examundo

CEH 中文模拟考试

70 题，附答案。指南和译文由软件制作并核对，目前还没有人工审阅。

更新日期：2026 年 11 月 25 日 · examundo.tech/zh/ceh/

系统入侵与攻击

1. 测试人员持有有效但权限较低的域凭据，为已注册服务主体名称（SPN）的账户请求服务票据（TGS），提取票据后尝试离线破解，以还原服务账户的明文密码。这种攻击叫什么？

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. Pass-the-ticket 攻击
C. Kerberoasting
D. Golden ticket 攻击

---

2. 在 Windows 网络的后渗透阶段，测试人员直接从 LSASS 内存中提取 NTLM 哈希，并用这个哈希通过 SMB 向第二台服务器认证，全程没有破解出明文密码。这描述的是哪种攻击技术？

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. Pass-the-hash 攻击
B. LLMNR/NBT-NS 投毒
C. Golden ticket 攻击
D. Kerberoasting

---

3. 测试人员知道目标密码的格式是一个大写字母、五个小写字母和两个数字（例如 Summer24）。针对一个 NTLM 哈希文件，下面哪条 hashcat 命令能正确攻击这个格式？

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?l?d?d
B. hashcat -m 1000 -a 0 hashes.txt ?u?l?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?l?d?d

---

4. 攻击者用命令 type malware.exe > notes.txt:hidden.exe，把一个恶意可执行文件藏进 NTFS 卷上某个正常文本文件的备用数据流（Alternate Data Stream）。这种技术的哪个特点使它能有效躲过一般的检查？

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. 这种技术在 FAT32 和 ext4 文件系统上的效果完全相同
B. 杀毒软件在任何情况下都无法扫描备用数据流
C. 隐藏的数据流会自动用 EFS 加密其内容
D. Windows 资源管理器显示的 notes.txt 文件大小不包含隐藏数据流的内容

---

5. 在 Linux 主机的后渗透评估中，测试人员运行 find / -perm -4000 -type f 2>/dev/null，发现 /usr/bin/find 本身设置了 SUID 位，属主是 root。下面哪种做法最能利用这个配置错误来提权?

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. 把 /usr/bin/find 二进制文件替换成反向 shell 载荷
B. 用 find 的 -exec 选项启动一个 root shell
C. 用 find 在 /etc/shadow 中搜索密码哈希
D. 直接修改 /etc/passwd，因为 find 有写权限

---

6. 取证分析人员发现一台被入侵的 Linux 服务器上，ps、netstat 和 ls 这几个程序被替换成修改过的版本，在常规查询中会隐藏攻击者的进程、网络连接和文件。这描述的是哪一类恶意工具?

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. 用户态 rootkit（Userland rootkit）
B. 逻辑炸弹（Logic bomb）
C. 特洛伊木马（Trojan horse）
D. 内核态 rootkit（Kernel-mode rootkit）

---

7. 攻击者在一台加入域的工作站上完成操作后，用 wevtutil cl Security 清除了 Windows 安全日志。即使日志内容已经没了，下面哪个痕迹最有可能显示日志被清除过?

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. System 日志，它无法用 wevtutil 清除，始终不会被动过
B. wevtutil.exe 的 Windows Prefetch 文件，命令执行后它会被自动删除
C. 日志自身记录的事件 ID 1102，内容为 "The audit log was cleared"
D. Security.evtx 文件的 $MFT 条目，它是不可变的，无法修改

---

8. 渗透测试人员拿到一个 Windows 密码哈希文件，想把哈希与一个很大的、预先计算好的哈希到明文对照表做比对，来还原明文密码。这用的是哪种技术?

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. 彩虹表攻击（Rainbow table attack）
B. 暴力破解（Brute-force attack）
C. Kerberoasting
D. 字典攻击（Dictionary attack）

---

9. 攻击者掌握了 krbtgt 账户的 NTLM 哈希，伪造出可访问域内任何服务的票据授予票据（TGT），而且在 krbtgt 密码被重置两次之前一直有效。这描述的是哪种攻击?

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. Silver ticket 攻击
B. Golden ticket 攻击
C. Pass-the-hash 攻击
D. DCSync 攻击

---

10. 攻击者已获得 Windows 系统的 SYSTEM 级访问权限，想建立基于注册表的持久化，让一个原生子系统（native subsystem）应用在会话管理器（Session Manager）初始化期间、Windows 子系统加载之前运行。哪个注册表位置支持这个执行阶段?

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

侦察与踩点

11. 测试人员枚举 target.com 的 DNS 记录，发现两条 MX 记录：mail.target.com 的优先级是 10，backupmx.target.com 的优先级是 20。下面哪个说法正确指出了主邮件交换服务器?

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 是主服务器，因为优先级数值越低，优先程度越高

B. backupmx.target.com 是主服务器，因为优先级数值越高，优先程度越高

C. 优先级数值会被忽略，MX 记录按字母顺序选择

D. 两台服务器同时使用，优先程度相同

---

12. 测试人员对目标的公网 IP 运行 traceroute，在开始扫描之前绘制网络路径，找出中间的路由器和防火墙。这项活动属于哪一类踩点（footprinting）？

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. 仅属于被动踩点

B. 社会工程学踩点

C. DNS 踩点

D. 网络踩点

---

13. 在踩点阶段，红队成员查询目标域名的 DNS 记录，为鱼叉式钓鱼活动做准备。哪种 DNS 记录类型最直接地提供该组织电子邮件基础设施的信息?

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. 渗透测试人员在侦察阶段执行 `dig axfr @ns1.target.com target.com`，尝试获取完整的 DNS 区域传送。从方法论的角度，这个操作最应归为哪种侦察?

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. 主动侦察，因为它直接向目标拥有并运营的系统发送查询

B. 被动侦察，因为 dig 是只读的诊断工具

C. 被动侦察，因为 DNS 查询永远不会接触目标监控的基础设施

D. 只有在传送成功并返回记录时才算主动侦察

---

15. 渗透测试人员用 netcat 直接连接目标的 25 端口，读取返回的服务器横幅（banner），以判断邮件服务器的软件和版本。这种技术属于：

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. 漏洞扫描
B. 枚举，不是踩点
C. 主动踩点（Active footprinting）
D. 被动踩点（Passive footprinting）

---

16. 哪个侦察工具是专门设计的模块化 OSINT 框架，可以自动从社交媒体、WHOIS 和搜索引擎等来源收集数据，并用基于图的可视化呈现它们之间的关系？

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. 测试人员用 telnet 对目标的邮件服务器做横幅抓取，收到响应 "220 mail.targetcorp.com ESMTP Postfix"。测试人员最直接了解到了什么？

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. 员工电子邮件地址的完整列表
B. 该域名的注册商和管理联系人
C. 邮件服务器软件，可能还有它的版本
D. 该组织完整的公网 IP 地址范围

---

18. 哪种 Google 搜索运算符组合最能有效地在指定目标域名上找出公开被索引、且包含字符串 'password' 的配置文件？

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. 在侦察阶段，一名道德黑客查询公共注册数据库，查找目标域名的注册人姓名、注册组织和管理联系人。这是在做什么？

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 区域传送
B. 端口扫描
C. WHOIS 查询
D. 横幅抓取

---

20. 分析人员想找出位于某个特定国家的联网设备，应该使用哪个 Shodan 搜索过滤器？

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:

网络与边界攻击

21. 在扫描一个子网时，测试人员发现某台主机开放了大量端口，所有端口的服务横幅都完全相同而且异常冗长，没有符合正常协议握手的响应，而且无论查询什么，响应速度都快得不正常。下面哪个结论最有依据?

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. 这台主机很可能是低交互蜜罐
B. 这台主机运行着入侵防御系统（IPS）
C. 这台主机位于负载均衡器后面
D. 这台主机是经过加固的生产服务器

---

22. 一名员工收到一封看似来自 IT 服务台的电子邮件，催促他立即通过邮件里的链接重置密码，链接指向一个假的登录页面。这属于哪种社会工程学技术?

