**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

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

**Cấp độ 2**

**Q.01**

| Giao thức nào ở tầng network được thực hiện khi ping đến 1 server ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | TCP |  | *0* |
|  | UDP |  | *0* |
|  | ICMP |  | *100* |
|  | HTTP |  | *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.02**

| HTTPS sử dụng giao thức nào để mã hóa dữ liệu ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | AES |  | *0* |
|  | 3DES. |  | *0* |
|  | SSL hoặc TLS. |  | *100* |
|  | MD5. |  | *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.03**

| Trên Firewall Cisco ASA, tính năng nào được sử dụng để chống tấn cống TCP Syn flood ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | TCP intercept feature |  | *100* |
|  | UDP intercept feature |  | *0* |
|  | ICMP intercept feature | ; | *0* |
|  | Access list |  | *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.04**

| Trong thiết bị wifi, WEP sử dụng giao thức nào dưới đây để mã hóa và kiểm tra tính toàn vẹn của dữ liệu ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | AES |  | *-100* |
|  | RC4 |  | *50* |
|  | 3DES |  | *-100* |
|  | CRC-32 |  | *50* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.05**

| Giao thức nào sau đây là Distance vector routing protocol? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | RIP |  | *50* |
|  | OSPF |  | *-100* |
|  | EIGRP |  | *50* |
|  | BGP |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.06**

| Khi ping đến server mà không thấy phản hồi về, bạn có thể chắc chắn rằng server đó đang down? | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Có. |  | *0* |
|  | Không, có thể do nguyên nhân kết nối mạng hoặc firewall block gói tin ICMP. |  | *100* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

**Q.07**

| Web server nào dưới đây được sử dụng phổ biến trên hệ điều hành Linux ?. | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | IIS |  | *0* |
|  | Apache |  | *100* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

**Q.08**

| Giá trị mặc định TTL trên hệ điều hành Linux là bao nhiêu ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 64 |  | *100* |
|  | 128 |  | *0* |
|  | 32 |  | *0* |
|  | 256 |  | *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**

| Câu lệnh nào được sử dụng để hiển thị bảng routing trên HĐH Linux? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Route print |  | *0* |
|  | Route -n |  | *100* |
|  | ifconfig |  | *0* |
|  | ipconfig |  | *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**

| Spoofing attack là gì ? Cho ví dụ. | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

-Spoofing attack là tấn công mà attacker giả mạo thiết bị hoặc user khác trên mạng nhằm mục đích vượt qua kiểm soát truy cập, đánh cắp dữ liệu, lây nhiễm malware...

Ví dụ:

-Các kiểu spoofing attack hay gặp: IP address spoofing attack, ARP spoofing attacks và DNS spoofing attacks.

**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

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

**Cấp độ 2**

**Q.01**

| Điều quan trọng nhất khi triển khai firewall là gì ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Keeping rule sets simple |  | *0* |
|  | Blocking spoofed traffic |  | *0* |
|  | Locating the network boundary |  | *0* |
|  | Writing a firewall policy |  | *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 ASA tính năng flood guard có thể ngăn chặn kiểu tấn công nào dưới đây ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | ARP spoofing |  | *0* |
|  | SYN attack |  | *100* |
|  | DNS poisoning |  | *0* |
|  | MAC hijacking |  | *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.03**

| Kỹ thuật nào sau đây được hacker sử dụng để vượt qua MAC filtering ở thiết bị phát wifi ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Spoof a physical address |  | *100* |
|  | Run a dictionary attack |  | *0* |
|  | Statically assign an IP address | ; | *0* |
|  | Set the NIC to promiscuous mode |  | *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.04**

| Hình thức tấn công nào dưới đây được thực hiện trước khi attacker tấn công session hijacking ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Social engineering |  | *-100* |
|  | Sniffing |  | *50* |
|  | Man-in-the-middle attack |  | *50* |
|  | Password cracking |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.05**

| Mô hình nào dưới đâylà mô hình Single Sign-On? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Kerberos. |  | *50* |
|  | OpenID. |  | *50* |
|  | TCP handshake. |  | *-100* |
|  | Certificates. |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.06**

| Hình thức hay được sử dụng trong stateless firewalls là? | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Access control lists |  | *100* |
|  | Inspect packet. |  | *0* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

**Q.07**

| Lệnh Ping và Tracert cùng sử dụng giao thức ICMP đúng hay sai ?. | | | *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.08**

| Cách sử dụng mật khẩu nào dưới đây là an toàn ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Appending a numeral to a previous password |  | *0* |
|  | Using a long and complex password |  | *100* |
|  | Using a short password based on a keyboard typing pattern. |  | *0* |
|  | Sharing a password with a co-worker |  | *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**

| Người dùng mở 2 trình duyệt chrome cùng một lúc và cùng truy vấn vào trang web [http://vnpt.vn](http://vnpt.vn/), trường nào sau đây là khác nhau giữa 2 connection này? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Source port number |  | *100* |
|  | Destination port number |  | *0* |
|  | Source IP address |  | *0* |
|  | Destination IP address. |  | *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**

| Keyloggers là gì ? Cho ví dụ. | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

-Keyloggers/Keystroke loggers là những chương trình phần mềm hoặc thiết bị phần cứng thực hiện ghi lại toàn bộ thao tác trên bàn phím của người dùng. Một số loại keyloggers còn có thể chụp lại màn hình, clipboard... Kết quả ghi được sẽ được gửi email hoặc upload lên ftp-server/website cho attacker.

Ví dụ: Một số phần mềm keyloggers:

- REFOG Free keylogger

- Actual keylogger

**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

**TÊN NĂNG LỰC: F063 - Thiết lập và duy trì an ninh mạng**

**Cấp độ 1**

**Biểu hiện:** Có những kiến thức cơ bản về an toàn thông tin bao gồm các khái niệm về dữ liệu và thông tin, các hệ thống thông tin và những yêu cầu cần phải bảo mật thông tin cũng như có các khái niệm mục tiêu bảo mật thông tin   
- Có thể phân biệt giữa khái niệm về các phần mềm độc hại máy tính như virus,malware,worm, phần mềm gián điệp , cũng như có những kiến thức cơ bản về việc sử dụng máy tính an toàn.

