**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.* | | |  |