Giải pháp nào cho phép kiểm tra hành vi , nhật ký và sự kiện ứng dụng để tìm kiếm hoạt động đáng ngờ?

NIDS

HIDS

Spyware

Host-base firewall

Alice chịu trách nhiệm về tưởng lửa trong tổ chức của mình và phải đảm bảo rằng tất cả các tưởng lửa đucợ cấu hình đúng cách. Gateway firewall được cấu hình như sau: chỉ cho phép l;ưu lượng kết nối đến trên một vài cổng cụ thể; tất cả lưu lượng truy cập ( được phép hoặc bị chặn) đucợ ghi lại và chuyển tiếp các bản ghi tới SIEM. Điều gì bị thiếu trong cấu hình trên?

Xác thực chứng thư số cho lưu lượng đến

Quy tắc cho kết nối đi

Không có gì, đây là một cấu hình tốt

Mã hóa tất cả lưu lượng truy cập



Một máy chủ (hoặc ứng dung) chặn các yêu cầu mà máy khách gửi tới một máy chủ khác thực hiện các yêu cầu mà nó có thể và sau đó chuyển tiếp các yêu cầu mà nó không thể xử lý đến máy chủ khác, do dó giúp cải thiện hiệu suất và năng cao độ an toàn cho hệ thoogns. Đáp án nào dưới đây là đúng với mô tả trên ?

IDPS

Proxy Server

DNS Server

Database Server

Proxy firewall thực hiện kiểm soát tất cả lưu lượng mạng từ tầng mạng cho đến tầng ... Của mô hình OSI

Tầng ứng dụng

Tầng phiên

Tầng vật lý

Tầng giao vân

Một máy chủ đang chạy một ứng dụng cơ sở dữ liệu quan trong. Ứng dụng này trao đổi dữ liệu sử dụng giao thức có mã hóa. Charlie muốn giám sát máy chủ này để biết được các hoạt động đáng ngờ và ngăn chặn bất kỳ cuộc tấn công tiềm ẩn năng cao nào. Giai pháp nào dưới đây là tốt nhất cho theo yêu cầu của Charlie?

HIPS

HIDS

NIDS

NIPS

Tường lửa nào sau đây theo dõi trạng thái hoạt động và đặc điểm của các kết nối mạng đi qua nó?

Tường lửa lọc gói

Tường lửa ứng dụng

Tường lửa trạng thái

Tường lửa phi trạng thái



alert tcp

(msg: "FIN Dos"; sid:1000001; flags:F;)

alert tcp any any -> 192.168.1.107 any

alert tcp any any

Juanita là một quản trị viên hệ thống tại một trường đai học lớn. Tại đây có nhiều hệ thống. Cô ấy phải giám sát và phân tích nhật ký trên mỗi hệ thống đó. Cách tiếp cận tốt nhất để cô ấy xem và phân tích nhật ký từ máy chủ trung tâm là gì ?

Port fowarding

IDS

SIEM

NAC



Dữ liệu được mã hóa bằng L2TP/IPsec trong VPN được đóng gói trong giao thức nào?

PPP

AH

TLS/SSL

ESP

AH được sử dụng trong Ipsec để làm gì ?

Chỉ xác thực phần tiêu đề gói tin

Xác thực và đảm bảo toàn ven dữ liệu

Mã hóa toàn bộ gói tin

Chỉ mã hóa phần tiêu đề gói tin

Phát biểu nào đúng

TCP đảm bảo rằng sau một khoảng thời gian nào đó, gói tin phải đến đích. Do đó tạo nên tính tin cậy của dịch vụ

TCP và HTTP là những giao thức được cài đặt ở tầng giao vận

Telnet, HTTP, SMTP, FTP là những giao thức được cài đặt ở tầng ứng dụng

IP là giao thức được cài đặt ở tầng liên kết dữ liệu

Sau khi phân tích kỹ lưỡng, người quản trin mạng đã phát hiện ra tin tặc xâm nhập mạng bằng cách truy cập thông qua máy chủ VPN được cấu hình giao thức SSTP. Tin tặc đã dò đáon tên đăng nhập và mật khẩu. Lựa chọn nào sau đâuy là tốt nhất để ngăn ngừa sự cố tương tụ?

