HỌC VIỆN KTMM
PHÒNG KT&ĐBCLĐT

ĐỀ THI CHÍNH THỨC
(Đề thi có 14 trang)

ĐỀ THI MẪU ĐỂ CÔNG BỐ
Môn thi: AN TOÀN MẠNG MÁY TÍNH
Thời gian làm bài: 60 phút, không kể thời gian phát đề

Họ, tên thí sinh: ....
Số báo danh: ....

Mã đề thi 949

Câu 1. Bộ lọc nào sau đây trong Wireshark cho phép hiển thị tất cả gói tin có cờ SYN được bật?

A. tcp.flags & 0x10
B. tcp.flags & syn
C. tcp.flags.syn==0
D. tcp.flags & 0x02

Câu 2. Martin muốn cài đặt một hệ thống kiểm soát mạng máy tính có khả năng ngăn chặn thất thoát các thông tin nhạy cảm của công ty. Giải pháp nào sau đây sẽ hiệu quả nhất để đạt được mục tiêu đó?

A. IDS
B. DLP
C. Firewall
D. IPS

Câu 3. Điều nào sau đây là phản hồi hợp lý từ hệ thống IDS khi nó phát hiện các gói tin có cổng và địa chỉ IP nguồn giống cổng và địa chỉ IP đích?

A. Ghi lại thông tin về các gói và loại bỏ chúng
B. Cho phép gói tin được xử lý bởi hệ thống mạng và ghi lại sự kiện
C. Phân giải địa chỉ đích và xử lý gói tin
D. Loại bỏ gói tin

Câu 4. Thông tin sau đây của Honeywall cho biết điều gì?

```
06/07-04:36:41.265114 0:C:29:14:47:F3 -> 0:C:29:2B:8E:58 type:0x800 len:0x4A
192.168.1.190:52580 -> 192.168.1.2:23 TCP TTL:47 TOS:0x0 ID:29911 IpLen:20 DgmLen:60
******S* Seq: 0x3652741A  Ack: 0x880F2F7B  Win: 0x10  TcpLen: 40
TCP Options (5) => MSS: 536 SackOK TS: 4294967295 0 WS: 10 EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/07-04:36:41.265353 0:C:29:2B:8E:58 -> 0:C:29:14:47:F3 type:0x800 len:0x4E
192.168.1.2:23 -> 192.168.1.190:52580 TCP TTL:128 TOS:0x0 ID:2360 IpLen:20 DgmLen:64
***A**S* Seq: 0x75B3EC22  Ack: 0x3652741B  Win: 0xFAF0  TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/07-04:36:41.265908 0:C:29:14:47:F3 -> 0:C:29:2B:8E:58 type:0x800 len:0x36
192.168.1.190:52580 -> 192.168.1.2:23 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3652741B  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A. Địa chỉ IP của máy đích là 192.168.1.190
B. Máy đích đang mở cổng dịch vụ 52580
C. Máy đích đang mở cổng dịch vụ 23
D. Địa chỉ IP của máy nguồn là 192.168.1.2

Câu 5. Dựa vào nội dung đoạn log dưới đây thì phát biểu nào sau đây là ĐÚNG?

