TỪ ĐIỂN CHUYÊN NGÀNH

Mục lục

A

access control vestibule · Account takeover (ATO) · Active reconnaissance · ADIA (Appliance for Digital Investigation and Analysis) · Aircrack-ng · aireplay-ng command · airmon-ng command · Airodump-ng · American Fuzzy Lop · API (Application Programming Interface) · Apple Remote Desktop · Apple Remote Desktop · application-based tests · arithmetic operators · ARP cache poisoning (ARP spoofing) · arrays · Asterisk

B

BackTrack · Badge cloning · Bash · Bash shell · Basic Service Set Identifier (BSSID) · bind shell · biometric control · BlackArch · BlackArch in Docker · BlackArch Linux · BLE (Bluetooth Low Energy) · BloodHound · Blowfish · blue team · Bluejacking · Bluesnarfing · Bluetooth Low Energy (BLE) attack · boolean operators · Brakeman · business associates

C

C-suite · Cain and Abel · CAINE (Computer Aided Investigative Environment) · California Consumer Privacy Act (CCPA) · Captive portal · CDK (Cloud Development Kit) · Censys · certificate management · certificate revocation list (CRL) · CeWL · chief executive officer (CEO) · chief financial officer (CFO) · chief information officer (CIO) · chief information officer (CIO) · chief information security officer (CISO) · chief operating officer (COO) · chief security officer (CSO) · chief technical officer (CTO) · Cisco Discovery Protocol (CDP) · Cisco's Encrypted Traffic Analytics (ETA), U. S. National Security Agency (NSA) · classes · Cloud · Cloud Custodian · Cloud malware injection attack · CloudBrute · Coagula · Comma-separated values (CSV) · Command and Control (C2) systems · Commodity Futures Trading Commission (CFTC) · Common Vulnerabilities and Exposures (CVE) · Common Vulnerability Scoring System (CVSS) · Common Weakness Enumeration (CWE) · Community cloud · Compliance Scan · conditionals · Conficker · Configuration compliance · covert channel · Credential attack · Credential harvesting · Credential Harvesting attack · Credential stuffing attack · critical findings

D

D2O attack (Direct-to-Origin attack) · Daemon · data exfiltration · data structures · Debugging · Decompilation · defensive security · DHCP spoofing · dictionaries · dig · DirBuster · Directory Information Tree (DIT) · directory traversal · Disassociation (Deauthentication) attack · Distinguished Name (DN) · DNS cache poisoning · DNS lookup · DNS poisoning · DNS

tunneling (DNS exfiltration) · DNSCat2 · DNSRecon · Domain Name System Security Extensions (DNSSEC) · DoS attack (Denial-of-Service) · Dradis · DRM (Digital Rights Management) · DropboxC2 (DBC2) · Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) · Dumpster diving · dynamic application security testing (DAST)

E

EAPHammer · Eavesdropping · edb Debugger · Elicitation · emergency contact · Empire · Empire · Encryption · Enum4linux · Enum4linux · Enumeration · EternalBlue · ethical hacking · European Union's General Data Protection Regulation (GDPR) · Evasion · Evasion · Evil Twin attack · EXIF (exchangeable image file format) · ExifTool · ExifTool · Exploit Chaining · Exploits · Extended Service Set Identifier (ESSID)

F

false negative · false positive · Federal Deposit Insurance Corporation (FDIC) Safeguards Act · Federal Financial Institutions Examination Council (FFIEC) · Federal Risk and Authorization Management Program (FedRAMP) · Federated authentication · Fern Wi-Fi Cracker · File Transfer Protocol Secure (FTPS) · fileless malware · Financial Institutions Letters (FILs) · FindSecBugs · Fingerprinting Organization with Collected Archives (FOCA) · Fog (Fog computing / Edge-fog) · Forensics · Fragmentation attack · fully qualified domain names (FQDNs) · Fuzz testing · Fuzzers · Fuzzing

G

Gantt Chart · General Data Protection Regulation (GDPR) · GitHub · Google dorks · GraphQL

H

Hacktivist · Hashcat · Health and Human Services (HHS) · Health Insurance Portability and Accountability Act of 1996 (HIPAA) · healthcare clearinghouse · healthcare plan · Horizontal privilege escalation · horizontal privilege escalation · host · host command · Hybrid cloud · Hydra

I

IaaS (Infrastructure as a Service) · ICS (Industrial Control System) · IDA · IIoT (Industrial Internet of Things) · IMAP (Internet Message Access Protocol) · Immunity Debugger · indicators of prior compromise · information security manager (ISM) · Information Systems Security Assessment Framework (ISSAF) · Initialization Vector (IV) attack · Insider threat · Interrogation · IoT (Internet of Things) · IPMI (Intelligent Platform Management Interface)

J

Jamming · Japan Computer Emergency Response Team (JPCERT) · JavaScript Object Notation (JSON) · job rotation · John the Ripper

K

Kali Linux · KARMA attack · Kerberoasting · Kerberos · Kerberos golden ticket attack · Kerberos silver ticket attack · key rotation · KisMAC · Kismet · known-environment testing ·

Krack attack · ksh

L

lateral movement · LDAP injection · LDAP-Based attack · LeakLooker · Lightweight Directory Access Protocol (LDAP) · Link-Local Multicast Name Resolution (LLMNR) · lists · living-off-the-land · logic constructs · loops

M

Mail User Agent (MUA) · Maltego · Management Information Base (MIB) · mandatory vacation · mantrap · master service agreement (MSA) · Mdk4 · Media Access Control (MAC) spoofing · media sanitization · Medusa and Ncrack · Metadata service attacks (cloud metadata attacks / IMDS abuse) · Metagoofil · Metasploit · Metasploit · Metasploit · Metasploit framework · Meterpreter commands (see table in 8.1.2) · Meterpreter module · Microsoft's Remote Desktop Protocol (RDP) · Mimikatz · Mimikatz · Mimikatz · msfconsole · multifactor authentication · Mutiny Fuzzing Framework

N

National Institute of Standards and Technology (NIST) · National Institute of Standards and Technology (NIST) · NBNSpoof · Nessus · NetBIOS Name Service (NetBIOS-NS) · Netcat commands (see table in 8.1.2) · Network Basic Input/Output System (NetBIOS) · network segmentation · network segmentation · Network share enumeration · New Technology LAN Manager (NTLM) · Nexpose · Nikto · Nikto · NIST SP 800-115 · Nmap · Nmap Scripting Engine (NSE) · non-disclosure agreement (NDA) · nslookup · nslookup command · Nyeta

O

Objdump · Object Exchange (OBEX) protocol · offensive security · OllyDbg · On-Path attack · Online Certificate Status Protocol (OCSP) · Open (OPN) · Open Security Content Automation Protocol (SCAP) · Open Web Application Security Project (OWASP) · Open Web Application Security Project (OWASP) · open-source intelligence (OSINT) · OpenStego · OpenVAS · operational control · OWASP Software Assurance Maturity Model (SAMM) · OWASP Zed Attack Proxy (ZAP)

P

PaaS (Platform as a Service) · packet inspection · Packet Inspection · packet storm (broadcast storm) · packetforge-ng command · Pacu · PALADIN · PAN (primary account number) · Parrot OS · Parrot OS · partially known environment test (gray-box) · Pass-the-hash · Pass-the-Hash attack (PtH) · Passive reconnaissance · Password dumps · Password Spraying attack · Patator · patch management · Payment Card Industry Data Security Standard (PCI DSS) · PCI Forensic Investigator (PFI) · Peach · Penetration Testing Execution Standard (PTES) · Perl · Persistence · personal identifiable information (PII) · physical control · Piggybacking · pip3 install h8mail command · Pivoting · platform as a service (PaaS) · POP3 (Post Office Protocol version 3) · PowerShell · PowerShell commands (see table in 8.2.3) · Preferred Network List

(PNL) · primary contact · Private cloud · Privilege escalation · process-level remediation · Proxychains · PsExec · Public cloud · Pupy · PwnDB · Python

Q

Quality Security Assessor (QSA) · Qualys

R

Radio-Frequency Identification (RFID) attack · RainbowCrack · RDP (Remote Desktop Protocol) · Reaver · Recon-ng · Reconnaissance · red team · reflected XSS · Resource exhaustion · Responder · RESTful API · Return on Investment (ROI) · reverse shell · RFID cloning · Risk acceptance · Risk assessment · Risk management · Risk-taking · Rogue Access Point · Rogue access points · role-based access control (RBAC) · Ruby

S

SaaS (Software as a Service) · SCADA (Supervisory Control And Data Acquisition) · Scanners · Scavenger · schtasks.exe command · ScoutSuite / Scout Suite · SDK (Software Development Kit) · Searchsploit · Searchsploit · searchsploit command · secrets management solution · Secure File Transfer Protocol (SFTP) · Secure SMTP (SSMTP) · Secure Sockets Layer (SSL) · secure software development life cycle (SSDLC) · Security Onion · sensitive data · Server Message Block (SMB) · Service Set Identifier (SSID) · service-level agreement (SLA) · Session Service (NetBIOS-SSN) · Shell · Shodan · Shoulder surfing · Side-channel attack · SIFT Workstation (SANS Investigative Forensic Toolkit) Workstation · Simple Network Management Protocol version 3 (SNMPv3) · Simple Object Access Protocol (SOAP) · Skadi · SMTP over SSL (SMTPS) · smtp-user-enum command · snmp-check command · snow · socat · Social engineering · Social-Engineer Toolkit (SET) · software as a service (SaaS) · Software assurance · Software Development Kit (SDK) · SonarQube · Sonic Visualiser · Spanning Tree Protocol (STP) · SpiderFoot · SpoofApp · SpoofCard · Spooftooph · SpotBugs · SQLmap · SSO (Single Sign-On) · State-Sponsored Attacker · statement of work (SOW) · static application security testing (SAST) · status reports · Steganography · steghide · string operators · sudo command · Sysinternals · system hardening

T

tcpdump command · tcsh · technical contact · technical control · The CERT division of Carnegie Mellon University · The GNU Project Debugger (GDB) · The Internet Corporation for Assigned Names and Numbers (ICANN) · theHarvester · time-of-day restriction · Timing Options (-T0–T5) · TinEye · Tor · trees · TrevorC2 · true negative · true positive

U

unethical hacking · unknown-environment test (black-box) · unknown-environment testing · Unknown-Environment Testing (black-box) · Unmanned Aerial Vehicle (UAV) · User Account Control (UAC) · User enumeration · user input sanitization and query parameterization · user training

V

Veil · Vertical privilege escalation · vertical privilege escalation · video surveillance · VMware · VNC · VNC · Vulnerability scanning

W

W3af · WannaCry · War Driving · War Flying · Web Application Description Language (WADL) · Website archiving/caching · WebSocket · WhatBreach · WHAX · whois · whois command · Whois Data Problem Reporting System (WDPRS) · WHoppiX · Wi-Fi Protected Access version 1 (WPA) · Wi-Fi Protected Setup (WPS) PIN attack · Wifite2 · WiGLE · WiGLE (Wireless Geographic Logging Engine) · Windows Common Internet File System (CIFS) · Windows Debugger · Windows Management Instrumentation (WMI) · Windows PowerShell · Windows Remote Management (WinRM) · Wired Equivalent Privacy (WEP) · Wireless Local Area Network (WLAN) · WMImplant · WPA version 2 (WPA2) · WPA version 3 (WPA3) · wsc2

X

X server forwarding · X server forwarding

Z

Zenmap

access control vestibule

Dịch: phòng kiểm soát truy cập

Giải thích: *mantrap, airlock*

Ví dụ: Để vào trung tâm dữ liệu, nhân viên phải đi qua một Access control vestibule (còn gọi là Mantrap).

Xem thêm: mantrap

↑ Lên đầu

Account takeover (ATO)

Dịch: Chiếm đoạt tài khoản

Giải thích: *Kẻ tấn công chiếm quyền điều khiển tài khoản người dùng (email, ngân hàng, SaaS…) bằng credential lấy được (phishing, credential stuffing, mua mật khẩu rò rỉ). Hậu quả: gian lận, rút tiền, mất dữ liệu. Phòng thủ: MFA, phát hiện bot/behavioural anomalies, rate-limiting, notify user.*

Ví dụ: Hacker dùng mật khẩu bị rò rỉ để đăng nhập vào tài khoản ngân hàng của nạn nhân và rút tiền.

↑ Lên đầu

Active reconnaissance

Dịch: trinh sát chủ động

Giải thích: *tương tác trực tiếp với mục tiêu — quét port, banner grabbing*

Ví dụ: Việc sử dụng Nmap để quét các cổng đang mở trên máy chủ của mục tiêu là một hình thức Active Reconnaissance.

↑ Lên đầu

ADIA (Appliance for Digital Investigation and Analysis)

Dịch: ADIA

Giải thích: *thiết bị/phần mềm hỗ trợ điều tra và phân tích số*

Ví dụ: Một điều tra viên sử dụng ADIA để tiến hành phân tích một ổ cứng đã được sao chép hình ảnh (image).

↑ Lên đầu

Aircrack-ng

Dịch: Aircrack-ng (bộ công cụ phân tích/an phá bảo mật Wi-Fi)

Giải thích: *Suite gồm nhiều tool dùng để thu thập, phân tích, và (kiểm thử) bẻ khóa mật khẩu WPA/WEP từ handshake/IVs; dùng trong kiểm thử bảo mật Wi-Fi.*

Ví dụ: Sau khi thu handshake WPA2, pentester chạy aircrack-ng handshake.cap -w rockyou.txt để thử phá mật khẩu.

↑ Lên đầu

aireplay-ng command

Dịch: Lệnh aireplay-ng (Aircrack-ng suite)

Giải thích: *Tiện ích dùng để tạo/gửi các frame Wi-Fi (deauth, fake auth, replay...) nhằm mục đích kiểm thử hoặc tương tác với AP/client khi thu thập*

handshake hoặc kiểm tra bảo mật. Được dùng trong pentest và khảo sát.

Ví dụ: Pentester dùng aireplay-ng --deauth 10 -a 00:11:22:33:44:55 -c 66:77:88:99:AA:BB wlan0mon để ngắt kết nối client, buộc thiết bị reconnect và thu handshake WPA2 cho kiểm thử bảo mật.

↑ Lên đầu

airmon-ng command

Dịch: Lệnh airmon-ng (trong Aircrack-ng suite)

Giải thích: *Tiện ích bật/tắt chế độ monitor trên card Wi-Fi (Linux) để thu packets thô; dùng trong khảo sát và sniffing không dây.*

Ví dụ: Chạy lệnh airmon-ng start wlan0 để bật chế độ monitor trên card Wi-Fi trước khi dùng Airodump-ng bắt gói.

↑ Lên đầu

Airodump-ng

Dịch: Airodump-ng (capture tool của Aircrack-ng)

Giải thích: *Thu và hiển thị thông tin AP và client, capture handshake/WEP IVs, lưu pcap cho phân tích; thường chạy cùng airmon-ng.*

Ví dụ: Chạy airodump-ng wlan0mon để hiển thị danh sách các AP và client đang kết nối, kèm theo thông tin kênh và mã hóa.

↑ Lên đầu

American Fuzzy Lop

Dịch: AFL

Giải thích: *fuzzer phổ biến để tìm lỗi phần mềm, crash, memory corruption*

Ví dụ: Một nhà nghiên cứu chạy AFL trong nhiều ngày trên một thư viện xử lý ảnh và đã phát hiện ra nhiều lỗ hổng tràn bộ đệm.

↑ Lên đầu

API (Application Programming Interface)

Dịch: Giao diện lập trình ứng dụng (API)

Giải thích: *Bộ quy tắc/endpoint cho phép ứng dụng tương tác (gọi chức năng, trao đổi dữ liệu). Rủi ro: lộ key, thiếu xác thực/authorization, thiếu rate-limit -> bị lạm dụng. Phòng thủ: auth mạnh (OAuth), rate limiting, input validation, logging, API gateway.*

Ví dụ: Ứng dụng di động gọi API GET /users/123 tới server để lấy thông tin người dùng.

↑ Lên đầu

Apple Remote Desktop

Dịch: Apple Remote Desktop

Giải thích: *công cụ/ứng dụng điều khiển từ xa cho macOS — tương tự RDP trên Windows.*

Ví dụ: Là công cụ điều khiển từ xa chính thức cho macOS. Trong môi trường sử dụng nhiều máy Mac, nó trở thành mục tiêu tương tự như RDP để di chuyển ngang.

↑ Lên đầu

Apple Remote Desktop

Dịch: Apple Remote Desktop

Giải thích: *phần mềm điều khiển máy Mac từ xa.*

Ví dụ: Trong mạng văn phòng, attacker chiếm được một máy Mac và dùng nó để quét tìm các máy khác đang bật dịch vụ Apple Remote Desktop nhằm chiếm quyền điều khiển.

↑ Lên đầu

application-based tests

Dịch: kiểm thử ứng dụng

Giải thích: *Tập trung vào web app, mobile app, API và logic nghiệp vụ.*

Ví dụ: Trong một bài kiểm thử ứng dụng, pentester đã tìm thấy một lỗ hổng Logic nghiệp vụ, cho phép anh ta thêm hàng vào giỏ hàng và checkout" với giá 0 đồng."

↑ Lên đầu

arithmetic operators

Dịch: toán tử số học

Giải thích: *+, -, *, /, % — phép toán số học cơ bản*

Ví dụ: Một script khai thác buffer overflow sử dụng Arithmetic Operators để tính toán chính xác địa chỉ trả về.

↑ Lên đầu

ARP cache poisoning (ARP spoofing)

Dịch: Đầu độc bộ nhớ đệm ARP / mạo danh ARP

Giải thích: *Gửi bản tin ARP giả để ánh xạ IP tới MAC của attacker, khiến lưu lượng được chuyển qua attacker (facilitating MITM). Thường xảy ra trong mạng LAN phẳng.*

Ví dụ: Máy nạn nhân gửi traffic cho gateway nhưng ARP trỏ gateway → attacker MAC.

↑ Lên đầu

arrays

Dịch: mảng

Giải thích: *cấu trúc lưu trữ danh sách có thứ tự*

Ví dụ: Một script brute-force đọc danh sách mật khẩu từ file và lưu chúng vào một Array để duyệt qua từng phần tử.

↑ Lên đầu

Asterisk

Dịch: Asterisk

Giải thích: *phần mềm PBX mã nguồn mở cho tổng đài/VoIP; nếu cấu hình yếu có thể bị khai thác để gọi trái phép hoặc nghe lén*

Ví dụ: Do cấu hình Asterisk (tổng đài VoIP) yếu kém và để mật khẩu mặc định, kẻ tấncông đã xâm nhập và thực hiện các cuộc gọi quốc tế trái phép, gây thiệt hại hàng ngàn đô la.

↑ Lên đầu

BackTrack

Dịch: BackTrack

Giải thích: *distro pentest cũ — tiền thân của Kali*

Ví dụ: Trước khi có Kali Linux, BackTrack là hệ điều hành tiêu chuẩn cho các chuyên gia pentest.

↑ Lên đầu

Badge cloning

Dịch: sao chép thẻ

Giải thích: *nhân bản thẻ truy cập RFID/magnetic để giả mạo quyền vào khu vực*

Ví dụ: Bằng cách sử dụng một thiết bị đọc RFID giấu trong túi xách và áp sát nhân viên mục tiêu trong thang máy, kẻ tấn công đã thành công thực hiện sao chép thẻ (badge cloning) và tạo ra một bản sao thẻ ra vào của họ.

↑ Lên đầu

Bash

Dịch: Bash

Giải thích: *Bourne Again Shell — Shell dòng lệnh phổ biến trên Linux/Unix.*

Ví dụ: Attacker nhận được một shell và chạy lệnh echo $SHELL, kết quả trả về là /bin/bash, cho biết đây là môi trường Bash.

Xem thêm: Shell

↑ Lên đầu

Bash shell

Dịch: Bash

Giải thích: *Bourne Again Shell — Shell dòng lệnh phổ biến trên Linux/Unix; thường dùng trong scripting/payloads*

Ví dụ: Pentester viết một script Bash shell để tự động quét một dải mạng và lưu kết quả vào file văn bản.

Xem thêm: Shell

↑ Lên đầu

Basic Service Set Identifier (BSSID)

Dịch: BSSID — Định danh BSS (thường là địa chỉ MAC của AP)

Giải thích: *Định danh duy nhất của một Basic Service Set; thường là MAC address của radio/AP, dùng để phân biệt AP ngay cả khi SSID giống nhau.*

Ví dụ: AP “Café_WiFi” có BSSID = AA:BB:CC:DD:EE:FF, giúp phân biệt với AP giả có cùng SSID.

↑ Lên đầu

bind shell

Dịch: bind shell

Giải thích: *máy mục tiêu mở cổng lắng nghe để attacker kết nối và nhận phiên dòng lệnh.*

Ví dụ: Payload chạy trên server, mở cổng 1337. Attacker từ máy mình dùng lệnh nc 1337 để kết nối và nhận shell.

↑ Lên đầu

biometric control

Dịch: kiểm soát sinh trắc học

Giải thích: *Xác thực bằng vân tay/face/iris làm yếu tố bảo mật vật lý/định danh*

Ví dụ: Nhân viên phải sử dụng vân tay để mở khóa laptop công ty. Đây là một Biometric Control.

↑ Lên đầu

BlackArch

Dịch: BlackArch

Giải thích: *Bản phân phối Linux dựa trên Arch, chuyên cho pentest, chứa hơn 2000 công cụ hacking.*

Ví dụ: Một nhà nghiên cứu bảo mật thích sử dụng BlackArch vì kho lưu trữ khổng lồ của nó, cung cấp nhiều công cụ chuyên sâu và hiếm gặp mà các bản phân phối khác không có.

↑ Lên đầu

BlackArch in Docker

Dịch: BlackArch in Docker

Giải thích: *chạy BlackArch trong container Docker — triển khai môi trường pentest*

Ví dụ: Một nhà phát triển sử dụng BlackArch in Docker để khởi chạy một công cụ bảo mật cụ thể nhằm kiểm tra ứng dụng của họ một cách nhanh chóng.

Xem thêm: BlackArch

↑ Lên đầu

BlackArch Linux

Dịch: BlackArch Linux

Giải thích: *distro pentest dựa trên Arch với nhiều tool*

Ví dụ: Một nhà nghiên cứu bảo mật sử dụng BlackArch Linux vì nó cung cấp rất nhiều công cụ chuyên biệt mà các distro khác không có sẵn.

↑ Lên đầu

BLE (Bluetooth Low Energy)

Dịch: Bluetooth Low Energy (BLE)

Giải thích: *Giao thức BLE cho thiết bị IoT/ble beacons; có vector tấn công pairing flaws, tracking. Phòng thủ: secure pairing modes, firmware updates, minimize advertising.*

Ví dụ: Vòng tay thông minh kết nối với điện thoại qua BLE để theo dõi nhịp tim người dùng.

↑ Lên đầu

BloodHound

Dịch: BloodHound

Giải thích: *công cụ phân tích Active Directory để tìm đường đi tấn công/attack paths trong domain.*

Ví dụ: Dùng để trinh sát và tìm đường tấn công trong môi trường Active Directory (AD). Nó giúp trực quan hóa các mối quan hệ để tìm con đường ngắn nhất chiếm quyền Domain Admin.

↑ Lên đầu

Blowfish

Dịch: Thuật toán mã hóa Blowfish

Giải thích: *Thuật toán mã hóa khối (symmetric block cipher) nhanh, thiết kế để thay thế DES. Khóa có độ dài biến đổi (32–448 bit). Ngày nay ít dùng cho mật mã mới (bởi AES phổ biến hơn), nhưng vẫn thấy trong một số ứng dụng/legacy systems.*

Ví dụ: Một số ứng dụng legacy dùng Blowfish cho encrypt/decrypt.

↑ Lên đầu

blue team

Dịch: đội xanh

Giải thích: *nhóm chuyên gia phòng thủ, giám sát và phản ứng trước các cuộc tấn công an ninh mạng*

Ví dụ: Đội xanh (blue team) đã phát hiện hành vi đáng ngờ trên máy chủ và nhanh chóng cô lập thiết bị bị nhiễm mã độc, ngăn chặn cuộc tấn công lan rộng.

↑ Lên đầu

Bluejacking

Dịch: Bluejacking

Giải thích: *Gửi tin nhắn (vCard) không mong muốn tới thiết bị Bluetooth gần đó (thường để gây phiền). Thường là trò quấy rối nhẹ, không ăn cắp dữ liệu.*

Ví dụ: Một người dùng gửi vCard “Hello!” ngẫu nhiên tới thiết bị Bluetooth khác trong phạm vi 10m mà không cần ghép nối — chỉ gây phiền, không trộm dữ liệu.

↑ Lên đầu

Bluesnarfing

Dịch: Bluesnarfing

Giải thích: *Trộm dữ liệu từ thiết bị Bluetooth (ví dụ contacts, calendar, files) bằng cách khai thác lỗ hổng/profiles mở — hành vi xâm phạm quyền riêng tư, có thể là tội phạm.*

Ví dụ: Attacker dùng điện thoại có phần mềm đặc biệt truy cập danh bạ và file từ điện thoại khác có Bluetooth bật và không yêu cầu xác thực.

↑ Lên đầu

Bluetooth Low Energy (BLE) attack

Dịch: Tấn công Bluetooth Low Energy (BLE attack)

Giải thích: *Các kỹ thuật khai thác lỗ hổng/điều chế trong BLE (pairing flaws, replay, spoofing, tracking) để làm lộ dữ liệu, vượt kiểm soát truy cập, hoặc theo*

dõi thiết bị. BLE có nhiều chế độ pairing khác nhau — cần hardening.

Ví dụ: Attacker khai thác lỗ hổng pairing BLE trên smartwatch để giả mạo thiết bị hợp lệ, đọc dữ liệu cảm biến hoặc vị trí người dùng.

↑ Lên đầu

boolean operators

Dịch: toán tử luận lý

Giải thích: *AND, OR, NOT — dùng trong biểu thức điều kiện*

Ví dụ: Một truy vấn tìm kiếm trong Shodan sử dụng Boolean Operators để tìm các máy chủ port:22" AND os:"Ubuntu"."

↑ Lên đầu

Brakeman

Dịch: Brakeman

Giải thích: *SAST tool chuyên cho Ruby on Rails — phân tích mã nguồn tìm security issues*

Ví dụ: Lập trình viên tích hợp Brakeman vào quy trình CI/CD của họ để tự động quét mã nguồn Ruby on Rails mỗi khi có thay đổi.