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（语音钓鱼）
B. Phishing（网络钓鱼）
C. Pretexting（假托）
D. Tailgating（尾随）

---

23. 攻击者用成千上万条伪造的 MAC 地址到端口的映射淹没交换机的 CAM 表，使交换机失效开放（fail open），像集线器一样把帧从每个端口广播出去。这是哪种攻击?

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（VLAN 跳跃）
B. DHCP starvation（DHCP 耗尽）
C. MAC flooding（MAC 泛洪）
D. ARP spoofing（ARP 欺骗）

---

24. 攻击者用成千上万个伪造的源 MAC 地址淹没交换机的 CAM 表。这种攻击的主要目的是什么?

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

A. 迫使交换机进入失效开放模式，像集线器一样把流量广播到所有端口
B. 使交换机的操作系统崩溃，造成拒绝服务
C. 获得交换机的管理控制台访问权限
D. 完全绕过 802.1X 基于端口的认证

---

25. 测试人员向防火墙后面的一台主机发送 TTL 值逐步递增的探测包，利用返回的 ICMP Time Exceeded 消息，判断 ACL 允许哪些具体端口通过防火墙。这用的是哪种技术?

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. 标准 traceroute 路径绘制
B. Firewalking（防火墙探测）
C. 通过 TTL 分析做操作系统指纹识别
D. 横幅抓取

---

26. 一种 IDS 规避技术：攻击者故意把攻击载荷拆散到许多小的 TCP 段中，并在包与包之间故意加入延迟，使 IDS 的重组超时先到期，无法匹配出完整的特征。这种技术叫：

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（会话拼接）
B. Polymorphic encoding（多态编码）
C. Firewalking
D. Fragmentation overlap（分片重叠）

---

27. 一名物理安全评估人员走向一扇刷卡门，正好有一名员工从里面出来。员工注意到评估人员，以为他是同事，主动替他扶住了门。这属于：

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（搭便车进入），因为员工是知情地允许对方进入
B. Tailgating（尾随），因为进入时没有任何授权
C. Shoulder surfing（肩窥）
D. Dumpster diving（翻垃圾）

---

28. 渗透测试人员精心构造恶意载荷数据，把它拆分成几个小的 IP 分片，再发往一个由基于特征的入侵检测系统保护的目标。这用的是哪种规避技术？

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. 泛洪（Flooding）
B. 分片（Fragmentation）
C. 欺骗（Spoofing）
D. 加密（Encryption）

---

29. 在一次获得授权的社会工程学评估中，攻击者给 IT 服务台打电话，冒充一位正在出差的高管，说急需重置密码，并提供伪造的员工编号和部门信息来建立可信度。这演示的是哪种社会工程学技术？

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（假托）
B. Tailgating（尾随）
C. Phishing（网络钓鱼）
D. Baiting（诱饵）

---

30. 测试人员通过注入序列号预测正确的伪造数据段，劫持了一个已认证的 TCP 会话。之后，合法客户端和服务器开始不停地互相发送无效的确认（ACK）包，而且始终无法重新同步。这种副作用叫什么？

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（SYN 泛洪）
B. DNS amplification（DNS 放大）
C. ACK storm（ACK 风暴）
D. ARP cache exhaustion（ARP 缓存耗尽）

Web 应用攻击

31. 一台生产环境的 Web 服务器每当发生未处理的异常，就会返回详细的堆栈跟踪，其中包括框架版本号和文件路径。这个弱点属于 OWASP Top 10 的哪一类？

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. 注入（Injection）
B. 安全配置错误（Security misconfiguration）
C. 加密机制失效（Cryptographic failures）
D. 身份识别和认证失效（Identification and authentication failures）

---

32. 测试人员在一个后台执行 ping 查询的网页表单字段中，提交了一个分号加上一条 Linux 命令，额外命令的输出出现在响应里。利用的是哪一类漏洞?

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 命令注入（OS command injection）
B. SQL 注入（SQL injection）
C. 不安全的反序列化（Insecure deserialization）
D. 跨站脚本（Cross-site scripting）

---

33. 测试人员提交了一个包含脚本标签的搜索查询，结果的错误页面未经编码就把载荷原样回显到 HTML 响应中，并在测试人员的浏览器里执行了。这属于哪种类型的跨站脚本（XSS）?

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. 反射型 XSS（Reflected XSS）
B. 盲 XSS（Blind XSS）
C. 存储型 XSS（Stored XSS）
D. 基于 DOM 的 XSS（DOM-based XSS）

---

34. 一个 Java Web 应用在 cookie 参数中接收序列化对象，并且不经验证就反序列化。测试人员用已知的利用链（gadget chain）构造了恶意的序列化载荷，并实现了远程代码执行。是什么根本原因使这次攻击成为可能?

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. 应用对攻击者可控的数据做反序列化，既没有限制类型，也没有完整性验证
B. 应用在传输 cookie 时使用了过时的 TLS 密码套件
C. 应用把会话状态保存在客户端 cookie 中，而不是服务器端
D. 应用没有给 cookie 设置 HttpOnly 标志

---

35. 一个 Web 应用允许用户输入一个 URL，服务器会获取它来生成缩略图预览。测试人员输入了一个内部云元数据地址，响应中包含了实例凭据。利用的是哪种漏洞?

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. 跨站脚本（Cross-site scripting）
B. 路径遍历（Path traversal）
C. 不安全的直接对象引用（Insecure direct object reference）
D. 服务端请求伪造（Server-side request forgery）

---

36. 一个应用从 cookie 中接收 base64 编码的序列化 Java 对象，并在服务器上不经验证就重建它，使攻击者可以用精心构造的对象触发远程代码执行。是哪种漏洞使这次攻击成为可能?

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. 跨站请求伪造（Cross-site request forgery）
B. 点击劫持（Clickjacking）
C. 不安全的反序列化（Insecure deserialization）
D. 访问控制失效（Broken access control）

---

37. 在受害者登录之前，攻击者给受害者发送一个带有预设会话标识符的链接。受害者认证之后，应用没有重新生成会话 ID，攻击者就用同一个标识符访问了已通过认证的会话。这是哪种攻击?

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. 点击劫持（Clickjacking）
B. 会话固定（Session fixation）
C. 通过数据包嗅探进行会话劫持
D. 跨站请求伪造（Cross-Site Request Forgery）

---

38. 渗透测试人员最常用哪个工具作为拦截代理，来检查和修改浏览器与 Web 应用之间的 HTTP 请求?

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. 在测试一个基于 Flask 的 Web 应用时，测试人员向反馈表单字段提交输入 '{{7*7}}'，随后渲染出来的页面显示的是 '49'，而不是字面字符串。这个现象证实了哪种漏洞?

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 注入，其中 7*7 被当作数据库算术表达式计算
B. 通过 Jinja2 模板引擎实现的服务端模板注入（SSTI）
C. 由未转义的 HTML 输出造成的反射型跨站脚本
D. 由 AngularJS 表达式沙箱处理的客户端模板注入

---

40. 当不受信任的用户输入未经适当过滤就被插入数据库查询，使攻击者能改变查询逻辑，这是哪种类型的攻击?

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. 跨站请求伪造（Cross-site request forgery）
B. SQL 注入（SQL injection）
C. 服务端请求伪造（Server-side request forgery）
D. 跨站脚本（Cross-site scripting）

无线网络攻击

41. 某组织在整个无线基础设施中启用了受保护管理帧（Protected Management Frames，802.11w）。这项控制主要缓解哪种常见的无线攻击技术?

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

A. 恶意 DHCP 服务器攻击
B. 对捕获的握手包进行离线字典攻击
C. WPS PIN 暴力破解攻击
D. 解除认证和解除关联帧欺骗

---

42. 测试人员想从一个 WPA2-PSK 网络获取凭据材料，又不想等合法客户端来认证。哪种技术最能达到这个目的?

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. 用 Reaver 进行 WPS PIN 暴力破解
B. 发送解除认证帧，等待捕获客户端的四次握手
C. 用 hcxdumptool 从 AP 的第一个 EAPOL 帧中捕获 PMKID
D. 对已连接到 AP 的客户端进行 ARP 欺骗

---

43. 红队成员架设了一个恶意接入点，广播与企业网络相同的 SSID 和相近的信号强度，诱使员工连接，然后拦截他们的流量。这描述的是哪种攻击？它与 Karma 攻击有什么区别?