Triển khai xác thực mật khẩu mạnh cho VPN

Triển khai giao thức IPsec máy trạm

Sử dụng xác thực đa nhân tố

Tích hợp VPN với máy chủ xác thực tập trung

Hệ thống "IDS" có chức năng gì?

Phát hiện sự xâm nhập và ngăn chặn một số tấn công trên giao thức TCP

Phát hiện và ngăn chặn tấn công trên TCP

Phát hiện sự xâm nhập

Ngăn chặn sự xâm nhập

công cụ nào dưới đây không phải là tên gọi của một loại Honeypot?

T-pot

Dionaea

OSSEC

HoneyThing

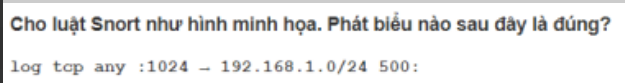
John đang chạy một IDS trên mạng của mình. Người dùng đôi khi báo cáo rằng IDS gắn cờ cho các lưu lượng truy cập hợp pháp là một cuộc tấn công. Đáp án nào sau đây mô tả điều này?

False flag

False negative

False trigger

False Positive

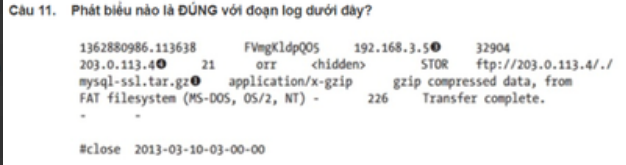


Ghi lại lưu lượng tcp từ các cổng lớn hơn hoặc bằng 1024 đến các cổng nhỏ hơn hoặc bằng 500

Không có phát biểu đúng

Ghi lại lưu lượng tcp từ các cổng nhỏ hơn hoặc bằng 1024 đến các cổng nhỏ hơn hoặc bằng 500

Ghi lại lưu lượng tcp từ các cổng nhỏ hơn hoặc bằng 1024 đến các cổng lớn hơn hoặc bằng 500



Giao thức FTP có hỗ trợ cả TCP và UDP

Tập tin mysql-ssl.tar.gz được tải về có kích thước là 32904 kb

Địa chỉ 192.168.3.5 thực hiện tải về tập tin mysql-ssl.tar.gz từ máy chủ ftp://203.0.113.4

Tập tin mysql-ssl.tar.gz được tải lên thành công qua ftp lên máy chủ 203.0.113.4

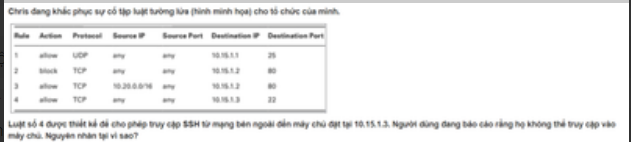
... Thực hiện việc theo dõi lưu lượng dữ liệu đến và đi để xác đinh các lưu lượng khả nghi. Trong trường hợp cần thiết cso thể tự động ngăn chặn các tấn công

IPS

NIDS

HIDS

DIDS



Cổng đích không được chỉ định

Tập luật khoong cso vấn đề gì. Chris nên kiểm tra các vấn đề khác

Giao thức không chính xác

Các luật được sắp xếp không đúng thứ tự

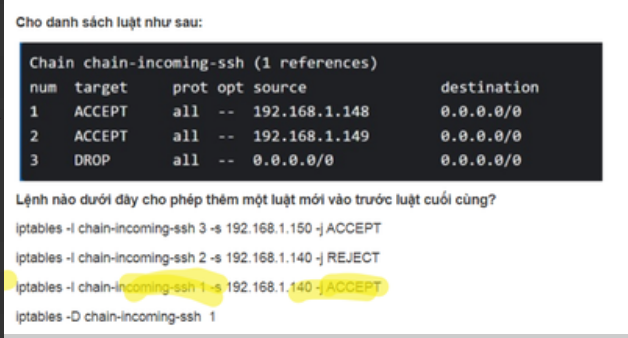
Mia là quản trị viên của một ngân hàng. Cô ấy chịu trách nhiệm đảm bảo an toàn cho kết nối của trang web của ngân hàng với khách hàng. Lựa chọn nào sau đây là tốt nhât để thực hiện việc này?

