Cheat - Sheet

Réseaux
Systèmes
Cybersécurité

⚠️ Règles d’or

- N’agis **jamais** sur un système dont tu n’as pas l’autorisation écrite.
- Documente tout : objectifs, scope, dates, comptes utilisés.
- Sauvegarde avant toute modification en production.
- Automatisation + idempotence : scripts répétables et réversibles.

---

01 - Concepts fondamentaux

- **Modèle OSI** : couche 1 (physique) → 7 (application). Savoir où agit un problème.
- **TCP vs UDP** : état de connexion, retransmission, utilités (TCP fiable, UDP léger).
- **Routage & Switching** : VLAN, trunking (802.1Q), STP, ACLs, VRF, BGP/OSPF
- **Adressage IP** : subnetting, CIDR, broadcast, gateway.
- **Services essentiels** : DNS, DHCP, NTP, LDAP/AD, SMTP, HTTP(S), RDP/SSH.
- **Principes de sécurité** : moindre privilège, défense en profondeur, segmentation, chiffrement end-to-end, journalisation.

---

02 - Réseaux - vérifications & dépannage rapide

(usage : administration / diagnostics en environnement contrôlé)

Informations interfaces

- Linux: `ip a` / `ip -s link` / `ss -tuln`
- Windows (PowerShell): `Get-NetIPAddress` / `Get-NetIPConfiguration` / `Get-NetTCPConnection`

Connectivité

- Ping basique : `ping <ip/hostname>`
- Route :
  - `ip route` / `route -n` / `traceroute <host>` (Linux)
  - `tracert <host>` (Windows)
- Ports ouverts :
  - `ss -tuln` (Linux)
  - `netstat -ano` (Windows)

DNS

- Linux: `dig @<server> <name> ANY` / `dig +short <name>`
- Windows: `nslookup <name> <server>`

Tests de performance

- Latence et débit (si dispo) : `iperf3` (client/serveur)
- Utilisation interface : `nload`, `iftop`, `vnstat`

Vérif. routage / tables

- Linux: `ip route show` / `ip rule show`
- Vérifier ARP: `ip neigh` / `arp -a`

---

03 - Sysadmin Linux - commandes utiles

- Infos système : `uname -a`, `lsb_release -a`
- Charge CPU/Mem : `top` / `htop` / `vmstat 1` / `free -h`
- Espace disque : `df -h` / `du -sh /path/*`
- Processus : `ps aux --sort=-%mem | head`
- Services : `systemctl status <service>` / `journalctl -u <service> -n 200`
- Logs courants : `/var/log/syslog`, `/var/log/messages`, `/var/log/auth.log`, `/var/log/secure`
- Gestion paquets :
  - Debian/Ubuntu `apt update && apt upgrade`
  - RHEL/CentOS `yum/dnf`
- Sudoers check : `sudo -l` (pour l'utilisateur courant)

---

04 - Sysadmin Windows - cmdlets & vérifs

- Infos système : `systeminfo`
- Services : `Get-Service -Name <name>` (PowerShell)
- Processus : `Get-Process | Sort-Object -Property CPU -Descending`
- Event logs : `Get-EventLog -LogName System -Newest 100` / `wevtutil qe System /c:100`
- Utilisateurs & groupes : `Get-LocalUser` / `Get-LocalGroupMember -Group "Administrators"`

---

05 - Sécurité - hardening rapide (checklist)

Systèmes

- Appliquer mises à jour OS + paquets critiques.
- Configurer **firewall host** (iptables/nftables, UFW, Windows Defender Firewall).
- Désactiver services inutiles.
- Sécuriser SSH : utiliser clés, désactiver root login, limiter utilisateurs, fail2ban.
- Mettre en place gestion des mots de passe / 2FA/MFA.

Réseau

- Segmenter réseau par VLAN ; séparer management / user / guests.
- ACLs sur switches/routeurs pour limiter flux non nécessaires.
- Bloquer SMB/RDP non nécessaires en edge.
- Utiliser VPN pour accès distant (IKEv2/strongSwan, OpenVPN, WireGuard).

Applications

- Mettre en place WAF (ex. ModSecurity) pour protection Web.
- Validations côté serveur (input validation, escaping).
- Utiliser CSP, HSTS, secure cookies.
- Scanner dépendances (SCA) pour vulnérabilités connues.

Auth / Identities

- Centraliser auth (AD/Azure AD/LDAP).
- MFA obligatoire pour accès sensibles.
- Revoir droits périodiquement (review access).

---

06 - Observabilité & détection

- **Centraliser logs** (ELK/EFK, Graylog, Splunk, Datadog).
- **Metrics** : Prometheus + Grafana pour infra, exporter (node_exporter).
- **Alerting** : règles claires (disk, CPU, error rate, auth failures).
- **IDS/IPS** : Suricata/Zeek/Suricata rules, sensor placement.
- **Endpoint detection** : EDR (CrowdStrike, SentinelOne, Elastic).
- **Baselines** : connaître le comportement normal pour détecter des anomalies.

---

07 - Réponse à incident (IR) - processus court

1. **Identifier** & isoler (containment).

2. **Collecter preuves** (logs, dumps) - préserver intégrité.
3. **Analyser** (scope, IOCs, TTPs).
4. **Éradiquer** (supprimer backdoors, patch).
5. **Rétablir** (restauration contrôlée).
6. **Post-mortem** & amélioration (lessons learned).

