**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

**TÊN NĂNG LỰC: Thiết lập và duy trì an ninh mạng**

**Cấp độ 4**

**Q.01**

| Trên firewall Cisco ASA, loại access list entry nào có thể được cấu hình để match nhiều entries chỉ với 1 câu lệnh ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Nested object-class |  | *0* |
|  | Class-map |  | *0* |
|  | Extended wildcard matching |  | *0* |
|  | Object groups. |  | *100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

**Q.02**

| Trên Firewall Cisco ASA, Bạn có thể tạo những loại object groups nào ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Protocol and Network |  | *50* |
|  | Service and ICMP type |  | *50* |
|  | DNS and DHCP |  | *-100* |
|  | DNS and ICMP type |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

**Q.03**

| Vishing là gì ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Virtualization hijacking |  | *0* |
|  | Phishing using a virus |  | *0* |
|  | VLAN(Virtual Local Area Network) based DoS (Denial of Service) attacks |  | *0* |
|  | VoIP (Voice over IP) based information gathering. |  | *100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

**Q.04**

| IPS sử dụng hình thức nào để bảo vệ hệ thống ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Signature-Based và Anomaly Based |  | *50* |
|  | Policy-Based và Protocol Analysis Based |  | *50* |
|  | Client Based |  | *-100* |
|  | Server Based và Client Based |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.05**

| Firewall có thể bảo vệ những lớp nào trong mô hình OSI? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Layer 1,2 và 3 |  | *0* |
|  | Layer 2,3 và 4. |  | *0* |
|  | Layer 3,4 và 7 |  | *100* |
|  | Layer 5,6 và 7 |  | *0* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.06**

| Domain Name System (DNS) poisoning là dấu hiệu của một cuộc tấn công Man-In-The-Middle. | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | True |  | *100* |
|  | False |  | *0* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

**Q.07**

| Dữ liệu không còn tính bảo mật( Confidentiality) khi dữ liệu bị không còn tính toàn vẹn ? | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | True |  | *0* |
|  | False |  | *100* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

**Q.08**

| Hệ thống sẽ có tính HA (High Availability) khi triển khai dịch biện pháp nào dưới đây? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | SSD storage |  | *0* |
|  | Offsite backups |  | *0* |
|  | Clustering |  | *100* |
|  | Optical network links |  | *0* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

**Q.09**

| Làm sao có thể ngăn chặn brute force attack trên router? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Config a limit the maximum number of login attempts |  | *100* |
|  | Config Vlan |  | *0* |
|  | Config Access-list |  | *0* |
|  | Config Mac-Security |  | *0* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

**Q.10**

| Tấn công có chủ đích APT là gì (Advanced Persistent Threat) ? | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

-Một cuộc tấn công có chủ đích APT là 1 cuộc tấn công dai dẳng có chủ đích vào một thực thể, thường là một cơ quan, tổ chức. Với mục đích:

+ Thu thập thông tin của đối tượng tấn công ( bí mật kinh doanh, chính trị...)

+ Làm mất uy tin của cơ quan, tổ chức.

+ Phá hoại, gây bất ổn hạ tầng CNTT...

Q11

| Một số Trojan ( cổng dịch vụ tương ứng ) thông dụng hiện nay | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | ICQ port 4590 |  | *50* |
|  | WinCrash 4092 |  | *50* |
|  | Remote Destop Port 3389 |  | *-100* |
|  | Telnet Port 23 |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

Q12

| Các biện pháp để đối phó với Trojan ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Tránh mở file đính kèm email nhận được từ những người gửi không rõ |  | *50* |
|  | Không sử dụng dịch vụ mạng |  | *-100* |
|  | Chặn tất cả các cổng không cần thiết tại các máy chủ và tường lửa |  | *50* |
|  | Mã hóa dữ liệu trước khi truyền trên mạng |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