SSL

PPTP

Ipsec

TLS



Một công ty đã triển khai IPsec VPN cho người dùng truy cập từ xa. Cần sử dụng phương pháp nào sau đây để đảm bảo an toàn nhất cho kết nối của công ty trong trường hợp này ?

Chế độ ESP-only

Chế độ Transport ( mặc định )

Chế độ AH-only

Chế độ Tunel ( mặc định )



Ping Sweep

Port Scan

Tracetoute

Three-way handshake

Micheal là một quản trị mạng cho công ty thương mại, bao gồm cả mạng riêng ảo VPN. Anh ấy đang muốn thiết lập chế độ an toàn cho IPsec khi kết nối VPN. Lựa chọn nào sau đây được xem là phù hợp nhất

Kết hợp ESP và AH

Transport

IKE

AH



Nội dung tệp tin được giám sát bị thay đổi

Nội dung của tệp tin giám sát không thay đổi

Giá trị băm mật khẩu của tài khoản root bị thay đổi

Tài khoản root bị tấn công

Luật nào dưới dây cho phép chặn các kết nối SMTP đi?

Iptables -A INPUT -p tcp --sport 25 -j REJECT

Iptables -A INPUT -p tcp --dport 25 -j REJECT

Iptables -A OUTPUT -p tcp --sport 25 -j REJECT

Iptables -A OUTPUT -p tcp --dport 25 -j REJECT

Lina đang tìm kiếm các đề xuất cho các dịch vụ giám sát nội bộ. Cô ấy muốn có khả năng giám sát tất cả lưu lượng truy cập đến và đi từ gateway cũng như khả năng chặn một số nội dung nhất định. Khuyến nghị nào sau đây đáp ứng nhu cầu của Lina ?

Đề nghị vài IPS trên cả giao diện bên trong và bên ngoài của gateway router

Đề nghị vài đặt tường lừa trên giao diện trong NIDS trên giao diện bên ngoài của gateway router

Cài đặt IDS trên giao diện bên trong và tường lửa trên giao diện bên ngoài của bộ định tuyến cổng

Thiết lập lọc IP trên cả giao diện bên trong và bên ngoài của gateway

Kỹ thuật RAID nào sau đây có mục đích tăng tốc độ đọc ghi?

RAID 0

RAID 2

RAID 1

RAID 5

Lựa chọn nào sau đây miêu tả phù hợp nhất với khái niệm " Thời gian phục hồi - RTO" (Recovery Time Objective)?

Thời gian xác thực dữ liệu sau sự cố

Thời gian khôi phục dữ liệu từ bản sao lưu sau sự cố

thời gian phục hồi ứng dụng sau sự cố

Thời gian xác minh ứng dụng sau sự cố

Cách nào sau đây là tốt nhất và đơn giản nhất để chống lại lỗ hổng trong hệ điều hành ?

Sao lưu hệ thống thưởng xuyên

Tắt hệ thống khi không sử dụng

Cài đặt lại hệ điều hành thoogn dụng

Cài đặt bản vá mới nhất

Điều nào sau đây đúng khi nói về IDS ?

HIDS không cần phải thiết lập trên từng host cần giám sát

HIDS không thể phân tích các dữ liệu mã hóa

NIDS không có khả năng phát hiện tấn công trên một máy

NIDS cho biết việc tấn công có thành công hay không

Tersa chịu trách nhiệm xử lý sự cố trong công ty ACME. Gần đây hệ thống của công ty xảy ra một sự cố và ảnh hưởng đến nhiều máy tính trong mạng. Trong quá trình xử lý sự cố, Teresa tiến hành thu thập dữ liệu từ SIEM để tổng hợp log từ 20 máy chủ của công ty. Công việc đầu tiên cô ấy nên làm là gì?

Xác định bản chất của cuộc tấn công

Loại bỏ các sự kiện trùng lặp

Chuyển tiếp Log

Xác định IP nguồn tấn công

John là một quản trị viên của mạng công ty Wayne đã nhận được cuộc gọi điện thoại từ một cá nhân tự xưng là nhân viên ngân hàng và yêu cầu anh ấy cung cấp một số thông tin tài chính cá nhân. Kiểu tấn công nào sau đây có thể đang xảy ra ?

spear phising

0-day exploit

Vishing

MiTM

Lựa chọn nào dưới đây không phải là tấn công chủ động

Tấn công giả mạo

Tấn công nghe lén

Tấn công replay

Tấn công từ chối dịch vụ

Packet filter firewall lọc gói tin tại .....

