\_\_\_\_\_\_\_\_\_\_là một thiết bị phần cứng hoặc một chương trình phần mềm thực hiện giám sát thao tác gõ của người dùng máy tính

Script Kiddie

Keylogger

Macro

Adware

Luật nào sau đây cho phép phát hiện tấn công dò quét mật khẩu treen FTP server xuất phát từ vùng LAN?

alert udp $ DMZ 21 --> $HOMENET any (msg:"FTP Brute Force Attack"; flow: from\_server, established, content:"530";pcre:"/^530\s+(Login|User)/smi"; classtype:unsuccessful-user; threshold:type threshhold, track by\_dst, count 5, seconds 60, sid 2002383; rev:3)

alert tcp $ any --> DMZ 21 $HOMENET any (msg:"FTP Brute Force Attack"; flow: from\_server, established, content:"530";pcre:"/^530\s+(Login|User)/smi"; classtype:unsuccessful-user; threshold:type threshhold, track by\_dst, count 5, seconds 60, sid 2002383; rev:3)

alert tcp $ any --> DMZ 21 $EXTERNAL\_NET any (msg:"FTP Brute Force Attack"; flow: from\_server, established, content:"530";pcre:"/^530\s+(Login|User)/smi"; classtype:unsuccessful-user; threshold:type threshhold, track by\_dst, count 5, seconds 60, sid 2002383; rev:3)

alert tcp $ any --> $HOMENET any (msg:"FTP Brute Force Attack"; flow: from\_server, established, content:"530";pcre:"/^530\s+(Login|User)/smi"; classtype:unsuccessful-user; threshold:type threshhold, track by\_dst, count 5, seconds 60, sid 2002383; rev:3)

John đang tìm kiếm tường lửa cho một công ty nhỏ, John lo ngại về các cuộc tấn công DoS, đặc biệt là SYN flood. Loại tưởng lửa nào sau đây sẽ bảo vệ tốt nhất chống lại SYN flood?

Bastion

Stateful packet inspection (SPI)

Packet filter

Application Gateway

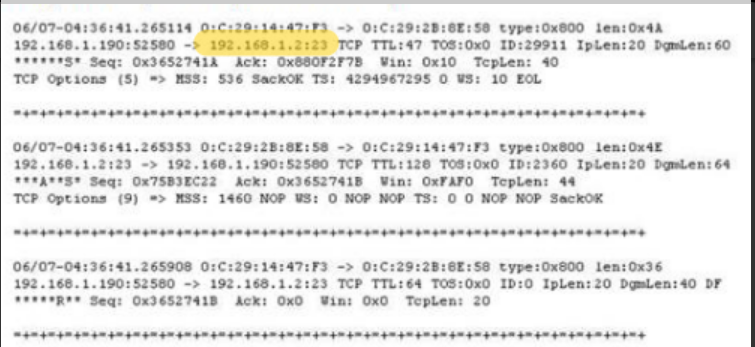
Phát biểu nào dưới đây là sai khi nói về tường lửa trạng thái?

Theo dõi mọi hoạt động của kết nối mạng đi qua nó

Lưu trạng thái của các phiên làm việc đang hoạt động

Sử dụng thông tin trạng thái để tăng tốc độ xử lý gói tin

An toàn hơn so với tưởng lửa lớp ứng dụng

Thông tin sau đây của Honeywall cho biết điều gì?

Máy đích đang mở cổng dịch vụ 23

Địa chỉ IP của máy đích là 192.168.1.190

Máy đích đang mở cổng dịch vụ 52580

Địa chỉ IP của máy nguồn là 192.168.1.2

Để ứng cứu sự cố an toàn thông tin được thuận lợi và nhanh chóng thì quy trình ứng cứu phải được đề cập trong giai đoạn nào khi triển khai mạng?

Phân tích, thiết kế an toàn mạng

Khảo sát mạng

Triển khai mạng

Vận hành, giám sát hoạt động của mạng

John đang quản lý hệ thống SIEM tại công ty mạng XYZ, Trước đó hệ thống mạng của công ty đã từng bị tấn công, một phần của cuộc tấn công này đã làm gián đoạn hoạt động của máy chủ NTP. Vấn đề nào sau đây của SIEM có khả năng bị ảnh hưởng nhất?

