

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

T1 tào qǔ xīn xī	T1 duì shǒu	T1 shè huì gōng chéng xué
T1 yǐng xiǎng	T1 jīn pò gǎn	T1 kǒng hè
T1 yí cì xìng mì mǎ	T1 mào chōng	T1 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 ruò	T1 mì mǎ gōng jī	T1 è yì ruǎn jiàn
T1 mì mǎ guǎn lǐ qì	T1 shēn fēn yàn zhèng	T1 zì diǎn
T1 líng rì lòu dòng	T1 lòu dòng lì yòng	T1 duō yīn sù shēn fēn 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 jiē rù diǎn	T1 shuāng bāo tāi è yì rè diǎn	T1 dòng jī
T1 gān rǎo gōng jī	T1 jiā mì de	T1 fú wù jí biāo shí fú
T1 xū nǚ zhuān yòng wǎng luò	T1 zhàn zhēng jià shǐ	T1 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
T2 CIA triad	T2 Confidentiality	T2 Integrity

T1 diào yú	T1 dà yǔ yán mó xíng	T1 shēn dù wěi zào
T1 wēi xié jiǎn cè yǔ xiǎng yìng	T1 rén gōng zhì néng fǔ zhù biān chéng gōng jù	T1 gòng xiǎng mì mì
T2 wán zhěng xìng	T2 bǎo mì xìng	T2 xìn xī ān quán sān yào sù

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

T2 hēi kè huó dòng fèn zǐ	T2 jiǎo běn xiǎo zi	T2 kě yòng xìng
T2 kuà guó fàn zuì zǔ zhī	T2 wǎng luò kǒng bù fèn zi	T2 nèi bù rén yuán
T2 gōng kāi lái yuán qíng bào	T2 zhēn chá	T2 jiē duàn

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

T2 jiè kǒu	T2 shè huì gōng chéng xué	T2 héng xiàng yí dòng
T2 cóng zhòng	T2 kǒng hè	T2 quán wēi
T2 jǐn pò gǎn	T2 shú xī	T2 xī quē

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

T2 lòu dòng	T2 wēi xié	T2 fēng xiǎn
T2 yán zhòng xìng	T2 kě néng xìng	T2 zī chǎn
T2 fēng xiǎn píng gū	T2 dìng xìng	T2 dìng liàng

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

T2 huǎn jiě	T2 zhuǎn yí	T2 guī bì
T2 wù lǐ	T2 shèng yú fēng xiǎn	T2 jiē shòu
T2 yù fáng xìng	T2 guǎn lǐ	T2 jì shù

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

T2 zòng shēn fáng yù	T2 jiū zhèng xìng	T2 jiǎn cè xìng
T2 () wěi suí (wèi chá jué)	T2 () wěi suí (huò xǔ kě)	T2 wù lǐ gōng jī
T2 mén jìn kǎ fù zhì	T2 fān lā jī sōu jí qíng bào	T2 jiān kuī

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 points of ingress and egress

T2 qīng zhuō zhèng cè	T2 lì zú diǎn	T2 jiàn pán jì lù qì
T2 mén jìn qián shì	T2 dú kǎ qì	T2 fáng zhuàng zhù
T2 chū rù kǒu	T2 yùn dòng chuán gǎn qì	T2 bù jiàn duàn diàn yuán

T3 ARP poisoning	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 wù lǐ dì zhǐ	T3 dì zhǐ jiě xī xié yì	T3 dì zhǐ jiě xī tóu dú
T3 jiāo huàn jī	T3 wù lǐ dì zhǐ fàn hóng	T3 zhōng jiān rén gōng jī
T3 yù míng xì tǒng	T3 yù míng tóu dú	T3 qiè tīng

T3 credential harvesting	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 fēn bù shì jù jué fú wù	T3 jù jué fú wù	T3 píng jù shōu jí
T3 huǎn jiě cuò shī	T3 zì dòng lòu dòng sǎo miáo qì	T3 fēi fǎ jiē rù diǎn
T3 wǎng luò fēn duàn	T3 Wi-Fi bǎo hù jiē rù dì sān dài	T3 fēn lí suì dào

T3 subnets	T3 screened subnet	T3 DMZ
T3 VLANs	T3 firewall	T3 Stateless
T3 Stateful	T3 access control list (ACL)	T3 log files