Tầng mạng hoặc tầng giao vận

Tầng liên kết dữ liệu

Tầng vật lý

Tầng ứng dụng

Đâu không phải là một giao thức VPN?

PTPP

IPSec

L2F

PPTP

Luật nào dưới đây cho phép chặn các kết nối từ một địa chỉ IP cụ thể đến một giao diện mạng cụ thể ?

Iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP -j DROP

Iptables -A INPUT -s 192.168.1.100 -d 192.168.1.1 -p TCP -j REJECT

Iptables -A INPUT -s 192.168.1.0/24 -i eth0 -d 192.168.1.1 -p TCP -j DROP

Iptables -A INPUT -s 192.168.1.100 -i eth0 -d 192.168.1.1 -p TCP -j DROP

Peter muốn ngăn tất cả lưu lượng truy cập vào hoặc ra khỏi hệ thống Linux bằng tưởng lửa IPtables. Lệnh nào sau đây không phải là một trong 3 Lệnh IPtables cần để thực hiện hành động này?

Iptables-policy FORWARD DROP

Iptables-policy OUTPUT DROP

Iptables-policy SERVICE DROP

Iptables-policy INPUT DROP

Jame chịu trách nhiệm về tưởng lửa của công ty. Jame cần cấu hình tưởng lửa để chi cho phét gửi hoặc nhân email được mã hóa. Luật nào sau đây là phù hợp?

Cho phép các cổng 25, 110 và 443. Chặn các cổng 465, 993, và 143

Chăn các cổng 465, 994, 464. Cho phép các cổng 25, 110 và 80

Chặn các cổng 25, 110, 143. Cho phép các cổng 465, 993, 995

Cho phép các cổng 25, 110, 143. Chặn các cổng 465, 993, 995

Elizabeth chịu trách nhiệm và đảm bảo an toàn thông tin tại công ty. Cô ấy muốn cung cấp cho quản trị viên tùy chọn đăng nhập từ xa và thực thi các chức năng dòng lệnh tuy nhiên cô ấy muốn điều này chỉ có thể thực hiện được thông qua kết nối an toàn, được mã hóa. Elizabeth nên thực hiện hành động nào trên tường lửa ?

Chặn cổng 23 và cho phép cổng 22

Chặn cổng 22 và cho phép cổng 21 và 20

Chăn cổng 23 và cho phép cổng 21 và 20

Chặn cổng 22 và cho phép cổng 23

Quản trị viên hệ thống của một tổ chức cần trợ giúp từ một nhà cung cấp bên ngoài để khắc phục sự cố khẩn cấp với hệ thống kiểm soát vật lý (PACS) của tổ chứ. PACS hiện không truy cập được internet bởi vì nó chạy hệ điều hành cũ. Quản trị viên nên chọn phương thức nào sau đây để đảm bảo an toàn và hiệu quả để xử lý trong tinh huống này ?

Thiết lập kênh VPN cho nhà cung cấp và hạn chế quyền truy cập PACS bằng cách chia sẻ truy cập

Yêu cầu nhà cung cấp bên ngoài đến và cung cấp quyền truy cập trực tiếp vào PACS

Tạm thời cho phép bên ngoài internet có thể truy cập tới PACS thông qua thiết lập tính năng chia sẻ truy cập

Thiết lập hội nghị trực tuyến bằng web trên máy tinh cảu quản trị viên sau đó kết nối tới PACS

Chính sách tài khoản nào nên được thiết lập để ngăn chặn các tấn công vào tài khoản người dùng?

