trên hệ thống mã hóa bất đối xứng, để giải mã ta sử dụng khóa nào:

## Khóa công khai bên gửi

## Khóa cá nhân bên gửi

## Khóa công khai bên nhận

## Khóa cá nhân bên nhận

# Chữ kí số dùng để:

## Phát hiện truy nhập trái phép

## Kiểm tra kết nối mạng

## **Kiểm tra định danh**

## Chuyển đổi địa chỉ

# Kĩ thuật nào cho phép kết nối đến mạng LAN của cty qua Internet thông qua 1 kênh được mã hóa an toàn:

## Kết nối qua mạng không dây sử dụng giao thức WEP

## Kết nối thông qua Telnet

## **Kết nối qua VPN**

## Kết nối thông qua Modem

# Hoạt động của virus có 4 giai đoạn:

## **Nằm im, lây nhiễm, khới sự và tàn phá**

## Lây nhiễm, nằm im, khới sự và tàn phá

## Khởi sự, lây nhiễm, nằm im và tàn phá

## Tất cả đều sai

# Chuẩn nào được chính phủ Mỹ sử dụng thay thế cho DES như là 1 chuẩn mã hóa dữ liệu:

## **AES**

## ECC

## DSA

## 3DES

# Hệ mật nào mà người gửi và người nhận thông điệp sử dụng các khóa mã khác nhau khi mã hóa và giải mã:

## Skipjack

## **Bất đối xứng**

## Đối xứng

## Blowfish

# Trong các giao thức đường hầm dưới đây, giao thức nào chỉ làm việc trên các mạng IP (Chọn >=1 đáp án):

## **L2TP**

## IPX

## PPTP

## **SLIP**

# Nhóm ứng dụng mạng nào có thể được sử dụng để phân tích và kiểm tra lưu lượng mạng:

## IDS/IPS

## **Sniffer**

## FTP

## Router

# Máy chủ RADIUS có mục đích để làm gì:

## Mã hóa

## Thỏa thuận tốc độ kết nối

## Packet Sniffing

## **Xác thực**

# Trong các mật khẩu dưới đây, mật khẩu nào là khó phá nhất đối với 1 thám mã:

## **!$aLtNb83**

## lnf0mr4t1on

## password123

## ThAngl0ng

# Trong an ninh mạng không dây, cơ cấu bảo mật nào là kém an toàn nhất:

## Mã hóa WEP 40 bit

## **Mã hóa WEP 128 bit**

## Bảo mật định danh mạng

## VPN

# Phương pháp điều khiển truy cập nào có hiệu quả và an toàn với mạng không dây (Chọn >=1 đáp án):

## **Lọc địa chỉ MAC**

## **Nhận dạng bảo mật mạng**

## Mã hóa WEP 40 bit

## VPN

# Thiết bị nào cho phép các máy trạm không dây truy cập vào mạng LAN rộng:

## VPN

## SHA

## **Wireless Access Point**

## Lọc MAC

# Thiết bị nào sử dụng bộ lọc gói và các quy tắc truy cập để kiểm soát truy cập đến các mạng riêng từ các mạng công cộng:

## **Firewall**

## Router

## Switch

## Điểm truy cập không dây

# Đối với tường lửa lọc gói, hình thức tấn công nào được thực hiện:

## **Giả mạo IP, tấn công đường đi nguồn, tấn công từng mẫu nhỏ**

## Thuật toán mã, giải mã và tính an toàn của kênh truyền

## ACL (Danh sách điều khiển truy cập)

## Tấn công thông điệp thì thời gian giải mã tỷ lệ kích thước khóa

# Trong hệ thống chứng thư số, khóa nào phải được sử dụng trong việc xác thực chữ ký của 1 người khác:

## Khóa công khai của bạn

## Khóa cá nhân của bạn

## **Khóa công khai của người cần xác thực**

## Khóa cá nhân của người cần xác thực

# Hệ mật nào mà người gửi và người nhận thông điệp sử dụng cùng 1 khóa mã khi mã hóa và giải mã:

## Bất đối xứng

## **Đối xứng**

# Khóa được sử dụng để ký vào 1 tài liệu trước khi gửi cho người khác:

## Khóa công khai của bên nhận

## Khóa công khai của bên gửi

## **Khóa cá nhân của bên gửi**

## Khóa cá nhân của bên nhận

# Kỹ thuật cho phép kết nối mạng LAN qua Internet:

## VPM

## VTM

## ATM

## VPN

## VBM

# Phương pháp điều khiển truy cập nào có hiệu quả và an toàn với mạng không dây:

## VPN

## SHA

## **Lọc MAC**

## Wireless Access Point

# Thuật giải MD5 cho ta 1 giá trị băm có độ dài:

## 512 bit

## **128 bit**

## 256 bit

## 156 bit

# Giao thức xác thực nào được sử dụng trong các mạng không dây (Chọn >=1 đáp án):

## 803.1

## **802.1X**

## **802.11a**

## **802.11b**

# Kỹ thuật nào được sử dụng để kết nối đến 1 máy chủ từ xa thông tin liên lạc qua một mạng không được bảo mật:

## **Telnet**

## VPN

## SLIP

## PPP

# Với tấn công dạng DoS, cách bảo vệ nào sau đây là tốt nhất có thể sử dụng nhằm chống lại tấn công tràn băng thông và bộ đệm của hệ thống:

