# **III. HẠNG 2 (280 CÂU)**

### (1) CÓ KIẾN THỨC CƠ BẢN VỀ NGÀNH CÔNG NGHỆ THÔNG TIN, TÁC CHIẾN KHÔNG GIAN MẠNG (GỒM 38 CÂU)

**Câu 1.Thuật toán "Support Vector Machine" (SVM) thường được sử dụng cho tác vụ nào trong AI?**

A. Học tăng cường (Reinforcement Learning)

B. Phân cụm (Clustering)

C. Hồi quy (Regression)

D. Phân loại (Classification**)**

**Đáp án: D**

**Câu 2. Trong Mạng nơ-ron tích chập (CNN), "Convolutional Layer" (Lớp tích chập) có chức năng gì?**

A. Làm phẳng dữ liệu đầu vào.

B. Tính toán xác suất cuối cùng của nhận dạng hình ảnh.

C. Trích xuất các đặc trưng từ dữ liệu hình ảnh.

D. Tạo nhãn cho dữ liệu để tăng tính chính xác của mô hình.

**Câu 3. Phương pháp "Drop out" được sử dụng trong việc huấn luyện mạng nơ-ron sâu để giải quyết vấn đề gì?**

A. Tăng tốc độ huấn luyện.

**Đáp án: A**

**Câu 4. "Transfer Learning" (Học chuyển giao) là một kỹ thuật AI mạnh mẽ, ý nghĩa của nó là gì?**

A. Huấn luyện một mô hình từ đầu cho mỗi tác vụ mới.

B. Tái sử dụng một mô hình cho các tác vụ tương tự.

C. Chuyển dữ liệu từ mô hình này sang mô hình khác.

D. Chuyển đổi mô hình huấn luyện.

**Đáp án: B**

**Câu 5. "RNN" (Recurrent Neural Networks) được thiết kế đặc biệt để xử lý loại dữ liệu nào hiệu quả nhất?**

A. Dữ liệu hình ảnh tĩnh.

B. Dữ liệu có tính tuần tự, chuỗi thời gian.

C. Dữ liệu cơ sở dữ liệu dạng bảng.

D. Dữ liệu dưới dạng sơ đồ.

**Đáp án: B**

**Câu 6. Trong học máy, sự đánh đổi "Bias-Variance Tradeoff" đề cập đến điều gì?**

A. Mối quan hệ giữa tốc độ tính toán và chi phí phần cứng.

B. Cân bằng giữa sai số do mô hình quá đơn giản (bias) và sai số do mô hình quá phức tạp, nhạy cảm với dữ liệu (variance).

C. Làm cho sai số do mô hình quá đơn giản (bias) tăng, sai số do mô hình quá phức tạp, nhạy cảm với dữ liệu (variance) giảm.

D. Làm cho sai số do mô hình quá đơn giản (bias) giảm, sai số do mô hình quá phức tạp, nhạy cảm với dữ liệu (variance) tăng.

**Đáp án: E**

**Câu 7. Kỹ thuật nào cho phép các tác nhân AI học hỏi thông qua tương tác với môi trường và nhận phần thưởng từ các hành động đúng?**

A. Học có giám sát (Supervised Learning)

B. Học không giám sát (Unsupervised Learning)

C. Học tăng cường (Reinforcement Learning)

D. Học bán giám sát (Semi-supervised Learning)

**Đáp án: C**

**Câu 8.**

A. Giảm chi phí vận hành.

B. Không cần lo lắng về việc quản lý hoặc duy trì máy chủ.

C. Không cần lo lắng về việc bảo mật vì đã có công ty bảo mật thực hiện.

D. Không cần lo lắng về việc quản lý nhân sự do giảm nhân sự vận hành.

**Đáp án: B**

**Câu 9. "Data Governance" (Quản trị dữ liệu) là yếu tố sống còn trong CĐS vì lý do gì?**

A. Nó giúp lưu trữ dữ liệu rẻ hơn.

B. Nó thiết lập các chính sách, quy trình để đảm bảo chất lượng, bảo mật, tuân thủ pháp lý và sử dụng hiệu quả dữ liệu trong toàn tổ chức.

C. Nó thiết lập các chính sách, quy trình để đảm bảo chất lượng, số lượng, tuân thủ pháp lý và sử dụng hiệu quả dữ liệu trong toàn tổ chức.

D. Nó thiết lập các chính sách, quy trình để đảm bảo bảo mật, số lượng, tuân thủ pháp lý và sử dụng hiệu quả dữ liệu trong toàn tổ chức.

**Đáp án: B**

**Câu 10. Trong mã hóa đối xứng, cùng một khóa được sử dụng để?**

A. Mã hóa và giải mã

B. Mã hóa và xác thực

C. Mã hóa và kiểm tra

D. Giải mã và xác thực

**Đáp án: A**

**Câu 11. Nhật ký IIS nằm ở đâu?**

A. %SystemDrive%\inetpub\logs\LogFiles

B. %SystemDrive%\inetpub\logs

C. %SystemDrive%\inetpub\

D. %SystemDrive%\inetpub\logs\W3SVC1

**Đáp án: A**

**Câu 12. Các thành phần cơ bản của một máy tính gồm:**

A. Bộ nhớ trong, CPU và khối phối ghép vào ra

B. Bộ nhớ trong, CPU và thiết bị ngoại vi

C. Bộ nhớ trong, CPU, khối phối ghép vào ra và thiết bị ngoại vi

D. Bộ nhớ trong, CPU, bộ nhớ ngoài, bộ phối ghép vào ra và thiết bị ngoại vi

**Đáp án: D**

**Câu 13. Event ID nào sau đây không nằm trong Application Log?**

A. 11707 – Installation completed successfully

B. 11724 – Application removal completed successfully

C. 7040 – Start type changed

D. 20001 – Plug and Play driver install attempted

**Đáp án: C**

**Câu 14. Trong số các cặp giao thức và cổng dịch vụ sau, cặp nào là đúng:**

A. SMTP: TCP Port 21

B. Telnet: UDP Port 23

C. HTTP: TCP Port 80

D. SFTP: TCP Port 69

**Đáp án: C**

**Câu 15. Để phân giải địa chỉ IP thành địa chỉ MAC, sử dụng giao thức:**

A. ARP

B. DHCP

C. RARP

D. ICMP

**Đáp án: A**

**Câu 16. Lệnh ping sử dụng các gói tin nào sau đây:**

A. echo

B. TTL

C. SYN

D. FIN

**Đáp án: A**

**Câu 17. Vị trí của IIS log file với phiên bản IIS 7-7.5:**

A. %SystemDrive%\inetpub\logs\LogFiles

B. %System root%\Temp\config

C. %System root%\System32\config

D. %System root%\System32\eventlog

**Đáp án: A**

**Câu 18. Đâu là quyền cao nhất trên hệ thống của Windows:**

A. Administrator

B. NT System

C. User

D. Admin

**Đáp án: B**

**Câu 19. Các thành phần trong lpv4 được gọi là gì?**

A. ocet

B. octa

C. octang

D. octet

**Đáp án: D**

**Câu 20. Trong các phần mềm ảo hóa, khi muốn thực hiện cấu hình máy ảo không cho phép truy cập ra mạng LAN của máy vật lý và ngược lại, ta sẽ lựa chọn cấu hình nào trong việc thiết lập mạng cho máy ảo trong các tùy chọn sau?**

A. Host only

B. Bridge

C. Broadcast

D. NAT

**Đáp án: A**

**Câu 21. Hãy chỉ ra phát biểu đúng trong các phát biểu sau?**

A. Để nâng cấp máy tính thành Domain Controller ta bắt buộc phải cài đặt dịch vụ Active Directory Domain Services

B. Để nâng cấp máy tính thành Domain Controller ta bắt buộc phải có Root Domain trước đó

C. Để nâng cấp máy tính thành Domain Controller ta cần cài đặt DHCP Server để quản lý địa chỉ IP

D. Để nâng cấp máy tính thành Domain Controller ta cần cài đặt DNS Server trước để phân giải tên miền

**Đáp án: A**

**Câu 22. Cho số ở hệ thập phân là 47, số ở hệ nhị phân tương đương là?**

A. 101111

B. 110111

C. 101011

D. 101110

**Đáp án: A**

**Câu 23. Khi thư mục có biểu tượng cái khóa ở bên cạnh thì thư mục đó là loại thư mục nào?**

A. Thư mục bị khóa không truy cập được.

B. Thư mục chỉ được phép truy cập với quyền Administrators

C. Thư mục được đánh dấu là đồng bộ hóa

D. Thư mục quá vượt quá giới hạn số lượng kết nối truy cập

**Đáp án: B**

**Câu 24. Trong giao thức IPsec, chế độ nào được sử dụng để bảo vệ gói tin giữa hai cổng VPN?**

A. Transport Mode

B. Tunnel Mode

C. Hybrid Mode

D. Open Mode

**Đáp án: B**

**Câu 25. Giao thức nào dưới đây hỗ trợ bảo mật cho việc gửi email?**

A. POP3

B. SMTP

C. SMTPS

D. IMAP

**Đáp án: C**

**Câu 26. Nhật ký trên hệ điều hành Linux được chia làm mấy loại?**

A. 2

B. 3

C. 4

D. 5

**Đáp án: C**

**Câu 27. Trong Linux, lệnh nào dùng để hiển thị dung lượng trống còn lại của ổ đĩa?**

A. ls

B. du

C. df

D. free

Đáp án: C

**Câu 28. Câu lệnh xóa file trên hệ điều hành Linux mà không có cảnh báo là gì?**

A. rm -rf

B. rm

C. cd

D. mv

**Đáp án: A**

**Câu 29. Câu lệnh nào có tác dụng xem lịch sử thực thi lệnh trên Linux?**

A. ifconfig

B. cat/etc/password

C. history

D. ps

**Đáp án: C**

**Câu 30. Câu lệnh nào có tác dụng xóa lịch sử thực thi lệnh trên Linux?**

A. history -c

B. history -f

C. history -h

D. history –e

**Đáp án: A**

**Câu 31. Bộ mã ASSCII mở rộng gồm bao nhiêu kí tự?**

A. 128

B. 256

C. 512

D. 1024

**Đáp án: B**

**Câu 32. Các giao thức bảo mật trên Internet như SSL, TSL, SSH hoạt động ở tầng nào trong mô hình OSI?**

A. Tầng 3

B. Tầng 4

C. Từ Tầng 4 đền Tầng 7

D. Từ Tầng 3 đến Tầng 7

**Đáp án: C**

**Câu 33. Trong mạng máy tính, giao thức nào dùng để phân giải tên miền sang địa chỉ IP?**

A. HTTP

B. FTP

C. DNS

D. SMTP

**Đáp án: C**

**Câu 34. Địa chỉ nào sau đây là địa chỉ** **broadcast của dải mạng 52.93.24.42/20?**

A. 52.93.0.255

B. 52.93.24.255

C. 52.93.32.255

D. 52.93.31.255

**Đáp án: D**

**Câu 35. Trong giải thuật SHA-512, 80 từ mở rộng (message schedule) được tạo ra từ đâu?**

A. Được khởi tạo cố định theo tiêu chuẩn SHA-512 (giá trị mặc định)

B. Được mở rộng từ toàn bộ khối dữ liệu (message block)

C. Được sinh ra chỉ từ một phần đầu của khối dữ liệu

D. Được tính toán ngẫu nhiên tại mỗi vòng lặp

**Đáp án: B**

**Câu 36. Chứng nhận số (Digital Certificate) không chứa các thành phần nào sau đây?**

A. Chữ ký số của tổ chức cấp chứng nhận

B. Thông tin về thuật toán mã hóa khóa công khai

C. Thuật toán dùng để tạo chữ ký số

D. Thông tin về người sở hữu chứng nhận

**Đáp án: D**

**Câu 37. Chứng nhận số chứa thành phần nào sau đây?**

A. Chữ ký

B. Thông tin thuật toán tạo mã khóa

C. Thuật toán tạo chữ ký

D. Thông tin về chủ sở hữu chứng nhận

**Đáp án: A**

**Câu 38. Một trong những ứng dụng chính của hàm băm là gì?**

A. Đảm bảo tính toàn vẹn và xác thực dữ liệu

B. Nâng cao hiệu quả của chữ ký số

C. Xác minh mật khẩu người dùng

D. Mã hóa dữ liệu truyền qua mạng

**Đáp án: A**

### (2) HIỂU BIẾT VỀ TRINH SÁT, PHÒNG THỦ, TẤN CÔNG MẠNG (GỒM 50 CÂU)

**Câu 1. Kỹ thuật nào mô tả việc kẻ tấn công sử dụng AI để tự động điều chỉnh chiến lược tấn công dựa trên phản ứng của hệ thống phòng thủ đối phương?**

A. Tấn công tĩnh (Static Attack)

B. Tấn công thích nghi (Adaptive Attack)

C. Tấn công bằng tay (Manual Attack)

D. Tấn công ngẫu nhiên (Random Attack)

**Đáp án: B**

**Câu 2. Phương pháp "Federated Learning" (Học liên kết) giải quyết thách thức nào khi áp dụng AI trong phòng thủ mạng?**

A. Cho phép đào tạo mô hình AI chung trên dữ liệu phân tán để tăng tốc độ xử lý của CPU.

B. Cho phép đào tạo mô hình AI chung trên dữ liệu phân tán mà không cần di chuyển dữ liệu ra khỏi nơi lưu trữ gốc.

C. Cho phép đào tạo mô hình AI chung trên dữ liệu phân tán để giảm băng thông mạng.

D. Cho phép đào tạo mô hình AI chung trên dữ liệu phân tán để mã hóa toàn bộ kết nối mạng.

**Đáp án: B**

**Câu 3. Khi kẻ tấn công sử dụng Generative AI (AI tạo sinh) để tạo ra các "deepfake" giọng nói hoặc khuôn mặt, mục tiêu tấn công mạng là gì?**

A. Làm giả cuộc gọi từ CEO để thực hiện lừa đảo.

B. Làm giả cuộc gọi từ SEO để thực hiện lừa đảo.

C. Để dò tìm ra mật khẩu ngẫu nhiên.

D. Để dò tìm ra mật khẩu lớp 2.

**Đáp án: A**

**Câu 4. Thuật ngữ nào mô tả sự cố khi một mô hình AI phòng thủ bị "đầu độc" (poisoning) trong quá trình huấn luyện bằng dữ liệu độc hại do kẻ tấn công chèn vào?**

A. Data Cleaning (Làm sạch dữ liệu)

B. Model Inversion Attack (Tấn công đảo ngược mô hình)

C. Data Poisoning Attack (Tấn công đầu độc dữ liệu)

D. Overfitting (Quá khớp)

**Đáp án: C**

**Câu 5. Kỹ thuật AI nào có thể được sử dụng để phân tích hàng tỷ bản ghi lưu lượng mạng (network logs) trong thời gian gần thực để tìm ra dấu vết của APT (Advanced Persistent Threats)?**

A. Hồi quy đơn giản (Simple Regression)

B. Xử lý ngôn ngữ tự nhiên (NLP) trên các tệp tin log.

C. Phân tích dữ liệu lớn (Big Data Analytics) kết hợp với Machine Learning.

D. Sử dụng bảng tính Excel.

**Đáp án: C**

**Câu 6. Việc sử dụng AI trong tấn công nhằm tự động phát triển các biến thể mã độc (malware variants) mới để trốn tránh sự phát hiện của phần mềm diệt virus truyền thống gọi là gì?**

A. Mã độc tĩnh (Static Malware)

B. Mã độc đa hình/siêu đa hình (Polymorphic/Metamorphic Malware)

C. Mã độc dựa trên chữ ký (Signature-based Malware)

D. Phần mềm an toàn.

**Đáp án: B**

**Câu 7. Hệ thống SOAR (Security Orchestration, Automation, and Response) tích hợp AI để làm gì?**

A. Để giảm thiểu hóa việc điều tra và ứng phó với sự cố bảo mật mà không cần nhiều sự can thiệp của con người.

B. Để tự động hóa việc điều tra và ứng phó với sự cố bảo mật mà không cần nhiều sự can thiệp của con người.

C. Để tăng tốc việc điều tra và ứng phó với sự cố bảo mật mà không cần nhiều sự can thiệp của con người.

D. Để tạo ra nhiều cảnh báo hơn mà không cần nhiều sự can thiệp của con người.

**Đáp án: B**

**Câu 8. Ưu điểm chính của mô hình AI dựa trên đồ thị (Graph-based AI models) trong phòng thủ mạng là gì?**

A. Khả năng tương quan hóa các mối quan hệ phức tạp và phụ thuộc lẫn nhau giữa các thực thể mạng (người dùng, thiết bị, IP, tệp tin) để phát hiện các mối đe dọa tinh vi.

B. Khả năng mô hình hóa các mối quan hệ phức tạp và phụ thuộc lẫn nhau giữa các thực thể mạng (người dùng, thiết bị, IP, tệp tin) để phát hiện các mối đe dọa tinh vi.