Xem thêm: Ruby

↑ Lên đầu

business associates

Dịch: đối tác kinh doanh

Giải thích: *cá nhân hoặc tổ chức có quyền truy cập dữ liệu nhạy cảm, ví dụ dữ liệu y tế, khi làm việc cùng nhà cung cấp dịch vụ chính*

Ví dụ: Công ty luật làm việc cho bệnh viện được coi là đối tác kinh doanh (business associate) vì họ có quyền truy cập vào dữ liệu y tế của bệnh nhân để xử lý các vụ kiện.

↑ Lên đầu

C-suite

Dịch: ban lãnh đạo cấp cao / đội ngũ điều hành cấp cao

Giải thích: *tập hợp các vị trí điều hành cao nhất trong công ty, ví dụ CEO, CFO, COO, CIO, CSO — những người ra quyết định chiến lược và chịu trách nhiệm toàn công ty.*

Ví dụ: Giám đốc an ninh (CSO) trình bày kế hoạch ngân sách bảo mật cho năm tới trước hội đồng C-suite để được phê duyệt.

↑ Lên đầu

Cain and Abel

Dịch: Cain and Abel

Giải thích: *tool phục hồi mật khẩu Windows — password cracking, sniffing, brute-force.*

Ví dụ: Một chuyên gia bảo mật sử dụng Cain and Abel để phân tích mạng và khôi phục các mật khẩu đã quên trong một môi trường được cho phép.

↑ Lên đầu

CAINE (Computer Aided Investigative Environment)

Dịch: CAINE

Giải thích: *hệ sinh thái điều tra pháp y máy tính*

Ví dụ: Đội ứng phó sự cố sử dụng CAINE để phân tích các hệ thống bị xâm nhập và thu thập bằng chứng.

↑ Lên đầu

California Consumer Privacy Act (CCPA)

Dịch: Đạo luật quyền riêng tư người tiêu dùng California (CCPA)

Giải thích: *quy định bảo vệ dữ liệu và quyền riêng tư cho cư dân California, Mỹ*

Ví dụ: Đạo luật quyền riêng tư người tiêu dùng California (CCPA) cho phép cư dân California yêu cầu các công ty xóa dữ liệu cá nhân của họ.

↑ Lên đầu

Captive portal

Dịch: Cổng bắt / trang đăng nhập bắt buộc

Giải thích: *Trang web trung gian yêu cầu người dùng xác thực hoặc chấp nhận điều khoản trước khi truy cập Internet (thường ở quán cà phê, khách sạn). Nếu cấu hình kém hoặc giả mạo, có thể dùng để thu credential.*

Ví dụ: Ở khách sạn, khi bạn kết nối Wi-Fi sẽ hiện trang đăng nhập để nhập số phòng. Attacker có thể tạo trang giả tương tự để đánh cắp mật khẩu Facebook.

↑ Lên đầu

CDK (Cloud Development Kit)

Dịch: Bộ công cụ phát triển hạ tầng/ứng dụng (CDK)

Giải thích: *Framework IaC (ví dụ AWS CDK) để định nghĩa hạ tầng bằng code; giúp deploy reproducible infra. Lưu ý bảo mật: secret handling, least-privilege IAM, review IaC.*

Ví dụ: Dùng AWS CDK để viết code TypeScript triển khai toàn bộ hạ tầng web gồm EC2, S3 và IAM.

↑ Lên đầu

Censys

Dịch: Censys

Giải thích: *search engine tương tự Shodan để tra host, certificate, exposed services*

Ví dụ: Một nhà nghiên cứu sử dụng Censys để tìm tất cả các website đang sử dụng một phiên bản OpenSSL có lỗ hổng Heartbleed.

Xem thêm: host, Shodan

↑ Lên đầu

certificate management

Dịch: quản lý chứng chỉ

Giải thích: *phát hành, gia hạn, thu hồi và lưu trữ chứng chỉ số/TLS*

Ví dụ: Quản trị viên sử dụng một công cụ tự động để theo dõi và gia hạn chứng chỉ SSL cho website của công ty trước khi nó hết hạn. Đây là một phần của Certificate Management.

↑ Lên đầu

certificate revocation list (CRL)

Dịch: danh sách thu hồi chứng chỉ (CRL)

Giải thích: *do CA phát hành, liệt kê các chứng chỉ đã bị thu hồi*

Ví dụ: Trước khi có OCSP, trình duyệt phải tải về một danh sách thu hồi chứng chỉ (CRL) nặng nề từ CA để kiểm tra xem chứng chỉ SSL đã bị thu hồi hay chưa.

↑ Lên đầu

CeWL

Dịch: CeWL

Giải thích: *tool thu thập từ vựng để phục vụ tấn công mật khẩu dựa trên website.*

Ví dụ: Pentester sử dụng CeWL để tạo một danh sách từ khóa từ trang web của công ty, hy vọng rằng nhân viên sẽ sử dụng các từ liên quan đến công ty để đặt mật khẩu.

↑ Lên đầu

chief executive officer (CEO)

Dịch: giám đốc điều hành (CEO)

Giải thích:

Ví dụ: CEO phê duyệt ngân sách an ninh mạng hàng năm và chịu trách nhiệm trước hội đồng quản trị về các sự cố lớn.

↑ Lên đầu

chief financial officer (CFO)

Dịch: giám đốc tài chính (CFO)

Giải thích:

Ví dụ: CFO đánh giá chi phí và lợi tức đầu tư (ROI) của việc mua một giải pháp bảo mật mới.

↑ Lên đầu

chief information officer (CIO)

Dịch: giám đốc thông tin / CNTT (CIO)

Giải thích:

Ví dụ: CIO chịu trách nhiệm triển khai các hệ thống công nghệ mới và đảm bảo chúng tuân thủ các chính sách bảo mật.

↑ Lên đầu

chief information officer (CIO)

Dịch: giám đốc công nghệ thông tin (CIO)

Giải thích: *lãnh đạo cấp cao phụ trách chiến lược CNTT tổng thể trong tổ chức*

Ví dụ: Giám đốc công nghệ thông tin (CIO) chịu trách nhiệm về toàn bộ hệ thống CNTT của công ty, bao gồm cả phần mềm nghiệp vụ, hạ tầng mạng và hỗ trợ người dùng.

↑ Lên đầu

chief information security officer (CISO)

Dịch: giám đốc an ninh thông tin (CISO)

Giải thích: *lãnh đạo cấp cao phụ trách chiến lược và chính sách an ninh mạng của tổ chức*

Ví dụ: Giám đốc an ninh thông tin (CISO) đã trình bày trước ban giám đốc về chiến lược an ninh mạng 5 năm và đề xuất ngân sách cho các công cụ bảo mật mới.

↑ Lên đầu

chief operating officer (COO)

Dịch: giám đốc vận hành (COO)

Giải thích:

Ví dụ: COO đảm bảo rằng quy trình ứng phó sự cố an ninh mạng được tích hợp liền mạch vào kế hoạch vận hành chung của công ty.

↑ Lên đầu

chief security officer (CSO)

Dịch: giám đốc an ninh (CSO)

Giải thích:

Ví dụ: CSO phát triển và thực thi chương trình an ninh thông tin tổng thể và báo cáo trực tiếp cho CEO hoặc hội đồng quản trị.

↑ Lên đầu

chief technical officer (CTO)

Dịch: giám đốc kỹ thuật (CTO)

Giải thích: *lãnh đạo cấp cao phụ trách công nghệ, nghiên cứu và phát triển sản phẩm*

Ví dụ: Giám đốc kỹ thuật (CTO) của công ty khởi nghiệp đó tập trung vào việc nghiên cứu công nghệ AI mới để tích hợp vào sản phẩm, giúp nó vượt lên trên đối thủ cạnh tranh.

↑ Lên đầu

Cisco Discovery Protocol (CDP)

Dịch: Cisco Discovery Protocol (CDP)

Giải thích: *Giao thức riêng của Cisco cho phép thiết bị Cisco công bố thông tin (model, IP, version) tới neighbor. Hữu ích cho quản trị; nhưng tiết lộ thông tin có thể làm lộ bề mặt tấn công nếu chạy trên cổng có host không đáng tin.*

Ví dụ: show cdp neighbors hiển thị thiết bị Cisco kề bên.

Xem thêm: host

↑ Lên đầu

Cisco's Encrypted Traffic Analytics (ETA), U. S. National Security Agency (NSA)

Dịch: Cisco ETA; NSA

Giải thích: *công nghệ/phương pháp phân tích traffic mã hóa để phát hiện mối đe dọa.*

Ví dụ: Một hệ thống mạng lớn sử dụng Cisco's ETA để phát hiện các hoạt động của mã độc bên trong các luồng HTTPS.

↑ Lên đầu

classes

Dịch: lớp

Giải thích: *lớp trong lập trình hướng đối tượng*

Ví dụ: Một công cụ pentest được viết bằng Python sử dụng các Classes để định nghĩa các đối tượng như 'Target', 'Vulnerability', và 'Report'.

↑ Lên đầu

Cloud

Dịch: Điện toán đám mây

Giải thích: *Cung cấp tài nguyên IT (compute, storage, mạng, dịch vụ) qua mạng Internet theo mô hình dịch vụ. Ưu: scale, pay-as-you-go, triển khai nhanh. Rủi ro: cấu hình sai, quản lý IAM kém, rò rỉ dữ liệu. Phòng thủ: quản trị quyền, Encryption, logging, patching, CSP best practices.*

Ví dụ: Một công ty triển khai hệ thống ERP trên AWS thay vì mua server vật lý tại văn phòng.

Xem thêm: Encryption

↑ Lên đầu

Cloud Custodian

Dịch: Cloud Custodian

Giải thích: *tool quản lý, kiểm soát tuân thủ chính sách Cloud.*

Ví dụ: Một công ty sử dụng Cloud Custodian để tự động thực thi một chính sách: 'xóa tất cả các bucket S3 không được mã hóa sau 24 giờ'.

Xem thêm: Cloud

↑ Lên đầu

Cloud malware injection attack

Dịch: Tấn công chèn/mã độc lên cloud (Malware injection)

Giải thích: *Kẻ tấn công chèn mã độc vào ứng dụng/instance/Cloud image hoặc container (qua lỗ hổng, compromised third-party libs, CI/CD hay supply-chain) để chiếm dữ liệu/ứng dụng. Phòng thủ: image signing, secure CI/CD, dependency scanning, runtime detection.*

Ví dụ: Kẻ tấn công tải lên image EC2 có chứa backdoor, sau đó người khác triển khai nhầm image này.

Xem thêm: Cloud

↑ Lên đầu

CloudBrute

Dịch: CloudBrute

Giải thích: *tool Enumeration tài khoản Cloud, kiểm tra quyền truy cập.*

Ví dụ: Attacker sử dụng CloudBrute để tìm kiếm các bucket S3 hoặc các blog lưu trữ của một công ty mục tiêu.

Xem thêm: Cloud, Enumeration

↑ Lên đầu

Coagula

Dịch: Coagula

Giải thích: *tool chuyển dữ liệu vào dạng âm thanh để Steganography.*

Ví dụ: Một nghệ sĩ sử dụng Coagula để nhúng các hình ảnh ẩn vào trong bản nhạc của mình như một dạng trứng phục sinh"."

Xem thêm: Steganography

↑ Lên đầu

Comma-separated values (CSV)

Dịch: CSV

Giải thích: *định dạng văn bản phân tách bằng dấu phẩy — lưu bảng dữ liệu*

Ví dụ: Pentester xuất danh sách các lỗ hổng tìm thấy ra một file CSV để dễ dàng mở và phân tích bằng Excel.

↑ Lên đầu

Command and Control (C2) systems

Dịch: hệ thống Command and Control (C2)

Giải thích: *hệ thống/infra dùng để điều khiển agent/malware trên máy bị chiếm.*

Ví dụ: Attacker sử dụng giao diện của máy chủ C2 để ra lệnh cho 100 máy đã chiếm quyền đồng loạt tải về và thực thi một mã độc tống tiền.

↑ Lên đầu

Commodity Futures Trading Commission (CFTC)

Dịch: Ủy ban Giao dịch Hàng hóa Tương lai Hoa Kỳ (CFTC)

Giải thích: *cơ quan giám sát thị trường phái sinh, đảm bảo an toàn giao dịch tài chính*

Ví dụ: Ủy ban Giao dịch Hàng hóa Tương lai Hoa Kỳ (CFTC) giám sát các sàn giao dịch để đảm bảo tính minh bạch và ngăn chặn các hành vi thao tác thị trường.

↑ Lên đầu

Common Vulnerabilities and Exposures (CVE)

Dịch: CVE

Giải thích: *danh mục chuẩn ghi nhận lỗ hổng đã biết, mỗi mục có mã định danh duy nhất*

Ví dụ: Lỗ hổng Log4Shell nổi tiếng được gán mã định danh là CVE-2021-44228, giúp các chuyên gia bảo mật trên toàn thế giới có thể nhanh chóng tra cứu và tham chiếu đến nó.

↑ Lên đầu

Common Vulnerability Scoring System (CVSS)

Dịch: CVSS

Giải thích: *hệ thống chấm điểm mức độ nghiêm trọng của lỗ hổng để ưu tiên xử lý*

Ví dụ: Theo Hệ thống chấm điểm lỗ hổng chung (CVSS), lỗ hổng Log4Shell được chấm điểm 10.0 (Mức độ Cực kỳ Nghiêm trọng - Critical) vì nó cho phép thực thi mã từ xa mà không cần xác thực.

↑ Lên đầu

Common Weakness Enumeration (CWE)

Dịch: CWE

Giải thích: *danh mục các kiểu điểm yếu phần mềm dẫn đến lỗ hổng bảo mật*

Ví dụ: Lập trình viên đã vi phạm CWE-89 (Improper Neutralization of Special Elements used in an SQL Command), một điểm yếu phổ biến dẫn đến lỗ hổng SQL Injection.

↑ Lên đầu

Community cloud

Dịch: Đám mây cộng đồng

Giải thích: *Hạ tầng chia sẻ giữa một nhóm tổ chức có yêu cầu tương tự (ví dụ ngành y tế). Kết hợp lợi ích public và private. Phòng thủ: governance, access control, hợp đồng ràng buộc.*

Ví dụ: Các bệnh viện cùng chia sẻ hạ tầng cloud riêng cho việc lưu trữ hồ sơ y tế.

↑ Lên đầu

Compliance Scan

Dịch: quét tuân thủ

Giải thích: *kiểm tra theo chuẩn PCI DSS, CIS, NIST, báo cáo mức tuân thủ*

Ví dụ: Hàng quý, công ty phải chạy một quét tuân thủ (Compliance Scan) theo chuẩn PCI DSS để đảm bảo không có cấu hình sai nào (như TLS 1.0) tồn tại trong vùng dữ liệu thẻ (Cardholder Data Environment).

↑ Lên đầu

conditionals

Dịch: cấu trúc điều kiện

Giải thích: *if, case — dùng để đưa ra quyết định trong code*

Ví dụ: Script tự động hóa sử dụng Conditionals để chỉ chạy module khai thác web nếu kết quả quét cổng cho thấy cổng 80 đang mở.

↑ Lên đầu

Conficker

Dịch: Conficker (worm)

Giải thích: *Worm mạng nhắm vào Windows (2008–), lây lan qua mạng/sử dụng lỗ hổng và cấu hình yếu; dùng để thiết lập botnet, backdoor.*

Ví dụ: Tận dụng lỗ hổng MS08-067 để lây nhiễm hàng triệu máy tính.

↑ Lên đầu

Configuration compliance

Dịch: tuân thủ cấu hình

Giải thích: *kiểm tra cấu hình hệ thống theo tiêu chuẩn/chính sách bảo mật*

Ví dụ: Một quản trị viên hệ thống sử dụng một công cụ tự động để quét và kiểm tra Configuration Compliance của các máy chủ Linux trong công ty.

↑ Lên đầu

covert channel

Dịch: covert channel

Giải thích: *kênh ngầm/kênh che giấu — phương thức truyền dữ liệu ẩn để né phát hiện, ví dụ covert timing/storage.*

Ví dụ: Attacker mã hóa dữ liệu thành các truy vấn DNS gửi đến một domain họ kiểm soát, qua mặt hệ thống giám sát chỉ cho phép lưu lượng DNS.

↑ Lên đầu

Credential attack

Dịch: tấn công thông tin xác thực

Giải thích: *brute-force, credential stuffing, phishing để đoạt tài khoản*

Ví dụ: Attacker thực hiện một cuộc Credential Attack bằng cách thử một vài mật khẩu phổ biến với tất cả các tài khoản người dùng tìm thấy được.

↑ Lên đầu

Credential harvesting

Dịch: Thu thập thông tin xác thực

Giải thích: *Kỹ thuật lừa hoặc thu thập credential (phishing, Captive portal, keylogger, endpoint compromise). Hậu quả: account takeover, lateral movement.*

Phòng thủ: phishing awareness, email filtering, MFA, password hygiene, monitor anomalies.

Ví dụ: Trang web giả mạo đăng nhập Microsoft 365 để đánh cắp tên người dùng và mật khẩu của nhân viên.

Xem thêm: Captive portal, lateral movement

↑ Lên đầu

Credential Harvesting attack

Dịch: Tấn công thu thập thông tin xác thực

Giải thích: *Kỹ thuật lừa nạn nhân nhập username/password (ví dụ qua Captive portal giả, phishing page, Evil Twin) để thu credential. Rất phổ biến trong tấn công lừa đảo mạng.*

Ví dụ: Attacker tạo captive portal Wi-Fi giả “FreeAirportWiFi” yêu cầu đăng nhập Facebook để truy cập Internet → thu username và mật khẩu của nạn nhân.

Xem thêm: Captive portal

↑ Lên đầu

Credential stuffing attack

Dịch: Tấn công nhồi nhét thông tin đăng nhập (Credential stuffing)

Giải thích: *Sử dụng danh sách credential (email/username + password) rò rỉ từ dịch vụ khác để tự động thử đăng nhập trên dịch vụ mục tiêu — dựa trên thói quen reuse password của người dùng. Hậu quả: account takeover, fraud. Phòng thủ: triển khai bảo vệ chống bot (rate-limit, IP reputation, CAPTCHA), credential stuffing detection, MFA, giám sát login anomalies, khuyến khích/ép reset mật khẩu sau breach.*

Ví dụ: Danh sách tài khoản bị rò rỉ từ Netflix được attacker dùng để thử đăng nhập vào Spotify hoặc Gmail — vì người dùng tái sử dụng mật khẩu.

↑ Lên đầu

critical findings

Dịch: phát hiện nghiêm trọng

Giải thích: *vấn đề lỗ hổng/riêng tư có tác động cao cần xử lý ngay*

Ví dụ: Lỗ hổng SQL Injection cho phép chiếm quyền quản trị được xếp loại là một Critical Finding.

↑ Lên đầu

D2O attack (Direct-to-Origin attack)

Dịch: Tấn công trực tiếp về origin (D2O)

Giải thích: *Tấn công DDoS/DoS nhắm thẳng vào IP origin (bỏ qua CDN/reverse-proxy) sau khi lộ địa chỉ origin, làm vô hiệu hóa tầng bảo vệ CDN. Phòng thủ: ẩn origin, use WAF/CDN rules, origin ACLs.*

Ví dụ: Sau khi phát hiện IP thật của máy chủ gốc, hacker tấn công DDoS trực tiếp vào IP đó, bỏ qua lớp bảo vệ Cloudflare.

↑ Lên đầu

Daemon

Dịch: daemon

Giải thích: *tiến trình nền chạy liên tục trên hệ thống Unix/Linux — ví dụ sshd, httpd — thường bị lợi dụng/nhắm tới.*

Ví dụ: Attacker chiếm được quyền root và cấu hình một daemon mới. Dịch vụ này sẽ chạy ẩn và mở một reverse shell về máy của attacker mỗi khi hệ thống khởi động.

↑ Lên đầu

data exfiltration

Dịch: data exfiltration

Giải thích: *hành vi/quá trình rút trộm dữ liệu ra khỏi mạng/máy chủ mục tiêu sang bên ngoài.*

Ví dụ: Đây là giai đoạn cuối và là mục tiêu chính của nhiều cuộc tấn công. Sau khi đã xâm nhập và tìm thấy dữ liệu giá trị, attacker phải tìm cách bí mật chuyển

dữ liệu đó ra khỏi mạng của nạn nhân.

↑ Lên đầu

data structures

Dịch: cấu trúc dữ liệu

Giải thích: *mảng, danh sách, cây, bảng băm, lớp…*

Ví dụ: Kết quả quét mạng được lưu vào một dictionary, trong đó mỗi địa chỉ IP là một key và danh sách các cổng mở là value.

↑ Lên đầu

Debugging

Dịch: gỡ lỗi

Giải thích: *phân tích/sửa lỗi để điều tra hoặc phát triển exploit/patch*

Ví dụ: Một nhà nghiên cứu lỗ hổng gắn một trình Debugger vào một ứng dụng bị crash để kiểm tra trạng thái của bộ nhớ và thanh ghi tại thời điểm xảy ra lỗi.

↑ Lên đầu

Decompilation

Dịch: dịch ngược mã

Giải thích: *chuyển mã nhị phân về dạng gần mã nguồn để phân tích*

Ví dụ: Một nhà phân tích mã độc sử dụng công cụ Ghidra để thực hiện Decompilation một file mã độc nhằm hiểu rõ cách thức hoạt động của nó.

↑ Lên đầu

defensive security

Dịch: an ninh phòng thủ

Giải thích: *các biện pháp/best-practices để phòng thủ — IDS/IPS, hardening, monitoring*

Ví dụ: Việc cấu hình tường lửa, cập nhật bản vá và giám sát log hệ thống là những hoạt động thuộc về Defensive Security.

↑ Lên đầu

DHCP spoofing

Dịch: Mạo danh DHCP

Giải thích: *Gửi phản hồi DHCP giả để cấp IP/gateway/DNS do attacker kiểm soát; nạn nhân có thể bị chuyển hướng traffic hoặc mất kết nối an toàn (MITM, phishing).*

Ví dụ: Attacker trong LAN chạy công cụ yersinia gửi phản hồi DHCP giả với gateway = 192.168.1.100 (máy attacker), khiến nạn nhân truy cập Internet thông qua attacker → MITM.

↑ Lên đầu

dictionaries

Dịch: bảng băm / đối tượng khóa-giá trị

Giải thích: *key-value pairs — ví dụ Python dict, JSON object*

Ví dụ: Một script lưu thông tin người dùng dưới dạng Dictionary, với 'username' là key và 'password_hash' là value.

Xem thêm: Python

↑ Lên đầu

dig

Dịch: dig

Giải thích: *tool tra cứu DNS chi tiết*

Ví dụ: Pentester dùng dig example.com ANY để yêu cầu tất cả các loại bản ghi DNS có sẵn của một tên miền.

↑ Lên đầu

DirBuster

Dịch: DirBuster

Giải thích: *tool brute-force thư mục/tệp trên webserver để tìm nội dung ẩn*

Ví dụ: Pentester sử dụng DirBuster với một danh sách từ khóa để khám phá ra một trang quản trị ẩn tại /admin-portal.

↑ Lên đầu

Directory Information Tree (DIT)

Dịch: Cây thông tin thư mục (DIT)

Giải thích: *Cấu trúc phân cấp trong LDAP/AD lưu trữ các đối tượng (users, computers, OUs). DIT định nghĩa cách tổ chức và truy vấn dữ liệu thư mục.*

Ví dụ: DC=example,DC=com → OU=Sales → CN=John Doe trong DIT.

↑ Lên đầu

directory traversal

Dịch: duyệt thư mục trái phép

Giải thích: *Lỗ hổng cho phép truy cập file/thư mục ngoài phạm vi cho phép bằng cách thao tác đường dẫn (ví dụ: ../../etc/passwd).*

Ví dụ: Bằng cách khai thác lỗ hổng duyệt thư mục trái phép (directory traversal) trên tham số ?filename=, kẻ tấn công đã nhập vào ../../../../etc/passwd và đọc được tệp tin chứa thông tin người dùng hệ thống.

↑ Lên đầu

Disassociation (Deauthentication) attack

Dịch: Tấn công ngắt kết nối (deauth/disassoc)

Giải thích: *Gửi frame deauth/disassoc giả khiến thiết bị bị ngắt khỏi AP; dùng để gây gián đoạn dịch vụ, ép client reconnect (phục vụ tấn công tiếp theo như Evil Twin hoặc WPA handshake capture).*

Ví dụ: Dùng aireplay-ng --deauth 100 -a -c để ngắt kết nối người dùng khỏi AP, buộc họ reconnect để thu handshake WPA2.

↑ Lên đầu

Distinguished Name (DN)

Dịch: Tên phân biệt (DN)

Giải thích: *Định danh đầy đủ một đối tượng trong LDAP/AD (ví dụ CN=John Doe,OU=Sales,DC=example,DC=com). Dùng để tham chiếu chính xác đối tượng trong các thao tác LDAP.*

Ví dụ: Dùng DN khi sửa đổi thuộc tính của một user qua LDAP.

↑ Lên đầu

DNS cache poisoning

Dịch: Độc hại bộ nhớ đệm DNS / Poisoning cache DNS

Giải thích: *Kỹ thuật tấn công thay đổi bản ghi DNS trong bộ nhớ đệm của resolver để trỏ tên miền sang IP do attacker kiểm soát — dẫn đến phishing, MITM hoặc redirect traffic.*

Ví dụ: Khi người dùng gõ bank.com, DNS bị poison trỏ tới server attacker → phishing.

↑ Lên đầu

DNS lookup

Dịch: tra cứu DNS

Giải thích: *quá trình truy vấn để lấy thông tin bản ghi tên miền: A, MX, CNAME, TXT…*

Ví dụ: Một thao tác tra cứu DNS (DNS lookup) đơn giản vào bản ghi MX (Mail Exchange) đã tiết lộ rằng công ty đang sử dụng dịch vụ email của Google (G Suite).

↑ Lên đầu

DNS poisoning

Dịch: đầu độc DNS

Giải thích: *sửa/tiêm bản ghi DNS giả vào cache hoặc server để chuyển hướng người dùng tới địa chỉ độc hại*

Ví dụ: Do bị đầu độc DNS (DNS poisoning), khi người dùng gõ mybank.com vào trình duyệt, máy tính của họ lại phân giải ra địa chỉ IP của máy chủ lừa đảo thay vì IP của ngân hàng.

↑ Lên đầu

DNS tunneling (DNS exfiltration)

Dịch: DNS tunneling

Giải thích: *kỹ thuật gửi dữ liệu ra ngoài qua truy vấn DNS.*

Ví dụ: Attacker sử dụng DNS tunneling để rút trộm dữ liệu từ một mạng bị cô lập, chỉ cho phép lưu lượng DNS đi ra ngoài.

