examundo

Thi thử CEH tiếng Việt

70 câu hỏi kèm đáp án. Hướng dẫn và bản dịch do phần mềm làm và kiểm tra.
Chưa có người nào kiểm tra lại.

Cập nhật ngày 25 tháng 11 năm 2026 · examundo.tech/vi/ceh/

Tấn công hệ thống

1. Một pentester có thông tin đăng nhập domain hợp lệ nhưng quyền thấp. Họ yêu cầu service ticket (TGS) cho các tài khoản đã đăng ký Service Principal Name (SPN), trích xuất ticket rồi bẻ khóa offline để lấy mật khẩu gốc của tài khoản dịch vụ. Cuộc tấn công này gọi là gì?

A tester with valid but low-privileged domain credentials requests service tickets (TGS) for accounts that have registered Service Principal Names, then extracts the tickets and attempts to crack them offline to recover the service account's plaintext password. What is this attack called?

A. AS-REP roasting
B. Tấn công pass-the-ticket
C. Kerberoasting
D. Tấn công golden ticket

---

2. Trong giai đoạn hậu khai thác (post-exploitation) trên mạng Windows, pentester trích xuất một NTLM hash trực tiếp từ bộ nhớ LSASS và dùng chính hash đó để xác thực sang máy chủ thứ hai qua SMB, mà không bẻ khóa để lấy mật khẩu gốc. Đây là kỹ thuật tấn công nào?

During post-exploitation on a Windows network, a tester extracts an NTLM hash directly from LSASS memory and uses that hash to authenticate to a second server via SMB, without ever cracking it to recover the plaintext password. Which attack technique does this describe?

A. Tấn công pass-the-hash
B. Đầu độc LLMNR/NBT-NS (LLMNR/NBT-NS poisoning)
C. Tấn công golden ticket
D. Kerberoasting

---

3. Pentester biết mật khẩu của mục tiêu có dạng một chữ hoa, năm chữ thường và hai chữ số (ví dụ Summer24). Lệnh hashcat nào nhắm đúng mẫu này vào một tệp hash NTLM?

A tester knows a target's password follows the pattern of one capital letter, five lowercase letters, and two digits (e.g., Summer24). Which hashcat command correctly targets this pattern against a file of NTLM hashes?

A. hashcat -m 1000 -a 3 hashes.txt ?u?l?l?l?l?d?d
B. hashcat -m 1000 -a 0 hashes.txt ?u?l?l?l?l?d?d
C. hashcat -m 1000 -a 3 hashes.txt ?l?l?l?l?l?u?d?d
D. hashcat -m 1800 -a 3 hashes.txt ?u?l?l?l?l?d?d

---

4. Kẻ tấn công giấu một tệp thực thi độc hại trong Alternate Data Stream của một tệp văn bản bình thường trên ổ NTFS bằng lệnh type malware.exe > notes.txt:hidden.exe. Đặc điểm nào khiến kỹ thuật này hiệu quả trong việc qua mặt kiểm tra thông thường?

An attacker hides a malicious executable inside an Alternate Data Stream of a legitimate text file on an NTFS volume using the command type malware.exe > notes.txt:hidden.exe. Which characteristic of this technique makes it effective for evading casual detection?

A. Kỹ thuật này hoạt động giống hệt trên hệ thống tệp FAT32 và ext4
B. Phần mềm diệt virus không thể quét Alternate Data Stream trong bất kỳ trường hợp nào
C. Luồng ẩn tự động mã hóa nội dung bằng EFS
D. Dung lượng của notes.txt hiển thị trong Windows Explorer không phản ánh nội dung của luồng ẩn

---

5. Trong lúc đánh giá hậu khai thác trên một máy Linux, pentester chạy find / -perm -4000 -type f 2>/dev/null và thấy chính /usr/bin/find có bit SUID và thuộc sở hữu của root. Hành động nào tận dụng cấu hình sai này TỐT NHẤT để leo thang đặc quyền?

During a post-exploitation assessment on a Linux host, a tester runs find / -perm -4000 -type f 2>/dev/null and discovers that /usr/bin/find itself has the SUID bit set and is owned by root. Which action would BEST leverage this misconfiguration to escalate privileges?

A. Thay thế tệp nhị phân /usr/bin/find bằng payload reverse shell
B. Chạy find với -exec để mở một root shell
C. Dùng find để tìm password hash trong /etc/shadow
D. Sửa trực tiếp /etc/passwd vì find có quyền ghi

---

6. Một chuyên gia điều tra số (forensics) phát hiện các tệp nhị phân ps, netstat và ls trên máy chủ Linux bị xâm nhập đã bị thay bằng bản sửa đổi, giấu tiến trình, kết nối mạng và tệp của kẻ tấn công khỏi các truy vấn thông thường. Đây là LOẠI công cụ độc hại nào?

A forensic analyst discovers that a compromised Linux server's `ps`, `netstat`, and `ls` binaries have been replaced with modified versions that hide the attacker's processes, network connections, and files from standard queries. What TYPE of malicious tool is described?

A. Userland rootkit
B. Logic bomb
C. Trojan horse
D. Kernel-mode rootkit

---

7. Kẻ tấn công dùng wevtutil cl Security để xóa log sự kiện Security của Windows sau khi hoàn tất thao tác trên một máy trạm thuộc domain. Dấu vết nào NHIỀU KHẢ NĂNG NHẤT cho thấy log đã bị xóa, dù nội dung log đã mất?

An attacker uses wevtutil cl Security to clear the Windows Security event log after completing an operation on a domain-joined workstation. Which artifact is MOST likely to reveal that log clearing occurred, even though the log's contents are gone?

A. Log System, không thể bị xóa bằng wevtutil và luôn còn nguyên
B. Tệp Prefetch của wevtutil.exe, tự động bị xóa sau khi lệnh chạy
C. Event ID 1102 ghi trong chính log đó, báo “The audit log was cleared”
D. Mục $MFT của tệp Security.evtx, bất biến và không thể bị sửa

---

8. Một pentester lấy được tệp hash mật khẩu Windows và muốn khôi phục mật khẩu gốc bằng cách đối chiếu hash với một bảng lớn được tính sẵn, ánh xạ hash sang mật khẩu. Đây là kỹ thuật nào?

A penetration tester obtains a Windows password hash file and wants to recover plaintext passwords by comparing the hashes against a large precomputed table of hash-to-plaintext mappings. Which technique is being used?

A. Tấn công rainbow table
B. Tấn công brute-force
C. Kerberoasting
D. Tấn công từ điển (dictionary attack)

---

9. Kẻ tấn công có NTLM hash của tài khoản krbtgt và giả mạo một Ticket Granting Ticket cho phép truy cập mọi dịch vụ trong domain, vẫn còn hiệu lực cho đến khi mật khẩu krbtgt được đặt lại hai lần. Đây là cuộc tấn công nào?

An attacker who has compromised the krbtgt account's NTLM hash forges a Ticket Granting Ticket that grants access to any service in the domain and remains valid until the krbtgt password has been reset twice. Which attack does this describe?

A. Tấn công silver ticket
B. Tấn công golden ticket
C. Tấn công pass-the-hash
D. Tấn công DCSync

---

10. Kẻ tấn công có quyền SYSTEM trên một máy Windows và muốn duy trì quyền truy cập (persistence) qua registry, chạy một ứng dụng native-subsystem trong lúc Session Manager khởi tạo, trước khi Windows subsystem được nạp. Vị trí registry nào hỗ trợ giai đoạn thực thi này?

An attacker has SYSTEM-level access to a Windows system and wants to establish registry-based persistence that launches a native-subsystem application during Session Manager initialization, before the Windows subsystem loads. Which registry location supports this execution phase?

A. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

B. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

C. HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute

D. HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Trinh sát (footprinting)

11. Một pentester liệt kê bản ghi DNS của target.com và thấy hai bản ghi MX: mail.target.com với priority 10 và backupmx.target.com với priority 20. Phát biểu nào xác định đúng máy chủ thư chính?

A tester enumerates DNS records for target.com and finds two MX records: mail.target.com with priority 10 and backupmx.target.com with priority 20. Which statement correctly identifies the primary mail exchanger?

A. mail.target.com là máy chính vì giá trị priority thấp hơn nghĩa là được ưu tiên hơn

B. backupmx.target.com là máy chính vì giá trị priority cao hơn nghĩa là được ưu tiên hơn

C. Giá trị priority bị bỏ qua; MX được chọn theo thứ tự bảng chữ cái

D. Cả hai máy chủ được dùng đồng thời với mức ưu tiên bằng nhau

---

12. Một pentester chạy traceroute tới địa chỉ IP công khai của mục tiêu để vẽ đường đi mạng và xác định các router, tường lửa trung gian trước khi quét. Hoạt động này thuộc loại footprinting nào?

A tester runs traceroute against a target's public IP address to map the network path and identify intermediate routers and firewalls before scanning begins. This activity falls under which footprinting category?

A. Chỉ là footprinting thụ động

B. Footprinting bằng social engineering

C. Footprinting DNS

D. Footprinting mạng

---

13. Trong giai đoạn footprinting, một thành viên red team truy vấn bản ghi DNS của tên miền mục tiêu để lên kế hoạch spear-phishing. Loại bản ghi DNS nào cho thông tin TRỰC TIẾP NHẤT về hạ tầng email của tổ chức?

During footprinting, a red team operator queries a target domain's DNS records to plan a spear-phishing campaign. Which DNS record type provides the MOST direct information about the organization's email infrastructure?

A. MX

B. NS

C. PTR

D. SOA

---

14. Một pentester chạy `dig axfr @ns1.target.com target.com` để thử lấy toàn bộ zone transfer DNS trong giai đoạn trinh sát của một đợt kiểm thử. Xét về phương pháp luận, xếp hành động này vào loại trinh sát nào là ĐÚNG NHẤT?

A penetration tester issues `dig axfr @ns1.target.com target.com` in an attempt to obtain a full DNS zone transfer during the reconnaissance phase of an engagement. From a methodology standpoint, this action is BEST classified as which type of reconnaissance?

A. Trinh sát chủ động, vì gửi truy vấn trực tiếp tới hệ thống do mục tiêu sở hữu và vận hành

B. Trinh sát thụ động, vì dig là công cụ chẩn đoán chỉ đọc

C. Trinh sát thụ động, vì truy vấn DNS không bao giờ chạm vào hạ tầng mà mục tiêu giám sát

D. Trinh sát chủ động chỉ khi việc chuyển vùng thành công và trả về bản ghi

---

15. Một pentester kết nối thẳng tới cổng 25 của mục tiêu bằng netcat và đọc banner máy chủ trả về để xác định phần mềm và phiên bản máy chủ thư. Kỹ thuật này là ví dụ của:

A penetration tester connects directly to a target's port 25 using netcat and reads the returned server banner to determine the mail server software and version. This technique is an example of:

A. Quét lỗ hổng (vulnerability scanning)

B. Enumeration, không phải footprinting

C. Footprinting chủ động

D. Footprinting thụ động

---

16. Công cụ trinh sát nào được thiết kế riêng làm framework OSINT dạng mô-đun, tự động thu thập dữ liệu từ mạng xã hội, WHOIS, công cụ tìm kiếm và hiển thị các mối quan hệ bằng đồ thị?