C. Khả năng mô hình hóa các mối quan hệ phức tạp và phụ thuộc lẫn nhau giữa các thực thể mạng (người dùng, thiết bị, IP, tệp tin) để phân tích các mối đe dọa tinh vi.

D. Khả năng biểu đồ hóa các mối quan hệ phức tạp và phụ thuộc lẫn nhau giữa các thực thể mạng (người dùng, thiết bị, IP, tệp tin) để phát hiện các mối đe dọa tinh vi.

**Đáp án: B**

**Câu 9. Một kẻ tấn công sử dụng AI để tự động tạo ra các danh sách mật khẩu tùy chỉnh dựa trên thông tin công khai của nạn nhân đang thực hiện loại tấn công nào hiệu quả hơn?**

A. Tấn công vét cạn truyền thống.

B. Tấn công từ điển có mục tiêu.

C. Tấn công DDoS.

D. Tấn công lừa đảo qua điện thoại.

**Đáp án: B**

**Câu 10. Tin tặc sử dụng truy vấn sau tại trình duyệt nhằm chiếm quyền hệ thống, đồng chí cho biết dạng tấn công này là gì?**

***http://victim.local/manage.php?resolve=btis.vn%0a`/sbin/php/var/www/html/images/dropper.php`%0a***

A. SSI injection

B. Ruby code injection

C. Server-side template injection

D. OS command injection

**Đáp án: D**

**Câu 11. Kỹ thuật nào giúp hacker chiếm quyền điều khiển máy tính từ xa?**

A. Remote Code Execution

B. Phishing

C. DoS Attack

D. DNS Poisoning

**Đáp án: A**

**Câu 12. Loại tấn công nào lợi dụng lỗi lập trình để ghi đè bộ nhớ?**

A. Phishing

B. Man-in-the-Middle

C. Buffer Overflow

D. SQL Injection

**Đáp án: C**

**Câu 13. Các hình thức, thủ đoạn được các đối tượng sử dụng để chiếm đoạt mạng xã hội?**

A. Sử dụng chương trình khuyến mãi - trúng thưởng hay Mini Game, Lỗ hổng bảo mật facebook

B. Phishing, Dò mật khẩu, Sử dụng trojan, Keylog, Sử dụng chương trình khuyến mãi - trúng thưởng hay Mini Game, Lỗ hổng bảo mật facebook

C. Dò mật khẩu, Sử dụng chương trình khuyến mãi - trúng thưởng hay Mini Game, Lỗ hổng bảo mật facebook

D. Phishing, Dò mật khẩu, Sử dụng chương trình khuyến mãi - trúng thưởng hay Mini Game, Lỗ hổng bảo mật facebook

**Đáp án: B**

**Câu 14. Trong mô hình phòng thủ nhiều lớp (Defense in Depth), lớp nào chịu trách nhiệm phát hiện và phản ứng sớm với hành vi bất thường trong hệ thống?**

A. Firewall lớp mạng

B. IDS/IPS và SIEM lớp giám sát

C. Endpoint Antivirus lớp thiết bị đầu cuối

D. Backup lớp khôi phục dữ liệu

Đáp án: B

**Câu 15. Trong hệ thống giám sát an ninh mạng, giao thức nào thường được sử dụng để truyền dữ liệu log từ thiết bị mạng về máy chủ phân tích tập trung (SIEM)?**

A. SNMP

B. Syslog

C. FTP

D. HTTP

Đáp án: B

**Câu 16. Loại mã nguồn độc hại nào có thể được cài đặt song không gây tác hại cho đến khi thỏa mãn điều kiện kích hoạt?**

A. Worm

B. Trojan horse

C. Logic bomb

D. Stealth virus

**Đáp án: C**

**Câu 17. Mã hóa bất đối xứng (public-key encryption) có đặc điểm nào sau đây:**

A. Khóa giải mã và khóa mã hóa là giống nhau

B. Khóa giải mã là bí mật, khóa mã hóa có thể công khai

C. Chỉ cần một khóa duy nhất để mã hóa và giải mã

D. Không thể dùng để đảm bảo tính bảo mật thông tin

**Đáp án: B**

**Câu 18. Mục nào không là tấn công chủ động.**

A. Tấn công nghe lén (eavesdropping)

B. Tấn công từ chối dịch vụ

C. Tấn công replay

D. Tấn công giả mạo (masquerade)

**Đáp án: A**

**Câu 19. Kiểu tấn công nào liên quan đến kẻ tấn công truy cập các tệp trong các thư mục khác với thư mục gốc.**

A. Directory traversal

B. SQL injection

C. Command injection

D. XML injection

**Đáp án: A**

**Câu 20. Cơ sở của một cuộc tấn công SQL injection là gì?**

A. Để chèn câu lệnh SQL thông qua đầu vào chưa được lọc

B. Để máy chủ SQL tấn công trình duyệt web máy khách

C. Để hiển thị mã SQL để nó có thể được kiểm tra

D. Để liên kết các máy chủ SQL thành một botnet

**Đáp án: A**

**Câu 21. Điều gì là duy nhất về tấn công cross-site scripting (XSS) so với các cuộc tấn công injection khác?**

A. XSS không tấn công máy chủ ứng dụng web để ăn cắp hoặc làm hỏng thông tin của nó.

B. Mã SQL được sử dụng trong một cuộc tấn công XSS

C. XSS yêu cầu sử dụng trình duyệt

D. Tấn công XSS hiếm khi được sử dụng nữa so với các cuộc tấn công injection khác

**Đáp án: A**

**Câu 22. ID của event Successful Logon là.**

A. 528

B. 529

C. 538

D. 628

**Đáp án: A**

**Câu 23. ID của event Successful Network Logon là:**

A. 538

B. 540

C. 578

D. 542

**Đáp án: B**

**Câu 24. Hình thức nào sau đây không phải là hình thức tấn công DoS?**

A. Teardrop

B. SYN attack

C. Smurf

D. IP Spoofing

**Đáp án: D**

**Câu 25. Ưu điểm chính của mã hóa khóa công khai so với mã hóa đối xứng là gì:**

A. Tốc độ mã hóa và giải mã nhanh hơn

B. Không cần chia sẻ khóa bí mật qua kênh an toàn

C. Dễ triển khai hơn mã hóa đối xứng

D. Không cần dùng khóa để giải mã dữ liệu

**Đáp án: B**

**Câu 26. Kỹ thuật nào dưới đây được sử dụng để che giấu mã độc bên trong tập tin hợp lệ nhằm tránh bị phát hiện bởi phần mềm diệt virus?**

A. Obfuscation

B. Hashing

C. Encryption

D. Encoding

**Đáp án: A**

**Câu 27. Giai đoạn đầu tiên khi tiến hành tấn công chiếm quyền điều khiển là gì?**

A. Duy trì kết nối

B. Chiếm quyền

C. Trinh sát thông tin

D. Dò quét

**Đáp án: C**

**Câu 28. Phương pháp footprinting nào sau đây không tác động đến hệ thống mục tiêu?**

A. Trinh sát OSINT

B. Traceroute

C. Ping

D. Dò quét

**Đáp án: A**

**Câu 29. Bước tiếp theo sẽ được thực hiện sau khi footprinting là gì?**

A. Scanning

B. Enumeration

C. System Hacking

D. Post Exploit

**Đáp án: A**

**Câu 30. Trong bảo mật thông tin, thuật ngữ 'Non-repudiation' nghĩa là gì?**

A. Bảo mật dữ liệu

B. Toàn vẹn dữ liệu

C. Ngăn chặn chối bỏ giao dịch

D. Kiểm soát truy cập

**Đáp án: C**

**Câu 31. Trong thuật toán mã hóa bất đối xứng RSA, khóa nào được dùng để mã hóa dữ liệu gửi đi?**

A. Khóa riêng

B. Khóa chung

C. Khóa tạm

D. Khóa bí mật

**Đáp án: B**

**Câu 32. Loại tấn công nào tận dụng tính năng tự động thực thi tập tin autorun.inf của hệ điều hành?**

A. SQL Injection

B. Autorun Malware

C. Cross-site Scripting

D. Phishing

**Đáp án: B**

**Câu 33. Hình thức tấn công nào thực hiện gửi liên tục các gói SYN mà không hoàn tất quá trình bắt tay 3 bước?**

A. SYN Flood

B. UDP Flood

C. ICMP Flood

D. HTTP Flood

**Đáp án: A**

**Câu 34. Tấn công "Credential Stuffing" là gì?**

A. Dùng thông tin đăng nhập bị rò rỉ để truy cập vào nhiều tài khoản khác

B. Tấn công bằng cách dò mật khẩu từng ký tự

C. Gửi mã độc qua email

D. Lây lan virus qua mạng LAN

**Đáp án: A**

**Câu 35. Kiểu tấn công nào mà hacker đóng giả một thiết bị hợp lệ trong mạng để đánh cắp thông tin?**

A. DoS

B. Man-in-the-Middle

C. Spoofing

D. Sniffing

**Đáp án: C**

**Câu 36. Chuẩn mã hóa nào được xem là kế nhiệm của DES?**

A. 3DES

B. AES

C. RC4

D. Blowfish

**Đáp án: B**

**Câu 37. Trong các loại mã độc sau, loại nào chuyên ghi lại thao tác bàn phím của người dùng?**

A. Spyware

B. Keylogger

C. Trojan

D. Ransomware

**Đáp án: B**

**Câu 38. Event ID nào ghi nhận sự thay đổi password tài khoản người dùng trong Windows Security log?**

A. 4624

B. 4723

C. 4634

D. 4647

**Đáp án: B**

**Câu 39. Chương trình độc hại nào thường hướng tới các sản phẩm Microsoft Office?**

A. Virus đa hình

B. Macro virus

C. Trojan

D. Worm

**Đáp án: B**

**Câu 40. Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin?**

A. Bí mật

B. Toàn vẹn

C. Sẵn sàng

D. Xác thực

**Đáp án: A**

**Câu 41. Loại mã nguồn độc hại nào có thể được cài đặt song không gây tác hại cho đến khi thỏa mãn điều kiện kích hoạt?**

A. Worm

B. Trojan horse

C. Logic bomb

D. Stealth virus

**Đáp án: C**

**Câu 42. Loại mã độc nào lây lan từ hệ thống này sang hệ thống khác hoặc từ mạng này sang mạng khác và gây ra các thiệt hại tương tự như virus đối với hệ thống bị nhiễm?**

A. Worm

B. Rootkit

C. Trojan

D. Adware

**Đáp án: A**

**Câu 43. “Scripting virus” là gì?**

A. Là các cảnh báo giả về virus. Các cảnh bảo giả này thường núp dưới dạng một yêu cầu khẩn cấp để bảo vệ hệ thống.

B. Là loại virus thường lây vào các file thực thi, đoạn mã virus sẽ được kích hoạt trước và tiếp tục thực hiện các hành vi phá hoại, lây nhiễm khi file thực thi.

C. Là loại virus được viết bằng các ngôn ngữ script như VBScript, JavaScript, Batch script.

D. Là loại virus tự động lây lan qua email và các liên kết độc hại.

**Đáp án: C**

**Câu 44. “Virus Hoax” là gì?**

A. Là các cảnh báo giả về virus. Các cảnh bảo giả này thường núp dưới dạng một yêu cầu khẩn cấp để bảo vệ hệ thống

B. Là loại Virus thường lây vào các file thực thi (ví dụ file có phần mở rộng .com, .exe, .dll) một đoạn mã để khi file được thực thi, đoạn mã virus sẽ được kích hoạt trước và tiếp tục thực hiện các hành vi phá hoại, lây nhiễm

C. Là loại virus được viết bằng các ngôn ngữ script như VBScript, JavaScript, Batch script.

D. Là những thông tin giả mạo nhằm đánh lừa người dùng.

**Đáp án: A**

**Câu 45. “File Virus” là gì?**

A. Là các cảnh báo giả về virus. Các cảnh bảo giả này thường núp dưới dạng một yêu cầu khẩn cấp để bảo vệ hệ thống

B. Là loại Virus thường lây vào các file thực thi (ví dụ file có phần mở rộng .com, .exe, .dll) một đoạn mã để khi file được thực thi, đoạn mã virus sẽ được kích hoạt trước và tiếp tục thực hiện các hành vi phá hoại, lây nhiễm

C. Là loại virus được viết bằng các ngôn ngữ script như VBScript, JavaScript, Batch script.

D. Là loại virus lây nhiễm qua các file dữ liệu, không nhất thiết là file thực thi, có thể lây lan khi file dữ liệu được mở hoặc chạy

**Đáp án: B**

**Câu 46. Mã độc “Backdoor” là gì?**

A. Là phần mềm dùng để đánh cắp thông tin của người dùng

B. Là một dạng Trojan. Khi xâm nhập vào máy tính sẽ mở ra một cổng dịch vụ cho phép tin tặc điều khiển máy tính nạn nhân.

C. Là loại Trojan nhằm mục đích quảng cáo

D. Là phần mềm độc hại cho phép truy cập trái phép vào hệ thống mà không cần sự đồng ý của người dùng

**Đáp án: B**

**Câu 47. Mã độc “Adware” là gì?**

A. Là phần mềm dùng để đánh cắp thông tin của người dùng

B. Là một dạng Trojan. Khi xâm nhập vào máy tính sẽ mở ra một cổng dịch vụ cho phép tin tặc điều khiển máy tính nạn nhân.

C. Là loại Trojan nhằm mục đích quảng cáo

D. Là phần mềm hiển thị quảng cáo không mong muốn trên thiết bị của người dùng

**Đáp án: C**

**Câu 48. Mã độc “Spyware” là gì?**

A. Là phần mềm dùng để đánh cắp thông tin của người dùng

B. Là một dạng Trojan. Khi xâm nhập vào máy tính sẽ mở ra một cổng dịch vụ cho phép tin tặc điều khiển máy tính nạn nhân.

C. Là loại Trojan nhằm mục đích quảng cáo

D. Là phần mềm gián điệp thu thập thông tin cá nhân hoặc hoạt động của người dùng mà không được phép

**Đáp án: A**

**Câu 49. Mã độc “Rootkit” là gì?**

A. Là một loại mã độc được dùng để ngăn chặn người dùng truy cập dữ liệu và sử dụng máy tính.

B. Là loại mã độc phát triển và lây lan mạnh mẽ nhất hiện nay, thường được phát tán qua email.

C. Là một chương trình máy tính được thiết kế để truy cập sâu vào hệ thống máy tính mà vẫn che giấu được sự hiện diện của nó và các phần mềm độc hại khác

D. Là những máy tính bị nhiễm virus và bị điều khiển thông qua Trojan, virus… Tin tặc lợi dụng sức mạnh của những máy tính bị nhiễm virus để thực hiện các hành vi phá hoại và ăn cắp thông tin

**Đáp án: C**

**Câu 50. Dạng tấn công từ chối dịch vụ “SYN Flood” là gì?**

A. Là khai thác điểm yếu trong chuỗi kết nối TCP, được gọi là bắt tay ba chiều. Máy chủ sẽ nhận được một thông điệp đồng bộ (SYN) để bắt đầu "bắt tay". Máy chủ nhận tin nhắn bằng cách gửi cờ báo nhận (ACK) tới máy lưu trữ ban đầu, sau đó đóng kết nối

B. là một giao thức mạng không session. Một UDP Flood nhắm đến các cổng ngẫu nhiên trên máy tính hoặc mạng với các gói tin UDP. Máy chủ kiểm tra ứng dụng tại các cổng đó nhưng không tìm thấy ứng dụng nào.

