T1 Social engineering	T1 adversary	T1 elicitation
T1 Intimidation	T1 Urgency	T1 impact
T1 challenge questions	T1 impersonate	T1 one-time password (OTP)

T1 套取信息 tào qǔ xìn xī	T1 对手 duì shǒu	T1 社会工程学 shè huì gōng chéng xué
T1 影响 yǐng xiǎng	T1 紧迫感 jǐn pò gǎn	T1 恐吓 kǒng hè
T1 一次性密码 yí cì xìng mì mǎ	T1 冒充 mào chōng	T1 安全问题 ān quán wèn tí

T1 malware	T1 password attack	T1 weak
T1 dictionary	T1 authentication	T1 password manager
T1 multifactor authentication (MFA)	T1 exploits	T1 zero days

T1 弱 ruò	T1 密码攻击 mì mǎ gōng jī	T1 恶意软件 è yì ruǎn jiàn
T1 密码管理器 mì mǎ guǎn lǐ qì	T1 身份验证 shēn fèn yàn zhèng	T1 字典 zì diǎn
T1 零日漏洞 líng rì lòu dòng	T1 漏洞利用 lòu dòng lì yòng	T1 多因素身份验证 duō yīn sù shēn fèn yàn zhèng

T1 motivation	T1 Evil twin	T1 access point
T1 SSID	T1 encrypted	T1 Jamming
T1 denial of service (DoS)	T1 War driving	T1 virtual private network (VPN)

T1 接入点 jiē rù diǎn	T1 双胞胎恶意热点 shuāng bāo tāi è yì rè diǎn	T1 动机 dòng jī
T1 干扰攻击 gān rǎo gōng jī	T1 加密的 jiā mì de	T1 服务集标识符 fú wù jí biāo shí fú
T1 虚拟专用网络 xū nǐ zhuān yòng wǎng luò	T1 驾车无线网络探测 jià chē wú xiàn wǎng luò tàn cè	T1 拒绝服务 jù jué fú wù

T1 deepfake	T1 Large language models (LLMs)	T1 phishing
T1 shared secret	T1 AI-enhanced coding tools	T1 threat detection and response
T1 passphrase	T2 CIA triad	T2 Confidentiality

T1 钓鱼 diào yú	T1 大语言模型 dà yǔ yán mó xíng	T1 深度伪造 shēn dù wěi zào
T1 威胁检测与响应 wēi xié jiǎn cè yǔ xiǎng yìng	T1 人工智能辅助编程工具 rén gōng zhì néng fǔ zhù biān chéng gōng jù	T1 共享秘密 gòng xiǎng mì mì
T2 保密性 bǎo mì xìng	T2 信息安全三要素 xìn xī ān quán sān yào sù	T1 密码短语 mì mǎ duǎn yǔ

T2 Integrity	T2 Availability	T2 script kiddie
T2 hacktivist	T2 insider	T2 cyberterrorist
T2 transnational criminal organisations	T2 phases	T2 reconnaissance

T2 脚本小子 jiǎo běn xiǎo zi	T2 可用性 kě yòng xìng	T2 完整性 wán zhěng xìng
T2 网络恐怖分子 wǎng luò kǒng bù fèn zi	T2 内部人员 nèi bù rén yuán	T2 黑客活动分子 hēi kè huó dòng fèn zǐ
T2 侦察 zhēn chá	T2 阶段 jiē duàn	T2 跨国犯罪组织 kuà guó fàn zuì zǔ zhī

T2 OSINT	T2 lateral movement	T2 social engineering
T2 Pretexting	T2 Authority	T2 Intimidation
T2 Consensus	T2 Scarcity	T2 Familiarity

T2

社会工程学

shè huì gōng chéng xué

T2

横向移动

héng xiàng yí dòng

T2

公开来源情报

gōng kāi lái yuán qíng bào

T2

恐吓

kǒng hè

T2

权威

quán wēi

T2

借口

jiè kǒu

T2

熟悉

shú xī

T2

稀缺

xī quē

T2

从众

cóng zhòng

T2 Urgency	T2 risk	T2 threat
T2 vulnerability	T2 asset	T2 likelihood
T2 severity	T2 quantitative	T2 qualitative