Q13

| Các công cụ để phát hiện ARP Spoofing ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | ARP Spoof |  | *50* |
|  | Solarwind |  | *-100* |
|  | NETCUT |  | *50* |
|  | SubSeven |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

Q14

| Các biện pháp chống DDOS ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Dựa theo vị trí cần triển khai ( nguồn tấn công, đích bị tấn công ) |  | *30* |
|  | Nâng cấp băng thông mạng |  | *-100* |
|  | Dựa trên các giao thức mạng IP, TCP, Application. |  | *40* |
|  | Dựa theo thời điểm hành động ( trước , trong và sau khi bị tấn công ) |  | *30* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

Q15

| Thứ tự các giai đoạn của một quá trình PenTest ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | **Reconnaissance, Scanning, Exploitation, Maintaining Access** |  | *100* |
|  | **Reconnaissance, Exploitation, Scanning, Maintaining Access** |  | *0* |
|  | **Reconnaissance, Scanning, Maintaining Access, Exploitation** |  | *0* |
|  | **Reconnaissance, Exploitation, Maintaining Access, Scanning** |  | *0* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

Q16

| Các qui tắc then chốt trong bảo mật ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 1.Nếu một người nào đó có thể thuyết phục bạn chạy chương trình của anh ta trên máy tính của bạn, Nó sẽ không còn là máy tính của bạn nữa.  2. Nếu một người nào đó truy cập vật lí không hạn chế tới máy tính của bạn. Nó sẽ không còn là máy tính của bạn nữa.  3. Các mật khẩu dễ nhận có thể làm hỏng hệ thống bảo mật mạnh.  4. Công nghệ không phải là tất cả |  | *100* |
|  | 1.Nếu một người nào đó có thể thuyết phục bạn chạy chương trình của anh ta trên máy tính của bạn, Nó sẽ không còn là máy tính của bạn nữa.  2. Nếu một người nào đó truy cập vật lí không hạn chế tới máy tính của bạn. Nó sẽ không còn là máy tính của bạn nữa.  3. Các mật khẩu dễ nhận có thể làm hỏng hệ thống bảo mật mạnh.  4.Hệ thống bảo mật tốt là hệ thống được đầu tư nhiều thiết bị bảo mật tiên tiến |  | *0* |
|  | 1.Chính sách bảo mật tốt quyết định đến công tác bảo mật  2. Nếu một người nào đó truy cập vật lí không hạn chế tới máy tính của bạn. Nó sẽ không còn là máy tính của bạn nữa.  3. Các mật khẩu dễ nhận có thể làm hỏng hệ thống bảo mật mạnh.  4.Hệ thống bảo mật tốt là hệ thống được đầu tư nhiều thiết bị bảo mật tiên tiến |  | *0* |
|  | 1.Chính sách bảo mật tốt là vấn đề quyết định đến công tác bảo mật  2. Nếu một người nào đó truy cập vật lí không hạn chế tới máy tính của bạn. Nó sẽ không còn là máy tính của bạn nữa.  3. Các mật khẩu dễ nhận có thể làm hỏng hệ thống bảo mật mạnh.  4. Bảo mật là quá trình đảm bảo sự toàn vẹn dữ liệu |  | *0* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

Q17

| Định Nghĩa nào sau đây là đúng ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | **SQL Injection là phương pháp mà kẻ tấn công dùng để lấy thông tin trên hệ CSDL của nạn nhân** |  | *50* |
|  | **SQL Injection cũng là một kỹ thuật để thực hiên tấn công từ chối dịch vụ-DoS .** |  | *50* |
|  | **Phương án để phòng chống tấn công SQL InJection là triển khai Network Firewall để kiểm soát truy cập** |  | *-100* |
|  | **Phương án để phòng chống tấn công SQL InJection là triển khai hệ thống Anti- Virus** |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Replace 'Right answer' with the correct answer, and each 'Wrong answer' with a plausible alternative. Add hints or feedback for each wrong answer too.* | | |  |