**Q.01**

| 3 yếu tố quan trọng nhất của an toàn an ninh thông tin (Information Security) ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Confidentiality, Integrity and Availability |  | *100* |
|  | Confidentiality, Vulnerability and Integrity |  | *0* |
|  | Confidentiality, Vulnerability and Availability |  | *0* |
|  | Confidentiality, Security policy and Availability. |  | *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.02**

| Biện pháp nào giúp máy tính của bạn an toàn hơn trong môi trường internet ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Thường xuyên cập nhật bản vá hệ điều hành và cập nhật các phần mềm trong máy tính. |  | *50* |
|  | Sử dụng hệ điều hành Windows server 2003. |  | *-100* |
|  | Cài đặt phần mềm diệt virus. |  | *50* |
|  | Không sử dụng firewall và chương trình anti-malware. |  | *-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**

| Sự khác biệt giữa virus máy tính và sâu máy tính (worm) là gì ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Worm không có khả năng tự lây nhiễm, còn virus có khả năng tự lây nhiễm. |  | *0* |
| B | Worm có khả năng tự nhân bản, lây nhiễm ra các máy tính khác. Còn virus muốn lây nhiểm phải có thao tác của con người như mở một file .exe .doc .xls hay gửi file đính kèm, copy file sang máy khác. |  | *100* |
| C | Worm có dung lượng lớn hơn virus. |  | *0* |
| D | Virus có dung lượng lớn hơn worm. |  | *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.04**

| Chương trình nào sau đây là malware ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Microsoft Word |  | *0* |
|  | Mozilla Firefox |  | *0* |
|  | Viruses, worms và trojans |  | *100* |
|  | Skype |  | *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.05**

| Độ mạnh tối thiểu của mật khẩu phải thỏa mãn yếu tố nào dưới đây ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Độ dài >=8 ký tự |  | *50* |
|  | Độ dài >=4 ký tự |  | *-100* |
|  | Sử dụng thông tin cá nhân làm mật khẩu |  | *-100* |
|  | Sử dụng kết hợp chữ cái, chữ số, ký hiệu trong mật khẩu và không sử dụng thông tin liên quan đến cá nhân trong mật khẩu. |  | *50* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.06**

| Bạn có thể bị nhiễm virus trong những trường hợp nào sau? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Mở một file đính kèm được gửi đến từ một người lạ khi bạn check mail. |  | *50* |
|  | Download free games, toolbars và các chương trình ứng dụng từ trang web bất kỳ trên internet. |  | *50* |
|  | Download bản vá lỗ hổng hệ điều hành từ trang chủ của Microsoft. |  | *-100* |
|  | Không mở file đính kèm được gửi đến từ những người lạ. |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.07**

| Anh/chị cho biết đơn vị nào là đơn vị để đo lường thông tin ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | TB |  | *50* |
|  | LB |  | *-100* |
|  | PB |  | *50* |
|  | KG |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.08**

| Keylogger là phần mềm thường trú trên hệ thống máy tính, thực hiện lưu lại toàn bộ những phím bạn đã bấm .  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.09**

| Wireshare là phần mềm mã nguồn mở dùng để dò quét lỗ hổng bảo mật .  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.10**

| Xác thực đa nhân tố là gì (multifactor authentication) ? Cho ví dụ. | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

- Là quá trình xác thực người dùng của hệ thống sử dụng từ 2 phương pháp khác nhau trở lên.

Ví dụ:

-Password và mã OTP gửi vào số điện thoại.

-Password và vân tay/mống mắt.

Q.11

| Tổ chức chính cấp phát chứng chỉ số được gọi là : | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | CA |  | *100* |
|  | RA |  | *0* |
|  | LRA |  | *0* |
|  | CRL |  | *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.12

| Hầu hết định dạng chứng chỉ công cộng được dùng trong môi trường  PKI là gì | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | X.509 |  | *100* |
|  | X.508 |  | *0* |
|  | RSA |  | *0* |
|  | PKE |  | *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.13

| Giao thức nào sau đây tương tự như SSL và được đề nghị dùng bổ  sung vào các giao thức bảo mật ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | TSL |  | *100* |
|  | SSH |  | *0* |
|  | RSH |  | *0* |
|  | X.509 |  | *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.* | | |  |

Q14

| Những chữ đầu của nhóm từ ACL là tên viết tắt của | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Arbitrary Code Language |  | *0* |
|  | Access Control Library |  | *0* |
|  | Access Control List |  | *100* |
|  | Allowed Computer List |  | *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.* | | |  |

Q15

| Thuật giải SHA-1 dùng để : | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Tạo khoá đối xứng |  | *0* |
|  | Tạo chữ ký số |  | *0* |
|  | Tạo một giá trị băm có độ dài cố định 160 bit |  | *100* |
|  | Tạo một giá trị băm có độ dài cố định 256 bit |  | *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

| Thuật giải SHA-1 dùng để : | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Tạo khoá đối xứng |  | *0* |
|  | Tạo chữ ký số |  | *0* |
|  | Tạo một giá trị băm có độ dài cố định 160 bit |  | *100* |
|  | Tạo một giá trị băm có độ dài cố định 256 bit |  | *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

| Sau khi một user được định danh và xác thực hệ thống, để cho phép user  dùng tài nguyên bạn phải thực hiện điều gì? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | . Phải được ủy quyền |  | *100* |
|  | Được truyền lại |  | *0* |
|  | Được mã hóa |  | *0* |
|  | Được enable |  | *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.18**

| Anh/chị cho biết giao thức nào được sử dụng để tạo môi trường bảo mật trong môi trường wifi ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | WAP |  | *0* |
|  | WPA |  | *100* |
|  | WTLS |  | *0* |
|  | WML |  | *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.19**

| Anh/chị cho biết với kiểu đánh giá ứng dụng nào thì người đánh giá có đầy đủ thông tin đối với mục tiêu cần đánh giá nhất? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | White box |  | 100 |
|  | Gray box |  | *0* |
|  | Black box |  | 0 |
|  | Glass box |  | 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.20**

| Anh/chị cho biết với kiểu thiết kế nào sẽ giới hạn việc truy cập các hệ thống từ phân vùng người dùng bên ngoài (outside) trong khi có thể bảo vệ người dùng và các hệ thống trong phân vùng mạng LAN? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
| A | DMZ |  | *100* |
| B | VLAN |  | *0* |
| C | I&A |  | *0* |
| D | Router |  | *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.21**

| Anh/chị cho biết loại tấn công nào được dùng để làm quá tải tài nguyên hệ thống? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Spoofing |  | *0* |
|  | Trojan |  | *0* |
|  | Man in the middle |  | *0* |
|  | Syn flood |  | *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.22**

| Anh/chị cho biết thành phần nào của một hệ thống NIDS sẽ thu thập dữ liệu | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Data source |  | *0* |
|  | Sensor |  | *100* |
|  | Event |  | *0* |
|  | Analyzer |  | *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.23**

| Anh/chị cho biết quá trình nào sẽ nâng cao an toàn bảo mật cho hệ điều hành, chống tấn công từ hacker? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Locking down |  | *0* |
|  | Sealing |  | *0* |
|  | Tuning |  | *0* |
|  | Hardening |  | *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.24**

| Anh/chị cho biết nguy cơ bảo mật chính khi sử dụng giao thức FTP là gì? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | File password được lưu trữ trong vùng đĩa không được bảo mật |  | *0* |
|  | User ID và password không được mã hóa |  | *100* |
|  | Các site FTP không được đăng ký |  | *0* |
|  | Quá trình truy vấn bộ nhớ có thể làm ảnh hưởng đến việc truy xuất file |  | *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.25**

