Audit-Forensic

Liste non exhaustive et à titre indicatif : RTFM !

Recherche d’indicateurs d'attaque et de compromission (IOA, IOC)

uptime (1)	- Indiquer depuis quand le système a été mis en route
free (1)	- Afficher la quantité de mémoire libre et utilisée du système
ps (1)	- Présenter un cliché instantané des processus en cours
pstree (1)	- afficher un arbre des processus
top (1)	- display Linux processes
pwdx (1)	- Afficher le répertoire de travail d'un processus
unhide (8)	- outil d'investigation post-mortem pour trouver des processus cachés
ip (8)	- show / manipulate routing, network devices, interfaces and tunnels
hosts (5)	- Table de correspondance statique des noms d'hôtes
ss (8)	- another utility to investigate sockets
unhide-tcp (8)	- forensic tool to find hidden TCP/UDP ports
lsof (8)	- list open files
mount (8)	- Monter un système de fichiers
lsmod (8)	- Show the status of modules in the Linux Kernel
modinfo (8)	- Show information about a Linux Kernel module
dmesg (1)	- Afficher et contrôler le tampon circulaire du noyau
systemctl (1)	- Control the systemd system and service manager
journalctl (1)	- Query the systemd journal
sysctl (8)	- Configurer les paramètres du noyau à chaud
sysctl.conf (5)	- Fichier de configuration et de chargement pour sysctl
whoami (1)	- Afficher l'identifiant d'utilisateur effectif
who (1)	- Montrer qui est connecté
w (1)	- Afficher les utilisateurs présents sur le système et leur activité
last (1)	- Afficher une liste des derniers utilisateurs connectés
passwd (1)	- Modifier le mot de passe d'un utilisateur
passwd (5)	- fichier des mots de passe
shadow (5)	- fichier des mots de passe cachés