Q18

| **Vulnerability Assessment là một quá trình trong Penetration Testing hoàn chỉnh ?** | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | True |  | *100* |
|  | False |  | *0* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

Q19

| Sự khác nhau giữa WHITE HAT HACKER và BLACK HAT HACKER bao gồm các khái niệm về : **sự cho phép, động cơ thúc đẩy**và**mục đích** | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | True |  | *100* |
|  | False |  | *0* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

Q20

| Các bước chuẩn bị đối với công tác xây dựng chính sách bảo mật | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

**I.Xác định đối tượng cần bảo vệ**Đây là mục tiêu đầu tiên và quan trọng nhất trong khi thiết lập một chính sách bảo mật. Người quản trị hệ thống cần xác định rõ những đối tượng nào là quan trọng nhất trong hệ thống cần bảo vệ; xác định rõ mức độ ưu tiên đối với những đối tượng đó. Ví dụ các đối tượng cần bảo vệ trên một hệ thống có thể là: Các máy chủ dịch vụ, các router, các điểm truy nhập hệ thống, các chương trình ứng dụng, hệ quản trị CSDL, các dịch vụ cung cấp …

Trong bước này cần xác định rõ phạm vi và ranh giới giữa các thành phần trong hệ thống để khi xảy ra sự cố trên hệ thống có thể cố lập các thành phần này với nhau, dễ dàng dò tìm nguyên nhân và cách khắc phục. Có thể chia các thành phần trên một hệ thống theo các cách sau:

· Phân tách các dịch vụ tùy theo mức độ truy cập và độ tin cậy

· Phân tách hệ thống theo các thành phần vật lý như các máy chủ (server), router, các máy trạm (workstation)…

· Phân tách theo phạm vi cung cấp của các dịch vụ như: các dịch vụ bên trong mạng (NIS, NFS …) và các dịch vụ bên ngoài như Web, FTP, Mail …

**II. Xác định nguy cơ đối với hệ thống**Các nguy cơ đối với hệ thống chính là các lỗ hổng bảo mật của các dịch vụ, hệ thống đó cung cấp. Việc xác định đúng đắn các nguy cơ này giúp người quản trị có thể tránh được những cuộc tấn công mạng, hoặc có biện pháp bảo vệ đúng đắn. Thông thường, một số nguy cơ này nằm ở các thành phần sau trên hệ thống:

1. Các điểm truy nhập

Các điểm truy nhập của hệ thống bất kỳ (Access Points) thường đóng vai trò quan trọng đối với mỗi hệ thống vì đây là điểm đầu tiên mà người sử dụng cũng như những người tấn công mạng quan tâm tới. Thông thường các điểm truy nhập thường phục vụ hầu hết người dùng trên mạng, không phụ thuộc vào quyền hạn cũng như dịch vụ mà người sử dụng dùng. Do đó, các điểm truy nhập thường là thành phần có tính bảo mật lỏng lẻo. Mặt khác, đối với nhiều hệ thống còn cho phép người sử dụng dùng các dịch vụ như Telnet, login để truy nhập vào hệ thống, đây là những dịch vụ có nhiều lỗ hổng bảo mật.

2. Không kiểm soát được cấu hình hệ thống

Không kiểm soát hoặc mất cấu hình hệ thống chiếm một tỷ lệ lớn trong số các lỗ hổng bảo mật. Ngày nay, có một số lượng lớn các phần mềm sử dụng, yêu cầu cấu hình phức tạp và đa dạng hơn, điều này cũng dẫn đến những khó khăn để người quản trị nắm bắt được cấu hình hệ thống. Để khắc phục hiện tượng này, nhiều hãng sản xuất phần mềm đã đưa ra những cấu hình khởi tạo mặc định, trong khi đó những cấu hình này không được xem xét kỹ lưỡng trong một môi trường bảo mật. Do đó, nhiệm vụ của người quản trị là phải nắm được hoạt động của các phần mềm sử dụng, ý nghĩa của các file cấu hình quan trọng, áp dụng các biện pháp bảo vệ cấu hình như sử dụng phương thức mã hóa hashing code (MD5).