| Anh/chị cho biết thuật toán mã hóa nào là bất đối xứng? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 3DES |  | *0* |
|  | AES |  | *0* |
|  | DES |  | *0* |
|  | RSA |  | *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.26**

| Anh/chị cho biết khái niệm nào sau đây dùng để chỉ tới khái niệm địa chỉ vật lý của một máy tính? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | DAC |  | *0* |
|  | RBAC |  | *0* |
|  | MAC |  | *100* |
|  | STAC |  | *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.27**

| Anh/chị cho biết tiến trình nào dùng để thu thập chứng cứ phục vụ điều tra sự cố an ninh thông tin trên hệ thống máy tính? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Virus scanning |  | *0* |
|  | Security policy |  | *0* |
|  | Computer forensics |  | *100* |
|  | Evidence gathering |  | *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.28**

| Anh/chị cho biết địa chỉ IPv6 có bao nhiêu bit | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 32 |  | *0* |
|  | 64 |  | *0* |
|  | 128 |  | *100* |
|  | 256 |  | *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.29**

| Anh/chị cho cách nào dùng để bảo vệ hệ thống của bạn khỏi kiểu tấn công brute-force attack? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Không để password mặc định |  | *25* |
|  | Không sử dụng password có thể có trong từ điển |  | *25* |
|  | Không sử dụng password liên quan đến hostname, domain name, hoặc các thông tin khác có thể tìm thấy bằng cách sử dụng Whois |  | *25* |
|  | Không sử dụng mật khẩu liên quan đến sở thích, động vật nuôi, mối quan hệ, ngày tháng năm sinh của bạn |  | *25* |
|  | Sử dụng một từ có hơn 21 ký tự từ một từ điển làm password |  | *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.30**

| Anh/chị cho biết kiểu tấn công chiếm phiên TCP/IP xảy ra ở lớp nào của mô hình OSI | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Transport |  | *100* |
|  | Data link |  | *0* |
|  | Network |  | *0* |
|  | Physical |  | *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.31**

| Đảm bảo an toàn cho hệ thống không chỉ là việc ngăn chặn các truy cập trái phép từ hacker mà còn bao gồm cả việc xây dựng hệ thống có khả năng khôi phục dịch vụ từ các nguyên nhân phát sinh khác, hoặc thậm chí xuất phát từ các thảm họa tự nhiên.  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.31**

| “Integrity – Tính toàn vẹn” không phải là mục tiêu hàng đầu của việc bảo mật thông tin  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.32**

| Mạng LAN là mạng trong cùng một tòa nhà, trung tâm thương mại hoặc trong một vùng địa lý nhỏ  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.33**

| Mạng peer-to-peer là mạng trong đó có một số lượng lớn các máy tính cùng chia sẻ tài nguyên phần cứng và các thông tin trên mạng  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.34**

| Một thiết bị wireless access point (AP) là thiết bị cho phép các máy tính truy cập vào một hệ thống mạng có dây bằng sử dụng sóng radio  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.35**

| Worm là một loại virus máy tính tự nó có khả năng lây lan, không chỉ giữa các file mà còn giữa các máy tính với nhau thông qua email và các lưu lượng Internet khác  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.36**

| Phần mềm trojan-horse là loại được thiết kế để ghi lại các thao tác trên bàn phím, chuột của máy tính nạn nhân.  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.37**

| Một máy tính có các cài đặt Hệ điều hành ở dạng mặc định sẽ không có các lỗ hổng bảo mật nào.  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.38**

| Dữ liệu khi được gửi trên mạng ở dạng clear text khi Basic Authentication được sử dụng để cấu hình trên web server.  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.39**

| **Chữ ký số**  là một dạng **chữ ký điện tử**, được mã hóa bằng khóa riêng của người gửi, được đính kèm theo văn bản nhằm đảm bảo cho người nhận định danh và xác thực đúng nguồn gốc, tính toàn vẹn của dữ liệu nhận được  Anh/chị cho biết phát biểu trên đúng hay sai? | | | *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.40**

| Anh/chị cho biết passwords được lưu ở đâu trong hệ điều hành Linux | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | /etc/shadow |  | *100* |
|  | /etc/passwd |  | *0* |
|  | /bin/password |  | *0* |
|  | /bin/shadow |  | *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.41**

| Anh/chị cho biết giao thức https sử dụng port nào? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 21 |  | *0* |
|  | 80 |  | *0* |
|  | 53 |  | *0* |
|  | 443 |  | *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.42**

| Anh/chị cho biết thành phần nào của hệ thống mà virus có thể ảnh hưởng tới? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Files |  | *30* |
|  | Sector hệ thống |  | *40* |
|  | Memory |  | *0* |
|  | CPU |  | *0* |
|  | DLL files |  | *30* |
|  | **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.43**

| Anh/chị cho biết trong các biện pháp dưới đây thì đâu là giải pháp bảo mật lớp 3 cho mạng WLAN ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Lọc địa chỉ MAC |  | *0* |
|  | Sử dụng WEP |  | *0* |
|  | Sử dụng WPA |  | *0* |
|  | Sử dụng VPN |  | *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.44**

| Anh/chị cho biết cách để nâng cao an toàn cho laptop khi truy cập mạng vào mạng wireless nào đó là gì? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Cài đặt và cấu hình firewall mềm trên máy tính |  | *50* |
|  | Sử dụng WEP |  | *0* |
|  | Sử dụng biện pháp lọc địa chỉ MAC |  | *0* |
|  | Tắt tính năng auto-connect |  | *50* |
|  | **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.45**

| Anh/chị cho biết ai có trách nhiệm trong việc thực hiện các biện pháp nâng cao bảo mật tại nơi làm việc? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Giám đốc Công nghệ thông tin |  | *40* |
|  | Trưởng phòng phụ trách mảng việc Công nghệ thông tin |  | *30* |
|  | Các nhân viên của công ty |  | *30* |
|  | Chủ cho thuê đất |  | *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.46**

| Anh/chị cho biết biện pháp để ngăn chặn việc ăn cắp các ổ cứng của server? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Khóa cửa phòng máy server |  | *40* |
|  | Khóa tủ rack server |  | *30* |
|  | Cài đặt firewall trên server |  | *0* |
|  | Yêu cầu khách hàng khi đến làm việc phải đeo thẻ |  | *30* |
|  | **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.47**

| Anh/chị cho biết hệ điều hành máy tính là gì? Nêu tên 03 hệ điều hành mà anh/chị biết? | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

- Hệ điều hành máy tính là một [phần mềm](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m) chạy trên [máy tính](https://vi.wikipedia.org/wiki/M%C3%A1y_t%C3%ADnh), dùng để điều hành, quản lý các [thiết bị phần cứng](https://vi.wikipedia.org/w/index.php?title=Thi%E1%BA%BFt_b%E1%BB%8B_ph%E1%BA%A7n_c%E1%BB%A9ng&action=edit&redlink=1) và các [tài nguyên phần mềm](https://vi.wikipedia.org/w/index.php?title=T%C3%A0i_nguy%C3%AAn_ph%E1%BA%A7n_m%E1%BB%81m&action=edit&redlink=1) trên [máy tính](https://vi.wikipedia.org/wiki/M%C3%A1y_t%C3%ADnh).