C. Ping of Death điều khiển các giao thức IP bằng cách gửi những đoạn mã độc đến một hệ thống

D. Cho phép kẻ tấn công sử dụng nguồn lực tối thiểu trong một cuộc tấn công và các mục tiêu trên máy chủ web

**Đáp án: A**

### (3) CÓ KIẾN THỨC VỀ HỆ THỐNG MẠNG, CÁC THÀNH PHẦN TRONG HỆ THỐNG MẠNG (GỒM 23 CÂU)

**Câu 1. Trong TCP/IP, số cổng nào dành riêng cho dịch vụ NetBIOS Session Service?**

A. 139

B. 445

C. 110

D. 443

**Đáp án: A**

**Câu 2. Kiến trúc mạng loại nào sử dụng các chân nối dạng T-connector?**

A. BUS

B. EXTENDED -STAR

C. RING

D. STAR

**Đáp án : A**

**Câu 3. Topo mạng cục bộ nào mà tất cả các trạm phân chia chung một đường truyền chính?**

A. Bus

B. Star

C. Ring

D. Hybrid

**Đáp án: A**

**Câu 4. Lớp nào trong mô hình OSI chịu trách nhiệm thiết lập, duy trì và kết thúc phiên làm việc giữa hai thiết bị?**

A. Transport

B. Application

C. Session

D. Network

**Đáp án: C**

**Câu 5. Phương thức nào mà trong đó cả hai bên đều có thể đồng thời gửi dữ liệu đi:**

A. Full-duplex

B. Simplex

C. Half-duplex

D. Khác

**Đáp án: A**

**Câu 6. Định tuyến tĩnh là loại định tuyến:**

A. Dùng cho mạng nhỏ cấu trúc đơn giản

B. Nhà quản trị chỉ việc cấu hình giao thức định tuyến cho Router

C. Nhà quản trị phải cấu hình từng dòng lệnh cho các mạng đích cần thiết

D. Router có thể giúp lựa chọn đường đi ngắn nhất trên mạng

**Đáp án: C**

**Câu 7. Một Hub tốc độ 100Mbps có 12 cổng thì tốc độ của mỗi cổng sẽ là:**

A. Tối đa 100Mbps khi có 12 máy tính cắm vào Hub

B. Tối thiểu 100Mbps khi chỉ có một máy tính cắm vào Hub

C. Tối đa 100Mbps khi chỉ có một máy tính cắm vào Hub

D. Tối thiểu 8.3Mbps khi có 12 máy tính cắm vào Hub

**Đáp án: C**

**Câu 8. Một máy chủ DCHP cần cấp phát tự động và đầy đủ các thông số nào sau đây cho các máy tính trong mạng?**

A. Địa chỉ IP, Subnet Mask, DNS Server

B. Địa chỉ IP, Subnet Mask, Default Gateway, Địa chỉ mạng

C. Địa chỉ IP, Subnet Mask, Default Gateway, DNS Server

D. Địa chỉ IP, Default Gateway, DNS Server, Địa chỉ mạng

**Đáp án: C**

**Câu 9. Hãy chọn câu chính xác nhất trong các câu sau đây?**

A. DNS dùng để thiết lập kết nối Internet

B. DNS trợ giúp cho truy cập Internet đơn giản nhất mà không cần các kỹ thuật khác

C. Mỗi một máy tính phân giải tên/địa chỉ phải có khả năng liên lạc được với ít nhất một DNS

D. DNS dùng để thiết lập tên định danh đến máy chủ mạng

**Đáp án: C**

**Câu 10. TCP là giao thức?**

A. Phi kết nối (Connectionless)

B. Hướng kết nối (Connection-oriented)

C. Định tuyến (Routing)

D. Mã hóa dữ liệu (Data Encryption)

**Đáp án: B**

**Câu 11. Để hạn chế sự đụng độ của các gói tin trên 1 đoạn mạng, người ta chia mạng thành các mạng nhỏ hơn và kết nối chúng lại bằng các thiết bị:**

A. Repeaters

B. Hubs

C. Bridges hoặc Switches

D. Router

**Đáp án: C**

**Câu 12. Địa chỉ IP lớp A có bao nhiêu bit dành cho phần mạng?**

A. 4

B. 8

C. 16

D. 12

**Đáp án: B**

**Câu 13. Trong mô hình OSI, quá trình đóng gói dữ liệu xảy ra như thế nào khi dữ liệu được gửi đi?**

A. Dữ liệu chỉ được xử lý tại tầng Transport trước khi gửi đi

B. Mỗi tầng thêm vào dữ liệu nhận được một header để tạo thành PDU của tầng đó

C. Mỗi tầng thêm vào dữ liệu nhận được một sector để tạo thành PDU của tầng đó

D. Quá trình đóng gói chỉ xảy ra ở tầng Network và Physical

**Đáp án: B**

**Câu 14. Cho địa chỉ IP 192.168.2.30/12, Subnet mask là?**

A. 255.240.0.0

B. 255.255.0.0

C. 255.255.255.0

D. 255.255.240.0

**Đáp án: A**

**Câu 15. Khối đầu tiên của lớp B có giá trị trong khoảng nào?**

A. 129 đến 191

B. 128 đến 191

C. 128 đến 193

D. 128 đến 192

**Đáp án: B**

**Câu 16. Phần nào trong địa chỉ IP được Router sử dụng khi tìm đường đi?**

A. Router address

B. Network address

C. FDDI

D. Host address

**Đáp án: B**

**Câu 17. Trong HEADER của IP PACKET có chứa:**

A. Source và Destination addresses

B. Source address

C. IP addresses

D. Destination address

**Đáp án: A**

**Câu 18. Cho trước 2 địa chỉ IP và Subnet mask, muốn xác định địa chỉ mạng của hai địa chỉ IP trên ta sử dụng phép toán?**

A. OR

B. AND

C. XOR

D. NOT

**Đáp án: B**

**Câu 19. Khi hai thiết bị trong mạng LAN muốn trao đổi dữ liệu, điều kiện tiên quyết là gì?**

A. Cùng Subnet Mask và cùng Default Gateway

B. Cùng lớp địa chỉ IP

C. Nằm trong cùng một mạng con (subnet)

D. Cùng dải MAC address

**Đáp án: C**

**Câu 20. Trong mô hình OSI, tầng nào chịu trách nhiệm xác định địa chỉ vật lý và truy cập môi trường truyền dẫn?**

A. Data Link

B. Network

C. Transport

D. Application

**Đáp án: A**

**Câu 21. Sử dụng IPSec có thể giúp đảm bảo những tính: tính xác thực, tính toàn vẹn, tính bảo mật và ?**

A. Khả năng sử dụng (Usability)

B. Tính không thể chối bỏ (Non-repudiation)

C. Security

D. Khả năng hoạt động (Operability)

**Đáp án: B**

**Câu 22. Giao thức nào chịu trách nhiệm kiểm soát kích thước và tốc độ trao đổi thông điệp HTTP giữa máy chủ và máy khách?**

A. TCP

B. ARP

C. DHCP

D. HTTP

**Đáp án: A**

**Câu 23. Giao thức nào cho phép truy cập từ xa trên máy tính Windows?**

A. RDP

B. SSH

C. SMB

D. Telnet

**Đáp án: A**

### (4) CÓ KHẢ NĂNG THỰC HIỆN KIỂM TRA AN TOÀN THÔNG TIN MÁY TÍNH CÁ NHÂN (GỒM 20 CÂU HỎI)

**Câu 1. Công cụ nào có thể cho biết tiến trình nào có file hoặc folder đang mở hoặc khóa?**

A. Process Explorer

B. Autoruns

C. Power Tools

D. Wireshark

**Đáp án: A**

**Câu 2. Công cụ nào có các tính năng tương tự như Task Manager?**

A. TCPView

B. Autoruns

C. Process Explorer

D. Wireshark

**Đáp án: C**

**Câu 3. Công cụ nào không có tính năng xác minh chữ ký mã nguồn (Code Signature Verification)?**

A. Process Explorer

B. Autoruns

C. TCPView

D. Wireshark

**Đáp án: C**

**Câu 4. Công cụ nào có tích hợp tính năng Check Virus Total?**

A. TCPView

B. Process Monitor

C. Process Explorer

D. Wireshark

**Đáp án: C**

**Câu 5. Tập tin hệ thống svchost.exe nằm trong thư mục nào là tập tin hệ thống hợp lệ?**

A. Windows\System32

B. Windows\System

C. Windows\ SystemTemp

D. Windows\ SystemResources

**Đáp án: A**

**Câu 6. Sử dụng công cụ nào để lấy mẫu mã độc nghi ngờ theo đường dẫn vào một thư mục?**

A. Process Explorer

B. PowerTools

C. TCpView

D. Autoruns

**Đáp án: B**

**Câu 7. File Service Host được cung cấp bởi Microsoft cho các hệ điều hành Windows hợp lệ là?**

A. svchost.exe

B. svch0st.exe

C. svchosts.exe

D. svchsost.exe

**Đáp án: A**

**Câu 8. Nhiều loại mã độc làm lỗi Registry thì sử dụng công cụ nào để sửa lỗi mất registry?**

A. Autoruns

B. PowerTools

C. XueTr

D. AllToolsInOne

**Đáp án: D**

**Câu 9. File hệ thống nào là một Máy chủ lưu trữ cho các tệp DDL và các tệp thực thi nhị phân của Mircosoft Windows?**

A. dllhost.exe

B. dllhost.inf

C. dll.host.exe

D. dllhost. winmd

**Đáp án: A**

**Câu 10. File hệ thống dllhost.exe hợp lệ nằm đúng trong thư mục nào?**

A. C:\Windows\System

B. C:\Windows\Security

C. C:\Windows\Setup

D. C:\Windows\System32

**Đáp án: D**

**Câu 11. Có thể sử dụng công cụ nào để cấu hình mức độ ưu tiên của một tiến trình Process?**

A. Autoruns

B. TCPView

C. Process Explorer

D. Wireshark

**Đáp án: C**

**Câu 12. Có thể sử dụng công cụ nào để tạm dừng (suspend) một tiến trình Process?**

A. Autoruns

B. Process Explorer

C. TCPView

D. Wireshark

**Đáp án: B**

**Câu 13. Tab Image Hijacks có trong công cụ nào sau đây?**

A. Autoruns

B. Process Explorer

C. TCPView

D. Wireshark

**Đáp án: A**

**Câu 14. Tab Boot Execute có trong công cụ nào sau đây?**

A. Autoruns

B. Process Explorer

C. TCPView

D. Wireshark

**Đáp án: A**

**Câu 15. Chương trình nào sau đây không phải là chương trình độc lập?**

A. Trojan

B. Worm

C. Virus

D. Spyware

**Đáp án: C**

**Câu 16. Process Monitor là công cụ dùng để**

A. Tìm kiếm và tiêu diệt mã độc trên máy tính

B. Giám sát và hiển thị tất cả hoạt động của hệ thống trong thời gian thực

C. Kiểm tra các chương trình tự động khởi động cùng hệ thống

D. Dò quét và hiển thị tất cả hoạt động của hệ thống trong thời gian thực

**Đáp án: B**

**Câu 17. Công cụ nào dưới đây là công cụ phân tích mã độc?**

A. Autoruns

B. IDA

C. Syslog-ng

D. Process Explorer

**Đáp án: B**

**Câu 18. Loại file nào sau đây thường có nguy cơ cao chứa virus macro?**

A. .exe

B. .doc (tập tin văn bản)

C. .jpg (hình ảnh)

D. .mp3 (file âm thanh)

**Đáp án: B**

**Câu 19. Công cụ nào sau đây không có trong bộ công cụ kiểm tra an toàn thông tin**

A. QRCode

B. Process Monitor

C. TCPViewX

D. CFF Explorer

**Đáp án: D**

**Câu 20. Thư mục nào chứa Events Log trong hệ điều hành Windows?**

A. \ProgramData\winevt\Logs

B. \Users\winevt\Logs

C. \System32\winevt\Logs

D. \System32 \Logs

**Đáp án: C**

### (5) HIỂU ĐƯỢC CẤU TẠO, TÍNH NĂNG KỸ CHIẾN THUẬT CỦA CÁC HỆ THỐNG TRINH SÁT, PHÒNG THỦ, TẤN CÔNG MẠNG (GỒM 43 CÂU)

**Câu 1. Thành phần nào là của hệ thống thu thập và phân tích log HP Arcsight?**

A. ADS

B. FMC

C. Logger

D. FMS

**Đáp án: C**

**Câu 2. Câu lệnh thay đổi thời gian tạo file trong hệ thống sử dụng meterpreter của Metasploit là gì?**

A. timestomp

B. timesto

C. tistomp

D. titomp

**Đáp án: A**

**Câu 3. Một hệ thống SIEM (Security Information and Event Management) giúp gì trong bảo mật?**

A. Theo dõi và phân tích nhật ký sự kiện để phát hiện mối đe dọa

B. Tăng tốc độ kết nối mạng

C. Bảo vệ khỏi phần mềm độc hại

D. Tạo mật khẩu mạnh tự động

**Đáp án: A**

**Câu 4. Công cụ nào dưới đây được sử dụng phổ biến để khai thác lỗ hổng và thực thi mã độc trên hệ thống đích?**

A. Nmap

B. Wireshark

C. Metasploit

D. Netcat

**Đáp án: C**

**Câu 5. Câu lệnh Nmap nào sau đây sử dụng để quét cổng 80 trên địa chỉ IP 192.168.0.10 sử dụng kết nối TCP?**

A. nmap –sU –p 80 192.168.0.10

B. nmap –sT –p 80 192.168.0.10

C. nmap –sS –p 80 192.168.0.10

D. nmap -sX -p 80 192.168.0.10

**Đáp án: B**

**Câu 6. Câu lệnh nmap nào sau đây sử dụng để quét cổng 80 trên địa chỉ IP 192.168.1.11 sử dụng kết nối UDP?**

A. nmap –sS –p 80 192.168.1.1

B. nmap –sU –p 80 192.168.1.11

C. nmap –sT –p 80 192.168.1.1

D. nmap -sX -p 80 192.168.1.1

**Đáp án: B**

**Câu 7. Câu lệnh nmap nào sau đây sử dụng để quét cổng 80 trên địa chỉ IP 192.168.1.12 sử dụng SYN Scan?**

A. nmap –sT –p 80 192.168.1.1

B. nmap –sU –p 80 192.168.1.12

C. nmap –sS –p 80 192.168.1.12

D. nmap -sX -p 80 192.168.1.1

**Đáp án: C**

**Câu 8. Câu lệnh nào dưới đây thực hiện quét Xmas bằng nmap?**

A. nmap -sA 192.168.1.254

B. nmap -sX 192.168.1.254

C. nmap -sV 192.168.1.254

D. nmap -sO 192.168.1.254

**Đáp án: B**

**Câu 9. Trong phân hệ Surface Web của hệ thống OpenMind có các thành phần nào?**

A. Web Pages, Search Engines, RSS

B. Web Pages, Search Engines, Deep Web - Social Networks

C. Search Engines, RSS, Surface Web

D. Các nguồn dữ liệu RSS và Web Pages

**Đáp án: A**

**Câu 10. Trong phân hệ Deep Web - Social Networks của hệ thống OpenMind có các thành phần nào?**

A. Facebook, Ahmia, Grams, Twitter, Vkontakte, Google, Youtube, Instagram

B. Facebook, Telegram, Tordex, Torch, Photos, Vkontakte, Google, Youtube, Instagram

C. Facebook, Telegram, Tumblr, Twitter, Vkontakte, Google, Youtube, Instagram

D. Facebook, Telegram, Tordex, Torch, Photos, Vkontakte, Google

**Đáp án: C**

**Câu 11. Trong phân hệ Dark Web của hệ thống OpenMind có các thành phần nào?**

A. Tordex, Torch, Twitter, Vkontakte, Engine, Haystack, Ahmia, Grams, Google.oniond, Not Evil

B. Tordex, Torch, Phobos, Onion Search Engine, Haystack, Ahmia, Grams, Google.oniond, Not Evil

C. Tordex, Telegram, Tordex, Haystack, Ahmia, Grams, Google.oniond, Not Evil

D. Tordex, Torch, Phobos, Onion Search Engine, Haystack, Ahmia, Grams, Google.oniond, Not Evil

**Đáp án: B**

**Câu 12. Trong hệ thống Maltego khái niệm Transform được định nghĩa như thế nào?**

A. Transform là đối tượng, là một ai đó hoặc cái gì đó, ví dụ như 1 DNS server, 1 tên người cụ thể, 1 công ty hay 1 website…

B. Transform là một đoạn mã để có thể tìm kiếm mối liên hệ giữa một thực thể này với một hoặc nhiều thực thể khác

C. Transform là kết nối giữa các thực thể, thể hiện kết nối logic giữa các thực thể với nhau

D. Transform một tập các đoạn mã được liên kết với nhau để tự động thực hiện các tác vụ lặp lại

**Đáp án: B**

**Câu 13. Trong hệ thống Maltego, dữ liệu đưa vào Entity nào sau đây đúng?**

A. Dark Web, Tên công ty, Websites, Tài khoản mạng xã hội, Domains, DNS Names

B. Tên công ty, Websites, Tài khoản mạng xã hội, Domains, DNS Names, Dark Web

C. Tên, Số điện thoại, Địa chỉ email, Tên công ty, Website, Tài khoản mạng xã hội, Domain, DNS Name

D. Tên, Số điện thoại, Địa chỉ email, Tên công ty, Dark Web, DNS Names

**Đáp án: C**

**Câu 14. Câu lệnh Nmap nào sau đây sử dụng để quét cổng 80 trên địa chỉ IP 192.168.0.1 sử dụng kết nối TCP?**

A. nmap –sU –p 80 192.168.0.1

B. nmap –sT –p 80 192.168.0.1

C. nmap –sS –p 80 192.168.0.1

D. nmap -sX -p 80 192.168.0.1

**Đáp án: B**

**Câu 15. Trong hệ thống giám sát Nagios, giao thức nào thường được sử dụng để client gửi yêu cầu lấy thông tin từ Nagios Server.**

