NSCT Cyber Security Cheat Sheet

By the NSCT Exam Editorial Team · Updated 2026-11-24 · Facts checked against official sources on 2026-11-24

Cyber Security carries 5% of the NSCT according to HEC's Areas of Competencies, and 2026 candidates averaged 47.2% accuracy in it, per the HEC NSCT report and APP. Print this page and keep it next to your practice; definitions follow Stallings and the NIST and OWASP documents named in each table.

Key definitions

Term	One line
Confidentiality / integrity / availability	Only authorised parties read / no unauthorised change / timely access
Threat / vulnerability / risk	Potential for harm / the weakness it exploits / likelihood × impact
Passive vs active attack (X.800)	Eavesdropping, traffic analysis (prevent) vs masquerade, replay, modification, DoS (detect and recover)
Least privilege	Minimum rights for the minimum time
Defence in depth	Independent layers; an attacker must beat them all
AAA	Authentication (who), authorisation (what you may do), accounting (what you did)
Non-repudiation	Sender cannot later deny the message (needs a digital signature)
Salt	Random value stored with a hash so identical passwords hash differently
Zero-day	A flaw with no patch yet
Zero trust (NIST SP 800-207)	No trust from network location; every request is verified
Chain of custody	Every evidence hand-over named, timed and signed

Cryptography

	Symmetric	Asymmetric
Keys	One shared secret	Public + private pair
Examples	DES, 3DES, AES	RSA, Diffie-Hellman, ECC
Speed	Fast, bulk data	Slow
Keys for n users	$n(n-1)/2$	n key pairs
Main problem	Key distribution	Trusting the public key

Goal	Key used
Confidentiality	Encrypt with the receiver's public key; receiver decrypts with their private key
Digital signature	Sign with the sender's private key; verify with the sender's public key

- **Hash sizes:** MD5 128 bits, SHA-1 160, SHA-256 256; output length never depends on input length.
- **Wi-Fi:** WEP (RC4, 24-bit IV) broken; WPA2 uses CCMP (AES); WPA3 uses SAE.
- **Quantum:** Shor breaks RSA and ECC; Grover halves effective symmetric key length (AES-128 → about 64 bits).

Formulas

Formula	Variables and notes
RSA: $n = pq$, $\varphi(n) = (p-1)(q-1)$	p, q primes
$d = e^{-1} \bmod \varphi(n)$; $C = m^e \bmod n$; $m = C^d \bmod n$	e public exponent, d private
SLE = asset value × EF	EF = exposure factor (fraction lost)
ALE = SLE × ARO	ARO = expected occurrences per year

Formula	Variables and notes
Defence-in-depth pass rate = $p_1 \times p_2 \times \ldots$	Each layer's pass rate
Amplification factor = reply size ÷ query size	Reflection DDoS
Syslog PRI = facility × 8 + severity	Severity 0 (Emergency) to 7 (Debug)
FPR = FP ÷ (FP + TN); precision = TP ÷ (TP + FP)	Detection quality

Worked numbers to check yourself

Question	Answer
RSA p = 3, q = 11, e = 3, m = 4	n = 33, φ = 20, d = 7 (3 × 7 = 21 ≡ 1), C = 4^3 mod 33 = 31; 31^7 mod 33 = 4
10 users, symmetric keys	10 × 9 / 2 = 45
Asset 100,000, EF 25%, once every five years	SLE 25,000; ARO 0.2; ALE 5,000
Three layers passing 20%, 30%, 50%	0.2 × 0.3 × 0.5 = 3% get through
Facility 4 (auth), severity 2 (Critical)	PRI = 34

OWASP Top 10 (2021)

Rank	Category
A01	Broken Access Control
A02	Cryptographic Failures
A03	Injection (includes XSS)
A04	Insecure Design
A05	Security Misconfiguration
A06	Vulnerable and Outdated Components
A07	Identification and Authentication Failures
A08	Software and Data Integrity Failures
A09	Security Logging and Monitoring Failures
A10	Server-Side Request Forgery (SSRF)

Fixes: SQL injection → parameterised queries; XSS → context-aware output encoding plus CSP; CSRF → anti-CSRF tokens and SameSite cookies.

Models, phases and lists

Item	Remember
DAC / MAC / RBAC / ABAC	Owner grants / system labels / via roles / rules over attributes
Bell-LaPadula (confidentiality)	No read up, no write down
Biba (integrity)	No read down, no write up
Auth factors	Know, have, are (static biometric), do (dynamic biometric); MFA needs different categories
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
NIST SP 800-61 Rev. 2 IR	Preparation; Detection and Analysis; Containment, Eradication and Recovery; Post-Incident Activity
NIST SP 800-86 forensics	Collection, examination, analysis, reporting
Order of volatility (RFC 3227)	Registers and cache → RAM → temp files → disk → remote logs → physical config → archives
Shared responsibility	Customer patches the guest OS in IaaS; provider in PaaS and SaaS; customer always owns data and access

Item	Remember
Unix permissions	755 = rwxr-xr-x; 644 = rw-r--r--; umask 027 → files 640, dirs 750
Cyber law (principle level)	PECA 2016 criminalises unauthorised access even with no change, data interference, electronic fraud and identity misuse; learn principles, not section numbers

X vs Y quick distinctions

Pair	Difference
Authentication vs authorisation	Who you are vs what you may do
Hashing vs encryption	One-way, no key vs reversible with a key
MAC vs digital signature	Shared key, no non-repudiation vs private key, non-repudiation
IDS vs IPS	Out of band, alerts vs inline, blocks
Signature vs anomaly detection	Misses zero-days vs catches them with more false positives
Virus vs worm vs Trojan	Needs a host file vs spreads alone vs user installs it
Phishing vs pharming	Lure message vs poisoned name resolution
XSS vs CSRF	Abuses user's trust in the site vs site's trust in the browser
Vertical vs horizontal escalation	User to root vs user A to user B
Rogue AP vs evil twin	Unauthorised AP on the LAN vs fake AP copying an SSID
Type 1 vs Type 2 hypervisor	Bare metal (ESXi, Xen, Hyper-V) vs on a host OS (VirtualBox)
Precursor vs indicator	Attack may come vs attack may have happened
RPO vs RTO	Data you can afford to lose vs time restoration may take
SAST vs DAST	Reads code vs attacks the running app

Classic traps

1. Replay is an active attack, even though the message is genuine.
2. Password plus PIN is one factor, not two.
3. d is the inverse of e mod φ(n), not mod n.
4. "Once every five years" means ARO = 0.2, not 5.
5. Firewall rules are top-down, first match wins, so "deny all" goes last.
6. A VPN protects data in transit, not an infected endpoint.
7. Umask removes permissions; it is not the permission itself.
8. "Typed the correct address and still reached the fake site" is pharming.
9. Swapping the Bell-LaPadula and Biba rules.
10. A deny-list is almost always the distractor; choose allow-list, server-side validation.
11. Capture RAM before imaging the disk; a matching hash does not cure a custody gap.
12. SaaS does not move all security to the vendor; an explicit IAM Deny always wins.

Keep going

- Full explanations: Cyber Security revision notes
- All 16 topics and quizzes: Cyber Security MCQs hub
- Deep pages: OWASP Top 10, symmetric vs asymmetric encryption, cyber laws and ethics
- Timed practice: subject-wise mock test

Next step

Write the OWASP list and the key-use table from memory, then take a 20-question Cyber Security set in the subject-wise mock test. When you are ready for every subject at once, sit a full NSCT mock test.