examundo

Simulado CEH em português

70 questões com respostas. Os guias e as traduções foram feitos e revisados por software. Ainda não foram revisados por nenhuma pessoa.

Atualizado em 25 de novembro de 2026 · examundo.tech/pt/ceh/

Ataques a sistemas

1. Um pentester com credenciais de domínio válidas, mas de baixo privilégio, solicita tickets de serviço (TGS) de contas que têm Service Principal Names (SPN) registrados, extrai esses tickets e tenta quebrá-los offline para recuperar a senha em texto puro da conta de serviço. Como se chama esse ataque?

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
C. Kerberoasting
D. Golden ticket

---

2. Durante a pós-exploração (post-exploitation) em uma rede Windows, um pentester extrai um hash NTLM direto da memória do LSASS e o usa para se autenticar em um segundo servidor via SMB, sem nunca quebrá-lo para obter a senha em texto puro. Qual técnica de ataque isso descreve?

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
B. Envenenamento de LLMNR/NBT-NS (LLMNR/NBT-NS poisoning)
C. Golden ticket
D. Kerberoasting

---

3. Um pentester sabe que a senha do alvo segue o padrão de uma letra maiúscula, cinco minúsculas e dois dígitos (por exemplo, Summer24). Qual comando hashcat mira corretamente esse padrão em um arquivo de hashes 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?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. Um atacante esconde um executável malicioso em um Alternate Data Stream (ADS) de um arquivo de texto legítimo em um volume NTFS, usando o comando type malware.exe > notes.txt:hidden.exe. Qual característica dessa técnica a torna eficaz para escapar de uma detecção superficial?

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. A técnica funciona igual em sistemas de arquivos FAT32 e ext4

B. O antivírus não consegue verificar Alternate Data Streams em nenhuma circunstância

C. O stream oculto criptografa o próprio conteúdo automaticamente com EFS

D. O tamanho do arquivo notes.txt mostrado no Windows Explorer não reflete o conteúdo do stream oculto

---

5. Durante uma avaliação de pós-exploração em um host Linux, um pentester executa find / -perm -4000 -type f 2>/dev/null e descobre que o próprio /usr/bin/find tem o bit SUID ativado e pertence ao root. Qual ação aproveitaria MELHOR essa configuração incorreta para escalar privilégios?

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. Substituir o binário /usr/bin/find por um payload de reverse shell

B. Executar o find com -exec para abrir um shell como root

C. Usar o find para procurar hashes de senha em /etc/shadow

D. Modificar o /etc/passwd diretamente, já que o find tem permissão de escrita

---

6. Um analista forense descobre que os binários `ps`, `netstat` e `ls` de um servidor Linux comprometido foram trocados por versões modificadas que escondem dos comandos padrão os processos, as conexões de rede e os arquivos do atacante. Que TIPO de ferramenta maliciosa é essa?

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. Rootkit de userland (Userland rootkit)

B. Bomba lógica (Logic bomb)

C. Cavalo de Troia (Trojan horse)

D. Rootkit em modo kernel (Kernel-mode rootkit)

---

7. Um atacante usa wevtutil cl Security para limpar o log de eventos Security do Windows depois de terminar uma operação em uma estação de trabalho ingressada no domínio. Qual artefato MAIS provavelmente revela que o log foi limpo, mesmo com o conteúdo apagado?

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. O log System, que não pode ser limpo com o wevtutil e sempre fica intacto

B. O arquivo Prefetch do wevtutil.exe, que é apagado automaticamente quando o comando roda

C. O Event ID 1102 registrado no próprio log, indicando “The audit log was cleared”

D. A entrada do $MFT para o arquivo Security.evtx, que é imutável e não pode ser modificada

---

8. Um pentester obtém um arquivo de hashes de senhas do Windows e quer recuperar as senhas em texto puro comparando os hashes com uma grande tabela pré-calculada que associa cada hash à senha em texto puro. Qual técnica está sendo usada?

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. Ataque com rainbow table

B. Ataque de força bruta (brute-force)

C. Kerberoasting

D. Ataque de dicionário (dictionary attack)

---

9. Um atacante que comprometeu o hash NTLM da conta krbtgt forja um Ticket Granting Ticket (TGT) que dá acesso a qualquer serviço do domínio e continua válido até a senha da krbtgt ser redefinida duas vezes. Qual ataque isso descreve?

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

---

10. Um atacante com acesso SYSTEM em um sistema Windows quer criar persistência pelo registro que execute um aplicativo do subsistema nativo durante a inicialização do Session Manager, antes de o subsistema Windows carregar. Qual local do registro permite essa fase de execução?

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

Reconhecimento e footprinting

11. Um pentester enumera os registros DNS de target.com e encontra dois registros MX: mail.target.com com prioridade 10 e backupmx.target.com com prioridade 20. Qual afirmação identifica corretamente o servidor de e-mail principal?

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 é o principal, porque um valor de prioridade menor indica preferência maior
B. backupmx.target.com é o principal, porque um valor de prioridade maior indica preferência maior
C. Os valores de prioridade são ignorados; os registros MX são escolhidos em ordem alfabética
D. Os dois servidores são usados ao mesmo tempo, com a mesma preferência

---

12. Um pentester executa traceroute contra o endereço IP público do alvo para mapear o caminho de rede e identificar roteadores e firewalls intermediários antes de começar a varredura. Essa atividade se enquadra em qual categoria de 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. Somente footprinting passivo
B. Footprinting por engenharia social
C. Footprinting de DNS
D. Footprinting de rede

---

13. Durante o footprinting, um operador de red team consulta os registros DNS de um domínio alvo para planejar uma campanha de spear-phishing. Qual tipo de registro DNS dá a informação MAIS direta sobre a infraestrutura de e-mail da organização?

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. Um pentester executa `dig axfr @ns1.target.com target.com` tentando obter uma transferência de zona DNS completa durante a fase de reconhecimento de um trabalho. Do ponto de vista da metodologia, que tipo de reconhecimento descreve MELHOR essa ação?

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. Reconhecimento ativo, porque envia uma consulta direta a um sistema que pertence ao alvo e é operado por ele
B. Reconhecimento passivo, porque o dig é um utilitário de diagnóstico somente de leitura
C. Reconhecimento passivo, porque consultas DNS nunca tocam a infraestrutura que o alvo monitora
D. Reconhecimento ativo somente se a transferência der certo e retornar registros

---

15. Um pentester se conecta diretamente à porta 25 do alvo com netcat e lê o banner devolvido pelo servidor para descobrir o software e a versão do servidor de e-mail. Essa técnica é um exemplo de:

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. Varredura de vulnerabilidades (vulnerability scanning)
B. Enumeração, não footprinting
C. Footprinting ativo
D. Footprinting passivo

---

16. Qual ferramenta de reconhecimento foi feita como framework OSINT modular que automatiza a coleta de dados de fontes como redes sociais, WHOIS e buscadores, e mostra as relações em uma visualização em grafo?

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. Um pentester usa telnet para fazer banner grabbing no servidor de e-mail do alvo e recebe a resposta “220 mail.targetcorp.com ESMTP Postfix”. O que ele descobriu de forma mais direta?

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. Uma lista completa de endereços de e-mail dos funcionários
B. O registrador do domínio e o contato administrativo
C. O software do servidor de e-mail e, possivelmente, sua versão
D. A faixa completa de endereços IP públicos da organização

---

18. Qual combinação de operadores de busca do Google seria MAIS eficaz para localizar arquivos de configuração indexados publicamente que contenham a palavra “password” em um domínio alvo específico?

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. Na fase de reconhecimento, um hacker ético consulta um banco de dados público de registro para descobrir o nome do titular, a organização registrante e o contato administrativo do domínio do alvo. Qual atividade está sendo feita?

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. Transferência de zona DNS (DNS zone transfer)
B. Varredura de portas (port scanning)
C. Consulta WHOIS (WHOIS lookup)
D. Banner grabbing

---

20. Qual filtro de busca do Shodan um analista usaria para encontrar dispositivos expostos na internet localizados em um país específico?