Ví dụ:

- Windows

- Linux: Ubuntu,..

- Unix: Solaris,..

**Q.49**

| Anh/chị cho biết chức năng chính của thiết bị Firewall? Kể tên 03 hãng cung cấp thiết bị Firewall mà anh/chị biết | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

- Quản lý và điều khiển luồng dữ liệu trên mạng

- Bảo vệ tài nguyên

- Xác thực quyền truy cập

- Ghi nhận và báo cáo các sự kiện

Ví dụ:

- Cisco

- F5

- Paloalto

**Q.50**

| Anh/chị cho biết tại Tập đoàn VNPT tên của Nhóm chuyên trách về ứng cứu sự cố mạng, máy tính là gì?  Anh/chị hãy kể tên 03 biện pháp để nâng cao an toàn bảo mật tại đơn vị đang công tác? | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

- VNPT-Cert

Ví dụ:

- Thường xuyên tổ chức các buổi đào tạo, tuyên truyền đảm nâng cao nhận thức an toàn thông tin cho cán bộ công nhân viên tại đơn vị

- Đơn vị cần có các chính sách về an toàn thông tin

- Trang bị các biện pháp kỷ thuật để ngăn chặn các xâm nhập, truy cập trái phép vào các dịch vụ, hệ thống.

**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

**NHÓM NĂNG LỰC: (CM)**

**TÊN NĂNG LỰC: F063-Thiết lập và duy trì an ninh mạng**

**F063.01**

| Anh/chị hay cho biết khi một kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web để thêm vào và thực thi các lệnh SQL bất hợp pháp thì cách tấn công đó được gọi là gì? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | SQL input attack |  | *0* |
|  | SQL Piggybacsheets attack |  | *0* |
|  | SQL Select attack |  | *0* |
|  | SQL Injection attack |  | *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.* | | |  |

**F063.02**

| Anh/chị cho biết thứ tự đúng của các gói tin gửi đi trong quá trình khởi tạo TCP theo phương pháp bắt tay 03 bước | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | FIN, FIN-ACK, ACK |  | *0* |
|  | SYN, URG, ACK |  | *0* |
|  | SYN, ACK, SUN-ACK |  | *0* |
|  | SYN, SYN-ACK, ACK |  | *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.* | | |  |

**F054.03**

| Anh/chị đang khai báo Vlan trên các cổng của thiết bị Switch R1, trị số Vlan nào sẽ được gán là Vlan mặc định | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Vlan 1003 |  | *0* |
| B | Vlan 1 |  | *100* |
| C | Vlan ON |  | *0* |
| D | Vlan 0 |  | *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.* | | |  |

**F063.04**

| Anh/chị cho biết hai kiểu cơ bản của tấn công? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | DoS |  | *-100* |
|  | Passive |  | *50* |
|  | Sniffing |  | *-100* |
|  | Active |  | *50* |
|  | Cracsheets |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**F063.05**

| Anh/chị cho biết trong thiết kế mạng loại nào cho phép nhiều thiết bị nội bộ cùng chia sẻ một địa chỉ Public | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | DNAT |  | *-100* |
|  | PAT |  | *100* |
|  | DNS |  | *-100* |
|  | DMZ |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**F063.06**

| Sniffing là một phương pháp tấn công chủ động.  Anh/chị cho biết đúng hay sai? | | | *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.* | | |  |

**F063.07**

| Việc nhanh chóng phát triển, tăng cường kết nối Internet làm tăng nguy cơ mất an toàn thông tin trong tổ chức của anh chị  Anh/chị cho biết đúng hay sai? | | | *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.* | | |  |

**F063.08**

| Anh/Chị cho biết cách thức nào sau đây được sử dụng phổ biến trong kỷ thuật Social engineering attack? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Qua điện thoại |  | *100* |
|  | Qua email |  | *0* |
|  | Gặp mặt trực tiếp |  | *0* |
|  | Mạng chia sẻ ngang hàng |  | *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.* | | |  |

**F063.09**

| Anh/chị cho biết cách tốt nhất để bảo mật cho thiết bị switch tránh việc truy cập ở lớp vật lý là gì? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Disable tất cả các port không sử dụng |  | *100* |
|  | Disable các tài khoản không cần thiết |  | *0* |
|  | Bật tính năng Access control list |  | *0* |
|  | In sẵn file cấu hình của thiết bị |  | *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.* | | |  |

**F063.Q10**

| Các bạn hãy định Nghĩa các khái niệm cơ bản về Virus, Worm, phần mềm gián điệp | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

Đáp án :

* **virus máy tính** (thường được người sử dụng gọi tắt là virus hay **vi-rút**) là những [chương trình](https://vi.wikipedia.org/wiki/Ch%C6%B0%C6%A1ng_tr%C3%ACnh) hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó tạo ra những tệp tin (file) bị nhiễm virus trên các thiết bị lưu trữ như đĩa cứng, đĩa mềm, thiết bị nhớ flash (phổ biến là usb),...
* **Sâu máy tính (*worm*)** là các chương trình cũng có khả năng tự nhân bản tự tìm cách lan truyền qua hệ thống [mạng](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng) (thường là qua hệ thống thư điện tử). Điểm cần lưu ý ở đây, ngoài gây tác hại cho máy bị nhiễm, nhiệm vụ chính của worm là phá các mạng (*network*) thông tin chia sẻ, làm giảm khả năng hoạt động hay ngay cả hủy hoại các mạng này. Nhiều nhà phân tích cho rằng worm khác với virus, họ nhấn mạnh vào đặc tính phá hoại mạng nhưng ở đây worm được là một loại virus đặc biệt. Worm nổi tiếng nhất được tạo bởi [Robert Morris](https://vi.wikipedia.org/w/index.php?title=Robert_Morris&action=edit&redlink=1) vào năm [1988](https://vi.wikipedia.org/wiki/1988). Nó có thể làm hỏng bất kì [hệ điều hành](https://vi.wikipedia.org/wiki/H%E1%BB%87_%C4%91i%E1%BB%81u_h%C3%A0nh) [UNIX](https://vi.wikipedia.org/wiki/Unix) nào trên Internet. Tuy vậy, có lẽ worm tồn tại lâu nhất là [virus happy99](https://vi.wikipedia.org/w/index.php?title=Virus_happy99&action=edit&redlink=1), hay các thế hệ sau đó của nó có tên là [Trojan](https://vi.wikipedia.org/wiki/Trojan). Các worm này sẽ thay đổi nội dung tệp wsok32.dll của [Windows](https://vi.wikipedia.org/wiki/Microsoft_Windows) và tự gửi bản sao của chính chúng đi đến các địa chỉ cho mỗi lần gửi điện thư hay message.
* **Phần mềm gián điệp (*spyware*)**

Đây là loại virus có khả năng thâm nhập trực tiếp vào [hệ điều hành](https://vi.wikipedia.org/wiki/H%E1%BB%87_%C4%91i%E1%BB%81u_h%C3%A0nh) mà không để lại "di chứng". Thường một số chương trình diệt virus có kèm trình diệt spyware nhưng diệt khá kém đối với các đợt "dịch".