```
6591 2013-03-09 21:38:38.160692 203.0.113.10❶ -> 192.168.3.5❸
 TCP 74 50376 > 21❷ [SYN] Seq=0 Win=14600 Len=0 MSS=1460
 SACK_PERM=1 TSval=695390 TSecr=0 WS=16
6592 2013-03-09 21:38:38.160702 192.168.3.5 -> 203.0.113.10
 TCP 74 21 > 50376 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
 SACK_PERM=1 TSval=276175 TSecr=695390 WS=32
6593 2013-03-09 21:38:38.161131 203.0.113.10 -> 192.168.3.5
 TCP 66 50376 > 21 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=695390 TSecr=276175
6594 2013-03-09 21:38:38.162679 192.168.3.5 -> 203.0.113.10
 FTP 86 Response: 220 (vsFTPd 2.3.4)
6595 2013-03-09 21:38:38.163164 203.0.113.10 -> 192.168.3.5
 TCP 66 50376 > 21 [ACK] Seq=1 Ack=21 Win=14608 Len=0 TSval=695391 TSecr=276175
6596 2013-03-09 21:38:38.164876 203.0.113.10 -> 192.168.3.5
 FTP 77 Request: USER 0M:)❹
6597 2013-03-09 21:38:38.164886 192.168.3.5 -> 203.0.113.10
 TCP 66 21 > 50376 [ACK] Seq=21 Ack=12 Win=5792 Len=0 TSval=276175 TSecr=695391
6598 2013-03-09 21:38:38.164888 192.168.3.5 -> 203.0.113.10
 FTP 100 Response: 331 Please specify the password.
6599 2013-03-09 21:38:38.166318 203.0.113.10 -> 192.168.3.5
 FTP 76 Request: PASS azz❺
```

A. Máy chủ FTP có địa chỉ là 203.0.113.10

B. Dịch vụ Telnet được sử dụng trên cổng 21

C. Quá trình bắt tay 3 bước được hoàn tất

D. Người dùng đăng nhập dịch vụ FTP thành công

Câu 6. Alice chịu trách nhiệm về tường lửa trong tổ chức của mình và phải đảm bảo rằng tất cả các tường lửa được cấu hình đúng cách. Gateway firewall được cấu hình như sau: chỉ cho phép lưu lượng kết nối đến trên một vài cổng cụ thể; tất cả lưu lượng truy cập (được phép hoặc bị chặn) được ghi lại và chuyển tiếp các bản ghi tới SIEM. Điều gì bị thiếu trong cấu hình trên?

A. Quy tắc cho kết nối đi

B. Mã hóa tất cả lưu lượng truy cập

C. Không có gì, đây là một cấu hình tốt.

D. Xác thực chứng thư số cho lưu lượng đến

Câu 7. Phát biểu nào dưới đây là SAI khi nói về SSTP (Secure Socket Tunneling Protocol)?

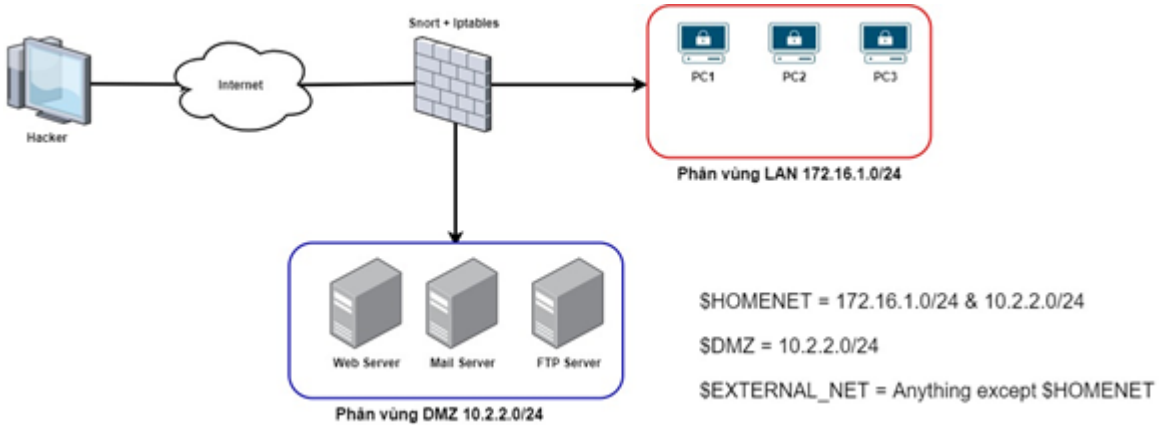
A. SSTP có mức độ bảo mật cao hơn PPTP

B. SSTP chỉ xác thực người dùng, không xác thực thiết bị

C. SSTP hỗ trợ xác thực bằng PSK

D. SSTP hỗ trợ cả 2 mô hình là Site-to-Site và Client-to-site

Câu 8. Luật nào sau đây cho phép phát hiện tấn công Smurf vào các máy tính trong mạng LAN?



A. alert icmp any any -> $HOMENET any (msg: “Smurf attack detected”; itype: 3; Sid: 5000002; rev: 1;)

B. alert icmp any any -> $HOMENET any (msg: “Smurf attack detected”; itype: 8; Sid: 5000002; rev: 1;)

C. alert icmp any any -> $HOMENET any (msg: “Smurf attack detected”; itype: 10; Sid: 5000002; rev: 1;)

D. alert icmp any any -> $HOMENET any (msg: “Smurf attack detected”; itype: 11; Sid: 5000002; rev: 1;)

Câu 9. Cho danh sách luật như sau:

```
Chain chain-incoming-ssh (1 references)
num  target     prot opt source               destination
1    ACCEPT     all  --  192.168.1.148        0.0.0.0/0
2    ACCEPT     all  --  192.168.1.149        0.0.0.0/0
3    DROP       all  --  0.0.0.0/0            0.0.0.0/0
```

Lệnh nào dưới đây cho phép thêm một luật mới vào trước luật cuối cùng?

A. `iptables -I chain-incoming-ssh 3 -s 192.168.1.150 -j ACCEPT`

B. `iptables -D chain-incoming-ssh 1`

C. `iptables -I chain-incoming-ssh 2 -s 192.168.1.140 -j REJECT`

D. `iptables -I chain-incoming-ssh 1 -s 192.168.1.140 -j ACCEPT`

Câu 10. Mạng VPN sử dụng tính năng nào để đảm bảo tính bí mật của thông tin trên kênh truyền?

A. Xác thực

B. Mã hóa

C. Đóng gói

D. Ghi nhật ký truyền

Câu 11. Khi đánh giá lưu lượng truy cập mạng của công ty, Peter thấy rằng hầu hết các trường hợp lây nhiễm mã độc là do người dùng truy cập các trang web độc hại. Peter muốn triển khai một giải pháp chặn các trang web này, quét tất cả lưu lượng truy cập web để tìm dấu hiệu của phần mềm độc hại và chặn phần mềm độc hại trước khi nó xâm nhập vào mạng công ty. Công nghệ nào sau đây sẽ là giải pháp tốt nhất?

A. IDS
B. UTM
C. SIEM
D. Firewall

Câu 12. Dựa trên hình, phát biểu nào sau đây về TCP stream là SAI.

A. Chương trình được sử dụng để phân tích gói tin ở đây là Wireshark
B. Yêu cầu được thực hiện thành công
C. HTTP client gửi một yêu cầu HTTP GET lên HTTP server
D. HTTP server chuyển hướng yêu cầu của client

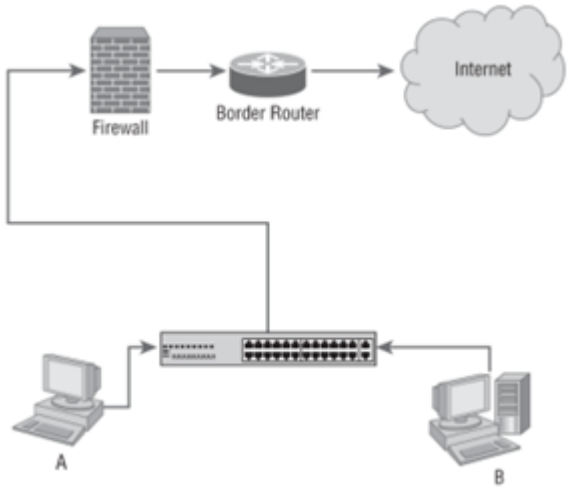
Câu 13. Peter thực hiện việc quét cổng dịch vụ (port) của hệ thống máy chủ cơ sở dữ liệu và thấy rằng port 3306 đang mở. Máy chủ có khả năng đang chạy cơ sở dữ liệu nào?

A. Microsoft SQL Server
B. MySQL
C. Oracle
D. Postgres

Câu 14. Tấn công nào dưới đây liên quan đến việc kẻ tấn công sửa địa chỉ IP nguồn của gói tin?

A. Whaling
B. Spear Phishing
C. Spoofing
D. Pharming

Câu 15. Lucca muốn ngăn các máy trạm trên mạng của mình tấn công lẫn nhau. Nếu mô hình mạng công ty của Lucca trông như hình dưới, phương án nào dưới đây là TỐT NHẤT để ngăn chặn máy tính A có thể tấn công máy tính B?



A. HIDS
B. HIPS
C. IPS
D. IDS

Câu 16. Michael đang muốn triển khai các giải pháp kiểm soát sử dụng mật mã để bảo vệ tổ chức của mình và các giải pháp kiểm soát phòng thủ theo chiều sâu để bảo vệ thông tin nhạy cảm được lưu trữ và truyền tải bởi máy chủ web. Giải pháp nào sau đây sẽ ít phù hợp nhất với yêu cầu của Michael?

A. VPN
B. FDE
C. DLP
D. TLS

Câu 17. Giải pháp sao lưu và phục hồi được sử dụng trong giai đoạn nào của quy trình ứng cứu sự cố an toàn thông tin mạng?

A. Tổng kết, đánh giá sự cố

B. Xử lý, gỡ bỏ và khôi phục

C. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

D. Kiểm tra, đánh giá hệ thống thông tin

Câu 18. Khi xem các tệp nhật ký của máy chủ web, người quản trị nhận thấy rằng rất nhiều yêu cầu đã truy cập vào trang web đang được điều hướng đến thư mục ***/scripts/..%c0%af../winnt/system32***. Loại tấn công nào đang xảy ra?

A. Cross-site scripting

B. Buffer overflow

C. SQL-injection

D. Path traversal

Câu 19. Câu lệnh nào dưới đây được sử dụng để xóa tạo 1 chain trong iptables?

A. `iptables -N old_chain`

B. `iptables -E old_chain`

C. `iptables -X old_chain`

D. `iptables -A old_chain`

Câu 20. John là quản trị viên của một hệ thống Linux. Anh ấy phải thiết lập lệnh nào dưới đây để cho phép một máy tính bên ngoài PING vào bên trong mạng?

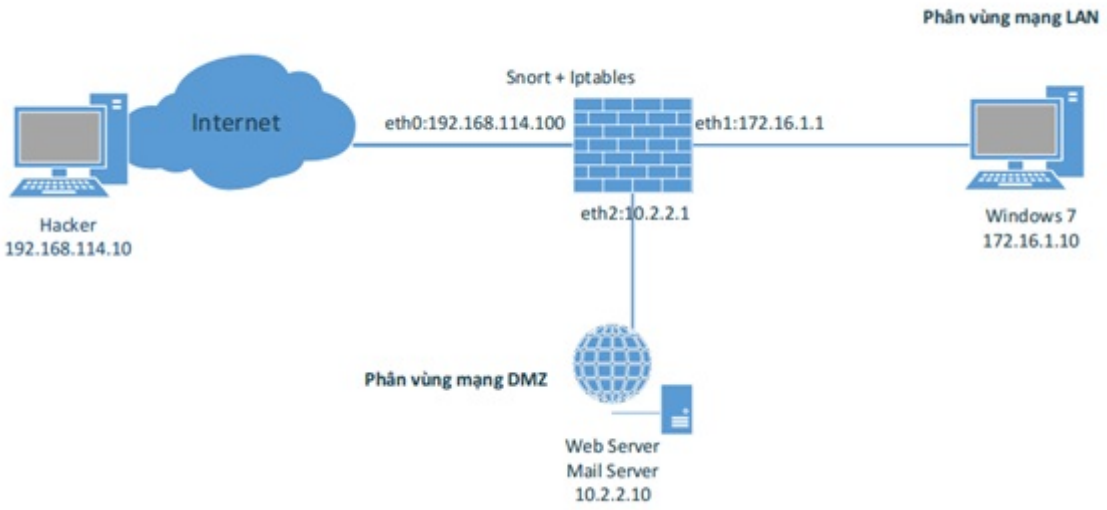
A. iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

B. iptables -I INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -I OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

C. iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

D. iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

Câu 21. Lệnh nào sau đây thực hiện chặn máy tính mọi kết nối TCP từ máy tính của Hacker với máy chủ trong phân vùng DMZ?



A. iptables -A INPUT -i eth0 -p tcp -s 192.168.114.10 -d 10.2.2.10 -m state --state NEW,ESTABLISHED -j DROP

B. iptables -A INPUT -i eth0 -p tcp -s 192.168.114.10 -m state --state NEW,ESTABLISHED -j DROP

C. iptables -A INPUT -i eth0 -s 192.168.114.10 -j REJECT

D. iptables -A INPUT -i eth0 -p tcp -s 192.168.114.10 -j DROP

Câu 22. Kỹ thuật nào được IDS sử dụng để kiểm tra một mẫu nhằm xác định hoạt động có phải là trái phép hay không?

A. Protocol Decoding
B. State Table
C. Session Splicing
D. Pattern Matching

Câu 23. Carrol chịu trách nhiệm về kết nối mạng trong công ty của mình. Bộ phận kinh doanh đang chuyển đổi sang VoIP. Hai giao thức mà cô ấy phải cho phép thông qua tường lửa là gì?

A. RADIUS và SNMP
B. SIP và RTP
C. TCP và UDP
D. RADIUS và SIP

Câu 24. Loại mã độc nào có khả năng tự thay đổi mã lệnh để tránh sự phát hiện?

A. Worm

B. Polymorphic malware

C. Armored virus

D. Remote access trojan

Câu 25. Thông qua hệ thống giám sát, Peter nghi ngờ rằng tin tặc thực hiện tấn công vào hệ thống Web Server. Kết quả phân tích gói tin thu được như hình dưới.

