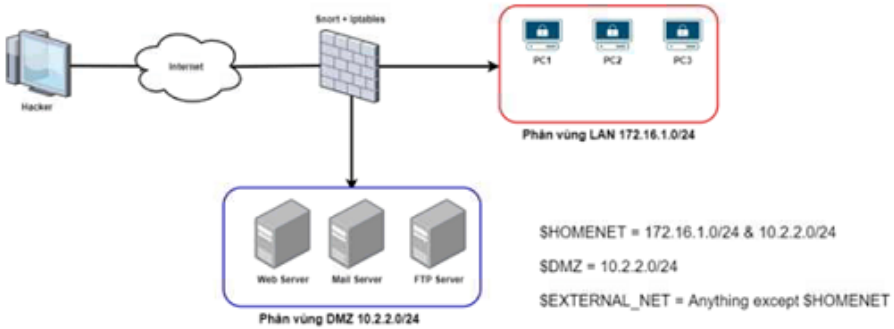
Câu 1. Luật nào sau đây cho phép phát hiện tấn công Web-LFI?



Lựa chọn đáp án đúng và chính xác nhất.

(A) ○ alert tcp $HOMENET 80 → $DMZ 80 (msg:"Web local file inclusion attack"; uricontent:"/etc/passwd"; nocase; classtype:web-application-attack; sid:2002387; priority:2;)

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

(C) ✓ alert tcp any any → $HOMENET 80 (msg:"Web local file inclusion attack"; uricontent:"/etc/passwd"; nocase; classtype:web-application-attack; sid:2002387; priority:2;)

(D) ○ alert tcp any any → $DMZ 80 (msg:"Web local file inclusion attack"; uricontent:"/etc/passwd"; nocase; classtype:web-application-attack; sid:2002387; priority:2;)

Câu 2. Trong quá trình ứng cứu sự cố, 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

Câu 3. 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 -i eth0 -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`

Câu 4. Peter – CEO của công ty Wayne đã nhận được email trông như có vẻ 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 đường link gửi kèm trong email để thay đổi các thông tin đó. Chọn đáp án phù hợp nhất cho loại tấn công có thể đang diễn ra.

(A) ○ Vishing

(B) ○ Pharming

(C) ○ Phishing

(D) ○ Whaling

Câu 5. Robert đang cấu hình VPN dựa trên IPsec. Anh ấy lo lắng việc bất kỳ ai cũng có thể chặn bắt gói tin để phân tích và lấy được thông tin về lưu lượng kết nối. Chế độ nào sau đây là tốt nhất để ngăn chặn điều này?

(A) ○ AH

(B) ○ ESP

(C) ✓ Transport

(D) ○ Tunneling

Câu 6. 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) ○ Session Splicing

(B) ○ Protocol Decoding

(C) ○ State Table

(D) ✓ Pattern Matching

Câu 7. 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

(D) ○ Bao gồm cả A, B, C

Câu 8. Elizabeth chịu trách nhiệm quản lý hệ thống SIEM cho một công ty. Cô ấy theo dõi màn hình hệ thống SIEM hàng ngày, kiểm tra hàng giờ. Lựa chọn nào sau đây sẽ là cách tiếp cận tốt nhất để 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 ký được chuyển tiếp tới email

(D) ○ Xem lại nhật ký của SIEM khi sự cố xảy ra

Câu 9. Giao thức IPsec hoạt động tại tầng nào trong mô hình OSI?

(A) ○ Tầng trình diễn

(B) ✓ Tầng mạng

(C) ○ Tầng vận chuyển

(D) ○ Tầng ứng dụng

Câu 10. 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) ○ Dịch vụ Telnet được sử dụng trên cổng 21

(B) ○ Quá trình bắt tay 3 bước được hoàn tất

(C) ○ Máy chủ FTP có địa chỉ là 203.0.113.10

(D) ✓ Người dùng đăng nhập dịch vụ FTP thành công

Câu 11. Dựa vào nội dung đoạn log dưới đây thì phát biểu nào sau đây là ĐÚNG:

```
2013-04-17T17:53:28+0000❶        cSb1GfCIIL9❷     192.168.2.108   53999   46.43.34.31
80      1       GET     the.earth.li    /~sgtatham/putty/latest/x86/putty.exe❹   http://
www.chiark.greenend.org.uk/~sgtatham/putty/download.html Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31 0       300     302❺
Found   -       -       -       (empty) -       -       -       text/html       -       -

2013-04-17T17:53:28+0000❸        cSb1GfCIIL9❹     192.168.2.108   53999   46.43.34.31
80      2       GET     the.earth.li    /~sgtatham/putty/0.62/x86/putty.exe❻     http://
www.chiark.greenend.org.uk/~sgtatham/putty/download.html Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31 0       483328
200❼    OK      -       -       -       (empty) -       -       -       application/
```