↑ Lên đầu

DNSCat2

Dịch: DNSCat2

Giải thích: *tool tạo kênh C2/tunnel mã hoá qua giao thức DNS — dùng để truyền lệnh/dữ liệu qua DNS.*

Ví dụ: Dùng để tạo một kênh C2 được mã hóa hoàn toàn qua giao thức DNS. Kỹ thuật này cực kỳ hiệu quả để vượt qua các tường lửa nghiêm ngặt nhất vì gần như không hệ thống nào chặn DNS.

↑ Lên đầu

DNSRecon

Dịch: DNSRecon

Giải thích: *công cụ thu thập & phân tích thông tin DNS phục vụ Reconnaissance và Enumeration*

Ví dụ: Pentester đã chạy DNSRecon với tùy chọn Zone Transfer" (truyền vùng) và thành công tải về toàn bộ bản ghi DNS của máy chủ tên miền do cấu hình sai."

Xem thêm: Enumeration, Reconnaissance

↑ Lên đầu

Domain Name System Security Extensions (DNSSEC)

Dịch: Tiện ích mở rộng Bảo mật Hệ thống Tên Miền (DNSSEC)

Giải thích: *Mở rộng cho DNS để xác thực tính toàn vẹn và nguồn gốc của đáp trả DNS bằng chữ ký số (digital signatures). Giúp chống DNS spoofing / cache poisoning bằng cách cho resolver biết bản ghi DNS có bị sửa hay không.*

Ví dụ: Trang web nic.vn có thể dùng DNSSEC để đảm bảo bản ghi DNS không bị sửa đổi.

↑ Lên đầu

DoS attack (Denial-of-Service)

Dịch: Tấn công từ chối dịch vụ (DoS/DDoS)

Giải thích: *Làm dịch vụ không sẵn sàng cho người dùng hợp lệ bằng cách làm tắc nghẽn băng thông hoặc cạn kiệt tài nguyên; DDoS sử dụng nhiều nguồn phân tán. Phòng thủ: CDN, WAF, DDoS protection, scaling, rate-limit.*

Ví dụ: Botnet Mirai gửi hàng triệu gói SYN đến web ngân hàng làm nghẽn băng thông.

↑ Lên đầu

Dradis

Dịch: Dradis

Giải thích: *tool/platform để thu thập, tổng hợp và báo cáo kết quả pentest/scan*

Ví dụ: Đội pentest nhập kết quả từ Nmap và Burp Suite vào Dradis để quản lý các lỗ hổng và viết báo cáo cuối cùng cho khách hàng.

↑ Lên đầu

DRM (Digital Rights Management)

Dịch: Quản lý quyền số (DRM)

Giải thích: *Các kỹ thuật/cơ chế bảo vệ nội dung số (bảo vệ bản quyền, kiểm soát playback). Sử dụng mã hóa, license server, watermarking. Lưu ý: có thể ảnh hưởng UX và privacy nếu triển khai quá chặt.*

Ví dụ: Netflix sử dụng DRM để mã hóa nội dung phim, ngăn người dùng ghi lại video bằng phần mềm chụp màn hình.

↑ Lên đầu

DropboxC2 (DBC2)

Dịch: DropboxC2 (DBC2)

Giải thích: *C2 sử dụng Dropbox làm kênh truyền/điều khiển để che giấu traffic.*

Ví dụ: Dùng để che giấu hoàn toàn lưu lượng C2 bằng cách sử dụng API của một dịch vụ đám mây hợp pháp như Dropbox làm kênh giao tiếp.

↑ Lên đầu

Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG)

Dịch: Dual_EC_DRBG

Giải thích: *cơ chế tạo số ngẫu nhiên dựa trên elip — từng có backdoor nghi ngờ.*

Ví dụ: Các tiêu chuẩn bảo mật hiện đại cấm sử dụng Dual_EC_DRBG do các lo ngại về tính toàn vẹn của nó.

↑ Lên đầu

Dumpster diving

Dịch: lục thùng rác

Giải thích: *tìm kiếm thông tin nhạy cảm trong rác/hồ sơ thải bỏ như hóa đơn, mật khẩu in ra*

Ví dụ: Bằng cách lục thùng rác (dumpster diving) phía sau văn phòng, kẻ tấn công đã tìm thấy một bản in danh sách nhân viên nội bộ và một hóa đơn cũ tiết lộ tên nhà cung cấp dịch vụ Internet của công ty.

↑ Lên đầu

dynamic application security testing (DAST)

Dịch: kiểm thử bảo mật ứng dụng động (DAST)

Giải thích: *thử nghiệm ứng dụng khi chạy để phát hiện lỗi bảo mật*

Ví dụ: Pentester sử dụng Burp Suite Scanner để thực hiện DAST trên một ứng dụng web đang hoạt động.

↑ Lên đầu

EAPHammer

Dịch: EAPHammer

Giải thích: *tool pentest Wi-Fi Enterprise — tấn công WPA2-Enterprise*

Ví dụ: Pentester sử dụng EAPHammer để thực hiện một cuộc tấn công Evil Twin" nhằm đánh cắp thông tin đăng nhập của người dùng vào mạng Wi-Fi doanh nghiệp."

↑ Lên đầu

Eavesdropping

Dịch: nghe lén

Giải thích: *chặn/đọc lưu lượng mạng không mã hóa giữa các bên*

Ví dụ: Kẻ tấn công đã thực hiện nghe lén (Eavesdropping) tại một quán cà phê Wi-Fi công cộng và bắt được mật khẩu đăng nhập của một người dùng do trang web đó không sử dụng HTTPS.

↑ Lên đầu

edb Debugger

Dịch: edb Debugger

Giải thích: *GUI debugger cho Linux — phân tích nhị phân.*

Ví dụ: Một nhà nghiên cứu lỗ hổng sử dụng edb Debugger để phân tích một file thực thi ELF trên Linux.

↑ Lên đầu

Elicitation

Dịch: khai thác thông tin (elicitation)

Giải thích: *kỹ thuật tinh tế thu thập thông tin từ nạn nhân qua trò chuyện, hỏi khéo mà nạn nhân không nhận ra*

Ví dụ: Bằng kỹ thuật khai thác thông tin (elicitation), kẻ tấn công đã giả làm đồng nghiệp và qua một cuộc trò chuyện phiếm trong thang máy, đã khéo léo hỏi được nhân viên IT về phiên bản hệ điều hành máy chủ mà không gây nghi ngờ.

↑ Lên đầu

emergency contact

Dịch: liên hệ khẩn cấp

Giải thích: *số/người liên hệ trong trường hợp sự cố nghiêm trọng*

Ví dụ: Nếu phát hiện một lỗ hổng nghiêm trọng có thể làm sập hệ thống, đội pentest sẽ gọi ngay cho Emergency Contact bất kể ngày hay đêm.

↑ Lên đầu

Empire

Dịch: Empire

Giải thích: *post-exploitation framework/agent dựa trên PowerShell và Python để điều khiển, chạy lệnh và C2.*

Ví dụ: Là một framework hậu khai thác mạnh mẽ, tập trung vào việc sử dụng các agent bằng PowerShell và Python. Nó cung cấp một hệ thống C2 hoàn chỉnh để quản lý các máy đã bị chiếm quyền.

Xem thêm: PowerShell, Python

↑ Lên đầu

Empire

Dịch: Empire (post-exploitation framework)

Giải thích: *Framework post-exploitation (PowerShell/agent-based) dùng cho red team để điều khiển, lateral movement, thu thập thông tin. Tương tự Metasploit ở mảng sau khai thác.*

Ví dụ: Red team sử dụng agent PowerShell để quản lý các endpoint trong engagement.

Xem thêm: lateral movement, Metasploit, PowerShell, red team

↑ Lên đầu

Encryption

Dịch: mã hóa

Giải thích: *bảo vệ dữ liệu — symmetric/asymmetric, TLS, AES…*

Ví dụ: Công ty sử dụng Encryption toàn bộ ổ đĩa để bảo vệ dữ liệu trên laptop của nhân viên trong trường hợp bị mất cắp.

↑ Lên đầu

Enum4linux

Dịch: enum4linux

Giải thích: *script Linux thu thập thông tin từ Windows/SMB/AD — users, shares, policies*

Ví dụ: Trong một cuộc kiểm thử nội bộ, pentester chạy Enum4linux trên một máy chủ để tìm kiếm các thư mục chia sẻ không được bảo vệ.

↑ Lên đầu

Enum4linux

Dịch: Enum4linux (SMB/NetBIOS enumeration tool)

Giải thích: *Script/khung để liệt kê thông tin từ SMB/NetBIOS/LDAP trên host Windows (ví dụ shares, users, groups, domain info). Hữu ích để thu thập thông tin trong đánh giá bảo mật.*

Ví dụ: enum4linux -a 192.168.1.10 → liệt kê người dùng, nhóm, chia sẻ mạng, domain info.

Xem thêm: host

↑ Lên đầu

Enumeration

Dịch: liệt kê

Giải thích: *thu thập chi tiết về dịch vụ, tài khoản, port sau trinh sát*

Ví dụ: Sau khi tìm thấy một máy chủ, pentester thực hiện Enumeration bằng Nmap để xác định chính xác các dịch vụ và phiên bản đang chạy trên từng cổng.

↑ Lên đầu

EternalBlue

Dịch: EternalBlue (exploit SMBv1 của NSA leaked)

Giải thích: *Một exploit nổi tiếng lợi dụng lỗ hổng trong SMBv1 của Windows (MS17-010) để thực thi mã từ xa. Đã được dùng trong nhiều malware (ví dụ WannaCry). Thông tin thường dùng để vá lỗi/kiểm tra hệ thống.*

Ví dụ: Được tích hợp trong Metasploit: exploit/windows/smb/ms17_010_eternalblue.

Xem thêm: WannaCry

↑ Lên đầu

ethical hacking

Dịch: hacking có đạo đức

Giải thích: *Hoạt động kiểm thử/tấn công được cho phép nhằm tìm lỗ hổng và giúp cải thiện bảo mật.*

Ví dụ: Một công ty đã thuê một chuyên gia ethical hacking để kiểm tra hệ thống, và anh ta đã phát hiện ra một lỗ hổng SQL Injection mà không làm rò rỉ bất kỳ dữ liệu nhạy cảm nào.

↑ Lên đầu

European Union's General Data Protection Regulation (GDPR)

Dịch: GDPR

Giải thích: *Quy định Bảo vệ Dữ liệu chung của EU — liên quan quyền riêng tư/dữ liệu cá nhân*

Ví dụ: Do GDPR, kết quả whois cho một tên miền .de thường không hiển thị tên và địa chỉ của chủ sở hữu.

↑ Lên đầu

Evasion

Dịch: né tránh

Giải thích: *kỹ thuật tránh phát hiện bởi AV/IDS/EDR hoặc logging.*

Ví dụ: Attacker sử dụng mã hóa và các kỹ thuật làm rối mã (obfuscation) trên payload của mình như một kỹ thuật Evasion.

↑ Lên đầu

Evasion

Dịch: né tránh

Giải thích: *kỹ thuật tránh phát hiện bởi AV/IDS/EDR và logging*

Ví dụ: Attacker sử dụng mã hóa và các kỹ thuật làm rối mã (obfuscation) trên payload của mình như một kỹ thuật Evasion.

↑ Lên đầu

Evil Twin attack

Dịch: Tấn công Evil Twin" (AP giả mạo giống hệt)"

Giải thích: *Tạo AP giả với cùng SSID/phần cấu hình như AP hợp lệ để dụ nạn nhân kết nối; attacker có thể sniff/đổi hướng traffic hoặc thực hiện Captive portal.*

Ví dụ: Attacker tạo AP tên “Café_Free_WiFi” giống hệt mạng thật của quán, người dùng kết nối nhầm → toàn bộ traffic bị sniff qua laptop attacker.

Xem thêm: Captive portal

↑ Lên đầu

EXIF (exchangeable image file format)

Dịch: EXIF

Giải thích: *metadata trong file ảnh — vị trí, model máy ảnh, timestamp…*

Ví dụ: Dữ liệu EXIF trong một bức ảnh trên mạng xã hội có thể vô tình làm lộ vị trí nhà của người đăng.

↑ Lên đầu

ExifTool

Dịch: ExifTool

Giải thích: *tiện ích đọc/ghi siêu dữ liệu EXIF, IPTC, XMP trong ảnh, file đa phương tiện, tài liệu*

Ví dụ: Bằng cách chạy ExifTool trên bức ảnh mà nghi phạm đăng tải, nhà điều tra đã trích xuất được tọa độ GPS chính xác (GPS coordinates) nơi bức ảnh được chụp.

↑ Lên đầu

ExifTool

Dịch: ExifTool

Giải thích: *tool đọc/ghi metadata file — EXIF, IPTC, XMP*

Ví dụ: Một điều tra viên sử dụng ExifTool để tìm tọa độ GPS và thời gian chụp từ một bức ảnh kỹ thuật số.

↑ Lên đầu

Exploit Chaining

Dịch: Xâu chuỗi khai thác / chuỗi khai thác (Exploit Chaining)

Giải thích: *Kỹ thuật phối hợp nhiều khai thác/lỗ hổng nối tiếp để đạt mục tiêu lớn hơn (ví dụ: khai thác lỗ hổng ban đầu để leo quyền rồi dùng lỗ hổng khác để di chuyển ngang). Phòng thủ: patch management nhanh, phân tách quyền (least privilege), network segmentation, EDR/IDS, giảm bề mặt tấn công.*

Ví dụ: Attacker khai thác lỗ hổng web (SQLi) để tải lên webshell, sau đó dùng privilege escalation (kernel exploit) để chiếm quyền root và di chuyển ngang sang server khác.

Xem thêm: network segmentation, patch management

↑ Lên đầu

Exploits

Dịch: exploit

Giải thích: *mã hoặc kỹ thuật lợi dụng lỗ hổng để thực thi hành vi trái phép trên hệ thống mục tiêu*

Ví dụ: Sau khi phát hiện máy chủ dính lỗ hổng MS17-010, pentester đã sử dụng một exploit (mã khai thác) công khai để giành quyền kiểm soát hệ thống (system shell).

↑ Lên đầu

Extended Service Set Identifier (ESSID)

Dịch: ESSID — Tên mạng mở rộng (ESS)

Giải thích: *Tên (tương tự SSID) đại diện cho một Extended Service Set — nhiều AP hợp thành một ESS để cung cấp roaming cùng một tên mạng. Trong thực tế ESSID hay được gọi là SSID.*

Ví dụ: Hệ thống Wi-Fi trường đại học có nhiều AP đều mang ESSID “Campus_WiFi” để sinh viên roaming mượt giữa các khu.

↑ Lên đầu

false negative

Dịch: âm tính giả

Giải thích: *hệ thống bỏ sót sự cố — không báo cảnh báo trong khi có xâm phạm*

Ví dụ: Một mã độc mới lọt vào hệ thống và đánh cắp dữ liệu mà không bị phần mềm diệt virus phát hiện. Đây là một False Negative.

↑ Lên đầu

false positive

Dịch: dương tính giả

Giải thích: *cảnh báo/alert nhưng thực tế không phải sự cố*

Ví dụ: Hệ thống IDS tạo ra một cảnh báo tấn công khi một quản trị viên đang thực hiện quét mạng định kỳ. Đây là một False Positive.

↑ Lên đầu

Federal Deposit Insurance Corporation (FDIC) Safeguards Act

Dịch: Đạo luật Bảo vệ của FDIC

Giải thích: *quy định về an ninh và bảo mật dữ liệu cho các tổ chức tài chính được bảo hiểm tiền gửi liên bang tại Hoa Kỳ*

Ví dụ: Ngân hàng đã phải nâng cấp hệ thống giám sát an ninh để tuân thủ các quy định trong Đạo luật Bảo vệ của FDIC.

↑ Lên đầu

Federal Financial Institutions Examination Council (FFIEC)

Dịch: Hội đồng kiểm tra các tổ chức tài chính liên bang (FFIEC)

Giải thích: *cơ quan Hoa Kỳ thiết lập tiêu chuẩn giám sát ngân hàng và bảo mật hệ thống tài chính*

Ví dụ: Các ngân hàng phải tuân thủ hướng dẫn an ninh mạng từ Hội đồng kiểm tra các tổ chức tài chính liên bang (FFIEC) để đảm bảo an toàn cho hệ thống của mình.

↑ Lên đầu

Federal Risk and Authorization Management Program (FedRAMP)

Dịch: Chương trình FedRAMP

Giải thích: *chương trình của chính phủ Hoa Kỳ để chuẩn hóa đánh giá, ủy quyền và giám sát an ninh các dịch vụ Cloud*

Ví dụ: Để bán dịch vụ cloud của mình cho các cơ quan liên bang, công ty công nghệ đó phải đạt được chứng nhận Chương trình FedRAMP.

Xem thêm: Cloud

↑ Lên đầu

Federated authentication

Dịch: Xác thực liên liên kết (Federated authentication)

Giải thích: *Mô hình SSO giữa các tổ chức/ứng dụng sử dụng trust (ví dụ SAML, OpenID Connect) để chia sẻ identity/assertions. Giúp hợp tác cross-domain. Rủi ro: trust misconfiguration, assertion abuse. Phòng thủ: validate assertions, strict metadata, short token lifetime, audit.*

Ví dụ: Người dùng sử dụng tài khoản đại học (IdP A) để đăng nhập vào hệ thống học trực tuyến quốc gia (SP B) thông qua SAML.

↑ Lên đầu

Fern Wi-Fi Cracker

Dịch: Fern Wi-Fi Cracker

Giải thích: *GUI tool tấn công mật khẩu Wi-Fi.*

Ví dụ: Một người mới bắt đầu trong lĩnh vực bảo mật sử dụng Fern Wi-Fi Cracker để thực hiện các cuộc tấn công Wi-Fi đầu tiên của mình.

↑ Lên đầu

File Transfer Protocol Secure (FTPS)

Dịch: FTP qua SSL/TLS (FTPS)

Giải thích: *Phiên bản FTP được bảo mật bằng SSL/TLS (mã hóa control/data channels). Khác với SFTP. FTPS thường dùng certificate và có nhiều chế độ (implicit/explicit).*

Ví dụ: Server FTP cung cấp FTPS implicit trên port 990.

↑ Lên đầu

fileless malware

Dịch: fileless malware

Giải thích: *mã độc không dựa trên file" — hoạt động trong bộ nhớ hoặc dùng công cụ hợp lệ của hệ thống để né phát hiện."*

Ví dụ: Là kỹ thuật tấn công tàng hình, trong đó mã độc hoạt động trực tiếp trong bộ nhớ (RAM) hoặc lợi dụng các công cụ có sẵn của hệ thống để né tránh các phần mềm diệt virus.

↑ Lên đầu

Financial Institutions Letters (FILs)

Dịch: Thư hướng dẫn các tổ chức tài chính (FILs)

Giải thích: *văn bản chính thức từ FDIC đưa ra các quy định, hướng dẫn về an toàn và bảo mật*

Ví dụ: FDIC đã ban hành một Thư hướng dẫn các tổ chức tài chính (FILs) mới, cảnh báo về các rủi ro an ninh mạng liên quan đến ransomware.

↑ Lên đầu

FindSecBugs

Dịch: FindSecBugs

Giải thích: *plugin SpotBugs để phát hiện lỗ hổng bảo mật trong Java*

Ví dụ: Trong quy trình SSDLC, FindSecBugs được tích hợp để tự động quét và cảnh báo về các lỗ hổng bảo mật trong code Java.

Xem thêm: SpotBugs

↑ Lên đầu

Fingerprinting Organization with Collected Archives (FOCA)

Dịch: FOCA

Giải thích: *tool OSINT thu thập metadata và fingerprint tài liệu/website*

Ví dụ: Pentester dùng FOCA để tải về các file PDF từ website mục tiêu và trích xuất ra tên người dùng, phiên bản phần mềm và tên các máy chủ nội bộ.

↑ Lên đầu

Fog (Fog computing / Edge-fog)

Dịch: Tính toán sương mù (Fog computing)

Giải thích: *Mô hình tính toán phân tán nằm giữa Cloud và edge: xử lý gần nguồn dữ liệu để giảm độ trễ. Rủi ro: nhiều điểm tấn công phân tán. Phòng thủ: secure edge nodes, consistent policy.*

Ví dụ: Camera giám sát xử lý nhận dạng khuôn mặt tại nút fog thay vì gửi toàn bộ video lên cloud.

Xem thêm: Cloud

↑ Lên đầu

Forensics

Dịch: pháp y số

Giải thích: *thu thập và phân tích bằng chứng sau sự cố an ninh*

Ví dụ: Sau một vụ rò rỉ dữ liệu, một đội Forensics được mời đến để phân tích ổ cứng của máy chủ bị xâm nhập.

↑ Lên đầu

Fragmentation attack

Dịch: Tấn công phân mảnh (Fragmentation attack)

Giải thích: *Lợi dụng cách xử lý frame phân mảnh ở layer 2 để truyền payload đặc biệt hoặc né detection; có thể dùng để tái tạo key stream hoặc bypass một số cơ chế bảo mật.*

Ví dụ: Attacker gửi các frame Wi-Fi bị phân mảnh đặc biệt để tái tạo key stream WEP và chèn payload tùy chỉnh, nhằm bypass cơ chế IDS lớp 2.

↑ Lên đầu

fully qualified domain names (FQDNs)

Dịch: tên miền đủ điều kiện (FQDN)

Giải thích: *địa chỉ DNS đầy đủ gồm hostname + domain, ví dụ: www.example.com*

Ví dụ: Để trỏ CNAME cho một tên miền phụ, bạn cần sử dụng tên miền đủ điều kiện (FQDNs), ví dụ như blog.congty.com, chứ không chỉ là blog.

↑ Lên đầu

Fuzz testing

Dịch: kiểm thử fuzz

Giải thích: *kỹ thuật thử nghiệm phần mềm với dữ liệu ngẫu nhiên để tìm lỗi/lỗ hổng*

Ví dụ: Fuzz Testing đã giúp phát hiện ra hàng nghìn lỗ hổng nghiêm trọng trong các phần mềm mã nguồn mở phổ biến.

↑ Lên đầu

Fuzzers

Dịch: fuzzers

Giải thích: *công cụ thực hiện Fuzz testing — kiểm thử đầu vào ngẫu nhiên*

Ví dụ: Các nhà nghiên cứu bảo mật sử dụng các Fuzzers khác nhau để tìm kiếm các lỗ hổng zero-day trong các trình duyệt web và các hệ điều hành.

Xem thêm: Fuzz testing

↑ Lên đầu

Fuzzing

Dịch: kiểm thử fuzz

Giải thích: *dùng dữ liệu ngẫu nhiên/độc hại để tìm crash/lỗ hổng*

Ví dụ: Một nhà nghiên cứu bảo mật sử dụng một công cụ Fuzzing để kiểm thử một thư viện xử lý ảnh và phát hiện ra một lỗ hổng buffer overflow.

↑ Lên đầu

Gantt Chart

Dịch: biểu đồ Gantt

Giải thích: *công cụ quản lý dự án thể hiện tiến độ, công việc và mốc thời gian bằng sơ đồ thanh ngang*

Ví dụ: Người quản lý dự án đã sử dụng biểu đồ Gantt để theo dõi tiến độ của các tác vụ và đảm bảo dự án hoàn thành đúng hạn.

↑ Lên đầu

General Data Protection Regulation (GDPR)

Dịch: Quy định bảo vệ dữ liệu chung (GDPR)

Giải thích: *luật bảo vệ dữ liệu cá nhân của Liên minh châu Âu - EU*

Ví dụ: Theo Quy định bảo vệ dữ liệu chung (GDPR), các công ty phải có được sự đồng ý rõ ràng của người dùng châu Âu trước khi thu thập dữ liệu cá nhân của họ.

↑ Lên đầu

GitHub

Dịch: Nền tảng GitHub (lưu mã nguồn & collaboration)

Giải thích: *Nơi lưu trữ mã nguồn, công cụ, exploit scripts, tài liệu; được dùng rộng rãi để chia sẻ code (bao gồm cả công cụ bảo mật và PoC). Trong an ninh, dùng để tìm PoC, công cụ hoặc chia sẻ dự án.*

Ví dụ: Công cụ Metasploit, Responder, Enum4linux, Exploit PoC thường được chia sẻ công khai trên GitHub.

↑ Lên đầu

Google dorks

Dịch: Google dorks

Giải thích: *kỹ thuật tìm kiếm nâng cao/chuỗi truy vấn để tìm file, cấu hình, thông tin nhạy cảm được index*

Ví dụ: Sử dụng Google dorks với truy vấn filetype:sql site:example.com, chuyên gia OSINT đã tìm thấy các tệp sao lưu cơ sở dữ liệu (database backup) mà Google đã vô tình lập chỉ mục.

↑ Lên đầu

GraphQL

Dịch: GraphQL

Giải thích: *ngôn ngữ truy vấn API do Facebook phát triển, cho phép client lấy đúng dữ liệu cần thiết từ server*

Ví dụ: Đội phát triển ứng dụng di động thích sử dụng GraphQL vì nó cho phép họ truy vấn chính xác những dữ liệu cần thiết trong một lần gọi API, thay vì phải gọi nhiều endpoint REST khác nhau.

↑ Lên đầu

Hacktivist

Dịch: hacktivist

Giải thích: *Kẻ/hạ tầng hacker mang động cơ chính trị/xã hội, tấn công để tuyên truyền, phản đối hoặc gây chú ý cho một vấn đề.*

Ví dụ: Nhóm Hacktivist Anonymous đã thực hiện một cuộc tấn công DDoS làm sập trang web của chính phủ để phản đối một bộ luật mới mà họ cho là bất công.

↑ Lên đầu

Hashcat

Dịch: Hashcat

Giải thích: *password cracking tool mạnh — hỗ trợ GPU, nhiều thuật toán hash.*

Ví dụ: Sau khi có được một cơ sở dữ liệu hash NTLM, pentester sử dụng Hashcat với một dàn GPU mạnh để bẻ khóa chúng trong thời gian ngắn nhất.

↑ Lên đầu

Health and Human Services (HHS)

Dịch: Bộ Y tế và Dịch vụ Nhân sinh Hoa Kỳ (HHS)

Giải thích: *cơ quan quản lý chính sách y tế, bao gồm cả quy định bảo mật dữ liệu sức khỏe như HIPAA*

Ví dụ: Bộ Y tế và Dịch vụ Nhân sinh Hoa Kỳ (HHS) là cơ quan chịu trách nhiệm thực thi các quy định bảo mật của HIPAA.