```
06/07-05:36:51.910966 0:C:29:2B:8E:58 -> 0:C:29:14:47:F3 type:0x800
len:0x77
192.168.1.2:1044 -> 192.168.1.190:4444 TCP TTL:128 TOS:0x0 ID:2494
IpLen:20 DgmLen:105 DF
***AP*** Seq: 0x34BB343A  Ack: 0x77AEB9A1  Win: 0xF9FC  TcpLen: 20
0D 0A 28 43 29 20 43 6F 70 79 72 69 67 68 74 20  ..(C) Copyright
31 39 38 35 2D 32 30 30 33 20 4D 69 63 72 6F 73  1985-2003 Micros
6F 66 74 20 43 6F 72 70 2E 0D 0A 0D 0A 43 3A 5C  oft Corp.....C:\
57 49 4E 44 4F 57 53 5C 73 79 73 74 65 6D 33 32  WINDOWS\system32
3E                                               >
```

Kết luận nào sau đây là phù hợp nhất?

A. Tin tặc đang cố gắng xâm nhập vào Web Server

B. Web Server sử dụng hệ điều hành Linux

C. Tin tặc đã xâm nhập được vào Web Server

D. Tin tặc đang tấn công quét cổng

Câu 26. Người quản trị muốn lựa chọn một thuật toán cân bằng tải để áp dụng cho hệ thống của mình, trong đó các máy chủ của hệ thống có hiệu suất làm việc khác nhau và thời gian kết nối của những người dùng cũng rất khác nhau. Vậy người quản trị nên lựa chọn thuật toán cân bằng tải nào là phù hợp nhất?

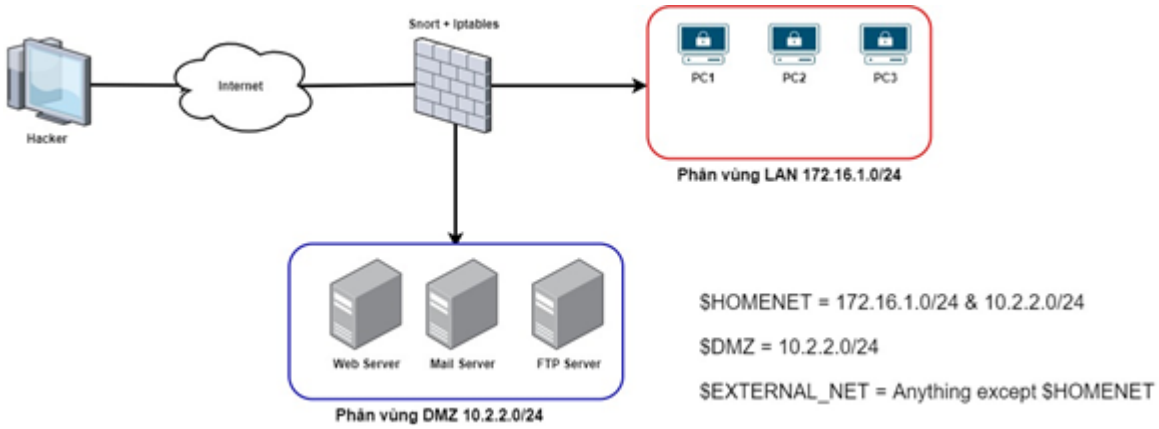
A. Thuật toán Weighted Least Connections

B. Thuật toán Least Connections

C. Thuật toán Round Robin

D. Thuật toán Weighted Round Robin

Câu 27. Luật nào sau đây cho phép phát hiện tấn công SQL Injection lên Webserver?



Lựa chọn đáp án đúng và phù hợp nhất.

A. alert tcp any any → $DMZ 80 (msg:"SQL Injection Attack"; content:"GET"; uricontent:"UNION"; classtype:web-application-attack; sid: 2002386; priority:1;)

B. alert tcp any any → $DMZ 80 (msg:"SQL Injection Attack"; detection_filter:track by_src, count 1000, seconds 1000; flags:S; classtype:web-application-attack; sid: 2002386; priority:1;)

C. alert tcp $HOMENET 80 → any any (msg:"SQL Injection Attack"; detection_filter:track by_src, count 1000, seconds 1000; flags:S; classtype:web-application-attack; sid: 2002386; priority:1;)

D. alert tcp $EXTERNAL_NET any → $HOMENET 80 (msg:"SQL Injection Attack"; content:"GET"; uricontent:"UNION"; classtype:web-application-attack; sid: 2002386; priority:1;)

Câu 28. Luật nào dưới đây cho phép cảnh báo khi có kết nối tới dịch vụ RDP trên máy chủ Web tại địa chỉ 192.168.1.97?

A. alert tcp any any -> 192.168.1.97 3389 (msg:"RDP to server"; GID:1; sid:1000008; rev:001; classtype:misc-activity;)

B. alert udp any any -> 192.168.1.97 3389 (msg:"RDP to server"; GID:1; sid:1000008; rev:001; classtype:misc-activity;)

C. alert tcp any 3389 -> 192.168.1.97 8080 (msg:"RDP to server"; GID:1; sid:1000008; rev:001; classtype:misc-activity;)

D. alert tcp 192.168.1.97 3389 -> any any (msg:"RDP to server"; GID:1; sid:1000008; rev:001; classtype:misc-activity;)

Câu 29. Một hệ thống có hai máy chủ A và B. Hệ thống này có áp dụng biện để đảm bảm 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?

A. Giải pháp chịu lỗi (failover)

B. Giải pháp cân bằng tải

C. Ứng phó sự cố

D. Phòng thủ theo chiều sâu