Outils IR courants

- `volatility` / `rekall` (memory forensics), `autopsy`/`sleuthkit`, `plaso` (timeline), `bulk_extractor`.

---

08 - Forensics - éléments à capturer

- Mémoire RAM (dump), images disque (dd/ewf), fichiers log, hash des fichiers, liste processus, connexions réseau, tâches planifiées, services, comptes utilisateurs récents, fichiers de démarrage.

---

09 - Cloud & virtualisation - points clefs

- **IAM** : least privilege, roles, policies.
- **Network** : Security Groups / NSG vs ACLs, private subnets, bastion hosts.
- **Storage** : chiffrer au repos, MFA Delete pour S3-like.
- **Logging & Monitoring** : CloudTrail/AzureActivity, CloudWatch/Azure Monitor, centraliser.
- **Patch management** : images AMI/VM golden + automation (Ansible/ARM/Terraform).
- **Secrets** : ne pas stocker en clair, utiliser Vault/Azure Key Vault/Secrets Manager.

---

10 - Pentest / CTF - méthodologie éthique (haut niveau)

1. **Reconnaissance passive** (OSINT, docs publiques).
2. **Reconnaissance active** (scan autorisé pour la portée définie).
3. **Enumération** (services, versions, users).
4. **Identification vulnérabilités** (CVEs, misconfig).
5. **Exploitation contrôlée** (uniquement dans scope).
6. **Post-exploitation & récupération** (documenter, capturer flags, cleanup).
7. **Rapport** (détails, PoC, recommandations).

Ne publie jamais d'exploits exploitables sans mitigation.

---

11 - Outils recommandés (catégories + exemples)

- **Recon / Scanning** : Nmap, Masscan (attention), Amass (subdomain), Shodan (OSINT).
- **Web** : Burp Suite (proxy), ZAP, Nikto, Gobuster/dirb.
- **Network analysis** : Wireshark, tcpdump, tshark.
- **Post-exploitation (lab only)** : Metasploit (use responsibly), PowerSploit (defensive review), LinPEAS/WinPEAS (priv esc checks).
- **Forensics/IR** : Volatility, Autopsy, FTK Imager, Sleuth Kit.
- **Monitoring** : Prometheus, Grafana, ELK/EFK, Suricata, Zeek.
- **Automation/Infra as Code** : Ansible, Terraform, Docker, Kubernetes.
- **Password/Hash tools (auth tests in scope)** : Hashcat, John (use with authorization).
- **EDR / AV** : Defender, CrowdStrike, SentinelOne (pour détection).

---

12 - Commandes utiles (exemples sûrs à usage admin / diagnostic)

> Toujours en environnement autorisé.

Network scan (info service)

- `nmap -sC -sV -oA scan-target <target>` → scan basique (scrips safe) *(utiliser uniquement dans scope autorisé)*

TCP/UDP listening

- `ss -tulnp` (Linux)
- `netstat -ano | more` (Windows)

Basic HTTP fetch

- `curl -I https://domain` → en-têtes HTTP
- `curl -v --resolve host:443:ip https://host/` → testing host header

Disk & memory

- `df -h` ; `du -sh /var/log/*` ; `free -h` ; `top`

Logs tailing

- `tail -F /var/log/syslog` ; `journalctl -f` ;
- Windows event viewer/`wevtutil`

---

13 - Hardening checklist rapide (ex. serveur Linux)

- Mettre à jour OS & paquets, activer unattended-upgrades si adapté.
- SSH : désactiver password auth, `PermitRootLogin no`, `AllowUsers`, port non-standard si besoin.
- Fail2ban / rate limiting.
- Configurer auditd, centraliser logs sur SIEM.
- Configurer firewall (nftables/iptables/ufw).
- Désactiver modules/services inutiles.
- Chiffrement disque (LUKS).
- Sauvegarde chiffrée et testée.

---

14 - Exemples de règles de détection (idéation, non-signature exacte)

- **Auth fail spike** : si échecs auth > X / 5 min → alerte.
- **New service on host** : démarrage d'un binaire non connu → signal.
- **Large outbound data** : trafic sortant vers IP non connue > seuil → alerte.
- **Unusual port listen** : nouveau service écoutant sur port inhabituel → enquête.

---

15 - Template court pour rapport technique

- Titre / identifiants, date, scope.
- Résumé exécutif (1 paragraphe).
- Méthodologie & autorisations.
- Observations (contexte, IOCs).
- Impact (CVSS/criticité).
- Preuves (logs, captures).
- Recommandations (priorisées).
- Annexes (commandes, configs, screenshots).

---

16 - Bibliothèques, ressources & formations

- OWASP Top 10, SANS Top 25, MITRE ATT&CK (TTPs).
- RFCs (RFC 791, 793, etc.), NIST SP800 series.
- Sites & cours : TryHackMe, HackTheBox (lab), SANS, Offensive Security (OSCP), Coursera/Azure/AWS security training.
- Livres : *Linux Hardening in Hostile Networks*, *Practical Malware Analysis*, *The Practice of Network Security Monitoring*.

---

17 - Checklists rapides imprimables

Avant mise en prod d'un service

- Auth & ACLs configurés
- TLS valide (HSTS)
- Logs centralisés
- Backups testés
- Scan vulnérabilité (SCA/DAST) réalisé

Si incident détecté

- Isoler la VM/hôte impacté
- Capturer mémoire (si suspect)
- Collecter logs & evidences
- Communiquer (stakeholders)
- Remediate & patch