A. HTTP

B. FTP

C. SMTP

D. SSH

**Đáp án: A**

**Câu 17. Nagios điều khiển plugin cục bộ trên client qua secure shell ssh bằng gì?**

A. Check\_by\_ssh plugin

B. Check\_nrpe plugin

C. Check\_hpjd plugin

D. Không có

**Đáp án: A**

**Câu 18. Hệ thống giám sát tấn công thay đổi giao diện sử dụng thư viện gì để xây dựng bot**

A. Puppeteer

B. Selenium

C. Scaypy

D. ReactJs

**Đáp án: A**

**Câu 19. Dò quét mạng không thực hiện chức năng nào sau đây?**

A. Nhận dạng máy trạm (host) đang hoạt động

B. Nhận dạng cổng (port) đang đóng mở

C. Lọc các nội dung trên mạng.

D. Nhận dạng dịch vụ (services) đang hoạt động

**Đáp án: C**

**Câu 20. Trong hệ thống trinh sát mạng, tính năng nào giúp phát hiện và ngăn chặn các hoạt động độc hại trên mạng?**

A. Firewall

B. IDS/IPS

C. VPN

D. Honeypot

**Đáp án: B**

**Câu 21. Cấu tạo của một hệ thống phòng thủ mạng bao gồm các thành phần nào sau đây?**

A. Firewall, Antivirus, VPN

B. IDS/IPS, Proxy Server, Honeypot

C. Router, Switch, Server

D. Backup Server, Load Balancer, DNS Server

**Đáp án: B**

**Câu 22. Tính năng kỹ thuật nào giúp hệ thống phòng thủ mạng phân tích và xác định các mối đe dọa mạng?**

A. Log Analysis

B. Packet Filtering

C. Intrusion Detection

D. Encryption

**Đáp án đúng: C**

**Câu hỏi 23. Trong hệ thống tấn công mạng, công cụ nào thường được sử dụng để giả mạo thông tin và xâm nhập vào hệ thống mục tiêu?**

A. Firewall

B. VPN

C. Honeypot

D. IDS/IPS

**Đáp án đúng: C**

**Câu 24. Đâu là hệ thống thu thập và phân tích log?**

A. NextAV

B. HP Arcsight

C. PRTG

D. NAC

**Đáp án: B**

**Câu 25. Công cụ nào phổ biến nhất để kiểm thử bảo mật web?**

A. Wireshark

B. Burp Suite

C. Nmap

D. Metasploit

**Đáp án: B**

**Câu 26. Hệ thống nào sau đây là hệ thống giám sát mạng?**

A. FMC/FMS

B. Qradar

C. Avalanche

D. Splunk

**Đáp án: B**

**Câu 27. Công cụ nào sau đây sử dụng để quét port và IP một cách nhanh chóng?**

A. Cain and Abel

B. Angry IP Scanner

C. Snort

D. Ettercap

**Đáp án: B**

**Câu 28. Công cụ nào thường được sử dụng trong Wi-Fi-hacking?**

A. Aircrack-ng

B. Wireshark

C. Norton

D. Ettercap

**Đáp án: A**

**Câu 29. Có bao nhiêu loại báo cáo trên Acunetix ?**

A. 3

B. 4

C. 5

D. 6

**Đáp án: B**

**Câu 30. Ưu điểm nào sau đây nổi bật nhất của công cụ Acunetix Web Vulnerability Scanner?**

A. Giao diện trực quan, dễ sử dụng

B. Tích hợp lượng lớn mẫu tấn công và lỗ hổng

C. Có khả năng ghi lại lịch sử và kết quả quét

D. Tự động cập nhật lỗ hổng theo cơ sở dữ liệu CVE

**Đáp án: B**

**Câu 31. Những nhược điểm của Acunetix Web Vulnerability Scanner là gì?**

A. Mã nguồn mở, dễ bị tấn công

B. Miễn phí, ít tính năng chuyên sâu

C. Ngốn tài nguyên và không miễn phí

D. Không tương thích với hệ điều hành Windows

**Đáp án: C**

**Câu 32. Công cụ nào sau đây có dùng để phá mã/giải mã**

A. Acunetix

B. Nessus

C. Hashcat

D. Metasploit

**Đáp án: C**

**Câu 33. Công cụ nào không được sử dụng để dò quét Website**

A. Acunetix, Nessus

B. Netsparker

C. Burpsuite Pro

D. Wireshark

**Đáp án: D**

**Câu 34. Tham số -O trong Nmap có ý nghĩa gì?**

A. Thực thi tất cả các script trong Nmap để dò quét hệ thống mục tiêu

B. Thu thập thông tin về các phiên bản “version” trên hệ thống mục tiêu

C. Thu thập thông tin về hệ điều hành mục tiêu

D. Không thực hiện ping đến mục tiêu dò quét

**Đáp án: C**

**Câu 35. Thời gian -T mặc định Nmap là ?**

A. T1

B. T2

C. T3

D. T4

**Đáp án: C**

**Câu 36. Sử dụng tùy chọn Nmap nào nếu không lo lắng về việc bị phát hiện và muốn thực hiện quét rất nhanh?**

A. -T0

B. -T5

C. –A

D. -T2

**Đáp án: B**

**Câu 37. Tùy chọn nào trong Nmap để xuất kết quả ra định dạnh file bất kì?**

A. -oN

B. -oX

C. –oG

D. -O

**Đáp án: A**

**Câu 38. Tham số thay thế các tùy chọn (-sV, O) của Nmap?**

A. -A

B. -Pn

C. -p

D. –T

**Đáp án: A**

**Câu 39. Câu lệnh khởi động công cụ Metasploit trên công cụ Kali Linux là gì?**

A. msfconsole

B. ping

C. ipconfig

D. msfdb -init

**Đáp án: A**

**Câu 40. Câu lệnh nào sử dụng để tìm kiếm các module liên quan đến mục tiêu trong metasploit?**

A. use

B. search

C. run

D. set

**Đáp án: B**

**Câu 41. Các khía cạnh không của thực thể trong Maltego là gì?**

A. Dạng thực thể

B. Giá trị của thực thể

C. Các thuộc tính

D. Các tên miền

**Đáp án: D**

**Câu 42. Hệ thống SIEM không hỗ trợ giám sát ở lớp bảo vệ nào?**

A. Lớp mạng (Network)

B. Lớp đầu cuối (Endpoint)

C. Lớp ứng dụng (Application)

D. Lớp vật lý (Physical)

**Đáp án: D**

**Câu 43. Hệ thống SIEM chủ yếu thu thập dữ liệu từ đâu?**

A. Thiết bị mạng (Firewall, Router)

B. Máy chủ và endpoint

C. Ứng dụng và dịch vụ đám mây

D. Thiết bị ngoại vi (USB, máy in)

**Đáp án: A**

### (6) CÓ KIẾN THỨC VỀ KỸ THUẬT GIẢ MẠO, ẨN DANH, XÓA DẤU VẾT TRONG THỰC HIỆN NHIỆM VỤ TÁC CHIẾN MẠNG (GỒM 23 CÂU HỎI)

**Câu 1. Công cụ nào sau đây đúng là một công cụ để thực hiện footprinting không bị phát hiện?**

A. Whois search

B. Traceroute

C. Ping sweep

D. Host scanning

D. Tin tặc nguy hiểm

**Đáp án: A**

**Câu 2. Sau khi có được tài khoản email của một người dùng trong mạng nội bộ, hacker có thể thực hiện tiếp công việc gì để mở rộng tấn công?**

A. Gửi thư đe dọa có gắn kèm đường dẫn độc hại.

B. Gửi thư giả mạo trong mạng nội bộ có gắn kèm đường dẫn độc hại

C. Đổi mật khẩu của người dùng và gửi thư đe dọa

D. Mã hóa tài khoản người dùng và gửi thư đe dọa có gắn kèm đường dẫn độc hại.

**Đáp án: B**

**Câu 3. Phương pháp nào sau đây không giúp duy trì kết nối lâu dài với hệ thống mục tiêu?**

A. Cài đặt mã độc backdoor

B. Tạo tài khoản quản trị mới trên hệ thống mục tiêu

C. Triển khai mã độc ransomware

D. Thay đổi cấu hình firewall để cho phép truy cập từ xa

**Đáp án: C**

**Câu 4. Kỹ thuật "MAC spoofing" được sử dụng để làm gì?**

A. Để vượt qua cơ chế kiểm soát truy cập theo MAC

B. Ghi lại mật khẩu trên máy nạn nhân

C. Mã hóa lưu lượng mạng để tránh bị phát hiện

D. Tăng tốc kết nối mạng

**Đáp án: A**

**Câu 5. Ẩn danh trong tác chiến mạng có tác dụng gì?**

A. Bảo vệ danh tính của người thực hiện nhiệm vụ

B. Tiết kiệm chi phí cho tổ chức

C. Tăng cường sự minh bạch trong quá trình thực hiện nhiệm vụ

D. Không có tác dụng gì

**Đáp án: A**

**Câu 6. Xóa dấu vết để làm gì?**

A. Giúp che giấu các hoạt động của người thực hiện nhiệm vụ

B. Tạo điều kiện cho việc kiểm tra và đánh giá sau này

C. Gây khó khăn cho việc quản lý và theo dõi nhiệm vụ

D. Làm giảm hiệu quả của quá trình thực hiện nhiệm vụ

**Đán án: A**

**Câu 7. Tại sao kỹ thuật giả mạo, ẩn danh và xóa dấu vết lại quan trọng trong tác chiến mạng?**

A. Giúp tăng cường bảo mật thông tin

B. Bảo vệ danh tính của cá nhân và tổ chức thực hiện nhiệm vụ

C. Tránh bị truy vết khi thực hiện các hoạt động cần giữ bí mật

D. Giúp nâng cao tốc độ kết nối mạng

**Đáp án: B**

**Câu 8. Chọn đáp án đúng về thực hiện ẩn danh trong thực hiện nhiệm vụ?**

A. Sử dụng bảo mật 2 lớp VPN và DCOM 4G

B. Dùng mạng cá nhân để thực hiện nhiệm vụ

C. Dùng mạng gia đình

D. Dùng mạng của đơn vị

**Đáp án: A**

**Câu 9. Một kiểu tấn công dùng địa chỉ giả mạo để đánh lừa hệ thống là gì?**

A. Sniffing

B. IP Spoofing

C. Keylogging

D. Backdoor

**Đáp án: B**

**Câu 10. Khi cố gắng xóa dấu vết hoạt động trên hệ thống, đâu là hành động không nên làm vì rất dễ bị phát hiện?**

A. Chỉnh sửa timestamp của file bằng công cụ forensics

B. Xóa toàn bộ file log bằng thao tác thủ công (xóa trực tiếp file log)

C. Sử dụng lệnh hệ thống có sẵn để xóa/sơ tán log theo quy trình đã mã hóa

D. Ghi đè dữ liệu log bằng công cụ chuyên dụng (overwrite)

**Đáp án: B**

**Câu 11. Kỹ thuật "Domain Generation Algorithm (DGA)" thường được các phần mềm độc hại (malware) sử dụng để duy trì tính ẩn danh và khả năng chống phát hiện (evasion) như thế nào?**

A. Bằng cách mã hóa toàn bộ lưu lượng C2 (Command and Control) bằng AES-256.

B. Bằng cách tự động tạo ra hàng loạt tên miền (domain names) mới mỗi ngày để liên lạc với máy chủ C2, khiến việc chặn dựa trên danh sách đen (blacklist) trở nên vô hiệu.

C. Bằng cách sử dụng địa chỉ IP tĩnh đã được mã hóa cứng trong mã nguồn mã độc.

D. Bằng cách sử dụng duy nhất một tên miền hợp pháp đã bị chiếm quyền kiểm soát.

**Đáp án: B**

**Câu 12. Trong phòng thủ mạng, "Tấn công Tương quan Lưu lượng" (Traffic Correlation Attack) là một phương pháp gỡ bỏ ẩn danh (de-anonymization) hiệu quả chống lại mạng lưới nào?**

A. Mạng nội bộ không kết nối Internet.

B. Mạng dùng VPN đơn giản.

C. Mạng Tor hoặc I2P.

D. Mạng dùng công nghệ Blockchain.

**Đáp án: C**

**Câu 13. Khi một kẻ tấn công sử dụng kỹ thuật "Living off the Land" (LotL) để tấn công, tính ẩn danh được duy trì như thế nào?**

A. Kẻ tấn công sử dụng các công cụ độc lập, khó nhận biết để tấn công nhanh, thực thi lệnh hiệu quả.

B. Kẻ tấn công lợi dụng các công cụ quản trị hệ thống hợp lệ để thực thi lệnh, hòa lẫn vào các hoạt động bình thường của hệ thống.

C. Kẻ tấn công sử dụng mã độc zero-day để tránh bị phát hiện.

D. Kẻ tấn công không sử dụng bất kỳ công cụ nào, chỉ dùng mạng xã hội.

**Đáp án: B**

**Câu 14. "Covert Channels" là kỹ thuật ẩn danh tinh vi được sử dụng trong tấn công để làm gì?**

A Để truyền dữ liệu hoặc lệnh điều khiển thông qua các kênh giao tiếp không mong đợi hoặc không được kiểm soát tạo ra các kết nối mạng nhanh hơn kết nối bình thường.

B. Để truyền dữ liệu hoặc lệnh điều khiển thông qua các kênh giao tiếp không mong đợi hoặc không được kiểm soát để vượt qua tường lửa.

C. Để truyền dữ liệu hoặc lệnh điều khiển thông qua các kênh giao tiếp không mong đợi hoặc không được kiểm soát từ VPN.

D. Để truyền dữ liệu hoặc lệnh điều khiển thông qua các kênh giao tiếp không mong đợi hoặc không được kiểm soát và mã hóa tệp tin bằng thuật toán RSA.

**Đáp án: B**

**Câu 15. Trong bối cảnh phòng thủ mạng, việc sử dụng "honeypots" (hệ thống bẫy) động có thể giúp chống lại các hoạt động ẩn danh của kẻ tấn công bằng cách nào?**

A. Honeypots cung cấp một môi trường được kiểm soát để thu hút, giam chân và phân tích hành vi của kẻ tấn công, giúp tự động tấn công ngược lại kẻ tấn công để lộ IP thật của họ.

B. Honeypots cung cấp một môi trường được kiểm soát để thu hút, giam chân và phân tích hành vi của kẻ tấn công, giúp gỡ bỏ lớp ẩn danh và hiểu rõ chiến thuật của họ.

C. Honeypots cung cấp một môi trường được kiểm soát để thu hút, giam chân và phân tích hành vi của kẻ tấn công, giúp tự động vá các lỗ hổng bảo mật.

D. Honeypots cung cấp một môi trường được kiểm soát để thu hút, giam chân và phân tích hành vi của kẻ tấn công, đóng vai trò như một VPN.

**Đáp án: B**

**Câu 16. Một thách thức lớn trong việc gỡ bỏ ẩn danh các tác nhân đe dọa (threat actors) là việc họ sử dụng kết hợp nhiều kỹ thuật (multi-layer obfuscation). Điều này đề cập đến việc gì?**

A. Kẻ tấn công chỉ sử dụng nhiều mã hóa khác nhau.

B. Kẻ tấn công sử dụng nhiều lớp bảo vệ.

C. Kẻ tấn công sử dụng nhiều mật khẩu khác nhau.

D. Kẻ tấn công sử dụng nhiều loại ngôn ngữ lập trình khác nhau.

**Đáp án: B**

**Câu 17. Kỹ thuật "DNS tunneling" là một phương pháp ẩn danh tinh vi vì nó cho phép kẻ tấn công làm gì?**

A. Truyền toàn bộ lưu lượng tấn công (tấn công trực tiếp vào máy chủ DNS) thông qua các truy vấn và phản hồi DNS, loại lưu lượng mạng thường ít bị giám sát chặt chẽ bởi tường lửa.

B. Truyền toàn bộ lưu lượng tấn công (lệnh C2 và dữ liệu bị đánh cắp) thông qua các truy vấn và phản hồi DNS, loại lưu lượng mạng thường ít bị giám sát chặt chẽ bởi tường lửa.

C. Truyền toàn bộ lưu lượng tấn công (thay đổi địa chỉ IP của máy chủ DNS) thông qua các truy vấn và phản hồi DNS, loại lưu lượng mạng thường ít bị giám sát chặt chẽ bởi tường lửa.

D. Truyền toàn bộ lưu lượng tấn công (lệnh C2 và dữ liệu bị đánh cắp) thông qua các truy vấn và phản hồi DNS, loại lưu lượng mạng thường xuyên bị giám sát chặt chẽ bởi tường lửa.

**Đáp án: B**

**Câu 18. Tại sao việc sử dụng máy ảo (Virtual Machines - VM) hoặc hệ điều hành chuyên biệt như Tails OS lại là kỹ thuật ẩn danh hiệu quả cho kẻ tấn công?**

A. Vì chúng giúp đảm bảo rằng không có dấu vết mã độc nào còn sót lại trên máy chủ sau khi phiên làm việc kết thúc.

B. Vì chúng giúp đảm bảo rằng không có dấu vết hoạt động hợp pháp nào còn sót lại trên máy chủ thực sau khi phiên làm việc kết thúc.

C. Vì chúng giúp đảm bảo rằng không có dấu vết hoạt động độc hại nào còn sót lại trên máy chủ thực sau khi phiên làm việc kết thúc.