T3 gé lí qū	T3 píng bì zì wǎng	T3 zì wǎng
T3 wú zhuàng tài	T3 fáng huǒ qiáng	T3 xū nǚ jú yù wǎng
T3 rì zhì wén jiàn	T3 fǎng wèn kòng zhì liè biǎo	T3 yǒu zhuàng tài

T3 network intrusion detection system (NIDS)	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 ān quán xìn xī yǔ shì jiàn guǎn lǐ	T3 wǎng luò rù qīn fáng yù xì tǒng	T3 wǎng luò rù qīn jiǎn cè xì tǒng
T3 jī xiàn	T3 jī yú yì cháng	T3 jī yú tè zhēng
T3 yù zhí	T3 gài lǚ de	T3 wǎng luò rù qīn zhǐ biāo

T3 alert fatigue	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 wù lián wǎng	T4 qiàn rù shì jì suàn jī	T3 jǐng bào pí láo
T4 bìng dú	T4 è yì ruǎn jiàn	T4 shǒu chí jì suàn jī
T4 yuǎn chéng fǎng wèn mù mǎ	T4 mù mǎ	T4 rú chóng

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

T4 jiàn pán jì lù qì	T4 jiàn dié ruǎn jiàn	T4 lè suǒ ruǎn jiàn
T4 nèi cún	T4 wú wén jiàn è yì ruǎn jiàn	T4 luó jí zhà dàn
T4 sàn liè zhí	T4 mì mǎ sàn liè hán shù	T4 wèi dǎ bǔ dīng de ruǎn jiàn

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

T4 qì yǒng	T4 kàng yuán xiàng	T4 kàng pèng zhuàng
T4 zì diǎn gōng jī	T4 bào lì pò jiě	T4 yán zhí
T4 cǎi hóng biǎo	T4 zhuàng kù	T4 mì mǎ pēn sǎ

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

T4 zuì zhǎng yǒu xiào qī	T4 zuì xiǎo cháng dù	T4 fù zá dù
T4 mì mǎ guǎn lǐ qì	T4 suǒ dìng	T4 mì mǎ lì shǐ
T4 zì dòng yùn xíng	T4 duō yīn sù shēn fēn yàn zhèng	T4 shēng wù tè zhēng

T4 acceptable use policy	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

T4 bǔ dīng	T4 fǎn è yì ruǎn jiàn	T4 kě jiē shòu shǐ yòng zhèng cè
T4 duān diǎn jiǎn cè yǔ xiāng yìng	T4 rù qīn zhǐ biāo	T4 zhǔ jī fáng huǒ qiáng
T5 zhù rù gōng jī	T5 guǎn lǐ xìng	T5 yìng yòng chéng xù

T5 Data validation	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 cān shù huà chá xún	T5 kuà zhàn jiǎo běn	T5 shù jù yàn zhèng
T5 mù lù biàn lì	T5 huǎn chōng qū	T5 huǎn chōng qū yì chū
T5 shǐ yòng zhōng shù jù	T5 chuán shū zhōng shù jù	T5 jìng tài shù jù

T5 regulated	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 gè rén shēn fèn xìn xī	T5 hé guī	T5 shòu jiān guǎn
T5 jī yú jué sè de fǎng wèn kòng zhì	T5 zhī fù kǎ xìn xī	T5 shòu bǎo hù jiàn kāng xìn xī
T5 qiáng zhì fǎng wèn kòng zhì	T5 zì zhǔ fǎng wèn kòng zhì	T5 jī yú guī zé de fǎng wèn kòng zhì

T5 principle of least privilege	T5 Cryptography	T5 plaintext
T5 key	T5 ciphertext	T5 keyspace
T5 Symmetric encryption	T5 AES	T5 block cipher

T5 míng wén	T5 mì mǎ xué	T5 zuì xiǎo quán xiàn yuán zé
T5 mì yào kōng jiān	T5 mì wén	T5 mì yào
T5 fēn zǔ mì mǎ	T5 gāo jí jiā mì biāo zhǔn	T5 duì chèn jiā mì

T5 Asymmetric encryption	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 gōng yào	T5 mì yào duì	T5 fēi duì chèn jiā mì
T5 ān quán shè jì	T5 tuǒ yuán qū xiàn mì mǎ xué	T5 sī yào
T5 tè shū zì fú	T5 shū rù qīng lǐ	T5 mò rèn ān quán

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

T5 shù jù xiè lù fāng hù	T5 mì guǎn	T5 shēn jì jì lù
		T5 SQL SQL zhù rù