T2 威胁 wēi xié	T2 风险 fēng xiǎn	T2 紧迫感 jǐn pò gǎn
T2 可能性 kě néng xìng	T2 资产 zī chǎn	T2 漏洞 lòu dòng
T2 定性 dìng xìng	T2 定量 dìng liàng	T2 严重性 yán zhòng xìng

T2 risk assessment	T2 Avoid	T2 Transfer
T2 Mitigate	T2 Accept	T2 residual risk
T2 physical	T2 technical	T2 managerial

T2 转移 zhuǎn yí	T2 规避 guī bì	T2 风险评估 fēng xiǎn píng gū
T2 剩余风险 shèng yú fēng xiǎn	T2 接受 jiē shòu	T2 缓解 huǎn jiě
T2 管理 guǎn lǐ	T2 技术 jì shù	T2 物理 wù lǐ

T2 preventative	T2 detective	T2 corrective
T2 defense-in-depth	T2 physical attacks	T2 Piggybacking
T2 Tailgating	T2 Shoulder surfing	T2 Dumpster diving

T2 纠正性 jiū zhèng xìng	T2 检测性 jiǎn cè xìng	T2 预防性 yù fáng xìng
T2 尾随（获许可） wěi suí （huò xǔ kě ）	T2 物理攻击 wù lǐ gōng jī	T2 纵深防御 zòng shēn fáng yù
T2 翻垃圾搜集情报 fān lā jī sōu jí qíng bào	T2 肩窥 jiān kuī	T2 尾随（未察觉） wěi suí （wèi chá jué ）

T2 Card cloning	T2 keylogger	T2 foothold
T2 clean desk policy	T2 bollards	T2 card readers
T2 access control vestibule	T2 uninterruptible power supply (UPS)	T2 motion sensors

T2

立足点

lì zú diǎn

T2

键盘记录器

jiàn pán jì lù qì

T2

门禁卡复制

mén jìn kǎ fù zhì

T2

读卡器

dú kǎ qì

T2

防撞柱

fáng zhuàng zhù

T2

清桌政策

qīng zhuō zhèng cè

T2

运动传感器

yùn dòng chuán gǎn qì

T2

不间断电源

bù jiàn duàn diàn yuán

T2

门禁前室

mén jìn qián shì

T2 points of ingress and egress	T2 command and control (C2)	T2 privileges
T2 exfiltration	T2 cost-effective	T2 expected loss
T2 turnstile	T2 surge protector	T3 ARP poisoning

T2

权限

quán xiàn

T2

命令与控制

mìng lìng yǔ kòng zhì

T2

出入口

chū rù kǒu

T2

预期损失

yù qī sǔn shī

T2

具有成本效益的

jù yǒu chéng běn xiào yì de

T2

数据外泄

shù jù wài xiè

T3

地址解析投毒

dì zhǐ jiě xī tóu dú

T2

浪涌保护器

làng yǒng bǎo hù qì

T2

闸机

zhá jī

T3 address resolution protocol (ARP)	T3 MAC addresses	T3 on-path attack
T3 MAC flooding	T3 switch	T3 eavesdropping
T3 DNS poisoning	T3 domain name system (DNS)	T3 credential harvesting

T3 中间人攻击 zhōng jiān rén gōng jī	T3 物理地址 wù lǐ dì zhǐ	T3 地址解析协议 dì zhǐ jiě xī xié yì
T3 窃听 qiè tīng	T3 交换机 jiāo huàn jī	T3 物理地址泛洪 wù lǐ dì zhǐ fàn hóng
T3 凭据收集 píng jù shōu jí	T3 域名系统 yù míng xì tǒng	T3 域名投毒 yù míng tóu dú

T3 denial of service (DoS)	T3 distributed denial of service (DDoS)	T3 rogue access point
T3 automated vulnerability scanner	T3 mitigation	T3 split tunneling
T3 WPA3	T3 Network segmentation	T3 subnets

T3 非法接入点 fēi fǎ jiē rù diǎn	T3 分布式拒绝服务 fēn bù shì jù jué fú wù	T3 拒绝服务 jù jué fú wù
T3 分离隧道 fēn lí suì dào	T3 缓解措施 huǎn jiě cuò shī	T3 自动漏洞扫描器 zì dòng lòu dòng sǎo miáo qì
T3 子网 zǐ wǎng	T3 网络分段 wǎng luò fēn duàn	T3 Wi-Fi 保护接入第三代 bǎo hù jiē rù dì sān dài