D. Vì chúng giúp đảm bảo rằng không có dấu vết hoạt động độc hại nào còn sót lại trên máy chủ ảo sau khi phiên làm việc kết thúc.

**Đáp án: C**

**Câu 19. Trong phòng thủ mạng, việc sử dụng các hệ thống "Network Traffic Analysis (NTA)" tiên tiến dựa trên AI nhằm mục đích chính nào liên quan đến ẩn danh?**

A. Để tự động chặn tất cả lưu lượng mạng ngay lập tức, tìm ra các hoạt động bất thường hoặc sử dụng kênh ẩn (covert channel) mà các hệ thống truyền thống bỏ qua, ngay cả khi kẻ tấn công đã che giấu IP nguồn.

B. Để phân tích các mẫu lưu lượng mạng phức tạp, tìm ra các hoạt động bất thường hoặc sử dụng kênh ẩn (covert channel) mà các hệ thống truyền thống bỏ qua, ngay cả khi kẻ tấn công đã che giấu IP nguồn.

C. Để mã hóa tất cả lưu lượng mạng nội bộ, tìm ra các hoạt động bất thường hoặc sử dụng kênh ẩn (covert channel) mà các hệ thống truyền thống bỏ qua, ngay cả khi kẻ tấn công đã che giấu IP nguồn.

D. Để mã hóa tất cả lưu lượng mạng nội bộ, tìm ra các hoạt động bất thường hoặc sử dụng kênh ẩn (covert channel) mà các hệ thống truyền thống bỏ qua, tạo báo cáo tuân thủ pháp luật tự động.

**Đáp án: B**

**Câu 20. Tấn công Pharming là một dạng tấn công giả mạo tinh vi hơn Phishing ở điểm nào?**

A. Nó sử dụng email lừa đảo chuyên nghiệp hơn.

B. Nó không yêu cầu người dùng tự nguyện truy cập vào trang web giả mạo mà tự động chuyển hướng họ.

C. Nó yêu cầu người dùng tự nguyện truy cập vào trang web giả mạo mà không tự động chuyển hướng họ.

D. Nó không yêu cầu người dùng tự nguyện truy cập vào trang web giả mạo mà không tự động chuyển hướng họ..

**Đáp án: B**

**Câu 21. Khái niệm "Operational Security" (OpSec) là cực kỳ quan trọng đối với việc ẩn danh của kẻ tấn công vì nó tập trung vào điều gì?**

A. Chỉ vào việc sử dụng công nghệ mã hóa mạnh để che giấu các thói quen, quy trình và hành vi của kẻ tấn công có thể vô tình làm lộ danh tính hoặc mục tiêu của họ.

B. Vào việc bảo vệ thông tin nhạy cảm thông qua việc che giấu các thói quen, quy trình và hành vi của kẻ tấn công có thể vô tình làm lộ danh tính hoặc mục tiêu của họ.

C. Vào việc đảm bảo che giấu các thói quen, quy trình và hành vi của kẻ tấn công có thể vô tình làm lộ danh tính hoặc mục tiêu của họ.

D. Vào việc chỉ sử dụng máy tính vào 1 thời điểm nhất định để che giấu các thói quen, quy trình và hành vi của kẻ tấn công có thể vô tình làm lộ danh tính hoặc mục tiêu của họ..

**Đáp án: B**

**Câu 22. Phương pháp phòng thủ "Traffic shaping" (Điều chỉnh lưu lượng mạng) có thể được sử dụng để chống lại các cuộc tấn công DDoS ẩn danh bằng cách nào?**

A. Bằng cách cho phép tất cả lưu lượng truy cập giới hạn trong 1 khoảng thời gian nhất định, làm giảm tác động của cuộc tấn công lên dịch vụ.

B. Bằng cách ưu tiên lưu lượng hợp pháp và giới hạn hoặc định hình lại lưu lượng bất thường hoặc từ các nguồn đáng ngờ, làm giảm tác động của cuộc tấn công lên dịch vụ.

C. Bằng cách sử dụng công nghệ để đoán mật khẩu của kẻ tấn công, làm giảm tác động của cuộc tấn công lên dịch vụ.

D. Bằng cách tắt chức năng định tuyến của bộ định tuyến, làm giảm tác động của cuộc tấn công lên dịch vụ.

**Đáp án: B**

**Câu 23. "Tấn công Side-Channel" (Tấn công kênh bên) có thể được sử dụng để gỡ bỏ ẩn danh hệ thống mã hóa bằng cách nào?**

A. Bằng cách tấn công trực tiếp vào thuật toán mã hóa để suy ra khóa mã bí mật.

B. Bằng cách đo lường các đặc điểm vật lý của máy tính thực hiện mã hóa để suy ra khóa mã bí mật.

C. Bằng cách sử dụng phương pháp vét cạn mật khẩu để suy ra khóa mã bí mật.

D. Bằng cách gửi email lừa đảo yêu cầu cung cấp khóa bí mật.

**Đáp án: B**

### (7) HIỂU VÀ THỰC HIỆN ĐƯỢC CÁC QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN KHI THỰC HIỆN NHIỆM VỤ THỰC TẾ (GỒM 20 CÂU HỎI)

**Câu 1. Tại sao không nên sử dụng email cá nhân để làm việc trong môi trường tổ chức?**

A. Vì email cá nhân không được kiểm soát và bảo mật nghiêm ngặt như email công việc

B. Email cá nhân có thể bị mất hoặc bị truy cập trái phép, gây rò rỉ thông tin

C. Gây khó khăn trong quản lý và truy vết các hoạt động công việc

D. Email cá nhân thường có dung lượng thấp hơn email công việc

**Đáp án: A**

**Câu 2. Những rủi ro bảo mật nào có thể xảy ra khi dùng email cá nhân cho công việc?**

A. Mất dữ liệu quan trọng do mất quyền kiểm soát email

B. Tấn công phishing hoặc malware dễ dàng hơn do bảo mật yếu

C. Rò rỉ thông tin nội bộ và vi phạm chính sách bảo mật của tổ chức

D. Email cá nhân có thể bị spam rất nhiều

**Đáp án: B**

**Câu 3. Làm thế nào để tổ chức quản lý việc cấp email công việc cho nhân viên mới?**

A. Cấp email công việc theo chuẩn chung của tổ chức, có quy trình xác thực

B. Cho phép nhân viên tự tạo email cá nhân để sử dụng

C. Không cấp email cho nhân viên mới

D. Giao cho nhân viên tự đăng ký email miễn phí trên mạng

**Đáp án: A**

**Câu 4. Chính sách sử dụng email trong tổ chức thường quy định những gì?**

A. Các quy tắc bảo mật khi sử dụng email công việc

B. Cấm sử dụng email cho mục đích cá nhân hoặc không hợp pháp

C. Quy trình lưu trữ và xóa email đúng quy định

D. Tự do gửi mail đến bất cứ đâu mà không cần kiểm soát

**Đáp án: A**

**Câu 5. Việc sử dụng email công việc giúp bảo vệ dữ liệu tổ chức như thế nào?**

A. Tăng khả năng kiểm soát và bảo mật thông tin

B. Giúp dễ dàng truy vết và kiểm tra khi có sự cố

C. Hạn chế việc rò rỉ dữ liệu ra ngoài tổ chức

D. Không có lợi ích gìvề bảo mật

**Đáp án: A**

**Câu 6. Khi không sử dụng một tài khoản email công việc nên được xử lý ra sao?**

A. Ngay lập tức khóa hoặc xóa tài khoản để tránh truy cập trái phép

B. Chuyển tiếp email quan trọng cho quản lý hoặc nhân viên thay thế

C. Lưu trữ dữ liệu theo chính sách lưu trữ của tổ chức

D. Không làm gìvà để nhân viên giữ tài khoản đó

**Đáp án: A**

**Câu 7. Các biện pháp nào nên áp dụng để bảo vệ tài khoản email công việc tránh bị xâm nhập?**

A. Sử dụng mật khẩu mạnh và thay đổi định kỳ

B. Kích hoạt xác thực hai yếu tố (2FA)

C. Cảnh báo khi có hoạt động đăng nhập bất thường

D. Chia sẻ mật khẩu với người khác để đề phòng mất tài khoản

**Đáp án: A**

**Câu 8. Làm sao để nhân viên phân biệt được email cá nhân và email công việc trong việc xử lý thông tin nhạy cảm?**

A. Sử dụng các email với tên miền riêng của tổ chức cho công việc

B. Cung cấp đào tạo về bảo mật và chính sách sử dụng email

C. Thường xuyên nhắc nhở và kiểm tra việc tuân thủ chính sách

D. Không cần phân biệt, có thể dùng chung email cá nhân và email công việc

**Đáp án: A**

**Câu 9. Đâu là một trong những hành vi vi phạm pháp luật trên không gian mạng ?**

A. Spam trên mạng xã hội, thư điện tử

B. Đăng tải tin tức chính thống

C. Đăng tải video nội dung giải trí

D. Đăng tải ảnh chụp phong cảnh

**Đáp án: A**

**Câu 10. Cái nào sau đây là chính sách của người gửi email được chấp thuận?**

A. Whitelist

B. Blacklist

C. Greylist

D. Greenlist

**Đáp án: A**

**Câu 11. Quy định bảo đảm an toàn thông tin trong nhiệm vụ thực tế áp dụng cho ai?**

A. Chỉ áp dụng cho người thực hiện nhiệm vụ

B. Áp dụng cho tất cả các bên liên quan đến nhiệm vụ

C. Chỉ áp dụng cho các nhà quản lý

D. Không có quy định cụ thể

**Đáp án: B**

**Câu 12. Tại sao việc tuân thủ quy định bảo đảm an toàn thông tin trong nhiệm vụ thực tế là cần thiết?**

A. Để tránh rủi ro an ninh mạng

B. Để bảo vệ thông tin và dữ liệu quan trọng

C. Để tăng cường sự tin cậy và hiệu quả của nhiệm vụ

D. Để giảm thiểu chi phí vận hành

**Đáp án: B**

**Câu 13. Quy định bảo đảm an toàn thông tin khi thực hiện nhiệm vụ thực tế có mục đích gì?**

A. Bảo vệ thông tin quan trọng

B. Đảm bảo an toàn cho người thực hiện nhiệm vụ

C. Ngăn chặn và phát hiện các cuộc tấn công mạng

D. Hỗ trợ phát triển phần mềm

**Đáp án: A**

**Câu 14. Tuân thủ các quy định bảo mật an toàn thông tin có tác dụng gì?**

A. Để tăng hiệu quả làm việc

B. Để bảo vệ thông tin và dữ liệu quan trọng

C. Để nâng cao trình độ cán bộ

D. Để giảm chi phí

**Đáp án: B**

**Câu 15. Hành vi nào sau đây được coi là vi phạm pháp luật trên không gian mạng?**

A. Chiếm đoạt tài khoản mạng xã hội

B. Đăng tải các thông tin độc hại vi phạm an ninh quốc gia, trật tự an toàn xã hội

C. Đăng tải tin giả

D. Sử dụng phần mềm bản quyền hợp pháp

**Đáp án: B**

**Câu 16. Hành vi nào dưới đây bị nghiêm cấm trên không gian mạng?**

A. Xuyên tạc lịch sử, phủ nhận thành quả cách mạng.

B. Đăng tải các hình ảnh cá nhân lên mạng xã hội.

C. Tra cứu, tìm kiếm thông tin, tư liệu trên Internet.

D. Tương tác với người thân qua mạng xã hội.

**Đáp án: A**

**Câu 17. Hành vi nào dưới đây không bị cấm thực hiện trên không gian mạng?**

A. Chiếm đoạt tài sản, tổ chức đáng bạc qua mạng Internet.

B. Tra cứu, tìm kiếm thông tin, tư liệu trên Internet.

C. Bịa đặt thông tin sai sự thật gây hoang mang dư luận.

D. Xuyên tạc lịch sử, phủ nhận thành quả cách mạng.

**Đáp án: B**

**Câu 18. Phương pháp điều khiển truy cập có hiệu quả và an toàn nhất đối với mạng không dây là:**

A. Mã hóa WEP 40 bit

B. VPN

C. Nhận dạng bảo mật mạng

D. Mã hóa WEP 128 bit

**Đáp án: C**

**Câu 19. Cơ cấu bảo mật nào sau đây được sử dụng với chuẩn không dây WAP?**

A. WTLS

B. SSL

C. HTTPS

D. Mã hóa WEP

**Đáp án: A**

**Câu 20. Kỹ thuật nào bảo đảm tính toàn vẹn trong an toàn thông tin?**

A. hashing

B. encryption

C. UPS

D. Passwords

**Đáp án: A**

### (8) CÓ KIẾN THỨC VỀ LỖ HỔNG BẢO MẬT, KỸ THUẬT TRINH SÁT TẤN CÔNG MẠNG; CÁC LỖ HỔNG PHỔ BIẾN CỦA CÁC THÀNH PHẦN TRONG HỆ THỐNG MẠNG (GỒM 23 CÂU HỎI)

**Câu 1. Lỗ hổng SQL Injection cho phép tin tặc có thể thực hiện chạy cách lệnh của hệ điều hành Microsoft Windows từ cổng 80/443 của ứng dụng web. Chức năng nào trong cơ sở dữ liệu MSSQL cho phép tin tặc có thể thực hiện chức năng này?**

A. command\_injector

B. sql\_shell

C. xp\_cmdshell

D. stored procedure

**Đáp án: C**

**Câu 2. Khi một hacker thực hiện dò quét mạng để tìm thiết bị còn lỗ hổng bảo mật, giai đoạn này gọi là?**

A. Trinh sát (Reconnaissance)

B. Gaining Access

C. Covering Tracks

D. Maintaining Access

**Đáp án: A**

**Câu 3. Lỗ hổng bảo mật "SQL Injection" xảy ra khi nào?**

A. Khi hacker khai thác lỗi trong mã JavaScript

B. Khi dữ liệu đầu vào không được kiểm tra và được thực thi trong câu lệnh SQL

C. Khi hệ thống bị quá tải

D. Khi tường lửa bị tắt

**Đáp án: B**

**Câu 4. Hình thức nào sau đây không phải là hình thức tấn công DoS?**

A. Teardrop

B. SYN attack

C. Smurf

D. SQLi

**Đáp án: D**

**Câu 5. Cú pháp tìm kiếm google dork nào sau đây giúp Google giới hạn kết quả tìm kiếm về những trang có chứa từ trong tiêu đề?**

A. inurl:

B. intitle:

C. site:

D. link:

**Đáp án: B**

**Câu 6. Kỹ thuật tấn công khả năng làm chậm hoặc dừng dịch vụ trên Web là?**

A. Chiếm hữu phiên làm việc

B. Tràn bộ đệm

C. Từ chối dịch vụ (DoS)

D. Chèn câu truy vấn SQL

**Đáp án: C**

**Câu 7. Công cụ nào sau đây thu thập thông tin tổng quan về mục tiêu.**

A. Netcraft

B. Pentest-tools

C. Dnsdumster.com

D. Shodan

**Đáp án: A**

**Câu 8. Công cụ nào sau đây sử dụng để khai thác lỗ hổng bảo mật?**

A. Breking Point

B. Acunetix

C. Nmap

D. Metasploit Framework

**Đáp án: D**

**Câu 9. Lỗ hổng bảo mật nào có thể gây lộ lọt thông tin cơ sở dữ liệu ứng dụng web.**

A. SQLi

B. XSS

C. CSRF

D. RFI

**Đáp án: A**

**Câu 10. Công cụ nào có thể sử dụng để dò quét phát hiện lỗ hổng CVE-2017-0143?**

A. Acunetix

B. Sqlmap

C. Nmap

D. Metasploit

**Đáp án: C**

**Câu 11. Trinh sát thông tin website đối tượng không sử dụng công cụ?**

A. Burp Suite

B. ZAP

C. Web Spider, Web Mirroring

D. FB, Tweetter, Linkedin

**Đáp án: D**

**Câu 12. Lỗ hổng A1 trong Top 10 lỗ hổng OWASP năm 2025 là gì?**

A. Injection

B. Broken Access Control

C. Cross-Site Scripting (XSS)

D. Insecure Direct Object References

**Đáp án: B**

**Câu 13. Lỗ hổng A2 trong Top 10 lỗ hổng OWASP năm 2025 là gì?**

A. Injection

B. Security Misconfiguration.

C. Cross-Site Scripting (XSS)

D. Insecure Direct Object References

**Đáp án: B**

**Câu 14. Lỗ hổng A3 trong Top 10 lỗ hổng OWASP năm 2025 là gì?**

A. Software Supply Chain Failures

B. Broken Authentication and Session Management

C. Cross-Site Scripting (XSS)

D. Insecure Direct Object References

**Đáp án: A**

**Câu 15. Lỗ hổng A4 trong Top 10 lỗ hổng lỗ hổng OWASP năm 2025 là gì?**

A. Injection

B. Broken Authentication and Session Management

C. Cross-Site Scripting (XSS)

D. Cryptographic Failures

**Đáp án: D**

**Câu 16. Lỗ hổng A5 trong Top 10 lỗ hổng lỗ hổng OWASP năm 2025 là gì?**

A. Injection

B. Broken Authentication and Session Management

C. Cross-Site Scripting (XSS)

D. Security Misconfiguration

**Đáp án: A**

**Câu 17. Lỗ hổng A6 trong Top 10 lỗ hổng lỗ hổng OWASP năm 2025 là gì?**

A. Insecure Design

B. Broken Authentication and Session Management

C. Cross-Site Scripting (XSS)

D. Vulnerable and Outdated Components

**Đáp án: A**

**Câu 18. Lỗ hổng A7 trong Top 10 lỗ hổng lỗ hổng OWASP năm 2025 là gì?**

A. Identification and Data Integrity Failures

B. Broken Authentication and Session Management

C. Cross-Site Scripting (XSS)

D. Authentication Failures

**Đáp án: A**

**Câu 19. Lỗ hổng A8 trong Top 10 lỗ hổng lỗ hổng OWASP năm 2025 là gì?**

A. Software and Data Integrity Failures

B. Broken Authentication and Session Management

C. Cross-Site Scripting (XSS)

D. Sensitive Data Exposure

**Đáp án: A**

**Câu 20. Lỗ hổng A9 trong Top 10 lỗ hổng lỗ hổng OWASP năm 2025 là gì?**

A. Cross-Site Request Forgery (CSRF)

B. Logging and Alerting Failures

C. Cross-Site Scripting (XSS)

D. Sensitive Data Exposur

**Đáp án: B**

**Câu 21. Lỗ hổng A10 trong Top 10 lỗ hổng lỗ hổng OWASP năm 2025 là gì?**

A. Cross-Site Request Forgery (CSRF)

B. Server-Side Request Forgery

C. Mishandling of Exceptional Conditions.

D. Sensitive Data Exposure

**Đáp án: C**

**Câu 22. Lỗ hổng Unicode Overflow là gì**

A. Là một lỗ hổng bảo mật cũ, sử dụng các bộ nhớ được stack chỉ tồn tại trong runtime. Lỗ hổng này thường xuất hiện ở trong C hoặc C++, vì người dùng có thể tự do sử dụng con trỏ ở trong các ứng dụng này

B. Xảy ra khi một phần bộ nhớ được gán cho heap, và dữ liệu được ghi vào bộ nhớ đó mà không cần kiểm tra. Việc này sẽ tạo ra một số cấu trúc dữ liệu quan trọng ở trong heap, chẳng hạn như heap header.