Trùng lặp sự kiện

Đồng bộ thời gian

Sự kiện không được ghi lại

Tương quan sự kiện

Phát biểu nào sau đây vè HoneyDrive là ĐÚNG?

HoneyDrive là môi trường tích hợp các honeypot

HoneyDrive là Honeypot

HoneyDrive không hỗ trợ phân tích mã độc

HoneyDrive là một dạng Honeypot tương tác cao

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

(A) iptables -A INPUT -s 192.168.1.0/24 -i eth0 -d 192.168.1.1 -p TCP -j DROP

B.) iptables -A INPUT -s 192.168.1.100 -i eth0 -d 192.168.1.1 -p TCP -j DROP

C). iptables -A INPUT -s 0/0 -d 192.168.1.1 -p TCP -j DROP

D).iptables -A INPUT -s 192.168.1.100 -d 192.168.1.1 -p TCP -j REJECT



Tấn công nào có thể đang diễn ra dựa vào đoạn log dưới đây?

Tấn công MiTM

Tấn công dò quét lỗ cổng

Tấn công bẻ khóa mật khẩu

Tấn công DNS

Phát biểu nào dưới đây không đúng về giao thức ESP

Trong chế độ đường hầm, toàn bộ gói tin IP được mã hóa

ESP vừa mã hóa, vừa xác thực dữ liệu

ESP sử dụng mật mã khóa công khai để mã hóa dữ liệu

ESP có khả năng chống lại tấn công phát lại

Nhật ký an toàn trên máy tính chứa đựng thông tin về các sự kiện xuất bên trong mạng và hệ thống của tổ chức. Tệp tin nhật ký của ứng dụng và máy chủ web rất hữu ích để phát hiện tấn công web. Nguồn gốc, bản chất và thời gian của tấn công có thể được xác định thông qua việc\_\_\_\_\_ của hệ thống bị xâm nhập

Phân tích tệp tin nhật ký

Lưu trữ tệp tin nhật ký

Thu thập tệp tin nhật ký

Cấu hình tệp tin nhật ký

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

Chế độ AH-only

Chế độ Transport(mặc định)

Chế độ ESP-only

Chế độ Tunnel(mặc định)

Phần nào được gọi là Rule Option trong luật Snort dưới đây

alert tcp any any - 192.168.1.107 any (msg: "FIN Dos"; sid: 10000001; flags: F)

(msg: "FIN Dos"; sid: 10000001; flags: F)

alert tcp any any - 192.168.1.107 any

msg: "FIN Dos"

alert tcp

Sau khi cố gắng đăng nhập đến một máy tính trong 3 lần, một người dùng thấy đã bị khóa tài khoản, không được phép truy cập vào hệ thống. Vấn đề này phù hợp nhất với điều gì dưới đây?

Hệ thống phát hiện xâm nhập đã vô hiệu hóa tài khoản của người dùng đó

Tài khoản đã bị vô hiệu hóa bởi chính sách an toàn

Tưởng lửa đã chặn khi truy cập đến máy tính

Cổng mạng đã bị vô hiệu hóa

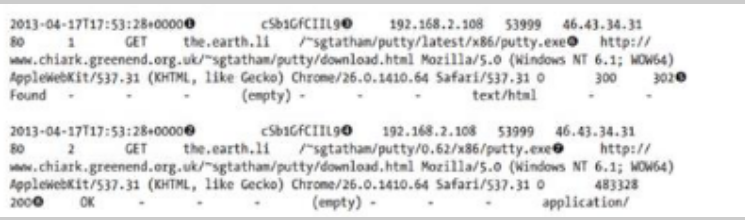
\_\_\_\_\_\_ thực hiện việc theo dõi các lưu lượng dữ liệu đến và đi để xác định các lưu lượng khả nghi.Trong trường hợp cần thiết có thể tự động ngăn chặn các tấn công.