↑ Lên đầu

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Dịch: Đạo luật HIPAA (1996)

Giải thích: *quy định bảo mật và quyền riêng tư đối với dữ liệu y tế tại Hoa Kỳ*

Ví dụ: Bệnh viện đã bị phạt hàng triệu đô la vì vi phạm Đạo luật HIPAA (1996) sau khi làm rò rỉ hồ sơ y tế của hàng ngàn bệnh nhân.

↑ Lên đầu

healthcare clearinghouse

Dịch: trung tâm xử lý dữ liệu y tế

Giải thích: *tổ chức trung gian xử lý, chuẩn hóa và truyền tải dữ liệu y tế/bảo hiểm*

Ví dụ: Một trung tâm xử lý dữ liệu y tế (healthcare clearinghouse) đã nhận dữ liệu khám bệnh từ phòng khám, chuẩn hóa nó theo định dạng chuẩn, và gửi cho công ty bảo hiểm để thanh toán.

↑ Lên đầu

healthcare plan

Dịch: kế hoạch bảo hiểm y tế

Giải thích: *chương trình bảo hiểm chi trả chi phí y tế cho cá nhân/tổ chức*

Ví dụ: Công ty bảo hiểm đã cung cấp một kế hoạch bảo hiểm y tế mới cho nhân viên, bao gồm cả chi trả cho dịch vụ nha khoa.

↑ Lên đầu

Horizontal privilege escalation

Dịch: Leo thang đặc quyền theo chiều ngang

Giải thích: *Khi attacker truy cập vào tài nguyên của user khác có cùng mức privilege (ví dụ user A xem dữ liệu user B) — do broken access control. Phòng*

thủ: proper authorization checks, per-user access controls, tests for IDOR/ACL bugs, logging.

Ví dụ: Người dùng A đổi ID trong URL từ /profile?id=1 thành /profile?id=2 để xem dữ liệu của người dùng B.

↑ Lên đầu

horizontal privilege escalation

Dịch: horizontal privilege escalation

Giải thích: *mở rộng quyền ngang — truy cập account/má khác cùng mức để đạt mục tiêu.*

Ví dụ: Là quá trình attacker đã có quyền truy cập vào một tài khoản và dùng nó để chiếm quyền của một tài khoản khác có cùng cấp độ đặc quyền, nhằm truy cập vào các dữ liệu hoặc hệ thống khác.

↑ Lên đầu

host

Dịch: host

Giải thích: *tool DNS lookup đơn giản — trả về A, MX, NS records…*

Ví dụ: Lệnh host example.com sẽ trả về các bản ghi A, AAAA, và MX của tên miền.

Xem thêm: DNS lookup

↑ Lên đầu

host command

Dịch: lệnh host

Giải thích: *công cụ dòng lệnh trong Linux/Unix để tra cứu và phân tích bản ghi DNS*

Ví dụ: Trên Linux, pentester đã sử dụng lệnh host -t mx example.com để nhanh chóng tìm ra máy chủ email (MX record) của công ty mục tiêu.

↑ Lên đầu

Hybrid cloud

Dịch: Đám mây lai (Hybrid cloud)

Giải thích: *Kết hợp public + private nhằm tận dụng cả hai (ví dụ burst workloads lên public). Rủi ro: tích hợp, data flow, cấu hình network phức tạp. Phòng thủ: quản lý mạng an toàn (VPN/Direct Connect), consistent IAM, monitoring across environments.*

Ví dụ: Công ty lưu dữ liệu nhạy cảm trên private cloud, còn dịch vụ web host trên Azure public cloud.

↑ Lên đầu

Hydra

Dịch: Hydra

Giải thích: *tool tấn công mật khẩu đa giao thức — brute-force, dictionary attack.*

Ví dụ: Attacker sử dụng Hydra để thực hiện một cuộc tấn công từ điển vào trang đăng nhập của một thiết bị router.

↑ Lên đầu

IaaS (Infrastructure as a Service)

Dịch: Cơ sở hạ tầng như một dịch vụ (IaaS)

Giải thích: *Cung cấp máy ảo, storage, network (ví dụ EC2, Compute Engine). Người dùng chịu trách nhiệm OS/app, provider quản lý infra. Rủi ro: misconfig VM, security group sai. Phòng thủ: hardening VM, patching, IAM, network segmentation.*

Ví dụ: Dùng Amazon EC2 để tạo và quản lý máy ảo chạy web server Apache.

Xem thêm: network segmentation

↑ Lên đầu

ICS (Industrial Control System)

Dịch: Hệ thống điều khiển công nghiệp (ICS)

Giải thích: *Hệ thống điều khiển (PLC, RTU, HMI) cho nhà máy, lưới điện, water treatment… Rủi ro: legacy protocols, availability-critical. Phòng thủ: network segmentation (OT/IT), monitoring, patch policy.*

Ví dụ: Hệ thống PLC điều khiển dây chuyền sản xuất trong nhà máy ô tô.

Xem thêm: network segmentation

↑ Lên đầu

IDA

Dịch: IDA

Giải thích: *Interactive Disassembler — phân tích mã nhị phân, reverse engineering.*

Ví dụ: Một nhà nghiên cứu bảo mật cấp cao sử dụng IDA Pro để phân tích một mã độc phức tạp và vẽ ra biểu đồ luồng thực thi của nó.

↑ Lên đầu

IIoT (Industrial Internet of Things)

Dịch: Internet vạn vật công nghiệp (IIoT)

Giải thích: *Thiết bị kết nối trong môi trường sản xuất/OT (sensors, actuators). Rủi ro: firmware, insecure protocols. Phòng thủ: device inventory, secure OTA, segmentation.*

Ví dụ: Cảm biến đo nhiệt độ gắn vào máy móc gửi dữ liệu về trung tâm điều khiển công nghiệp qua mạng OT.

↑ Lên đầu

IMAP (Internet Message Access Protocol)

Dịch: Giao thức IMAP (truy cập mail)

Giải thích: *Giao thức để truy cập, quản lý hộp thư trên server mà không cần tải xuống vĩnh viễn — hỗ trợ folder, đồng bộ nhiều thiết bị. Thích hợp cho môi trường nhiều thiết bị truy cập cùng hộp thư.*

Ví dụ: Gmail qua IMAP đồng bộ thư mục trên laptop và điện thoại.

↑ Lên đầu

Immunity Debugger

Dịch: Immunity Debugger

Giải thích: *Windows Debugger nâng cao — hỗ trợ phân tích exploit.*

Ví dụ: Một pentester sử dụng Immunity Debugger với các script Python để tự động hóa việc tìm kiếm các byte xấu (bad characters) khi viết exploit.

Xem thêm: Windows Debugger

↑ Lên đầu

indicators of prior compromise

Dịch: chỉ báo đã từng bị xâm phạm

Giải thích: *IOCs cho thấy hệ thống từng bị tấn công — file, registry, network artefacts*

Ví dụ: Đội an ninh quét toàn bộ hệ thống để tìm kiếm các file có hash khớp với danh sách Indicators of Prior Compromise của một nhóm hacker vừa được công bố.

↑ Lên đầu

information security manager (ISM)

Dịch: quản lý an ninh thông tin (ISM)

Giải thích: *người chịu trách nhiệm vận hành chương trình an ninh thông tin trong tổ chức*

Ví dụ: Quản lý an ninh thông tin (ISM) chịu trách nhiệm đảm bảo rằng các bản vá (patches) bảo mật được cài đặt kịp thời cho tất cả các máy chủ của công ty.

↑ Lên đầu

Information Systems Security Assessment Framework (ISSAF)

Dịch: ISSAF

Giải thích: *Khung đánh giá an ninh hệ thống thông tin, cung cấp phương pháp luận cho đánh giá và kiểm thử.*

Ví dụ: Một pentester chuyên nghiệp đã sử dụng ISSAF vì nó cung cấp các quy trình đánh giá chi tiết và các vector tấn công cụ thể cho từng loại công nghệ, ví dụ như cho hệ thống VPN.

↑ Lên đầu

Initialization Vector (IV) attack

Dịch: Tấn công Vector Khởi tạo (IV attack)

Giải thích: *Lợi dụng yếu tố IV không an toàn (ví dụ WEP) để khai thác tính lặp/khuyết điểm trong thuật toán mã hóa, làm giảm tính bảo mật và khả năng khôi phục khóa. Thường liên quan tới WEP/WPA-TKIP yếu.*

Ví dụ: Trong mạng WEP, attacker thu thập hàng nghìn gói tin có IV trùng lặp để dùng thuật toán RC4 cracking khôi phục khóa bí mật.

↑ Lên đầu

Insider threat

Dịch: mối đe dọa nội bộ

Giải thích: *Nhân viên/đối tác có quyền truy cập lợi dụng vị trí để gây hại, rò rỉ dữ liệu hoặc làm tổn hại hệ thống.*

Ví dụ: Một nhân viên kế toán bất mãn đã trở thành mối đe dọa nội bộ khi anh ta cố tình sao chép và bán dữ liệu tài chính nhạy cảm của công ty cho đối thủ cạnh tranh.

↑ Lên đầu

Interrogation

Dịch: hỏi cung (interrogation)

Giải thích: *hỏi trực tiếp, thường dồn ép để buộc tiết lộ thông tin; trong Social engineering là hỏi thẳng để kiểm tra phản ứng*

Ví dụ: Trong một kịch bản social engineering, kẻ tấn công giả làm nhân viên an ninh và sử dụng kỹ thuật hỏi cung (interrogation), dồn dập hỏi nhân viên: Anh có chắc đã khóa máy tính không? Tôi vừa thấy màn hình của anh sáng đèn." để kiểm tra phản ứng và sự tự tin của họ."

Xem thêm: Social engineering

↑ Lên đầu

IoT (Internet of Things)

Dịch: Internet vạn vật (IoT)

Giải thích: *Thiết bị kết nối mạng (sensor, camera, smart device). Rủi ro: firmware yếu, default creds, thiếu update -> botnet, data leak. Phòng thủ: network segmentation, device inventory, firmware update policy, strong auth.*

Ví dụ: Hệ thống camera IP giám sát gửi dữ liệu hình ảnh về cloud để phân tích hành vi.

Xem thêm: network segmentation

↑ Lên đầu

IPMI (Intelligent Platform Management Interface)

Dịch: Giao diện quản lý nền tảng thông minh (IPMI)

Giải thích: *Giao diện OOB cho quản lý server (BMC/iDRAC/iLO) cung cấp console, power control, KVM; nếu cấu hình yếu (default creds, open network) có thể dẫn tới takeover cấp thấp. Phòng thủ: hardening, segmentation, change default creds, restrict management network.*

Ví dụ: Quản trị viên dùng IPMI để bật/tắt hoặc truy cập console server Dell từ xa; nếu để mặc định admin/admin thì hacker có thể chiếm quyền điều khiển vật lý server.

↑ Lên đầu

Jamming

Dịch: Gây nhiễu (jamming)

Giải thích: *Phát sóng gây nhiễu trên kênh RF để làm gián đoạn giao tiếp không dây (Wi-Fi/Bluetooth). Dùng để làm mất dịch vụ hoặc ép thiết bị chuyển kênh; có thể là hành vi phá hoại/phi pháp.*

Ví dụ: Kẻ tấn công dùng thiết bị phát nhiễu ở tần số 2.4GHz làm mất kết nối Wi-Fi trong phòng họp để gây gián đoạn.

↑ Lên đầu

Japan Computer Emergency Response Team (JPCERT)

Dịch: Đội Ứng phó Sự cố Máy tính Nhật Bản (JPCERT)

Giải thích: *tổ chức quốc gia của Nhật chuyên cảnh báo/ứng phó sự cố an ninh mạng*

Ví dụ: Đội Ứng phó Sự cố Máy tính Nhật Bản (JPCERT) đã phối hợp với các nhà cung cấp dịch vụ Internet (ISP) để đánh sập (takedown) một mạng botnet lớn đang hoạt động tại nước này.

↑ Lên đầu

JavaScript Object Notation (JSON)

Dịch: JSON

Giải thích: *định dạng trao đổi dữ liệu nhẹ, dùng rộng rãi*

Ví dụ: Một công cụ quét lỗ hổng API trả về kết quả dưới dạng một file JSON, trong đó liệt kê chi tiết các endpoint và lỗ hổng tương ứng.

↑ Lên đầu

job rotation

Dịch: luân chuyển công việc

Giải thích: *giảm gian lận, tăng minh bạch, đa kỹ năng*

Ví dụ: Một nhân viên quản lý kho được yêu cầu thực hiện Job Rotation sang vị trí khác trong 1 tháng để người thay thế có thể kiểm tra và phát hiện các sai phạm tiềm ẩn.

↑ Lên đầu

John the Ripper

Dịch: John the Ripper

Giải thích: *password cracker phổ biến — brute-force, dictionary attack.*

Ví dụ: Sau khi trích xuất các hash mật khẩu từ một file /etc/shadow, pentester sử dụng John the Ripper để bẻ khóa chúng.

↑ Lên đầu

Kali Linux

Dịch: Kali Linux

Giải thích: *bản phân phối Linux chuyên dụng cho pentesting và forensic*

Ví dụ: Một pentester khởi động máy tính của mình vào Kali Linux để bắt đầu một cuộc kiểm thử xâm nhập.

↑ Lên đầu

KARMA attack

Dịch: Tấn công KARMA

Giải thích: *Kỹ thuật mạo danh AP trả lời các probe request của client (dựa trên PNL) để dụ client tự kết nối vào AP attacker — thường dùng để thu traffic hoặc thực hiện Captive portal/Credential harvesting.*

Ví dụ: Client có trong PNL “Home_WiFi” gửi probe request; AP giả (attacker) phản hồi “Home_WiFi available” → client tự động kết nối → attacker thu thông tin đăng nhập qua captive portal giả.

Xem thêm: Captive portal, Credential harvesting

↑ Lên đầu

Kerberoasting

Dịch: Kerberoasting (tấn công bẻ khóa ticket dịch vụ Kerberos)

Giải thích: *Kỹ thuật yêu cầu TGS cho service account (được mã hóa bằng password-derived key), lấy xuống và offline-crack để tìm mật khẩu service account. Thường nhắm vào service accounts có mật khẩu yếu.*

Ví dụ: Kẻ tấn công lấy ticket của service account và brute-force offline để tìm mật khẩu.

↑ Lên đầu

Kerberos

Dịch: Kerberos (giao thức xác thực dựa trên vé)

Giải thích: *Hệ thống xác thực mạng dùng vé (tickets) để chứng thực người dùng và dịch vụ trong domain (Windows AD thường dùng Kerberos làm primary auth). Ưu điểm: không truyền mật khẩu plaintext; hỗ trợ mutual auth.*

Ví dụ: Windows domain sử dụng Kerberos TGT/TGS để authenticating user to services.

Xem thêm: Kerberos

↑ Lên đầu

Kerberos golden ticket attack

Dịch: Tấn công vé vàng" Kerberos (Golden Ticket)"

Giải thích: *Kỹ thuật tạo vé Kerberos giả (TGT) với quyền rộng — cho phép impersonate bất kỳ account domain nào. Rủi ro nghiêm trọng khi attacker có được key của domain (KRBTGT). (Mô tả mục đích và hậu quả — không hướng dẫn cách thực hiện.)*

Ví dụ: (Mục đích/hậu quả) Kẻ tấn công với key domain có thể tạo vé cho bất kỳ user nào và duy trì truy cập lâu dài.

Xem thêm: Kerberos

↑ Lên đầu

Kerberos silver ticket attack

Dịch: Tấn công vé bạc" Kerberos (Silver Ticket)"

Giải thích: *Tạo vé dịch vụ Kerberos (TGS) giả cho một service cụ thể (ví dụ HTTP/SMB) bằng cách dùng key của dịch vụ đó — dẫn tới truy cập trái phép tới service mà không cần full domain compromise. (Mô tả hậu quả.)*

Ví dụ: Kẻ tấn công tạo ticket cho cifs/server để truy cập share smb mà không có user password.

Xem thêm: Kerberos

↑ Lên đầu

key rotation

Dịch: luân phiên/thay đổi khóa mật mã định kỳ

Giải thích:

Ví dụ: Chính sách của công ty yêu cầu thực hiện Key Rotation cho khóa mã hóa cơ sở dữ liệu mỗi 90 ngày.

↑ Lên đầu

KisMAC

Dịch: KisMAC (Wi-Fi scanner/sniffer cho macOS)

Giải thích: *Ứng dụng quét/giám sát Wi-Fi trên macOS (tương tự Kismet), hỗ trợ thu handshake, phân tích mạng; dùng cho pentest và khảo sát.*

Ví dụ: Pentester dùng KisMAC trên macOS để thu gói tin WPA handshake từ mạng văn phòng, phục vụ kiểm thử độ mạnh mật khẩu.

Xem thêm: Kismet

↑ Lên đầu

Kismet

Dịch: Kismet (wireless detector/sniffer/IDS)

Giải thích: *Công cụ passive để phát hiện AP/client, thu packet, phát hiện rogue AP và phân tích spectrum; dùng cho khảo sát mạng và phát hiện xâm nhập Wi-Fi.*

Ví dụ: Kỹ sư an ninh dùng Kismet để quét toàn bộ AP trong tòa nhà, phát hiện 2 AP không hợp lệ (rogue AP) trong hệ thống Wi-Fi nội bộ.

↑ Lên đầu

known-environment testing

Dịch: kiểm thử hộp trắng

Giải thích: *pentester được cung cấp đầy đủ thông tin như code, cấu hình, tài liệu*

Ví dụ: Nhờ có kiểm thử hộp trắng (known-environment testing) và quyền truy cập vào mã nguồn, chuyên gia bảo mật đã phát hiện ra một lỗ hổng logic phức tạp.

↑ Lên đầu

Krack attack

Dịch: Tấn công KRACK (Key Reinstallation Attack)

Giải thích: *Lỗi trong quá trình handshake WPA2 cho phép kẻ tấn công buộc tái cài đặt key, gây lộ/chia sẻ key tạm thời và giải mã traffic — là lỗ hổng giao thức/triển khai WPA2 từng được công bố (đã có bản vá).*

Ví dụ: Laptop trong mạng Wi-Fi WPA2 bị attacker gần đó ép tái cài đặt key trong quá trình handshake, cho phép attacker giải mã traffic HTTPS yếu hoặc HTTP plain text.

↑ Lên đầu

ksh

Dịch: ksh

Giải thích: *Korn Shell — Shell dòng lệnh trên Unix.*

Ví dụ: Attacker nhận được một shell và chạy lệnh echo $SHELL, kết quả trả về là /bin/bash, cho biết đây là môi trường Bash.

Xem thêm: Shell

↑ Lên đầu

lateral movement

Dịch: lateral movement

Giải thích: *kỹ thuật di chuyển ngang trong mạng sau khi có initial access để tiếp cận mục tiêu giá trị.*

Ví dụ: Sau khi chiếm được máy của một nhân viên, attacker sử dụng mật khẩu lấy được từ máy đó để đăng nhập vào máy chủ kế toán. Quá trình đó gọi là Lateral Movement.

↑ Lên đầu

LDAP injection

Dịch: tiêm LDAP

Giải thích: *Tương tự SQLi nhưng với truy vấn LDAP; có thể tiết lộ dữ liệu hoặc bypass xác thực nếu input không được kiểm soát.*

Ví dụ: Bằng cách nhập *)(uid=*) vào ô tìm kiếm người dùng, kẻ tấn công đã khai thác lỗ hổng tiêm LDAP (LDAP injection) để bypass bộ lọc và lấy về danh sách toàn bộ nhân viên trong hệ thống Active Directory.

↑ Lên đầu

LDAP-Based attack

Dịch: Tấn công dựa trên LDAP

Giải thích: *Các kỹ thuật khai thác dịch vụ LDAP (ví dụ truy vấn lộ thông tin, injection, lạm dụng phân quyền) để thu thập danh sách người dùng, cấu trúc domain, hoặc sửa đổi thư mục. Thường xuất hiện khi LDAP/AD cấu hình yếu.*

Ví dụ: Thủ công viên thu thập danh sách user bằng truy vấn LDAP khi directory cho phép anonymous bind.

↑ Lên đầu

LeakLooker

Dịch: LeakLooker

Giải thích: *công cụ/dịch vụ tìm kiếm dữ liệu rò rỉ công khai để kiểm tra breach/credential leaks*

Ví dụ: Công cụ LeakLooker đã quét các kho lưu trữ công khai và tìm thấy một tệp backup.zip chứa thông tin nhạy cảm của công ty bị tải lên nhầm.

↑ Lên đầu

Lightweight Directory Access Protocol (LDAP)

Dịch: Giao thức truy cập thư mục (LDAP)

Giải thích: *Giao thức truy vấn và sửa đổi dịch vụ thư mục (ví dụ Active Directory). Dùng để tìm user, group, policy — cũng là nguồn thông tin giá trị cho attacker nếu không được bảo vệ.*

Ví dụ: Quản trị viên dùng ldapsearch để tìm user và thuộc tính trong AD.

↑ Lên đầu

Link-Local Multicast Name Resolution (LLMNR)

Dịch: Giải quyết tên multicast cục bộ (LLMNR)

Giải thích: *Cơ chế thay thế DNS trong mạng cục bộ (link-local) để phân giải tên máy khi DNS không trả lời. Dùng trong mạng Windows; có rủi ro bị spoofing (mạo danh) nên thường bị tắt trong môi trường bảo mật cao.*

Ví dụ: Khi bạn gõ ping LAPTOP01 mà DNS không phản hồi, Windows sẽ tự động dùng LLMNR để hỏi các máy khác trong mạng “Có ai là LAPTOP01 không?”.

↑ Lên đầu

lists

Dịch: danh sách

Giải thích: *danh sách tuần tự — list*

Ví dụ: Script Python sử dụng một List để lưu trữ danh sách các subdomain tìm thấy trong giai đoạn trinh sát.

↑ Lên đầu

living-off-the-land

Dịch: living-off-the-land

Giải thích: *kỹ thuật lợi dụng các công cụ/hàm sẵn có trên hệ thống để tấn công, tránh dùng mã độc tách biệt.*

Ví dụ: Là một triết lý tấn công tàng hình. Attacker ưu tiên sử dụng các công cụ và chức năng có sẵn trên hệ điều hành (như PowerShell, WMI, Task Scheduler) thay vì tải lên các file mã độc riêng, nhằm tránh bị phát hiện.

↑ Lên đầu

logic constructs

Dịch: cấu trúc logic

Giải thích: *if/then/else, switch — cấu trúc điều khiển trong lập trình*

Ví dụ: Trong một script, pentester sử dụng Logic Constructs để kiểm tra if một cổng đang mở then thực hiện quét chi tiết cổng đó.

↑ Lên đầu

loops

Dịch: vòng lặp

Giải thích: *for, while — dùng trong script/automation*

Ví dụ: Attacker sử dụng một vòng lặp for loop để thử từng mật khẩu trong một danh sách cho đến khi tìm được mật khẩu đúng.

↑ Lên đầu

Mail User Agent (MUA)

Dịch: Trình đọc thư (MUA)

Giải thích: *Ứng dụng người dùng dùng để đọc/gửi email (ví dụ Outlook, Thunderbird, mobile mail apps). MUA giao tiếp với MTA/IMAP/POP3 để quản lý hộp thư.*

Ví dụ: Outlook là một MUA kết nối tới Exchange/IMAP.

↑ Lên đầu

Maltego

Dịch: Maltego

Giải thích: *công cụ phân tích liên kết OSINT trực quan, mô tả mối quan hệ giữa domain, email, IP, tổ chức…*

Ví dụ: Chuyên gia điều tra đã sử dụng Maltego để vẽ một biểu đồ trực quan, cho thấy mối liên hệ phức tạp giữa kẻ tình nghi, các công ty vỏ bọc, và các địa chỉ IP mà hắn sử dụng.

↑ Lên đầu

Management Information Base (MIB)

Dịch: Cơ sở thông tin quản lý (MIB)

Giải thích: *Cấu trúc dữ liệu (cây OID) định nghĩa các đối tượng mà SNMP có thể đọc/ghi (ví dụ: cpuLoad, ifDescr). MIB cho phép SNMP manager hiểu ý nghĩa các giá trị trên thiết bị.*

Ví dụ: Khi snmpget truy vấn 1.3.6.1.2.1.1.1.0, SNMP trả về mô tả hệ thống (sysDescr).

↑ Lên đầu

mandatory vacation

Dịch: nghỉ phép bắt buộc

Giải thích: *biện pháp kiểm soát nhân sự để phát hiện gian lận/hoạt động trái phép khi người giữ vị trí vắng mặt*

Ví dụ: Trưởng phòng tài chính phải thực hiện Mandatory Vacation trong 2 tuần liên tục, trong thời gian đó một kiểm toán viên sẽ rà soát lại các giao dịch của ông.

↑ Lên đầu

mantrap

Dịch: mantrap

Giải thích: *phòng kiểm soát truy cập/airlock — dùng 2 cửa để kiểm soát ra/vào vật lý*

Ví dụ: Để vào trung tâm dữ liệu, nhân viên phải đi qua một Mantrap.

↑ Lên đầu

master service agreement (MSA)

Dịch: thỏa thuận dịch vụ tổng thể (MSA)

Giải thích: *hợp đồng khung quy định các điều khoản chung giữa hai bên, áp dụng cho nhiều dự án/dịch vụ*

Ví dụ: Thay vì ký hợp đồng mới mỗi lần, hai công ty đã ký một thỏa thuận dịch vụ tổng thể (MSA) để quy định các điều khoản pháp lý chung cho tất cả các dự án trong tương lai.

↑ Lên đầu

Mdk4

Dịch: Mdk4

Giải thích: *tool pentest Wi-Fi — deauth, Fuzzing, tấn công mạng không dây.*

Ví dụ: Pentester sử dụng Mdk4 để thực hiện một cuộc tấn công deauthentication nhằm ngắt kết nối tất cả người dùng khỏi một mạng Wi-Fi.

Xem thêm: Fuzzing

↑ Lên đầu

Media Access Control (MAC) spoofing

Dịch: Giả mạo địa chỉ MAC

Giải thích: *Thay đổi địa chỉ MAC của giao diện mạng để mạo danh thiết bị khác (ví dụ để vượt qua lọc dựa trên MAC, né danh sách đen, hoặc trốn định danh). Dùng cho mục đích hợp pháp (thử nghiệm) và phi pháp.*

Ví dụ: Kỹ thuật viên test thay MAC để truy cập mạng có filter dựa trên MAC.