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. 解除认证攻击；它在冒充网络之前先迫使客户端断开连接
B. Evil twin 攻击；它会响应客户端曾经探测过的每一个 SSID
C. Karma 攻击；它冒充一个特定的已知 SSID，而不是应答客户端发出的每个探测请求
D. Evil twin 攻击；它冒充一个特定的已知 SSID，而不是应答客户端发出的每个探测请求

---

44. 测试人员针对一个启用了 WPS 的接入点，想恢复 WPA2 密码。哪种攻击利用某些芯片组生成 E-S1/E-S2 随机数（enrollee nonce）时随机性太弱的缺陷，使 WPS PIN 能在几秒内离线算出，而不是在线暴力破解？

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. 针对 RSN IE 的 PMKID 攻击
B. 用 Reaver 进行在线 WPS PIN 暴力破解
C. 针对四次握手的 KRACK 攻击
D. Pixie Dust 攻击

---

45. 一名渗透测试人员已获授权评估某企业 WPA2-PSK 网络，想捕获四次握手来做离线字典攻击。最常用哪种技术迫使已连接的客户端重新认证，以便捕获握手？

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. 用 aireplay-ng 发送解除认证帧
B. 用 SSL strip 代理降级连接
C. 对客户端进行 ARP 缓存投毒
D. 向客户端发送伪造的 DNS 响应

---

46. 渗透测试人员架设了一个恶意接入点，广播与合法企业网络相同的 SSID，诱使员工连接，以便截获他们的凭据。这描述的是哪种攻击？

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. Evil twin 攻击
B. ARP 欺骗攻击
C. Bluejacking 攻击
D. WPS PIN 攻击

---

47. 评估人员收集大量流量，分析 RC4 密码使用的重复初始化向量（IV）的规律，几分钟内就破解了一个旧的 WEP 密钥。这利用了 WEP 的哪个根本设计缺陷？

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 允许攻击者把交换降级到较弱的密码套件
B. TKIP 的 Michael 完整性检查可以用 chopchop 攻击绕过
C. 四次握手完全没有消息完整性码
D. 24 位的 IV 空间太小，会频繁造成密钥流碰撞

---

48. 哪种无线社会工程学攻击会让恶意接入点对附近客户端首选网络列表中的任意 SSID 的探测请求作出肯定响应，而不是冒充某个特定的已知网络？

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. Karma 攻击
B. 恶意 DHCP 攻击
C. Evil twin 攻击
D. 解除认证攻击

---

49. 一名研究人员披露了一个漏洞：处于中间人位置的攻击者可以操纵握手重传，迫使已使用过的加密密钥被重新安装，从而在不知道密码的情况下解密客户端流量。这种攻击叫什么？

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. Evil twin 攻击
B. WPS PIN 暴力破解攻击
C. PMKID 攻击
D. KRACK 攻击

---

50. 某网络以“过渡模式”（transition mode）广播 WPA3-Personal，以兼容旧的 WPA2 客户端。这种配置带来了什么风险?

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

A. 攻击者可以迫使客户端降级到较弱的 WPA2 握手，从而进行传统的离线字典攻击

B. AP 为了向后兼容而以明文广播 PSK

C. SAE 的零知识证明对所有连接的客户端都被完全禁用

D. 802.11w 受保护管理帧只对 WPA3 客户端强制启用，消除了 WPA2 客户端的解除认证风险

密码学

51. 渗透测试人员发现，当提交被修改过的 CBC 加密 cookie 时，Web 应用对无效填充和无效 MAC 返回不同的错误消息。这种行为使哪种攻击成为可能?

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. 选择明文攻击（Chosen-plaintext attack）

B. 中间相遇攻击（Meet-in-the-middle attack）

C. 填充预言攻击（Padding oracle attack）

D. 生日攻击（Birthday attack）

---

52. 在一次无线评估中，测试人员用 aireplay-ng 对客户端发起解除认证后，用 airodump-ng 捕获了 WPA2 四次握手。接下来测试人员最可能用哪个工具离线恢复预共享密钥?

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. Metasploit 的 psexec 模块

---

53. 测试人员发现一台旧的 Web 服务器虽然也支持 TLS 1.2，却仍然接受 SSLv3 连接。对于可以被迫回退到 SSLv3 的客户端，哪种攻击变得可行?

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. 测试人员观察到网络流量中有客户端与服务器之间的 Diffie-Hellman 密钥交换。哪种情况会使共享密钥有可能通过预先计算的、Logjam 式攻击被实际恢复出来?

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. 服务器证书使用 2048 位的 RSA 签名密钥

B. 服务器协商使用常被重复使用的 512 位或 1024 位 DH 组

C. 服务器使用 P-256 曲线的 ECDHE

D. 客户端和服务器协商 AES-256-GCM 密码套件

---

55. 哪种加密类型对数据的加密和解密使用同一个密钥?

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

A. 非对称加密（Asymmetric encryption）

B. 对称加密（Symmetric encryption）

C. 数字签名（Digital signature）

D. 哈希（Hashing）

---

56. 用户想对一封电子邮件做数字签名，让收件人既能确认发件人身份，又能确认邮件在传输中没有被改动。下面哪个过程最能说明签名是如何生成的?

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. 用共享的对称密钥加密消息摘要
B. 用收件人的公钥加密整封邮件
C. 先对邮件做哈希，再用发件人的私钥加密这个哈希值
D. 先对邮件做哈希，再用收件人的公钥加密这个哈希值

---

57. 无线网络审计员直接从接入点发出的第一个 EAPOL 帧中捕获了一个 PMKID 哈希，没有观察到客户端完成四次握手，也没有做解除认证（deauthentication）攻击。这描述的是哪种 WPA2-PSK 攻击技术?

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. Evil twin 攻击（邪恶双胞胎）
B. WPS PIN 暴力破解攻击
C. KRACK 密钥重装攻击
D. 基于 PMKID 的离线攻击

---

58. 在一次网络安全评估中，工程师发现两台主机在不安全的信道上建立了共享密钥，而且密钥本身从未被传输。这描述的是哪种密码学机制?

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. RSA 数字签名
B. AES-256 加密
C. HMAC 认证
D. Diffie-Hellman 密钥交换

---

59. 首席信息安全官（CISO）要求：即使以后 Web 服务器的长期 RSA 私钥被攻破，也不能解密之前捕获的 TLS 流量。哪种密钥交换机制满足这个要求?

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. Kerberos 票据交换
B. 没有临时（ephemeral）成分的预共享密钥交换
C. 临时 Diffie-Hellman（DHE 或 ECDHE）
D. 静态 RSA 密钥交换

---

60. 安全架构师需要选一个 RSA 密钥长度，按 NIST SP 800-57 的建议，其强度大致相当于 128 位对称密钥。应该选哪个密钥长度?

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 位
B. 2048 位
C. 1024 位
D. 15360 位

道德黑客概述

61. 在攻击前阶段，测试人员运行了 'nmap -sV -p 445 10.10.10.5'，确认 SMB 端口开放并拿到了版本信息。为了提取共享名称、用户账户列表和空会话（null session）信息，测试人员下一步应该进入方法论中的哪个阶段?