(A) Intrusion prevention system

(B) Distributed intrusion detection system

(C) Network Intrusion detection system

(D) Host intrusion detection system



Dựa vào nội dung đoạn log dưới đây thì phát biểu nào sau đây là đúng

(A) . Clent thực hiện việc upload tập tin putty.exe và lưu trữ tại domainname/~sgtatham/putty/lastest/x86/putty.exe trên Webserver

B). Client thực hiện việc download tập tin download.html

C). Client gửi một request GET tới port 53999 trên Webserver

D). Webserver thực hiện chuyển hướng link download từ ~sgtatham/putty/lastest/x86/putty.exe tới ~sgtatham/putty/0.62/x86/putty.exe

Câu lệnh nào dưới đây được sử dụng để xóa tạo 1 chain trong Iptables?

iptables -A old\_chain

iptables -E old\_chain

iptables -X old\_chain

iptables -N old\_chain

Một hệ thống có hai máy chủ A và B. Hệ thống này có áp dụng biện để đảm bảo tính liên tục sao cho A sẽ phản hồi tất cả các yêu cầu nếu không có bất kỳ lỗi phần cứng nào hoặc không có người nào can thiệp vào cáp mạng của nó và không có bất kỳ thảm họa nào xảy ra với trung tâm dữ liệu. Và trong trường hợp máy chủ A không thể đáp ứng được các yêu cầu thì máy chủ B có thể tiếp quản. Hãy cho biết hệ thống đã áp dụng biện pháp nào?

Giải pháp cân bằng tải

Ứng phó sự cố

Giải pháp chịu lỗi (failover)

Phòng thủ theo chiều sâu

Dominick chịu trách nhiệm về hệ thống IDS/IPS tại một công ty bảo hiểm quy mô vừa. Công ty muốn ưu tiên khả năng phát hiện và ngăn chặn kịp tức thời các cuộc tấn công tiềm tàng thì các hệ thống IDS/IPS này cần phải được triển khai như thế nào? Chọn đáp án chính xác nhất

Triển khai ở chế độ Passive

Triển khai ở chế độ Inline detection

Triển khai ở chế độ Inline Protection

Triển khai ở chế độ Sniffer

Trong quá trình thực hiện giám sát an toàn thông tin, việc lưu giữ nhạt ký hệ thống trong sáu tháng hoặc lâu hơn có thể có giá trị cho những hoạt động nào sau đây?

Quản lý định danh và thẩm quyền

Điều khiển truy cập vật lý và logic

Khôi phục sau thảm họa và vân hành liên tục

Điều tra số và xử lý sự cố

Mô tả nào dưới đây là SAI về HIDS?

Cài đặt đơn giản, dễ dàng và dùng trên các máy riêng lẻ

Có khả năng phát hiện các tấn công trên một máy cụ thể

Có mức độ hiển thị và kiểm soát tốt hơn so với NIDS

Không ảnh hưởng tới hoạt động của máy chủ mà trên đó nó được thiết lập

Tạo luật nào dưới đây nên được thiết lập trên tường lửa như là luật mặc định

iptables -A INPUT -j chain-states

iptables -A OUTPUT -j chain-states

iptables -A INPUT -p tcp -m tcp -j DROP

iptables -A OUTPUT -p tcp -j DROP

iptables -A OUTPUT -p tcp -m tcp -j DROP

iptables -P INPUT DROP

iptables -P OUTPUT FORWARD

iptables -P OUTPUT DROP

iptables -A INPUT -i lo -j DROP

iptables -A OUTPUT -o -lo -j DROP

Teresa chịu trách nhiệm xử lý sự cố cho công ty ACME. Gần đây hệ thống của công ty vừa 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

Chuyển tiếp log

Xác định nguồn tấn công

Loại bỏ các sự kiện trùng lặp

Xác định bản chất cuộc tấn công

Thuật toán nào sau đây trong Loadbalancing lựa chọn máy chủ dựa vào công suất định mức của máy chủ?

Fastest

Weighted Round Robin

Round Robin

Least Connections

eter cang thiết lập luật cho IDS của công ty nhằm bảo vệ hệ thống Webserver. Anh ấy muốn hệ thống IDS sẽ đưa ra cảnh báo tấn công ICMP Flood nếu trong vòng 1 phút Webserver nhận được vượt quá 5000 -MGP request - Luật nào dưới đây cho phép thực hiện việc này ?