3. Những bug phần mềm sử dụng

Những bug phần mềm tạo nên những lỗ hổng của dịch vụ là cơ hội cho các hình thức tấn công khác nhau xâm nhập vào mạng; Các chương trình trojans và virus là những ví dụ cụ thể. Do đó, người quản trị phải thường xuyên cập nhật tin tức trên các nhóm tin về bảo mật và từ nhà cung cấp phần mềm để phát hiện những lỗi của phần mềm sử dụng. Khi phát hiện có bug cần thay thế hoặc ngừng sử dụng phần mềm đó chờ nâng cấp lên phiên bản tiếp theo.

4. Những nguy cơ trong nội bộ mạng

Một hệ thống không những chịu tấn công từ ngoài mạng, mà có thể bị tấn công ngay từ bên trong. Có thể là vô tình hoặc cố ý, các hình thức tấn công bên trong mạng vẫn thường xảy ra trên một số hệ thống lớn. Chủ yếu với hình thức tấn công ở bên trong mạng là người tấn công có thể tiếp cận về mặt vật lý đối với các thiết bị trên hệ thống, đạt được quyền truy nhập không hợp lệ tại ngay hệ thống đó.

**III. Xác định phương án thực thi chính sách bảo mật**Sau khi thiết lập được một chính sách bảo mật, một hoạt động tiếp theo là lựa chọn các phương án thực thi một chính sách bảo mật. Một chính sách bảo mật là hoàn hảo khi nó có tính thực thi cao. Để đánh giá tính thực thi này, có một số tiêu chí để lựa chọn đó là:

1. Tính đúng đẵn

Đây là tiêu chí đầu tiên và quan trọng nhất để lựa chọn một chính sách bảo mật. Nó đảm bảo cho sự thành công của chính sách đó. Ví dụ, nếu như một hệ thống thường xuyên có các nguy cơ bị tấn công từ bên ngoài, một chính sách bảo mật cần phải đảm bảo kiểm soát được các truy nhập của khách hàng vào hệ thống bằng việc xây dựng các thủ tục quản lý tài khoản người dùng chặt chẽ và kỹ càng.

2. Tính thân thiện

Một chính sách bảo mật cần thiết lập các công cụ bảo mật thân thiện với người quản trị và dễ dàng thực thi các chính sách bảo mật. Đồng thời, còn đảm bảo các biện pháp bảo mật trên hệ thống không làm khó khăn hoặc bất tiện đối với người sử dụng. Ví dụ, những chính sách nhằm kiểm tra tính hợp lệ khi khách hàng truy nhập vào hệ thống; những chính sách về bảo vệ mật khẩu như yêu cầu khách hàng đối mật khẩu trong một thời gian xác định… các chính sách này phải có tính “trong suốt” đối với khách hàng sử dụng hệ thống.

3. Tính hiệu quả

Sau cùng, một chính sách bảo mật được quyết định bởi các nhà quản lý; họ quan tâm đến hiệu quả mà chính sách đó mang lại. Một chính sách bảo mật có thể đảm bảo hệ thống an toàn, tin cậy, nhưng lại cần có chi phí quá cao so với lợi nhuận mà hệ thống đó đem lại sẽ không được quyết định thực thi. Tuy nhiên, trong một khía cạnh khác, có thể các chính sách không thể đem lại hiệu quả ngay, do đó cần xem xét mức độ chi phí bảo mật hệ thống đối với một thời gian dài cùng với các lợi nhuận khác đem lại từ hệ thống bảo mật như nâng cao chất lượng dịch vụ bằng tính ổn định của hệ thống, …