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:

Redes e perímetro

21. Ao varrer uma sub-rede, um pentester encontra um host com muitas portas abertas, todas com banners de serviço idênticos e anormalmente detalhados, sem respostas que correspondam a handshakes de protocolo legítimos e com tempos de resposta anormalmente rápidos, seja qual for a consulta. Qual conclusão é a MAIS justificada?

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. O host provavelmente é um honeypot de baixa interação (low-interaction honeypot)
B. O host está rodando um sistema de prevenção de intrusão (IPS)
C. O host está atrás de um balanceador de carga (load balancer)
D. O host é um servidor de produção reforçado (hardened)

---

22. Um funcionário recebe um e-mail que parece vir do helpdesk de TI, pedindo a redefinição imediata da senha por um link que leva a uma página de login falsa. Qual técnica de engenharia social isso representa?

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. Um atacante inunda a tabela CAM de um switch com milhares de mapeamentos falsos de endereço MAC para porta, fazendo o switch entrar em modo fail-open e transmitir quadros por todas as portas, como um hub. Qual ataque está sendo executado?

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. Um atacante inunda a tabela CAM de um switch com milhares de endereços MAC de origem inventados. Qual é o objetivo principal desse ataque?

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

A. Forçar o switch ao modo fail-open para que transmita o tráfego por todas as portas, como um hub
B. Derrubar o sistema operacional do switch para causar negação de serviço
C. Obter acesso administrativo ao console do switch
D. Contornar totalmente a autenticação 802.1X baseada em porta

---

25. Um pentester envia pacotes de sondagem com valores de TTL crescentes em direção a um host atrás de um firewall e usa as mensagens ICMP Time Exceeded recebidas para descobrir quais portas específicas a ACL deixa passar pelo firewall. Qual técnica está sendo usada?

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. Mapeamento de caminho com traceroute comum
B. Firewalking
C. Identificação do sistema operacional (OS fingerprinting) pelo TTL
D. Banner grabbing

---

26. Uma técnica de evasão de IDS em que o atacante espalha deliberadamente o payload do ataque em muitos segmentos TCP pequenos, enviados com atraso intencional entre os pacotes, para que o tempo limite de remontagem do IDS expire antes de a assinatura completa ser reconhecida, é conhecida como:

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. Codificação polimórfica (polymorphic encoding)
C. Firewalking
D. Sobreposição de fragmentos (fragmentation overlap)

---

27. Um avaliador de segurança física se aproxima de uma porta com controle por crachá no momento em que um funcionário está saindo. O funcionário percebe o avaliador, supõe que é um colega e segura a porta aberta de bom grado. Isso é um exemplo de:

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, porque o funcionário permitiu a entrada de forma consciente
B. Tailgating, porque a entrada ocorreu sem nenhuma autorização
C. Shoulder surfing
D. Dumpster diving

---

28. Um pentester cria dados de payload maliciosos divididos em vários fragmentos IP pequenos e os envia a um alvo protegido por um sistema de detecção de intrusão (IDS) baseado em assinaturas. Qual técnica de evasão está sendo usada?

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. Fragmentação (fragmentation)
C. Spoofing
D. Criptografia (encryption)

---

29. Durante uma avaliação autorizada de engenharia social, um atacante liga para o help desk de TI fingindo ser um executivo em viagem que precisa urgentemente redefinir a senha, e informa matrícula e departamento inventados para ganhar credibilidade. Qual técnica de engenharia social está sendo demonstrada?

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. Depois que um pentester sequestra uma sessão TCP autenticada injetando segmentos falsificados com um número de sequência previsto corretamente, o cliente e o servidor legítimos passam a trocar um fluxo contínuo de pacotes de confirmação inválidos que nunca se ressincronizam. Como se chama esse efeito colateral?

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. Esgotamento do cache ARP (ARP cache exhaustion)

Aplicações web

31. Um servidor web de produção devolve stack traces detalhados, com números de versão do framework e caminhos de arquivos, sempre que ocorre uma exceção não tratada. Em qual categoria do OWASP Top 10 essa falha se encaixa?

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. Injeção (Injection)
B. Configuração incorreta de segurança (Security misconfiguration)
C. Falhas criptográficas (Cryptographic failures)
D. Falhas de identificação e autenticação (Identification and authentication failures)

---

32. Um pentester envia um ponto e vírgula seguido de um comando Linux em um campo de formulário web que faz uma consulta de ping no back-end, e a saída do comando adicional é devolvida na resposta. Qual classe de vulnerabilidade foi explorada?

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. Injeção de comandos do SO (OS command injection)
B. Injeção de SQL (SQL injection)
C. Desserialização insegura (Insecure deserialization)
D. Cross-site scripting

---

33. Um pentester envia uma consulta de busca com uma tag script, e a página de erro devolve o payload imediatamente na resposta HTML sem codificação, e o script é executado no navegador do pentester. Qual tipo de cross-site scripting é esse?

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. XSS refletido (Reflected XSS)
B. XSS cego (Blind XSS)
C. XSS armazenado (Stored XSS)
D. XSS baseado em DOM (DOM-based XSS)

---

34. Uma aplicação web Java aceita um objeto serializado em um parâmetro de cookie e o desserializa sem validação. Um pentester monta um payload serializado malicioso usando uma cadeia de gadgets (gadget chain) conhecida e consegue execução remota de código. Qual causa raiz permitiu esse ataque?

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. A aplicação desserializa dados controlados pelo atacante sem restrição de tipo nem verificação de integridade
B. A aplicação usa um conjunto de cifras TLS desatualizado no transporte do cookie
C. A aplicação guarda o estado da sessão em um cookie no cliente, em vez de no servidor
D. A aplicação não define a flag HttpOnly no cookie

---

35. Uma aplicação web permite que o usuário informe uma URL que o servidor busca para gerar uma prévia em miniatura. Um pentester informa um endereço interno de metadados da nuvem, e a resposta inclui credenciais da instância. Qual vulnerabilidade foi explorada?

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. Referência direta insegura a objetos (Insecure direct object reference, IDOR)
D. Server-side request forgery (SSRF)

---

36. Uma aplicação aceita um objeto Java serializado em base64 vindo de um cookie e o reconstrói no servidor sem validação, permitindo que um atacante cause execução remota de código com um objeto manipulado. Qual vulnerabilidade permitiu esse ataque?

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. Desserialização insegura (Insecure deserialization)
D. Controle de acesso quebrado (Broken access control)

---

37. Antes de a vítima fazer login, um atacante envia a ela um link com um identificador de sessão já definido. Depois que a vítima se autentica, a aplicação não gera um novo ID de sessão, e o atacante usa o mesmo identificador para acessar a sessão já autenticada. Qual ataque é esse?

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. Fixação de sessão (Session fixation)
C. Sequestro de sessão por captura de pacotes (session hijacking via packet sniffing)
D. Cross-Site Request Forgery

---

38. Qual ferramenta é MAIS usada por pentesters como proxy de interceptação (intercepting proxy) para inspecionar e modificar requisições HTTP entre um navegador e uma aplicação 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. Ao testar uma aplicação web feita em Flask, um pentester envia a entrada '{{7*7}}' em um campo de formulário de feedback, e a página renderizada passa a mostrar '49' em vez do texto literal. Qual vulnerabilidade esse comportamento confirma?

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. Injeção de SQL em que 7*7 é avaliado como expressão aritmética do banco de dados
B. Server-side template injection (SSTI) por meio do mecanismo de templates Jinja2
C. Cross-site scripting refletido por saída HTML sem escape
D. Injeção de template no cliente processada pelo sandbox de expressões do AngularJS

---

40. Qual tipo de ataque ocorre quando uma entrada não confiável do usuário é inserida em uma consulta de banco de dados sem a devida sanitização, permitindo que o atacante altere a lógica da consulta?

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. Injeção de SQL
C. Server-side request forgery
D. Cross-site scripting

Redes sem fio

41. Uma organização ativa o Protected Management Frames (802.11w) em toda a sua infraestrutura sem fio. Qual técnica comum de ataque a redes sem fio esse controle mitiga PRINCIPALMENTE?