Câu 30. Mark chịu trách nhiệm đảm bảo an toàn thông tin cho một ngân hàng có quy mô nhỏ. Hệ thống gồm một tường lửa vành đai và tường lửa ở mỗi phân đoạn mạng. Các tường lửa này đều được cấu hình để ghi lại nhật ký và Mark kiểm tra nhật ký này thường xuyên. Bước nào sau đây Mark nên làm để nâng cao khả năng quản trị hệ thống?

A. Tích hợp với Honeypot

B. Tích hợp với Honeynet

C. Tích hợp với SIEM

D. Tích hợp với Domain Controller

Câu 31. Chức năng của mạng Honeynet là gì?

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

B. Phát hiện và ngăn chặn xâm nhập

C. Kiểm soát mạng dựa vào tập luật có sẵn

D. Thu hút, phân tích và cảnh báo xâm nhập

Câu 32. 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 truy cập vật lý (PACS) của tổ chức. PACS hiện không truy cập được Internet bởi vì nó đang chạy hệ điều hành cũ. Quản trị viên nên chọn phương pháp nào sau đây để đảm bảo an toàn và hiệu quả để xử lý trong tình huống này?

A. Thiết lập hội nghị trực tuyến bằng web trên máy tính của quản trị viên, sau đó kết nối tới PACS

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

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

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

Câu 33. IKE phase 1 sử dụng chế độ nào để thiết lập SA (Security Association) mà trong đó sử dụng 6 thông điệp để thỏa thuận các thông số với nhau?

A. Aggressive mode

B. Quick mode

C. Passive mode

D. Main mode

Câu 34. Thuật toán nào sau đây trong Loadbalancing lựa chọn máy chủ dựa vào công suất định mức của máy chủ?

A. Least Connections

B. Weighted Round Robin

C. Round Robin

D. Fastest

Câu 35. Để bảo vệ dữ liệu của công ty của mình trước các thảm hỏa xảy ra thì lựa chọn nào dưới đây sẽ là tối ưu nhất?

A. Sao lưu tất cả dữ liệu vào đĩa và lưu trữ những đĩa này ở một nơi an toàn trong nhà của người quản trị mạng.

B. Sao lưu tất cả dữ liệu vào đĩa và lưu trữ những đĩa này ở một thành phố khác.

C. Sao lưu tất cả dữ liệu vào đĩa và lưu trữ những đĩa này ở một nơi an toàn trong hầm chứa của công ty.

D. Sao lưu tất cả dữ liệu vào đĩa và lưu trữ những đĩa này ở một nơi khác trong cùng một thành phố.

Câu 36. Joe sử dụng Wireshark để bắt các gói tin trong mạng VPN. Quá trình nào đang diễn ra trong ảnh dưới đây. Chọn phương án chính xác nhất?

No.	Time	Source	Destination	SrcPrt	DstPrt	Info
7	2017-04-14 22:38:14.281969	172.16.1.70	172.16.1.71	500	500	Quick Mode
8	2017-04-14 22:38:14.282573	172.16.1.71	172.16.1.70	500	500	Quick Mode
9	2017-04-14 22:38:14.445523	172.16.1.70	172.16.1.71	500	500	Quick Mode

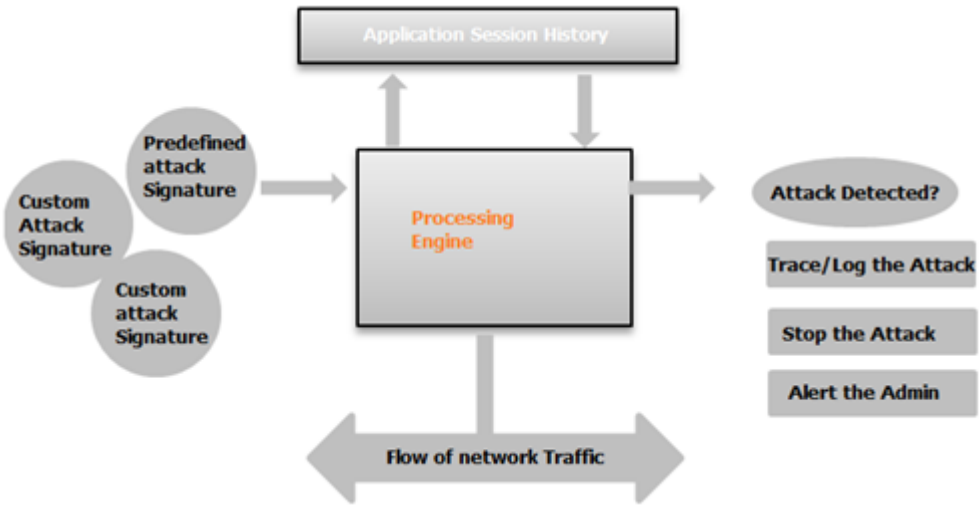
A. Khởi tạo kết nối IKE

B. IKE phase 1

C. IKE phase 2

D. Có thể là IKE phase 1 hoặc IKE phase 2

Câu 37. Mô hình dưới đây là mô hình mô phỏng cho hệ thống IDS nào?



A. Anomaly – based system

B. Stateless IDS

C. Stateful IDS

D. Signature-based system

Câu 38. Peter thực hiện giám sát an toàn thông tin cho 1 hệ thống máy chủ và phát hiện thấy có một số gói tin nghi ngờ có chứa mã độc. Công cụ nào sau đây thường KHÔNG được sử dụng trong quá trình phân tích gói tin?.

A. Nmap **B**. NetworkMiner **C**. Wireshark **D**. Xplico

Câu 39. Cho đoạn nhật ký của hệ thống giám sát như sau:

```
** Alert 1540815355.847397: -
ossec,syscheck,pci_dss_11.5,gpg13_4.11,gdpr_II_5.1.f,
2018 Oct 29 13:15:55 (ubuntu) 10.0.0.144->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
File '/test/hello' checksum changed.
Old md5sum was: '2a4732b1de5db823e94d662d207b8fb2'
New md5sum is : '146c07ef2479cedcd54c7c2af5cf3a80'
Old sha1sum was: 'b89f4786dcf00fb1c4ddc6ad282ca0feb3e18e1b'
New sha1sum is : 'e1efc99729beb17560e02d1f5c15a42a985fe42c'
Old sha256sum was:
'a8a3ea3ddbea6b521e4c0e8f2cca8405e75c042b2a7ed848baaa03e867355bc2'
New sha256sum is :
'a7998f247bd965694ff227fa325c81169a07471a8b6808d3e002a486c4e65975'
Old modification time was: 'Mon Oct 29 13:15:19 2018', now it is
'Mon Oct 29 13:15:54 2018'
(Audit) User: 'root (0)'
(Audit) Login user: 'test (1000)'
(Audit) Effective user: 'root (0)'
(Audit) Group: 'root (0)'
(Audit) Process id: '26089'
(Audit) Process name: '/bin/nano'
```

Đoạn nhật ký này cảnh báo điều gì?

A. Nội dung của tệp tin giám sát không thay đổi

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

C. Tài khoản root bị tấn công

D. Nội dung tệp tin được giám sát bị thay đổi

Câu 40. Mark đang tìm kiếm một máy chủ proxy cho mạng của mình. Mục đích của máy chủ proxy là để đảm bảo rằng các máy chủ web được ẩn khỏi các máy khách bên ngoài. Tất cả các máy chủ web khác nhau sẽ được hiển thị với thế giới bên ngoài như thể chúng là máy chủ proxy. Loại máy chủ proxy nào là tốt nhất theo yêu cầu của Mark?

A. Firewall

B. Forward

C. Transparent

D. Reverse

Câu 41. Phát biểu nào dưới đây là KHÔNG đúng về giao thức ESP?

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

B. ESP vừa mã hóa, vừa xác thực dữ liệu

C. ESP có khả năng chống lại tấn công phát lại

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

Câu 42. 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 (DNS redirection)?

A. SAM

B. hosts

C. Services

D. /etc/passwd

Câu 43. Peter 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 sẽ bị ảnh hưởng bởi điều này?

A. Radius **B**. Kerberos **C**. IPSec **D**. DNSSEC

Câu 44. Lệnh nào dưới đây cho phép xóa bỏ 1 rule cụ thể của 1 chain được chỉ định?

A. `iptables -R chain` **B**. `iptables –R chain rulenum`

C. `iptables -D chain rulenum` **D**. `iptables -D chain`

Câu 45. Để giảm thiểu việc chiếm dụng không gian ổ đĩa, bộ phận IT của một tổ chức mới đây đã áp dụng chính sách là đặt thời hạn lưu trữ cho email đã gửi là sáu tháng. Lựa chọn nào sau đây là cách tốt nhất để đảm bảo an toàn khi chính sách này được thực thi?

A. Tạo một bản sao lưu được mã hóa hàng ngày của các email có liên quan.

B. Thực hiện nén đĩa tự động trên máy chủ email

C. Di chuyển các email có liên quan vào thư mục "Đã lưu trữ".

D. Cấu hình máy chủ email để xóa các email có liên quan.

Câu 46. Giải pháp nào là tốt nhất để bảo vệ dữ liệu trên một máy tính xách tay trong trường hợp nó bị lấy cắp?

A. Mã hóa dữ liệu

B. Khóa đĩa mềm

C. Lưu trữ đều đặn trên CD-ROM

D. Thiết lập mật khẩu trên hệ điều hành

Câu 47. 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 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.