Which reconnaissance tool is purpose-built as a modular OSINT framework that automates data collection from sources such as social media, WHOIS, and search engines, presenting relationships in a graph-based visualization?

A. Maltego

B. Responder

C. Nmap

D. Hydra

---

17. Pentester chạy lệnh banner grabbing bằng telnet vào máy chủ thư của mục tiêu và nhận phản hồi “220 mail.targetcorp.com ESMTP Postfix”. Phản hồi này cho pentester biết trực tiếp nhất điều gì?

A tester runs a banner-grabbing command against a target's mail server using telnet and receives the response "220 mail.targetcorp.com ESMTP Postfix". What has the tester most directly learned?

A. Danh sách đầy đủ email của nhân viên

B. Nhà đăng ký tên miền và liên hệ quản trị

C. Phần mềm máy chủ thư và có thể cả phiên bản

D. Toàn bộ dải địa chỉ IP công khai của tổ chức

---

18. Tổ hợp toán tử tìm kiếm Google nào HIỆU QUẢ NHẤT để tìm các tệp cấu hình đã được lập chỉ mục công khai có chứa chuỗi 'password' trên một tên miền cụ thể?

Which Google search operator combination would MOST effectively locate publicly indexed configuration files containing the string 'password' on a specific target domain?

A. link:target.com password

B. site:target.com inurl:admin password

C. site:target.com filetype:conf intext:password

D. cache:target.com "password"

---

19. Trong giai đoạn trinh sát, một ethical hacker truy vấn cơ sở dữ liệu đăng ký công khai để tìm tên người đăng ký, tổ chức đăng ký và liên hệ quản trị của tên miền mục tiêu. Hoạt động nào đang được thực hiện?

During the reconnaissance phase, an ethical hacker queries a public registry database to find the registrant name, registering organization, and administrative contact for a target's domain name. Which activity is being performed?

A. DNS zone transfer

B. Quét cổng (port scanning)

C. Tra cứu WHOIS

D. Banner grabbing

---

20. Bộ lọc tìm kiếm Shodan nào mà nhà phân tích sẽ dùng để tìm các thiết bị kết nối internet nằm trong một quốc gia cụ thể?

Which Shodan search filter would an analyst use to find internet-facing devices located specifically within a given country?

A. hostname:
B. country:
C. org:
D. geo:

Tấn công mạng và vành đai

21. Khi quét một subnet, pentester thấy một máy mở rất nhiều cổng, mọi cổng đều có banner dịch vụ giống hệt nhau và dài bất thường, không có phản hồi khớp với bắt tay giao thức thật, và thời gian phản hồi nhanh bất thường với mọi truy vấn. Kết luận nào có cơ sở NHẤT?

While scanning a subnet, a tester finds a host exposing numerous open ports, all with identical and unusually verbose service banners, no responses matching legitimate protocol handshakes, and abnormally fast response times regardless of the query. Which conclusion is MOST justified?

A. Máy này có khả năng là honeypot tương tác thấp
B. Máy này đang chạy hệ thống ngăn chặn xâm nhập (IPS)
C. Máy này nằm sau một load balancer
D. Máy này là máy chủ production đã được gia cố bảo mật (hardened)

22. Một nhân viên nhận email có vẻ đến từ bộ phận hỗ trợ IT, yêu cầu đặt lại mật khẩu ngay qua một liên kết dẫn tới trang đăng nhập giả. Đây là kỹ thuật social engineering (tấn công phi kỹ thuật) nào?

An employee receives an email appearing to be from the IT helpdesk, urging an immediate password reset through an embedded link that leads to a fake login page. Which social engineering technique does this represent?

A. Vishing
B. Phishing
C. Pretexting
D. Tailgating

23. Kẻ tấn công làm tràn bảng CAM của switch bằng hàng nghìn ánh xạ MAC-cổng giả mạo, khiến switch "fail open" và phát khung ra mọi cổng như hub. Đây là cuộc tấn công nào?

An attacker floods a switch's CAM table with thousands of forged MAC address-to-port mappings, causing the switch to fail open and broadcast frames out every port like a hub. Which attack is being performed?

A. VLAN hopping
B. DHCP starvation
C. MAC flooding
D. ARP spoofing

24. Kẻ tấn công làm tràn bảng CAM của switch bằng hàng nghìn địa chỉ MAC nguồn giả. Mục tiêu chính của cuộc tấn công này là gì?

An attacker floods a switch's CAM table with thousands of fabricated source MAC addresses. What is the primary goal of this attack?

A. Ép switch vào chế độ fail-open để phát lưu lượng ra mọi cổng như hub
B. Làm sập hệ điều hành của switch để gây từ chối dịch vụ
C. Có quyền quản trị qua console của switch
D. Vượt hoàn toàn xác thực cổng 802.1X

25. Pentester gửi các gói dò có giá trị TTL tăng dần tới một máy sau tường lửa, dùng các thông báo ICMP Time Exceeded trả về để xác định cổng cụ thể nào mà ACL cho đi qua tường lửa. Đây là kỹ thuật nào?

A tester sends probe packets with incrementally increasing TTL values toward a host behind a firewall, using the resulting ICMP Time Exceeded messages to determine which specific ports the ACL permits to pass through the firewall. Which technique is being performed?

A. Vẽ đường đi bằng traceroute thông thường
B. Firewalking
C. Nhận diện OS qua phân tích TTL
D. Banner grabbing

---

26. Kỹ thuật né IDS trong đó kẻ tấn công cố ý chia payload thành nhiều đoạn TCP nhỏ gửi cách nhau có chủ đích, để thời gian chờ ghép lại của IDS hết trước khi khớp được chữ ký đầy đủ, được gọi là:

An IDS evasion technique in which an attacker deliberately spreads an attack payload across many small TCP segments transmitted with intentional inter-packet delay, so that the IDS's reassembly timeout expires before the complete signature can be matched, is known as:

A. Session splicing
B. Mã hóa đa hình (polymorphic encoding)
C. Firewalking
D. Fragmentation overlap

---

27. Một chuyên gia đánh giá an ninh vật lý đến gần cửa có khóa thẻ đúng lúc một nhân viên đi ra. Nhân viên thấy người đó, tưởng là đồng nghiệp và tự nguyện giữ cửa cho vào. Đây là ví dụ của:

A physical security assessor approaches a badge-secured door just as an employee is exiting. The employee notices the assessor, assumes they are a coworker, and voluntarily holds the door open for them. This is an example of:

A. Piggybacking, vì nhân viên biết và cho phép vào
B. Tailgating, vì người vào không được ai cho phép
C. Shoulder surfing
D. Dumpster diving

---

28. Một pentester tạo dữ liệu độc hại chia thành nhiều mảnh IP nhỏ rồi gửi tới mục tiêu được bảo vệ bởi hệ thống phát hiện xâm nhập dựa trên chữ ký. Kỹ thuật né tránh nào đang được dùng?

A penetration tester crafts malicious payload data split across several small IP fragments before sending it toward a target protected by a signature-based intrusion detection system. Which evasion technique is being employed?

A. Flooding
B. Phân mảnh (fragmentation)
C. Giả mạo (spoofing)
D. Mã hóa

---

29. Trong một đợt đánh giá social engineering được ủy quyền, kẻ tấn công gọi bộ phận hỗ trợ IT, giả làm một giám đốc đang đi công tác cần đặt lại mật khẩu gấp, đưa ra mã nhân viên và phòng ban bịa để tạo uy tín. Đây là kỹ thuật social engineering nào?

During an authorized social engineering assessment, an attacker calls the IT help desk posing as a traveling executive who urgently needs a password reset, offering fabricated employee ID and department details to build credibility. Which social engineering technique is being demonstrated?

A. Pretexting
B. Tailgating
C. Phishing
D. Baiting

---

30. Sau khi pentester chiếm phiên TCP đã xác thực bằng cách chèn các đoạn giả mạo với sequence number dự đoán đúng, client và server hợp pháp bắt đầu trao đổi liên tục các gói xác nhận không hợp lệ mà không bao giờ đồng bộ lại. Hiện tượng phụ này gọi là gì?

After a tester hijacks an authenticated TCP session by injecting spoofed segments with a correctly predicted sequence number, the legitimate client and server begin exchanging a continuous stream of invalid acknowledgment packets that never resynchronize. What is this side effect called?

A. SYN flood
B. DNS amplification
C. ACK storm
D. ARP cache exhaustion

Tấn công ứng dụng web

31. Một máy chủ web production trả về stack trace chi tiết, gồm số phiên bản framework và đường dẫn tệp, mỗi khi xảy ra ngoại lệ không được xử lý. Điểm yếu này thuộc danh mục OWASP Top 10 nào?

A production web server returns detailed stack traces, including framework version numbers and file paths, whenever an unhandled exception occurs. Which OWASP Top 10 category does this weakness fall under?

A. Injection
B. Security misconfiguration
C. Cryptographic failures
D. Identification and authentication failures

---

32. Pentester nhập dấu chấm phẩy kèm một lệnh Linux vào ô biểu mẫu web đang thực hiện tra cứu ping ở backend, và kết quả của lệnh thêm đó được trả về trong phản hồi. Loại lỗ hổng nào đã bị khai thác?

A tester submits a semicolon followed by a Linux command into a web form field that performs a network ping lookup on the backend, and the additional command's output is returned in the response. Which vulnerability class was exploited?

A. OS command injection
B. SQL injection
C. Insecure deserialization
D. Cross-site scripting

---

33. Pentester gửi một truy vấn tìm kiếm chứa thẻ script. Trang lỗi trả về đưa ngay payload đó vào phản hồi HTML mà không encode ký tự, và payload chạy trong trình duyệt của pentester. Đây là loại cross-site scripting nào?

A tester submits a search query containing a script tag, and the resulting error page immediately echoes the payload back into the HTML response without encoding, executing in the tester's browser. Which type of cross-site scripting is this?

A. Reflected XSS
B. Blind XSS
C. Stored XSS
D. DOM-based XSS

---

34. Một ứng dụng web Java nhận một đối tượng tuần tự hóa (serialized) trong tham số cookie và giải tuần tự hóa mà không kiểm tra. Pentester tạo payload tuần tự hóa độc hại bằng gadget chain đã biết và thực thi mã từ xa thành công. Nguyên nhân gốc nào đã cho phép cuộc tấn công này?

A Java web application accepts a serialized object in a cookie parameter and deserializes it without validation. A tester crafts a malicious serialized payload using a known gadget chain and achieves remote code execution. Which root cause enabled this attack?

A. Ứng dụng giải tuần tự hóa dữ liệu do kẻ tấn công kiểm soát mà không giới hạn kiểu hay xác minh tính toàn vẹn
B. Ứng dụng dùng bộ mã hóa TLS lỗi thời để truyền cookie
C. Ứng dụng lưu trạng thái phiên ở cookie phía client thay vì phía server
D. Ứng dụng không đặt cờ HttpOnly cho cookie

---

35. Một ứng dụng web cho người dùng nhập URL để máy chủ tải về tạo bản xem trước hình thu nhỏ. Pentester nhập địa chỉ metadata đám mây nội bộ và phản hồi chứa thông tin đăng nhập của instance. Lỗ hổng nào đã bị khai thác?