A. Alert icmp any any --> SDMZ any (msg:"ICMP flood"; sid 10000001; rev:1; classtype:icmp-event;detection\_filter:track by\_dst, count 5000, seconds 1;)

B. Alert icmp any any --> SDMZ any (msg:"ICMP flood"; sid 10000001; rev:1; classtype:icmp-event;detection\_filter:track by\_dst, count 5000, seconds 600;)

C. Alert icmp any any --> SDMZ any (msg:"ICMP flood"; sid 10000001; rev:1; classtype:icmp-event;detection\_filter:track by\_dst, count 5000, seconds 60;)

D. Alert udp any any --> SDMZ any (msg:"ICMP flood"; sid 10000001; rev:1; classtype:icmp-event;detection\_filter:track by\_dst, count 5000, seconds 60;)

Pêtrr đang thực hiện điều tra số trên một chiếc máy tính nghi ngờ bị tấn công. Pêtrr nhận thấy một số kết nối mạng sử dụng SSL trên các cổng không phổ biến, bản sao của svhost.exe và cmd.exe trong thư mục %TEMP%, và các tệp RDP đã kết nối với một địa chỉ IP bên ngoài. Tấn công nào có thể diễn ra ở đây?

Ransomware

APT

MiTM

DDoS

Mery được hướng dẫn để đưa một hệ thống bị ảnh hưởng bởi sự cố trở lại môi trường của công ty và đảm bảo rằng hệ thống đó sẽ không gây ra một sự cố khác. Mary tiến hành các hoạt động khôi phục hệ thống thông tin dữ liệu và kết nối; cấu hình hệ thống an toàn, bổ sung các thiết bị, phần cứng phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin. Vây Mary đã hoàn thành bước nào trong quá trình ứng cứu sự cố?

Tổng kết, đánh giá

Ngăn chặn

Khôi phục

Chuẩn bị

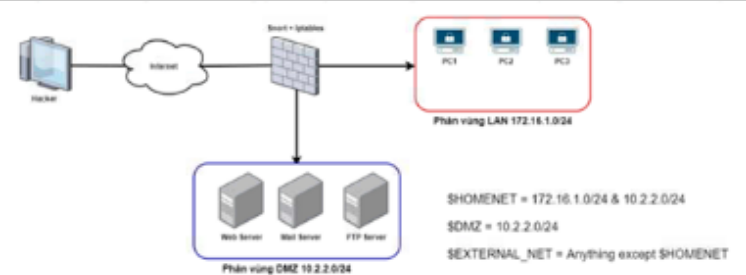
Robert dang cấu hình VPN dựa trên IPsecAnh ấy lo lắng việc bất kỳ ai cũng có thể chặn bắt gói tin cả phân tích và lấy được thông tin và lưu lượng kết nối. Chế độ nào sau đây là tốt nhất để ngăn chặn điều này?

AH

ESP

Transport

Tunneling



alert tcp any any --> $HOMENET any (msg:"SYN scan attack"; detection\_filter:track by\_src, count 1000, seconds 5, flags:S; classtype:network-scan; sid:200384; rev:2;)

alert tcp any any --> $HOMENET any (msg:"SYN scan attack"; detection\_filter:track by\_src, count 1000, seconds 5; classtype:network-scan; sid:200384; rev:2;)

alert tcp any any --> $HOMENET any (msg:"SYN scan attack"; detection\_filter:track by\_src, count 1000, seconds 1000, flags:S; classtype:network-scan; sid:200384; rev:2;)

alert tcp $HOMENET any --> any any (msg:"SYN scan attack"; detection\_filter:track by\_src, count 1000, seconds 5, flags:S; classtype:network-scan; sid:200384; rev:2;)

John là quản trị viên của một hệ thống Linux. Anh ấy phải thiết lập tập lệnh nào dưới đây để cho phép một máy tính bên ngoài PING vào ben trong mạng?

iptables -I INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -I OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-reply-j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

Frank là quản trị viên của một NIDS đơn giản. Tuy nhiên, NIDS dường như chỉ phát hiện được các cuộc tấn công có trong cơ sở dữ liệu. Để NIDS này có thể phát hiện được các tấn công mới thì cần bổ sung công nghệ gì?

Passive Scanning

Statistical anomaly scanning

Signature Scanning

Acticve Scanning

Hệ thống HIPS thường được triển khai ở chế độ giám sát hoặc học tập trong quá trình triển khai ban đầu của chúng. Mục tiêu của việc bắt đầu ở chế độ này là gì?