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. 横幅抓取
B. 枚举
C. 主动侦察
D. 漏洞扫描

---

62. 哪个术语指的是：经组织授权，使用与恶意攻击者相同的技术来测试其系统漏洞的安全专业人员？

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. 黑帽黑客（black hat hacker）
B. 白帽黑客（white hat hacker）
C. 灰帽黑客（gray hat hacker）
D. 脚本小子（script kiddie）

---

63. 攻击者用畸形的 TCP SYN 数据包淹没一家医院的患者预约 Web 服务器，导致医护人员六个小时无法访问该系统。这次攻击主要破坏了 CIA 三要素中的哪一项？

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. 完整性（Integrity）
B. 可用性（Availability）
C. 机密性（Confidentiality）
D. 不可否认性（Non-repudiation）

---

64. 在一次授权的测试中，测试人员在尝试任何利用之前，用 Nmap 找出目标子网中的开放端口、运行的服务和操作系统版本。这项活动属于黑客方法论的哪个阶段？

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. 维持访问
B. 侦察
C. 扫描和枚举
D. 获取访问权限

---

65. 一位安全研究员没有任何合同，个人自发行动，只是浏览某公司的公开登录门户，就发现了一个存储型 XSS 漏洞。她没有进一步利用，而是私下把漏洞报告给了厂商的安全团队。这个人最应该归为：

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. 黑客行动主义者（hacktivist）
B. 灰帽黑客（gray hat hacker）
C. 自杀式黑客（suicide hacker）
D. 白帽黑客（white hat hacker）

---

66. 某组织想衡量其 SOC（安全运营中心）发现并响应一次隐蔽的、多阶段模拟入侵的速度，事先不通知防守方，也不要求列出范围内的所有漏洞。这种工作最应该称为：

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. 漏洞赏金计划（bug bounty program）
B. 渗透测试（penetration test）
C. 漏洞评估（vulnerability assessment）
D. 红队演练（red team engagement）

---

67. 渗透测试公司和客户之间签署了一份文件，规定了具体的测试方法、允许的测试时间段、紧急联系人和升级流程，并明确把生产环境的支付网关排除在测试之外。这份文件最应该归为：

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. 主服务协议（Master Service Agreement，MSA）
B. 保密协议（Non-Disclosure Agreement，NDA）
C. 交战规则（Rules of Engagement，ROE）
D. 工作说明书（Statement of Work，SOW）

---

68. 在一次授权的外部渗透测试中，测试人员在客户的 Web 服务器上发现了一些凭据，这些凭据也能成功登录一个第三方 SaaS 平台，而这个平台没有出现在已签署的范围文件中。测试人员最恰当的第一步行动是什么？

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. 因为第三方系统不在已签署的范围内，所以在最终报告中省略这个发现

B. 立即用这些凭据测试第三方平台，确认这个发现是否可被利用

C. 停止，不测试第三方系统，并按照 ROE 的升级流程向客户报告这个发现

D. 对第三方平台只利用到足以证明影响的程度，然后停止

---

69. 渗透测试人员运行了 'nmap -sV -p445 10.0.5.20'，发现端口开放后，又用 'enum4linux' 从该主机提取共享名称和用户账户列表。这一系列操作代表道德黑客方法论中的哪两个阶段？

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. 踩点（footprinting），然后清除痕迹

B. 枚举，然后维持访问

C. 侦察，然后获取访问权限

D. 扫描，然后枚举

---

70. 渗透测试人员在 Shodan.io 上搜索目标组织连接到互联网的设备，没有直接向目标网络发送任何数据包。这项活动属于：

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. 漏洞扫描

B. 主动侦察

C. 被动侦察

D. 枚举

正确答案

1. C Kerberoasting 用有效的域凭据为注册了 SPN 的账户请求服务票据，再离线破解票据中由服务账户密钥加密的部分来还原密码。AS-REP roasting 针对关闭了 Kerberos 预认证的账户，而且完全不需要有效凭据。Golden ticket 是用被攻陷的 krbtgt 哈希伪造 TGT，并不请求正常的服务票据。Pass-the-ticket 是重用被盗的有效票据，不是离线破解。

2. A Pass-the-hash 直接把捕获的哈希当作身份证明提交，因为 NTLM 认证本来就不需要明文密码。Kerberoasting 针对 Kerberos 服务票据做离线破解，不是直接重用哈希。Golden ticket 用 krbtgt 哈希伪造 Kerberos TGT。LLMNR/NBT-NS 投毒通过伪造名称解析来捕获哈希，但题中描述的不是这一步。

3. A 正确的命令里，哈希类型 -m 1000 对应 NTLM，-a 3 是掩码攻击（mask attack），掩码 ?u?l?l?l?l?l?d?d 依次是 1 个大写、5 个小写、2 个数字，正好是 8 位。掩码写成 ?l?l?l?l?l?u?d?d，大写就到了第六位，位置不对。用 -a 0 是字典（直接）模式，需要词表而不是掩码。用 -m 1800 是 sha512crypt，不是 NTLM。

4. D NTFS 把数据流与主数据流分开存放，所以普通的目录列表和资源管理器显示的 notes.txt 大小都不包含隐藏的内容，一般靠文件大小做的检查就会失效，除非用 dir /r 或 Sysinternals streams 之类的工具。ADS 不会自动用 EFS 加密。备用数据流是 NTFS 特有的功能，FAT32 和 ext4 不支持。现代 AV/EDR 会扫描 ADS，所以说它们完全无法扫描是错的。

5. B SUID 程序以其属主的有效 UID 运行，所以属主为 root 的 find 可以用 find . -exec /bin/sh -p \; -quit 以 root 身份执行任意命令，立刻得到 root shell。直接修改 /etc/passwd 的前提是 find 有写入任意文件的权限，而它本身并没有。替换二进制文件需要对该文件或所在目录有写权限，低权限用户通常没有，而且 -exec 更简单。用 find 搜索 /etc/shadow 并不会显示其内容，拿到哈希后还要再破解，不能立刻得到 root shell。

6. A 把 ps、ls、netstat 这类系统程序替换成被木马化的版本来隐藏攻击痕迹，是典型的用户态（应用层）rootkit。内核态 rootkit 也能隐藏，但它是挂钩系统调用或修改内核数据结构，不是替换用户空间的程序。特洛伊木马是把恶意代码伪装成正常软件，而题中的隐藏行为最符合用户态 rootkit。逻辑炸弹在特定条件下触发载荷，本身没有隐藏功能。

7. C 用 wevtutil 清除安全日志时，系统本身会生成事件 ID 1102（"The audit log was cleared"），它是刚清空的日志里少数保留下来的记录，SOC 分析人员或 SIEM 关联规则能立刻发现有人篡改。运行命令不会自动删除 wevtutil.exe 的 Prefetch 文件，它反而会多留下一份痕迹。System 日志也可以用 wevtutil cl System 清除，所以说它无法清除是错的。NTFS 的 $MFT 条目并非不可变，也不是调查人员判断日志被清除的主要依据。

8. A 彩虹表攻击用预先计算好的哈希链映射到候选明文，不必现场重新计算哈希，就能根据哈希快速查出密码，是用存储空间换速度。字典攻击是实时对词表里的常见密码做哈希，不使用预先计算的表。暴力破解要穷举所有字符组合，既彻底又慢，也不是基于表。Kerberoasting 是针对 Active Directory 服务账户票据提取可破解的哈希，并不说明之后用什么方法查找。RainbowCrack 这类工具，以及加盐（salting）这种防御手段，都与这个概念直接相关。

9. B Golden ticket 用 krbtgt 账户的哈希伪造整个域通用的 TGT，让攻击者长期拥有几乎不受限制的访问权限，直到 krbtgt 凭据被轮换两次。Silver ticket 是用某个服务账户的哈希只为单个服务伪造 TGS，访问范围更窄。DCSync 滥用域复制权限（DS-Replication-Get-Changes）直接拉取密码哈希，并不伪造票据。Pass-the-hash 是重用 NTLM 哈希做直接的 NTLM 认证，不涉及伪造 Kerberos 票据。

10. C HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute 会在会话管理器（SMSS.exe）初始化阶段、Windows 子系统加载之前运行原生应用。这些是为原生子系统编写的 PE 可执行文件，不是普通的 Win32 程序。默认值是用于磁盘检查的 'autocheck autochk *'。Sysinternals Autoruns 会列出 BootExecute 条目，所以这个位置并不能天然躲过常规的自启动枚举。Run 键在登录时启动程序，Userinit 控制登录初始化，User Shell Folders 指定每个用户的外壳文件夹路径，都不符合题中的原生早期启动执行。

11. A 按照 RFC 5321，邮件服务器先选数值最小的 MX 记录，只有首选主机连不上时才退而使用数值更大的记录，所以优先级 10 优先于 20。因此 mail.target.com 是主服务器；说 backupmx.target.com 是主服务器就把规则弄反了，这是考试里的经典陷阱。MX 优先级是严格的优先顺序，不是平均分担负载，除非两条记录的优先级数值相同。DNS 解析不会按字母顺序决定 MX，只看数值优先级字段（优先级相同时随机选择）。