**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

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

**Cấp độ 2**

**Q.01**

| Nếu không phải do attacker tấn công thì backdoor có thể lây nhiễm từ cách nào sau đây? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Disabled by a replay attack |  | *0* |
|  | Connected to via a man-in-the-middle attack. |  | *0* |
|  | Left in the code by a programmer. |  | *100* |
|  | Activated when providing legitimate credentials. |  | *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.02**

| Trong Active FTP mode, port nào được sử dụng để thiết lập kênh điều khiển ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 20 |  | *0* |
|  | 21 |  | *100* |
|  | 22 |  | *0* |
|  | 23 |  | *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.03**

| Trên firewall ASA, access list entry nào được sử dụng trong cấu hình access-list mà cho phép match multiple entries với chỉ 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.04**

| Lệnh nào sau đây được sử dụng để lưu cấu hình trên switch? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | #wr |  | *50* |
|  | #save |  | *-100* |
|  | #write config |  | *-100* |
|  | #**copy running-config startup-config** |  | *50* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.05**

| Hình thức tấn công nào dưới đây là social engineering attack? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Man in the middle |  | *-100* |
|  | Phising |  | *50* |
|  | Virus. |  | *-100* |
|  | tailgating |  | *50* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.06**

| Bạn cần giải mã một file mã hóa sử dụng mã hóa bất đối xứng, khóa nào cần được sử dụng để giải mã? | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Private key. |  | *100* |
|  | Public key. |  | *0* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

**Q.07**

| 2 Vlan khác nhau có thể được gán vào 2 subnet của mạng hay không ?. | | | *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.08**

| Nếu bạn mở cổng TCP/21 mà dịch vụ FTP vẫn bị firewall block, vậy bạn cần thực hiện bước nào dưới đây để dịch vụ ftp hoạt động được ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Open TCP/20 |  | *100* |
|  | Open UDP/21 |  | *0* |
|  | Open TCP/22 |  | *0* |
|  | Close TCP/21 |  | *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**

| Hình thức mã hóa nào dưới đây không dựa trên block cipher? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | AES |  | *0* |
|  | DES |  | *0* |
|  | Blowfish |  | *0* |
|  | RC4 |  | *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.10**

| Phishing là gì ? Cho ví dụ. | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

-Phishing là việc xây dựng những hệ thống lừa đảo nhằm đánh cắp các thông tin nhạy cảm như username, password, thông tin thẻ tín dụng...

Ví dụ: Attacker gửi 1 email tới nhân viên công ty A với nội dung là hệ thống email của công ty đang nâng cấp yêu cầu người dùng cung cấp thông tin username/password để xác thực. Email có đường link để mở form xác thực giả mạo giống với trang email của công ty A. Sau khi nạn nhân nhập thông tin vào form đó ngay lập tức tài khoản của nạn nhân bị đánh cắp.

**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

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

**Cấp độ 2**

**Q.01**

| Port nào được dịch vụ chia sẻ file, máy in trên mạng - SMB over TCP/IP sử dụng? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 443 |  | *0* |
|  | 179. |  | *0* |
|  | 139 |  | *0* |
|  | 445 |  | *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**

| Biện pháp hữu hiệu chống lại tấn công SQL injection ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | IPS |  | *0* |
|  | Firewall |  | *0* |
|  | Web and database design |  | *100* |
|  | IDS |  | *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.03**

| Công cụ nào được sử dụng để khai thác lỗ hổng SQL injection? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | sqlmap |  | *100* |
|  | SQLextractor |  | *0* |
|  | Angry scan | ; | *0* |
|  | Toad |  | *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.04**

| Hình thức tấn công nào dưới đây không liên quan đến tấn công man-in-the-middle ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Domain Name System (DNS) poisoning |  | *-100* |
|  | Distributed Denial of Service (DDoS) |  | *50* |
|  | Rogue proxy server |  | *-100* |
|  | Crack Password |  | *50* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.05**

| Hình thức tấn công nào dưới đây là DDoS ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | SYN floods |  | *50* |
|  | ICMP floods |  | *50* |
|  | ARP poisoning |  | *-100* |
|  | Phishing |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.06**

| Worms có khả năng tự nhân bản và không cần tới tác động của người dùng để kích hoạt? | | | *TF* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | False. |  | *0* |
|  | True. |  | *100* |
|  | **General Feedback:** |  |  |
| *Swap 'True' and 'False' to put the right answer first. Do not include hints/feedback.* | | |  |

**Q.07**

| SQL Injection thành công, attacker sẽ có khả năng truy vấn đến database của hệ thống ? | | | *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.08**

| Loại NAT nào thường được sử dụng để public web server từ trong mạng LAN ra ngoài internet? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Static NAT |  | *100* |
|  | Dynamic NAT |  | *0* |
|  | PAT |  | *0* |
|  | None of the above |  | *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**

| Trường nào dưới đây được sử dụng để nhận biết gói tin được gửi đi trong cùng mạng hay khác mạng? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Destination port number |  | *0* |
|  | Subnet Mask |  | *100* |
|  | Destination network address |  | *0* |
|  | Domain name of the destination |  | *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**

| SQL Injection attack là gì ? Cho ví dụ. | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

-SQL injection attack là một dạng của tấn công khai thác lỗ hổng bảo mật của ứng dụng web, attacker có thể insert hoặc ‘inject’ một phần hay toàn bộ câu lệnh SQL để ứng dụng web xử lý và truy vấn vào database. Khi tấn công truy vấn vào database thành công attacker có thể select, insert, create, update hoặc delete dữ liệu lưu trong database.

Ví dụ: Trên ứng dụng web, có 1 form cho phép người dùng nhập nội dung tìm kiếm danh sách các sản phẩm của công ty.

Người lập trình không kiểm tra nội dung người dùng nhập vào, và gửi thẳng nội dung đó vào truy vấn đến database theo cú pháp.

Select \* from TBL\_DATA where Ten\_SP=A;

Thay vì chỉ nhập nội dung là A, attacker nhập nội dung tìm kiếm là: A or 1=1;

Khi đó câu lệnh tìm kiếm:

Select \* from TBL\_DATA where Ten\_SP=A or 1=1;

--> Toàn bộ dữ liệu trong bảng TBL\_DATA attacker có thể xem được.