(A) ○ Client thực hiện việc upload tập tin putty.exe và lưu trữ tại domainname/~sgtatham/putty/latest/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) ✓ Web server thực hiện chuyển hướng link download từ /~sgtatham/putty/latest/x86/putty.exe tới /~sgtatham/putty/0.62/x86/putty.exe

Câu 12. _____ 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

Câu 13. Peter đang 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 "IMCP request". Luật nào dưới đây cho phép thực hiện việc này?

(A) ○ alert icmp any any -> $DMZ any (msg:"ICMP flood"; sid:1000001; rev:1; classtype:icmp-event; detection_filter:track by_dst, count 5000, seconds 1;)

(B) ○ alert icmp any any -> $DMZ any (msg:"ICMP flood"; sid:1000001; rev:1; classtype:icmp-event; detection_filter:track by_dst, count 5000, seconds 600;)

(C) ✓ alert icmp any any -> $DMZ any (msg:"ICMP flood"; sid:1000001; rev:1; classtype:icmp-event; detection_filter:track by_dst, count 5000, seconds 60;)

(D) ○ alert udp any any -> $DMZ any (msg:"ICMP flood"; sid:1000001; rev:1; classtype:icmp-event; detection_filter:track by_dst, count 5000, seconds 60;)

Câu 14. 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?

(A) ○ Trùng lặp sự kiện

(B) ✓ Đồng bộ thời gian

(C) ○ Sự kiện không được ghi lại

(D) ○ Tương quan sự kiện

Câu 15. Câu lệnh nào dưới đây được sử dụng để xóa tạo 1 chain trong iptables?

(A) ○ `iptables -A old_chain`

(B) ○ `iptables -E old_chain`

(C) ✓ `iptables -X old_chain`

(D) ○ `iptables -N old_chain`

Câu 16. Cho luật Snort như hình minh họa. Phát biểu nào sau đây là đúng?

```
log tcp any :1024 → 192.168.1.0/24 500:
```

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

(B) ○ Ghi lại tất cả lưu lượng tcp tới mạng con 192.168.1.0/24

(C) ○ Ghi lại lưu lượng tcp từ các cổng nhỏ hơn hoặc bằng 1024 đến các cổng nhỏ hơn hoặc bằng 500

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

Câu 17. Trong quá trình thực hiện giám sát an toàn thông tin, việc lưu giữ nhật ký hệ thống trong sáu tháng hoặc lâu hơn có thể có giá trị cho những hoạt động nào sau đây?

(A) ○ Quản lý định danh và thẩm quyền

(B) ○ Điều khiển truy cập vật lý và logic

(C) ○ Khôi phục sau thảm họa và vận hành liên tục

(D) ✓ Điều tra số và xử lý sự cố

Câu 18. 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 dưới đây là tốt nhất?

(A) ○ Xác thực gói tin trong mạng

(B) ○ Xác thực người dùng sử dụng mật khẩu mạnh

(C) ○ Xác thực người dùng sử dụng chứng thư số

(D) ○ Xác thực máy chủ ứng dụng Web

Câu 19. **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 sử dụng mật mã khóa công khai để mã hóa dữ liệu

(D) ○ ESP có khả năng chống lại tấn công phát lại

Câu 20. **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?**

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

(B) ○ Tự động tạo ngoại lệ cho các hành động hoặc tệp tin cụ thể

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

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

Câu 21. **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"; sid:1000001; flags:F;)

(B) ○ alert tcp any any → 192.168.1.107 any

(C) ○ msg: "FIN Dos";

(D) ○ alert tcp

Câu 22. **John đang tìm kiếm tường lửa mới cho một công ty nhỏ. John lo ngại về các cuộc tấn công DoS, đặc biệt là SYN flood. Loại tường lửa nào sẽ bảo vệ tốt nhất chống lại SYN flood?**

(A) ○ Bastion

(B) ○ Stateful packet inspection (SPI)

(C) ✓ Packet filter

(D) ○ Application gateway

Câu 23. 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?