12. D Traceroute 绘制数据包到达目标所经过的逐跳路径，能显示中间的路由器、ISP，以及可能的防火墙或负载均衡器边界，这正属于网络踩点（Network footprinting）。它不是被动的，因为 traceroute 会向目标 IP 直接发送 TTL 递增的数据包并观察响应。它也不是社会工程学踩点，后者是针对人收集信息；也不是 DNS 踩点，后者关注的是名称解析记录，而不是网络路径拓扑。

13. A MX（邮件交换）记录列出负责接收该域名邮件的服务器主机名和优先级，直接暴露钓鱼操作人员需要伪造或攻击的邮件基础设施。NS 记录只标明区域的权威名称服务器，与邮件处理无关。SOA 记录包含序列号、刷新间隔等区域管理数据，与邮件路由无关。PTR 记录用于 IP 到主机名的反向查询，与邮件投递路径无关。

14. A 区域传送请求是直接发给目标自己的权威名称服务器的，对方可以记录日志、限速或告警，所以不管工具本身是不是只读，它都是主动侦察。被动侦察依靠第三方来源（WHOIS 注册机构、搜索引擎缓存、证书透明度日志），从不与目标拥有的系统交互。分类取决于有没有交互，而不是结果，所以 AXFR 失败了也仍然是主动的。工具只读与否，和能不能被发现无关。

15. C 横幅抓取（banner grabbing）要与目标服务建立直接的 TCP 连接并读取它返回的响应，这是与目标基础设施的直接交互，所以属于主动踩点。它不是被动的，因为目标系统知道这个连接并作出了响应。它不是漏洞扫描，后者要探测已知的弱点，而不只是识别软件和版本。它仍然属于踩点技术，发生在信息收集阶段，早于正式的枚举。

16. A Maltego 通过大量 OSINT 转换（transform）把发现的人员、域名、电子邮件地址和组织等实体关联起来，再用交互式图展示这些关系，是侦察阶段可视化关联分析的标准选择。Nmap 是用于主动扫描的网络和端口扫描器，Hydra 是系统入侵阶段用的凭据暴力破解工具，Responder 用于在网络攻击中对 LLMNR/NBT-NS 流量投毒。这三个都不具备 OSINT 图可视化功能。

17. C 横幅抓取获取的是开放服务返回的问候或响应字符串。“邮件服务器软件，可能还有它的版本”是最佳答案：这个 SMTP 横幅暴露了邮件传输代理（Postfix）和主机名，但没有版本号，其他横幅则可能泄露版本。它不会显示组织的 IP 范围，那需要 ASN 或 WHOIS 查询。注册商和管理联系人来自 WHOIS，不是服务横幅。员工邮箱列表需要另外做 OSINT 收集，单靠一个横幅得不到。横幅抓取是典型的主动踩点技术。

18. C 查询 "site:target.com filetype:conf intext:password" 把结果限定在目标域名内，再限定为已被索引的 .conf 文件，并要求文本里含有 'password'，符合目标。inurl:admin 只针对 URL 路径里含有 'admin' 的页面，与配置文件无关。link: 是已弃用的运算符，过去用来搜索链接到某个 URL 的页面，不是搜索域名内的内容。cache: 过去用来取回 Google 保存的页面快照，但 Google 已经停用了这个功能。

19. C WHOIS 查询会向区域互联网注册机构（ARIN、RIPE 等）或域名注册商查询，返回与域名注册相关的所有者信息，例如注册人姓名、组织和联系方式。DNS 区域传送复制的是整个 DNS 区域文件，而不是注册人数据。横幅抓取获取的是开放端口返回的服务响应头。端口扫描识别主机上端口的开放、关闭或被过滤状态，不返回注册人信息。WHOIS 是基础的被动踩点步骤，在接触目标之前就可以进行。

20. B Shodan 的 'country:' 过滤器把结果限定为 IP 地理位置与所给两字母国家代码相符的设备，例如 country:US。'geo:' 过滤器按具体的经纬度坐标搜索，而不是按国家名称。'org:' 过滤器按与该 IP 关联的组织或 ISP 名称搜索，不是按地理位置。'hostname:' 过滤器匹配特定的主机名字符串，与按国家过滤无关。

21. A 低交互蜜罐（low-interaction honeypot）用固定、通用的横幅来模拟服务，很少实现完整的协议逻辑，所以响应往往不一致或过于统一，回复速度也快得不自然。经过加固的生产服务器会严格遵守协议行为，通常还会尽量减少开放端口，而不是开放很多。负载均衡器分发流量，但不会在各个服务上伪造相同的横幅。IPS 会主动阻断或重置恶意流量，不会在开放端口上生成虚假的冗长横幅。

22. B 网络钓鱼用欺骗性的电子邮件，往往冒充 IT 支持之类的可信来源，诱使受害者点击恶意链接或在仿冒页面上输入凭据。语音钓鱼（vishing）依靠语音电话，不是电子邮件，所以不对。假托（pretexting）使用编造的身份或情境，通过邮件或当面交流都可能发生；对于这封带有假登录页链接的邮件，“网络钓鱼”是最具体的答案。尾随是未经授权进入场所的物理安全问题，与邮件欺骗无关。

23. C MAC 泛洪用虚假条目塞满交换机容量有限的内容寻址存储器（CAM）表，表满后许多交换机会进入失效开放状态，把流量广播到所有端口，使攻击者能在交换网络上被动嗅探。ARP 欺骗篡改的是主机上的 ARP 缓存，不是交换机的 CAM 表。VLAN 跳跃利用中继（trunk）配置错误来跨越 VLAN 边界。DHCP 耗尽是耗光 DHCP 地址池。只有 CAM 表溢出符合这种具体的交换机失效模式。

24. A “迫使交换机进入失效开放模式，像集线器一样把流量广播到所有端口”描述的正是 MAC 泛洪想要达到的嗅探效果。MAC 泛洪会耗尽容量有限的 CAM（内容寻址存储器）表；之后目的 MAC 地址未知的帧可能被泛洪到同一 VLAN 内的其他转发端口，攻击者就能捕获一部分发给其他主机的流量。目的地已知的流量仍然可以正常交换。使操作系统崩溃是另一种拒绝服务手法，不是这里的目的。获得管理控制台权限要靠凭据或漏洞利用类攻击，不是耗尽表项。绕过 802.1X 与此无关，因为 MAC 泛洪针对的是转发表，不是认证。

25. B Firewalking 专门针对一个已知网关使用 TTL 递增的技术，根据防火墙另一侧是否返回 Time Exceeded 消息，来枚举 ACL 允许通过防火墙的端口和协议。标准 traceroute 绘制到目的地的网络路径，目的不是找出 ACL 规则集。通过 TTL 分析做操作系统指纹识别，是根据响应中的初始 TTL 值推断操作系统，不是过滤规则。横幅抓取是从开放端口获取服务版本字符串，与 TTL 操控无关。

26. A Session splicing（也叫 session slicing）利用 IDS 重组时间预算有限的弱点，故意把载荷分成大量很小的 TCP 段并加上延迟，让传感器在完整特征出现之前就重组超时并丢弃，而目标主机的超时通常更长或没有超时，仍然能收到并重组出完整载荷。分片重叠利用的是重组顺序的歧义，不是时间。Firewalking 用 TTL 操控来探测防火墙规则，多态编码则是改变载荷的字节模式来躲避检测，而不是改变发送的时间。

27. A Piggybacking 是指有授权的人知情地（即使是误信）让另一个人进入，比如误以为评估人员属于这里而扶住门，虽然这个同意是基于欺骗，但同意是存在的。相反，Tailgating 指未经授权的人在有授权的人完全不知情的情况下跟着通过受控入口。翻垃圾是找回被丢弃的敏感材料，肩窥是偷看别人输入凭据，两者都不适用于这个物理进入的场景。

28. B 分片规避把攻击载荷拆到多个 IP 分片中，使特征匹配引擎在任何一个数据包里都看不到完整的恶意字节序列，尤其是当 IDS 与目标主机的重组方式不同时。加密隐藏的是载荷内容，不是拆分分片。泛洪是耗尽资源，不是隐藏特征。欺骗伪造的是源地址，不是载荷结构。基于分片的规避是很常见的 IDS 绕过技术。