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

A. Ataques de servidor DHCP falso (rogue DHCP)
B. Ataques de dicionário offline contra handshakes capturados
C. Ataques de força bruta ao PIN do WPS
D. Falsificação de quadros de desautenticação e desassociação (deauthentication and disassociation)

---

42. Um pentester quer obter material de credencial de uma rede WPA2-PSK sem esperar que um cliente legítimo se autentique. Qual técnica atinge MELHOR esse objetivo?

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. Executar um ataque de força bruta ao PIN do WPS com o Reaver

B. Enviar quadros de desautenticação e esperar para capturar o handshake de 4 vias de um cliente

C. Capturar o PMKID do primeiro quadro EAPOL do AP com o hcxdumptool

D. Fazer ARP spoofing contra clientes já conectados ao AP

---

43. Um operador de red team monta um ponto de acesso falso (rogue access point) que transmite o mesmo SSID e uma intensidade de sinal parecida com a de uma rede corporativa, para atrair funcionários a se conectarem, e então intercepta o tráfego deles. Qual ataque isso descreve, e como ele difere de um ataque Karma?

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. Ataque de desautenticação; força os clientes a desconectar antes de imitar a rede

B. Evil twin; responde a todo SSID que um cliente já procurou

C. Ataque Karma; imita um SSID específico e conhecido, em vez de responder a todas as sondagens (probe requests) de um cliente

D. Evil twin; imita um SSID específico e conhecido, em vez de responder a todas as sondagens (probe requests) de um cliente

---

44. Um pentester mira um ponto de acesso com WPS ativado, esperando recuperar a senha WPA2. Qual ataque explora a geração fraca de números aleatórios nos nonces E-S1/E-S2 do enrollee em certos chipsets, permitindo calcular o PIN do WPS offline em segundos, em vez de força bruta 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. Ataque PMKID contra o RSN IE

B. Força bruta online do PIN do WPS com o Reaver

C. Ataque KRACK contra o handshake de quatro vias

D. Ataque Pixie Dust

---

45. Um pentester autorizado avalia uma rede corporativa WPA2-PSK e quer capturar o handshake de quatro vias para um ataque de dicionário offline. Qual técnica é MAIS usada para forçar um cliente conectado a se reautenticar e permitir a captura do 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. Enviar quadros de desautenticação com o aireplay-ng

B. Rebaixar a conexão com um proxy de SSL strip

C. Fazer envenenamento de cache ARP contra o cliente

D. Enviar respostas DNS falsificadas ao cliente

---

46. Um pentester configura um ponto de acesso falso que transmite o mesmo SSID de uma rede corporativa legítima para atrair funcionários a se conectarem e interceptar suas credenciais. Qual ataque isso descreve?

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

B. ARP spoofing

C. Bluejacking

D. Ataque ao PIN do WPS

---

47. Um avaliador quebra uma chave WEP antiga em minutos coletando muito tráfego e analisando padrões de vetores de inicialização (IV) repetidos usados com a cifra RC4. Qual falha fundamental de projeto do WEP isso explora?

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. O SAE permite que o atacante force o uso de uma suíte de cifras mais fraca

B. A verificação de integridade Michael do TKIP pode ser burlada com um ataque chopchop

C. O handshake de quatro vias não tem nenhum código de integridade de mensagem

D. O espaço de IV de 24 bits é pequeno o bastante para causar colisões frequentes no keystream

---

48. Qual ataque de engenharia social em redes sem fio faz um ponto de acesso falso responder de forma afirmativa às sondagens (probe requests) de QUALQUER SSID da lista de redes preferidas de um cliente próximo, em vez de imitar uma rede específica e conhecida?

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. Ataque Karma

B. Ataque de DHCP falso (rogue DHCP)

C. Ataque evil twin

D. Ataque de desautenticação

---

49. Um pesquisador divulga uma vulnerabilidade que permite a um atacante posicionado como man-in-the-middle manipular as retransmissões do handshake e forçar a reinstalação de uma chave de criptografia já usada, possibilitando decifrar o tráfego do cliente sem conhecer a senha. Como se chama esse ataque?

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

B. Força bruta ao PIN do WPS

C. Ataque PMKID

D. KRACK

---

50. Uma rede transmite WPA3-Personal em “modo de transição” (transition mode) para manter compatibilidade com clientes WPA2 antigos. Qual risco essa configuração traz?

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

A. Um atacante pode forçar um cliente a voltar ao handshake WPA2, mais fraco (downgrade), permitindo um ataque de dicionário offline tradicional

B. O AP transmite a PSK em texto puro para manter a compatibilidade com versões anteriores

C. A prova de conhecimento zero (zero-knowledge proof) do SAE é totalmente desativada para todos os clientes

D. O 802.11w Protected Management Frames passa a ser obrigatório só para clientes WPA3, eliminando o risco de deauth para clientes WPA2

Criptografia

51. Um pentester descobre que uma aplicação web devolve mensagens de erro diferentes para padding inválido e para MAC inválido quando um cookie modificado, criptografado em CBC, é enviado. Qual ataque esse comportamento viabiliza?

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. Ataque de texto claro escolhido (chosen-plaintext attack)
B. Ataque meet-in-the-middle
C. Ataque de padding oracle (padding oracle attack)
D. Ataque do aniversário (birthday attack)

---

52. Durante uma avaliação de rede sem fio, um pentester captura um handshake de 4 vias do WPA2 com o airodump-ng depois de desautenticar um cliente com o aireplay-ng. Qual ferramenta ele MAIS provavelmente usaria em seguida para recuperar a chave pré-compartilhada 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. módulo psexec do Metasploit

---

53. Um pentester descobre que um servidor web antigo ainda aceita conexões SSLv3, embora também suporte TLS 1.2. Qual ataque se torna viável contra clientes que podem ser forçados a recuar (fall back) para o 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. Um pentester observa tráfego de rede com uma troca de chaves Diffie-Hellman entre um cliente e um servidor. Qual condição tornaria viável recuperar o segredo compartilhado por meio de um ataque pré-calculado, no estilo Logjam?

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. O certificado do servidor usa uma chave de assinatura RSA de 2048 bits
B. O servidor negocia um grupo DH de 512 ou 1024 bits amplamente reutilizado
C. O servidor usa ECDHE com a curva P-256
D. O cliente e o servidor negociam a suíte de cifras AES-256-GCM

---

55. Qual tipo de criptografia usa a mesma chave para cifrar e decifrar os dados?

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

A. Criptografia assimétrica (asymmetric encryption)
B. Criptografia simétrica (symmetric encryption)
C. Assinatura digital (digital signature)
D. Hash (hashing)

---

56. Um usuário quer assinar digitalmente um e-mail para que o destinatário possa verificar a identidade do remetente e também que a mensagem não foi alterada no caminho. Qual processo descreve MELHOR como a assinatura é gerada?

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. Criptografar o resumo da mensagem (message digest) com uma chave simétrica compartilhada

B. Criptografar a mensagem inteira com a chave pública do destinatário

C. Calcular o hash da mensagem e depois criptografar o hash com a chave privada do remetente

D. Calcular o hash da mensagem e depois criptografar o hash com a chave pública do destinatário

---

57. Um auditor de redes sem fio captura um único hash PMKID diretamente do primeiro quadro EAPOL de um ponto de acesso, sem observar nenhum cliente completar o handshake de 4 vias e sem fazer um ataque de desautenticação (deauthentication). Qual técnica de ataque contra WPA2-PSK isso descreve?

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. Ataque evil twin

B. Ataque de força bruta ao PIN do WPS

C. Ataque de reinstalação de chave KRACK

D. Ataque offline baseado em PMKID

---

58. Durante uma avaliação de segurança de rede, um engenheiro observa dois hosts estabelecendo uma chave secreta compartilhada por um canal inseguro, sem nunca transmitir a chave em si. Qual mecanismo criptográfico isso descreve?

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. Assinatura digital RSA

B. Criptografia AES-256

C. Autenticação HMAC

D. Troca de chaves Diffie-Hellman

---

59. Um CISO determina que, se a chave privada RSA de longo prazo do servidor web for comprometida no futuro, isso não deve permitir descriptografar o tráfego TLS capturado antes. Qual mecanismo de troca de chaves atende a esse requisito?