A web application lets users enter a URL that the server fetches to generate a thumbnail preview. A tester enters an internal cloud metadata address and the response includes instance credentials. Which vulnerability was exploited?

A. Cross-site scripting
B. Path traversal
C. Insecure direct object reference
D. Server-side request forgery

---

36. Một ứng dụng nhận đối tượng Java tuần tự hóa mã hóa base64 từ cookie và dựng lại trên máy chủ mà không kiểm tra, cho phép kẻ tấn công thực thi mã từ xa bằng một đối tượng chế sẵn. Lỗ hổng nào đã cho phép cuộc tấn công này?

An application accepts a base64-encoded serialized Java object from a cookie and reconstructs it on the server without validation, allowing an attacker to trigger remote code execution with a crafted object. Which vulnerability enabled this attack?

A. Cross-site request forgery
B. Clickjacking
C. Insecure deserialization
D. Broken access control

---

37. Trước khi nạn nhân đăng nhập, kẻ tấn công gửi cho họ một liên kết chứa session ID đặt sẵn. Sau khi nạn nhân xác thực, ứng dụng không tạo lại session ID, và kẻ tấn công dùng chính ID đó để vào phiên đã xác thực. Đây là cuộc tấn công nào?

Before a victim logs in, an attacker sends the victim a link containing a pre-set session identifier. After the victim authenticates, the application does not regenerate the session ID, and the attacker uses the same identifier to access the now-authenticated session. Which attack is this?

A. Clickjacking
B. Session fixation
C. Chiếm phiên bằng nghe lén gói tin (session hijacking via packet sniffing)
D. Cross-Site Request Forgery

---

38. Công cụ nào được pentester dùng PHỔ BIẾN NHẤT làm proxy chặn bắt (intercepting proxy) để kiểm tra và sửa các yêu cầu HTTP giữa trình duyệt và ứng dụng web?

Which tool is MOST commonly used by penetration testers as an intercepting proxy to inspect and modify HTTP requests between a browser and a web application?

A. Burp Suite
B. Hashcat
C. Nmap
D. Wireshark

---

39. Khi kiểm thử một ứng dụng web Flask, pentester nhập '{{7*7}}' vào ô phản hồi của biểu mẫu, và trang hiển thị sau đó cho ra '49' thay vì chuỗi nguyên văn. Hành vi này xác nhận lỗ hổng nào?

During testing of a Flask-based web application, a tester submits the input '{{7*7}}' into a feedback form field, and the rendered page subsequently displays '49' instead of the literal string. Which vulnerability is confirmed by this behavior?

A. SQL injection, trong đó 7*7 được cơ sở dữ liệu tính như biểu thức số học
B. Server-side template injection (SSTI) qua template engine Jinja2
C. Reflected cross-site scripting do đầu ra HTML không được escape
D. Client-side template injection do sandbox biểu thức AngularJS xử lý

---

40. Loại tấn công nào xảy ra khi đầu vào không tin cậy của người dùng được chèn vào truy vấn cơ sở dữ liệu mà không được làm sạch đúng cách, cho phép kẻ tấn công thay đổi logic của truy vấn?

Which type of attack occurs when untrusted user input is inserted into a database query without proper sanitization, allowing an attacker to alter the query's logic?

A. Cross-site request forgery
B. SQL injection
C. Server-side request forgery
D. Cross-site scripting

Tấn công Wi-Fi

41. Một tổ chức bật Protected Management Frames (802.11w) trên toàn bộ hạ tầng không dây. Biện pháp này CHỦ YẾU giảm thiểu kỹ thuật tấn công không dây phổ biến nào?

An organization enables Protected Management Frames (802.11w) across its wireless infrastructure. Which common wireless attack technique does this control PRIMARILY mitigate?

A. Tấn công rogue DHCP server
B. Tấn công từ điển offline vào handshake đã bắt
C. Tấn công brute-force mã PIN WPS
D. Giả mạo khung deauthentication và disassociation

---

42. Pentester muốn lấy dữ liệu xác thực từ mạng WPA2-PSK mà không phải chờ một client hợp lệ xác thực. Kỹ thuật nào đạt mục tiêu này TỐT NHẤT?

A tester wants to obtain credential material from a WPA2-PSK network without waiting for a legitimate client to authenticate. Which technique BEST accomplishes this goal?

A. Chạy tấn công brute-force mã PIN WPS bằng Reaver
B. Gửi khung deauthentication rồi chờ bắt 4-way handshake của client
C. Bắt PMKID từ khung EAPOL đầu tiên của AP bằng hcxdumptool
D. Thực hiện ARP spoofing vào các client đang kết nối với AP

---

43. Một thành viên red team dựng một rogue access point phát cùng SSID và cường độ tín hiệu tương đương mạng công ty để dụ nhân viên kết nối, rồi chặn lưu lượng của họ. Đây là tấn công nào, và nó khác tấn công Karma ở điểm nào?

A red team operator sets up a rogue access point broadcasting the same SSID and comparable signal strength as a corporate network to lure employees into connecting, then intercepts their traffic. This describes which attack, and how does it differ from a Karma attack?

A. Tấn công deauthentication; nó ép client ngắt kết nối trước khi giả mạo mạng
B. Tấn công evil twin; nó trả lời mọi SSID mà client từng dò tìm
C. Tấn công Karma; nó giả mạo một SSID cụ thể đã biết thay vì trả lời mọi yêu cầu dò của client
D. Tấn công evil twin; nó giả mạo một SSID cụ thể đã biết thay vì trả lời mọi yêu cầu dò của client

---

44. Pentester nhắm vào một access point bật WPS, hy vọng khôi phục mật khẩu WPA2. Tấn công nào khai thác việc sinh số ngẫu nhiên yếu ở các nonce E-S1/E-S2 của enrollee trên một số chipset, cho phép tính mã PIN WPS offline trong vài giây thay vì brute-force online?

A tester targets an access point with WPS enabled, hoping to recover the WPA2 passphrase. Which attack exploits weak random number generation in certain chipsets' E-S1/E-S2 enrollee nonces, allowing the WPS PIN to be computed offline in seconds rather than brute-forced online?

A. Tấn công PMKID vào RSN IE
B. Brute-force PIN WPS online bằng Reaver
C. Tấn công KRACK vào four-way handshake
D. Tấn công Pixie Dust

---

45. Một pentester được ủy quyền đánh giá mạng WPA2-PSK của công ty và muốn bắt four-way handshake để tấn công từ điển offline. Kỹ thuật nào được dùng PHỔ BIẾN NHẤT để ép một client đang kết nối xác thực lại, từ đó bắt được handshake?

A penetration tester has authorization to assess a corporate WPA2-PSK network and wants to capture the four-way handshake for an offline dictionary attack. Which technique is MOST commonly used to force a connected client to reauthenticate so the handshake can be captured?

A. Gửi khung deauthentication bằng aireplay-ng
B. Hạ cấp kết nối bằng proxy SSL strip
C. Đầu độc bộ đệm ARP của client
D. Gửi phản hồi DNS giả mạo cho client

---

46. Một pentester dựng rogue access point phát cùng SSID với mạng công ty hợp pháp để dụ nhân viên kết nối và chặn thông tin đăng nhập của họ. Đây là tấn công nào?

A penetration tester sets up a rogue access point broadcasting the same SSID as a legitimate corporate network to lure employees into connecting so their credentials can be intercepted. Which attack does this describe?

A. Tấn công evil twin
B. Tấn công ARP spoofing
C. Tấn công bluejacking
D. Tấn công PIN WPS

---

47. Một chuyên gia đánh giá bẻ khóa WEP cũ trong vài phút bằng cách thu một lượng lớn lưu lượng và phân tích các mẫu initialization vector lặp lại dùng với mật mã RC4. Lỗi thiết kế cơ bản nào của WEP bị khai thác?

An assessor cracks a legacy WEP key in minutes by collecting a large volume of traffic and analyzing patterns of repeated initialization vectors used with the RC4 cipher. Which fundamental design flaw in WEP does this exploit?

A. SAE cho phép kẻ tấn công hạ cấp trao đổi xuống bộ mã yếu hơn
B. Kiểm tra toàn vẹn Michael của TKIP có thể bị vượt bằng tấn công chopchop
C. Four-way handshake hoàn toàn không có mã toàn vẹn thông điệp
D. Không gian IV 24 bit quá nhỏ, khiến keystream thường xuyên bị trùng

---

48. Trong tấn công social engineering không dây nào, rogue access point trả lời "có" cho probe request của BẤT KỲ SSID nào trong danh sách mạng ưa thích của client gần đó, thay vì giả mạo một mạng cụ thể đã biết?

Which wireless social-engineering attack causes a rogue access point to respond affirmatively to probe requests for ANY SSID contained in a nearby client's preferred network list, rather than impersonating one specific known network?

A. Tấn công Karma
B. Tấn công rogue DHCP
C. Tấn công evil twin
D. Tấn công deauthentication

---

49. Một nhà nghiên cứu công bố lỗ hổng cho phép kẻ tấn công ở vị trí man-in-the-middle thao túng việc truyền lại handshake và ép cài lại khóa mã hóa đã dùng, giúp giải mã lưu lượng client mà không biết mật khẩu. Cuộc tấn công này gọi là gì?

A researcher discloses a vulnerability that allows an attacker positioned as a man-in-the-middle to manipulate handshake retransmissions and force reinstallation of an already-used encryption key, enabling decryption of client traffic without knowing the passphrase. What is this attack called?

A. Tấn công evil twin
B. Tấn công brute-force PIN WPS
C. Tấn công PMKID
D. Tấn công KRACK

---

50. Một mạng phát WPA3-Personal ở "transition mode" để tương thích với client WPA2 cũ. Cấu hình này tạo ra rủi ro nào?

A network broadcasts WPA3-Personal in 'transition mode' to maintain compatibility with legacy WPA2 clients. Which risk does this configuration introduce?

A. Kẻ tấn công có thể ép client hạ cấp xuống handshake WPA2 yếu hơn, cho phép tấn công từ điển offline truyền thống
B. AP phát PSK ở dạng văn bản rõ để giữ tương thích ngược
C. Bằng chứng zero-knowledge của SAE bị tắt hoàn toàn với mọi client kết nối
D. Protected Management Frames 802.11w chỉ bắt buộc với client WPA3, loại bỏ rủi ro deauth cho client WPA2

Mật mã học

51. Một pentester phát hiện ứng dụng web trả về thông báo lỗi khác nhau cho padding không hợp lệ so với MAC không hợp lệ khi gửi một cookie mã hóa CBC đã bị sửa. Hành vi này cho phép tấn công nào?

A penetration tester discovers that a web application returns distinct error messages for invalid padding versus invalid MAC when a modified CBC-encrypted cookie is submitted. Which attack does this behavior enable?

A. Tấn công chosen-plaintext
B. Tấn công meet-in-the-middle
C. Tấn công padding oracle
D. Tấn công birthday

---

52. Trong một đợt đánh giá không dây, pentester bắt 4-way handshake WPA2 bằng airodump-ng sau khi deauth một client bằng aireplay-ng. Tiếp theo pentester NHIỀU KHẢ NĂNG NHẤT sẽ dùng công cụ nào để khôi phục khóa chia sẻ trước (pre-shared key) offline?