T3 screened subnet	T3 DMZ	T3 VLANs
T3 firewall	T3 Stateless	T3 Stateful
T3 access control list (ACL)	T3 log files	T3 network intrusion detection system (NIDS)

T3

虚拟局域网

xū nǐ jú yù wǎng

T3

隔离区

gé lí qū

T3

屏蔽子网

píng bì zǐ wǎng

T3

有状态

yǒu zhuàng tài

T3

无状态

wú zhuàng tài

T3

防火墙

fáng huǒ qiáng

T3

网络入侵检测系统

wǎng luò rù qīn jiǎn cè xì tǒng

T3

日志文件

rì zhì wén jiàn

T3

访问控制列表

fǎng wèn kòng zhì liè biǎo

T3 network intrusion prevention system (NIPS)	T3 security information and event management (SIEM)	T3 Signature-based
T3 Anomaly-based	T3 baseline	T3 network-based indicators of compromise
T3 probabilistic	T3 threshold	T3 alert fatigue

T3

基于特征

jī yú tè zhēng

T3

安全信息与事件管理

ān quán xìn xī yǔ shì jiàn guǎn lǐ

T3

网络入侵防御系统

wǎng luò rù qīn fáng yù xì tǒng

T3

网络入侵指标

wǎng luò rù qīn zhǐ biāo

T3

基线

jī xiàn

T3

基于异常

jī yú yì cháng

T3

警报疲劳

jǐng bào pí láo

T3

阈值

yù zhí

T3

概率的

gài lǜ de

T4 embedded computer	T4 Internet of Things (IoT)	T4 handheld computers
T4 malware	T4 Virus	T4 Worm
T4 Trojan	T4 remote access trojan (RAT)	T4 Ransomware

T4 手持计算机 shǒu chí jì suàn jī	T4 物联网 wù lián wǎng	T4 嵌入式计算机 qiàn rù shì jì suàn jī
T4 蠕虫 rú chóng	T4 病毒 bìng dú	T4 恶意软件 è yì ruǎn jiàn
T4 勒索软件 lè suǒ ruǎn jiàn	T4 远程访问木马 yuǎn chéng fǎng wèn mù mǎ	T4 木马 mù mǎ

T4 Spyware	T4 Keylogger	T4 Logic bomb
T4 fileless malware	T4 RAM	T4 unpatched software
T4 cryptographic hash function	T4 hash	T4 collision resistant

T4

逻辑炸弹

luó jí zhà dàn

T4

键盘记录器

jiàn pán jì lù qì

T4

间谍软件

jiàn dié ruǎn jiàn

T4

未打补丁的软件

wèi dǎ bǔ dīng de ruǎn jiàn

T4

内存

nèi cún

T4

无文件恶意软件

wú wén jiàn è yì ruǎn jiàn

T4

抗碰撞

kàng pèng zhuàng

T4

散列值

sàn liè zhí

T4

密码散列函数

mì mǎ sàn liè hán shù

T4 pre-image resistance	T4 deprecated	T4 salt
T4 brute force	T4 dictionary attack	T4 password spraying
T4 credential stuffing	T4 rainbow table	T4 complexity

T4 盐值 yán zhí	T4 弃用 qì yòng	T4 抗原像 kàng yuán xiàng
T4 密码喷洒 mì mǎ pēn sǎ	T4 字典攻击 zì diǎn gōng jī	T4 暴力破解 bào lì pò jiě
T4 复杂度 fù zá dù	T4 彩虹表 cǎi hóng biǎo	T4 撞库 zhuàng kù

T4 minimum length	T4 maximum age	T4 password history
T4 lockout	T4 password manager	T4 biometric
T4 multifactor authentication (MFA)	T4 autorun	T4 acceptable use policy