**ĐỀ THI ĐÁNH GIÁ NĂNG LỰC**

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

**Cấp độ 3**

**Q.01**

| Trên Firewall Cisco ASA, Interface nào có giá trị security-level lớn nhất ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Interface outside |  | *0* |
|  | Interface inside |  | *100* |
|  | Interface DMZ |  | *0* |
|  | Interface DMZ và outside. |  | *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.02**

| Firewall Cisco ASA có những mode nào ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Single mode. |  | *-100* |
|  | Routed mode. |  | *50* |
|  | Transparent mode. |  | *50* |
|  | Multiple mode. |  | *-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**

| Trên Firewall Cisco ASA, căn cứ vào hình vẽ trên hãy chỉ ra loại NAT được sử dụng ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Static NAT |  | *0* |
|  | Dynamic PAT |  | *0* |
|  | Dynamic NAT |  | *100* |
|  | Identity NAT |  | *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.04**

| Ý nghĩa quan trọng nhất của một Virtual Server trên Application Firewall F5-ASM là gì ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Đại diện cho một Server bên trong mạng |  | *0* |
|  | Định tuyến kết nối từ client vào server. |  | *0* |
|  | NAT địa chỉ thật của server nội bộ ra địa chỉ ảo. |  | *0* |
|  | Cân bằng tải lưu lượng truyền vào các servers trong 1 pool mà nó đại diện. |  | *100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.05**

| Application Firewall F5-ASM có các chức năng nào sau đây? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Bảo mật ứng dụng ở lớp 7. (theo mô hình OSI). |  | *50* |
|  | Bảo mật ứng dụng ở lớp 3. ( theo mô hình OSI). |  | *50* |
|  | Bảo mật ứng dụng ở lớp 1. ( theo mô hình OSI). |  | *-100* |
|  | Bảo mật ứng dụng ở tất cả các lớp (theo mô hình OSI). |  | *-100* |
|  | **Correct Feedback:** |  |  |
|  | **Incorrect Feedback:** |  |  |
|  | **Partially Correct Feedback:** |  |  |
|  | **General Feedback:** |  |  |
| *Enter two right and two wrong answers.* | | |  |

**Q.06**

| Trên Firewall Cisco ASA, Theo mặc định: 2 vùng DMZ khác nhau có cùng giá trị security-level có thể kết nối và trao đổi dữ liệu được với nhau. | | | *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.07**

| Application Firewall F5-ASM có chức năng chống tấn công DoS. | | | *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.08**

| DoS Prevent policy trên firewall F5-ASM sử dụng phương thức nào để chặn tấn công DoS ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Không thể chặn được |  | *-100* |
|  | Client Side Integrity Defense và CAPTCHA Challenge |  | *50* |
|  | Request Blocking |  | *50* |
|  | IP Blocking |  | *-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.09**

| Fail-Over trên firewall F5-asm đang ở mode active/standby xảy ra khi? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Đổi địa chỉ IP server ở vùng inside |  | *0* |
|  | Khai báo thêm Vlan mới |  | *0* |
|  | Unit active bị mất nguồn |  | *100* |
|  | Unit Standby cấu hình force active |  | *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 từ chối dịch vụ là gì (Denial of Service – DoS attack) ? Cho ví dụ. | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

-Một cuộc tấn công DoS làm cho người dùng không thể truy cập vào các tài nguyên của hệ thống. Như làm cho các tài nguyên CPU, RAM... của máy chủ luôn ở trạng thái quá tải, hoặc làm cho nghẽn đường truyền kết nối đến máy chủ.

Ví dụ:

-Tấn công DoS vào một website, ứng dụng. Khách hàng không thể truy cập vào website.

Q.11

| Phiên bản phần mềm trên Firewall F5 – ASM đang sử dụng tại TT CNTT ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | BIG-IP 11.6.0 Build 5.0.429 Hotfix HF5 |  | *100* |
|  | BIG-IP 11.4.1 Build 637.0 Hotfix HF3 |  | *0* |
|  | BIG-IP 11.5.1 Build 2.0.121 Hotfix HF2 |  | *0* |
|  | BIG-IP 11.2.1 Build 2.0.121 Hotfix HF2 |  | *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.12

| Các module tính năng trong giải pháp bảo mật của F5 là gì ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | ASM |  | *50* |
|  | ACL |  | *-100* |
|  | APM |  | *50* |
|  | SSO |  | *-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.13

| Các tính năng module ASM của F5 là gì ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Giải pháp thống nhất trong việc quản lý an toàn bảo mật đối với truy cập từ xa, mạng LAN, mạng không dây thông qua một giao diện quản lý |  | *0* |
|  | Giải pháp bảo mật stateful, full-proxy đối với các nguy cơ tấn công mạng với các giao thức HTTP/s, DNS, FTP, SMTP |  | *0* |
|  | Giải pháp bảo mật đối với ứng dụng web truyền thống, trên môi trường ảo hóa, đám mây. Kết hợp của nhiều giải pháp quản lý traffic, network Firewall, truy cập ứng dụng, DDos Protection, SSL Inspection, DNS sercutity. |  | *100* |
|  | Giải pháp bảo mật giao thức HTTP như buffer overflow, command Injection, blocking –spam SMTP , FTP Sercurity |  | *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.14

| Tính năng module APM của F5 là gì ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Giải pháp thống nhất trong việc quản lý an toàn bảo mật đối với truy cập từ xa, mạng LAN, mạng không dây thông qua một giao diện quản lý |  | *100* |
|  | Giải pháp bảo mật stateful, full-proxy đối với các nguy cơ tấn công mạng với các giao thức HTTP/s, DNS, FTP, SMTP |  | *0* |
|  | Giải pháp bảo mật đối với ứng dụng web truyền thống, trên môi trường ảo hóa, đám mây. Kết hợp của nhiều giải pháp quản lý traffic, network Firewall, truy cập ứng dụng, DDos Protection, SSL Inspection, DNS sercutity. |  | *0* |
|  | Giải pháp bảo mật giao thức HTTP như buffer overflow, command Injection, blocking –spam SMTP , FTP Sercurity |  | *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.* | | |  |

Q15

| Các tính năng cấu hình HA group của giải pháp F5 là gì ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Vlan Fail -safe |  | *50* |
|  | DDOS Detection |  | *-100* |
|  | Gateway fail- safe |  | *50* |
|  | ICMP response |  | *-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.* | | |  |