During a wireless assessment, a tester captures a WPA2 4-way handshake using airodump-ng after deauthenticating a client with aireplay-ng. Which tool would the tester MOST likely use next to recover the pre-shared key offline?

A. sqlmap
B. Responder
C. hashcat
D. Mô-đun psexec của Metasploit

---

53. Pentester phát hiện một máy chủ web cũ vẫn chấp nhận kết nối SSLv3 dù cũng hỗ trợ TLS 1.2. Tấn công nào trở nên khả thi với các client có thể bị ép lùi về SSLv3?

A tester discovers that a legacy web server still accepts SSLv3 connections even though it also supports TLS 1.2. Which attack becomes feasible against clients that can be forced to fall back to SSLv3?

A. Heartbleed
B. POODLE
C. BEAST
D. CRIME

---

54. Pentester quan sát lưu lượng mạng cho thấy trao đổi khóa Diffie-Hellman giữa client và server. Điều kiện nào khiến việc khôi phục bí mật chung bằng tấn công tính sẵn kiểu Logjam trở nên khả thi?

A tester observes network traffic showing a Diffie-Hellman key exchange between a client and server. Which condition would make the shared secret feasibly recoverable via a precomputed, logjam-style attack?

A. Chứng chỉ của máy chủ dùng khóa ký RSA 2048 bit
B. Máy chủ thương lượng một nhóm DH 512 bit hoặc 1024 bit được dùng lại phổ biến
C. Máy chủ dùng ECDHE với đường cong P-256
D. Client và server thương lượng bộ mã AES-256-GCM

---

55. Loại mã hóa nào dùng cùng một khóa để vừa mã hóa vừa giải mã dữ liệu?

Which type of encryption uses the same key for both encrypting and decrypting data?

A. Mã hóa bất đối xứng (asymmetric)
B. Mã hóa đối xứng (symmetric)
C. Chữ ký số
D. Hàm băm (hashing)

---

56. Một người dùng muốn ký số một email để người nhận có thể xác minh cả danh tính người gửi lẫn việc nội dung không bị thay đổi trên đường truyền. Quy trình nào mô tả TỐT NHẤT cách tạo chữ ký?

A user wants to digitally sign an email so the recipient can verify both the sender's identity and that the message was not altered in transit. Which process BEST describes how the signature is generated?

A. Mã hóa bản tóm tắt thông điệp (message digest) bằng khóa đối xứng dùng chung
B. Mã hóa toàn bộ thông điệp bằng khóa công khai của người nhận
C. Băm thông điệp, rồi mã hóa giá trị băm bằng khóa riêng của người gửi
D. Băm thông điệp, rồi mã hóa giá trị băm bằng khóa công khai của người nhận

---

57. Một chuyên gia kiểm tra mạng không dây thu được một giá trị băm PMKID trực tiếp từ khung EAPOL đầu tiên của access point, mà không cần thấy client hoàn tất 4-way handshake và không cần tấn công deauthentication. Đây là kỹ thuật tấn công WPA2-PSK nào?

A wireless auditor captures a single PMKID hash directly from an access point's first EAPOL frame without observing a client complete the 4-way handshake or performing a deauthentication attack. Which WPA2-PSK attack technique does this describe?

A. Tấn công evil twin
B. Tấn công brute-force mã PIN WPS
C. Tấn công cài đặt lại khóa KRACK
D. Tấn công offline dựa trên PMKID

---

58. Trong một đợt đánh giá an ninh mạng, một kỹ sư thấy hai máy (host) thiết lập một khóa bí mật chung qua kênh không an toàn mà không hề truyền chính khóa đó. Đây là cơ chế mật mã nào?

During a network security assessment, an engineer observes two hosts establishing a shared secret key over an insecure channel without ever transmitting the key itself. Which cryptographic mechanism does this describe?

A. Chữ ký số RSA
B. Mã hóa AES-256
C. Xác thực HMAC
D. Trao đổi khóa Diffie-Hellman

---

59. Một CISO yêu cầu rằng nếu khóa riêng RSA dài hạn của máy chủ web bị lộ trong tương lai thì cũng không được giải mã được lưu lượng TLS đã bị ghi lại trước đó. Cơ chế trao đổi khóa nào đáp ứng yêu cầu này?

A CISO mandates that a future compromise of the web server's long-term RSA private key must not allow decryption of previously captured TLS traffic. Which key exchange mechanism satisfies this requirement?

A. Trao đổi vé Kerberos
B. Trao đổi khóa chia sẻ trước (pre-shared key) không có thành phần tạm thời
C. Diffie-Hellman tạm thời (DHE hoặc ECDHE)
D. Trao đổi khóa RSA tĩnh

---

60. Một kiến trúc sư bảo mật cần chọn độ dài khóa RSA có độ mạnh mật mã xấp xỉ khóa đối xứng 128 bit, theo khuyến nghị NIST SP 800-57. Nên chọn độ dài khóa nào?

A security architect needs an RSA key size that provides cryptographic strength roughly equivalent to a 128-bit symmetric key, per NIST SP 800-57 recommendations. Which key length should be selected?

A. 3072 bit
B. 2048 bit
C. 1024 bit
D. 15360 bit

Tổng quan ethical hacking

61. Trong giai đoạn trước khi tấn công, một người kiểm thử chạy “nmap -sV -p 445 10.10.10.5” và xác nhận cổng SMB đang mở cùng thông tin phiên bản. Để lấy tên thư mục chia sẻ (share), danh sách tài khoản người dùng và thông tin null session, người kiểm thử nên thực hiện giai đoạn nào TIẾP THEO của phương pháp luận?

During a pre-attack phase, a tester runs 'nmap -sV -p 445 10.10.10.5' and confirms an open SMB port with version information. To extract share names, user account listings, and null session details, the tester should NEXT perform which phase of the methodology?

A. Lấy banner (banner grabbing)
B. Liệt kê (enumeration)
C. Trinh sát chủ động (active reconnaissance)
D. Quét lỗ hổng (vulnerability scanning)

---

62. Thuật ngữ nào chỉ một chuyên gia bảo mật được tổ chức cho phép kiểm thử hệ thống của họ để tìm lỗ hổng, bằng những kỹ thuật giống kẻ tấn công độc hại?

Which term describes a security professional who is authorized by an organization to test its systems for vulnerabilities using the same techniques as malicious attackers?

A. Hacker mũ đen (black hat)
B. Hacker mũ trắng (white hat)
C. Hacker mũ xám (gray hat)
D. Script kiddie

---

63. Kẻ tấn công làm ngập máy chủ web đặt lịch khám của một bệnh viện bằng các gói TCP SYN dị dạng, khiến nhân viên hợp pháp không truy cập được hệ thống trong sáu giờ. Thành phần nào của bộ ba CIA bị ảnh hưởng CHỦ YẾU bởi cuộc tấn công này?

An attacker floods a hospital's patient-scheduling web server with malformed TCP SYN packets, preventing legitimate staff from accessing the system for six hours. Which component of the CIA triad is PRIMARILY compromised by this attack?

A. Tính toàn vẹn (Integrity)
B. Tính sẵn sàng (Availability)
C. Tính bí mật (Confidentiality)
D. Chống chối bỏ (Non-repudiation)

---

64. Trong một đợt kiểm thử được ủy quyền, người kiểm thử dùng Nmap để xác định các cổng mở, dịch vụ đang chạy và phiên bản hệ điều hành trên toàn mạng con mục tiêu, trước khi thử khai thác bất kỳ điểm yếu nào. Hoạt động này thuộc giai đoạn nào của quy trình hacking?

During an authorized engagement, a tester uses Nmap to identify open ports, running services, and operating system versions across a target subnet before attempting any exploitation. Which phase of the hacking methodology does this activity represent?

A. Duy trì truy cập (maintaining access)
B. Trinh sát (reconnaissance)
C. Quét và liệt kê (scanning and enumeration)
D. Giành quyền truy cập (gaining access)

---

65. Một nhà nghiên cứu bảo mật, tự hành động mà không có hợp đồng nào, phát hiện lỗi stored XSS trên cổng đăng nhập công khai của một công ty chỉ nhờ duyệt trang đó. Cô không khai thác lỗi thêm và báo riêng cho đội bảo mật của nhà cung cấp. Cách phân loại người này ĐÚNG NHẤT là:

A security researcher, acting on her own without any contract, discovers a stored XSS flaw on a company's public login portal simply by browsing it. She does not exploit the flaw further and privately discloses it to the vendor's security team. This individual is BEST classified as a:

A. Hacktivist
B. Hacker mũ xám (gray hat)
C. Suicide hacker
D. Hacker mũ trắng (white hat)

---

66. Một tổ chức muốn đo SOC của mình phát hiện và phản ứng nhanh đến đâu trước một cuộc xâm nhập mô phỏng kín đáo, nhiều giai đoạn, mà không báo trước cho bên phòng thủ và không cố liệt kê mọi lỗ hổng trong phạm vi. Cách gọi ĐÚNG NHẤT cho hoạt động này là:

An organization wants to measure how quickly its SOC detects and responds to a stealthy, multi-stage simulated intrusion, without alerting defenders beforehand and without attempting to catalog every vulnerability in scope. This engagement is BEST described as a:

A. Chương trình bug bounty
B. Kiểm thử xâm nhập (penetration test)
C. Đánh giá lỗ hổng (vulnerability assessment)
D. Hoạt động red team (red team engagement)

---

67. Một văn bản đã ký giữa công ty pentest và khách hàng quy định phương pháp kiểm thử cụ thể, khung giờ được phép kiểm thử, quy trình báo cáo khẩn cấp lên các đầu mối liên hệ, và loại trừ rõ ràng cổng thanh toán đang vận hành (production) khỏi phạm vi kiểm thử. Văn bản này ĐÚNG NHẤT là loại nào?

A signed document between a pentest firm and its client defines the exact testing methodology, permitted testing windows, emergency contact escalation procedures, and an explicit exclusion of the production payment gateway from testing. This document is BEST classified as the:

A. Thỏa thuận dịch vụ khung (Master Service Agreement, MSA)

B. Thỏa thuận bảo mật thông tin (Non-Disclosure Agreement, NDA)

C. Quy tắc thực hiện kiểm thử (Rules of Engagement, ROE)

D. Bản mô tả công việc (Statement of Work, SOW)

---

68. Trong một đợt kiểm thử xâm nhập bên ngoài được ủy quyền, người kiểm thử tìm thấy thông tin đăng nhập trên máy chủ web của khách hàng, và thông tin này cũng đăng nhập thành công vào một nền tảng SaaS của bên thứ ba không hề có trong văn bản phạm vi đã ký. Hành động ĐẦU TIÊN phù hợp NHẤT của người kiểm thử là gì?

During an authorized external penetration test, a tester discovers credentials on the client's web server that also successfully authenticate to a third-party SaaS platform not listed anywhere in the signed scope document. What is the tester's MOST appropriate FIRST action?