C. Là một lỗi tràn số học, xảy ra khi kết quả của một phép toán số nguyên không nằm trong giới hạn bộ nhớ.

D. Là việc cung cấp các ký tự Unicode vào input của ASCII sẽ vượt qua giới hạn tối đa của ASCII, từ đó làm tràn buffer.

**Đáp án: D**

**Câu 23. Các kỹ thuật tìm kiếm lỗ hổng là gì?**

A. Kỹ thuật lẩn tránh bộ lọc, Sử dụng web proxy, Kỹ thuật vượt bộ lọc XSS, Kỹ thuật khai thác lỗi ở client-side.

B. Sử dụng web proxy, Kỹ thuật vượt bộ lọc XSS, Kỹ thuật khai thác lỗi ở client-side.

C. Kỹ thuật vượt bộ lọc XSS, Kỹ thuật khai thác lỗi ở client-side

D. Gửi truy vấn hợp lệ đến máy chủ để xác thực

**Đáp án: A**

### (9) HIỂU VỀ QUY TRÌNH TRINH SÁT, KIỂM THỬ, KHAI THÁC LỖ HỔNG BẢO MẬT (GỒM 20 CÂU HỎI)

**Câu 1. Câu lệnh nào dưới đây thực hiện quét Xmas bằng nmap**

A. nmap -sA 192.168.1.254

B. nmap -sX 192.168.1.254

C. nmap -sV 192.168.1.254

D. nmap -sO 192.168.1.254

**Đáp án: B**

**Câu 2. Câu lệnh Nmap nào sau đây sử dụng để quét cổng 80 trên địa chỉ IP 192.168.0.1 sử dụng kết nối TCP?**

A. nmap –sU –p 80 192.168.0.1

B. nmap –sT –p 80 192.168.0.1

C. nmap –sS –p 80 192.168.0.1

D. nmap -sX -p 80 192.168.0.1

**Đáp án: B**

**Câu 3. Câu lệnh nmap nào sau đây sử dụng để quét cổng 80 trên địa chỉ IP 192.168.1.1 sử dụng giao thức UDP?**

A. nmap –sS –p 80 192.168.1.1

B. nmap –sU –p 80 192.168.1.1

C. nmap –sT –p 80 192.168.1.1

D. nmap -sX -p 80 192.168.1.1

**Đáp án: B**

**Câu 4. Câu lệnh nmap nào sau đây sử dụng để quét cổng 80 trên địa chỉ IP 192.168.1.1 sử dụng SYN Scan?**

A. nmap –sT –p 80 192.168.1.1

B. nmap –sU –p 80 192.168.1.1

C. nmap –sS –p 80 192.168.1.1

D. nmap -sX -p 80 192.168.1.1

**Đáp án: C**

**Câu 5. Trinh sát thu thập thông tin về chủ sở hữu, nhà cung cấp sử dụng công cụ nào sau đây?**

A. Nmap

B. Whois và ARIN Lookups

C. Website Informer

D. Nslookup

**Đáp án: B**

**Câu 6. Response code nào trả về khi người dùng truy cập thành công vào trang web?**

A. 100-199

B. 200-299

C. 300-399

D. 400-499

**Đáp án: B**

**Câu 7. Lệnh python nào dưới đây dùng để triển khai server nội bộ?**

A. python3 -a https.server 9000

B. python3 -m http.server 9000

C. python3 -m https.server 9000

D. python3 -a http.server 9000

**Đáp án: B**

**Câu 8. File cấu hình nào trên webserver sử dụng để quy định cho phép hoặc chặn truy cập của người dùng vào các trang?**

A. robots.txt

B. web.config

C. host.txt

D. index.html

**Đáp án: A**

**Câu 9. Ping sử dụng giao thức nào?**

A. ICMP

B. TCP

C. UDP

D. FTP

**Đáp án: A**

**Câu 10. Trong giai đoạn trinh sát (reconnaissance), mục tiêu chính của pentester là gì?**

A. Khai thác trực tiếp lỗ hổng bảo mật

B. Thu thập càng nhiều thông tin về hệ thống mục tiêu để phục vụ các giai đoạn tấn công tiếp theo

C. Thực hiện quét port toàn mạng và chiếm quyền quản trị

D. Cài mã độc để duy trì truy cập lâu dài

**Đáp án: B**

**Câu 11. Kỹ thuật tấn công SQL Injection như thế nào?**

A. Tin tặc lợi dụng lỗ hổng việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ thống CSDL để chèn vào các đoạn truy vấn độc hại nhằm truy cập trái phép và lấy thông tin từ CSDL của người dùng.

B. Tin tặc lợi dụng lỗ hỏng của việc kiểm tra website để chèn vào các đoạn truy vấn độc hại nhằm truy cập trái phép và lấy thông tin từ CSDL của người dùng.

C. Tin tặc khai thác lỗi đầu vào không được kiểm soát đúng cách trong ứng dụng web để thực hiện truy vấn SQL độc hại nhằm truy cập trái phép và lấy thông tin từ CSDL của người dùng.

D. Là kỹ thuật tấn công nhằm truy cập và thao túng dữ liệu trong hệ quản trị cơ sở dữ liệu thông qua lỗ hổng bảo mật trong ứng dụng web để chèn vào các đoạn truy vấn độc hại nhằm truy cập trái phép và lấy thông tin từ CSDL của người dùng.

**Đáp án: A**

**Câu 12. Đâu không phải là biện pháp phòng chống SQL Injection.**

A. Sử dụng câu lệnh SQL động mà không kiểm tra đầu vào

B. Sử dụng Prepared Statements (câu lệnh đã chuẩn bị trước)

C. Kiểm tra và lọc dữ liệu đầu vào

D. Giới hạn quyền truy cập CSDL cho tài khoản ứng dụng

**Đáp án: A**

**Câu 13. XSS là viết tắt của cụm từ nào?**

A. Cross-Site Scripting

B. Cross-Script Siting

C. Cross-Site Sitting

D. Cross-Site Signing

**Đáp án: A**

**Câu 14. Những tác động nào sau đây thường gặp khi bị tấn công XSS?**

A. Đánh cắp phiên của người dùng

B. Đánh cắp dữ liệu nhạy cảm

C. Thay đổi giao diện trang web

D. Làm chậm hiệu suất trang web

**Đáp án: A**

**Câu 15. Trong quy trình kiểm thử bảo mật (penetration testing), giai đoạn nào thường diễn ra sau khi khai thác lỗ hổng thành công?**

A. Reconnaissance (trinh sát)

B. Scanning (dò quét)

C. Post-Exploitation (hậu khai thác)

D. Reporting (báo cáo)

**Đáp án: C**

**Câu 16.** **Thu thập thông tin có những dạng nào?**

A. Thu thập thụ động và thu thập chủ động

B. Thu thập dữ liệu và phân tích dữ liệu

C. Quét mạng và khai thác lỗ hổng

D. Phân tích mã độc và phát hiện virus

**Đáp án: A**

**Câu 17. Scanning thuộc dạng nào trong quá trình thu thập thông tin?**

A. Thu thập thụ động

B. Thu thập chủ động

C. Phân tích dữ liệu

D. Giám sát mạng

**Đáp án: B**

**Câu 18. SYN scan là gì?**

A. Khi Client chưa có kết nối tới Server nhưng vẫn tạo ra gói FIN với số port nhất định gửi tới Server cần scan. Nếu Server gửi về gói ACK thì Client biết Server đó mở port. Nếu Server gửi về gói RST thì Client biết Server đó đóng port.

B. Khi Client gửi gói SYN với một thông số Port nhất định tới Server nếu Server gửi về gói SYN/ACK thì Client biết Port đó trên Server được mở. Nếu Server gửi về cho Client gói RST/SYN thì biết port đó trên Server đóng

C. Client sẽ gửi tới Server những gói TCP với số port nhất định cần scan mà không chứa các thống số Flag như : FIN, URG, PSH, nếu Server gửi lại gói RST thì biết port đó trên Server bị đóng.

D. Client sẽ gửi những gói tin TCP với số port nhất định cần scan chứa nhiều thông số Flag như: FIN, URG, PSH. Nếu Server trả về gói RST tôi biết port đó trên Server bị đóng.

**Đáp án: B**

**Câu 19. Kỹ thuật nào hiệu quả nhất trong việc xác định xem việc tăng cường đào tạo bảo mật người dùng cuối có mang lại lợi ích cho tổ chức hay không?**

A. Network sniffing

B. Vulnerability scanning

C. Application security testing

D. Social engineering

**Đáp án: D**

**Câu 20. Phương pháp nào sau đây được sử dụng để tìm ra các lỗ hổng bảo mật trong một hệ thống bằng cách kiểm tra và phân tích các mã nguồn, cấu hình hệ thống hoặc các tệp tin đã được biên dịch?**

A. Penetration Testing

B. Vulnerability Scanning

C. Code Review

D. Social Engineering

**Đáp án: C.**

### (10) NẮM ĐƯỢC CÁC BIỆN PHÁP PHÒNG THỦ CHỦ ĐỘNG, KHẮC PHỤC SỰ CỐ MẠNG (GỒM 20 CÂU HỎI)

**Câu 1. Các ứng dụng hay thiết bị bảo mật nào sau đây nên được sử dụng để theo dõi và cảnh báo về truy cập trái phép**

A. Phần mềm phòng chống mã độc

B. Thiết bị chuyển mạch (Switch)

C. Hệ thống phát hiện xâm nhập (IDS)

D. Công cụ phân tích mạng

**Đáp án: C**

**Câu 2. Trong quy trình xử lý lỗ hổng bảo mật, bước nào là quan trọng nhất để đảm bảo an toàn lâu dài?**

A. Ghi nhận sự cố và lưu trữ log

B. Vá lỗ hổng và xác minh lại sau khi khắc phục

C. Xóa dữ liệu log cũ để tiết kiệm dung lượng

D. Chặn toàn bộ kết nối Internet

**Đáp án: B**

**Câu 3. Khi phát hiện một hệ thống trong mạng nội bộ có dấu hiệu bị khai thác lỗ hổng bảo mật, bước đầu tiên cần thực hiện là gì?**

A. Ngắt kết nối thiết bị đó khỏi mạng để khoanh vùng sự cố

B. Quét toàn bộ hệ thống mạng để tìm thêm các máy bị lây nhiễm

C. Báo cáo sự cố lên cấp trên sau 24 giờ

D. Cài lại hệ điều hành ngay lập tức

**Đáp án: A**

**Câu 4. Các tập tin nào sau đây có khả năng chứa virus nhất?**

A. database.dat

B. bigpic.jpeg

C. note.txt

D. picture.gif.exe

**Đáp án: D**

**Câu 5. Nên cài mức truy cập mặc định là mức nào sau đây?**

A. Full access

B. No access

C. Read access

D. Write access

**Đáp án: B**

**Câu 7. Mục đích của một máy chủ RADIUS là?**

A. Packet Sniffing

B. Mã hóa

C. Xác thực

D. Thỏa thuận tốc độ kết nối

**Đáp án: C**

**Câu 8. Chọn thiết bị mạng không dây (bộ phát wifi) như thế nào để đảm bảo an toàn thông tin khi sử dụng?**

A. Chọn thiết bị có nguồn gốc xuất xứ rõ ràng, thương hiệu uy tín, có khả năng bảo mật và loại bỏ mã độc, ngăn chặn sự thâm nhập bất hợp pháp từ bên ngoài

B. Chọn thiết bị có nguồn gốc xuất xứ, thương hiệu nổi tiếng của nước ngoài

C. Chọn thiết bị có nguồn gốc xuất xứ rõ ràng, thương hiệu uy tín, có khả năng bảo mật và loại bỏ mã độc, ngăn chặn sự thâm nhập ngẫu nhiên từ bên ngoài

D. Chọn thiết bị có nguồn gốc xuất xứ rõ ràng, thương hiệu uy tín, có khả năng bảo mật và loại bỏ mã độc, ngăn chặn ngẫu nhiên sự thâm nhập bất hợp pháp từ bên ngoài

**Đáp án: A**

**Câu 9. Trong mô hình ma trận truy cập,"namesalary"....**

A. Time-Dependent

B. Date-Dependent

C. Context-Dependent

D. History-Dependent

**Đáp án: C**

**Câu 10. LAC và LNS là các thành phần của giao thức nào ?**

A. IPSec

B. PPP

C. PPTP

D. L2TP

**Đáp án: D**

**Câu 11. Một trong những nguồn gốc chính của mối đe dọa an ninh mạng là gì?**

A. Phần mềm độc hại (Malware)

B. Thiết bị phần cứng lỗi thời

C. Môi trường mạng ổn định

D. Tín hiệu mạng yếu

**Đáp án: A**

**Câu 12. VPN giúp bảo vệ thông tin bằng cách nào?**

A. Ngăn chặn phần mềm độc hại

B. Mã hóa dữ liệu truyền tải

C. Xóa lịch sử duyệt web

D. Giảm băng thông sử dụng

**Đáp án: B**

**Câu 13. Một trong các biện pháp nâng cao năng lực phòng thủ mạng là gì?**

A. Tổ chức diễn tập, kiểm thử thâm nhập thường xuyên

B. Không cho phép truy cập internet

C. Chỉ phụ thuộc vào tường lửa

D. Cấm toàn bộ USB

**Đáp án: A**

**Câu 14. Để phòng thủ chủ động trong hệ thống mạng máy tính, biện pháp nào sau đây là quan trọng nhất?**

A. Cập nhật phần mềm định kỳ.

B. Thực hiện kiểm tra bảo mật định kỳ.

C. Thiết lập mạng riêng ảo (VPN).

D. Mở rộng phạm vi kiểm tra mạng.

**Đáp án: A.**

**Câu 15. Trong hệ điều hành Windows, công cụ nào sau đây được sử dụng để quản lý các chứng chỉ số và khóa công khai?**

A. Windows Defender

B. Microsoft Edge

C. Credential Manager

D. Windows Firewall

**Đáp án: C**

**Câu 16. Trong hệ điều hành Windows**, **công cụ nào thường được sử dụng để mã hóa tệp và thư mục?**

A. Bitlocker

B. Windows Defender

C. Encrypting File System

D. Windows Firewall

**Đáp án: C**

**Câu 17. Nguyên nhân chính dẫn đến việc website bị tấn công Deface là gì?**

A. Lỗi cấu hình máy chủ web

B. Sử dụng giao thức HTTP không mã hóa

C. Thiếu kiểm tra đầu vào dữ liệu người dùng

D. Tải trang web quá chậm

**Đáp án: C**

**Câu 18. Công cụ hoặc phương pháp nào thường được sử dụng để thu thập và phân tích dấu vết của các cuộc tấn công mạng?**