Q16

| Tính năng module AFM của F5 là gì ? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Giải pháp thống nhất trong việc quản lý an toàn bảo mật đối với truy cập từ xa, mạng LAN, mạng không dây thông qua một giao diện quản lý |  | *0* |
|  | Giải pháp bảo mật stateful, full-proxy đối với các nguy cơ tấn công mạng với các giao thức HTTP/s, DNS, FTP, SMTP |  | *100* |
|  | Giải pháp bảo mật đối với ứng dụng web truyền thống, trên môi trường ảo hóa, đám mây. Kết hợp của nhiều giải pháp quản lý traffic, network Firewall, truy cập ứng dụng, DDos Protection, SSL Inspection, DNS sercutity. |  | *0* |
|  | Giải pháp bảo mật giao thức HTTP như buffer overflow, command Injection, blocking –spam SMTP , FTP Sercurity |  | *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

| Các Tính năng application Sercurity của module ASM - F5 là gì ? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Data Guard |  | *50* |
|  | Attack Signature |  | *50* |
|  | Sercurity Profile |  | *-100* |
|  | DDOS Profile |  | *-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

| Trường có công dụng kiểm tra sự toàn vẹn của gói tin (TCP, UDP, ICMP) là tham số TTL ? | | | *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.* | | |  |

Q19

| Giao thức thường được sử dụng với mạng riêng ảo (VPN)? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | IPSec |  | *50* |
|  | SSH |  | *50* |
|  | SSL/TSL |  | *-100* |
|  | Kerberos |  | *-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.* | | |  |

Q20

| ***FTP Trojans*** hoạt động như thế nào ? | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

**Đáp án:**

* FTP Trojans cài đặt FTP server trên máy nạn nhân, nó mở cổng FTP.
* Attacker có thể kết nối đến máy của nạn nhân bằng cách sử dụng cổng FTP để tải bất kỳ file nào tồn tại trên máy tính của nạn nhân.

Q21.

| Phương pháp tấn công DoS có các gói tin gửi từ attacker có các thông số rất khó hiểu để chia ra các phần (fragment) là? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Smurf |  | *0* |
|  | ARP Spoofing |  | *0* |
|  | Ping of death |  | *0* |
|  | Teardrop |  | *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.* | | |  |

| Kỹ thuật sử dụng các gói tin giả mạo chiếm đoạt kết nối giữa máy tính nạn nhân với máy đích? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | TCP Hijacking |  | *100* |
|  | Eavesdropping |  | *0* |
|  | SYN Flooding |  | *0* |
|  | Message replays |  | *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.* | | |  |

Q22

| Trường có công dụng kiểm tra sự toàn vẹn của gói tin (TCP, UDP, ICMP) là trường checksum ? | | | *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.* | | |  |

Q23

Q24

| Hình thức nào sau đây không phải là hình thức tấn công DoS? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Smurf |  | *0* |
|  | ARP Spoofing |  | *100* |
|  | Ping of death |  | *0* |
|  | Teardrop |  | *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.* | | |  |

Q25.

| Việc sử dụng đội quân zombie tấn công trên mạng là hình thức? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | DDOS |  | *100* |
|  | Buffer Overlow |  | *0* |
|  | DoS |  | *0* |
|  | Repudiation |  | *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.* | | |  |

Q26

| .Các server như: Web, Mail thường được đặt trong vùng nào dưới đây? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Single-Homed Bastion Host System |  | *0* |
|  | Dual-Homed Bastion Host System |  | *0* |
|  | Screened Subnets |  | *0* |
|  | Demilitarized Zones |  | *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.* | | |  |

Q27

| Phương thức thông dụng để chia sẻ một kết nối internet cho nhiều máy khác trong mạng là: | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | NAT |  | *0* |
|  | Routing Service |  | *0* |
|  | Remote Access Service |  | *0* |
|  | ICS (Internet Connection Sharring) |  | *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.* | | |  |

Q28

| Máy Windows Server 2003 có 2 thiết bị giao tiếp mạng: một giao tiếp Internet và một giao tiếp với các Client. Người quản trị triển khai NAT trên Windows Server này để chia sẻ kết nối internet. Sau khi triển khai xong thì Server giao tiếp internet tốt, còn các Client thì không giao tiếp được mặc dùng đã khai báo đúng và đủ các thông số IP cho Clients. Nguyên nhân dẫn đến tình trạng trên: | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Do Hệ Điều hành trên Client không hỗ trợ giao tiếp internet qua NAT Server |  | *0* |
|  | Do Windows Server dùng phiên bản Standard, không hỗ trợ SecureNAT |  | *0* |
|  | Do dịch vụ “Basic Firewall” ngăn không cho các Client giao tiếp internet |  | *100* |
|  | Khi triển khai NAT, người quản trị đã chọn sai thiết bị giao tiếp internet. |  | *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.* | | |  |

Q29

| Metasploit Framework là công cụ tấn công khai thác lỗ hổng để lấy Shell của máy nạn nhân. Ngay sau khi cài đặt, chạy công cụ này thì gặp sự cố: tất cả các lệnh gõ trên Metasploit không được thi hành. Nguyên nhân là do: | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Do không kết nối được tới máy nạn nhân |  | *100* |
|  | Do không cài đặt công cụ Metasploit vào ổ C |  | *0* |
|  | Do máy nạn nhân không cho phép tấn công |  | *0* |
|  | Do Phần mềm Anti Virus trên máy tấn công đã khóa (blocked) không cho thi hành. |  | *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.* | | |  |

Q30

| Hình thức tấn công Ping of Death là cách thức mà Attacker gửi các gói tin ICMP với kích thước lớn đến nạn nhân ( phải phân mảnh thành nhiều gói tin ) , dẫn đến máy tính nạn nhân không có khả năng xử lý dẫn tới hệ thống bị overload | | | *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.* | | |  |

Q31

| Bạn là người quản trị mạng tại trung tâm. Máy Server ISA1 cung cấp truy cập Internet cho tất cả máy trong mạng. Để phòng tránh người dùng vô tình tải và thực thi các tập tin virus (dạng \*.exe, \*.com, \*.dll,…). Bạn chọn giải pháp nào sau đây? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Lập một Access Rule cấm người dùng truy cập HTTP |  | *0* |
|  | Lập một Access Rule cho phép truy cập HTTP. Trong hộp thoại “Content Type” của Access Rule này: bỏ chọn “Application” |  | *0* |
|  | Tạo một “Content Type” trong đó chứa danh sách tập tin Virus. Tạo Access Rule cấm người dùng truy cập HTTP trên Content này. |  | *100* |
|  | Lập một Access Rule cấm truy cập HTTP vào các Web Site phát tán Virus |  | *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.* | | |  |

Q32

| Giao thức IP Security (IPSec) được thực hiện tại lớp nào | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Application |  | *0* |
|  | Transport |  | *0* |
|  | Netwwork |  | *100* |
|  | Data Link |  | *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.* | | |  |

Q33

| Các định Nghĩa nào sau đây là đúng | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Virus máy tính Tự động lan và lây nhiễm giữa các hệ thống. |  | *-100* |
|  | Virus có thể Phát tán qua các phần đính kèm với thư điện tử |  | *50* |
|  | Virus Gần như không thể phát tán trừ khi bạn mở hoặc chạy một chương trình bị nhiễm. |  | *50* |
|  | Virus phát tán qua nội dung thư điện tử |  | *-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.* | | |  |