29. A 假托（pretexting）是攻击者编造一个情境或虚假身份来建立信任，操纵目标去做某件事，例如重置密码。网络钓鱼依靠欺骗性的电子消息（邮件或短信），不是实时的冒充情境。尾随是跟在有授权的人后面通过受控门的物理手段。诱饵是用实物或数字形式的诱惑（例如感染病毒的 U 盘）引诱受害者，这个场景里没有。

30. C 会话被劫持并失去同步后，客户端和服务器各自持有的序列号，对方都不再认为有效；一方发出的每个包都会让另一方回复一个带有期望序列号的 ACK，这个 ACK 又被拒绝，形成自我维持的 ACK 循环，称为 ACK 风暴，直到连接超时或被重置。SYN 泛洪是滥用三次握手的拒绝服务技术，与此无关。ARP 缓存耗尽属于第二层投毒，与 TCP 序列号无关。DNS 放大是基于反射的流量型 DoS，与 TCP 会话失步没有关系。

31. B 安全配置错误包括在生产环境中保留详细错误信息或调试信息等问题，这会泄露框架和版本细节，帮助攻击者识别技术栈并针对已知漏洞下手；修复方法是关闭调试模式并返回通用的错误页面。注入不对，因为这里没有用户输入改变命令或查询逻辑。身份识别和认证失效不对，因为这个场景与登录或会话处理无关。加密机制失效不对，因为题中没有描述弱加密或敏感数据暴露。

32. A 附加分号之类的 shell 元字符，把任意系统命令接在原本的 ping 调用后面，是 OS 命令注入的典型特征，让攻击者以 Web 服务器进程的权限执行命令。跨站脚本针对的是受害者的浏览器，不是服务器的 shell。SQL 注入操纵的是数据库查询语法，不是操作系统命令。不安全的反序列化利用的是对序列化对象的不安全重建，与串联 shell 命令是完全不同的攻击面。

33. A 反射型 XSS 是输入未经保存、立刻被回显在服务器响应中；受害者点击构造好的链接或提交恶意表单就能触发，所以它不是持久的。存储型 XSS 不对，因为载荷会保存在服务器端（比如数据库里），并对每个访问受影响页面的访客执行。基于 DOM 的 XSS 不对，因为漏洞完全存在于操作 DOM 的客户端 JavaScript 中，不需要服务器往返。盲 XSS 不对，因为载荷是在看不到的环境（比如管理后台）中触发，攻击者不会立即得到反馈。

34. A 不安全的反序列化漏洞出现在应用对不可信输入做反序列化时，既没有限制允许的类，也没有验证数据完整性，攻击者就能提供利用链（gadget chain），即一串正常的类，在反序列化时它们的副作用被串联起来而实现代码执行。TLS 密码套件的强度影响的是传输保密性，与反序列化逻辑无关。把会话保存在客户端是另一种设计选择，与利用链（gadget chain）利用无关。缺少 HttpOnly 会让 XSS 能窃取 cookie，但它本身不会让精心构造的序列化对象造成远程代码执行。

35. D SSRF 是指服务器自身被迫向攻击者选定的目的地发出请求，这里访问的是平时无法从公网访问的内部元数据服务。跨站脚本是在受害者的浏览器中执行，不是在发出外部请求的服务器上。不安全的直接对象引用是通过可操控的标识符越权访问某个对象，不是获取任意 URL。路径遍历是利用文件系统路径序列跳出目录，不是远程 HTTP 请求。

36. C 不安全的反序列化是指不可信的序列化数据被重建成对象，却没有验证类型或完整性，使攻击者构造的对象调用到本不该执行的代码路径，往往借助 classpath 上已有的利用链（gadget chain），最终造成远程代码执行。跨站请求伪造是伪造已认证的请求，不是操纵对象重建。访问控制失效指授权没有被正确执行，与对象处理无关。点击劫持是用透明框架做的界面欺骗攻击，与序列化机制无关。

37. B 会话固定是指攻击者在认证之前给受害者强加或提供一个已知的会话标识符，而应用在登录成功后没有签发新的会话 ID，攻击者就能重用这个预设的 ID 访问已认证的会话。通过数据包嗅探劫持会话需要拦截传输中的现有会话令牌，不是预先植入。CSRF 是借用受害者自己有效的会话 cookie 伪造改变状态的请求，点击劫持是诱骗受害者点击伪装的界面元素，两者都不涉及预先分配会话 ID。修复方法是在权限变化（例如登录）时始终重新生成会话 ID。

38. A Burp Suite 的 Proxy 工具位于浏览器和目标应用之间，能捕获实时的 HTTP 和 HTTPS 请求与响应，并允许手动或自动修改，这对测试注入、认证和业务逻辑缺陷至关重要。Nmap 不对，因为它是网络和端口扫描器，不是 HTTP 代理。Hashcat 不对，因为它是对捕获的哈希进行破解的密码破解工具。Wireshark 不对，因为它是被动的抓包和分析工具，不是能修改实时应用请求的交互式代理。

39. B '{{7*7}}' 载荷被渲染成 '49'，是在 Flask 默认模板引擎 Jinja2 中检测 SSTI 的经典测试，说明输入被当作模板语法解析并计算，而不是当作普通数据。反射型 XSS 在浏览器中应表现为可执行的脚本或 HTML 标记，不会在服务器端做算术。AngularJS 模板注入是另一种客户端攻击面，与返回响应的 Flask 后端无关。SQL 注入发生在数据库查询环境中，无法解释 HTML 中的算术计算。如果能逃出模板沙箱，SSTI 可以升级为远程代码执行。

40. B SQL 注入是指攻击者提供的、含有 SQL 元字符（', --, OR 1=1）的输入被直接拼接进查询字符串，改变了查询逻辑，从而绕过认证或窃取数据。跨站脚本不对，因为它是把脚本注入浏览器输出，不是数据库查询。跨站请求伪造不对，因为它是强迫已认证用户的浏览器提交不想要的请求，不涉及操纵查询。服务端请求伪造不对，因为它让服务器向意料之外的内部或外部目的地发出请求，而不是操纵 SQL 逻辑。

41. D 802.11w 对健壮管理帧（robust management frames）提供加密保护，包括单播和广播的解除认证（deauthentication）与解除关联（disassociation）帧，从而缓解针对已建立的受保护关联的“解除认证和解除关联帧欺骗（Deauthentication and disassociation frame spoofing）”。它不会增强 PSK 抵御离线破解的能力，因为这个弱点在于密码本身，不在管理帧层。WPS 暴力破解针对的是单独的注册器 PIN 机制，不受 PMF 影响。恶意 DHCP 攻击发生在 802.11 MAC 层之上。

42. C PMKID 攻击不需要客户端：AP 本身会在四次握手的第 1 条消息（M1）的 RSN 信息元素里给出 PMKID，所以测试人员只需要能看到 AP，不需要有已关联的客户端。基于解除认证的握手捕获需要有客户端在线并重新认证。WPS 暴力破解针对的是单独的 PIN 机制，不是 PSK 本身。ARP 欺骗是中间人技术，不是凭据捕获方法。

43. D Evil twin 模仿一个被针对的、已知的 SSID，骗客户端以为自己连的是合法的企业网络。相反，Karma 攻击监听探测请求，并动态地用客户端正在搜索的任何 SSID 来应答，冒充客户端首选网络列表中的任何网络，而不是某个固定名称。解除认证是另一种干扰技术，有时会配合这两种攻击使用，但题中的描述不是它。

44. D Pixie Dust 攻击的对象是 WPS 实现有缺陷的接入点：用来证明知道 PIN 的 E-S1/E-S2 随机数可以预测，或者熵很低。由于这些随机数很弱，只需捕获一次 WPS 交换，攻击者就能在几秒到几分钟内离线暴力破解出 PIN，而在线破解则需要数小时。Reaver 经典的在线暴力破解有速率限制，也很容易被发现或锁定。PMKID 针对的是 WPA2-PSK 认证材料，与 WPS 无关。KRACK 利用的是握手处理中的密钥重装，属于完全不同的一类漏洞。