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. Troca de tickets Kerberos

B. Troca de chave pré-compartilhada (PSK) sem componente efêmero

C. Diffie-Hellman efêmero (DHE ou ECDHE)

D. Troca de chaves RSA estática

---

60. Um arquiteto de segurança precisa de um tamanho de chave RSA com força criptográfica aproximadamente equivalente a uma chave simétrica de 128 bits, segundo as recomendações da NIST SP 800-57. Qual tamanho de chave deve ser escolhido?

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 bits

B. 2048 bits

C. 1024 bits

D. 15360 bits

Fundamentos de hacking ético

61. Em uma fase pré-ataque, um pentester executa 'nmap -sV -p 445 10.10.10.5' e confirma uma porta SMB aberta com informações de versão. Para extrair nomes de compartilhamentos, listas de contas de usuário e detalhes de sessão nula (null session), qual fase da metodologia o pentester deve executar EM SEGUIDA?

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. Captura de banners (banner grabbing)
B. Enumeração (enumeration)
C. Reconhecimento ativo (active reconnaissance)
D. Varredura de vulnerabilidades (vulnerability scanning)

---

62. Qual termo descreve um profissional de segurança autorizado por uma organização a testar seus sistemas em busca de vulnerabilidades usando as mesmas técnicas de atacantes mal-intencionados?

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 black hat
B. Hacker white hat
C. Hacker gray hat
D. Script kiddie

---

63. Um atacante inunda o servidor web de agendamento de pacientes de um hospital com pacotes TCP SYN malformados, impedindo que a equipe legítima acesse o sistema por seis horas. Qual componente da tríade CIA é PRINCIPALMENTE comprometido por esse ataque?

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. Integridade
B. Disponibilidade
C. Confidencialidade
D. Não repúdio

---

64. Durante um trabalho autorizado, um pentester usa o Nmap para identificar portas abertas, serviços em execução e versões de sistema operacional em uma sub-rede alvo, antes de tentar qualquer exploração. Qual fase da metodologia de hacking essa atividade representa?

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. Manutenção de acesso (maintaining access)
B. Reconhecimento (reconnaissance)
C. Varredura e enumeração (scanning and enumeration)
D. Obtenção de acesso (gaining access)

---

65. Uma pesquisadora de segurança, agindo por conta própria e sem nenhum contrato, descobre uma falha de XSS armazenado no portal de login público de uma empresa apenas navegando nele. Ela não explora a falha além disso e a comunica de forma privada à equipe de segurança do fornecedor. A MELHOR classificação para essa pessoa é:

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. Hacktivista
B. Hacker gray hat
C. Suicide hacker
D. Hacker white hat

---

66. Uma organização quer medir com que rapidez seu SOC detecta e responde a uma invasão simulada, furtiva e em várias etapas, sem avisar os defensores antes e sem tentar catalogar todas as vulnerabilidades do escopo. A MELHOR descrição desse trabalho é:

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. Programa de bug bounty
B. Teste de invasão (penetration test)
C. Avaliação de vulnerabilidades (vulnerability assessment)
D. Exercício de red team (red team engagement)

---

67. Um documento assinado entre uma empresa de pentest e seu cliente define a metodologia exata de teste, as janelas de teste permitidas, os procedimentos de escalonamento para contatos de emergência e a exclusão explícita do gateway de pagamento de produção dos testes. A MELHOR classificação para esse documento é:

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. Contrato-mestre de serviços (Master Service Agreement, MSA)
B. Acordo de confidencialidade (Non-Disclosure Agreement, NDA)
C. Regras de engajamento (Rules of Engagement, ROE)
D. Declaração de trabalho (Statement of Work, SOW)

---

68. Durante um teste de invasão externo autorizado, um pentester encontra no servidor web do cliente credenciais que também autenticam com sucesso em uma plataforma SaaS de terceiros que não consta em nenhum lugar do documento de escopo assinado. Qual é a ação MAIS adequada que o pentester deve tomar PRIMEIRO?

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. Omitir a descoberta do relatório final, já que o sistema de terceiros está fora do escopo assinado
B. Testar imediatamente as credenciais na plataforma de terceiros para confirmar que a falha é explorável
C. Parar, não testar o sistema de terceiros e comunicar a descoberta ao cliente conforme o procedimento de escalonamento das ROE
D. Explorar a plataforma de terceiros só o suficiente para demonstrar o impacto e depois parar

---

69. Um pentester executa 'nmap -sV -p445 10.0.5.20' e, depois de ver a porta aberta, usa o 'enum4linux' para obter nomes de compartilhamentos e listas de contas de usuário do host. Quais duas fases da metodologia de ethical hacking essa sequência de ações representa?

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. Footprinting seguido de ocultação de rastros (covering tracks)
B. Enumeração seguida de manutenção de acesso
C. Reconhecimento seguido de obtenção de acesso
D. Varredura seguida de enumeração

---

70. Um pentester pesquisa no Shodan.io para identificar dispositivos da organização alvo expostos na internet, sem enviar nenhum pacote diretamente à rede do alvo. Essa atividade é um exemplo de:

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. Varredura de vulnerabilidades
B. Reconhecimento ativo
C. Reconhecimento passivo
D. Enumeração

Resposta correta

1. C No Kerberoasting, você usa credenciais de domínio válidas para pedir tickets de serviço de contas com SPN e os quebra offline para obter a senha. O AS-REP roasting mira contas com pré-autenticação Kerberos (Kerberos pre-authentication) desativada e nem exige credenciais válidas. O golden ticket forja um TGT com o hash da krbtgt, sem pedir tickets legítimos. O pass-the-ticket reutiliza um ticket roubado, sem quebrá-lo offline.

2. A No pass-the-hash, o próprio hash capturado serve como prova de identidade, porque o NTLM não precisa da senha em texto puro para autenticar. O Kerberoasting mira tickets de serviço Kerberos para quebra offline, não reutiliza hashes. O golden ticket forja TGTs com o hash da krbtgt. O envenenamento de LLMNR/NBT-NS captura hashes por resolução de nomes falsa, mas não descreve a reutilização do hash.

3. A O comando correto usa -m 1000 (NTLM), -a 3 (ataque por máscara, mask attack) e a máscara ?u?l?l?l?l?l?d?d: uma maiúscula, cinco minúsculas e dois dígitos. A versão com ?u na sexta posição erra a ordem. O -a 0 é o modo de dicionário (straight) e pede uma wordlist, não uma máscara. O -m 1800 é sha512crypt, tipo de hash errado para NTLM.

4. D O NTFS guarda o stream separado do fluxo de dados principal. Por isso a listagem de diretório e o tamanho mostrado no Explorer para notes.txt não incluem o payload oculto. Ferramentas como dir /r ou o streams da Sysinternals revelam o stream. O ADS é um recurso exclusivo do NTFS, não existe em FAT32 nem ext4. Antivírus e EDR modernos verificam ADS, e o EFS não é aplicado automaticamente.

5. B Um binário SUID roda com o UID efetivo do dono. Com o find SUID root, o comando find . -exec /bin/sh -p \; -quit abre um shell root na hora. Substituir o binário exige permissão de escrita no arquivo ou na pasta, que um usuário comum dificilmente tem. Editar o /etc/passwd também não é algo que o find permita sozinho. Procurar em /etc/shadow não mostra o conteúdo e ainda exigiria quebrar as senhas.

6. A Trocar binários do sistema como ps, ls e netstat por versões adulteradas para esconder rastros é o comportamento clássico de um rootkit de userland. O rootkit em modo kernel esconde coisas interceptando chamadas de sistema ou alterando estruturas do kernel, não trocando binários. O cavalo de Troia se disfarça de software legítimo. A bomba lógica dispara por uma condição e não esconde nada.

7. C Limpar o log Security com o wevtutil gera o Event ID 1102, “The audit log was cleared”, que fica como uma das poucas entradas no log recém-esvaziado e acusa a adulteração para o SOC ou o SIEM. O Prefetch do wevtutil.exe não é apagado, e o log System também pode ser limpo (wevtutil cl System). As entradas do $MFT não são imutáveis, mas não são o principal sinal de limpeza de logs.