Q34

| Sau khi dùng Sniffing software để bắt thông tin phân tích gói thông tin gửi đi từ host, có dạng: Protocol :TCP; Destination Port: 80; Source IP 192.168.3.8; Destination IP 203. 162.4.132; SYN=1, ACK=0. Cho biết host trên đang làm gì? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Máy 203. 162.4.132 đang yêu cầu kết nối với FTP server tại 192.168.3.8 |  | *0* |
|  | Máy 192.168.3.8 đang yêu cầu kết nối với Mail server tại 203. 162.4.132 |  | *0* |
|  | Máy 192.168.3.8 đang yêu cầu kết nối với server tại 203. 162.4.132 |  | *0* |
|  | Máy 192.168.3.8 đang yêu cầu kết nối với Web server tại 203. 162.4.132 |  | *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.* | | |  |

Q35

| Thiết lập quyền điều khiển từ xa của hacker đến máy nạn nhân là tác động hay gặp nhất của Virus máy tính ? | | | *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.* | | |  |

Q36

| Bạn cần cấm việc dò quét từ mạng khác theo giao thức ICMP. Bạn phải set lệnh deny ICMP với tham số nào? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Type = 3, Code = 1 |  | *100* |
|  | Type = 3, Code = 6 |  | *0* |
|  | Type = 3, Code = 7 |  | *0* |
|  | Type = 3, Code = 0 |  | *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.* | | |  |

Q37

| Công ty ABC có máy chủ quản lý Website cung cấp thông tin trên Internet tại địa chỉ 203.162.4.115. Hãy cài đặt tập luật cho Server này | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 203.162.4.115 – 80 - Any – 80 |  | *0* |
|  | 203.162.4.115 – Any - 203.162.4.115 – 80 - Any |  | *0* |
|  | Any – Any - 203.162.4.115 – 80 Allow |  | *100* |
|  | Any – Any - 203.162.4.115 – 80 – Deny |  | *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.* | | |  |

Q38

| Tường lửa (firewall) có thể ngăn chặn các kiểu tấn công Social Engineering ? | | | *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.* | | |  |

Q39

| Công ty ABC có Mail Server tại địa chỉ 203.162.4.116. Hãy cài đặt tập luật cho Server này: | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | 203.162.4.116 – 25 - Any – 80 - Allow |  | *0* |
|  | 203.162.4.116 – Any - 203.162.4.115 – 80 - Any |  | *0* |
|  | Any – Any - 203.162.4.116 – 25 - Allow |  | *0* |
|  | Any – Any - 203.162.4.115 – 25 |  | *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.* | | |  |

Q40

| Điều nào dưới đây là thành phần của an ninh mạng? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Authentication |  | *25* |
|  | Auditing |  | *25* |
|  | Strong Encryption |  | *25* |
|  | Security Policies |  | *25* |
|  | SMTP |  | *-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.* | | |  |

Q41

| Có thể kiểm tra các port đang mở với? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | MSConfig |  | *0* |
|  | Tracert |  | *0* |
|  | WhiteShark |  | *0* |
|  | ipconfig |  | *0* |
|  | Netstat |  | *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.* | | |  |

Q42

| Các quy tắc (rule) của firewall được xác định bởi? | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Tên rule |  | *25* |
|  | Giao thức |  | *25* |
|  | Điều kiện |  | *25* |
|  | Hành động |  | *25* |
|  | Chính sách |  | *-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.* | | |  |

Q43

| ứng dụng thường để dùng đính kèm Trojan với một tập tin khác là One EXE Maker | | | *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.* | | |  |

Q44

| Để thực hiện cuộc tấn công Trojan-Backdoor. Hacker sẽ thực hiện: | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Trojan Server được cài trên máy nạn nhân – Hacker điều khiển bằng Trojan Client |  | *0* |
|  | Hacker dùng Trojan Client, tấn công vào máy nạn nhân qua các port nhận đươc từ kỹ thuật Scanning |  | *0* |
|  | Hacker dùng Trojan Server, tấn công vào máy nạn nhân qua các port nhận đươc từ kỹ thuật Scanning. |  | *0* |
|  | Trojan Client được cài trên máy nạn nhân – Hacker điều khiển bằng Trojan Server |  | *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.* | | |  |

Q45

| Trojan là một phương thức tấn công kiểu | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng |  | *0* |
|  | Đánh cắp dữ liệu của nạn nhân truyền trên mạng |  | *0* |
|  | Tấn công làm tê liệt hệ thống mạng của nạn nhân |  | *0* |
|  | Điều khiển máy tính nạn nhân từ xa thông qua phần mềm cài sẵn trong máy nạn nhân |  | *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.* | | |  |

Q46

| Sniffing là một phương thức tấn công kiểu: | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Điều khiển máy tính nạn nhân từ xa |  | *0* |
|  | Đánh cắp dữ liệu của nạn nhân truyền trên mạng |  | *100* |
|  | Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng |  | *0* |
|  | Tấn công làm tê liệt hệ thống mạng của nạn nhân |  | *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.* | | |  |

Q47

| PGP có thể được dùng để ? ( Pretty Good Privacy ) | | | *MA* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Chứng thực |  | *50* |
|  | Nén |  | *-100* |
|  | Mã hóa |  | *50* |
|  | Diệt 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.* | | |  |

Q48

| ***Bạn có thể mô tả cách thức thực hiện cụ thể một cuôc tấn công ARP spoofing*** trong mạng LAN? | | | *ES* |
| --- | --- | --- | --- |
| **#** |  |  |  |
|  |  |  |  |
| *Don't forget to include the deadline!* | | |  |

Đáp án :

* Có thể dùng các công cụ như NetCut, ARPSpoof để thực hiện
* Xác định thông tin địa chỉ GateWay, địa chỉ IP của máy tính trong Mạng LAN mà attacker muốn thực hiện.
* Thực hiện tấn công bằng cách gửi giả mạo ARP message đến máy tính nạn nhân để máy tính nạn nhân hiểu địa chỉ IP GW tương ứng với địa chỉ MAC của máy tấn công.
* Kết quả máy tính nạn nhân không truy cập được dịch vụ và mọi thông tin gửi đi từ máy tính nạn nhân

Attacker có thể theo dõi và thu thập.

Q49

| Kỹ thuật nhằm tăng tốc độ thực thi và giảm kích thước chương trình virus được gọi là? | | | *MC* |
| --- | --- | --- | --- |
| **#** | **Answers** | **Hints/Feedback** | **Grade** |
|  | Biến hình |  | *100* |
|  | Tối ưu |  | *0* |
|  | Ngụy Trang |  | *0* |
|  | Mã hóa |  | *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.* | | |  |

Q50

| ARP Spoofing là hình thức tấn công mà Attacker giả mạo việc gửi bản tin ARP đến nạn nhân để thực hiện hành vi nghe lén, thay đổi thông tin hay làm gián đoạn dịch vụ | | | *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.* | | |  |

**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, …