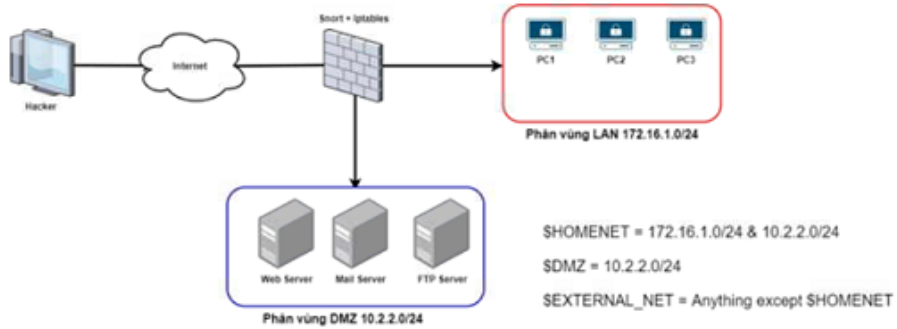
(A) ○ AH

(B) ○ IKE

(C) ✓ Kết hợp ESP và AH

(D) ○ Transport

Câu 24. Luật nào sau đây có khả năng phát hiện tấn công SYN scan lên phân vùng LAN của hệ thống?



Lựa chọn đáp án đúng và chính xác nhất.

(A) ✓ 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;)

(B) ○ 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;)

(C) ○ 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;)

(D) ○ 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;)

Câu 25. 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?

(A) ○ Honeynet

(B) ○ Network proxy

(C) ✓ Port mirroring

(D) ○ Network tap

Câu 26. _____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.

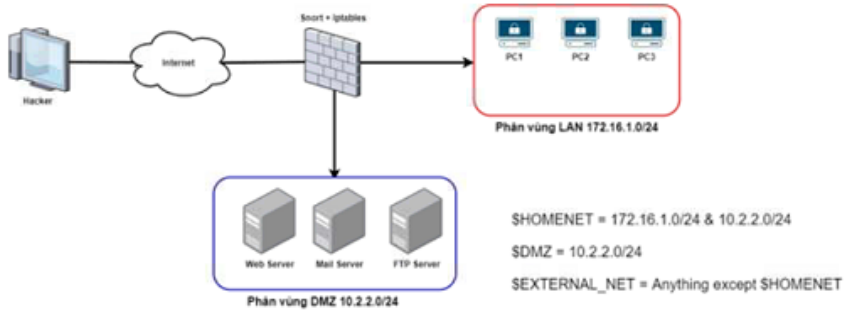
(A) ○ State Table

(B) ○ Packet Filter

(C) ○ Access Control List (ACL)

(D) ○ Session Splicing

Câu 27. Luật nào sau đây cho phép phát hiện tấn công dò quét mật khẩu lên FTP Server xuất phát từ phân vùng LAN?



Lựa chọn đáp án đúng và chính xác nhất.

(A) ○ 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 threshold, track by_dst, count 5, seconds 60; sid:2002383; rev:3;)

(B) ✓ alert tcp $HOMENET any → $DMZ 21 (msg:"FTP Brute force Attack"; flow:from_server, established; content:"530 "; pcre:"/^530\s+(Login|User)/smi"; classtype:unsuccessful-user; threshold:type threshold, track by_dst, count 5, seconds 60; sid:2002383; rev:3;)

(C) ○ alert tcp $EXTERNAL_NET any → $DMZ 21 (msg:"FTP Brute force Attack"; flow:from_server, established; content:"530 "; pcre:"/^530\s+(Login|User)/smi"; classtype:unsuccessful-user; threshold:type threshold, track by_dst, count 5, seconds 60; sid:2002383; rev:3;)

(D) ○ alert tcp $DMZ any → $HOMENET 21 (msg:"FTP Brute force Attack"; flow:from_server, established; content:"530 "; pcre:"/^530\s+(Login|User)/smi"; classtype:unsuccessful-user; threshold:type threshold, track by_dst, count 5, seconds 60; sid:2002383; rev:3;)

Câu 28. Phát biểu nào dưới đây là SAI về tường lửa có trạng thái?

(A) ○ Theo dõi mọi hoạt động của kết nối mạng đi qua nó

(B) ○ Lưu trạng thái của các phiên làm việc đang hoạt động.

(C) ✓ Sử dụng thông tin trạng thái để tăng tốc độ xử lý gói tin.

(D) ○ An toàn hơn so với tường lửa lớp ứng dụng

Câu 29. Tấn công nào có thể đang diễn ra dựa vào đoạn log dưới đây?

(A) ○ Tấn công MiTM (Man in the Middle)

(B) ○ Tấn công dò quét cổng

(C) ○ Tấn công bẻ khóa mật khẩu

(D) ○ Tấn công DNS

Câu 31. Tập luật nào dưới đây nên được thiết lập trên tường lửa như là luật mặc định?