Vô hiệu hóa tài khoản không dùng đến

Giới hạn số lần đăng nhập sai

Thiết lập thời gian hết hạn tài khoản

Hạn chế khoảng thời gian đăng nhâp

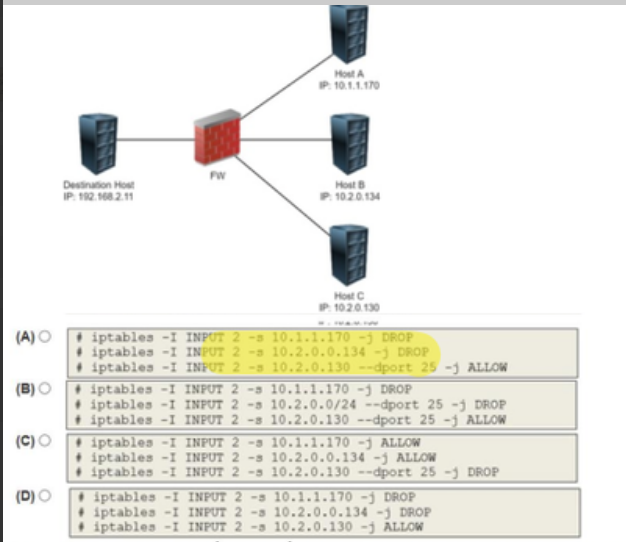
Trong quá trình làm việc. Peter khong phai block dải địa chỉ ip 221.194.15.0/28 bằng tưởng lửa IPTables. Lệnh nào sau đây cho Peter khắc phục vấn đề này ?

iptables -R INPUT -s 221.194.47.0/24 -j REJECT

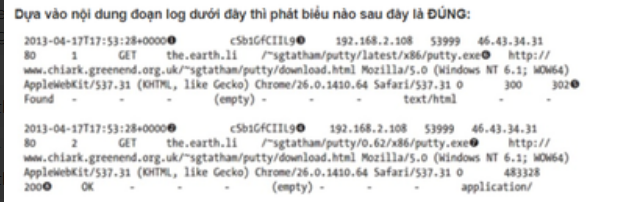
iptables -D INPUT -s 221.194.47.0/24 -j REJECT

iptables -D INPUT -s 221.194.47.0/24 -j ACCEPT

iptables -A INPUT -s 221.194.47.0/24 -j REJECT







Web server thực hiện chuyển hướng link download từ /~sgtatham/putty/latest/x86/putty.exe tới /~sgtatham/putty/0.62/x86/putty.exe

Client thực hiện gửi request Get Tới port 53999 trên web server

Client thực hiện việc download tập tin download.html

Client thực hiện việc upload tập tin putty.exe và lưu trữ tại domainame/~sgtatham/putty/latest/x86/putty.exe trên Webserver

Một công ty gần đây đã gặp phải tình trạn dữ liệu bị đánh cắp qua mạng công ty. Để đối phó với vi phạm, một chuyên gia attt khuyên người chủ công ty nên triển khai một giải pháp giám sát. Chuyên gia cho bt giải pháp có thể được thực hiện mà không cần mua thêm bất kì phần cứng mạng nào. Giải pháp nào sau đây nên được sử dụng để triển khai?

Network tap

Port mirroring

Honeynet

Network Proxy

Loại sao lưu nào dưới đây có tốc độc sao lưu nhanh nahast nhưng khôi phục dữ liệu chậm nhất ?

Sao lưu vì sai

Sao lưu định kỳ

Sao lưu gia tăng

Sao lưu đầy đủ

Tấn công SQL Injection thường giúp đoạt được quyền truy cập vào scwo sở dữ liệu bằng cách khai thác hệ thông của .....

Database server

Web application

Router

Operating System

Một quản trị viên hệ thống đang cấu hình VPN site-to-site. Giao thức nào được sử dụng để thực hiện quá trình trao đổi khóa và thỏa thuận các tham số bí mật ?

ESP

IKE

AH

PPP

Perter chịu trách nhiệm đảm bảo an toàn thông tin cho hệ thống của công ty. Trong quá trình rà soát, Peter đã phát hiện ra rằng NTP ( Network Time Protocol) không hoạt động bình thường. Giao thức nào có thể ảnh hưởng bới điều này?

DNSSEC

Radius

Kerberos

Ipsec

Điều nào sau đây đúng với HIDS?

HIDS hoạt động ảnh hưởng tới hiệu suất của máy trạm

HIDS giám sát toàn bộ mạng

HIDS không hiệu quả trong mạng dựa trên Switch

HIDS giám sát một mạng duy nhất

Các cuộc tấn công MiTM thường sử dụng giao thức nào sau đây ?