Tự động đưa vào danh sách trắng các hành động hoặc tệp mà hệ thống đã biết

Tự động đưa vào danh sách trắng các hành động hoặc tệp àm hệ thống đã biết

Xây dựng đường cơ sở về các sự kiện bình thường hoặc an toàn của hệ thống để xem xét

Xác định tệp nào không an toàn để truy cập và đưa chúng vào danh sách đen

Một quản trị viên đã phát hiện ra một sự cố liên quan đến phần mềm độc hại. Dựa vào quy trình ứng phó sự cố theo Thông tư số 20/2017/TT-BTTTT, bước tiếp theo ta phải làm gì?

Gỡ bỏ

Ngăn chặn

Phục hồi

Xác định sự cố

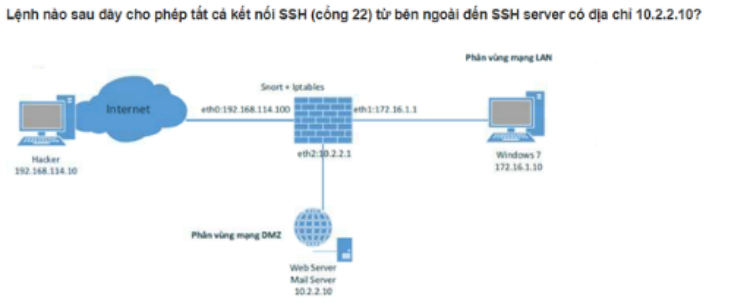
Trong quá trình ứng cứu sự có, Susan cho phép hệ thống truy cập lại vào mạng bình thường. Susan đang thực hiện giai đoạn nào của quy trình ứng phó sự cố?

A) . Ngăn chặn, gỡ bỏ và phục hồi

B) . Chuẩn bị

C) . Tổng kết, đánh giá

D) . Phát hiện và phân tích

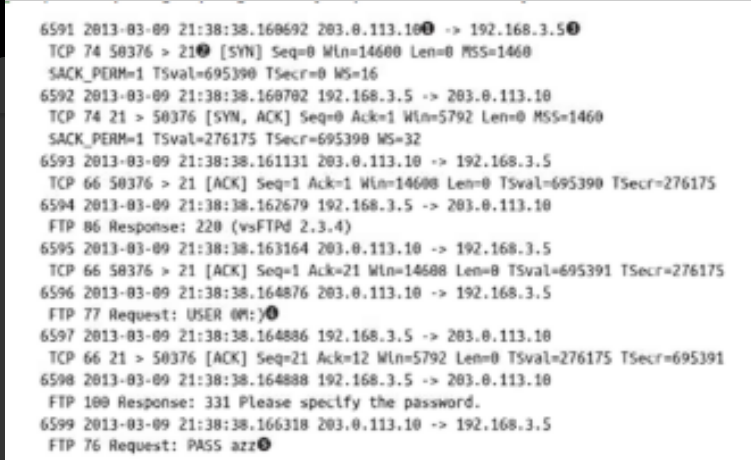


iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-destination 192.168.114.100

iptables -t nat -A PREROUTING -p tcp -i eth0 0d 192.168.114.100 --dport 2 -j DNAT --to-destination 10.2.2.10

iptables -t nat -A POSTROUTING -i eth2 -p tcp -sports 22 -j SNAT --to-destination 10.2.2.10

iptables -A INPUT -o eth0 -p tcp --sport 22 -m state NEW, ESTABLISHED -j ACCEPT



Dựa vào nội dụng đoạn log dưới đây thì phát biểu nào sau đây là đúng

Dịch vụ Telnet được sử dụng trên cổng 21

Quá trính bắt tay 3 bước được hoàn tất

Máy chủ FTP có địa chỉ là 203.0.113.10

Người dùng đăng nhập dịch vụ FTP thành công

Vào một buổi sáng, John kiểm tra các hành động đăng nhập trên máy chủ nhật ký của công ty. Anh ấy thấy rằng tài khoản DBAmin có 05 lần đăng nhập sai được cảnh báo. Tuy nhiên tài khoản DBAmin này chỉ là tài khoản giả lập do John tạo ra và được sử dụng để thu hút tấn công. Giải pháp nào đang được John sử dụng trong trường hợp này?