A. Bỏ phát hiện này khỏi báo cáo cuối vì hệ thống của bên thứ ba nằm ngoài phạm vi đã ký

B. Thử ngay thông tin đăng nhập trên nền tảng bên thứ ba để xác nhận có khai thác được không

C. Dừng lại, không kiểm thử hệ thống bên thứ ba, và báo phát hiện cho khách hàng theo quy trình báo cáo sự cố trong ROE

D. Khai thác nền tảng bên thứ ba vừa đủ để chứng minh tác động, rồi dừng

---

69. Một người kiểm thử xâm nhập chạy “nmap -sV -p445 10.0.5.20” và sau khi thấy cổng mở thì dùng “enum4linux” để lấy tên share và danh sách tài khoản người dùng từ máy đó. Chuỗi hành động này thể hiện hai giai đoạn nào của phương pháp luận ethical hacking?

A penetration tester runs 'nmap -sV -p445 10.0.5.20' and, after finding the port open, uses 'enum4linux' to pull share names and user account listings from the host. Which two phases of the ethical hacking methodology does this sequence of actions represent?

A. Thu thập dấu vết (footprinting) rồi xóa dấu vết (covering tracks)

B. Liệt kê (enumeration) rồi duy trì truy cập (maintaining access)

C. Trinh sát (reconnaissance) rồi giành quyền truy cập (gaining access)

D. Quét (scanning) rồi liệt kê (enumeration)

---

70. Một người kiểm thử xâm nhập tìm trên Shodan.io để xác định các thiết bị nối Internet của tổ chức mục tiêu, mà không gửi bất kỳ gói tin nào trực tiếp vào mạng của mục tiêu. Hoạt động này là ví dụ của:

A penetration tester searches Shodan.io to identify internet-facing devices belonging to the target organization, without sending any packets directly to the target's network. This activity is an example of:

A. Quét lỗ hổng (vulnerability scanning)

B. Trinh sát chủ động (active reconnaissance)

C. Trinh sát thụ động (passive reconnaissance)

D. Liệt kê (enumeration)

Đáp án đúng

1. C Kerberoasting dùng thông tin đăng nhập domain hợp lệ để xin service ticket của các tài khoản có SPN, rồi bẻ khóa offline phần được mã hóa bằng khóa của tài khoản dịch vụ. Ticket RC4 dùng NTLM hash làm khóa, ticket AES dùng khóa AES sinh từ mật khẩu. AS-REP roasting nhắm vào tài khoản tắt Kerberos pre-authentication và không cần thông tin đăng nhập hợp lệ. Golden ticket giả mạo TGT bằng hash krbtgt. Pass-the-ticket chỉ dùng lại ticket đã đánh cắp, không bẻ khóa.

2. A Pass-the-hash đưa chính hash đã bắt được làm bằng chứng danh tính, vì NTLM không cần mật khẩu gốc khi xác thực. Kerberoasting nhắm vào service ticket Kerberos để bẻ khóa offline, không dùng lại hash. Golden ticket giả mạo TGT bằng hash krbtgt. Đầu độc LLMNR/NBT-NS chỉ bắt hash bằng cách giả mạo phân giải tên, không phải dùng lại hash đã có.

3. A Lệnh đúng dùng -m 1000 (NTLM), -a 3 (tấn công theo mặt nạ, mask attack) và mặt nạ ?u?l?l?l?l?l?d?d: một chữ hoa, năm chữ thường, hai chữ số. Mặt nạ có chữ hoa ở vị trí thứ sáu là sai vị trí. -a 0 là tấn công từ điển, cần wordlist chứ không dùng mặt nạ. -m 1800 là sha512crypt, không phải NTLM.

4. D NTFS lưu dữ liệu của luồng ẩn tách riêng khỏi luồng chính, nên danh sách thư mục và dung lượng Explorer hiển thị cho notes.txt không tính phần ẩn. Muốn thấy phải dùng dir /r hoặc công cụ streams của Sysinternals. ADS chỉ có trên NTFS, không có trên FAT32 hay ext4, và không tự mã hóa bằng EFS. Các AV/EDR hiện đại vẫn quét được ADS.

5. B Tệp SUID chạy với UID hiệu lực của chủ sở hữu, nên find SUID root có thể chạy lệnh bất kỳ với quyền root, ví dụ find . -exec /bin/sh -p \; -quit, cho root shell ngay. Thay tệp find cần quyền ghi mà người dùng quyền thấp thường không có. find không tự cấp quyền ghi /etc/passwd. Tìm ra tệp /etc/shadow không có nghĩa là đọc được nội dung, và có hash rồi vẫn phải bẻ khóa thêm.

6. A Thay các tệp hệ thống như ps, ls, netstat bằng bản trojan để che dấu vết là hành vi điển hình của userland rootkit (rootkit ở tầng ứng dụng). Kernel-mode rootkit cũng che giấu nhưng bằng cách hook system call hoặc sửa cấu trúc dữ liệu kernel, không thay tệp ở user space. Trojan horse là mã độc giả dạng phần mềm hợp lệ. Logic bomb chỉ kích hoạt khi có điều kiện và không có chức năng che giấu.

7. C Xóa log Security bằng wevtutil tự sinh Event ID 1102, “The audit log was cleared”, là một trong số ít mục còn lại trong log vừa bị xóa, giúp SOC hoặc SIEM phát hiện ngay. Tệp Prefetch của wevtutil.exe không tự bị xóa, ngược lại còn là dấu vết thêm. Log System cũng xóa được bằng wevtutil cl System. $MFT không bất biến và cũng không phải nguồn chính để phát hiện việc xóa log.

8. A Rainbow table dùng các chuỗi hash tính sẵn, ánh xạ tới mật khẩu ứng viên, nên tra cứu nhanh mà không phải tính hash lại, đổi dung lượng lưu trữ lấy tốc độ. Tấn công từ điển băm danh sách từ ngay lúc chạy. Brute-force thử mọi tổ hợp ký tự, chậm và không dựa trên bảng. Kerberoasting lấy ticket dịch vụ trong Active Directory, không phải cách tra hash. Thêm salt là một cách phòng chống.

9. B Golden ticket giả mạo TGT cho cả domain bằng hash krbtgt, cho kẻ tấn công quyền truy cập lâu dài, gần như không giới hạn, cho đến khi krbtgt được đổi hai lần. Silver ticket chỉ giả mạo TGS cho một dịch vụ bằng hash tài khoản dịch vụ, phạm vi hẹp hơn. DCSync lạm dụng quyền replication để lấy hash. Pass-the-hash dùng lại hash NTLM, không giả mạo ticket Kerberos.

10. C HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute chạy các ứng dụng native trước khi Windows subsystem nạp, trong giai đoạn khởi tạo Session Manager (SMSS.exe). Giá trị mặc định là 'autocheck autochk *' để kiểm tra đĩa. Sysinternals Autoruns liệt kê được BootExecute. Khóa Run chạy lúc đăng nhập, Userinit điều khiển khởi tạo đăng nhập, User Shell Folders chỉ chứa đường dẫn thư mục shell.

11. A Theo RFC 5321, máy chủ thư chọn bản ghi MX có số priority thấp nhất trước, chỉ chuyển sang số cao hơn khi máy ưu tiên không liên lạc được. Vì vậy 10 được ưu tiên hơn 20. Đáp án đảo ngược quy tắc này là bẫy quen thuộc. MX là thứ tự ưu tiên chặt chẽ, không chia tải đều, trừ khi hai bản ghi có cùng giá trị. DNS không dùng thứ tự bảng chữ cái.

12. D Traceroute vẽ đường đi từng chặng của gói tin tới mục tiêu, lộ ra router, ISP và ranh giới tường lửa hoặc load balancer, nên thuộc network footprinting. Nó không thụ động vì gửi gói tin TTL tăng dần thẳng tới IP mục tiêu. Nó không phải footprinting bằng social engineering (tấn công phi kỹ thuật), vốn thu thập thông tin từ con người, cũng không phải footprinting DNS, vốn dùng bản ghi phân giải tên.

13. A Bản ghi MX (Mail Exchange) liệt kê tên máy và mức ưu tiên của các máy chủ nhận email cho tên miền, cho thấy ngay hạ tầng thư mà kẻ phishing cần giả mạo hoặc nhắm tới. NS chỉ xác định máy chủ tên có thẩm quyền của vùng. SOA chứa dữ liệu quản trị vùng như số serial và chu kỳ làm mới. PTR tra ngược từ IP sang tên máy, không liên quan đường đi của thư.

14. A Yêu cầu zone transfer được gửi thẳng tới máy chủ tên có thẩm quyền của mục tiêu, nơi có thể ghi log, giới hạn tốc độ hoặc cảnh báo, nên đây là trinh sát chủ động dù công cụ chỉ đọc. Trinh sát thụ động dùng nguồn bên thứ ba như WHOIS, bộ nhớ đệm công cụ tìm kiếm, log certificate transparency. Việc phân loại dựa vào sự tương tác, không dựa vào kết quả, nên AXFR thất bại vẫn là chủ động.

15. C Banner grabbing cần mở kết nối TCP trực tiếp tới dịch vụ và đọc phản hồi, tức là tương tác thẳng với hạ tầng mục tiêu, nên là footprinting chủ động. Không thụ động vì hệ thống mục tiêu biết và phản hồi kết nối. Không phải quét lỗ hổng, vốn dò điểm yếu đã biết chứ không chỉ nhận diện phần mềm và phiên bản. Nó vẫn là footprinting, xảy ra ở giai đoạn thu thập thông tin trước enumeration.

16. A Maltego liên kết các thực thể như người, tên miền, email, tổ chức tìm được qua nhiều transform OSINT, rồi hiển thị quan hệ thành đồ thị tương tác, là lựa chọn chuẩn cho phân tích liên kết trực quan khi trinh sát. Nmap là công cụ quét mạng và cổng chủ động, Hydra dò mật khẩu đăng nhập (brute force), Responder đầu độc LLMNR/NBT-NS. Ba công cụ này không vẽ đồ thị OSINT.

17. C Banner grabbing lấy chuỗi chào mà dịch vụ đang mở trả về. Banner SMTP này cho biết phần mềm chuyển thư (Postfix) và tên máy, nhưng không có số phiên bản; banner khác có thể lộ phiên bản. Dải IP phải tra qua ASN hoặc WHOIS. Nhà đăng ký và liên hệ quản trị đến từ WHOIS. Danh sách email nhân viên cần thu thập OSINT riêng.

18. C Truy vấn "site:target.com filetype:conf intext:password" giới hạn kết quả trong tên miền mục tiêu, chỉ lấy tệp .conf đã lập chỉ mục và yêu cầu có 'password' trong nội dung. inurl:admin chỉ lọc đường dẫn có 'admin', không liên quan tệp cấu hình. link: là toán tử đã bị bỏ, từng tìm trang liên kết tới một URL. cache: từng trả về bản lưu của Google, nhưng tính năng này đã bị ngừng.

19. C Tra cứu WHOIS truy vấn các cơ quan đăng ký internet khu vực (ARIN, RIPE...) hoặc nhà đăng ký tên miền để lấy thông tin chủ sở hữu như tên, tổ chức, liên hệ. DNS zone transfer sao chép cả tệp vùng DNS, không phải dữ liệu người đăng ký. Banner grabbing lấy header phản hồi của cổng đang mở. Quét cổng xác định cổng mở, đóng hoặc bị lọc. WHOIS là bước footprinting thụ động cơ bản, làm trước khi tiếp xúc trực tiếp với mục tiêu.