A. Triển khai ở chế độ Sniffer

B. Triển khai ở chế độ Inline detection

C. Triển khai ở chế độ Passive

D. Triển khai ở chế độ Inline protection

Câu 48. Statefull firewall sử dụng _____ để lưu giữ thông tin về trạng thái các kết nối.

A. Routing table **B**. Network Address Translation table

C. Access Control List **D**. State table

Câu 49. Sau khi thu thập và phân tích được hành vi tấn công của tin tặc lên mạng Honeynet, người quản trị cần phải làm gì?

A. Đề xuất giải pháp phòng chống

B. Cách ly máy tính đang bị tấn công trong mạng Honeynet

C. Ngăn chặn ngay lập tức tấn công đang diễn ra

D. Không cần thực hiện việc gì cả vì đây là mạng giả lập

Câu 50. Lệnh nào sau đây cho phép ngăn chặn tấn công DoS như SYN Flood?

A. `iptables -A INPUT -p udp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT`

B. `iptables -A OUTPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT`

C. `iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT`

D. `iptables -A INPUT -p tcp --dport 80 -m limit --limit 1000/minute --limit-burst 100 -j DROP`

Câu 51. Giao thức IPsec hoạt động tại tầng nào trong mô hình OSI?

A. Tầng vận chuyển

B. Tầng trình diễn

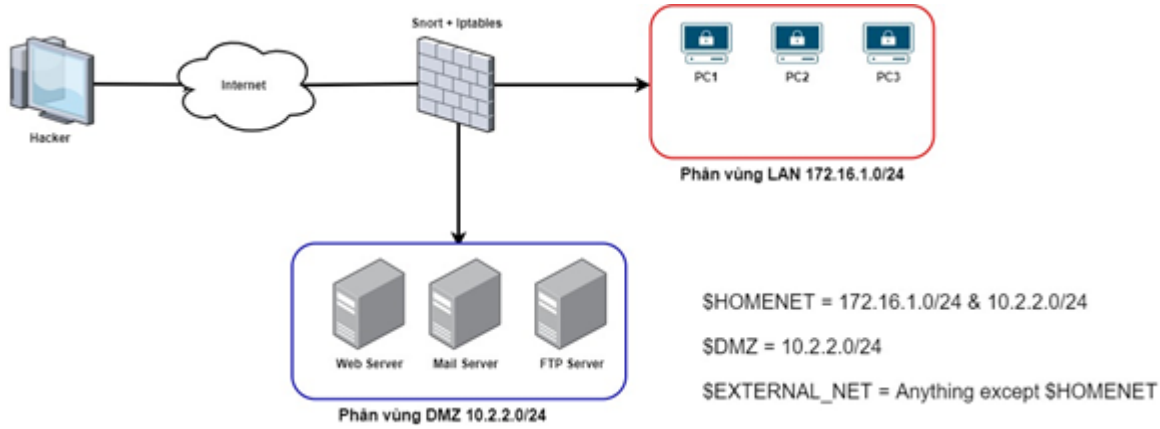
C. Tầng mạng

D. Tầng ứng dụng

Câu 52. Kỹ thuật SYN flood lợi dụng điểm yếu tại _____ trong mô hình OSI để thực hiện tấn công từ chối dịch vụ.

A. Tầng ứng dụng **B**. Tầng giao vận **C**. Tầng trình diễn **D**. Tầng vật lý

Câu 53. Luật nào sau đây cho phép phát hiện tấn công SYN Flood tới Mail Server?



Lựa chọn đáp án đúng và chính xác nhất.

A. alert tcp any any → $DMZ 25 (msg:"SYN flood attack"; flags:F; threshold:type threshold, track by_src, count 1000, seconds 5; classtype:attempted-dos; sid:200385; rev:3;)

B. alert tcp any any → $HOMENET 25 (msg:"SYN flood attack"; flags:S; threshold:type threshold, track by_src, count 1000, seconds 5; classtype:attempted-dos; sid:200385; rev:3;)

C. alert tcp $DMZ 25 → any any (msg:"SYN flood attack"; flags:S; threshold:type threshold, track by_src, count 1000, seconds 5; classtype:attempted-dos; sid:200385; rev:3;)

D. alert tcp any any → $DMZ 25 (msg:"SYN flood attack"; flags:S; threshold:type threshold, track by_src, count 1000, seconds 5; classtype:attempted-dos; sid:200385; rev:3;)

Câu 54. Công ty X sở hữu máy chủ email có địa chỉ 131.171.127.11. Peter muốn bảo vệ máy chủ này khỏi việc nhận bất kỳ email nào từ mạng con 192.168.1.0/24 có chứa từ khóa "hacking". Luật Snort nào sau đây chính xác nhất với yêu cầu của Peter?

A. alert tcp 192.168.1.0/24 any → 131.171.127.11 25 (content:"malicious packet"; msg: "hacking"; sid:2000001;)

B. alert tcp 131.171.127.11 25 → 192.168.1.0/24 any (content: "hacking"; msg: "malicious packet"; sid:2000001;)

C. alert tcp 192.168.1.0/24 any → 131.171.127.11 25 (content: "hacking"; msg: "malicious packet"; sid:2000001;)

D. alert tcp 192.168.1.24 any → 131.171.127.11 25 (content: "hacking"; msg: "malicious packet"; sid:2000001;)

Câu 55. 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:1000001; flags:F;)
```