A. Log Analyzer

B. Forensic Tools

C. Network Packet Capture

D. Hệ thống SIEM

**Đáp án: D**

**Câu 19. Biện pháp phòng thủ chủ động là hành động nào sau đây?**

A. Cài đặt Firewall

B. Quét virus định kỳ

C. Theo dõi SIEM và phân tích

D. Sử dụng VPN

**Đáp án đúng: C**

**Câu 20. Biện pháp nào sau đâu là cần thiết để khắc phục sự cố mạng một cách nhanh chóng nhất?**

A. Backup dữ liệu định kỳ

B. Sử dụng IDS/IPS

C. Thuê chuyên gia phân tích nguyên nhân sự cố

D. Cập nhật phần mềm định kỳ

**Đáp án đúng: A**

## III. HẠNG 2 (30 CÂU)

### (1) CÓ KIẾN THỨC CƠ BẢN VỀ NGÀNH CÔNG NGHỆ THÔNG TIN, TÁC CHIẾN KHÔNG GIAN MẠNG. (GỒM 06 CÂU)

**Câu 1.** Tạo chuỗi tìm kiếm Google để tìm file định dạng .sql bất kỳ nằm trong thư mục hoặc thư mục con của thư mục trên máy chủ web “/wp-content/uploads/”, mà trong nội dung file đó có chứa một trong các từ "username", "user name", "uname", "user", "userid", "user id" và một trong các từ "password", "pass word", "pwd", "pw"

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dụng thực hiện** | **Điểm** | **Ghi chú** |
| 1 | Truy cập vào google (https://www.google.com/) | **4** |  |
| 2 | Gõ link: inurl:/wp-content/uploads/ ext:sql "username" | "user name" | "uname" | "user" | "userid" | "user id" AND "password" | "pass word" | "pwd" | "pw"    inurl: Tìm kiếm trong đường dẫn  ext: extension – đuôi file  | : hoặc  AND: và | **6** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 2.** Sử dụng công cụ Whois tìm kiếm một số thông tin (domain id, created on, registrant id, registrant name, registrant city) về tên miền “eccouncil.org”

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dụng thực hiện** | **Điểm** | **Ghi chú** |
| 1 | Truy cập công cụ Whois (https://www.whois.com/) | **4** |  |
| 2 | Gõ tên miền “eccouncil.org” vào ô tìm kiếm | **6** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 3: Sử dụng công cụ Zone H tìm kiếm các trang gov.vn bị tấn công thay đổi giao diện.**

| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| --- | --- | --- | --- |
| Bước 1 | Khởi động công cụ (https://zone-h.org/) | **3** |  |
| Bước 2 | Tìm kiếm domain: gov.vn | **3** |  |
| Bước 3 | Kiểm tra kết quả tìm kiếm | **4** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 4. Tạo chuỗi tìm kiếm Google để tìm các file có định dạng .log nằm trong thư mục hoặc thư mục con của thư mục /logs/ trên máy chủ web, mà trong nội dung file đó có chứa một trong các từ "admin", "administrator", "root" và một trong các từ "password", "passwd", "pwd".**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dụng thực hiện** | **Điểm** | **Ghi chú** |
| 1 | Truy cập vào google (https://www.google.com/) | **4** |  |
| 2 | Gõ link: inurl:/logs/ ext:log ("admin" | "administrator" | "root") AND ("password" | "passwd" | "pwd")    inurl:/logs/: Tìm kiếm trong các URL có chứa /logs/.  ext:log: Chỉ tìm các tệp có đuôi .log.  ("admin" | "administrator" | "root"): Nội dung file phải chứa ít nhất một từ trong nhóm này.  AND ("password" | "passwd" | "pwd"): Đồng thời phải chứa ít nhất một từ trong nhóm này.  |: Nghĩa là “hoặc” giữa các từ khóa.  AND: Cả hai nhóm điều kiện đều phải thỏa mãn. | **6** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 5: Sử dụng công cụ Nikto dò quét website mục tiêu https://vnexperts.vn/**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dụng thực hiện** | **Điểm** | **Ghi chú** |
| 1 | Mở terminal trên kali | **2** |  |
| 2 | Cài đặt công cụ Nikto    Dò quét địa chỉ tên miền mục tiêu | **3** |  |
| 3 | Xem kết quả: | **5** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 6: Sử dụng công cụ Sublist3r dò quét các subdomain của mục tiêu https://vnexperts.vn/**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dụng thực hiện** | **Điểm** | **Ghi chú** |
| 1 | Mở terminal trên kali | **2** |  |
| 2 | Cài đặt công cụ Sublist3r  Dò quét địa chỉ tên miền mục tiêu | **3** |  |
| 3 | Xem kết quả: | **5** |  |
|  | **Tổng điểm** | **10** |  |

### (2) HIỂU BIẾT VỀ TRINH SÁT, PHÒNG THỦ, TẤN CÔNG MẠNG. (GỒM 04 CÂU)

**Câu 1.** **Sử dụng nmap trên kali linux để dò quét trang web www.vnexperts.net bằng phương thức UDP Scan với số port từ 1 đến 1024, không sử dụng ping.**

| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| --- | --- | --- | --- |
| Bước 1 | Mở Kali Linux trong Vmware | **3** |  |
| Bước 2 | Mở Terminal | **3** |  |
| Bước 3 | Chạy câu lệnh  sudo -sU -P ‘1-1024’ -V -P0 [www.vnexperts.net](http://www.vnexperts.net) | **4** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 2. Sử dụng Metasploit Framework trên Kali Linux, tìm kiếm module exploit/multi/http/struts\_dmi\_rest\_exec và chọn sử dụng module này.**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Mở Kali Linux trong Vmware | **1** |  |
| Bước 2 | Mở Terminal | **1** |  |
| Bước 3 | Mở msfconsole bằng lệnh msfconsole | **2** |  |
| Bước 4 | Gõ câu lệnh  search name: Apache Struts REST Plugin | **2** |  |
| Bước 5 | Gõ câu lệnh  use exploit/multi/http/struts\_dmi\_rest\_exec | **4** |  |
|  | **Tổng điểm** | **10** |  |

**3. Trinh sát thu thập thông tin tưởng lửa bào vệ website sử dụng công cụ whatwaf**

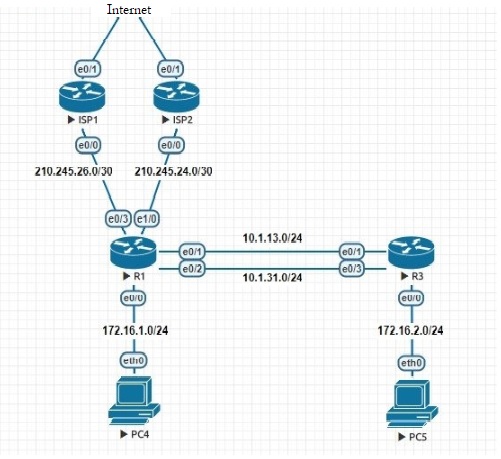
|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Cài đặt công cụ whatwaf  - https://github.com/Ekultek/WhatWaf | 3 |  |
| Bước 2 | - Kiểm tra tưởng lửa trên mục tiêu:  ./whatwaf -u <https://www.facebook.com> | 4 |  |
| Bước 3 | Kiểm tra kết quả | 3 |  |
|  | **Tổng điểm** | 10 |  |

**Câu 4: Trinh sát địa chỉ thông tin đặt máy chủ nơi đặt máy chủ và nhà cung cấp dịch vụ bằng công cụ Check hot**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Truy cập công cụ (<https://check-host.net/>) | 3 |  |
| Bước 2 | - Tìm kiếm thông tin mục tiêu | 4 |  |
| Bước 3 | Kiểm tra kết quả tìm kiếm | 3 |  |
|  | **Tổng điểm** | 10 |  |

### (3) CÓ KIẾN THỨC VỀ HỆ THỐNG MẠNG, CÁC THÀNH PHẦN TRONG HỆ THỐNG MẠNG (GỒM 02 CÂU)

**Câu 1. Cho mô hình sau:**

****

**- Thực hiện đấu nối thiết bị và cấu hình các cấu hình cơ bản**

**- Cấu hình Static route để PC4, PC5 có thể giao tiếp được với nhau.**

**- Config static default route để các máy trong mạng có thể đi ra được Internet.**

**- Sử dụng Static Routing với IP SLA để thực hiện track đường truyền.**

| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| --- | --- | --- | --- |
| 1 | Static Route để PC4, PC5 giao tiếp được với nhau  Syntax của Static Route sẻ có dạng như sau:  *“ip route <Địa chỉ mạng của mạng cần đến> <Subnet mask mạng muốn đi đến> <Next-hop hoặc Outbound interface> <Thông số AD (Nếu cần sử dụng)>”*  VD: ip route 1.1.1.0 255.255.255.0 192.168.1.1         ip route 1.1.1.0 255.255.255.0 e0/0  Thông số AD như mình đã nói ở bài trước, dùng để xác định độ ưu tiên của route. Ở đây ta sử dụng để dự phòng đường đi với Static Route. Mặc định thông số AD của Static Route là 1.  R1: Thực hiên cấu hình Static Route có dự phòng đường đi theo sơ đồ. Ở đây ta sử dụng next-hop là IP của R3 và ngược lại.  R1-ITFORVN(config)#ip route 172.16.2.0 255.255.255.0 10.1.13.3  R1-ITFORVN(config)#ip route 172.16.2.0 255.255.255.0 10.1.31.3 10  Route có AD cao hơn được gọi là “floating static route”. Lúc này khi ta show ip route static ta chỉ thấy được route có AD cao hơn. Muốn thấy floating static route ta tiến hành shutdown interface e0/1 của R1 thì ta sẻ thấy được route này được thay thế trong Routing Table.  Ngoài ra chúng ta còn có thể cấu hình Static Route bằng cổng outbound của R1:  R1-ITFORVN(config)#ip route 172.16.2.0 255.255.255.0 e0/1  R1-ITFORVN(config)#ip route 172.16.2.0 255.255.255.0 e0/2  Tương tự trên R3:  R3-ITFORVN(config)#ip route 172.16.1.0 255.255.255.0 10.1.13.1  R3-ITFORVN(config)#ip route 172.16.1.0 255.255.255.0 10.1.31.1 10  Thực hiện kiểm tra route  R1-ITFORVN(config)#do sh ip route static  [H2. Thực Hiện "show ip route static" trên R1 để kiểm tra](https://itforvn.com/wp-content/uploads/2018/06/H2.-Show-ip-route-.jpg)H2. Thực Hiện “show ip route static” trên R1 để kiểm tra  R3-ITFORVN(config)#do sh ip route static  [H3. Thực Hiện "show ip route static" trên R3 để kiểm tra](https://itforvn.com/wp-content/uploads/2018/06/H3.-Show-ip-route-.jpg)H3. Thực Hiện “show ip route static” trên R3 để kiểm tra  Ở đây có kí tự “S” đứng đầu route có nghĩa là Route này được định tuyến bằng Static Routing. “S\*” là định tuyến bằng Static Default Routing.  Khi ta thực hiện shutdown trên port e0/1 của R1 thì lưu lượng sẻ chuyển xuống đường dưới để đi thể hiện tính dự phòng của static routing trong bài lab này:  R1-ITFORVN(config)#int e0/1  R1-ITFORVN(config-if)#shut  Lưu lượng đã đi xuống đường dưới.  [H4. Thực Hiện "show ip route static" trên R1 để kiểm tra tính dự phòng của Static Routing](https://itforvn.com/wp-content/uploads/2018/06/H4.-D%E1%BB%B1-ph%C3%B2ng-v%E1%BB%9Bi-Static-route.jpg)H4. Thực Hiện “show ip route static” trên R1 để kiểm tra tính dự phòng của Static Routing  Thực hiện “ping” qua lại kiểm tra kết nối giữa các client.  Ở đây ta dùng VPCS (Virtual PC) nên phải tiến hành set địa chỉ IP cho PC trước nhé các Đồng chí. PC4 (IP thuộc lớp mạng 172.16.1.0/24), PC5(IP thuộc lớp mạng 172.16.2.0/24).  PC5:  [H5. Thực hiện "ping" kiểm tra kết nối giữa các Clients](https://itforvn.com/wp-content/uploads/2018/06/H5.-Ki%E1%BB%83m-tra-k%E1%BA%BFt-n%E1%BB%91i.jpg)H5. Thực hiện “ping” kiểm tra kết nối giữa các Clients  Thực hiện ping thành công từ PC5 -> PC4  PC4:  [H6. Thực hiện "ping" kiểm tra kết nối giữa các Clients](https://itforvn.com/wp-content/uploads/2018/06/H7.-Ki%E1%BB%83m-tra-k%E1%BA%BFt-n%E1%BB%91i.jpg)H6. Thực hiện “ping” kiểm tra kết nối giữa các Clients  Thực hiện ping thành công từ PC4 -> PC5 | 2 |  |
| 2 | Config static default route  Để các máy trong mạng có thể đi ra được Internet.  Ở đây ta tiến hành dùng Static Default Route.  Syntax:*“ip route 0.0.0.0 0.0.0.0 <Next-hop hoặc Outbound interface> <Thông số AD (Nếu cần)>”.*  Dãy*“0.0.0.0 0.0.0.0”* đại diện cho tất cả các địa chỉ IP trên toàn thế giới.  R1:  R1-ITFORVN(config)#ip route 0.0.0.0 0.0.0.0 e0/3  R1-ITFORVN(config)#ip route 0.0.0.0 0.0.0.0 e0/1 5  R3:  R3-ITFORVN(config)#ip route 0.0.0.0 0.0.0.0 Ethernet0/1  R3-ITFORVN(config)#ip route 0.0.0.0 0.0.0.0 Ethernet0/3 5  ISP1:  ISP1(config)#ip route 172.16.0.0 255.255.0.0 210.245.26.2  ISP2:  ISP2(config)#ip route 172.16.0.0 255.255.0.0 210.245.24.2    Test:  Tạo interface loopback trên ISP1: 11.11.11.11/32  ISP1(config)#int lo0  ISP1config-if)#ip add 11.11.11.11 255.255.255.255  ISP1(config-if)#exit  PC4:  [H7. Thực hiện "ping" kiểm tra kết nối đi Internet khi dùng Static Default Routing](https://itforvn.com/wp-content/uploads/2018/06/H8.-Ki%E1%BB%83m-tra-k%E1%BA%BFt-n%E1%BB%91i.jpg)H7. Thực hiện “ping” kiểm tra kết nối đi Internet khi dùng Static Default Routing  Ping ra Internet thật: 8.8.8.8  [H8. Thực hiện "ping" kiểm tra kết nối đi Internet khi dùng Static Default Routing](https://itforvn.com/wp-content/uploads/2018/06/H9-Ki%E1%BB%83m-tra-k%E1%BA%BFt-n%E1%BB%91i.jpg)H8. Thực hiện “ping” kiểm tra kết nối đi Internet khi dùng Static Default Routing[H9. Thực hiện "ping" kiểm tra kết nối đi Internet khi dùng Static Default Routing](https://itforvn.com/wp-content/uploads/2018/06/H10.-Ki%E1%BB%83m-tra-k%E1%BA%BFt-n%E1%BB%91i.jpg)H9. Thực hiện “ping” kiểm tra kết nối đi Internet khi dùng Static Default Routing  Ping ra Internet thật: 8.8.8.8  [H10. Thực hiện "ping" kiểm tra kết nối đi Internet khi dùng Static Default Routing](https://itforvn.com/wp-content/uploads/2018/06/H6.-Ki%E1%BB%83m-tra-k%E1%BA%BFt-n%E1%BB%91i.jpg)H10. Thực hiện “ping” kiểm tra kết nối đi Internet khi dùng Static Default Routing  Ở bài lab này nếu thực hiện trên EVE thì ta phải thực hiện NAT trên các ISP để đi ra được Internet thật nhé các Đồng chí. Ở đây các Đồng chí có thể đặt int lo0 trên các ISP thì không cần NAT. | 3 |  |
| 3 | Sử dụng Static Routing với IP SLA  Để thực hiện track đường truyền ISP1 nếu đường truyền này có vấn đề sẻ tự động chuyển sang ISP2 để đi Internet.  R1-ITFORVN(config)#ip sla 1  R1-ITFORVN(config-ip-sla)#icmp-echo 210.245.26.1  R1-ITFORVN(config-ip-sla-echo)#frequency 5  R1-ITFORVN(config)#ip sla schedule 1 start-time now life forever  R1-ITFORVN(config)#track 1 ip sla 1  R1-ITFORVN(config)#ip route 0.0.0.0 0.0.0.0 Ethernet0/3 track 1  R1-ITFORVN(config)#ip route 0.0.0.0 0.0.0.0 Ethernet1/0 10  Thực hiện test bằng cách shutdown int e0/0 của ISP1:  ISP1(config)#int e0/0  ISP1(config-if)#shutdown  Trước khi ta thực hiện test:  Hiện R1 đang route chính đi qua interface e0/3 để đi Internet  [H11. Thực hiện "show ip route static" để kiểm tra lưu lượng khi cấu hình dự phòng IP SLA](https://itforvn.com/wp-content/uploads/2018/06/H11.-Static-Route.jpg)H11. Thực hiện “show ip route static” để kiểm tra lưu lượng khi cấu hình dự phòng IP SLA  Ta thấy R1: báo log như sau :  R1-ITFORVN(config)#  \*Jun 24 21:41:37.715: %TRACK-6-STATE: 1 ip sla 1 state Up -> Down  Log này cho biết. “Track” đã track failed vì interface của ISP đã down. Khi interface trên down thì route “0.0.0.0/0 is directly connected, Ethernet0/3” sẻ bị tháo ra khỏi bảng định tuyến và thay bằng route dự phòng ta đã cấu hình sẳn.  Sau khi ta shutdown interface trên ISP1 thì lưu lượng đã tự chuyển sang ISP2 để đi Internet.  [H12. Thực hiện "show ip route static" để kiểm tra lưu lượng đã chuyển hướng khi cấu hình dự phòng IP SLA](https://itforvn.com/wp-content/uploads/2018/06/H12.-Static-Route.jpg)H12. Thực hiện “show ip route static” để kiểm tra lưu lượng đã chuyển hướng khi cấu hình dự phòng IP SLA  Ta có thể tracroute để tiến hành check.  [H13. Thực hiện "traceroute" để kiểm tra lưu lượng khi chưa chuyển hướng](https://itforvn.com/wp-content/uploads/2018/06/H14.-IP-SLA.jpg) H13. Thực hiện “traceroute” để kiểm tra lưu lượng khi chưa chuyển hướng  Lưu lượng đã chuyển sang ISP2.  [H14. Thực hiện "traceroute" để kiểm tra lưu lượng khi đã chuyển hướng](https://itforvn.com/wp-content/uploads/2018/06/H15.-IP-SLA.jpg) H14. Thực hiện “traceroute” để kiểm tra lưu lượng khi đã chuyển hướng | 5 |  |
|  | Tổng | 10 |  |