(A) ○ iptables -A INPUT -j chain-states

iptables -A OUTPUT -j chain-states

(B) ○ iptables -A INPUT -p tcp -m tcp -j DROP

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

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

(C) ○ iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT DROP

(D) ○ iptables -A INPUT -i lo -j DROP

iptables -A OUTPUT -o lo -j DROP

Câu 30. 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 -I INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -I OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

(B) ✓ iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

(C) ○ iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -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 32. Bạn nhận được một cuộc điện thoại từ một nhân viên báo cáo rằng máy trạm của anh ta đang hoạt động không bình thường. Bạn thu thập thông tin từ hệ thống phát hiện xâm nhập và nhận thấy lưu lượng mạng bất thường từ máy trạm, và bạn xác định sự kiện có thể là một sự cố. Bạn báo cáo sự kiện cho người quản lý của mình, người này sau đó sẽ bắt đầu thu thập bằng chứng và chuẩn bị cho các bước tiếp theo. Đây là giai đoạn nào của quy trình ứng cứu sự cố (theo Thông tư 20/2017/TT-BTTTT quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng)?

(A) ○ Ngăn chặn

(B) ○ Gỡ bỏ

(C) ✓ Xác định sự cố

(D) ○ Chuẩn bị

Câu 33. 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?

(A) ○ 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 –state ESTABLISHED -j ACCEPT

(B) ✓ 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 –state ESTABLISHED -j ACCEPT

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

(D) ○ 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 –state ESTABLISHED -j ACCEPT

Câu 34. 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) ✓ Máy đích đang mở cổng dịch vụ 23

(B) Địa chỉ IP của máy đích là 192.168.1.190

(C) Máy đích đang mở cổng dịch vụ 52580

(D) Địa chỉ IP của máy nguồn là 192.168.1.2

Câu 35. Mô tả nào dưới đây là SAI về HIDS?

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

(B) ✓ Có khả năng phát hiện các tấn công trên một máy cụ thể

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

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

Câu 36. 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 anh ta phải làm gì?

(A) Gỡ bỏ

(B) ✓ Ngăn chặn

(C) Phục hồi

(D) Xác định sự cố

Câu 37. 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?

(A) ✓ Phân tích, thiết kế an toàn mạng

(B) ○ Khảo sát mạng

(C) ○ Triển khai mạng

(D) ○ Vận hành, giám sát hoạt động của mạng

Câu 38. 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) ○ Oracle

(B) ○ Microsoft SQL Server

(C) ✓ MySQL

(D) ○ Postgres

Câu 39. Phát biểu nào sau đây về HoneyDrive là ĐÚNG?

(A) ○ HoneyDrive là môi trường tích hợp các honeypot

(B) ○ HoneyDrive là Honeynet

(C) ○ HoneyDrive không hỗ trợ phân tích mã độc

(D) ✓ HoneyDrive là một dạng Honeypot tương tác cao

Câu 40. John lo lắng về việc kẻ tấn công đang liệt kê (enumerating) tất cả mạng của mình. Giao thức nào có thể giúp ít nhất giảm thiểu vấn đề này?

(A) ○ LDAPS

(B) ○ TLS

(C) ✓ HTTPS

(D) ○ IPSec

Câu 41. 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 nhập vào hệ thống. Vấn đề này phù hợp nhất với điều gì dưới đây?

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

(B) ✓ Tài khoản đã bị vô hiệu hóa bởi chính sách an toàn

(C) ○ Tường lửa đã chặn khi truy cập đến máy tính

(D) ○ Cổng mạng bị vô hiệu hóa

Câu 42. Thuật toán nào sau đây trong Loadbalancing lựa chọn máy chủ dựa vào công suất định mức của máy chủ?

(A) Fastest

(B) Weighted Round Robin

(C) Round Robin

(D) Least Connections

Câu 43. 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?

(A) Chuyển tiếp log

(B) Xác định IP nguồn tấn công

(C) Loại bỏ các sự kiện trùng lặp

(D) Xác định bản chất cuộc tấn công

Câu 44. Tường lửa thực hiện kiểm tra sâu gói tin nhờ kỹ thuật _____.

(A) Protocol Decoding

(B) Pattern Matching

(C) IP Spoofing

(D) Session Splicing

Câu 45. 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) Thu thập tệp tin nhật ký

(D) Cấu hình tệp tin nhật ký

Câu 46. IKE sử dụng cổng dịch vụ mặc định nào dưới đây?

(A) 135

(B) 500

(C) 514

(D) 530

Câu 47. 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 DBAdmin có 05 lần đăng nhập sai được cảnh báo. Tuy nhiên tài khoản DBAdmin 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?