↑ Lên đầu

media sanitization

Dịch: media sanitization

Giải thích: *quá trình xóa/khử dữ liệu trên thiết bị lưu trữ để không thể phục hồi — ví dụ: wipe, degauss, physical destruction.*

Ví dụ: Là quy trình mang tính phòng thủ, đảm bảo dữ liệu trên các thiết bị lưu trữ cũ (ổ cứng, USB) bị xóa vĩnh viễn và không thể phục hồi trước khi thải loại thiết bị.

↑ Lên đầu

Medusa and Ncrack

Dịch: Medusa, Ncrack

Giải thích: *tool tấn công mật khẩu mạnh mẽ, đa giao thức.*

Ví dụ: Quản trị viên sử dụng Ncrack để kiểm tra xem có bất kỳ thiết bị nào trong mạng của họ đang sử dụng mật khẩu mặc định hay không.

↑ Lên đầu

Metadata service attacks (cloud metadata attacks / IMDS abuse)

Dịch: Tấn công dịch vụ metadata

Giải thích: *Tấn công lợi dụng instance metadata service (IMDS) trên VM Cloud để lấy IAM credentials hoặc metadata nhạy cảm — thường qua SSRF hoặc lạm dụng cấu hình IMDS cũ. Phòng thủ: dùng IMDSv2, hạn chế quyền IAM instance, validate/patch ứng dụng.*

Ví dụ: Hacker lợi dụng lỗ hổng SSRF trong ứng dụng web trên AWS EC2 để truy cập metadata service và lấy IAM token.

Xem thêm: Cloud

↑ Lên đầu

Metagoofil

Dịch: Metagoofil

Giải thích: *OSINT tool trích xuất metadata từ tài liệu công khai.*

Ví dụ: Pentester sử dụng Metagoofil để tìm kiếm các tên người dùng và đường dẫn mạng nội bộ bị rò rỉ trong các tài liệu trên website của công ty.

↑ Lên đầu

Metasploit

Dịch: Metasploit

Giải thích: *framework khai thác/exploit phổ biến cho pentest — modules, payload, post-exploit.*

Ví dụ: Pentester sử dụng Metasploit để chạy exploit EternalBlue, tự động tấn công và nhận về một phiên Meterpreter.

↑ Lên đầu

Metasploit

Dịch: Metasploit

Giải thích: *framework khai thác/exploit phổ biến cho pentest — chứa modules, payloads như Meterpreter*

Ví dụ: Pentester sử dụng Metasploit để chạy exploit EternalBlue, tự động tấn công và nhận về một phiên Meterpreter.

↑ Lên đầu

Metasploit

Dịch: Framework Metasploit

Giải thích: *Khung công cụ phổ biến để kiểm thử xâm nhập (penetration testing), khai thác lỗ hổng, tạo payload và mô phỏng tấn công. Dùng bởi chuyên gia bảo mật để kiểm thử hoặc bởi attacker nếu bị lạm dụng.*

Ví dụ: Dùng lệnh msfconsole → use exploit/windows/smb/ms17_010_eternalblue để khai thác lỗ hổng SMB.

↑ Lên đầu

Metasploit framework

Dịch: Metasploit framework

Giải thích: *khung khai thác/phát triển exploit và payload phổ biến cho pentest.*

Ví dụ: Pentester dùng Metasploit (msfconsole) để chạy exploit EternalBlue, tự động tấn công và nhận về một phiên Meterpreter.

↑ Lên đầu

Meterpreter commands (see table in 8.1.2)

Dịch: các lệnh Meterpreter

Giải thích: *tập lệnh/lệnh dùng để tương tác với phiên Meterpreter.*

Ví dụ: Trong phiên Meterpreter, attacker dùng lệnh migrate để di chuyển tiến trình của mình vào explorer.exe nhằm ẩn mình và duy trì truy cập.

↑ Lên đầu

Meterpreter module

Dịch: Meterpreter module

Giải thích: *mô-đun/agent Meterpreter trong Metasploit — payload tương tác mạnh để điều khiển hệ thống.*

Ví dụ: Sau khi có phiên Meterpreter, attacker chạy lệnh screenshot để chụp màn hình desktop của nạn nhân, hoặc hashdump để lấy mật khẩu.

Xem thêm: Metasploit

↑ Lên đầu

Microsoft's Remote Desktop Protocol (RDP)

Dịch: RDP

Giải thích: *giao th?c di?u khi?n máy tính t? xa c?a Microsoft.*

Ví dụ: Attacker quét và tìm thấy một server có cổng 3389 (RDP) đang mở. Chúng tiến hành dò mật khẩu quản trị viên cho đến khi thành công và chiếm được toàn quyền điều khiển server.

↑ Lên đầu

Mimikatz

Dịch: Mimikatz (công cụ trích xuất thông tin chứng thực)

Giải thích: *Công cụ mạnh để trích xuất credential (hash, plaintext, ticket Kerberos) từ bộ nhớ Windows, dump LSASS, và thao tác token. Dùng trong kiểm thử xâm nhập/Forensics; nếu bị lạm dụng thì dẫn tới đánh cắp credential.*

Ví dụ: Trong lab/hợp pháp, pentester dùng Mimikatz để minh họa rò rỉ credential sau khi có local admin.

Xem thêm: Forensics, Kerberos

↑ Lên đầu

Mimikatz

Dịch: Mimikatz

Giải thích: *tool khai thác credentials Windows — hash, token, plain text passwords.*

Ví dụ: Sau khi có quyền admin, attacker chạy Mimikatz với lệnh sekurlsa::logonpasswords để lấy toàn bộ mật khẩu dưới dạng chữ rõ (plaintext) từ bộ nhớ.

↑ Lên đầu

Mimikatz

Dịch: Mimikatz

Giải thích: *công cụ trích xuất credential trên Windows — lấy mật khẩu, hash, ticket Kerberos…*

Ví dụ: Là công cụ huyền thoại" để đánh cắp thông tin xác thực (credentials) trên Windows. Đây là thứ đầu tiên attacker sẽ chạy sau khi có được quyền admin trên một máy tính."

Xem thêm: Kerberos

↑ Lên đầu

msfconsole

Dịch: msfconsole

Giải thích: *giao diện dòng lệnh chính của Metasploit Framework, dùng để triển khai exploit, payload, module tấn công*

Ví dụ: Sau khi xác định máy chủ chạy Windows 7 và dính lỗi MS17-010, pentester đã khởi chạy msfconsole, use" (sử dụng) mô-đun "eternalblue" và "exploit" (khai thác) thành công để có được Shell."

Xem thêm: Metasploit, Metasploit framework

↑ Lên đầu

multifactor authentication

Dịch: xác thực đa yếu tố

Giải thích: *MFA — kết hợp mật khẩu + OTP/biometric/token*

Ví dụ: Để đăng nhập vào email, nhân viên phải nhập mật khẩu và sau đó nhập một mã OTP gồm 6 chữ số từ ứng dụng trên điện thoại. Đó là MFA.

↑ Lên đầu

Mutiny Fuzzing Framework

Dịch: Mutiny Fuzzing Framework

Giải thích: *framework Fuzzing nâng cao*

Ví dụ: Mutiny Fuzzing Framework được sử dụng để tìm kiếm các lỗ hổng trong việc triển khai giao thức TLS của một máy chủ.

Xem thêm: Fuzzing

↑ Lên đầu

National Institute of Standards and Technology (NIST)

Dịch: Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST)

Giải thích: *Tổ chức ban hành tiêu chuẩn và hướng dẫn về an ninh, mật mã và quản trị rủi ro.*

Ví dụ: Công ty chúng tôi đang áp dụng Khung an ninh mạng (Cybersecurity Framework) của NIST để xây dựng, đánh giá và cải thiện chương trình bảo mật của mình.

↑ Lên đầu

National Institute of Standards and Technology (NIST)

Dịch: Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST)

Giải thích: *ban hành tiêu chuẩn, hướng dẫn về an ninh, mật mã, quản trị rủi ro*

Ví dụ: Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) là nơi ban hành Khung An ninh mạng (Cybersecurity Framework) mà rất nhiều tổ chức trên thế giới áp dụng.

↑ Lên đầu

NBNSpoof

Dịch: NBNSpoof (mạo danh NetBIOS Name Service)

Giải thích: *Kỹ thuật/tập lệnh dùng để giả mạo phản hồi NetBIOS-NS, khiến máy nạn nhân tin rằng một tên máy trỏ tới địa chỉ IP của attacker — thường*

dùng trong tấn công MITM (man-in-the-middle) trên LAN.

Ví dụ: Kẻ tấn công chạy công cụ Responder trong mạng LAN; khi máy nạn nhân hỏi “Ai là FILESERVER?”, Responder trả lời “Tôi!” → nạn nhân gửi thông tin đăng nhập cho attacker.

↑ Lên đầu

Nessus

Dịch: Nessus

Giải thích: *trình quét lỗ hổng thương mại/phổ biến*

Ví dụ: Một công ty thuê đội pentest bên ngoài, và họ sử dụng Nessus để thực hiện bước quét lỗ hổng ban đầu.

↑ Lên đầu

NetBIOS Name Service (NetBIOS-NS)

Dịch: Dịch vụ tên NetBIOS (NetBIOS-NS)

Giải thích: *Thành phần NetBIOS chịu trách nhiệm đăng ký và phân giải tên NetBIOS (tên máy) trong LAN. Dùng để tìm địa chỉ IP tương ứng tên NetBIOS; nếu bị giả mạo có thể dẫn đến chuyển hướng lưu lượng.*

Ví dụ: Khi máy A gửi yêu cầu “Tên PC-SERVER có IP là gì?”, NetBIOS-NS sẽ trả lời IP tương ứng. Hoặc Hacker có thể giả mạo phản hồi này (NBNSpoof) khiến máy A tin rằng PC-SERVER = 192.168.1.100 (máy attacker).

↑ Lên đầu

Netcat commands (see table in 8.1.2)

Dịch: các lệnh Netcat

Giải thích: *Netcat — tiện ích đọc/ghi qua kết nối mạng, dùng mở Shell, chuyển port, tunneling.*

Ví dụ: Để truyền file, attacker chạy nc -lvp 1234 > received_file trên máy mình và nc 1234 < secret_file trên máy nạn nhân.

Xem thêm: Shell

↑ Lên đầu

Network Basic Input/Output System (NetBIOS)

Dịch: Hệ thống I/O Cơ bản Mạng (NetBIOS)

Giải thích: *Giao diện API cũ để ứng dụng trên mạng cục bộ (LAN) thực hiện đặt tên, phiên và gửi datagram trên mạng NetBIOS. Thường xuất hiện trong mạng Windows cũ; có thể bị lợi dụng để thu thập tên máy, chia sẻ tài nguyên.*

Ví dụ: Trong mạng nội bộ Windows cũ, khi bạn mở File Sharing (\COMPUTER-NAME\C$), Windows dùng NetBIOS để tìm máy tính có tên đó

↑ Lên đầu

network segmentation

Dịch: phân đoạn mạng

Giải thích: *tách mạng thành vùng để giới hạn truy cập và di chuyển ngang*

Ví dụ: Công ty thực hiện Network Segmentation bằng cách tạo ra các VLAN riêng biệt cho mạng Wi-Fi khách, mạng nhân viên và mạng máy chủ.

↑ Lên đầu

network segmentation

Dịch: network segmentation

Giải thích: *phân đoạn mạng — biện pháp phòng thủ tách mạng thành các vùng để giới hạn di chuyển ngang.*

Ví dụ: Là một biện pháp phòng thủ cốt lõi để ngăn chặn hoặc làm chậm quá trình di chuyển ngang của attacker. Mạng được chia thành nhiều vùng nhỏ và có các quy tắc tường lửa kiểm soát giao tiếp giữa các vùng.

↑ Lên đầu

Network share enumeration

Dịch: liệt kê chia sẻ mạng

Giải thích: *tìm kiếm các thư mục hoặc tài nguyên được chia sẻ qua mạng*

Ví dụ: Sử dụng công cụ smbclient, pentester đã thực hiện Network share enumeration và phát hiện ra một ổ đĩa chia sẻ tên KeToan" bị mở "public" cho mọi người."

↑ Lên đầu

New Technology LAN Manager (NTLM)

Dịch: NT LAN Manager (NTLM)

Giải thích: *Cơ chế xác thực cũ của Microsoft (challenge-response) dùng hash mật khẩu; dùng trong môi trường Windows legacy. Có nhiều vấn đề bảo mật (có thể bị relay, brute-force hoặc lộ hash), vì vậy Kerberos được khuyến nghị trong domain hiện đại.*

Ví dụ: Khi người dùng đăng nhập SMB hoặc RDP, Windows gửi NTLM hash.

Xem thêm: Kerberos

↑ Lên đầu

Nexpose

Dịch: Nexpose

Giải thích: *vulnerability scanner — Rapid7*

Ví dụ: Đội ngũ an ninh sử dụng Nexpose để theo dõi và quản lý vòng đời của các lỗ hổng trong toàn bộ tổ chức.

↑ Lên đầu

Nikto

Dịch: Nikto

Giải thích: *web server scanner tìm lỗ hổng và cấu hình sai*

Ví dụ: Pentester chạy Nikto trên một địa chỉ IP để nhanh chóng kiểm tra xem máy chủ web có các lỗ hổng phổ biến hay không.

↑ Lên đầu

Nikto

Dịch: Nikto

Giải thích: *trình quét máy chủ web mã nguồn mở phát hiện file/cấu hình không an toàn và lỗ hổng web server phổ biến*

Ví dụ: Chạy Nikto chống lại máy chủ web của mục tiêu đã nhanh chóng phát hiện ra rằng máy chủ này đang chạy một phiên bản Apache cũ và có thư mục /cgi-bin/ đang bị mở.

↑ Lên đầu

NIST SP 800-115

Dịch: NIST SP 800-115

Giải thích: *Ấn phẩm đặc biệt của NIST hướng dẫn kỹ thuật kiểm thử bảo mật và pentesting.*

Ví dụ: Khi lập kế hoạch cho một cuộc pentest, người quản lý đã tham khảo tài liệu NIST SP 800-115 để đảm bảo tuân thủ đúng các phương pháp luận kỹ thuật về kiểm thử và đánh giá bảo mật.

↑ Lên đầu

Nmap

Dịch: Network Mapper (Nmap)

Giải thích: *Công cụ quét mạng để khám phá host, cổng, dịch vụ, hệ điều hành; dùng cho khảo sát mạng (Reconnaissance) trong cả quản trị mạng và kiểm thử bảo mật.*

Ví dụ: nmap -sS 192.168.1.0/24 → quét SYN các cổng mở trong mạng LAN.

Xem thêm: host, Reconnaissance

↑ Lên đầu

Nmap Scripting Engine (NSE)

Dịch: Công cụ script của Nmap (NSE)

Giải thích: *Khung mở rộng cho Nmap cho phép chạy scripts để thực hiện tác vụ nâng cao (vuln detection, brute-force, dịch vụ fingerprinting, v.v.). Giúp tự động hóa các kiểm tra chi tiết khi quét mạng.*

Ví dụ: nmap --script smb-vuln* -p 445 192.168.1.0/24 để tìm các lỗ hổng SMB trong mạng.

Xem thêm: Nmap

↑ Lên đầu

non-disclosure agreement (NDA)

Dịch: thỏa thuận bảo mật thông tin (NDA)

Giải thích: *hợp đồng cam kết không tiết lộ thông tin mật giữa các bên*

Ví dụ: Trước khi bắt đầu cuộc họp về sản phẩm mới, tất cả mọi người tham dự đều phải ký thỏa thuận bảo mật thông tin (NDA).

↑ Lên đầu

nslookup

Dịch: nslookup

Giải thích: *tool dòng lệnh tra cứu bản ghi DNS*

Ví dụ: Pentester sử dụng nslookup example.com để nhanh chóng tìm ra địa chỉ IP của website mục tiêu.

↑ Lên đầu

nslookup command

Dịch: lệnh nslookup

Giải thích: *công cụ dòng lệnh để truy vấn DNS và phân giải tên miền*

Ví dụ: Tôi dùng lệnh nslookup google.com để xem các địa chỉ IP (bản ghi A) tương ứng với tên miền đó.

↑ Lên đầu

Nyeta

Dịch: Nyeta

Giải thích: *giữ nguyên tên — lưu ý: có thể bạn muốn nói Nyetya / NotPetya" (ransomware/wiper nổi tiếng) — nếu đúng thì sửa lại."*

Ví dụ: Đây là một loại mã độc hủy diệt (wiper), giả dạng làm mã độc tống tiền (ransomware) nhưng mục tiêu chính là phá hủy dữ liệu và làm tê liệt hệ thống vĩnh viễn.

↑ Lên đầu

Objdump

Dịch: Objdump

Giải thích: *tool dòng lệnh phân tích nhị phân — disassembly, sections, symbols.*

Ví dụ: Một lập trình viên sử dụng objdump -d để xem mã assembly của chương trình C mà họ vừa biên dịch.

↑ Lên đầu

Object Exchange (OBEX) protocol

Dịch: Giao thức Object Exchange (OBEX)

Giải thích: *Giao thức cấp phép truyền đối tượng (file, vCard) qua Bluetooth/IrDA; được dùng bởi dịch vụ OBEX FTP/Push. Nếu cấu hình/mapping kém, có thể bị lạm dụng để transfer file không mong muốn.*

Ví dụ: Một thiết bị bật dịch vụ OBEX FTP mà không yêu cầu xác thực → attacker có thể gửi file độc hại qua Bluetooth mà người dùng không biết.

↑ Lên đầu

offensive security

Dịch: an ninh chủ động

Giải thích: *hoạt động tấn công mô phỏng — red team, pentest, exploit dev*

Ví dụ: Pentest và phát triển exploit là những hoạt động cốt lõi của Offensive Security.

Xem thêm: red team

↑ Lên đầu

OllyDbg

Dịch: OllyDbg

Giải thích: *debugger mã nhị phân Windows — phân tích malware, reverse engineering.*

Ví dụ: Một nhà phân tích mã độc sử dụng OllyDbg để theo dõi từng bước thực thi của một file virus.

↑ Lên đầu

On-Path attack

Dịch: Tấn công trên đường truyền (On-Path)

Giải thích: *Thuật chung cho các tấn công nơi attacker nằm trên con đường truyền giữa hai endpoints và có thể đọc/chỉnh sửa/chuyển tiếp traffic (tương tự MITM nhưng nhấn mạnh vị trí của attacker).*

Ví dụ: Attacker kiểm soát router trung gian và chặn/đổi nội dung HTTP.

↑ Lên đầu

Online Certificate Status Protocol (OCSP)

Dịch: Giao thức trạng thái chứng chỉ trực tuyến (OCSP)

Giải thích: *cơ chế kiểm tra nhanh trạng thái thu hồi của chứng chỉ TLS*

Ví dụ: Khi bạn truy cập một trang web HTTPS, trình duyệt sẽ gửi một yêu cầu Giao thức trạng thái chứng chỉ trực tuyến (OCSP) đến CA để kiểm tra nhanh xem chứng chỉ của trang đó có còn hợp lệ hay không.

↑ Lên đầu

Open (OPN)

Dịch: Mở (không có bảo mật — Open)

Giải thích: *Mạng Wi-Fi không yêu cầu mật khẩu (không mã hóa); phù hợp cho mạng công cộng nhưng rất rủi ro vì traffic không được mã hóa bên link layer.*

Ví dụ: Wi-Fi “Airport_Free_WiFi” là mạng mở, không có mã hóa, nên attacker có thể dễ dàng sniff traffic HTTP.

↑ Lên đầu

Open Security Content Automation Protocol (SCAP)

Dịch: SCAP

Giải thích: *chuẩn/khung tự động hóa quét & đánh giá cấu hình, lỗ hổng, compliance*

Ví dụ: Một tổ chức chính phủ sử dụng một công cụ tương thích SCAP để xác minh rằng các máy chủ của họ tuân thủ các hướng dẫn bảo mật bắt buộc.

↑ Lên đầu

Open Web Application Security Project (OWASP)

Dịch: Open Web Application Security Project (OWASP)

Giải thích:

Ví dụ: Lập trình viên sử dụng danh sách OWASP Top 10 làm kim chỉ nam để tránh các lỗi bảo mật web phổ biến khi viết code.

↑ Lên đầu

Open Web Application Security Project (OWASP)

Dịch: OWASP

Giải thích: *Dự án mã nguồn mở về bảo mật ứng dụng web, nổi tiếng với bộ OWASP Top 10.*

Ví dụ: Nhóm phát triển phần mềm được đào tạo về OWASP Top 10 để họ có thể viết mã nguồn an toàn hơn, đặc biệt là cách phòng chống lỗi A01: Broken

Access Control" (Kiểm soát truy cập bị hỏng)."

↑ Lên đầu

open-source intelligence (OSINT)

Dịch: tình báo nguồn mở (OSINT)

Giải thích: *thu thập thông tin từ nguồn công khai như social media, DNS, whois*

Ví dụ: Toàn bộ quá trình sử dụng Google, Shodan, và a Harvester để thu thập thông tin được gọi chung là OSINT.

Xem thêm: whois

↑ Lên đầu

OpenStego

Dịch: OpenStego

Giải thích: *tool Steganography — giấu dữ liệu trong ảnh.*

Ví dụ: Một người dùng sử dụng OpenStego để ẩn một tài liệu văn bản quan trọng vào bên trong một bức ảnh trước khi gửi nó qua email.

Xem thêm: Steganography

↑ Lên đầu

OpenVAS

Dịch: OpenVAS

Giải thích: *open-source vulnerability scanner*

Ví dụ: Quản trị viên hệ thống thiết lập OpenVAS để thực hiện quét lỗ hổng hàng tuần trên toàn bộ mạng nội bộ.

↑ Lên đầu

operational control

Dịch: biện pháp kiểm soát vận hành

Giải thích: *giám sát, backup, quản lý sự cố*

Ví dụ: Đội ngũ SOC thực hiện việc giám sát log hệ thống hàng ngày và quy trình sao lưu dữ liệu hàng tuần là các Operational Control.

↑ Lên đầu

OWASP Software Assurance Maturity Model (SAMM)

Dịch: OWASP SAMM

Giải thích: *framework/khung đánh giá độ chín chắn an ninh phần mềm theo các hoạt động tổ chức*

Ví dụ: Công ty sử dụng OWASP SAMM để tự đánh giá hiện trạng và xây dựng một lộ trình cải thiện an ninh phần mềm trong ba năm tới.

↑ Lên đầu

OWASP Zed Attack Proxy (ZAP)

Dịch: OWASP ZAP

Giải thích: *DAST proxy/tool để test bảo mật ứng dụng web*

Ví dụ: Một chuyên gia bảo mật sử dụng OWASP ZAP để tự động quét ứng dụng web của họ nhằm tìm kiếm các lỗ hổng như XSS và SQL Injection.

↑ Lên đầu

PaaS (Platform as a Service)

Dịch: Nền tảng như một dịch vụ (PaaS)

Giải thích: *Cung cấp nền tảng (runtime, middleware) để triển khai ứng dụng (ví dụ App Engine). Giảm gánh nặng quản trị infra; người dùng focus code. Rủi ro: lộ config/app secrets, supply-chain libraries. Phòng thủ: secret management, dependency scanning, least privilege.*

Ví dụ: Developer triển khai ứng dụng Node.js lên Google App Engine mà không cần quản lý server.

↑ Lên đầu

packet inspection

Dịch: kiểm tra gói tin

Giải thích: *phân tích header/nội dung gói mạng — cơ bản hoặc Deep Packet Inspection' class='in-link'>Packet Inspection*

Ví dụ: Hệ thống IPS (Intrusion Prevention System) thực hiện packet inspection trên toàn bộ lưu lượng truy cập vào để tìm kiếm các dấu hiệu (signatures) của mã độc.

Xem thêm: packet inspection, Packet Inspection

↑ Lên đầu

Packet Inspection

Dịch: kiểm tra gói tin

Giải thích: *phân tích nội dung header/payload của gói mạng — có thể là basic hoặc Deep Packet Inspection' class='in-link'>Packet Inspection*

Ví dụ: Tường lửa thế hệ mới (NGFW) đã thực hiện kiểm tra gói tin (Packet Inspection) sâu (Deep Packet Inspection) để phát hiện và chặn lưu lượng truy cập của BitTorrent, ngay cả khi nó chạy trên cổng 80.

Xem thêm: packet inspection, Packet Inspection

↑ Lên đầu

packet storm (broadcast storm)

Dịch: Bão gói tin (broadcast storm)

Giải thích: *Tình trạng lưu lượng broadcast hoặc multicast tăng vọt trong mạng (do loop, misconfig, hoặc tấn công) dẫn tới tắc nghẽn băng thông, làm chậm hoặc ngắt toàn bộ mạng layer 2.*

Ví dụ: Do loop giữa hai switch không có STP, dẫn tới tăng dồn broadcast và mạng bị nghẽn.

↑ Lên đầu

packetforge-ng command

Dịch: Lệnh packetforge-ng (Aircrack-ng suite)

Giải thích: *Tiện ích tạo packet Wi-Fi tùy chỉnh (ví dụ deauth, ARP, fake packets) để replay/inject trong bài kiểm thử; hữu ích để tạo lưu lượng mẫu cho cracking hoặc kiểm tra AP.*

Ví dụ: Pentester dùng packetforge-ng -0 -a -h -k 255.255.255.255 -l 255.255.255.255 -y keystream.xor -w arp-request để tạo ARP packet giả để replay và tăng tốc cracking WEP.

↑ Lên đầu

Pacu

Dịch: Pacu

Giải thích: *AWS exploitation framework — pentest Cloud.*

Ví dụ: Sau khi có được một bộ khóa API của AWS, pentester sử dụng Pacu để tự động thực hiện các kỹ thuật leo thang đặc quyền và khai thác các dịch vụ khác.

Xem thêm: Cloud

↑ Lên đầu

PALADIN

Dịch: PALADIN

Giải thích: *forensic live CD — môi trường pháp y trực tiếp*

Ví dụ: Một kỹ thuật viên sử dụng PALADIN để tạo một bản sao pháp y (forensic image) của một ổ đĩa mà không làm thay đổi dữ liệu gốc.

↑ Lên đầu

PAN (primary account number)

Dịch: số tài khoản chính (PAN)

Giải thích: *dãy số trên thẻ thanh toán, thường 14–19 chữ số*

Ví dụ: Quy định PCI DSS yêu cầu các doanh nghiệp phải mã hóa số tài khoản chính (PAN) khi lưu trữ để ngăn chặn hành vi trộm cắp thẻ.