T4 密码历史 mì mǎ lì shǐ	T4 最长有效期 zuì cháng yǒu xiào qī	T4 最小长度 zuì xiǎo cháng dù
T4 生物特征 shēng wù tè zhēng	T4 密码管理器 mì mǎ guǎn lǐ qì	T4 锁定 suǒ dìng
T4 可接受使用政策 kě jiē shòu shǐ yòng zhèng cè	T4 自动运行 zì dòng yùn xíng	T4 多因素身份验证 duō yīn sù shēn fèn yàn zhèng

T4 Anti-malware software	T4 patch	T4 host-based firewall
T4 indicator of compromise (IoC)	T4 endpoint detection and response (EDR)	T5 Applications
T5 administrative	T5 injection attack	T5 Data validation

T4

主机防火墙

zhǔ jī fáng huǒ qiáng

T4

补丁

bǔ dīng

T4

反恶意软件

fǎn è yì ruǎn jiàn

T5

应用程序

yìng yòng chéng xù

T4

端点检测与响应

duān diǎn jiǎn cè yǔ xiǎng yìng

T4

入侵指标

rù qīn zhǐ biāo

T5

数据验证

shù jù yàn zhèng

T5

注入攻击

zhù rù gōng jī

T5

管理性

guǎn lǐ xìng

T5 Cross-site scripting (XSS)	T5 parameterised queries	T5 Buffer overflow
T5 buffer	T5 Directory traversal	T5 at rest
T5 in transit	T5 in use	T5 regulated

T5

缓冲区溢出

huǎn chōng qū yì chū

T5

参数化查询

cān shù huà chá xún

T5

跨站脚本

kuà zhàn jiǎo běn

T5

静态数据

jìng tài shù jù

T5

目录遍历

mù lù biàn lì

T5

缓冲区

huǎn chōng qū

T5

受监管

shòu jiān guǎn

T5

使用中数据

shǐ yòng zhōng shù jù

T5

传输中数据

chuán shū zhōng shù jù

T5 compliance	T5 personally identifiable information (PII)	T5 protected health information (PHI)
T5 payment card information (PCI)	T5 Role-based (RBAC)	T5 Rule-based (RuBAC)
T5 Discretionary (DAC)	T5 Mandatory (MAC)	T5 principle of least privilege

T5

受保护健康信息

shòu bǎo hù jiàn kāng xìn xī

T5

个人身份信息

gè rén shēn fèn xìn xī

T5

合规

hé guī

T5

基于规则的访问控制

jī yú guī zé de fǎng wèn kòng zhì

T5

基于角色的访问控制

jī yú jué sè de fǎng wèn kòng zhì

T5

支付卡信息

zhī fù kǎ xìn xī

T5

最小权限原则

zuì xiǎo quán xiàn yuán zé

T5

强制访问控制

qiáng zhì fǎng wèn kòng zhì

T5

自主访问控制

zì zhǔ fǎng wèn kòng zhì

T5 Cryptography	T5 plaintext	T5 key
T5 ciphertext	T5 keyspace	T5 Symmetric encryption
T5 AES	T5 block cipher	T5 Asymmetric encryption

T5 密钥 mì yào	T5 明文 míng wén	T5 密码学 mì mǎ xué
T5 对称加密 duì chèn jiā mì	T5 密钥空间 mì yào kōng jiān	T5 密文 mì wén
T5 非对称加密 fēi duì chèn jiā mì	T5 分组密码 fēn zǔ mì mǎ	T5 高级加密标准 gāo jí jiā mì biāo zhǔn

T5 key pair	T5 public key	T5 private key
T5 elliptic curve cryptography (ECC)	T5 Secure by design	T5 Secure by default
T5 input sanitization	T5 special characters	T5 accounting

T5 私钥 sī yào	T5 公钥 gōng yào	T5 密钥对 mì yào duì
T5 默认安全 mò rèn ān quán	T5 安全设计 ān quán shè jì	T5 椭圆曲线密码学 tuǒ yuán qū xiàn mì mǎ xué
T5 审计记录 shěn jì jì lù	T5 特殊字符 tè shū zì fú	T5 输入清理 shū rù qīng lǐ

T5 honeypot	T5 data loss prevention (DLP)	T5 SQL injection

T5 SQL 注入 SQL zhù rù	T5 数据泄露防护 shù jù xiè lòu fáng hù	T5 蜜罐 mì guàn