45. A 解除认证帧会伪造 AP 的 MAC 地址，通知客户端断开连接；客户端自动重连时会重新进行四次握手，这时可以用 airodump-ng 之类的工具捕获，再用 hashcat 或 aircrack-ng 离线破解。ARP 投毒和 DNS 欺骗是第二、三层的中间人技术，不能迫使客户端重新做无线认证，SSL stripping 针对的是 HTTPS 会话，不是 WPA2 密钥交换。解除认证攻击之所以有效，是因为 WPA2 中 802.11 管理帧未经认证，这是已知的设计缺陷，后来由 802.11w 受保护管理帧解决。

46. A Evil twin 攻击是架设一个恶意接入点，模仿合法网络的 SSID（通常还有 BSSID），骗用户连接，以捕获他们的流量和凭据；它常配合解除认证帧，把客户端从真正的 AP 上踢下来。ARP 欺骗是针对已在网络内的主机的第二层技术，不是冒充 AP 的方法。WPS PIN 攻击是通过暴力破解攻击合法 AP 的 WPS 实现，不是假 AP。Bluejacking 是通过蓝牙发送未经请求的消息，与冒充 Wi-Fi SSID 无关。

47. D WEP 的 24 位初始化向量只有大约 1670 万种取值，在繁忙的网络里几个小时内就会被重复使用（碰撞）；捕获到这些碰撞后，aircrack-ng 之类的工具可以用 FMS 或 PTW 攻击等技术，通过统计方法恢复 RC4 密钥。TKIP 及其 Michael 检查是 WPA 的保护措施，不属于 WEP。SAE 降级攻击针对的是 WPA3，不是 WEP。WEP 确实有完整性机制（ICV），只是在密码学上很弱，并不是没有。

48. A Karma 攻击源自最初的 KARMA 工具包，它监控附近客户端广播的定向探测请求（这些客户端在寻找保存在首选网络列表中的 SSID）并作出响应，可能使客户端自动关联到这个恶意 AP。相反，Evil twin 攻击冒充的是某个特定的合法无线网络；该网络不必当前可见，也不必复制它的 BSSID。解除认证攻击只是断开客户端，并不收集探测请求。恶意 DHCP 攻击发生在关联之后，不涉及 SSID 探测响应欺骗。

49. D 密钥重装攻击（KRACK）利用 WPA2 四次握手，重放第 3 条消息，骗客户端重置 nonce 并重新安装已在使用的会话密钥，从而重置密钥流，使数据包可被解密或重放。它既不需要密码，也不会暴露密码，这与 PMKID 和字典攻击不同。Evil twin 是利用社会工程学的恶意 AP，WPS PIN 暴力破解针对的是无关的 8 位 PIN 机制。

50. A 过渡模式在同一个信标中同时通告 WPA2 和 WPA3 安全，对 Dragonblood 类降级攻击的研究表明，恶意 AP 或链路上的攻击者可以迫使同时支持两种模式的客户端使用旧的 WPA2 四次握手进行关联，这个握手可以被捕获，并像纯 WPA2 网络一样遭受离线字典破解。通过 WPA3 连接的客户端，SAE 仍然完全有效；两种模式下 PSK 都不会以明文广播；而 WPA2 这一侧的 PMF 通常是可选的，不是强制的，所以针对这些客户端的解除认证风险依然存在。

51. C 填充预言攻击利用的是应用泄露了解密后的填充是否有效，使攻击者在没有密钥的情况下逐字节恢复 CBC 模式的明文（例如 POODLE、Vaudenay 最初的攻击）。生日攻击针对的是哈希碰撞，不是填充验证。中间相遇攻击需要两次密文计算来找到匹配的中间值，与错误消息泄露无关。选择明文攻击需要攻击者控制加密，不是观察解密的错误响应。解密行为上任何可观察的差异都可能成为可被利用的侧信道。

52. C hashcat 支持模式 22000（WPA-PBKDF2-PMKID+EAPOL），可以用 GPU 加速、配合词表对捕获的 WPA2 握手做离线破解，是捕获之后的标准下一步。Responder 用于有线或本地网络上的 LLMNR/NBT-NS 投毒，不是离线握手破解。sqlmap 自动化 SQL 注入利用，与无线加密无关。Metasploit 的 psexec 模块执行的是经过认证的远程代码执行，不是从握手捕获中恢复密码。在进行任何捕获或破解之前，都必须获得测试目标网络的授权。

53. B POODLE（Padding Oracle On Downgraded Legacy Encryption）专门利用 SSLv3 中不确定的 CBC 填充验证，攻击者先迫使协议降级，再逐字节恢复明文。Heartbleed 是 OpenSSL 心跳扩展中的内存越界读取漏洞，与协议降级无关。CRIME 利用 TLS 层压缩泄露机密，不需要回退到 SSLv3。BEAST 针对的是 TLS 1.0 中 CBC 链接的弱点，不是 SSLv3 特有的降级攻击。彻底禁用 SSLv3 是标准的缓解措施。

54. B Logjam 式攻击利用的是许多服务器重复使用少数几个标准 DH 素数这一事实；国家级攻击者可以为这些共用的 512 位和 1024 位组预先计算离散对数表，实现近乎实时的密钥恢复。使用 P-256 的 ECDHE 采用椭圆曲线数学，在这个强度下没有类似的、可大规模使用的预计算破解。AES-256-GCM 是对称密码，与 DH 交换本身无关。RSA 签名密钥的长度影响的是证书认证，不是 DH 组的离散对数强度。

55. B 对称加密（例如 AES、DES、3DES）用同一个共享密钥完成加密和解密，速度快，但需要安全地分发密钥。非对称加密使用公钥/私钥对，所以两个操作用的是不同的密钥。哈希是单向函数，生成固定长度的摘要，不可逆，所以无法“解密”任何东西。数字签名依靠非对称密钥来证明真实性和完整性，不是用单个共享密钥加密数据。

56. C 数字签名（digital signature）的做法是：先对邮件做哈希（hash），得到固定长度的摘要，再用发件人的私钥加密。收件人用发件人的公钥解密，并与自己算出的哈希值比对，就能确认身份和完整性。用收件人的公钥加密整封邮件只能保密，不能证明来源。用收件人的公钥加密哈希值，别人无法验证。对称密钥需要事先交换，也做不到不可否认性（non-repudiation）。

57. D 基于 PMKID 的离线攻击（PMKID-based offline attack）利用部分接入点在第一个 EAPOL-Key 消息中带上的 PMKID，攻击者用 hcxdumptool 等工具捕获后，再用 hashcat 离线破解 PSK，不需要完整的四次握手，也不需要主动解除认证。KRACK 利用的是握手重传时的随机数重用。Evil twin 是冒充合法接入点。WPS PIN 暴力破解针对的是另外的 WPS 协议。足够强的随机 PSK 能抵御离线猜测。

58. D Diffie-Hellman 让双方用公开值和各自的私有指数做模幂运算（modular exponentiation），各自算出同一个共享密钥，所以密钥从未在线路上传送。窃听者截获的只是公开值，没有私有指数就没有用。RSA 数字签名用来认证数据，不能建立共享的对称密钥。AES-256 是对称加密算法，需要预先共享密钥。HMAC 提供消息完整性和认证，不负责协商密钥。

59. C 临时 Diffie-Hellman（ephemeral Diffie-Hellman）在每次握手时生成新的、只用于本次会话的密钥对，用完就丢弃私有指数。所以以后即使拿到服务器的长期密钥，也算不出过去的会话密钥，这就是完全前向保密（perfect forward secrecy）。静态 RSA 用服务器的长期公钥加密预主密钥（pre-master secret），密钥一旦被盗，所有已捕获的会话都能解密，TLS 1.3 因此删除了它。没有临时成分的 PSK 每次都重用同一个密钥，也就没有前向保密。Kerberos 是认证协议，不是 TLS 的密钥交换机制。

60. A NIST SP 800-57 第 1 部分的强度对照表（comparable-strength table）把 128 位对称密钥对应到 3072 位 RSA，因为因数分解算法不断改进，RSA 的强度比密钥长度增长得慢得多。1024 位 RSA 只相当于约 80 位的安全强度，已不建议使用。2048 位 RSA 约相当于 112 位，低于 128 位的目标。15360 位 RSA 相当于 256 位对称强度，远超需求，还会带来不必要的性能开销。