↑ Lên đầu

Parrot OS

Dịch: Parrot OS

Giải thích: *Hệ điều hành Linux cho pentest, bảo mật, ẩn danh và pháp y số, nhẹ hơn Kali.*

Ví dụ: Do cấu hình máy tính xách tay hơi yếu, pentester đã chọn cài Parrot OS vì nó nhẹ hơn Kali nhưng vẫn cung cấp đầy đủ các công cụ cần thiết cho công việc.

↑ Lên đầu

Parrot OS

Dịch: Parrot OS

Giải thích: *distro pentest/privacy-focused*

Ví dụ: Một pentester lựa chọn sử dụng Parrot OS vì nó nhẹ hơn và có giao diện thân thiện hơn cho công việc hàng ngày.

↑ Lên đầu

partially known environment test (gray-box)

Dịch: kiểm thử hộp xám

Giải thích: *Pentester chỉ biết một phần thông tin, mô phỏng attacker có kiến thức hạn chế hoặc insider.*

Ví dụ: Một cuộc kiểm thử hộp xám (gray-box) đã được thực hiện, trong đó pentester được cung cấp một tài khoản người dùng thường để mô phỏng một nhân viên có quyền truy cập cơ bản.

↑ Lên đầu

Pass-the-hash

Dịch: Pass-the-hash

Giải thích: *kỹ thuật dùng hash mật khẩu cắp được để xác thực ở các dịch vụ/má khác mà không cần cleartext password.*

Ví dụ: Là một kỹ thuật di chuyển ngang phổ biến trong môi trường Windows. Attacker không cần biết mật khẩu gốc, chỉ cần đánh cắp được bản hash của mật khẩu để dùng nó xác thực với các máy chủ khác.

↑ Lên đầu

Pass-the-Hash attack (PtH)

Dịch: Tấn công Truyền-hash" (Pass-the-Hash)"

Giải thích: *Kỹ thuật tấn công trên Windows domain nơi attacker sử dụng trực tiếp hash mật khẩu (thay vì plaintext) để xác thực tới dịch vụ/host khác (ví dụ SMB/NTLM) và di chuyển ngang trong mạng. Tấn công này lợi dụng việc hệ thống chấp nhận challenge-response dựa trên hash. Giảm rủi ro: dùng Kerberos, hạn chế reuse credentials, triển khai LM/NTLM hardening, bật SMB signing, tách quyền và dùng MFA.*

Ví dụ: Kẻ tấn công sử dụng hash NTLM để truy cập SMB của máy khác mà không cần mật khẩu.

Xem thêm: host, Kerberos

↑ Lên đầu

Passive reconnaissance

Dịch: trinh sát thụ động

Giải thích: *thu thập thông tin từ nguồn công khai, không tương tác trực tiếp với mục tiêu*

Ví dụ: Một pentester thực hiện Passive Reconnaissance bằng cách tìm kiếm thông tin về công ty trên Google, mạng xã hội, và các bản ghi DNS công khai.

↑ Lên đầu

Password dumps

Dịch: dump mật khẩu

Giải thích: *tập hợp dữ liệu tài khoản/mật khẩu bị rò rỉ hoặc trích xuất từ hệ thống, thường ở dạng file/DB*

Ví dụ: Kẻ tấn công đã tải xuống một tệp dump mật khẩu (Password dumps) từ một diễn đàn hacker và sử dụng nó để thực hiện tấn công credential stuffing" (thử mật khẩu) vào các dịch vụ khác."

↑ Lên đầu

Password Spraying attack

Dịch: Tấn công phun mật khẩu (Password Spraying)

Giải thích: *Kỹ thuật brute-force theo chiều rộng: attacker thử một số mật khẩu phổ biến trên nhiều tài khoản (thay vì thử nhiều mật khẩu trên một tài khoản) để tránh trigger khóa tài khoản. Hiệu quả khi nhiều tài khoản dùng mật khẩu yếu/common. Phòng thủ: áp dụng chính sách mật khẩu mạnh, rate-limiting, lockout thresholds, monitoring failed attempts, dùng MFA.*

Ví dụ: Attacker thử mật khẩu phổ biến “Winter2025!” trên hàng trăm tài khoản Office 365 công ty để tránh bị khóa tài khoản — và tìm thấy 1 tài khoản yếu.

↑ Lên đầu

Patator

Dịch: Patator

Giải thích: *tool brute-force da nang — FTP, SSH, SMB, HTTP…*

Ví dụ: Pentester sử dụng Patator để thực hiện một cuộc tấn công brute-force vào một trang đăng nhập có cơ chế bảo vệ chống brute-force phức tạp.

↑ Lên đầu

patch management

Dịch: quản lý bản vá

Giải thích: *quy trình phát hiện, thử nghiệm và triển khai patch cho OS/app*

Ví dụ: Công ty có chính sách Patch Management nghiêm ngặt, yêu cầu tất cả các bản vá an ninh nghiêm trọng phải được cài đặt trong vòng 72 giờ.

↑ Lên đầu

Payment Card Industry Data Security Standard (PCI DSS)

Dịch: Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS)

Giải thích: *bộ tiêu chuẩn bắt buộc để bảo vệ dữ liệu thẻ tín dụng và giao dịch tài chính*

Ví dụ: Bất kỳ công ty nào xử lý, lưu trữ, hoặc truyền tải dữ liệu thẻ tín dụng đều phải tuân thủ nghiêm ngặt Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) để tránh bị phạt nặng.

↑ Lên đầu

PCI Forensic Investigator (PFI)

Dịch: điều tra viên pháp y PCI (PFI)

Giải thích: *chuyên gia được PCI chứng nhận để điều tra sự cố vi phạm dữ liệu thẻ*

Ví dụ: Sau khi phát hiện bị tấn công và mất dữ liệu thẻ, ngân hàng đã lập tức thuê một điều tra viên pháp y PCI (PFI) để điều tra và xác định quy mô của vụ vi phạm.

↑ Lên đầu

Peach

Dịch: Peach

Giải thích: *framework Fuzzing để tìm lỗi bảo mật trên ứng dụng và giao thức*

Ví dụ: Một chuyên gia bảo mật sử dụng Peach Fuzzer để kiểm tra một giao thức mạng tùy chỉnh nhằm tìm kiếm các lỗ hổng tiềm ẩn.

Xem thêm: Fuzzing

↑ Lên đầu

Penetration Testing Execution Standard (PTES)

Dịch: PTES

Giải thích: *Chuẩn thực thi kiểm thử xâm nhập, mô tả các giai đoạn và quy trình của một bài pentest.*

Ví dụ: Tiêu chuẩn PTES định nghĩa rõ 7 giai đoạn của một cuộc pentest, trong đó giai đoạn Post Exploitation" (Hậu khai thác) là rất quan trọng để xác định rủi ro kinh doanh thực sự sau khi đã xâm nhập."

↑ Lên đầu

Perl

Dịch: Perl

Giải thích: *ngôn ngữ lập trình — ExifTool viết bằng Perl; hay dùng xử lý văn bản/metadata*

Ví dụ: Pentester sử dụng ExifTool (viết bằng Perl) để trích xuất metadata từ các file ảnh thu thập được.

Xem thêm: ExifTool, Perl

↑ Lên đầu

Persistence

Dịch: duy trì truy cập

Giải thích: *kỹ thuật giữ quyền kiểm soát sau khi xâm nhập*

Ví dụ: Để tạo Persistence, attacker tạo một Scheduled Task trên Windows để tự động chạy một reverse shell mỗi khi người dùng đăng nhập.

↑ Lên đầu

personal identifiable information (PII)

Dịch: thông tin định danh cá nhân (PII)

Giải thích: *dữ liệu có thể dùng để nhận diện cá nhân như tên, CMND, email, số điện thoại…*

Ví dụ: Theo luật GDPR, số Căn cước công dân, địa chỉ email, và số điện thoại đều được coi là thông tin định danh cá nhân (PII) và phải được bảo vệ nghiêm ngặt.

↑ Lên đầu

physical control

Dịch: biện pháp kiểm soát vật lý

Giải thích: *khóa, camera, thẻ từ, bảo vệ*

Ví dụ: Phòng máy chủ được bảo vệ bởi cửa khóa thẻ từ, camera giám sát và bảo vệ. Đây đều là các Physical Control.

↑ Lên đầu

Piggybacking

Dịch: piggybacking

Giải thích: *giống tailgating nhưng người có quyền cố ý hoặc bị lừa giữ cửa cho kẻ xâm nhập*

Ví dụ: Bằng cách piggybacking, kẻ mạo danh (impersonator) đã tay xách hai hộp cà phê lớn, lịch sự nhờ một nhân viên giữ cửa hộ, và nhân viên đó đã vô tình giúp kẻ tấn công đi qua khu vực kiểm soát.

↑ Lên đầu

pip3 install h8mail command

Dịch: lệnh pip3 install h8mail

Giải thích: *cài đặt công cụ h8mail để kiểm tra email bị lộ/rò rỉ qua các nguồn công khai*

Ví dụ: Để chuẩn bị cho giai đoạn OSINT, pentester đã gõ lệnh pip3 install h8mail vào terminal để cài đặt công cụ kiểm tra rò rỉ email.

↑ Lên đầu

Pivoting

Dịch: Pivoting

Giải thích: *kỹ thuật sử dụng máy bị chiếm làm điểm trung gian để truy cập/scan/tấn công đoạn mạng khác.*

Ví dụ: Dùng khi attacker đã chiếm được một máy tính và muốn tấn công các máy khác nằm sâu hơn trong mạng nội bộ mà không thể truy cập trực tiếp từ bên ngoài. Máy tính đã bị chiếm quyền được dùng làm bàn đạp"."

↑ Lên đầu

platform as a service (PaaS)

Dịch: nền tảng như một dịch vụ (PaaS)

Giải thích: *Mô hình cung cấp môi trường nền tảng như OS, middleware, DB để triển khai ứng dụng mà không cần quản lý hạ tầng.*

Ví dụ: Lập trình viên triển khai ứng dụng của họ lên Heroku, một dịch vụ nền tảng như một dịch vụ (PaaS), giúp họ không cần lo lắng về việc cài đặt hay cập nhật hệ điều hành.

↑ Lên đầu

POP3 (Post Office Protocol version 3)

Dịch: Giao thức POP3 (nhận mail)

Giải thích: *Giao thức truy xuất email từ mail server về mail client — thường tải thư về máy và (tuỳ cấu hình) xóa trên server. Dùng khi người dùng muốn lưu bản sao cục bộ.*

Ví dụ: Mail client cấu hình POP3 sẽ tải thư xuống máy và có thể xóa trên server.

↑ Lên đầu

PowerShell

Dịch: PowerShell

Giải thích: *Shell/kịch bản mạnh trên Windows — thường dùng cho post-exploit và fileless attacks*

Ví dụ: Attacker sử dụng một lệnh PowerShell để tải và thực thi mã độc trực tiếp trên bộ nhớ nhằm qua mặt các phần mềm diệt virus.

Xem thêm: Shell

↑ Lên đầu

PowerShell commands (see table in 8.2.3)

Dịch: các lệnh PowerShell

Giải thích: *các lệnh/kịch bản PowerShell — thường được dùng trong post-exploit, lateral movement, hoặc fileless attack.*

Ví dụ: Là công cụ chính cho các hoạt động hậu khai thác trên môi trường Windows hiện đại. Các lệnh PowerShell được dùng cho mọi thứ, từ thu thập thông tin, đánh cắp mật khẩu đến Lateral Movement.

Xem thêm: lateral movement, PowerShell

↑ Lên đầu

Preferred Network List (PNL)

Dịch: Danh sách mạng ưu tiên (PNL)

Giải thích: *Danh sách SSID mà thiết bị client lưu trữ và ưu tiên kết nối tự động. Lộ PNL có thể tiết lộ các mạng trước đây người dùng đã kết nối (ví dụ SSID công ty) và bị lợi dụng để dựng Evil Twin/rogue AP.*

Ví dụ: Điện thoại tự động tìm SSID “Café_WiFi” trong PNL, attacker dựng AP giả cùng tên để đánh lừa thiết bị.

↑ Lên đầu

primary contact

Dịch: liên hệ chính

Giải thích: *người chịu trách nhiệm chính liên hệ khi cần*

Ví dụ: Trong hợp đồng pentest, Giám đốc dự án phía khách hàng được chỉ định là Primary Contact.

↑ Lên đầu

Private cloud

Dịch: Đám mây riêng (Private cloud)

Giải thích: *Hạ tầng Cloud dành riêng cho một tổ chức (on-premise hoặc hosted). Ưu: kiểm soát, compliance; chi phí và vận hành cao hơn. Phòng thủ: tiêu chuẩn bảo mật on-prem, network controls, patching.*

Ví dụ: Một ngân hàng xây dựng hệ thống OpenStack nội bộ để lưu trữ dữ liệu khách hàng.

Xem thêm: Cloud

↑ Lên đầu

Privilege escalation

Dịch: Leo thang đặc quyền

Giải thích: *Hành vi hoặc exploit để tăng quyền từ thấp lên cao (ví dụ user -> admin). Là bước điển hình trong xâm nhập nội bộ để mở rộng quyền. Phòng thủ: patching, least privilege, EDR, privilege monitoring, use of immutable infrastructure.*

Ví dụ: Hacker khai thác lỗ hổng trong dịch vụ để nâng quyền từ người dùng thường lên quản trị viên.

↑ Lên đầu

process-level remediation

Dịch: khắc phục ở cấp tiến trình

Giải thích: *xử lý/đóng tiến trình bị xâm phạm, patch/process isolation, restart theo chính sách*

Ví dụ: Hệ thống EDR phát hiện một tiến trình đáng ngờ và tự động thực hiện Process-level Remediation bằng cách chấm dứt tiến trình đó và cách ly file thực thi.

↑ Lên đầu

Proxychains

Dịch: Proxychains

Giải thích: *tool định tuyến lưu lượng qua proxy để ẩn IP.*

Ví dụ: Pentester sử dụng Proxychains kết hợp với Nmap để quét mục tiêu thông qua mạng Tor, che giấu địa chỉ IP thật của mình.

↑ Lên đầu

PsExec

Dịch: PsExec

Giải thích: *tiện ích của Sysinternals cho remote command execution trên Windows — hay dùng để lateral movement.*

Ví dụ: Là một công cụ hợp pháp của Microsoft nhưng lại được attacker sử dụng cực kỳ phổ biến để thực hiện Lateral Movement trong mạng Windows.

Xem thêm: lateral movement, Sysinternals

↑ Lên đầu

Public cloud

Dịch: Đám mây công cộng

Giải thích: *Dịch vụ Cloud do bên thứ ba cung cấp cho nhiều khách hàng (shared infra). Ưu: tiết kiệm, scale. Rủi ro: tenant isolation, compliance. Phòng thủ: Encryption at rest/in transit, IAM, VPC, logging.*

Ví dụ: Sử dụng AWS S3 để lưu trữ file cho ứng dụng web.

Xem thêm: Cloud, Encryption

↑ Lên đầu

Pupy

Dịch: Pupy (remote RAT/framework)

Giải thích: *Remote administration/implant framework (RAT) đa nền tảng được dùng để điều khiển từ xa, thu thập thông tin, thực thi lệnh. Thường xuất hiện trong bối cảnh malware hoặc red-team engagements.*

Ví dụ: Hacker triển khai Pupy payload trên máy nạn nhân, mở kết nối ngược về máy chủ điều khiển (C2).

↑ Lên đầu

PwnDB

Dịch: PwnDB

Giải thích: *cơ sở dữ liệu/diễn đàn tập hợp thông tin về leak, dump tài khoản, credential breaches*

Ví dụ: Kẻ tấn công đã truy vấn cơ sở dữ liệu PwnDB và tìm thấy mật khẩu cũ (dưới dạng hash) của Giám đốc điều hành, vốn đã bị rò rỉ từ một diễn đàn khác.

↑ Lên đầu

Python

Dịch: Python

Giải thích: *ngôn ngữ lập trình phổ biến trong pentest để viết script, công cụ, exploit*

Ví dụ: Một nhà nghiên cứu bảo mật viết một exploit PoC bằng Python để kiểm thử một lỗ hổng vừa được phát hiện.

↑ Lên đầu

Quality Security Assessor (QSA)

Dịch: đánh giá viên bảo mật PCI (QSA)

Giải thích: *chuyên gia/công ty được PCI chứng nhận để đánh giá tuân thủ PCI DSS*

Ví dụ: Hàng năm, một đánh giá viên bảo mật PCI (QSA) sẽ đến công ty chúng tôi để kiểm toán toàn bộ hệ thống, nhằm xác nhận chúng tôi tuân thủ PCI DSS.

↑ Lên đầu

Qualys

Dịch: Qualys

Giải thích: *nền tảng quản lý lỗ hổng & compliance*

Ví dụ: Một tập đoàn lớn sử dụng nền tảng Qualys để đảm bảo tất cả các chi nhánh của họ trên toàn cầu đều tuân thủ chính sách bảo mật chung.

↑ Lên đầu

Radio-Frequency Identification (RFID) attack

Dịch: Tấn công RFID (giao tiếp sóng vô tuyến định danh)

Giải thích: *Các kỹ thuật khai thác giao tiếp RFID (e.g., Eavesdropping, replay, skimming) để đọc/giả mạo/biến đổi thông tin trên tag/thẻ không tiếp xúc (ví dụ thẻ cửa, thẻ transit, thanh toán). Hệ quả: lộ thông tin định danh, truy cập trái phép.*

Ví dụ: Kẻ tấn công dùng đầu đọc RFID 13.56 MHz đặt gần cửa văn phòng để thu thập tín hiệu từ thẻ nhân viên khi họ đi qua → sao chép để truy cập trái phép.

Xem thêm: Eavesdropping

↑ Lên đầu

RainbowCrack

Dịch: RainbowCrack

Giải thích: *tool crack mật khẩu bằng rainbow tables.*

Ví dụ: Pentester sử dụng RainbowCrack với một bộ rainbow tables đã được tính toán trước để bẻ khóa các hash LM của Windows.

↑ Lên đầu

RDP (Remote Desktop Protocol)

Dịch: RDP (Remote Desktop Protocol)

Giải thích: *giao thức/ứng dụng cho điều khiển từ xa Windows — thường là mục tiêu cho truy cập từ xa hoặc khai thác.*

Ví dụ: Là giao thức quản trị từ xa phổ biến nhất cho Windows. Nếu bị lộ ra Internet, nó trở thành mục tiêu hàng đầu cho các cuộc tấn công brute-force mật khẩu.

↑ Lên đầu

Reaver

Dịch: Reaver

Giải thích: *tool khai thác WPS PIN để truy cập mạng Wi-Fi*

Ví dụ: Pentester sử dụng Reaver để tấn công vào mã PIN của WPS và lấy được mật khẩu Wi-Fi trong vài giờ.

↑ Lên đầu

Recon-ng

Dịch: Recon-ng

Giải thích: *framework OSINT modular để thu thập và tổ chức thông tin trinh sát*

Ví dụ: Pentester sử dụng Recon-ng với các module khác nhau để tự động tìm kiếm subdomain, email, và các thông tin rò rỉ liên quan đến mục tiêu.

↑ Lên đầu

Reconnaissance

Dịch: trinh sát

Giải thích: *thu thập thông tin ban đầu về mục tiêu — host, domain, dịch vụ*

Ví dụ: Giai đoạn Reconnaissance bao gồm việc sử dụng các công cụ như whois, theHarvester và a Harvester để thu thập thông tin ban đầu.

Xem thêm: host

↑ Lên đầu

red team

Dịch: đội đỏ

Giải thích: *nhóm chuyên gia mô phỏng kẻ tấn công để kiểm tra khả năng phòng thủ của tổ chức*

Ví dụ: Đội đỏ (red team) đã thành công mô phỏng một cuộc tấn công APT, xâm nhập vào mạng và lấy được dữ liệu nhạy cảm mà không bị phát hiện.

↑ Lên đầu

reflected XSS

Dịch: XSS phản chiếu

Giải thích: *XSS khi script độc hại được phản hồi trực tiếp trong URL/tham số request, chỉ chạy khi nạn nhân click link.*

Ví dụ: Lỗ hổng XSS phản chiếu (reflected XSS) xảy ra khi kẻ tấn công gửi cho nạn nhân một đường link (.../search.php?q=), và đoạn mã độc được thực thi khi nạn nhân nhấp vào link đó.

↑ Lên đầu

Resource exhaustion

Dịch: Cạn kiệt tài nguyên

Giải thích: *Loại tấn công làm tiêu thụ CPU, RAM, file-descriptors, connection pool… khiến service chậm hoặc sập — dạng con của DoS. Phòng thủ: throttling, quotas, circuit breakers, proper input validation.*

Ví dụ: Script gửi liên tục 1 triệu request khiến web server bị treo do đầy connection pool.

↑ Lên đầu

Responder

Dịch: Công cụ Responder

Giải thích: *Tool thu thập và mạo danh nhiều giao thức mạng cục bộ (LLMNR, NBT-NS, MDNS, HTTP, SMB...) để bắt và thu credential hash hoặc khuyến dụ hệ thống kết nối tới attacker. Thường dùng trong kiểm thử nội bộ để phát hiện rủi ro.*

Ví dụ: Chạy responder -I eth0 để bắt các hash NTLM từ máy trong LAN.

↑ Lên đầu

RESTful API

Dịch: API RESTful

Giải thích: *Kiến trúc/chuẩn giao tiếp web dùng HTTP để thao tác tài nguyên — GET/POST/PUT/DELETE, phổ biến trong dịch vụ web.*

Ví dụ: Hầu hết các ứng dụng di động hiện đại đều sử dụng RESTful API để giao tiếp với máy chủ, ví dụ như gửi một yêu cầu GET đến /api/users/123 để lấy thông tin người dùng.

↑ Lên đầu

Return on Investment (ROI)

Dịch: lợi tức đầu tư (ROI)

Giải thích: *chỉ số đo lường hiệu quả lợi nhuận so với chi phí đầu tư*

Ví dụ: Việc đầu tư vào hệ thống tường lửa mới đã mang lại lợi tức đầu tư (ROI) cao, vì nó giúp công ty tiết kiệm được hàng tỷ đồng chi phí khắc phục sự cố sau một cuộc tấn công ransomware.

↑ Lên đầu

reverse shell

Dịch: reverse shell

Giải thích: *máy mục tiêu kết nối ngược tới attacker, cung cấp phiên dòng lệnh cho attacker.*

Ví dụ: Attacker chạy lệnh nc -lvp 4444 trên máy mình để lắng nghe. Payload trên máy nạn nhân sẽ thực thi lệnh kết nối đến IP của attacker tại cổng 4444.

↑ Lên đầu

RFID cloning

Dịch: Sao chép thẻ/tag RFID (RFID cloning)

Giải thích: *Tạo bản sao thẻ RFID hợp lệ bằng cách đọc dữ liệu từ thẻ gốc và ghi vào thẻ rỗng/emulator. Dùng để vượt kiểm soát truy cập vật lý (door access, turnstile). Phòng thủ: dùng thẻ có bảo mật mạnh (challenge-response, key diversification), patch reader để phát hiện duplicate, kiểm soát vật lý, logging/alarms.*

Ví dụ: Attacker đọc dữ liệu từ thẻ ra vào tòa nhà (MIFARE Classic) rồi ghi lại vào thẻ trắng → mở được cửa giống thẻ gốc.

↑ Lên đầu

Risk acceptance

Dịch: thụ động chấp nhận rủi ro

Giải thích: *quyết định không áp dụng biện pháp kiểm soát mà chấp nhận hậu quả tiềm tàng*

Ví dụ: Sau khi phân tích, ban giám đốc quyết định chấp nhận rủi ro (Risk acceptance) đối với lỗ hổng Tự động hoàn thành mật khẩu" (Password autocomplete) vì chi phí sửa chữa cao hơn tác động tiềm ẩn của nó."

↑ Lên đầu

Risk assessment

Dịch: đánh giá rủi ro

Giải thích: *quá trình phân tích mối đe dọa, điểm yếu và xác suất để xác định mức độ rủi ro*

Ví dụ: Một bài đánh giá rủi ro (Risk assessment) đã xác định rằng lỗ hổng SQL Injection trên máy chủ thanh toán là rủi ro Cực kỳ nghiêm trọng" (Critical) do nó có thể làm lộ dữ liệu thẻ tín dụng."

↑ Lên đầu

Risk management

Dịch: quản lý rủi ro

Giải thích: *quá trình nhận diện, đánh giá và xử lý rủi ro để giảm thiểu tác động tiêu cực*

Ví dụ: Quy trình quản lý rủi ro (Risk management) của chúng tôi yêu cầu phải quét lỗ hổng hàng quý và báo cáo các rủi ro nghiêm trọng trực tiếp cho CISO.

↑ Lên đầu

Risk-taking

Dịch: chủ động chấp nhận rủi ro

Giải thích: *hành động hoặc quyết định chủ động đối mặt rủi ro để đạt được mục tiêu/lợi ích*

Ví dụ: Việc công ty quyết định đưa máy chủ staging" ra ngoài Internet mà không có tường lửa là một hành động chấp nhận rủi ro (Risk-taking) nguy hiểm để đẩy nhanh tiến độ kiểm thử."

↑ Lên đầu

Rogue Access Point

Dịch: Access Point trái phép / giả mạo

Giải thích: *Thiết bị AP không được phép đặt trong mạng (do user hoặc attacker). Có thể dùng để lừa người dùng kết nối, thu thập traffic, phát tán malware.*

Ví dụ: Một nhân viên tự mang router cá nhân cắm vào cổng LAN công ty để dùng Wi-Fi riêng — tạo thành một AP trái phép.

↑ Lên đầu

Rogue access points

Dịch: điểm truy cập giả mạo

Giải thích: *mạng Wi-Fi giả mạo để đánh cắp dữ liệu hoặc redirect traffic.*

Ví dụ: Attacker thiết lập một Rogue Access Point có tên giống hệt mạng Wi-Fi của công ty để lừa nhân viên kết nối vào.

↑ Lên đầu

role-based access control (RBAC)

Dịch: kiểm soát truy cập dựa trên vai trò (RBAC)

Giải thích:

Ví dụ: Theo mô hình RBAC, nhân viên phòng kế toán chỉ có quyền truy cập vào các thư mục tài chính, không thể xem các thư mục của phòng nhân sự.