20. B Bộ lọc “country:” thu hẹp kết quả về các thiết bị có vị trí địa lý của IP khớp mã quốc gia hai chữ cái, ví dụ country:US. “geo:” tìm theo tọa độ vĩ độ và kinh độ, không theo tên quốc gia. “org:” tìm theo tổ chức hoặc ISP gắn với IP, không phải vị trí. “hostname:” tìm thiết bị theo chuỗi tên máy, không liên quan quốc gia.

21. A Honeypot tương tác thấp giả lập dịch vụ bằng banner chung đã soạn sẵn và hiếm khi cài đủ logic giao thức, nên phản hồi đồng nhất hoặc không nhất quán và rất nhanh. Máy chủ production đã gia cố sẽ tuân thủ đúng giao thức và thường hạn chế cổng mở. Load balancer chia tải nhưng không tạo banner giống hệt ở nhiều dịch vụ. IPS chặn hoặc reset lưu lượng độc hại, không tạo banner giả.

22. B Phishing dùng email lừa đảo, thường giả danh nguồn đáng tin như bộ phận IT, để dụ nạn nhân bấm liên kết độc hại hoặc nhập thông tin đăng nhập vào trang giả. Vishing dùng cuộc gọi thoại, không dùng email. Pretexting dùng danh tính hoặc kịch bản bịa và cũng có thể qua email, nhưng “Phishing” là đáp án cụ thể nhất cho email dẫn tới trang đăng nhập giả. Tailgating là xâm nhập vật lý.

23. C MAC flooding làm quá tải bảng CAM (content-addressable memory) hữu hạn của switch bằng các mục giả. Khi đầy, nhiều switch rơi vào trạng thái fail-open và phát lưu lượng ra mọi cổng, cho phép nghe lén thụ động trên mạng switch. ARP spoofing thao túng bộ đệm ARP của máy, không phải bảng CAM. VLAN hopping lạm dụng cấu hình trunk sai. DHCP starvation làm cạn dải địa chỉ DHCP.

24. A Ép switch vào chế độ fail-open để phát lưu lượng ra mọi cổng như hub chính là kết quả nghe lén mà MAC flooding hướng tới. Bảng CAM hữu hạn bị tràn, nên khung có MAC đích chưa biết có thể bị phát sang các cổng khác trong cùng VLAN, giúp kẻ tấn công bắt một phần lưu lượng của máy khác. Lưu lượng có đích đã biết vẫn được chuyển bình thường. Làm sập OS, chiếm console hay vượt 802.1X là các hướng khác, không liên quan.

25. B Firewalking dùng kỹ thuật tăng TTL với một gateway đã biết để liệt kê cổng và giao thức mà ACL cho đi qua tường lửa, dựa vào việc có nhận được Time Exceeded từ phía sau tường lửa hay không. Traceroute thông thường chỉ vẽ đường đi, không nhằm tìm quy tắc ACL. Nhận diện OS qua TTL suy ra hệ điều hành từ TTL ban đầu. Banner grabbing lấy chuỗi phiên bản dịch vụ, không liên quan TTL.

26. A Session splicing (còn gọi session slicing) khai thác giới hạn thời gian ghép lại của IDS: payload được nhỏ giọt qua nhiều đoạn TCP rất nhỏ có độ trễ, khiến cảm biến hết thời gian và bỏ ghép trước khi đủ mẫu chữ ký, trong khi máy đích thường có thời gian chờ dài hơn hoặc không có nên vẫn ghép được. Fragmentation overlap dựa vào thứ tự ghép mơ hồ, không dựa thời gian. Firewalking dùng TTL. Mã hóa đa hình đổi mẫu byte.

27. A Piggybacking xảy ra khi người có quyền biết và cho người khác vào (dù tưởng nhầm), như giữ cửa vì nghĩ người đó là đồng nghiệp: có sự đồng ý, dù do bị lừa. Ngược lại, tailgating là người không được phép đi theo qua cửa mà người có quyền không hề biết. Dumpster diving là lục rác lấy tài liệu nhạy cảm, shoulder surfing là nhìn trộm khi ai đó nhập thông tin đăng nhập, cả hai không áp dụng ở đây.

28. B Né bằng phân mảnh chia payload ra nhiều mảnh IP để bộ máy khớp chữ ký không bao giờ thấy trọn dãy byte độc hại trong một gói, nhất là khi IDS ghép mảnh khác với máy đích. Mã hóa che nội dung nhưng không chia mảnh. Flooding làm quá tải tài nguyên chứ không che chữ ký. Spoofing giả địa chỉ nguồn, không đổi cấu trúc payload.

29. A Pretexting là dựng một kịch bản hoặc danh tính giả để tạo lòng tin và khiến mục tiêu làm theo, ví dụ đặt lại mật khẩu. Phishing dùng tin nhắn điện tử lừa đảo (email, SMS), không phải đóng giả trực tiếp. Tailgating là đi theo người có quyền qua cửa an ninh. Baiting dụ bằng mồi vật lý hoặc số, như USB nhiễm mã độc, không có trong tình huống này.

30. C Khi phiên bị chiếm và mất đồng bộ, client và server mỗi bên giữ sequence number mà bên kia không còn coi là hợp lệ. Mỗi gói một bên gửi lại gây ra một ACK từ bên kia chứa số mong đợi, rồi lại bị từ chối, tạo vòng lặp ACK tự duy trì gọi là ACK storm cho đến khi kết nối hết thời gian hoặc bị reset. SYN flood, ARP cache exhaustion và DNS amplification không liên quan mất đồng bộ phiên TCP.

31. B Security misconfiguration gồm các lỗi như thông báo lỗi dài dòng hoặc thông tin debug để bật trên production, làm lộ framework và phiên bản giúp kẻ tấn công nhận diện stack và nhắm vào lỗ hổng đã biết; cách sửa là tắt chế độ debug và trả trang lỗi chung. Không phải Injection vì không có đầu vào nào làm đổi lệnh hay truy vấn. Không liên quan đăng nhập hay phiên, cũng không có mã hóa yếu.

32. A Thêm ký tự đặc biệt của shell như dấu chấm phẩy để nối một lệnh hệ thống tùy ý vào lệnh ping là dấu hiệu điển hình của OS command injection, cho phép chạy lệnh với quyền của tiến trình web server. XSS nhắm vào trình duyệt nạn nhân, không phải shell máy chủ. SQL injection thao túng cú pháp truy vấn cơ sở dữ liệu. Insecure deserialization khai thác việc dựng lại đối tượng tuần tự hóa không an toàn.

33. A Reflected XSS xảy ra khi đầu vào được phản chiếu ngay trong phản hồi của máy chủ mà không được lưu lại; nạn nhân tự kích hoạt khi bấm liên kết được chế sẵn hoặc gửi biểu mẫu độc hại, nên gọi là loại không lưu trữ (non-persistent). Stored XSS lưu payload phía máy chủ, ví dụ trong cơ sở dữ liệu, và chạy với mọi người xem trang. DOM-based XSS nằm hoàn toàn trong JavaScript phía client. Blind XSS kích hoạt ở nơi attacker không thấy, như trang quản trị.

34. A Lỗ hổng insecure deserialization xuất hiện khi ứng dụng giải tuần tự hóa đầu vào không tin cậy mà không giới hạn lớp cho phép hay xác minh toàn vẹn, cho kẻ tấn công đưa vào gadget chain: chuỗi các lớp hợp lệ mà tác dụng phụ khi nối nhau lúc giải tuần tự hóa dẫn tới chạy mã. Độ mạnh TLS ảnh hưởng bảo mật đường truyền. Lưu phiên ở client là lựa chọn thiết kế khác. Thiếu HttpOnly chỉ giúp trộm cookie qua XSS.

35. D SSRF xảy ra khi chính máy chủ bị ép gửi yêu cầu tới đích do kẻ tấn công chọn, ở đây là dịch vụ metadata nội bộ vốn không truy cập được từ internet công cộng. XSS chạy trong trình duyệt nạn nhân, không phải trên máy chủ gửi yêu cầu ra ngoài. IDOR (insecure direct object reference) là truy cập trái phép đối tượng qua mã định danh bị sửa, không phải tải URL tùy ý. Path traversal dùng chuỗi đường dẫn để thoát khỏi thư mục, không gửi yêu cầu HTTP từ xa.

36. C Insecure deserialization xảy ra khi dữ liệu tuần tự hóa không tin cậy được dựng lại thành đối tượng mà không kiểm tra kiểu hay tính toàn vẹn, cho đối tượng chế sẵn kích hoạt đường chạy mã ngoài ý muốn, thường qua gadget chain có sẵn trên classpath, dẫn tới thực thi mã từ xa. CSRF giả mạo một yêu cầu đã xác thực. Broken access control là lỗi phân quyền. Clickjacking là tấn công che giao diện bằng khung trong suốt.

37. B Session fixation xảy ra khi kẻ tấn công ép hoặc cung cấp một session ID đã biết cho nạn nhân trước khi xác thực, và ứng dụng không cấp ID mới sau khi đăng nhập thành công, nên kẻ tấn công dùng lại ID đó để vào phiên đã xác thực. Chiếm phiên bằng nghe lén phải chặn token đang truyền, không đặt sẵn. CSRF và clickjacking không gán sẵn session ID. Cách sửa là luôn tạo lại session ID khi quyền thay đổi, ví dụ lúc đăng nhập.

38. A Proxy của Burp Suite nằm giữa trình duyệt và ứng dụng đích, bắt và cho phép sửa thủ công hoặc tự động các yêu cầu, phản hồi HTTP và HTTPS đang chạy, rất cần để kiểm thử injection, xác thực và lỗi logic nghiệp vụ. Nmap là công cụ quét mạng và cổng, không phải proxy HTTP. Hashcat bẻ khóa mật khẩu từ hash đã bắt. Wireshark bắt và phân tích gói tin thụ động, không sửa yêu cầu đang chạy.

39. B Payload '{{7*7}}' hiển thị thành '49' là phép thử chuẩn cho SSTI trong Jinja2, template engine mặc định của Flask: đầu vào bị phân tích và tính như cú pháp template thay vì dữ liệu thường. Reflected XSS sẽ hiện thành script hoặc HTML chạy trong trình duyệt, không tính toán phía máy chủ. Template injection của AngularJS là bề mặt phía client, khác với backend Flask. SQL injection nằm trong truy vấn cơ sở dữ liệu. SSTI có thể leo thành RCE nếu thoát được sandbox.

40. B SQL injection xảy ra khi đầu vào chứa ký tự đặc biệt của SQL (', --, OR 1=1) được nối thẳng vào chuỗi truy vấn, đổi logic để vượt xác thực hoặc lấy cắp dữ liệu. XSS chèn script vào đầu ra của trình duyệt, không vào truy vấn cơ sở dữ liệu. CSRF ép trình duyệt người dùng đã xác thực gửi yêu cầu ngoài ý muốn, không sửa truy vấn. SSRF khiến máy chủ gửi yêu cầu tới đích ngoài ý muốn, không thao túng SQL.