## Ngừng kích hoạt dịch vụ WEB trên máy chủ WEB

## Đổi Subnet Mask

## Cài đặt phần mềm Antivirus

## **Chặn giao thức ICMP**

# Mục đích của chữ ký số:

## **Để kiểm tra định danh người gửi**

## Để bảo mật tài liệu sao cho người ngoài không đọc được

## Cung cấp 1 chứng chỉ

## Thu hồi 1 chứng chỉ

# Công cụ/Cơ chế bảo mật mạng không dây:

## SHA

## **WPA**

## WTA

## VCA

# DES sử dụng khối khóa được tạo bởi:

## 8 bit ngẫu nhiên

## 32 bit ngẫu nhiên

## 16 bit ngẫu nhiên

## **56 bit ngẫu nhiên**

# Thực thể nào sau đây cho phép phát hành, quản lý, và phân phối các chứng thư số:

## RA

## **CA**

## NSA

## PKI

# Hệ thống nào được cài đặt trên Host để cung cấp 1 tính năng phát hiện truy nhập trái phép:

## NIDS

## VPN

## **HIDS**

## Network sniffer

# Nhóm thiết bị hay phần mềm nào dưới đây nên được sử dụng nhằm theo dõi và cảnh báo tới nhà quản trị mạng khi có truy cập trái phép:

## Chương trình Antivirus

## **Hệ thống IDS**

## Router/Switch

## Dụng cụ phân tích mạng

# Nếu ta muốn kí vào 1 tài liệu và gửi cho người khác, ta dùng:

## **Khóa cá nhân của bạn**

## Khóa công khai của bạn

## Tính không chối từ

## Tất cả đều đúng

# Tấn công Smurf sử dụng giao thức nào trong quá trình kiểm soát:

## **ICMP**

## TCP

## UDP

## IP

# Thuật giải SHA là:

## Dùng trong thuật giải tạo chữ ký số

## Hàm băm 1 chiều

## Luôn trả về giá trị băm 160 bit

## **Tất cả đều đúng**

## Tất cả đều sai

# Các phát biểu nào sau đây là đúng:

## Tấn công thông điệp thì thời gian giải mã tỷ lệ kích thước khóa

## **Tất cả đều đúng**

## Hầu hết các thuật toán mã hóa là đối xứng

## Hầu hết các thuật toán mã hóa đối xứng đều dựa trên Ficstel

# Dạng tấn công nào gây ra khiến làm việc truy cập của người dùng đến các tài nguyên mạng bị từ chối (Chọn >=1 đáp án):

## Worm

## Logic Bomb

## **DOS**

## **DDOS**

# Kỹ thuật nào cho phép các địa chỉ mạng bên trong được “che dấu” khỏi các mạng bên ngoài và cho phép vài host của mạng bên trong sử dụng các địa chỉ trùng với mạng bên ngoài:

## VPN

## VLAN

## **NAT**

## IPSpoofing

# 2 giao thức sử dụng IPSec:

## **IP Authentication Header, IP Encapsulating Sercurity Payload**

## Phát hiện thay đổi, sử dụng bất bình thường

## Symmetrical, Phân phối khóa

## VPN, lọc MAC

# Trên 1 mạng không dây chuẩn 802.11b sử dụng giao thức bảo mật WEP, mức mã hóa nào dưới đây nên được thiết lập:

## 64 bit

## 32 bit

## **128 bit**

## 16 bit

# Loại tấn công nào cần sử dụng nhiều hơn 1 máy tính để tấn công nạn nhân:

## **DDOS**

## DOS

## Tấn công UDP

## Worm

# SHA là:

## Tính không chối từ

## **Băm 1 chiều, tạo chữ kí số, cho giá trị hàm băm 160 bit**

## Khóa cá nhân của bạn

## Kiểm tra định danh người gửi

\_THE END\_

Chúc các anh em thi tốt ^^!!!

**This document is**

**Edited by** Nam Nguyen Hai

**From Source**: Quân,

Việt “cao”,

Vượng “Stiga”,

Đỗ Anh Vũ,

Phạm Nghĩa NTT,

Trần An,

Thành “sâu sắc”,

Cường Phạm,

“Thánh cắt” Hưng Yên – Kiên GD,

“Thánh giật” Bắc Ninh - Duẩn “729”.