61. B 枚举（enumeration）紧接在扫描之后，在这个阶段测试人员主动提取用户名、共享名称、组成员和空会话数据，常用 enum4linux 或 rpcclient 这类工具。漏洞扫描找的是已知 CVE 和配置错误，不是用户名或共享。横幅抓取（banner grabbing）已经由 nmap 的版本扫描（-sV）完成，也拿不到共享和用户细节。主动侦察（active reconnaissance）是更早的信息收集阶段，在端口扫描之前，不是识别服务之后的下一步。

62. B 白帽黑客（white hat hacker）得到系统所有者的明确许可，并遵守签署的测试范围，所以行为合法、合乎道德。黑帽黑客没有授权，为个人利益或恶意目的行事。灰帽黑客没有许可就测试系统，但没有恶意，这仍然是违法的。脚本小子缺乏深入的技术能力，通常只会运行现成的工具，不管有没有授权。区分白帽和其他类型的关键就是授权。

63. B SYN 泛洪（SYN flood）是一种拒绝服务（denial-of-service）技术，耗尽服务器资源，让授权用户无法访问系统，直接攻击的是可用性，也就是需要时数据和服务能被访问。机密性指数据不被未授权披露，这里没有数据泄露。完整性指数据不被未授权修改，这里也没有记录被改动。不可否认性指行为可以追溯到责任人，它不属于经典的 CIA 三要素，是用来考你有没有把两种框架混在一起的干扰项。

64. C 扫描和枚举（scanning and enumeration）需要直接、主动地与目标主机交互，比如用 Nmap 做端口扫描、服务版本检测和操作系统指纹识别（OS fingerprinting），以画出攻击面的技术地图。侦察（reconnaissance）是更早的信息收集阶段，可以是被动的（OSINT），也可以是主动的，但在直接探测端口之前。获取访问权限指真正利用漏洞取得立足点，这里还没发生。维持访问是系统被攻陷后建立持久性，在攻击链（kill chain）中靠后得多。

65. B 灰帽黑客（gray hat hacker）没有正式授权，也没有签署测试合同，但没有恶意，常常负责任地披露发现的问题，正好符合这个情景。白帽黑客在测试前必须有明确的合同或授权，这里没有。自杀式黑客为了曝光目标，明知会被起诉也不顾后果。黑客行动主义者出于政治或社会目的，不是中立地发现漏洞。考试中的关键区分点是授权状态加上意图，而不是所用的技术。

66. D 红队演练（red team engagement）以目标为导向，评估面对真实对手时的检测和响应能力，而不是追求覆盖所有漏洞，通常也不会事先通知防守方。传统渗透测试覆盖面更广，通常有时间限制，目标是在范围内找出尽可能多的可利用漏洞。漏洞评估只做扫描和报告，不进行利用，也不是目标导向的模拟。漏洞赏金计划由大众参与、持续进行，没有题目描述的这种有协调、按场景推进的结构。

67. C 交战规则（Rules of Engagement，ROE）规定测试本身的操作细节：方法、允许的测试时间、紧急联系人，以及像支付网关这样的范围排除项。工作说明书（SOW）规定交付成果、时间表和费用，不涉及操作边界。保密协议（NDA）只管所交换信息的保密，不涉及测试流程。主服务协议（MSA）确定双方关系的总体法律和商业条款，不规定具体的测试细节或排除项。

68. C 测试任何没有在已签署范围中明确授权的系统，哪怕只是一点点，也会让测试人员面临民事责任和 CFAA（美国计算机欺诈和滥用法）风险，因为第三方从未同意被测试。正确的专业做法是在边界处停下，按交战规则（Rules of Engagement）规定的渠道上报，由客户决定如何和第三方处理。完整测试或者“只是确认一下”凭据，都属于对范围外系统的未授权访问。悄悄省略重要的安全发现，也违反了披露义务，而这个发现本身不能被进一步利用。

69. D nmap 服务扫描确认 445 端口（SMB）开放，这是扫描（scanning）活动，用来摸清存活的主机和服务。随后 enum4linux 主动向这个开放的服务查询共享名称、用户和组数据等详细信息，这就是枚举（enumeration）。所以这个顺序是“扫描，然后枚举”。侦察和踩点可以是被动收集信息，也可以是主动交互。获取访问权限需要利用漏洞，这里还没发生。清除痕迹发生在入侵之后。

70. C 被动侦察（passive reconnaissance）不与目标系统直接交互，使用 Shodan、WHOIS、DNS 记录和社交媒体等来源收集信息，在目标网络上不留痕迹。主动侦察需要与目标直接交互，比如 ping 扫描或端口扫描，可能被记录或发现。枚举是更靠后、更具侵入性的阶段，通过直接连接提取用户名或共享等细节。漏洞扫描会主动探测存活系统中的已知弱点，同样需要直接交互，也可能被发现。

英文关键词

footprinting	踩点（足迹收集）	攻击前收集目标的域名、邮箱、网络等信息
passive reconnaissance	被动侦察	不接触目标系统的信息收集
active reconnaissance	主动侦察	直接与目标系统互动，可能被记录
OSINT	公开来源情报	从公开资料收集到的信息
enumeration	枚举	连接服务，取得用户名、共享名等细节
banner grabbing	抓取横幅	读取服务返回的软件和版本信息
zone transfer (AXFR)	区域传送	复制整个 DNS 区域的记录
WHOIS lookup	WHOIS 查询	查询域名的注册人和联系人
rules of engagement (ROE)	交战规则	规定测试方法、时间和禁区的文件
scope	测试范围	授权可以测试的系统
white hat hacker	白帽黑客	有授权的安全测试人员
gray hat hacker	灰帽黑客	没有授权，但没有恶意
red team engagement	红队演练	模拟真实对手，测试检测和响应
CIA triad	CIA 三要素	机密性、完整性和可用性
pass-the-hash	哈希传递攻击	直接用 NTLM 哈希认证

Kerberoasting	Kerberoasting 攻击	申请服务票据后离线破解服务账户密码
golden ticket	黄金票据	用 krbtgt 哈希伪造的 TGT
rainbow table	彩虹表	预先算好的哈希与明文对照表
salting	加盐	哈希前加入随机值，用来防彩虹表
privilege escalation	权限提升（提权）	从低权限取得更高权限
persistence	持久化	重启后仍能保持访问的手段
rootkit	rootkit（隐藏型恶意工具）	隐藏进程、文件和连接的恶意工具
Alternate Data Stream (ADS)	备用数据流	NTFS 文件中可隐藏数据的附加流
MAC flooding	MAC 泛洪	填满交换机 CAM 表以便嗅探
pretexting	假托	编造身份或情景骗取信任
tailgating	尾随	趁人不察觉跟着进门
session hijacking	会话劫持	夺取已经认证的会话
session fixation	会话固定	登录前预先设定会话 ID 再使用
honeypot	蜜罐	引诱并观察攻击者的假系统
firewalking	防火墙探测	用 TTL 判断防火墙放行哪些端口
evasion	规避	躲过 IDS 或防火墙检测的方法
cross-site scripting (XSS)	跨站脚本	恶意脚本在受害者浏览器中执行
SQL injection	SQL 注入	用输入改变数据库查询的逻辑
server-side request forgery (SSRF)	服务端请求伪造	让服务器替攻击者发出请求
insecure deserialization	不安全的反序列化	不验证就把外来数据还原成对象
evil twin	邪恶双胞胎（假热点）	冒充特定 SSID 的恶意接入点
4-way handshake	四次握手	WPA2 客户端与 AP 建立密钥的过程
deauthentication	解除认证	用伪造的帧让客户端断线
perfect forward secrecy	完全前向保密	长期密钥泄露也解不开过去的会话
downgrade attack	降级攻击	迫使双方改用较弱的协议

Examundo 是独立网站，与主办这些考试的机构没有隶属关系，也未获其认可。题目均为原创，不是考试真题。 examundo.tech/zh/ceh/