Rule-based access control

Honeypot

Role-based access control

Blacklist

Giao thức IPsec hoạt động tại tầng nào trong mô hình OSI?

Tầng trình diễn

Tầng mạng

Tần vận chuyển

Tầng ứng dụng

Tường lửa thực hiện kiểm tra sâu gói tin nhờ kỹ thuật\_\_\_\_\_\_\_

Protocol Decoding

Pattern Matching

IP Spoofing

Session Splicing

Lệnh nào dưới đây cho phép xóa bỏ 1 rule cụ thể của 1 chain được chỉ định?

iptables -R chain

iptables -D chain rulenum

iptables -R chain rulenum

iptables -D chain

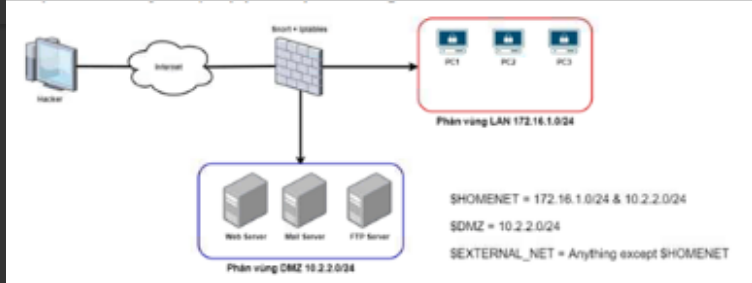
Michael là một quản trị mạng cho công ty thương mại, bao gồm cả mạng riêng ảo VPN. Anh ấy đang muốn thiết lập chế độ an toàn nhất cho IPsec khi kết nối VPN. Lựa chọn nào sau đây được xem là phù hợp nhất

AH

IKE

Kết hợp AH và ESP

Transport



Luật nào sau đây cho phép phát hiện tấn công Web-LFi?

(A) O alert top SHOMENET 80-$DMZ 80 (msg : "Web local file inclusion attack; urkicontent : "/etc/passwd"; nocase; classtype : web-application-attack; sid : 2002387 : priority : 2:)

(B) O alert top any anyany any (msg : "Web local file inclusion attack"; uricontent : "/etc/passwd"; nocase; classtype : web-application-attack; sid : 2002387; priority : 2:)

(C)Valert top any any-SHOMENET 80 (msg"Web local file inclusion attack"; uricontent : "/etc/passwd"; nocase; classtype : web-application-attack; sid : 2002387; priority : 2:;)

(D) O alert top any any-SDMZ 80 (msg"Web local file inclusion attack; uricontent : "/etc/passwd"; nocase; classtype : web-application-attack; sid : 2002387; priority : 2;)

Tệp nào sau đây tin tặc có thể sửa đổi sau khi giành quyền truy cập vào hệ thống để thực hiện tấn công chuyển hướng DNS?

Services

SAM

hosts

/etc/passwd

Peter thực hiện việc quét cổng dịch vụ (port) của hệ thống máy chủ cơ sở dữ liệu và thấy rằng port 3306 đang mở. Máy chủ có khả năng đang chạy cơ sở dữ liệu nào?

Oracle

Microsoft SQL Server

MySQL

Postgres

Cho luật snort như hình minh họa, Phát biểu nào sau đây là đúng?

log tcp any :1024 - 192.168.1.0/24 500:

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

Ghi lại tất cả lưu lượng TCP tới mạng con 192.168.1.0/24

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

Carrol chịu trách nhiệm về kết nối mạng trong công ty của mình. Bộ phận kinh danh đang chuyển đổi sang VoIP. Hai giao thức mà cô ấy phải cho phép thông qua tường lửa là gì?

TCP và UDP

SIP và RTP

RADIUS và SNMP

RADIUS và SIP

Elizabeth chịu trách nhiệm quản lý hệ thống SIEM cho một công ty. Có áy theo dõi màn hình hệ thống SIEM hàng ngày, kiểm tra hàng giờLựa chọn nào sau đây sẽ là cách tiếp cận tốt nhất cũ cô ấy cập nhật các vấn đề xuất hiện trong nhật ký?

(A) . Không cần làm gì thêm

B.) Tự động cảnh báo

(C). Nhật kỳ được chuyển tiếp tới email.