↑ Lên đầu

Ruby

Dịch: Ruby

Giải thích: *ngôn ngữ lập trình — nhiều module Metasploit viết bằng Ruby*

Ví dụ: Để tấn công một lỗ hổng mới, pentester tùy chỉnh một module có sẵn của Metasploit được viết bằng Ruby.

Xem thêm: Metasploit, Ruby

↑ Lên đầu

SaaS (Software as a Service)

Dịch: Phần mềm như một dịch vụ (SaaS)

Giải thích: *Ứng dụng được host bởi nhà cung cấp, người dùng dùng qua web (ví dụ Office365, Salesforce). Rủi ro: data residency, account compromise. Phòng thủ: SSO + MFA, DLP, audit logging, contractual SLAs.*

Ví dụ: Doanh nghiệp sử dụng Microsoft 365 hoặc Google Workspace qua trình duyệt.

Xem thêm: host

↑ Lên đầu

SCADA (Supervisory Control And Data Acquisition)

Dịch: Hệ thống giám sát & thu thập dữ liệu (SCADA)

Giải thích: *Kiểm soát và giám sát quá trình công nghiệp từ xa; thường kết hợp với ICS. Bảo vệ tương tự ICS: air-gapped patterns, strong authentication, anomaly detection.*

Ví dụ: Trung tâm điều hành lưới điện giám sát và điều khiển trạm biến áp từ xa qua hệ thống SCADA.

↑ Lên đầu

Scanners

Dịch: công cụ quét

Giải thích: *bao gồm vulnerability Scanners, port Scanners, web Scanners, v.v.*

Ví dụ: Một cuộc kiểm thử xâm nhập thường bắt đầu bằng việc sử dụng các Scanners khác nhau để thu thập thông tin về mục tiêu.

Xem thêm: Scanners

↑ Lên đầu

Scavenger

Dịch: Scavenger

Giải thích: *công cụ OSINT/breach-hunting thu thập & phân tích thông tin rò rỉ*

Ví dụ: Chuyên gia OSINT đã sử dụng Scavenger để tự động hóa việc rà soát các dịch vụ pastebin và các kho lưu trữ công cộng, tìm kiếm bất kỳ thông tin nào liên quan đến tên miền của khách hàng.

↑ Lên đầu

schtasks.exe command

Dịch: Lệnh schtasks.exe

Giải thích: *Tiện ích dòng lệnh Windows để lên lịch/quản lý tác vụ định kỳ (task scheduler). Dùng hợp pháp cho automation; cũng có thể bị lạm dụng trong post-exploitation để duy trì Persistence.*

Ví dụ: schtasks /Create /SC DAILY /TN Backup" /TR "backup.bat" /ST 02:00"

Xem thêm: Persistence

↑ Lên đầu

ScoutSuite / Scout Suite

Dịch: ScoutSuite

Giải thích: *tool đánh giá cấu hình bảo mật Cloud — AWS, Azure, GCP.*

Ví dụ: Một kỹ sư DevOps sử dụng ScoutSuite để kiểm tra môi trường đám mây của công ty và đảm bảo nó tuân thủ các thực hành tốt nhất về bảo mật.

Xem thêm: Cloud

↑ Lên đầu

SDK (Software Development Kit)

Dịch: Bộ công cụ phát triển phần mềm (SDK)

Giải thích: *Thư viện + công cụ giúp dev tích hợp dịch vụ/feature; rủi ro khi SDK bị compromise (supply-chain) hoặc lộ secret trong config.*

Ví dụ: Nhà phát triển tích hợp Facebook SDK để đăng nhập bằng Facebook; nếu SDK lỗi thời, có thể bị lộ token truy cập.

↑ Lên đầu

Searchsploit

Dịch: Searchsploit

Giải thích: *Lệnh CLI để tìm exploit/PoC trong cơ sở dữ liệu Exploit-DB offline; dùng trong thu thập PoC khi pentest.*

Ví dụ: Pentester dùng lệnh searchsploit vsftpd 2.3.4 để tìm mã khai thác có sẵn cho dịch vụ FTP mục tiêu.

↑ Lên đầu

Searchsploit

Dịch: Searchsploit

Giải thích: *tool tra cứu exploit từ Exploit-DB*

Ví dụ: Sau khi xác định một dịch vụ đang chạy phiên bản vsftpd 2.3.4, pentester dùng searchsploit vsftpd 2.3.4 để tìm exploit tương ứng.

↑ Lên đầu

searchsploit command

Dịch: Lệnh searchsploit (trong Exploit-DB local)

Giải thích: *Công cụ dòng lệnh để tìm các khai thác (exploit) và PoC từ cơ sở dữ liệu Exploit-DB offline trên máy local. Hữu ích cho penetration testers khi tra cứu lỗ hổng theo tên sản phẩm/CVE.*

Ví dụ: searchsploit vsftpd 2.3.4 → hiển thị khai thác backdoor command execution" có sẵn."

↑ Lên đầu

secrets management solution

Dịch: giải pháp quản lý bí mật

Giải thích: *vaults như HashiCorp Vault, Azure Key Vault — quản lý API keys, mật khẩu, token*

Ví dụ: Thay vì viết mật khẩu database vào file cấu hình, ứng dụng sẽ gọi tới một Secrets Management Solution để lấy mật khẩu khi cần.

↑ Lên đầu

Secure File Transfer Protocol (SFTP)

Dịch: Giao thức truyền tệp an toàn (SFTP)

Giải thích: *Giao thức truyền file hoạt động trên SSH (Secure Shell). Cung cấp kênh mã hóa và xác thực, thường an toàn hơn FTP/FTPS về mặt cấu trúc; phổ biến cho truyền file an toàn giữa server và client.*

Ví dụ: sftp user@server dùng để upload/download file qua SSH.

Xem thêm: Shell

↑ Lên đầu

Secure SMTP (SSMTP)

Dịch: SMTP đơn giản bảo mật (SSMTP)

Giải thích: *Thường dùng để chỉ việc gửi mail qua SMTP với cơ chế bảo mật (ví dụ TLS). Lưu ý: ssmtp" còn là tên một package/utility Linux (smaller MTA) dùng gửi mail từ máy chủ local ra SMTP relay — đã ít được dùng/không khuyến nghị trên hệ thống hiện đại."*

Ví dụ: Máy chủ dùng ssmtp để chuyển mail hệ thống tới SMTP relay với TLS.

↑ Lên đầu

Secure Sockets Layer (SSL)

Dịch: Secure Sockets Layer (SSL)

Giải thích: *giao thức mã hóa truyền tải — tiền thân TLS, hiện dùng chung cho TLS/SSL*

Ví dụ: Mặc dù thuật ngữ Secure Sockets Layer (SSL) vẫn được sử dụng phổ biến, nhưng trên thực tế, các máy chủ web hiện đại đều đã chuyển sang sử dụng giao thức TLS 1.3 an toàn hơn.

↑ Lên đầu

secure software development life cycle (SSDLC)

Dịch: vòng đời phát triển phần mềm an toàn (SSDLC)

Giải thích:

Ví dụ: Theo SSDLC, đội ngũ phát triển phải thực hiện phân tích mã tĩnh (SAST) và đánh giá các thư viện mã nguồn mở trước khi phát hành phiên bản

mới.

↑ Lên đầu

Security Onion

Dịch: Security Onion

Giải thích: *distro Linux cho IDS/NSM/forensic — giám sát an ninh mạng*

Ví dụ: Một quản trị viên mạng triển khai Security Onion để giám sát toàn bộ lưu lượng mạng và nhận cảnh báo về các hoạt động đáng ngờ.

↑ Lên đầu

sensitive data

Dịch: dữ liệu nhạy cảm

Giải thích: *thông tin giá trị — ví dụ PII, thông tin tài chính, khóa bí mật — mục tiêu chính để exfiltrate.*

Ví dụ: Đây chính là kho báu" mà attacker nhắm tới. Toàn bộ quá trình tấn công thường xoay quanh việc tìm kiếm và đánh cắp các loại dữ liệu này."

↑ Lên đầu

Server Message Block (SMB)

Dịch: Giao thức chia sẻ tệp/điều khiển phiên (SMB)

Giải thích: *Giao thức mạng (chủ yếu Windows) cho chia sẻ file, printer, RPC qua mạng. Phiên bản cũ (SMBv1) có nhiều lỗ hổng; SMB thường là mục tiêu lớn trong tấn công mạng nội bộ.*

Ví dụ: Truy cập \\SERVER\\Documents qua Windows Explorer → dùng SMB (TCP/445).

↑ Lên đầu

Service Set Identifier (SSID)

Dịch: SSID — Tên bộ dịch vụ / tên mạng Wi-Fi

Giải thích: *Tên nhận dạng mạng không dây hiển thị cho người dùng; client dùng SSID để chọn AP/ESS để kết nối.*

Ví dụ: Tên Wi-Fi hiển thị “FPT_Home_5GHz” chính là SSID mà người dùng chọn để kết nối.

↑ Lên đầu

service-level agreement (SLA)

Dịch: thỏa thuận mức dịch vụ (SLA)

Giải thích: *cam kết giữa nhà cung cấp dịch vụ và khách hàng về chất lượng, độ tin cậy và thời gian đáp ứng dịch vụ*

Ví dụ: Thỏa thuận mức dịch vụ (SLA) của chúng tôi cam kết thời gian uptime" (hoạt động) của máy chủ là 99.9% mỗi tháng."

↑ Lên đầu

Session Service (NetBIOS-SSN)

Dịch: Dịch vụ phiên NetBIOS (NetBIOS-SSN)

Giải thích: *Cung cấp kênh kết nối có trạng thái (session) giữa hai ứng dụng qua NetBIOS — dùng khi cần truyền dữ liệu đảm bảo thứ tự/đáng tin cậy (tương tự TCP).*

Ví dụ: Khi bạn mở \\SERVER\\SharedFolder, Windows tạo phiên NetBIOS giữa máy bạn và máy SERVER để truyền file qua TCP/139.

↑ Lên đầu

Shell

Dịch: Shell

Giải thích: *quyền truy cập/phiên dòng lệnh trên hệ thống mục tiêu — tức cửa sổ lệnh" mà attacker có thể dùng để chạy lệnh."*

Ví dụ: Sau khi khai thác một web server, attacker có được Shell và chạy lệnh whoami để kiểm tra danh tính người dùng hiện tại.

↑ Lên đầu

Shodan

Dịch: Shodan

Giải thích: *search engine cho thiết bị/dịch vụ kết nối Internet — tìm host/vulnerable services*

Ví dụ: Pentester sử dụng Shodan để tìm kiếm các máy chủ trong dải IP của mục tiêu đang mở cổng RDP (3389) và có lỗ hổng đã biết.

Xem thêm: host

↑ Lên đầu

Shoulder surfing

Dịch: nhìn trộm qua vai

Giải thích: *quan sát trực tiếp khi người khác nhập mật khẩu, PIN hoặc dữ liệu nhạy cảm*

Ví dụ: Kẻ gian đã sử dụng kỹ thuật nhìn trộm qua vai (shoulder surfing) tại một quán cà phê, lén nhìn và ghi nhớ được mật khẩu mà nạn nhân đang gõ trên máy tính xách tay.

↑ Lên đầu

Side-channel attack

Dịch: Tấn công side-channel

Giải thích: *Lấy thông tin nhạy cảm (key, dữ liệu) bằng cách quan sát thời gian xử lý, điện năng, cache behavior, electromagnetic emissions… Thường là tấn công trên phần cứng/crypto implementation. Phòng thủ: constant-time algorithms, noise, hardware mitigations.*

Ví dụ: Kẻ tấn công đo thời gian xử lý phép toán RSA để suy ra khóa bí mật (private key).

↑ Lên đầu

SIFT Workstation (SANS Investigative Forensic Toolkit) Workstation

Dịch: SIFT Workstation

Giải thích: *môi tru?ng forensic chu?n SANS d? phân tích máy tính, evidence, malware.*

Ví dụ: Một chuyên gia pháp y số sử dụng SIFT Workstation để thực hiện phân tích chi tiết bộ nhớ (RAM) của một máy tính bị nhiễm mã độc.

↑ Lên đầu

Simple Network Management Protocol version 3 (SNMPv3)

Dịch: Giao thức Quản lý Mạng đơn giản phiên bản 3 (SNMPv3)

Giải thích: *Phiên bản bảo mật hơn của SNMP — hỗ trợ xác thực (authentication) và mã hóa (privacy/Encryption) cho thông điệp quản lý. Nên dùng SNMPv3 trong môi trường cần bảo mật.*

Ví dụ: snmpwalk -v3 -u admin -a SHA -A password" -x AES -X "encryptionkey" 192.168.1.1"

Xem thêm: Encryption

↑ Lên đầu

Simple Object Access Protocol (SOAP)

Dịch: giao thức truy cập đối tượng đơn giản (SOAP)

Giải thích: *chuẩn giao tiếp dựa trên XML, dùng để trao đổi dữ liệu giữa các ứng dụng qua HTTP/HTTPS*

Ví dụ: API cũ của ngân hàng vẫn đang sử dụng Simple Object Access Protocol (SOAP), một giao thức hoạt động dựa trên các thông điệp XML phức tạp.

↑ Lên đầu

Skadi

Dịch: Skadi

Giải thích: *distro forensic / pentest, dùng để phân tích dữ liệu số*

Ví dụ: Một đội SOC sử dụng Skadi để phân tích log từ hàng nghìn thiết bị nhằm tìm kiếm các dấu hiệu của một cuộc tấn công.

↑ Lên đầu

SMTP over SSL (SMTPS)

Dịch: SMTP qua SSL/TLS (SMTPS)

Giải thích: *Giao thức SMTP bảo mật — kết nối SSL/TLS trực tiếp (ví dụ cổng 465) hoặc STARTTLS (nâng cấp từ plaintext -> TLS). Dùng để mã hóa truyền tải mail giữa client và server, bảo vệ credentials và nội dung.*

Ví dụ: Email client gửi mail qua port 465 với TLS/SSL.

↑ Lên đầu

smtp-user-enum command

Dịch: Lệnh smtp-user-enum

Giải thích: *Công cụ dùng để đi tìm tài khoản người dùng qua giao thức SMTP (thường bằng cách thử gửi lệnh VRFY/EXPN hoặc phân tích phản hồi khi gửi mail). Dùng trong thu thập thông tin/kiểm thử bảo mật; cần chú ý đạo đức và pháp lý — không dùng trái phép.*

Ví dụ: Dùng trên môi trường kiểm thử để xác định danh sách user có tồn tại trên mail server.

↑ Lên đầu

snmp-check command

Dịch: Lệnh snmp-check

Giải thích: *Công cụ dòng lệnh để liệt kê thông tin thu được từ dịch vụ SNMP (dùng community string) — ví dụ cấu hình, OID quan trọng, usernames, system info. Hữu ích cho kiểm thử bảo mật/khảo sát thiết bị; cần quyền truy cập SNMP.*

Ví dụ: snmp-check -c public 192.168.1.1 để liệt kê OID và thông tin thiết bị

↑ Lên đầu

snow

Dịch: snow

Giải thích: *tool Steganography/ẩn dữ liệu trong text hoặc media.*

Ví dụ: Attacker sử dụng snow để che giấu một thông điệp ngắn gọn trong một file văn bản có vẻ như vô hại.

Xem thêm: Steganography

↑ Lên đầu

socat

Dịch: socat

Giải thích: *tiện ích dòng lệnh mạnh tương tự netcat, dùng để forward socket, tunneling, proxy.*

Ví dụ: Attacker dùng socat để tạo một relay, chuyển tiếp lưu lượng từ một cổng trên máy A đến một cổng khác trên máy B, giúp kết nối vào một dịch vụ nằm sâu trong mạng.

↑ Lên đầu

Social engineering

Dịch: tấn công xã hội

Giải thích: *dùng thao tác tâm lý để lừa người dùng tiết lộ thông tin hoặc thực hiện hành động có hại*

Ví dụ: Kẻ tấn công đã sử dụng tấn công xã hội (social engineering) bằng cách gọi điện giả làm bộ phận IT, lừa nhân viên kế toán cung cấp mật khẩu của cô ấy.

↑ Lên đầu

Social-Engineer Toolkit (SET)

Dịch: Bộ công cụ Kỹ thuật Xã hội (SET)

Giải thích: *Framework để tạo/tự động hóa các cuộc tấn công social-engineering (phishing page, payload delivery, Credential harvesting). Dùng trong red-team/phishing simulations; cần dùng có đạo đức và pháp lý.*

Ví dụ: Trong lab pentest, chuyên viên dùng setoolkit tạo phishing page giả trang đăng nhập Office 365 để huấn luyện nhân viên nhận diện tấn công lừa đảo.

Xem thêm: Credential harvesting

↑ Lên đầu

software as a service (SaaS)

Dịch: phần mềm như một dịch vụ (SaaS)

Giải thích: *Mô hình cung cấp ứng dụng chạy trên Cloud, người dùng chỉ cần truy cập qua web/app.*

Ví dụ: Công ty sử dụng Microsoft 365, một dạng phần mềm như một dịch vụ (SaaS), nên việc bảo mật chủ yếu tập trung vào quản lý danh tính và cấu hình, thay vì vá lỗi máy chủ.

Xem thêm: Cloud

↑ Lên đầu

Software assurance

Dịch: đảm bảo phần mềm

Giải thích: *quy trình/khả năng đảm bảo phần mềm an toàn, giảm rủi ro bảo mật*

Ví dụ: Chương trình Software Assurance của công ty yêu cầu tất cả các lập trình viên phải tham gia khóa đào tạo về lập trình an toàn hàng năm.

↑ Lên đầu

Software Development Kit (SDK)

Dịch: bộ công cụ phát triển phần mềm (SDK)

Giải thích: *tập hợp thư viện, API, tài liệu và công cụ hỗ trợ lập trình ứng dụng*

Ví dụ: Facebook cung cấp một bộ công cụ phát triển phần mềm (SDK) cho phép các lập trình viên dễ dàng tích hợp tính năng Đăng nhập bằng Facebook" vào ứng dụng của họ."

↑ Lên đầu

SonarQube

Dịch: SonarQube

Giải thích: *công cụ kiểm tra chất lượng mã, bao gồm bảo mật, code smells*

Ví dụ: Một đội phát triển sử dụng SonarQube để đảm bảo rằng mã nguồn của họ luôn đạt các tiêu chuẩn cao về chất lượng và bảo mật.

↑ Lên đầu

Sonic Visualiser

Dịch: Sonic Visualiser

Giải thích: *phân tích audio — dùng trong forensic hoặc Steganography.*

Ví dụ: Một điều tra viên sử dụng Sonic Visualiser để phân tích một file âm thanh đáng ngờ và tìm thấy một tín hiệu bất thường có chứa dữ liệu ẩn.

Xem thêm: Steganography

↑ Lên đầu

Spanning Tree Protocol (STP)

Dịch: Giao thức Cây Phân lớp (Spanning Tree Protocol)

Giải thích: *Giao thức layer 2 dùng trong switch mạng để tránh loop bằng cách tắt/mở các đường dẫn dự phòng và tạo cấu trúc cây không vòng lặp. Nếu bị cấu hình sai hoặc bị tấn công (BPDU spoofing) có thể gây mất kết nối hoặc thay đổi topology.*

Ví dụ: STP tắt một cổng dự phòng để tránh loop; khi link chính gãy, port dự phòng bật lên.

↑ Lên đầu

SpiderFoot

Dịch: SpiderFoot

Giải thích: *công cụ OSINT tự động, thu thập dữ liệu từ hàng trăm nguồn như DNS, IP, web, mạng xã hội*

Ví dụ: Bằng cách chạy SpiderFoot, chuyên gia OSINT đã thu thập và trực quan hóa mối liên hệ giữa tên miền mục tiêu với hàng trăm dải IP, tài khoản mạng xã hội và các tệp bị rò rỉ.

↑ Lên đầu

SpoofApp

Dịch: SpoofApp

Giải thích: *ứng dụng cho phép giả mạo số điện thoại/caller ID, gửi cuộc gọi/tin nhắn giả — thường bị lợi dụng cho Social engineering*

Ví dụ: Kẻ tấn công đã sử dụng SpoofApp để thực hiện một cuộc gọi Vishing (lừa đảo qua giọng nói), khiến nạn nhân thấy số điện thoại của ngân hàng thật đang hiển thị trên màn hình.

Xem thêm: Social engineering

↑ Lên đầu

SpoofCard

Dịch: SpoofCard

Giải thích: *dịch vụ/ứng dụng thương mại giả mạo caller ID, thay đổi giọng nói, che giấu danh tính khi gọi*

Ví dụ: Một nhà báo đã sử dụng SpoofCard để che giấu số điện thoại thật của mình khi gọi điện cho một nguồn tin nhạy cảm nhằm bảo vệ danh tính.

↑ Lên đầu

Spooftooph

Dịch: Spooftooph

Giải thích: *tool giả mạo MAC address trên Bluetooth/Wi-Fi*

Ví dụ: Một người dùng sử dụng Spooftooph để thay đổi địa chỉ MAC của mình nhằm truy cập vào một mạng Wi-Fi công cộng có giới hạn thời gian.

↑ Lên đầu

SpotBugs

Dịch: SpotBugs

Giải thích: *tool kiểm tra lỗi phần mềm Java — tìm bug, security issues*

Ví dụ: Lập trình viên chạy SpotBugs trên mã nguồn Java của họ để cải thiện chất lượng và giảm thiểu lỗi trước khi phát hành.

↑ Lên đầu

SQLmap

Dịch: SQLmap

Giải thích: *tool tự động phát hiện và khai thác SQL injection*

Ví dụ: Sau khi phát hiện một dấu hiệu của SQL injection, pentester sử dụng SQLmap để tự động khai thác và kết xuất toàn bộ bảng người dùng.

↑ Lên đầu

SSO (Single Sign-On)

Dịch: Đăng nhập một lần (SSO)

Giải thích: *Cơ chế cho phép người dùng đăng nhập một lần để truy cập nhiều dịch vụ/ứng dụng. Tiện lợi và giảm password fatigue. Rủi ro: single point of failure/compromise. Phòng thủ: bảo vệ IdP (Identity Provider), MFA, monitoring, session management.*

Ví dụ: Nhân viên đăng nhập bằng tài khoản Google và tự động truy cập Jira, Slack, GitHub mà không cần nhập lại mật khẩu.

↑ Lên đầu

State-Sponsored Attacker

Dịch: kẻ tấn công được nhà nước tài trợ

Giải thích: *Tác nhân/nhóm do chính phủ hậu thuẫn, thường là APT, thực hiện gián điệp mạng hoặc chiến tranh mạng.*

Ví dụ: Nhóm APT29, một tác nhân tấn công được nhà nước bảo trợ, đã thực hiện một chiến dịch gián điệp mạng kéo dài nhiều năm nhằm đánh cắp bí mật quân sự từ các quốc gia đối thủ.

↑ Lên đầu

statement of work (SOW)

Dịch: bản tuyên bố phạm vi công việc (SOW)

Giải thích: *tài liệu mô tả chi tiết các nhiệm vụ, mục tiêu và sản phẩm bàn giao của một dự án*

Ví dụ: Bản tuyên bố phạm vi công việc (SOW) mô tả rõ ràng rằng đội pentest sẽ kiểm tra 10 địa chỉ IP và bàn giao báo cáo cuối cùng sau 2 tuần.

↑ Lên đầu

static application security testing (SAST)

Dịch: kiểm thử bảo mật ứng dụng tĩnh (SAST)

Giải thích: *phân tích mã nguồn/mã biên dịch để tìm lỗ hổng*

Ví dụ: Một quy trình CI/CD tích hợp một công cụ SAST để tự động quét mã nguồn mỗi khi một lập trình viên đẩy code mới lên.

↑ Lên đầu

status reports

Dịch: báo cáo tình trạng/trạng thái

Giải thích: *cập nhật tiến độ, kết quả, trạng thái sửa chữa*

Ví dụ: Trưởng nhóm pentest gửi Status Reports hàng tuần cho khách hàng để họ nắm được tình hình kiểm thử.

↑ Lên đầu

Steganography

Dịch: Steganography

Giải thích: *kỹ thuật giấu dữ liệu bên trong file ảnh/audio/text để che giấu truyền tin.*

Ví dụ: Attacker dùng Steganography để giấu một file chứa mật khẩu vào bên trong một file ảnh PNG, sau đó gửi file ảnh này qua email để qua mặt các hệ thống phòng chống mất mát dữ liệu (DLP).

↑ Lên đầu

steghide

Dịch: steghide

Giải thích: *công cụ Steganography dùng để nhúng/đóng gói file vào ảnh hoặc audio — lệnh steghide để nhúng/giải nén dữ liệu.*

Ví dụ: Attacker dùng lệnh steghide embed -cf kitten.jpg -ef passwords.txt để nhúng file passwords.txt vào trong file ảnh kitten.jpg.

Xem thêm: Steganography, steghide

↑ Lên đầu

string operators

Dịch: toán tử xử lý chuỗi

Giải thích: *nối chuỗi, substring, regex — thao tác trên chuỗi*

Ví dụ: Pentester viết script sử dụng String Operators để trích xuất các địa chỉ email từ một file text lớn.

↑ Lên đầu

sudo command

Dịch: lệnh sudo

Giải thích: *lệnh nâng quyền trên Unix/Linux — dùng để thực thi lệnh với quyền user khác hoặc root.*

Ví dụ: Là lệnh cơ bản nhất để thực hiện Vertical Privilege Escalation trên Linux/Unix. Attacker sau khi có quyền user thường sẽ tìm các lỗi cấu hình sudoers để có thể chạy lệnh với quyền root.

↑ Lên đầu

Sysinternals

Dịch: Sysinternals

Giải thích: *bộ công cụ của Microsoft cho quản trị/Forensics/pentest trên Windows — ví dụ PsExec, Procmon, Autoruns.*

Ví dụ: Là bộ công cụ quản trị mạnh mẽ của Microsoft nhưng thường bị attacker lạm dụng để sống trên đất địch" (LotL) cho các hoạt động hậu khai thác."

Xem thêm: Forensics, PsExec

↑ Lên đầu

system hardening

Dịch: tăng cường bảo mật hệ thống

Giải thích: *gộp các biện pháp giảm bề mặt tấn công — tắt dịch vụ không cần thiết, cấu hình secure, harden OS/application.*

Ví dụ: Trước khi đưa một máy chủ web ra Internet, quản trị viên thực hiện System Hardening bằng cách đóng các cổng không sử dụng và vô hiệu hóa tài khoản mặc định.

