cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccMột phương Denial Of Service

Một dịch vụ

Một kiểu kết

thức liên

Phương thức tấn (DoS) là? (chọn 1)

mạng

nối mạng

kết mạng

công từ chối dịch vụ

Có mấy hình thức tấn công social Enginerring? (chọn 1) 1 2 3 4

Shoulder surfing và Dumpter Diving thuộc hình thức tấn công nào trong social Enginerring? (chọn 1) Human-Based

Không thuộc hình thức nào.

Computer-Based bao gồm những dạng nào sau đây: (chọn nhiều)

Computer- Based Trojan

Email Attack/Phishin g Fake Website

không phải các dạng trên.

Có thể kiểm tra trạng thái các cổng (đóng/mở) sử dụng công cụ nào dưới đây? (chọn 2) nmap ipconfig nslookup netstat

Kỹ thuật tạo ra 1 trang web giả mạo thuộc hình thức tấn công nào? (Chọn 1) Mã độc Phishing Keylogger Sniffer

Mật khẩu nào dưới đây được coi là khó phá nhất đối với hacker? (chọn 1) abc123 123456 2052018 Pa$$w0rD

Chiều dài tối thiểu của mật khẩu để đảm bảo độ an toàn cần phải là: (Chọn 1) 12 đến 15 ký tự 3 đến 5 ký tự 8 ký tự 1 đến 3 ký tự

Kỹ thuật khai thác bằng cách chèn các câu truy vấn SQL bất hợp pháp vào Hệ quản trị CSDL thường được áp dụng cho? (Chọn 1)

Popup Windows

Khai thác SQL Injection XSS LFI CSRF

Thực thi đoạn code nào dưới đây để có thể biết PHP Enviroment đã được cài đặt đúng? (chọn 1) phpinfo() phpstatus() phptest() phpcheck()

Đoạn mã javascript sau đây thực thi hành động nào? (Chọn 1): <script>alert("Test by BKNET")</script>

Chèn thêm bảng "Test by Hiển thị popup

Xóa cơ sở dữ

BKNET" "Test by

liệu "Test by

vào trong BKNET"

BKNET"

CSDL

Không hiển thị thông tin gì

Để tìm kiếm các subdomain của 1 website ta có thể sử dụng toán tử tìm kiếm nâng cao nào? (Chọn 1) inurl filetype site link

Ransomware là loại mã độc sau khi lây nhiễm vào hệ thống sẽ có nhiệm vụ? (Chọn 1)

Tự động Không làm gì

chạy ứng cả Mở 1 cổng

dụng

Mã hóa dữ liệu và tống tiền

Virus Macro chỉ có khả năng tấn công vào các File? (Chọn 1)

MS excel/ms word/yaho o mail Tất cả các loại file

Giai đoạn đầu của Hacking/Pentesting là gì? (Chọn 1)

MS Excel/ms word/ms outlook mail

MS excel/ms word/ms powerpoint

Information Gathering Scaning

Gaining Access Exploit

Công cụ nào sau đây được sử dụng trong giai đoạn Information Gathering (Chọn 1) ping tracert pathping dmitry

Chương trình nào sau đây không phải là chương trình chống Virus (Chọn 1) Bitdefender AVG Kaspersky IDA Pro

Phát biểu nào sau đây là đúng khi nói về Web động (Chọn 1)

Là website được viết bằng các ngôn ngữ phía

Là website có DB, Là website

có Admin CP, được Là website có

có những

viết bằng các ngôn hình ảnh động

văn bản

ngữ lập trình phía

chạy client như:

trên HTML,

trình duyệt Javascript, CSS...

server như: php, ASPx, Java, python, ruby...

Lỗ hổng XSS (Cross Site Scripting) có mấy dạng tấn công? (Chọn 1) 1 2 3 4

Website hoạt động dựa trên giao thức nào? (chọn 1) HTTP/HTTPS FTP DHCP SFTP

Đâu là các dạng tấn công của XSS? (Chọn nhiều) Reflected Stored

Padding Oracle DOM Based

Tham số nào trong nmap được dùng để xác định phiên bản dịch vụ và HĐH? (Chọn 1) -sV -O -sS -P -sP -S -sT -A

Công cụ nào sau đây được sử dụng trong bước Scaning để tìm kiếm lỗ hổng bảo mật? (Chọn 1)

Windows Defender Nessus Olly DBG ncat

Phương pháp tấn công Password nào được Hacker sử dụng để "đoán" mật khẩu? (Chọn 1) Brute force

Dictionary Attack

Cain & Able Sniffer

Ứng dụng nào sau đây là Web Client? (Chọn 1) IE IIS Nginx Apache

Sử dụng công cụ setoolkit trong Kali Linux là hình thức nào trong Social Enginnering? (Chọn 1) Human-Based

Computer- Based

Dumpter Diving Shoulder Surfing

Giao thức HTTP hoạt động ở cổng bao nhiêu? (Chọn 1) 80 81 443 465

Công cụ nào sau đây được sử dụng để dò tìm lỗ hổng? (chọn 1) Nessus Nexpose OpenVAS Cả ba đáp án

Phương pháp tấn công nào sau đây còn có tên gọi khác là: "dot dot slash" (chọn 1) XSS CSRF

Path Traversal DoS

Giao thức HTTPS hoạt động ở cổng bao nhiêu (Chọn 1) 53 80 443 445