D). Xem lại nhật ký của SIEM khi sự có xảy ra.

Mạng Intranet VPN thường được sử dụng để kết nối?

A.)Các văn phòng chi nhánh của tổ chức với mạng Intranet trung tâm.

B). Các văn phòng chi nhánh với nhau

C). Chỉ trong một chi nhánh

A, B C đều đúng

Kỹ thuật nào được IDS sử dụng để kiểm tra một mẫu nhằm xác định hoạt động có phải là trái phép hay không?

Session Splicing

Protocol Decoding

State Table

Pattern Matching

Yếu tố nào sau đây thường được sử dụng kết hợp với một thẻ thông minh để thực hiện xác thực mạnh?

Thẻ nhớ

Mã PIN

USB-Token

Quét võng mạc

Edward chịu trách nhiệm về đảm bảo an toàn ứng dụng web tại một công ty bảo hiểm lớn. Anh ấy muốn có một phương pháp xác thực mạnh để giảm thiểu các rủi ro bị tấn công. Lựa chọn nào sau đây là tốt nhất?

Xác thực gói tin trong mạng

Xác thực người dùng sử dụng mật khẩu mạnh

Xác thực người dùng sử dụng chứng thư số

Xác thực máy chủ ứng dụng Web

John lo lắng về việc kẻ tấn công đang liệt kê (enumerating) tất cả mạng của mình. Giao thức nào sau đây có thể giúp ít nhất giảm thiểu vấn đề này?

LDAPS

TLS

HTTPS

IPsec

Peter – CHO của công ty Wayne đã nhận được emall trong như có và từ ngân hàng với thông báo về việc các thông tin thẻ tín dụng của anh ấy có thể đã bị lộ và cần phải truy cập vào lường linh gửi kèm trong email để thay đổi của thông tin đó. Chọn đáp án phù hợp nhất cho loại tấn công có thể đang diễn ra.

Vishing

Pharming

Phishing

Whaling

\_\_\_\_\_\_\_\_\_\_\_\_\_là một tập các câu lệnh thường được lưu trữ trên firewall(router, switch) dùng để điều khiển truy cập vào, ra hệ thống mạng với các hành động tương ứng cho phép hoặc cấm

State Table

Packet Filter

Access Control List (ACL)

Session Splicing

Luật nào sau đây cho phép toàn bộ các địa chỉ IP kết nối đến máy chủ POP3S có địa chỉ IP 202.54.1.20 và các kết nối đi từ máy chủ này?

iptables -A INPUT -p tcp -s 0/0 -sport 1024:65535 -d 202.54.1.20 -dport 995 -m state -state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p TCP -s 202.54.1.20 -sport 995 -d 0/0 -dport 1024:65535 -m state NEW,ESTABLISH -j ACCEPT

iptables -A INPUT -p tcp -s 202.54.1.20 -sport 1024:65535 -d 0/0 -dport 995 -m state -state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p TCP -s 0/0 -sport 995 -d 202.54.1.20 -dport 1024:65535 -m state NEW,ESTABLISH -j ACCEPT

iptables -A INPUT -p tcp -s 0/0 -sport 1024:65535 -d 202.54.1.20 -dport 995 -m state -state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p TCP -s 202.54.1.20 -sport 995 -d 0/0 -dport 995 -m state NEW,ESTABLISH -j ACCEPT

iptables -A INPUT -p tcp -s 172.16.0.0/0 -sport 1024:65535 -d 202.54.1.20 -dport 995 -m state -state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p TCP -s 202.54.1.20 -sport 995 -d 172.16.0.0/0 -dport 1024:65535 -m state NEW,ESTABLISH -j ACCEPT

Một công ty gần đây đã gặp phải tình trạng 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 biết giải pháp có thể được thực hiện mà không cần mua thêm bất kỳ phần cứng mạng nào. Giải pháp nào sau đây nên được sử dụng để triển khai?

Honeynet

Network proxy

Port mirroring

Network tap

Pêtrr muốn triển khai dịch vụ truyền file bằng cách sử dụng SSH. Lựa chọn nào sau đây là đúng?

LDAPS

SFTP

SSH

FTPS

IKE sử dụng cổng dịch vụ mặc định nào dưới đây?

135

500

514

530