41. D 802.11w bảo vệ bằng mật mã các khung quản lý quan trọng, gồm khung deauthentication và disassociation unicast và broadcast, giúp chống giả mạo các khung này nhắm vào các kết nối đã được bảo vệ. Nó không làm khóa PSK khó bẻ offline hơn, vì điểm yếu nằm ở mật khẩu, không ở lớp khung quản lý. Brute-force WPS nhắm vào cơ chế PIN riêng không bị PMF ảnh hưởng. Rogue DHCP hoạt động ở tầng trên lớp MAC 802.11.

42. C Tấn công PMKID không cần client: chính AP để lộ PMKID trong RSN information element ở thông điệp 1 (M1) của 4-way handshake, nên pentester chỉ cần thấy AP, không cần client đang kết nối. Bắt handshake bằng deauth cần có client và client phải xác thực lại. Brute-force WPS nhắm vào cơ chế PIN riêng, không phải PSK. ARP spoofing là kỹ thuật man-in-the-middle, không phải cách lấy thông tin xác thực.

43. D Evil twin bắt chước một SSID mục tiêu đã biết để client tưởng đang vào mạng công ty thật. Ngược lại, Karma lắng nghe probe request và trả lời động bằng bất kỳ SSID nào client đang tìm, giả mạo mọi mạng trong danh sách mạng ưa thích của client thay vì một tên cố định. Deauthentication là kỹ thuật gây gián đoạn riêng, đôi khi đi kèm cả hai nhưng không khớp mô tả đề bài.

44. D Pixie Dust khai thác các AP dùng WPS với bộ sinh số ngẫu nhiên dễ đoán hoặc entropy thấp cho nonce E-S1/E-S2, dùng để chứng minh biết PIN. Vì nonce yếu, chỉ cần bắt một lần trao đổi WPS là có thể brute-force PIN offline trong vài giây đến vài phút, thay vì hàng giờ khi làm online. Brute-force online của Reaver bị giới hạn tốc độ và dễ bị phát hiện, khóa. PMKID nhắm vào xác thực WPA2-PSK, không liên quan WPS. KRACK khai thác việc cài lại khóa trong handshake.

45. A Khung deauthentication giả địa chỉ MAC của AP và báo client ngắt kết nối; khi client tự kết nối lại, four-way handshake được gửi lại và có thể bắt bằng công cụ như airodump-ng, rồi bẻ khóa offline bằng hashcat hoặc aircrack-ng. ARP poisoning và DNS spoofing là kỹ thuật MITM ở tầng 2 và 3, không ép xác thực lại không dây. SSL stripping nhắm vào HTTPS, không phải trao đổi khóa WPA2. Deauth hiệu quả vì khung quản lý 802.11 trong WPA2 không được xác thực; 802.11w (PMF) khắc phục điểm yếu này.

46. A Evil twin dựng một rogue access point bắt chước SSID, và thường cả BSSID, của mạng hợp pháp để người dùng kết nối vào, từ đó bắt lưu lượng và thông tin đăng nhập; thường đi kèm khung deauth để đẩy client khỏi AP thật. ARP spoofing là kỹ thuật tầng 2 nhắm vào máy đã ở trong mạng, không giả mạo AP. Tấn công PIN WPS brute-force AP thật, không dùng AP giả. Bluejacking gửi tin không mong muốn qua Bluetooth, không liên quan SSID Wi-Fi.

47. D IV 24 bit của WEP chỉ có khoảng 16.7 triệu giá trị, trên mạng bận sẽ bị dùng lại (trùng) trong vài giờ; các trùng lặp bắt được cho phép công cụ như aircrack-ng khôi phục khóa RC4 bằng thống kê qua tấn công FMS hoặc PTW. TKIP và kiểm tra Michael là lớp giảm thiểu của WPA, không phải WEP. Tấn công hạ cấp SAE thuộc WPA3. WEP có cơ chế toàn vẹn (ICV), chỉ là yếu về mật mã, không phải không có.

48. A Tấn công Karma, dựa trên bộ công cụ KARMA gốc, theo dõi các directed probe request mà client gần đó phát đi để tìm SSID lưu trong danh sách mạng ưa thích, rồi trả lời các yêu cầu đó, có thể khiến client tự động kết nối với rogue AP. Evil twin thì giả mạo một mạng hợp pháp cụ thể; mạng đó không cần đang hiện diện và không bắt buộc sao chép BSSID. Deauth chỉ ngắt client, không thu probe. Rogue DHCP hoạt động sau khi kết nối.

49. D Key Reinstallation Attack (KRACK) khai thác four-way handshake của WPA2 bằng cách phát lại thông điệp 3, lừa client đặt lại nonce và cài lại khóa phiên đang dùng, làm keystream bị đặt lại và cho phép giải mã hoặc phát lại gói tin. Nó không cần và không lộ mật khẩu, khác với PMKID và tấn công từ điển. Evil twin là AP giả kiểu social engineering, còn brute-force WPS nhắm vào cơ chế PIN 8 chữ số không liên quan.

50. A Transition mode quảng bá cả bảo mật WPA2 và WPA3 trong cùng beacon, và nghiên cứu về các tấn công hạ cấp kiểu Dragonblood cho thấy rogue AP hoặc kẻ tấn công trên đường truyền có thể ép client hỗ trợ cả hai kết nối bằng 4-way handshake WPA2 cũ, rồi bắt và bẻ từ điển offline như trên mạng WPA2 thuần. SAE vẫn hoạt động đầy đủ với client kết nối bằng WPA3; PSK không bao giờ được phát văn bản rõ; PMF thường chỉ tùy chọn với phía WPA2, nên rủi ro deauth vẫn còn.

51. C Padding oracle khai thác việc ứng dụng để lộ padding sau giải mã có hợp lệ hay không, cho phép khôi phục bản rõ của CBC từng byte mà không cần khóa (ví dụ POODLE, tấn công gốc của Vaudenay). Tấn công birthday nhắm vào va chạm hash, không phải kiểm tra padding. Meet-in-the-middle tính từ hai phía để tìm giá trị trung gian khớp nhau, không liên quan thông báo lỗi lộ ra. Chosen-plaintext cần kẻ tấn công điều khiển việc mã hóa, không phải quan sát lỗi giải mã.

52. C hashcat hỗ trợ mode 22000 (WPA-PBKDF2-PMKID+EAPOL) để bẻ khóa offline handshake WPA2 bằng GPU với wordlist, là bước tiếp theo chuẩn sau khi bắt được. Responder dùng để đầu độc LLMNR/NBT-NS trên mạng có dây hoặc mạng cục bộ, không bẻ handshake. sqlmap tự động khai thác SQL injection. Mô-đun psexec của Metasploit thực thi mã từ xa đã xác thực, không khôi phục mật khẩu từ handshake. Phải có ủy quyền kiểm thử mạng trước khi bắt hay bẻ khóa.

53. B POODLE, tức Padding Oracle On Downgraded Legacy Encryption, khai thác việc SSLv3 kiểm tra padding CBC không xác định sau khi kẻ tấn công ép hạ cấp giao thức, cho phép khôi phục bản rõ từng byte. Heartbleed là lỗi đọc vượt bộ nhớ trong phần mở rộng heartbeat của OpenSSL, không liên quan hạ cấp giao thức. CRIME khai thác nén ở tầng TLS để lộ bí mật, không cần lùi về SSLv3. BEAST nhắm vào điểm yếu chuỗi CBC trong TLS 1.0. Tắt hẳn SSLv3 là cách giảm thiểu chuẩn.

54. B Tấn công kiểu Logjam khai thác việc nhiều máy chủ dùng lại một số ít số nguyên tố DH chuẩn. Kẻ tấn công có nguồn lực cấp quốc gia có thể tính sẵn bảng logarit rời rạc cho các nhóm 512 bit và 1024 bit dùng chung này, rồi khôi phục khóa gần như theo thời gian thực. ECDHE với P-256 chưa có cách phá tính sẵn tương tự. AES-256-GCM là mã đối xứng, không thuộc trao đổi DH. Khóa ký RSA chỉ ảnh hưởng xác thực chứng chỉ.

55. B Mã hóa đối xứng (ví dụ AES, DES, 3DES) dùng một khóa bí mật chung cho cả mã hóa và giải mã, nên nhanh nhưng cần phân phối khóa an toàn. Mã hóa bất đối xứng dùng cặp khóa công khai và riêng, mỗi phép toán dùng khóa khác nhau. Hàm băm là hàm một chiều tạo ra giá trị độ dài cố định và không đảo ngược được, nên không thể “giải mã”. Chữ ký số dựa trên khóa bất đối xứng để chứng minh tính xác thực và toàn vẹn, không mã hóa dữ liệu bằng một khóa chung.

56. C Chữ ký số (digital signature) được tạo bằng cách băm thông điệp thành một giá trị băm (digest), rồi mã hóa giá trị đó bằng khóa riêng của người gửi. Người nhận giải mã bằng khóa công khai của người gửi và so với giá trị băm họ tự tính, nhờ đó biết được nguồn gốc và tính toàn vẹn. Mã hóa bằng khóa công khai của người nhận chỉ bảo mật nội dung, không chứng minh người gửi. Khóa đối xứng cần trao đổi trước và không đảm bảo chống chối bỏ (non-repudiation).

57. D Tấn công offline dựa trên PMKID lấy PMKID từ thông điệp EAPOL-Key đầu tiên mà access point (AP) có hỗ trợ gửi ra. Kẻ tấn công thu nó bằng công cụ như hcxdumptool rồi dò PSK offline bằng hashcat, không cần 4-way handshake đầy đủ hay deauth. Mật khẩu PSK mạnh, ngẫu nhiên giúp chống dò offline. KRACK khai thác việc dùng lại nonce khi handshake được gửi lại. Evil twin là giả mạo một AP, còn tấn công PIN WPS nhắm vào giao thức WPS riêng.

58. D Diffie-Hellman cho hai bên tự tính ra cùng một bí mật bằng phép lũy thừa modulo trên các giá trị công khai và số mũ riêng. Vì vậy bí mật không bao giờ được gửi đi, và các giá trị bị chặn bắt được là vô dụng nếu không có số mũ riêng. Chữ ký RSA xác thực dữ liệu nhưng không tạo khóa đối xứng chung. AES-256 là mã đối xứng cần khóa có sẵn, còn HMAC chỉ đảm bảo toàn vẹn và xác thực thông điệp.

59. C Diffie-Hellman tạm thời (ephemeral) tạo một cặp khóa mới cho mỗi lần bắt tay rồi bỏ số mũ riêng. Dù sau này khóa dài hạn của máy chủ bị lộ, cũng không tính lại được khóa của các phiên cũ. Đó là bảo mật chuyển tiếp hoàn hảo (perfect forward secrecy). RSA tĩnh dùng khóa công khai dài hạn nên lộ khóa riêng là giải mã được mọi phiên đã ghi, vì vậy TLS 1.3 đã bỏ nó. PSK thuần dùng lại cùng một bí mật. Kerberos không phải cách trao đổi khóa của TLS.