8. A O ataque com rainbow table usa cadeias de hashes pré-calculadas, ligadas a senhas candidatas. Assim, achar a senha a partir do hash é uma consulta rápida, sem recalcular nada: troca-se espaço de armazenamento por velocidade. O ataque de dicionário calcula o hash de uma lista de palavras na hora. A força bruta testa todas as combinações. O Kerberoasting só obtém hashes de tickets de serviço. O salting é a defesa contra rainbow tables.

9. B O golden ticket forja um TGT válido para todo o domínio usando o hash da krbtgt, dando acesso persistente e quase ilimitado até a senha da krbtgt ser trocada duas vezes. O silver ticket forja um TGS de um único serviço com o hash dessa conta de serviço, com alcance menor. O DCSync abusa de direitos de replicação para puxar hashes. O pass-the-hash reutiliza um hash NTLM e não forja tickets Kerberos.

10. C O valor BootExecute, em HKLM\System\CurrentControlSet\Control\Session Manager, executa aplicativos nativos antes de o subsistema Windows carregar, na inicialização do Session Manager (SMSS.exe). São executáveis PE do subsistema nativo, não programas Win32 comuns. O conteúdo padrão é “autocheck autochk *”. A chave Run inicia programas no logon, Userinit cuida da inicialização do logon e User Shell Folders define pastas do shell.

11. A Pela RFC 5321, os servidores de e-mail escolhem primeiro o registro MX com o menor valor numérico e só passam para os maiores se o host preferido estiver fora do ar. Por isso 10 é preferido a 20. Inverter essa regra é uma pegadinha clássica de prova. Não há ordem alfabética: só o campo de prioridade conta. Só há divisão de carga quando dois registros têm o mesmo valor, e aí a ordem é aleatória.

12. D O traceroute mapeia o caminho salto a salto até o alvo e revela roteadores, provedores e possíveis limites de firewall ou balanceador. Isso é footprinting de rede (network footprinting). Não é passivo, pois envia pacotes com TTL crescente direto ao IP do alvo e observa as respostas. Também não é engenharia social, que coleta informação de pessoas, nem footprinting de DNS, que trata de registros de nomes.

13. A Os registros MX (Mail Exchange) listam os servidores que recebem e-mail do domínio e suas prioridades. Isso mostra direto a infraestrutura de e-mail que um atacante de phishing quer falsificar ou atacar. O NS só identifica os servidores de nomes autoritativos da zona. O SOA traz dados administrativos da zona, como número de série e intervalos. O PTR faz a consulta reversa de IP para nome e não tem relação com a entrega de e-mail.

14. A A solicitação de transferência de zona vai direto ao servidor de nomes autoritativo do próprio alvo, que pode registrar, limitar ou alertar sobre ela. Por isso é reconhecimento ativo, mesmo que a ferramenta só leia dados. O reconhecimento passivo usa fontes de terceiros (registros WHOIS, caches de buscadores, logs de Certificate Transparency). O que define o tipo é a interação, não o resultado: um AXFR que falha continua sendo ativo.

15. C O banner grabbing exige abrir uma conexão TCP direta com o serviço e ler a resposta, ou seja, interagir com a infraestrutura do alvo. Por isso é footprinting ativo, e não passivo. Não é varredura de vulnerabilidades, que testa falhas conhecidas em vez de só identificar software e versão. Continua sendo footprinting, pois acontece na coleta de informações, antes da enumeração formal.

16. A O Maltego liga entidades como pessoas, domínios, e-mails e organizações encontradas por várias transforms OSINT e mostra as relações em um grafo interativo. Por isso é a escolha padrão para análise visual de vínculos no reconhecimento. O Nmap é um scanner de rede e portas. O Hydra quebra credenciais por força bruta. O Responder envenena tráfego LLMNR/NBT-NS. Nenhum dos três gera grafos OSINT.

17. C O banner grabbing captura a mensagem de saudação que um serviço aberto devolve. Esse banner SMTP mostra o agente de transferência de e-mail (Postfix) e o nome do host, mas sem número de versão. Outros banners podem revelar a versão. A faixa de IPs exige consultas de ASN ou WHOIS. Registrador e contato vêm do WHOIS. Listas de e-mails exigem outra coleta OSINT. Esse é um exemplo clássico de footprinting ativo.

18. C A consulta site:target.com filetype:conf intext:password limita os resultados ao domínio, a arquivos .conf indexados e ao texto "password", que é exatamente o objetivo. O inurl:admin só filtra URLs com "admin" e não tem relação com arquivos de configuração. O operador link: foi descontinuado e buscava páginas que apontam para uma URL. O cache: mostrava a cópia guardada pelo Google, recurso que foi encerrado.

19. C A consulta WHOIS pergunta a registros regionais da internet (ARIN, RIPE etc.) ou a registradores de domínio e devolve dados de titularidade, como nome, organização e contatos. A transferência de zona DNS copia o arquivo inteiro da zona, não dados do titular. O banner grabbing captura respostas de serviços em portas abertas. A varredura de portas só identifica portas abertas, fechadas ou filtradas. O WHOIS é um passo passivo, feito antes de qualquer contato com o alvo.

20. B O filtro country: limita os resultados a dispositivos cuja geolocalização do IP corresponde ao código de país de duas letras informado, como country:US. O geo: busca por coordenadas de latitude e longitude, não por país. O org: busca pelo nome da organização ou do provedor do IP. O hostname: busca por um nome de host, sem relação com localização.

21. A Honeypots de baixa interação simulam serviços com banners genéricos e prontos e raramente implementam o protocolo completo. O resultado são respostas uniformes ou inconsistentes e rápidas demais. Um servidor de produção reforçado segue o protocolo corretamente e costuma ter poucas portas abertas. Balanceadores distribuem tráfego e não inventam banners idênticos. Um IPS bloqueia ou reinicia tráfego malicioso, não gera banners falsos.

22. B O phishing usa e-mails enganosos, muitas vezes se passando por uma fonte confiável como o suporte de TI, para levar a vítima a clicar em links maliciosos ou digitar credenciais em uma página falsa. O vishing usa ligações de voz. O pretexting usa uma identidade ou cenário inventado e pode ocorrer por e-mail, mas "phishing" é a resposta mais específica aqui. O tailgating é uma invasão física, sem relação com e-mail.

23. C O MAC flooding sobrecarrega a tabela CAM (content-addressable memory) do switch, que tem tamanho limitado, com entradas falsas. Quando ela enche, muitos switches entram em fail open e enviam o tráfego por todas as portas, o que permite capturar tráfego (sniffing) em uma rede comutada. O ARP spoofing manipula caches ARP dos hosts. O VLAN hopping explora erros de configuração de trunk. O DHCP starvation esgota o pool de endereços DHCP.

24. A O objetivo é forçar o fail-open para conseguir capturar o tráfego (sniffing). O MAC flooding sobrecarrega a tabela CAM (content-addressable memory), de tamanho limitado. Quadros com MAC de destino desconhecido podem então ser enviados às outras portas da mesma VLAN, e o atacante captura parte do tráfego de outros hosts. O tráfego com destino conhecido continua comutado normalmente. Derrubar o SO é outro tipo de DoS, o console exige credenciais ou exploits, e o 802.1X trata de autenticação.

25. B O firewalking usa o aumento do TTL contra um gateway conhecido para descobrir quais portas e protocolos a ACL permite, conforme voltem mensagens Time Exceeded de além do firewall. O traceroute comum mapeia o caminho até o destino, mas não busca regras de ACL. O OS fingerprinting por TTL deduz o sistema operacional pelo TTL inicial das respostas, não as regras de filtragem. O banner grabbing captura versões de serviços e não usa TTL.

26. A No session splicing (ou session slicing), o payload é enviado aos poucos em muitos segmentos TCP pequenos e com atraso. O sensor estoura o tempo de remontagem e descarta o que montou antes de ver a assinatura inteira, enquanto o host alvo, com tempo maior ou sem limite, remonta tudo. A sobreposição de fragmentos explora ambiguidade na ordem de remontagem, não o tempo. O firewalking mapeia regras com TTL, e a codificação polimórfica muda o padrão de bytes do payload.

27. A No piggybacking, uma pessoa autorizada permite a entrada de outra de forma consciente, mesmo que por engano, como ao segurar a porta achando que o avaliador pertence ali. Há consentimento, ainda que baseado em engano. No tailgating, a pessoa não autorizada passa por uma entrada segura sem que a pessoa autorizada saiba. O dumpster diving é vasculhar lixo atrás de material sensível, e o shoulder surfing é espiar alguém digitando credenciais.