↑ Lên đầu

tcpdump command

Dịch: lệnh tcpdump

Giải thích: *công cụ dòng lệnh để chụp/hiển thị gói tin mạng trên Unix/Linux*

Ví dụ: Để nhanh chóng kiểm tra xem máy chủ có đang gửi lưu lượng (traffic) đến một IP đáng ngờ hay không, admin đã chạy lệnh tcpdump host 1.2.3.4 trên

terminal.

↑ Lên đầu

tcsh

Dịch: tcsh

Giải thích: *Tenex C Shell — biến thể của csh, Shell cho Unix.*

Ví dụ: Attacker nhận được một shell và chạy lệnh echo $SHELL, kết quả trả về là /bin/bash, cho biết đây là môi trường Bash.

Xem thêm: Shell

↑ Lên đầu

technical contact

Dịch: liên hệ kỹ thuật

Giải thích: *người chịu trách nhiệm về mặt kỹ thuật/kỹ sư liên hệ*

Ví dụ: Khi cần làm rõ về kiến trúc mạng, đội pentest sẽ liên hệ với Technical Contact là Trưởng nhóm mạng của khách hàng.

↑ Lên đầu

technical control

Dịch: biện pháp kiểm soát kỹ thuật

Giải thích: *ví dụ: firewall, IDS/IPS, mã hóa*

Ví dụ: Công ty triển khai tường lửa (firewall) và hệ thống phát hiện xâm nhập (IDS). Đây là các Technical Control.

↑ Lên đầu

The CERT division of Carnegie Mellon University

Dịch: Phòng CERT thuộc Đại học Carnegie Mellon

Giải thích: *đơn vị nghiên cứu/ứng cứu sự cố an ninh mạng, nổi tiếng về nghiên cứu bảo mật*

Ví dụ: Phòng CERT thuộc Đại học Carnegie Mellon là một trong những tổ chức đầu tiên và uy tín nhất thế giới, chuyên nghiên cứu và công bố các lỗ hổng bảo mật.

↑ Lên đầu

The GNU Project Debugger (GDB)

Dịch: GDB

Giải thích: *debugger mã nguồn mở cho Linux/Unix.*

Ví dụ: Một nhà nghiên cứu bảo mật sử dụng GDB để phân tích một file nhị phân và tìm ra vị trí gây ra lỗi tràn bộ đệm.

↑ Lên đầu

The Internet Corporation for Assigned Names and Numbers (ICANN)

Dịch: ICANN

Giải thích: *tổ chức quản lý tên miền và phân bổ tài nguyên Internet*

Ví dụ: ICANN là tổ chức đặt ra các quy định mà các nhà đăng ký tên miền như GoDaddy phải tuân theo.

↑ Lên đầu

theHarvester

Dịch: theHarvester

Giải thích: *tool OSINT thu thập email, host, subdomain từ nguồn công khai*

Ví dụ: Attacker sử dụng theHarvester để xây dựng một danh sách email nhân viên, chuẩn bị cho một chiến dịch tấn công phishing.

Xem thêm: host

↑ Lên đầu

time-of-day restriction

Dịch: hạn chế truy cập theo khung giờ định sẵn

Giải thích:

Ví dụ: Hệ thống được cấu hình Time-of-day Restriction để chặn tất cả các lượt đăng nhập VPN từ bên ngoài trong khoảng thời gian từ 10 giờ tối đến 6 giờ sáng.

↑ Lên đầu

Timing Options (-T0–T5)

Dịch: tùy chọn thời gian (-T0..-T5)

Giải thích: *điều chỉnh tốc độ/quy mô quét: T0 rất chậm/ẩn, T5 nhanh/ồn*

Ví dụ: Khi thực hiện pentest trong giờ hành chính, chuyên gia bảo mật đã dùng tùy chọn thời gian (-T0..-T5) ở mức T2 (Polite) để quét chậm, tránh làm nghẽn băng thông của khách hàng.

↑ Lên đầu

TinEye

Dịch: TinEye

Giải thích: *reverse image search — tìm nguồn gốc/metadata ảnh.*

Ví dụ: Một nhà báo sử dụng TinEye để xác minh xem một bức ảnh được đăng trên mạng xã hội là thật hay đã được lấy từ một nguồn khác.

↑ Lên đầu

Tor

Dịch: Tor

Giải thích: *mạng ẩn danh — dùng để ẩn IP, Evasion, OSINT, C2.*

Ví dụ: Một attacker điều khiển hệ thống C2 của mình thông qua mạng Tor để làm cho việc truy tìm nguồn gốc của cuộc tấn công trở nên khó khăn hơn.

Xem thêm: Evasion

↑ Lên đầu

trees

Dịch: cây

Giải thích: *cấu trúc cây — dùng cho phân cấp/thuật toán*

Ví dụ: BloodHound sử dụng một cấu trúc dữ liệu dạng Tree để biểu diễn các mối quan hệ và đường đi tấn công trong Active Directory.

↑ Lên đầu

TrevorC2

Dịch: TrevorC2

Giải thích: *C2 framework — dùng website/HTTP để ẩn kênh điều khiển.*

Ví dụ: Dùng để ẩn kênh C2 trong các truy cập website bình thường. Agent sẽ truy cập một trang web trông có vẻ vô hại để lấy lệnh được giấu trong mã nguồn trang.

↑ Lên đầu

true negative

Dịch: âm tính đúng

Giải thích: *không có cảnh báo và thực tế không có sự cố*

Ví dụ: Trong một ngày làm việc không có sự cố an ninh nào, và hệ thống IDS cũng không tạo ra cảnh báo nào. Đây là trạng thái True Negative.

↑ Lên đầu

true positive

Dịch: dương tính đúng

Giải thích: *cảnh báo đúng là sự cố*

Ví dụ: Hệ thống phát hiện và chặn một kết nối ra ngoài tới một máy chủ C2 đã biết. Đây là một True Positive.

↑ Lên đầu

unethical hacking

Dịch: hacking phi đạo đức

Giải thích: *Tấn công trái phép với mục đích xấu như trộm dữ liệu, phá hoại, tống tiền...*

Ví dụ: Kẻ tấn công đã thực hiện hành vi unethical hacking khi xâm nhập trái phép vào cơ sở dữ liệu của một cửa hàng trực tuyến để đánh cắp thông tin thẻ tín dụng của khách hàng.

↑ Lên đầu

unknown-environment test (black-box)

Dịch: kiểm thử hộp đen

Giải thích: *Pentester không biết gì về hệ thống, mô phỏng attacker từ bên ngoài.*

Ví dụ: Trong bài kiểm thử hộp đen (black-box), đội tấn công chỉ được cung cấp tên miền của công ty và phải tự mình khám phá mọi thứ như một hacker bên ngoài.

↑ Lên đầu

unknown-environment testing

Dịch: kiểm thử hộp đen

Giải thích: *pentester không biết gì về hệ thống, mô phỏng attacker bên ngoài*

Ví dụ: Trong bài kiểm thử hộp đen (unknown-environment testing), đội pentest chỉ được cung cấp tên công ty và phải tự mình khám phá mọi thứ như một hacker bên ngoài.

↑ Lên đầu

Unknown-Environment Testing (black-box)

Dịch: kiểm thử hộp đen

Giải thích: *pentester không biết thông tin hệ thống, mô phỏng attacker bên ngoài*

Ví dụ: Trong bài kiểm thử hộp đen (Unknown-Environment Testing), đội pentest không được cung cấp bất kỳ thông tin gì ngoài tên miền của công ty.

↑ Lên đầu

Unmanned Aerial Vehicle (UAV)

Dịch: Phương tiện bay không người lái (UAV / drone)

Giải thích: *Thiết bị bay điều khiển từ xa có thể mang bộ thu/phát Wi-Fi/Bluetooth để dò tìm, phát hiện rogue AP, hoặc (nếu bị lạm dụng) phục vụ tấn công mạng/vật lý.*

Ví dụ: Drone chuyên dụng bay khảo sát an ninh mạng không dây, phát hiện vùng phủ sóng và AP không được phép.

↑ Lên đầu

User Account Control (UAC)

Dịch: User Account Control (UAC)

Giải thích: *cơ chế kiểm soát nâng quyền trên Windows — mục tiêu tấn công thường tìm kỹ thuật bỏ qua/elevate UAC.*

Ví dụ: Attacker sử dụng kỹ thuật UAC Bypass" để chạy một cửa sổ lệnh với quyền quản trị viên (Administrator) mà không làm hiện lên bảng thông báo của UAC."

↑ Lên đầu

User enumeration

Dịch: liệt kê người dùng

Giải thích: *kỹ thuật xác định danh sách tài khoản người dùng hợp lệ trong hệ thống*

Ví dụ: Hacker đã sử dụng kỹ thuật User enumeration trên cổng SMTP (lệnh VRFY) để lấy được danh sách địa chỉ email của toàn bộ nhân viên trong công ty.

↑ Lên đầu

user input sanitization and query parameterization

Dịch: làm sạch dữ liệu đầu vào và tham số hóa truy vấn

Giải thích: *ngăn SQL injection, XSS — validate/escape input và dùng prepared statements.*

Ví dụ: Lập trình viên sử dụng Query Parameterization (prepared statements) để đảm bảo dữ liệu người dùng nhập vào không thể can thiệp vào logic của câu lệnh SQL.

↑ Lên đầu

user training

Dịch: đào tạo người dùng

Giải thích: *awareness training — phishing, password hygiene, incident reporting*

Ví dụ: Công ty tổ chức các buổi User Training hàng quý và gửi các email giả lập phishing để kiểm tra nhận thức của nhân viên.

↑ Lên đầu

Veil

Dịch: Veil

Giải thích: *framework tạo payload tránh phát hiện AV/EDR.*

Ví dụ: Pentester sử dụng Veil để tạo một file thực thi độc hại có tỷ lệ bị phát hiện (FUD - Fully Undetectable) cao.

↑ Lên đầu

Vertical privilege escalation

Dịch: Leo thang đặc quyền theo chiều dọc

Giải thích: *Khi attacker nâng từ account có ít quyền (user) lên account có quyền cao hơn (admin/root). Phòng thủ: patching, role separation, monitoring privileged actions, use of least-privilege accounts.*

Ví dụ: Người dùng thông thường truy cập được giao diện quản trị do lỗi kiểm tra quyền truy cập.

↑ Lên đầu

vertical privilege escalation

Dịch: vertical privilege escalation

Giải thích: *leo thang đặc quyền theo cấp — từ user lên admin/root.*

Ví dụ: Là quá trình attacker nâng quyền từ một tài khoản có đặc quyền thấp (user) lên một tài khoản có đặc quyền cao hơn (Administrator/root) trên cùng một máy.

↑ Lên đầu

video surveillance

Dịch: giám sát video

Giải thích: *camera CCTV để kiểm soát an ninh vật lý và làm bằng chứng*

Ví dụ: Bộ phận an ninh xem lại băng ghi hình từ hệ thống Video Surveillance để điều tra một vụ mất cắp thiết bị.

↑ Lên đầu

VMware

Dịch: VMware

Giải thích: *Bộ phần mềm ảo hóa thương mại, mạnh cho doanh nghiệp, gồm VMware Workstation, ESXi...*

Ví dụ: Trong môi trường doanh nghiệp, quản trị viên hệ thống sử dụng VMware ESXi để ảo hóa hàng chục máy chủ trên một máy chủ vật lý duy nhất, giúp tối ưu hóa tài nguyên phần cứng.

Xem thêm: VMware

↑ Lên đầu

VNC

Dịch: VNC

Giải thích: *giao thức điều khiển máy tính từ xa, cross-platform.*

Ví dụ: Pentester phát hiện một máy chủ có cổng 5900 (VNC) đang mở và không yêu cầu mật khẩu. Họ dùng VNC client kết nối thẳng vào và thấy toàn bộ màn hình desktop của máy chủ đó.

↑ Lên đầu

VNC

Dịch: VNC

Giải thích: *Virtual Network Computing — giao thức/ứng dụng điều khiển desktop từ xa, có thể bị lợi dụng để remote access.*

Ví dụ: Là giao thức điều khiển từ xa đa nền tảng. Thường bị attacker lợi dụng khi các hệ thống VNC được cấu hình với mật khẩu yếu hoặc không có mật khẩu.

↑ Lên đầu

Vulnerability scanning

Dịch: quét lỗ hổng

Giải thích: *quét tự động để phát hiện lỗ hổng trên host/ứng dụng*

Ví dụ: Công ty thực hiện Vulnerability Scanning hàng tháng trên toàn bộ hệ thống để đảm bảo các bản vá được cập nhật đầy đủ.

Xem thêm: host

↑ Lên đầu

W3af

Dịch: W3af

Giải thích: *web application attack and audit framework — web vulnerability scanner/exploitation*

Ví dụ: Pentester cấu hình W3af với các plugin phù hợp để thực hiện một cuộc tấn công toàn diện vào một ứng dụng web mục tiêu.

↑ Lên đầu

WannaCry

Dịch: WannaCry (ransomware)

Giải thích: *Ransomware từng lan rộng toàn cầu (2017), khai thác EternalBlue để lây lan qua SMB và mã hóa dữ liệu nạn nhân; ví dụ điển hình về tác động của exploit chưa được vá.*

Ví dụ: Sau khi lây nhiễm, WannaCry đổi tên file thành .WNCRY và hiển thị thông báo đòi tiền chuộc Bitcoin.

Xem thêm: EternalBlue

↑ Lên đầu

War Driving

Dịch: War Driving (lái xe dò tìm Wi-Fi)

Giải thích: *Hành vi dò tìm, thu thập thông tin mạng không dây (SSID, BSSID, kênh, bảo mật) bằng thiết bị di động khi di chuyển — thường để khảo sát bề mặt tấn công hoặc lập bản đồ mạng công cộng.*

Ví dụ: Nhóm bảo mật lái xe quanh thành phố dùng laptop + anten thu tín hiệu Wi-Fi, ghi lại SSID/BSSID bằng Kismet.

↑ Lên đầu

War Flying

Dịch: War Flying (bay dò tìm Wi-Fi bằng drone/plane)

Giải thích: *Tương tự War Driving nhưng dùng UAV/phi cơ để thu thập tín hiệu không dây trên khu vực rộng — dùng cho khảo sát/inventory mạng không dây quy mô lớn.*

Ví dụ: Nhóm bảo mật lái xe quanh thành phố dùng laptop + anten thu tín hiệu Wi-Fi, ghi lại SSID/BSSID bằng Kismet.

Xem thêm: War Driving

↑ Lên đầu

Web Application Description Language (WADL)

Dịch: ngôn ngữ mô tả ứng dụng web (WADL)

Giải thích: *tài liệu XML mô tả dịch vụ web RESTful*

Ví dụ: Pentester đã phân tích tệp Web Application Description Language (WADL) để lập bản đồ các điểm cuối (endpoints) và phương thức (methods) của dịch vụ RESTful trước khi bắt đầu tấn công.

↑ Lên đầu

Website archiving/caching

Dịch: lưu trữ/đệm website

Giải thích: *tra cứu bản sao lịch sử từ Wayback Machine hoặc cache search engine để khôi phục nội dung đã thay đổi/xóa*

Ví dụ: Trang web hiện tại đã an toàn, nhưng nhờ lưu trữ/đệm website (sử dụng Google Cache), kẻ tấn công đã tìm thấy một phiên bản cũ của trang /config.txt có chứa mật khẩu.

↑ Lên đầu

WebSocket

Dịch: WebSocket

Giải thích: *giao thức kết nối hai chiều, full-duplex giữa client và server — thường bị khai thác/được dùng làm kênh C2 hoặc truyền dữ liệu bất đồng bộ trong web.*

Ví dụ: Một mã độc sử dụng WebSocket để duy trì kết nối liên tục với C2 server, cho phép attacker gửi lệnh và nhận kết quả gần như ngay lập tức.

↑ Lên đầu

WhatBreach

Dịch: WhatBreach

Giải thích: *công cụ/dịch vụ tra cứu vụ rò rỉ dữ liệu liên quan đến tên miền hoặc email*

Ví dụ: Bằng cách sử dụng WhatBreach, chuyên gia bảo mật đã nhập vào tên miền congty.com và phát hiện ra công ty này đã từng bị rò rỉ dữ liệu trong một vụ tấn công năm 2019.

↑ Lên đầu

WHAX

Dịch: WHAX

Giải thích: *distro pentest cũ — tiền thân của nhiều distro tấn công*

Ví dụ: Nhiều chuyên gia bảo mật kỳ cựu đã bắt đầu sự nghiệp của mình với các công cụ như WHAX.

↑ Lên đầu

whois

Dịch: whois

Giải thích: *truy vấn thông tin đăng ký domain/địa chỉ liên hệ*

Ví dụ: Attacker sử dụng whois để tìm tên và email của người quản trị kỹ thuật của một domain, nhằm mục đích tấn công lừa đảo.

↑ Lên đầu

whois command

Dịch: lệnh whois

Giải thích: *công cụ truy vấn thông tin đăng ký tên miền: chủ sở hữu, nhà đăng ký, DNS, ngày tạo/hết hạn*

Ví dụ: Sử dụng lệnh whois target.com, chuyên gia OSINT đã tìm thấy tên, email, và số điện thoại của người đã đăng ký tên miền đó.

↑ Lên đầu

Whois Data Problem Reporting System (WDPRS)

Dịch: WDPRS

Giải thích: *hệ thống của ICANN để báo cáo vấn đề với dữ liệu whois*

Ví dụ: Một nhà nghiên cứu báo cáo một tên miền được dùng cho mục đích lừa đảo thông qua WDPRS vì nó sử dụng thông tin đăng ký giả mạo.

Xem thêm: whois

↑ Lên đầu

WHoppiX

Dịch: WHoppiX

Giải thích:

Ví dụ: WHoppiX là một công cụ lịch sử, tiền thân của các hệ điều hành pentest hiện đại hơn.

↑ Lên đầu

Wi-Fi Protected Access version 1 (WPA)

Dịch: WPA (bảo mật Wi-Fi — phiên bản 1)

Giải thích: *Tiêu chuẩn bảo mật kế thừa WEP, giới thiệu TKIP để cải thiện bảo mật; hiện đã lỗi thời/ít an toàn so với WPA2.*

Ví dụ: Router cũ cấu hình WPA-TKIP, dễ bị brute-force hoặc khai thác, vì vậy được khuyến nghị nâng cấp lên WPA2/AES.

↑ Lên đầu

Wi-Fi Protected Setup (WPS) PIN attack

Dịch: Tấn công mã PIN WPS

Giải thích: *Khai thác cơ chế WPS (PIN 8 chữ số) để bẻ khóa PSK; WPS PIN yếu/kém thiết kế dẫn tới brute-force khả thi. (Lưu ý: mô tả rủi ro, không chỉ cách thực hiện.)*

Ví dụ: Kẻ tấn công dùng reaver -i wlan0mon -b brute-force mã PIN WPS 8 chữ số trên router cũ, trích xuất được PSK của Wi-Fi “MyHomeNet”.

↑ Lên đầu

Wifite2

Dịch: Wifite2

Giải thích: *tool tự động tấn công mạng Wi-Fi — brute-force WEP/WPA/WPA2*

Ví dụ: Một pentester sử dụng Wifite2 để nhanh chóng kiểm tra xem các mạng Wi-Fi trong khu vực có sử dụng mật khẩu yếu hay không.

↑ Lên đầu

WiGLE

Dịch: WiGLE (Wireless Geographic Logging Engine)

Giải thích: *Dịch vụ/website và cơ sở dữ liệu chứa bản đồ điểm truy cập Wi-Fi thu thập công cộng (SSID, BSSID, vị trí). Dùng cho nghiên cứu, khảo sát — cũng có thể tiết lộ lịch sử mạng công cộng.*

Ví dụ: Người dùng tải dữ liệu từ WiGLE để xem bản đồ các điểm Wi-Fi quanh khu vực, bao gồm SSID và tọa độ GPS.

↑ Lên đầu

WiGLE (Wireless Geographic Logging Engine)

Dịch: WiGLE

Giải thích: *database và tool thu thập dữ liệu vị trí Wi-Fi.*

Ví dụ: Một nhà nghiên cứu sử dụng WiGLE để tìm kiếm và vẽ bản đồ các điểm truy cập Wi-Fi trong một thành phố.

↑ Lên đầu

Windows Common Internet File System (CIFS)

Dịch: Giao thức CIFS (Common Internet File System trên Windows)

Giải thích: *Phiên bản/biến thể của SMB dùng để chia sẻ tập tin/printer giữa Windows hosts. CIFS/SMB là bề mặt tấn công thường gặp (e.g., lỗ hổng, credential reuse).*

Ví dụ: Legacy servers expose shares via CIFS/SMB.

↑ Lên đầu

Windows Debugger

Dịch: Windows Debugger

Giải thích: *công cụ gỡ lỗi ứng dụng Windows — WinDbg.*

Ví dụ: Một kỹ sư sử dụng WinDbg để phân tích một file dump (memory dump) sau khi hệ thống bị màn hình xanh chết chóc" (BSOD)."

↑ Lên đầu

Windows Management Instrumentation (WMI)

Dịch: WMI (Windows Management Instrumentation)

Giải thích: *Khung quản lý/giám sát hệ thống Windows cho phép truy vấn trạng thái, chạy lệnh, quản lý cấu hình từ xa. Công cụ tuyệt vời cho quản trị và scripting; cũng thường được dùng cho lateral movement trong môi trường tấn công.*

Ví dụ: Quản trị viên dùng WMI để lấy danh sách process: wmic process list.

Xem thêm: lateral movement

↑ Lên đầu

Windows PowerShell

Dịch: Windows PowerShell

Giải thích: *Shell/kịch bản dòng lệnh nâng cao trên Windows, hỗ trợ cmdlet và scripting.*

Ví dụ: Attacker sử dụng một script PowerShell để tải và chạy mã độc trực tiếp trên RAM, không ghi file ra đĩa, nhằm đánh cắp mật khẩu.

Xem thêm: Shell

↑ Lên đầu

Windows Remote Management (WinRM)

Dịch: Windows Remote Management (WinRM)

Giải thích: *cơ chế/Windows service cho quản trị từ xa dựa trên WS-Management — có thể bị lợi dụng cho remote execution.*

Ví dụ: Là một dịch vụ quản trị từ xa hợp pháp của Windows. Attacker có thể lạm dụng WinRM để thực thi lệnh từ xa và thực hiện Lateral Movement nếu họ đã đánh cắp được thông tin đăng nhập hợp lệ.

↑ Lên đầu

Wired Equivalent Privacy (WEP)

Dịch: WEP (bảo mật tương đương có dây — WEP)

Giải thích: *Cơ chế bảo mật Wi-Fi cũ, đã bị bẻ khóa dễ dàng do thiết kế yếu; không còn an toàn, không nên dùng.*

Ví dụ: Mạng văn phòng cũ vẫn dùng WEP 64-bit, pentester chỉ mất vài phút thu đủ IV và phá khóa bằng Aircrack-ng.

↑ Lên đầu

Wireless Local Area Network (WLAN)

Dịch: Mạng cục bộ không dây (WLAN)

Giải thích: *Mạng LAN sử dụng công nghệ không dây (Wi-Fi) để kết nối thiết bị; bao gồm AP, client, controller, SSID, security settings.*

Ví dụ: Mạng Wi-Fi trong văn phòng gồm 3 Access Point liên kết qua controller tạo thành một WLAN phục vụ nhân viên.

↑ Lên đầu

WMImplant

Dịch: WMImplant

Giải thích: *post-exploit tool dùng WMI/PowerShell để thực thi lệnh và làm kênh điều khiển.*

Ví dụ: Attacker có quyền admin trên một máy, họ dùng WMImplant để thực thi lệnh trên các máy tính khác trong cùng mạng mà không cần phải cài backdoor.

Xem thêm: PowerShell

↑ Lên đầu

WPA version 2 (WPA2)

Dịch: WPA2 (bảo mật Wi-Fi — phiên bản 2)

Giải thích: *Chuẩn bảo mật phổ biến (sử dụng AES/CCMP) cho Wi-Fi; cung cấp chế độ Personal (PSK) và Enterprise (802.1X). Vẫn được dùng rộng rãi nhưng WPA3 được khuyến nghị cho môi trường mới.*

Ví dụ: Mạng Wi-Fi gia đình cấu hình WPA2-PSK với mật khẩu mạnh “MyHome@2025” để bảo vệ kết nối an toàn.

↑ Lên đầu

WPA version 3 (WPA3)

Dịch: WPA3 (bảo mật Wi-Fi — phiên bản 3)

Giải thích: *Phiên bản nâng cao (đã chuẩn hóa) với cải tiến an toàn như SAE (robust password-based auth), forward secrecy, cải thiện bảo vệ cho mạng công cộng; khuyến nghị triển khai trên thiết bị hỗ trợ.*

Ví dụ: Laptop hỗ trợ WPA3 dùng cơ chế SAE để xác thực, ngăn ngừa tấn công từ điển offline vào mật khẩu Wi-Fi.

↑ Lên đầu

wsc2

Dịch: WSC2

Giải thích: *WebSocket C2 — PoC/framework dùng WebSocket làm kênh C2.*

Ví dụ: Attacker cài agent WSC2 lên máy nạn nhân. Agent này sẽ tạo kết nối WebSocket ra ngoài tới C2 server, cho phép attacker gửi lệnh và nhận kết quả một cách bí mật.

Xem thêm: WebSocket

↑ Lên đầu

X server forwarding

Dịch: X server forwarding

Giải thích: *kỹ thuật hiển thị GUI từ Linux server qua SSH*

Ví dụ: Attacker lừa quản trị viên SSH vào một server độc hại có bật X11 forwarding. Khi quản trị viên mở một ứng dụng đồ họa, cửa sổ sẽ hiện ra, nhưng attacker có thể ghi lại các thông tin được nhập vào.

↑ Lên đầu

X server forwarding

Dịch: X server forwarding

Giải thích: *chuyển tiếp X11 — cho phép chạy ứng dụng GUI trên remote host nhưng hiển thị local; có thể lộ kênh/được lợi dụng trong pentest.*

Ví dụ: Dùng trong môi trường Linux/Unix để chạy ứng dụng đồ họa từ xa. Attacker có thể lợi dụng kênh này để chụp màn hình hoặc bắt các thao tác bàn phím (keylogging) nếu kiểm soát được kết nối.

Xem thêm: host

↑ Lên đầu

Zenmap

Dịch: Zenmap

Giải thích: *giao diện GUI cho Nmap — quét mạng và fingerprinting*

Ví dụ: Một người mới bắt đầu sử dụng Zenmap để thực hiện quét cổng một cách dễ dàng mà không cần phải nhớ các cú pháp lệnh phức tạp của Nmap.

Xem thêm: Nmap

↑ Lên đầu