**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.