28. B A evasão por fragmentação divide o payload em vários fragmentos IP, de modo que o mecanismo de assinaturas nunca vê a sequência maliciosa completa em um único pacote, sobretudo se o IDS remonta os fragmentos de forma diferente do host alvo. A criptografia esconde o conteúdo, mas não divide o payload. O flooding sobrecarrega recursos. O spoofing falsifica o endereço de origem, não a estrutura do payload.

29. A No pretexting, o atacante cria um cenário ou identidade falsa para ganhar confiança e levar o alvo a agir, como redefinir uma senha. O phishing usa mensagens eletrônicas enganosas (e-mail ou SMS), não uma farsa ao vivo. O tailgating é seguir uma pessoa autorizada por uma porta segura. O baiting atrai a vítima com uma isca física ou digital, como um pendrive infectado, o que não aparece aqui.

30. C Com a sessão sequestrada e dessincronizada, cliente e servidor guardam números de sequência que o outro lado não aceita. Cada pacote enviado gera um ACK com o número esperado, que também é rejeitado, e isso cria um ciclo que se alimenta sozinho, o ACK storm, até a conexão expirar ou ser reiniciada. O SYN flood abusa do handshake de três vias. O esgotamento do cache ARP é da camada 2. O DNS amplification é um DoS por reflexão.

31. B A configuração incorreta de segurança inclui mensagens de erro detalhadas ou informações de depuração deixadas ativas em produção. Elas expõem versões e detalhes do framework, que ajudam o atacante a identificar as tecnologias usadas e escolher exploits. A correção é desativar o modo debug e mostrar páginas de erro genéricas. Não é injeção, pois nenhuma entrada altera comandos ou consultas. Também não envolve login, sessão ou criptografia fraca.

32. A Acrescentar um metacaractere de shell, como o ponto e vírgula, para encadear um comando de sistema à chamada do ping é a marca da injeção de comandos do SO. O atacante executa comandos com os privilégios do processo do servidor web. O cross-site scripting atinge o navegador da vítima, não o shell do servidor. A injeção de SQL manipula consultas de banco de dados. A desserialização insegura explora a reconstrução de objetos serializados, outra superfície de ataque.

33. A No XSS refletido, a entrada é devolvida de imediato na resposta do servidor, sem ser guardada. A vítima o dispara ao seguir um link manipulado ou enviar um formulário malicioso, por isso não é persistente. No XSS armazenado, o payload fica salvo no servidor, por exemplo no banco de dados, e atinge todo visitante da página. No XSS baseado em DOM, a falha está só no JavaScript do cliente. No XSS cego, o payload dispara em um contexto fora de vista, como um painel de admin.

34. A A desserialização insegura ocorre quando a aplicação desserializa entrada não confiável sem limitar as classes permitidas nem verificar a integridade. O atacante então fornece uma gadget chain: uma sequência de classes legítimas cujos efeitos, encadeados na desserialização, executam código. A cifra TLS afeta a confidencialidade do transporte. Guardar a sessão no cliente é outra decisão de projeto. A falta de HttpOnly permite roubo de cookie via XSS, mas não causa RCE.

35. D No SSRF, o próprio servidor é induzido a fazer uma requisição a um destino escolhido pelo atacante. Aqui ele alcançou um serviço interno de metadados, normalmente inacessível pela internet pública. O cross-site scripting roda no navegador da vítima, não no servidor que faz chamadas de saída. O IDOR é acesso não autorizado a um objeto por um identificador manipulável. O path traversal usa sequências de caminho para sair de um diretório, não requisições HTTP remotas.

36. C A desserialização insegura acontece quando dados serializados não confiáveis viram objetos sem validação de tipo ou integridade. Um objeto manipulado pode acionar caminhos de código não previstos, muitas vezes por gadget chains presentes no classpath, e levar à execução remota de código. O cross-site request forgery forja uma requisição autenticada. O controle de acesso quebrado é falha de autorização. O clickjacking é um ataque de interface com enquadramento transparente.

37. B Na fixação de sessão, o atacante impõe ou fornece à vítima um ID de sessão conhecido antes da autenticação, e a aplicação não emite um ID novo após o login. Assim ele reutiliza o ID para entrar na sessão autenticada. No sequestro por sniffing, o token de uma sessão existente é interceptado no trânsito. O CSRF forja uma requisição com o cookie da própria vítima, e o clickjacking induz um clique em um elemento disfarçado. A correção é gerar um novo ID de sessão a cada mudança de privilégio, como o login.

38. A O Proxy do Burp Suite fica entre o navegador e a aplicação alvo e captura requisições e respostas HTTP e HTTPS ao vivo, permitindo modificá-las à mão ou de forma automática. Isso é essencial para testar injeção, autenticação e falhas de lógica de negócio. O Nmap é um scanner de rede e portas, não um proxy HTTP. O Hashcat quebra senhas a partir de hashes capturados. O Wireshark só captura e analisa pacotes de forma passiva.

39. B O payload '{{7*7}}' renderizado como '49' é o teste clássico de SSTI no Jinja2, o mecanismo de templates padrão do Flask: a entrada é interpretada e avaliada como sintaxe de template, não tratada como dado. O XSS refletido apareceria como script ou HTML no navegador, sem fazer a conta no servidor. A injeção de template do AngularJS é do lado do cliente. A injeção de SQL ocorre em consultas de banco. A SSTI pode chegar à execução remota de código se o sandbox for escapado.

40. B Na injeção de SQL (SQL injection), a entrada do atacante com metacaracteres SQL (', --, OR 1=1) é concatenada direto na consulta e muda sua lógica, para burlar a autenticação ou extrair dados. O cross-site scripting injeta script na saída do navegador, não em consultas. O cross-site request forgery força o navegador de um usuário autenticado a enviar uma requisição indesejada. O server-side request forgery faz o servidor acessar destinos não previstos.

41. D O 802.11w protege criptograficamente os quadros de gerenciamento robustos, incluindo os de desautenticação e desassociação (unicast e broadcast). Isso reduz a falsificação desses quadros contra associações protegidas já estabelecidas. Ele não fortalece a PSK contra quebra offline, pois a fraqueza está na própria senha. A força bruta no WPS ataca um mecanismo de PIN separado. Ataques de DHCP falso ocorrem acima da camada MAC do 802.11.

42. C O ataque PMKID não depende de cliente: o próprio AP revela o PMKID no elemento de informação RSN (RSN information element) da mensagem 1 (M1) do handshake de 4 vias. Basta o AP estar visível, sem cliente associado. A captura de handshake por deauth exige um cliente presente que se reautentique. A força bruta no WPS ataca outro mecanismo de PIN, não a PSK. O ARP spoofing é man-in-the-middle, não captura de credenciais.

43. D O evil twin imita um SSID específico e conhecido para fazer o cliente achar que entrou na rede corporativa legítima. O ataque Karma, ao contrário, ouve as probe requests e responde com o SSID que o cliente procura, imitando qualquer rede da lista de redes preferidas, e não um nome fixo. A desautenticação é outra técnica de interrupção, às vezes combinada com os dois, mas não é o que a pergunta descreve.

44. D O Pixie Dust explora APs cuja implementação de WPS gera números aleatórios previsíveis ou com pouca entropia nos nonces E-S1/E-S2, usados para provar o conhecimento do PIN. Com nonces fracos, capturar uma única troca WPS permite descobrir o PIN offline em segundos ou minutos, e não em horas, como online. A força bruta clássica do Reaver é limitada e fácil de detectar e bloquear. O PMKID mira o material de autenticação da PSK. O KRACK explora a reinstalação de chave no handshake.

45. A Os quadros de desautenticação falsificam o MAC do AP e mandam o cliente se desconectar. Quando ele se reconecta sozinho, o handshake de quatro vias acontece de novo e pode ser capturado com o airodump-ng, para quebra offline com hashcat ou aircrack-ng. ARP poisoning e DNS spoofing são técnicas de MITM das camadas 2 e 3 e não forçam reautenticação Wi-Fi. O SSL strip ataca sessões HTTPS. O ataque funciona porque, no WPA2, os quadros de gerenciamento 802.11 não são autenticados, falha tratada pelo 802.11w.