60. A Bảng độ mạnh tương đương trong NIST SP 800-57 Phần 1 xếp khóa đối xứng 128 bit tương ứng với RSA 3072 bit. RSA 1024 bit chỉ tương đương khoảng 80 bit bảo mật và đã bị loại bỏ. RSA 2048 bit tương đương khoảng 112 bit, thấp hơn mức 128 bit cần có. RSA 15360 bit tương đương đối xứng 256 bit, vượt xa yêu cầu và làm hệ thống chậm đi không cần thiết.

61. B Liệt kê (enumeration) đến sau quét. Ở giai đoạn này người kiểm thử chủ động lấy tên người dùng, tên share, nhóm và dữ liệu null session, thường bằng enum4linux hoặc rpcclient. Quét lỗ hổng tìm CVE và cấu hình sai đã biết, không lấy danh sách người dùng hay share. Lấy banner đã được lệnh nmap -sV làm xong và không cho ra chi tiết share hay người dùng. Trinh sát chủ động là bước thu thập thông tin rộng hơn, diễn ra trước khi quét cổng.

62. B Hacker mũ trắng làm việc khi có sự cho phép rõ ràng của chủ hệ thống và theo phạm vi đã ký, nên hoạt động hợp pháp và đúng đạo đức. Hacker mũ đen hành động không được phép, vì lợi ích cá nhân hoặc ác ý. Hacker mũ xám kiểm thử khi chưa được phép nhưng không có ý xấu, và việc đó vẫn là bất hợp pháp. Script kiddie thiếu kỹ năng sâu và chỉ chạy công cụ có sẵn mà không hiểu. Yếu tố phân biệt mũ trắng với các nhóm còn lại là sự cho phép.

63. B SYN flood là kỹ thuật từ chối dịch vụ (denial of service), làm cạn tài nguyên máy chủ để người dùng hợp lệ không vào được hệ thống. Vì vậy nó tấn công trực tiếp vào tính sẵn sàng, tức là dữ liệu và dịch vụ phải dùng được khi cần. Tính bí mật liên quan đến việc lộ dữ liệu, và ở đây không có dữ liệu nào bị lộ. Tính toàn vẹn liên quan đến việc sửa dữ liệu trái phép, và không có bản ghi nào bị thay đổi. Chống chối bỏ không thuộc bộ ba CIA cổ điển nên là đáp án gây nhiễu.

64. C Quét và liệt kê là tương tác trực tiếp, chủ động với máy mục tiêu: quét cổng, nhận diện dịch vụ và phiên bản, nhận dạng hệ điều hành (OS fingerprinting) bằng Nmap để vẽ bản đồ bề mặt tấn công. Trinh sát là giai đoạn thu thập thông tin trước đó, có thể thụ động (OSINT) hoặc chủ động, nhưng chưa dò trực tiếp từng cổng. Giành quyền truy cập là khai thác thật để có chỗ đứng, việc này chưa xảy ra. Duy trì truy cập là cài cơ chế bám trụ sau khi đã chiếm được hệ thống, rất muộn về sau.

65. B Hacker mũ xám hành động khi chưa có ủy quyền chính thức hay hợp đồng, nhưng không có ý xấu và thường báo lỗi một cách có trách nhiệm, đúng như tình huống này. Mũ trắng cần có hợp đồng hoặc sự cho phép rõ ràng trước khi kiểm thử, ở đây không có. Suicide hacker chấp nhận bị truy tố để phơi bày mục tiêu, bất chấp hậu quả. Hacktivist hành động vì mục đích chính trị hoặc xã hội. Điểm phân biệt thường gặp là tình trạng ủy quyền cùng ý định, không phải kỹ thuật dùng.

66. D Red team làm việc theo mục tiêu, đánh giá khả năng phát hiện và phản ứng trước một đối thủ thực tế, không nhằm phủ hết mọi lỗ hổng, và thường bên phòng thủ không được báo trước. Kiểm thử xâm nhập thường rộng hơn, giới hạn thời gian và cố tìm càng nhiều lỗ hổng khai thác được càng tốt trong phạm vi. Đánh giá lỗ hổng chỉ quét và báo cáo, không khai thác, và không mô phỏng theo mục tiêu. Bug bounty là hình thức cộng đồng, liên tục, không có kịch bản phối hợp như mô tả.

67. C Rules of Engagement quy định các chi tiết vận hành của chính đợt kiểm thử: phương pháp, giờ được phép, đầu mối khẩn cấp và các hạng mục bị loại trừ như cổng thanh toán. SOW nêu sản phẩm bàn giao, thời hạn và chi phí, không nêu ranh giới vận hành. NDA chỉ nói về bảo mật thông tin trao đổi, không về quy trình kiểm thử. MSA đặt ra điều khoản pháp lý và thương mại chung cho mối quan hệ với khách hàng, không nêu chi tiết kỹ thuật hay loại trừ.

68. C Kiểm thử hay khai thác hệ thống không được ghi trong phạm vi đã ký, dù rất ít, có thể khiến người kiểm thử chịu trách nhiệm dân sự và vi phạm luật CFAA, vì bên thứ ba chưa hề đồng ý. Cách đúng là dừng ở ranh giới và báo theo kênh trong ROE, để khách hàng quyết định cách xử lý. Chỉ thử "để xác nhận" cũng đã là truy cập trái phép. Giấu phát hiện quan trọng cũng vi phạm nghĩa vụ báo cáo, dù không được khai thác thêm.

69. D Lệnh nmap cho biết cổng 445 (SMB) đang mở, đây là hoạt động quét, dùng để xác định máy đang chạy và dịch vụ. Sau đó enum4linux chủ động hỏi dịch vụ đó để lấy tên share, người dùng và nhóm, đây chính là liệt kê. Trinh sát hay footprinting có thể là thụ động hoặc chủ động. Giành quyền truy cập cần khai thác một lỗ hổng, việc này chưa xảy ra. Xóa dấu vết chỉ diễn ra sau khi đã xâm nhập.

70. C Trinh sát thụ động thu thập thông tin mà không tương tác trực tiếp với hệ thống mục tiêu, dùng các nguồn như Shodan, WHOIS, bản ghi DNS và mạng xã hội, nên không để lại dấu vết trên mạng mục tiêu. Trinh sát chủ động cần tương tác trực tiếp, như quét ping hay quét cổng, và có thể bị ghi log hoặc phát hiện. Liệt kê là giai đoạn sau, xâm lấn hơn, lấy chi tiết như tên người dùng hay share qua kết nối trực tiếp. Quét lỗ hổng cũng chủ động dò hệ thống đang chạy nên dễ bị phát hiện.

Từ tiếng Anh cần biết

White hat hacker	Hacker mũ trắng	Người kiểm thử bảo mật khi chủ hệ thống cho phép
Gray hat hacker	Hacker mũ xám	Người thử hệ thống không được phép nhưng không có ác ý
Penetration test	Kiểm thử xâm nhập	Thử khai thác lỗ hổng trong phạm vi được phép

Red team engagement	Diễn tập đội đỏ	Giả lập tấn công để đo khả năng phát hiện và phản ứng
Rules of Engagement (ROE)	Quy tắc thực hiện kiểm thử	Văn bản ghi cách làm, giờ làm và phần cấm thử
Scope	Phạm vi	Danh sách hệ thống được phép kiểm thử
Availability	Tính sẵn sàng	Người có quyền dùng được hệ thống khi cần
Integrity	Tính toàn vẹn	Dữ liệu không bị sửa trái phép
Footprinting	Thu thập dấu vết	Gom thông tin về mục tiêu trước khi tấn công
Passive reconnaissance	Trinh sát thụ động	Thu thập thông tin mà không chạm vào hệ thống mục tiêu
Active reconnaissance	Trinh sát chủ động	Gửi yêu cầu thẳng tới hệ thống của mục tiêu
OSINT	Tình báo nguồn mở	Thông tin lấy từ các nguồn công khai
Banner grabbing	Đọc banner dịch vụ	Đọc lời chào của dịch vụ để biết phần mềm
Zone transfer (AXFR)	Chuyển vùng DNS	Sao chép toàn bộ tệp vùng DNS từ máy chủ
Enumeration	Liệt kê	Lấy tên người dùng, nhóm và thư mục chia sẻ
Credentials	Thông tin đăng nhập	Tên người dùng, mật khẩu hoặc bằng chứng danh tính khác
Hash	Giá trị băm	Chuỗi độ dài cố định từ hàm một chiều
Pass-the-hash	Dùng lại giá trị băm	Xác thực bằng hash NTLM mà không cần mật khẩu gốc
Kerberoasting	Tấn công vé dịch vụ Kerberos	Xin vé dịch vụ rồi bẻ mật khẩu ngoại tuyến
Golden ticket	Vé vàng	TGT giả, tạo bằng hash của tài khoản krbtgt
Rainbow table	Bảng cầu vồng	Bảng tính sẵn để tra mật khẩu từ hash
Privilege escalation	Leo thang đặc quyền	Từ quyền thấp giành lấy quyền cao hơn
Persistence	Duy trì truy cập	Cách giữ quyền truy cập đã có, kể cả khi máy khởi động lại
Rootkit	Rootkit	Phần mềm che giấu tiến trình, tệp và kết nối của kẻ tấn công
Sniffing	Nghe lén mạng	Bắt và đọc gói tin đi trên mạng
MAC flooding	Làm tràn bảng CAM	Làm đầy bảng CAM để switch phát như hub
Social engineering	Tấn công phi kỹ thuật	Lừa con người để lấy thông tin hoặc quyền vào
Pretexting	Dựng kịch bản giả	Dùng danh tính hoặc câu chuyện giả để được tin
Tailgating	Đi bám theo	Theo người có quyền qua cửa mà họ không biết
Evasion	Né tránh phát hiện	Cách làm cho IDS hoặc tường lửa không nhận ra
Honeypot	Hệ thống bẫy	Máy giả để dụ và theo dõi kẻ tấn công
Session hijacking	Chiếm phiên	Chiếm một phiên làm việc đã được xác thực
Session fixation	Cố định phiên	Gài sẵn session ID trước khi nạn nhân đăng nhập
Cross-site scripting (XSS)	Chèn mã vào trang web	Mã độc chạy trong trình duyệt của nạn nhân

Server-side request forgery (SSRF)	Giả mạo yêu cầu từ máy chủ	Làm máy chủ gửi yêu cầu tới nơi kẻ tấn công chọn
Insecure deserialization	Giải tuần tự không an toàn	Dựng lại đối tượng từ dữ liệu chưa kiểm tra
Evil twin	Điểm truy cập giả	AP giả dùng cùng SSID với mạng thật
Four-way handshake	Bắt tay bốn bước	Trao đổi khóa giữa máy khách và AP trong WPA2
Downgrade attack	Tấn công hạ cấp	Ép hai bên dùng giao thức cũ và yếu hơn
Perfect forward secrecy	Bảo mật chuyển tiếp hoàn hảo	Lộ khóa dài hạn vẫn không giải mã được phiên cũ

Examundo là trang độc lập, không liên kết với các đơn vị tổ chức những kỳ thi này và không được các đơn vị này phê duyệt. Câu hỏi được soạn riêng, không lấy từ đề thi thật. examundo.tech/vi/ceh/