A. msg: "FIN Dos";

B. alert tcp

C. alert tcp any any → 192.168.1.107 any

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

Câu 56. Giải pháp nào sau đây thường được sử dụng để bảo mật đầu cuối?

A. Antimalware **B**. HIDS **C**. Firewall **D**. VPN

Câu 57. Loại sao lưu nào dưới đây có tốc độ sao lưu nhanh nhất nhưng khôi phục dữ liệu chậm nhất?

A. Sao lưu vi sai **B**. Sao lưu gia tăng **C**. Sao lưu đầy đủ **D**. Sao lưu định kỳ

Câu 58. _____bao gồm console và sensor/sensors.

A. Protocol IDS (PIDS) **B**. Distributed IDS (DIDS)

C. Network-based IDS (NIDS) **D**. Host-based IDS (HIDS)

Câu 59. Nhật ký an toàn trên máy tính chứa đựng thông tin về các sự kiện xuất hiện 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.

A. Phân tích tệp tin nhật ký **B**. Lưu trữ tệp tin nhật ký

C. Cấu hình tệp tin nhật ký **D**. Thu thập tệp tin nhật ký

Câu 60. _____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 như cho phép hoặc cấm.

A. Access Control List (ACL) **B**. Packet Filter

C. State Table **D**. Session Splicing

---------- *Hết* ----------