46. A No evil twin, um AP falso imita o SSID de uma rede legítima, e muitas vezes o BSSID, para levar os usuários a se conectarem e permitir a captura de tráfego e credenciais. Costuma vir junto com quadros de deauth para tirar os clientes do AP real. O ARP spoofing é uma técnica de camada 2 contra hosts já na rede. O ataque ao PIN do WPS faz força bruta no AP legítimo. O bluejacking envia mensagens por Bluetooth, sem ligação com o SSID.

47. D O IV de 24 bits do WEP tem apenas cerca de 16,7 milhões de valores, que em uma rede movimentada são reutilizados (colidem) em poucas horas. Com as colisões capturadas, ferramentas como o aircrack-ng recuperam a chave RC4 por estatística, com ataques como FMS ou PTW. O TKIP e o Michael são uma camada do WPA, não do WEP. O downgrade do SAE vale para o WPA3. O WEP tem verificação de integridade (ICV), mas ela é fraca.

48. A O Karma, baseado na ferramenta KARMA original, monitora as probe requests dirigidas que clientes próximos enviam procurando SSIDs da sua lista de redes preferidas e responde a elas. Assim, os clientes podem se associar automaticamente ao AP falso. O evil twin imita uma rede legítima específica, que nem precisa estar visível, e não precisa copiar o BSSID. A desautenticação só desconecta clientes. O DHCP falso age depois da associação e não falsifica respostas de SSID.

49. D O Key Reinstallation Attack (KRACK) explora o handshake de quatro vias do WPA2 reenviando a mensagem 3. O cliente reinicia o nonce e reinstala uma chave de sessão que já estava em uso, o que reinicia o keystream e permite decifrar ou repetir pacotes. Ele não exige nem revela a senha, e isso o distingue do PMKID e de ataques de dicionário. O evil twin é um AP falso de engenharia social, e a força bruta ao WPS ataca um PIN de 8 dígitos, outro mecanismo.

50. A O modo de transição anuncia WPA2 e WPA3 no mesmo beacon. Pesquisas sobre ataques de downgrade da família Dragonblood mostraram que um AP falso ou um atacante no caminho pode levar um cliente compatível com os dois a usar o handshake WPA2 de 4 vias. Esse handshake pode ser capturado e atacado offline com dicionário. O SAE continua funcionando para clientes WPA3, a PSK nunca é enviada em texto puro, e o PMF costuma ser opcional na parte WPA2, então o risco de deauth continua.

51. C O padding oracle attack explora uma aplicação que revela se o padding decifrado era válido, o que permite recuperar o texto claro do CBC byte a byte sem a chave (por exemplo, o POODLE e o ataque original de Vaudenay). O ataque do aniversário trata de colisões de hash, não de validação de padding. O meet-in-the-middle exige dois cálculos de texto cifrado para achar um valor intermediário igual. O chosen-plaintext exige controle sobre o que é cifrado, não a observação de erros de decifração.

52. C O hashcat suporta o modo 22000 (WPA-PBKDF2-PMKID+EAPOL) para quebra offline acelerada por GPU de handshakes WPA2 com uma wordlist, o passo padrão depois da captura. O Responder serve para envenenamento de LLMNR/NBT-NS em redes cabeadas ou locais, não para quebrar handshakes. O sqlmap automatiza injeção de SQL. O módulo psexec do Metasploit faz execução remota autenticada de código, não recupera senhas de handshakes. É preciso autorização para testar a rede.

53. B O POODLE (Padding Oracle On Downgraded Legacy Encryption) explora a validação de padding CBC não determinística do SSLv3, depois que o atacante força um downgrade de protocolo. Isso permite recuperar o texto claro byte a byte. O Heartbleed é uma leitura de memória além do limite na extensão heartbeat do OpenSSL, sem relação com downgrade. O CRIME explora a compressão do TLS e não precisa de SSLv3. O BEAST ataca uma fraqueza de encadeamento CBC no TLS 1.0. A mitigação padrão é desativar o SSLv3.

54. B Os ataques estilo Logjam exploram o fato de que muitos servidores reutilizam poucos primos DH padrão. Atacantes de nível estatal conseguem pré-calcular tabelas de logaritmo discreto para esses grupos de 512 e 1024 bits e recuperar a chave quase em tempo real. O ECDHE com P-256 usa curvas elípticas e não tem quebra equivalente com pré-cálculo amplo. O AES-256-GCM é a cifra simétrica, alheia à troca DH. O tamanho da chave RSA de assinatura afeta a autenticação do certificado, não a força do grupo DH.

55. B A criptografia simétrica (por exemplo, AES, DES, 3DES) usa uma única chave secreta compartilhada para cifrar e decifrar. É rápida, mas exige uma distribuição segura da chave. A assimétrica usa um par de chaves, pública e privada, e cada operação usa uma chave diferente. O hash é uma função de mão única que gera um resumo de tamanho fixo e não é reversível, então não “decifra” nada. A assinatura digital usa chaves assimétricas para provar autenticidade e integridade.

56. C A assinatura digital (digital signature) é feita calculando o hash da mensagem e criptografando esse hash com a chave privada do remetente. O destinatário descriptografa com a chave pública do remetente e compara com o hash que ele mesmo calculou. Criptografar com a chave pública do destinatário só dá confidencialidade, não prova a origem. Criptografar o hash com essa chave impediria que outros verificassem a assinatura. Uma chave simétrica compartilhada exige troca prévia de chaves e não dá não repúdio (non-repudiation).

57. D No ataque offline baseado em PMKID, o atacante captura o PMKID que alguns pontos de acesso enviam na primeira mensagem EAPOL-Key. Uma ferramenta como o hcxdumptool faz a captura, e o hashcat quebra a PSK offline, sem handshake completo nem deauth. O KRACK explora a reutilização de nonce na retransmissão do handshake. O evil twin imita um AP legítimo, e o ataque ao PIN do WPS usa outro protocolo.

58. D O Diffie-Hellman permite que duas partes calculem o mesmo segredo usando exponenciação modular com valores públicos e expoentes privados. O segredo nunca trafega na rede. Quem intercepta só vê valores públicos, inúteis sem os expoentes privados. A assinatura RSA autentica dados, mas não cria um segredo simétrico. O AES-256 é uma cifra simétrica que precisa de chave já combinada, e o HMAC garante integridade e autenticação, não negociação de chave.

59. C O Diffie-Hellman efêmero gera um par de chaves novo a cada handshake e descarta o expoente privado depois. Por isso, roubar a chave de longo prazo do servidor não permite recuperar chaves de sessões passadas. Isso é o sigilo de encaminhamento perfeito (perfect forward secrecy). Na troca RSA estática, o pre-master secret é criptografado com a chave pública de longo prazo do servidor, então o roubo da chave privada abre todas as sessões capturadas. PSK sem parte efêmera reutiliza o mesmo segredo. Kerberos é um protocolo de autenticação.

60. A A tabela de força comparável da NIST SP 800-57 Parte 1 associa uma chave simétrica de 128 bits a uma chave RSA de 3072 bits. A segurança do RSA cresce de forma subexponencial com o tamanho da chave. RSA de 1024 bits equivale a cerca de 80 bits de segurança e está obsoleto. RSA de 2048 bits equivale a cerca de 112 bits, abaixo do alvo. RSA de 15360 bits equivale a 256 bits simétricos, muito além do pedido, e pesa no desempenho sem necessidade.

61. B A enumeração vem depois da varredura. Nela o pentester extrai ativamente nomes de usuário, de compartilhamentos, grupos e dados de sessão nula, geralmente com ferramentas como enum4linux ou rpcclient. A varredura de vulnerabilidades procura CVEs e configurações erradas, não usuários e compartilhamentos. A captura de banners já foi feita pelo nmap -sV. O reconhecimento ativo é uma etapa anterior e mais ampla, que vem antes da varredura de portas.