(A) ○ Rule-based access control

(B) ✓ Honeypot

(C) ○ Role-based access control

(D) ○ Blacklist

Câu 48. Yếu tố nào sau đây thường được sử dụng kết hợp với một thẻ thông minh để thực hiện xác thực mạnh?

(A) ○ Thẻ nhớ

(B) ✓ Mã PIN

(C) ○ USB-token

(D) ○ Quét võng mạc

Câu 49. Peter muốn triển khai dịch vụ truyền file bằng cách sử dụng SSH. Lựa chọn nào sau đây là đúng?

(A) ○ LDAPS

(B) ○ SFTP

(C) ○ SSH

(D) ✓ FTPS

Câu 50. 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?

(A) ✓ Passive scanning

(B) ○ Statistical anomaly scanning

(C) ○ Signature scanning

(D) ○ Active scanning

Câu 51. Lệnh nào dưới đây cho phép xóa bỏ 1 rule cụ thể của 1 chain được chỉ định?

(A) ○ `iptables -R chain`

(B) ✓ `iptables -D chain rulenum`

(C) ○ `iptables -R chain rulenum`

(D) ○ `iptables -D chain`

Câu 52. Peter đang thực hiện điều tra số trên một chiếc máy tính nghi ngờ bị tấn công. Peter nhận thấy một số kết nối mạng sử dụng SSL trên các cổng không phổ biến, bản sao của svchost.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 đã diễn ra ở đây?

(A) ✓ Ransomware

(B) APT

(C) MiTM

(D) DDoS

Câu 53. 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?

(A) Chế độ AH-only

(B) Chế độ Transport (mặc định)

(C) Chế độ ESP-only

(D) ✓ Chế độ Tunnel (mặc định)

Câu 54. 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 Passive

(B) Triển khai ở chế độ Inline detection

(C) ✓ Triển khai ở chế độ Inline protection

(D) Triển khai ở chế độ Sniffer

Câu 55. Mary 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. Vậy Mary đã hoàn thành bước nào trong quá trình ứng cứu sự cố (theo Thông tư 20/2017/TT-BTTTT quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng)?

(A) Tổng kết, đánh giá

(B) Ngăn chặn

(C) ✓ Khôi phục

(D) Chuẩn bị

Câu 56. _____ là một thiết bị phần cứng hoặc một chương trình phần mềm thực hiện giám sát thao tác gõ phím của người dùng máy tính.

(A) Script kiddie

(B) ✓ Keylogger

(C) Macro

(D) Adware

Câu 57. 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) ○ TCP và UDP

(B) ○ SIP và RTP

(C) ○ RADIUS và SNMP

(D) ○ RADIUS và SIP

Câu 58. 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)?

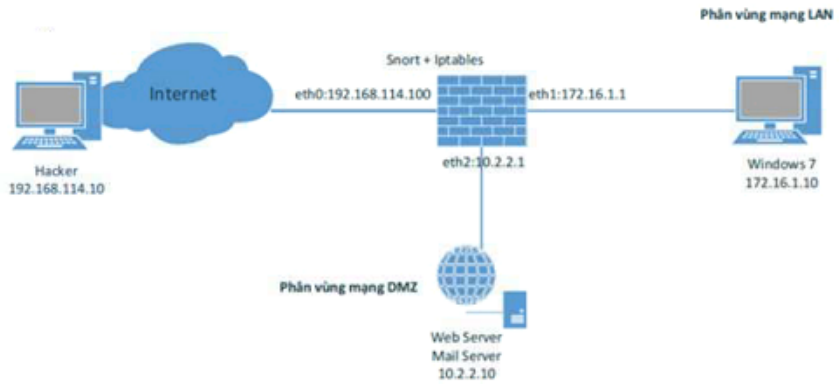
(A) ○ Services

(B) ○ SAM

(C) ○ hosts

(D) ○ /etc/passwd

Câu 59. Lệnh nào sau đây cho phép tất cả kết nối SSH (cổng 22) từ bên ngoài đến SSH server có địa chỉ 10.2.2.10?



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

(B) ○ iptables -t nat -A PREROUTING -p tcp -i eth0 -d 192.168.114.100 --dport 22 -j DNAT --to-destination 10.2.2.10

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

(D) ○ iptables -A INPUT –o eth0 -p tcp --sport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

Câu 60. 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 cân bằng tải

(B) ○ Ứng phó sự cố

(C) ○ Giải pháp chịu lỗi (failover)

(D) ○ Phòng thủ theo chiều sâu