**Câu 2. Cho mô hình như sau:**



**Đ/c Cấu hình đặt tên, đặt password enable và cấu hình telnet trên Switch Cisco với vlan quản trị là vlan1**

| **TT** | **Nội dung thực hiện** | **ĐIểm** | **Ghi chú** |
| --- | --- | --- | --- |
| Bước 1 | **- Đặt tên cho switch:**  Switch>  Switch>enable  Switch#configure terminal  Switch(config)#hostname Switch\_01 | 1 |  |
| Bước 2 | **- Đặt Password enable cho Switch**  Switch\_01(config)#enable password cisco | 1 |  |
| Bước 3 | **- Đặt địa chỉ IP quản trị cho switch**  Switch\_01(config)#interface vlan 1  Switch\_01(config-if)#ip address 192.168.1.254 255.255.255.0  Switch\_01(config-if)#no shutdown  Switch\_01(config-if)#exit | 3 |  |
| Bước 4 | **- Mở telnet:**  Switch\_01(config)#line vty 0 4  Switch\_01(config-line)#password cisco  Switch\_01(config-line)#login  Switch\_01(config-line)#exit | 5 |  |
|  | **Tổng điểm** | **10** |  |

### (4) CÓ KHẢ NĂNG THỰC HIỆN KIỂM TRA AN TOÀN THÔNG TIN MÁY TÍNH CÁ NHÂN (GỒM 02 CÂU HỎI)

**Câu 1. Cách bật tính năng kiểm tra VirusTotal trên Process XP?**

**Đáp án:**

| TT | Nội dung thực hiện | Điểm | Ghi chú |
| --- | --- | --- | --- |
| 1 | Mở Process Explorer bằng quyền admin | 2 |  |
| 2 | Vào tab Option chọn VirusTotal.com chọn Check VirusTotal.com | 2 |  |
| 3 | Vào tab View chọn Select Columns | 3 |  |
| 4 | Trong tab Select Columns tích chọn ô Virus Total    - Kết quả: | 3 |  |

**Câu 2: Sử dụng công cụ TCPView liệt kê các tiến trình có hoạt động giao tiếp với bên ngoài.**

| TT | Nội dung thực hiện | Điểm | Ghi chú |
| --- | --- | --- | --- |
| 1 | Sử dụng TCPView  - Khởi chạy chương trình: Click chuột phải chọn chạy quyền Administrator, chọn Run as administrator    Màn hình xuất hiện: Chọn Agree (cho lần khởi chạy đầu tiên). Khởi chạy thành công giao diện của TCPView xuất hiện: | 2 |  |
| 2 | Sử dụng TCPView  - Khi Đồng chí khởi động TCPView, nó sẽ liệt kê tất cả các điểm cuối TCP và UDP đang hoạt động, phân giải tất cả các địa chỉ IP thành các phiên bản tên miền của chúng. Đồng chí có thể sử dụng nút trên thanh công cụ hoặc mục menu để chuyển đổi hiển thị các tên đã phân giải. TCPView hiển thị tên của tiến trình sở hữu mỗi điểm cuối, bao gồm cả tên dịch vụ (nếu có).  - Theo mặc định, TCPView cập nhật mỗi giây, nhưng Đồng chí có thể sử dụng mục menu Options|Refresh Rate.  + Các điểm cuối thay đổi trạng thái từ bản cập nhật này sang bản cập nhật tiếp theo được đánh dấu bằng màu vàng;  + Những điểm bị xóa được hiển thị bằng màu đỏ  + Các điểm cuối mới được hiển thị bằng màu xanh lục. | 4 |  |
| 3 | Đóng các kết nối TCP / IP đã thiết lập bằng cách chọn File|Close Connections hoặc bằng cách nhấp chuột phải vào kết nối và chọn Close Connections từ menu ngữ cảnh.  - Lưu TCPView bằng cách chọn File|Save (Ctrl + S) | 4 |  |

### (5) HIỂU ĐƯỢC CẤU TẠO, TÍNH NĂNG KỸ CHIẾN THUẬT CỦA CÁC HỆ THỐNG TRINH SÁT, PHÒNG THỦ, TẤN CÔNG MẠNG (GỒM 02 CÂU HỎI)

**Câu 1. Sử dụng hệ thống Maltego, trích xuất thông tin mục tiêu có địa chỉ email là** [**tranchien1841@gmail.com**](mailto:tranchien1841@gmail.com)

**Đáp án:**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| B1 | Chọn Entity Email Address  C:\Users\ngocs\OneDrive\Máy tính\6.10\photo_2022-10-06_07-50-17.jpg | 2 |  |
| B2 | Điền thông tin Email và Chọn All Transforms  C:\Users\ngocs\OneDrive\Máy tính\6.10\photo_2022-10-06_07-50-20.jpg | 3 |  |
| B3 | Xem kết quả  C:\Users\ngocs\OneDrive\Máy tính\6.10\photo_2022-10-06_07-50-22.jpg | 5 |  |
|  | Tổng điểm | 10 |  |

**Câu 2. Sử dụng hệ thống Nagios trên mạng Internet, tiến hành cấu hình thêm, xóa trang cổng “https://seagames2021.com” vào hệ thống bằng MobaXterm.**

**Đáp án:**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| B1 | Sử dụng MobaXterm để SSHC:\Users\PC\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Screenshot_1.png | 1 |  |
| B2 | Truy cập theo đường dẫn /usr/local/nagios/etc/objects/Screenshot_2 | 3 |  |
| B3 | Thêm trang cổng  + Mở file command.cfg: Copy câu lệnh theo mẫu có sẵn, chỉnh sửa theo tên miền được yêu cầu.  + Mở file web.cfg: Copy câu lệnh theo mẫu có sẵn, chỉnh sửa theo tên miền được yêu cầu, đặt tên.  + Chạy câu lệnh “systemctl restart nagios”  Screenshot_3 | 3 |  |
| B4 | Xóa trang cổng  + Mở file web.cfg: Xóa câu lệnh đã cấu hình theo tên miền được yêu cầu ở bước 3  + Mở file command.cfg: Xóa câu lệnh đã cấu hình theo tên miền được yêu cầu ở bước 3.  + Chạy câu lệnh “systemctl restart nagios”Screenshot_4 | 3 |  |
|  | Tổng điểm | 10 |  |

### (6) CÓ KIẾN THỨC VỀ KỸ THUẬT GIẢ MẠO, ẨN DANH, XÓA DẤU VẾT TRONG THỰC HIỆN NHIỆM VỤ TÁC CHIẾN MẠNG (GỒM 03 CÂU HỎI)

**Câu 1: Dò quét trang https://vietnamnet.vn sử dụng công cụ nikto của Kali Linux?**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Truy cập máy kali | **2** |  |
| Bước 2 | Sử dụng câu lệnh nikto -h https://vietnamnet.vn | **6** |  |
| Bước 3 | Thu thập thông tin | **2** |  |
|  | **Tổng điểm** | **10** |  |

|  |
| --- |
| **Câu 2: Tạo một session kết nối netcat (mạng local, cổng 9999) trong Kali Linux và đưa ra kết quả hiển thị trên terminal?** |
| |  |  |  |  | | --- | --- | --- | --- | | **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** | | Bước 1 | Mở đồng thời 2 Terminal trong Kali Linux | **2** |  | | Bước 2 | Terminal-1 sử dụng câu lệnh *nc -lvnp 9999* | **3** |  | | Bước 3 | Terminal-2 sử dụng câu lệnh *nc 127.0.0.1 9999* | **3** |  | | Bước 4 | Xem kết quả | **2** |  | |  | **Tổng điểm** | **10** |  | |

1. **Thực hành ẩn danh sử dụng OpenVPN**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Cài đặt openvpn client  - Tải tệp tin cài: <https://openvpn.net/downloads/openvpn-connect-v3-windows.msi>  - Tiến hành cài đặt theo hướng dẫn | 2 |  |
| Bước 2 | Import file cấu hình openvpn, ví dụ: sonnnVC.ovpn | 3 |  |
| Bước 3 | Kết nối OpenVPN | 3 |  |
| Bước 4 | Ngắt kết nối | 2 |  |
|  | **Tổng điểm** | 10 |  |

### (7) HIỂU VÀ THỰC HIỆN ĐƯỢC CÁC QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN KHI THỰC HIỆN NHIỆM VỤ THỰC TẾ (GỒM 02 CÂU HỎI)

**Câu 1. Sử dụng Shodan tìm kiếm cách đăng nhập theo mặc định các thiết bị CameraIp của hãng Vivotek có trên mạng Internet tại Việt Nam.**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Truy cập vào trang “Shodan.io” trên trình duyệt | **2** |  |
| Bước 2 | Gõ thông tin tìm kiếm “VVTK-HTTP-Server” country:vn | **3** |  |
| Bước 3 | Sử dụng danh sách user, mật khẩu mặc định của thiết bị Vivotek Camera để đăng nhập vào các IP đã tìm được | **3** |  |
| Bước 4 | Thu thập thông tin | **2** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 2. Sử dụng công cụ Hydra để dò quét mật khẩu dịch vụ smb trên máy nạn nhân có địa chỉ IP: 192.168.1.129**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Sử dụng Nmap dò quét để xác định nạn nhân đang sử dụng dịch vụ smb: nmap -sS 192.168.1.129 –p 445 | **3** |  |
| Bước 2 | Sử dụng công cụ Hydra để dofquets mật khẩu: hydra -L /root/Desktop/username.txt -P /root/Desktop/password.txt -t 1 192.168.1.129 smb | **4** |  |
| Bước 3 | Thu thập thông tin | **3** |  |
|  | **Tổng điểm** | **10** |  |

### (8) CÓ KIẾN THỨC VỀ LỖ HỔNG BẢO MẬT, KỸ THUẬT TRINH SÁT TẤN CÔNG MẠNG; CÁC LỖ HỔNG PHỔ BIẾN CỦA CÁC THÀNH PHẦN TRONG HỆ THỐNG MẠNG. (GỒM 03 CÂU HỎI)

**Câu 1: Thực hiện tìm kiếm module khai thác CVE-2017-0143, sau đó chọn và hiển thị cấu hình của module?**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Mở máy kali, khởi động metasploit: msfconsole | **3** |  |
| Bước 2 | - Tìm module khai thác lỗ hổng CVE-2017-0143: search cve-2017-0143;  - Chỉnh các tham số mã khai thác:  + use exploit/windows/smb/ms17\_010\_eternalblue  + show options hoặc gõ options | **5** |  |
| Bước 3 | Xem kết quả | **2** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 2: Thực hiện cấu hình các tham số trong module khai thác lỗ hổng CVE-2017-0143?**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Chon module khai thác lỗ hổng cve-2017-0143:  + use exploit/windows/smb/ms17\_010\_eternalblue | **3** |  |
| Bước 2 | - Chỉnh các tham số mã khai thác:  + show options  + set rhost <ip mục tiêu>  + set lhost <ip kẻ tấn công>  + set lport <cổng lắng nghe trên máy kẻ tấn công> | **5** |  |
| Bước 3 | Xem kết quả | **2** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 3. Trinh sát thu thập thông tin subdomain sử dụng công cụ subfinder**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest | 3 |  |
| Bước 2 | Thu thập thông tin subdomain của mục tiêu, ví dụ: mod.gov.vn | 4 |  |
| Bước 3 | Kiểm tra kết quả | 3 |  |
|  | **Tổng điểm** | **10** |  |

### (9) HIỂU VỀ QUY TRÌNH TRINH SÁT, KIỂM THỬ, KHAI THÁC LỖ HỔNG BẢO MẬT (GỒM 04 CÂU HỎI)

**Câu 1: Thực hiện dò quét cổng từ 1000 đến 5000 của một ip sử dụng công cụ Nmap?**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Mở máy kali linux; mở 01 giao diện terminal | **2** |  |
| Bước 2 | Quét cổng 1000 đến 5000 trên mục tiêu với công cụ nmap: nmap 192.168.88.1 -p 1000-5000 | **5** |  |
| Bước 3 | Thu thập thông tin | **3** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 2: Thực hiện dò quét mục tiêu sử dụng tất cả các script có trong Nmap?**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Mở máy kali linux; mở 01 giao diện terminal | **2** |  |
| Bước 2 | Quét mục tiêu với công cụ nmap sử dụng tất cả script: nmap -sC 192.168.88.1 | **5** |  |
| Bước 3 | Thu thập thông tin | **3** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 3. Trinh sát thu thập thông tin sử dụng công cụ DNSDumpter**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Truy cập vào trang: https://dnsdumpster.com/ | 3 |  |
| Bước 2 | Gõ tên miền mục tiêu cần tìm kiếm vào ô tìm kiếm, ví dụ: 24h.com | 4 |  |
| Bước 3 | Kiểm tra kết quả | 3 |  |
|  | **Tổng điểm** | **10** |  |

**Câu 4. Sử dụng công cụ nuclei để dò quét lỗ hổng bảo mật web**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | + Cài đặt công cụ nuclei  sudo apt install nuclei | 3 |  |
| Bước 2 | + Sử dụng công cụ nuclei để quét mục tiêu:  nuclei -u http://testphp.vulnweb.com/ | 4 |  |
| Bước 3 | + Kiểm tra kết quả | 3 |  |
|  | **Tổng điểm** | **10** |  |

### (10) NẮM ĐƯỢC CÁC BIỆN PHÁP PHÒNG THỦ CHỦ ĐỘNG, KHẮC PHỤC SỰ CỐ MẠNG (GỒM 02 CÂU HỎI)

**Câu 1: Các bước tiến hành đánh giá điểm yếu web bằng công cụ Acunetix**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Đăng nhập vào hệ thống Acunetix; | **2** |  |
| Bước 2 | Quét mục tiêu với Acunetix:  + Tạo Target.  + Cấu hình các thông số General cho Target.  + Quét website với chế độ đăng nhập trang web.  + Cấu hình Crawl website.  + Cấu hình HTTP.  + Cấu hình quét website qua proxy.  + Cấu hình quét Advanced.  + Loại dò quét.  + Lịch dò quét.  + Khởi chạy Scan. | **8** |  |
|  | **Tổng điểm** | **10** |  |

**Câu 2: Thực hiện kiểm tra tình trạng máy mục tiêu thông qua lệnh Ping và trang https://check-host.net/?**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Nội dung thực hiện** | **Điểm** | **Ghi chú** |
| Bước 1 | Mở 01 giao diện cmd trên máy Windows; Kiểm tra tình trạng mục tiêu bằng câu lệnh ping: ping 8.8.8.8 | **4** |  |
| Bước 2 | Truy cập vào website “https://check-host.net”: nhập địa chỉ ip cần check và chọn ping hoặc http | **4** |  |
| Bước 3 | Xem thông tin kết quả | **2** |  |
|  | **Tổng điểm** | **10** |  |