62. B O hacker white hat age com permissão explícita do dono do sistema e segue um escopo assinado, então sua atividade é legal e ética. O black hat age sem autorização, por ganho pessoal ou má intenção. O gray hat testa sem permissão, mas sem má intenção, e isso continua sendo ilegal. O script kiddie tem pouca habilidade técnica e usa ferramentas prontas sem entendê-las. A autorização é o que separa o white hat dos demais.

63. B O SYN flood é uma técnica de negação de serviço (denial of service) que esgota os recursos do servidor, e os usuários autorizados não conseguem acessar o sistema. Isso ataca diretamente a disponibilidade, que garante acesso a dados e serviços quando necessário. Confidencialidade trata de divulgação indevida de dados, e nada foi exposto. Integridade trata de alteração indevida, e nenhum registro foi alterado. O não repúdio não faz parte da tríade CIA clássica.

64. C Varredura e enumeração envolvem interação direta e ativa com os hosts alvo: varredura de portas, detecção de serviços e versões e identificação do sistema operacional (OS fingerprinting) com ferramentas como o Nmap. O objetivo é montar um mapa técnico da superfície de ataque. O reconhecimento é a fase anterior de coleta de informações, passiva ou ativa, antes de sondar portas. Obter acesso é explorar de fato, o que ainda não ocorreu. Manter acesso vem muito depois.

65. B Hackers gray hat agem sem autorização formal nem contrato assinado, mas sem má intenção, e muitas vezes comunicam as falhas de forma responsável. É exatamente este caso. O white hat precisa de contrato ou autorização explícita antes de testar, e aqui não houve. O suicide hacker aceita ser processado para expor um alvo, sem se importar com as consequências legais. O hacktivista tem motivação política ou social. O que decide é a autorização combinada com a intenção, não a técnica.

66. D O red team trabalha com objetivos e avalia a capacidade de detecção e resposta contra um adversário realista, sem buscar cobertura total de vulnerabilidades. Normalmente os defensores não são avisados. O teste de invasão tradicional tem mais cobertura, prazo definido e busca o maior número possível de vulnerabilidades exploráveis no escopo. A avaliação de vulnerabilidades só varre e reporta, sem explorar. O bug bounty é contínuo e aberto a muitas pessoas, sem cenário coordenado.

67. C As Regras de Engajamento definem os detalhes operacionais do teste: metodologia, horários permitidos, contatos de emergência e exclusões de escopo, como o gateway de pagamento. A Declaração de Trabalho define entregas, prazos e custo, não os limites operacionais. O NDA cobre apenas a confidencialidade das informações trocadas. O Contrato-Mestre fixa as condições legais e comerciais gerais da relação, sem detalhar o teste.

68. C Testar ou explorar qualquer sistema fora do escopo assinado, mesmo de leve, expõe o pentester a responsabilidade civil e a problemas com a lei CFAA, porque o terceiro nunca autorizou o teste. O correto é parar no limite e escalar pelo canal definido nas Regras de Engajamento, e o cliente decide o que fazer com o terceiro. Testar as credenciais, mesmo só para confirmar, já é acesso não autorizado. Omitir uma descoberta relevante também viola o dever de comunicação do pentester.

69. D A varredura do nmap mostra que a porta 445 (SMB) está aberta. Isso é varredura (scanning), que mapeia hosts ativos e serviços. Depois o enum4linux consulta esse serviço aberto e obtém nomes de compartilhamentos, usuários e grupos, o que define a enumeração. Reconhecimento e footprinting podem ser passivos ou ativos. Obter acesso exige explorar uma vulnerabilidade, o que não ocorreu. Ocultar rastros (covering tracks) só acontece depois do comprometimento.

70. C O reconhecimento passivo (passive reconnaissance) coleta informações sem interagir diretamente com os sistemas do alvo. Usa fontes como Shodan, WHOIS, registros DNS e redes sociais, e não deixa rastro na rede do alvo. O reconhecimento ativo exige interação direta, como ping sweeps ou varreduras de portas, que podem ser registradas e detectadas. A enumeração é uma fase posterior e mais intrusiva. A varredura de vulnerabilidades também sonda sistemas ativos e seria detectável.

Palavras-chave em inglês

footprinting	levantamento de informações	Coleta de dados sobre o alvo antes do ataque.
passive reconnaissance	reconhecimento passivo	Buscar informações sem enviar nada aos sistemas do alvo.
active reconnaissance	reconhecimento ativo	Buscar informações interagindo direto com o alvo.
OSINT	inteligência de fontes abertas	Informação obtida em fontes públicas, como redes sociais e buscadores.
banner grabbing	captura de banner	Ler a resposta inicial de um serviço para saber qual programa ele usa.
zone transfer (AXFR)	transferência de zona	Pedido que copia todos os registros DNS de uma zona.
scanning	varredura, escaneamento	Fase que descobre hosts, portas abertas, serviços e sistemas.
enumeration	enumeração	Fase que extrai usuários, grupos e compartilhamentos de um serviço.
privilege escalation	escalada de privilégios	Conseguir mais permissões do que a conta tinha.
maintaining access	manutenção do acesso	Fase que mantém a entrada em um sistema já invadido.
covering tracks	apagar rastros	Esconder sinais do ataque, por exemplo limpando logs.
pass-the-hash	uso direto do hash	Autenticar com o hash NTLM sem conhecer a senha.
Kerberoasting	ataque a tickets de serviço	Pedir tickets de serviço e quebrar a senha da conta offline.
golden ticket	TGT forjado	Ticket do Kerberos falso, criado com o hash da conta krbtgt.
rainbow table	tabela arco-íris	Tabela pré-calculada que liga hashes a senhas em texto.
brute-force attack	ataque de força bruta	Testar todas as combinações possíveis de caracteres.
dictionary attack	ataque de dicionário	Testar uma lista de senhas prováveis.
rootkit	rootkit	Programa que esconde processos, arquivos e conexões do atacante.
honeypot	sistema isca	Sistema falso, feito para atrair e observar atacantes.
firewalking	mapeamento de regras do firewall	Usar o TTL para descobrir que portas o firewall deixa passar.

session splicing	divisão da sessão	Dividir o ataque em segmentos TCP pequenos e lentos para enganar o IDS.
MAC flooding	inundação de MAC	Encher a tabela CAM do switch com endereços falsos.
ARP spoofing	falsificação de ARP	Alterar o cache ARP dos hosts para desviar o tráfego.
session hijacking	sequestro de sessão	Tomar uma sessão que outra pessoa já autenticou.
denial of service (DoS)	negação de serviço	Ataque que impede usuários legítimos de usar um sistema.
social engineering	engenharia social	Enganar pessoas para obter acesso ou informação.
pretexting	pretexto	Inventar uma identidade ou história para ganhar confiança.
tailgating	entrar atrás sem ser visto	Passar por uma porta controlada sem que o funcionário perceba.
piggybacking	entrar com a ajuda de alguém	Entrar porque um funcionário deixa, mesmo enganado.
SQL injection	injeção de SQL	Entrada que muda a lógica de uma consulta ao banco de dados.
cross-site scripting (XSS)	script entre sites	Código do atacante que roda no navegador da vítima.
server-side request forgery (SSRF)	falsificação de requisição no servidor	Fazer o servidor acessar um destino escolhido pelo atacante.
insecure deserialization	desserialização insegura	Reconstruir objetos não confiáveis sem validar tipo ou integridade.
session fixation	fixação de sessão	Dar à vítima um ID de sessão conhecido antes do login.
evil twin	ponto de acesso gêmeo falso	Wi-Fi falso que imita um SSID conhecido.
deauthentication frame	quadro de desautenticação	Quadro que manda o cliente sair da rede Wi-Fi.
four-way handshake	handshake de quatro vias	Troca de quatro mensagens que cria as chaves da sessão WPA2.
digital signature	assinatura digital	Hash cifrado com a chave privada, que prova origem e integridade.
perfect forward secrecy	sigilo de encaminhamento perfeito	Roubar a chave do servidor depois não abre sessões antigas.
rules of engagement (ROE)	regras de engajamento	Documento com métodos, horários, contatos e limites do teste.

O Examundo é independente. Não é afiliado às entidades que fazem essas provas nem tem a aprovação delas. As questões são originais, não são da prova real. examundo.tech/pt/ceh/