ARP

FTP

SCP

SIP

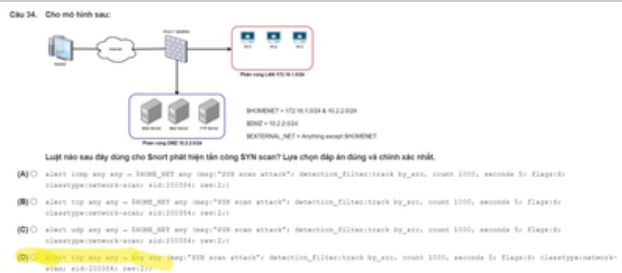
Angenla muốn chăn lưu lượng truy cập đến một máy chủ đọc hại có địa chỉ IP 10.24.31.11. Với tường lửa iptables được sử dụng?

iptables -A OUTPUT -d 10.24.31.11 -j DROP

iptables -A INPUT -d 10.24.31.11 -j ADD

iptables -block -ip 10.24.31.11 -j ADD

iptables -block-host 10.24.31.11 -j DROP



Cách sao lưu nào dưới đây có thể tiết kiệm được không gian bộ nhớ

Chỉ sử dụng sao lưu toàn phần

Sử dụng mã hóa

Sử dụng sao lưu gia tăng

Sử dụng hàm băm

Chức năng của mạng Honeynet là gì ?

Thu hút phân tích và cảnh báo xâm nhập

Phát hiện và ngắn chặn xâm nhập

Kiểm soát mạng dựa vào một tập luật có sẵn

Phân tích, cảnh báo và ngăn chặn mã độc dựa trên mẫu

IPS có khả năng nào sau đây mà IDS không có ?

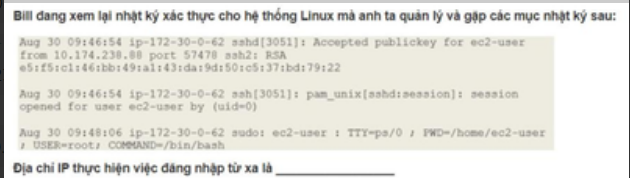
Cảnh báo tấn công

Ngăn chặn tấn công

Phát hiện tấn công

Giám sát tấn công



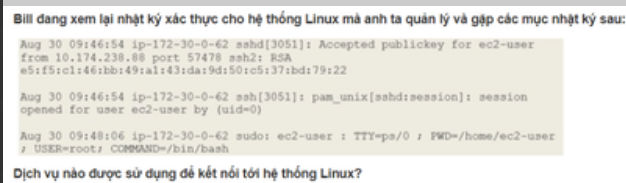


9.48.6.0

10.174.238.88

62.0.30.172

172.30.0.62



VPN

Telnet

SSH

HTTPS

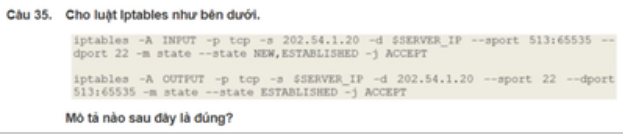
Tấn công APT là viết tắt của?

Applied Persistent Threat

Advanced Programmed Threat

Advanced Persistent Tool

Advanced Persistent Threat



SSH server có địa chỉ là 202.54.1.20

Khong có mô tả nào đúng

Cho phép kết nối SSH từ địa chỉ ip 202.51.1.20

Chi cho phép kết nối SSH từ địa chỉ IP 202.51.1.20 thông qua port 513

John chịu trách nhiệm về đảm bảo an toàn cho máy chủ email trong công ty. John muốn thực hiện mã hóa tất cả các email. John nên triên khai giao thức nào?

IMAP

POP3S

SMTP-S

S/MINE

Tường lửa nào sau đây không phải là sản phẩm thương mại?

Juniper

Cisco

CheckPoint

Iptable



Aler TCP

Alert TCP any any

(msg: "FIN Dos", sid:1000001: flag F;)

Alert TCP any any --> 192.168.1.107 any

... Thường được sử dụng đảm bảo an toàn cho kết nối từ nhà riêng hoặc người dùng từ xa.

Router-to-router VPNs

Remote access VPNs

Peer-to-Peer VPNs

Site-to-site VPNs