9.2 Kali video / doc

Utilisés pour décoder ou récupérer un mot de passe
Ex : **John the Ripper**, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, et Medusa

--> https://www.youtube.com/watch?v=wj-moIzMJtI

Vulnérabilité du résolveur DNS Outils de piratage sans fil
Ex : **Aircrack-ng**, Kismet, InSSIDer, KisMAC, Firesheep et NetStumbler

--> https://www.youtube.com/watch?v=9bEovGdMPtc

Analyse et de piratage réseau sonder les périphériques réseau, les serveurs et hôtes pour les ports TCP ou UDP ouverts
Ex : Nmap, SuperScan, Angry IP Scanner, et NetScanTools

--> https://www.youtube.com/watch?v=dkmTVVmiG5A

Outils de création de paquets peut nécessiter le redémarrage du résolveur ouvert DNS ou des services
sonder et tester robustesse d'un pare-feu en utilisant des paquets spécialement conçus
Ex : Hping, Scapy, **Socat**, Yersinia, Netcat, Nping, et Nemesis

--> https://www.youtube.com/watch?v=vX5YZ1jO7Zo

Renifleurs de paquets l'acteur de menace envoie deux réponses ARP usurpées gratuitement en utilisant sa propre adresse MAC pour les adresses IP de destination indiquées.
Utilisés pour capturer et analyser les paquets au sein de LAN Ethernet ou WLAN
Ex : Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, et SSLstrip

--> https://www.youtube.com/watch?v=M0hZ5ko32is

Détecteurs de rootkit vérificateur d'intégrité des répertoires et des fichiers utilisé par les chapeaux blancs pour détecter les root kits installés.
Ex : AIDE, Netfilter et PF: OpenBSD Packet Filter

--> https://www.youtube.com/watch?v=ZtI4QhOZLNM

Fuzzers Générateurs de bruits pour rechercher des vulnérabilités
Ex : Skipfish, Wapiti, et W3af

--> https://www.youtube.com/watch?v=kIIeLA78E-k

Outils d'investigation : Utilisés par les pirates à chapeau blanc pour flairer toute trace de preuves existant dans un ordinateur
Ex : Maltego, Helix, Maltego, et Encase

-->

Débogueurs
Utilisés par les chapeaux noirs pour faire de l'ingénierie inverse sur des fichiers binaires lors de l'écriture d'exploits.
Attaquant doit usurper l'adresse IP d'un hôte prédire le numéro de séquence suivant et envoyer un ACK à l'autre hôte
également utilisés par les chapeaux blancs lors de l'analyse des logiciels malveillants
Ex : GDB, WinDbg, IDA Pro et **Immunity Debugger**

--> https://www.youtube.com/watch?v=iQf1OvTREvg

OS de piratage
OS spécialement conçus, préchargés avec des outils optimisés pour le piratage
Ex : Kali Linux, Knoppix, BackBox Linux

-->

Outils de chiffrement
coder les données afin d'empêcher tout accès non autorisé aux données cryptées
Ex : VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN et Stunnel

--> https://www.youtube.com/watch?v=J2JKh9mOy8U

--> https://www.youtube.com/watch?v=6CqT96d4-8Y

Outils d'exploitation des vulnérabilités
Déterminer si un hôte distant est vulnérable à une attaque de sécurité
Ex : Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, et Netsparker

--> https://www.youtube.com/shorts/jBTW8wWnkqU

Analyseurs devulnérabilité
Analysent un réseau ou un système pour identifier les ports ouverts
utilisé également pour rechercher vulnérabilités connues et analyser les MV, BYOD périphériques et BDD client
Ex : Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, et Open VAS

--> https://www.youtube.com/watch?v=EaA5pLAwnkc

--> https://www.youtube.com/watch?v=vvp_OnKjhik

Revision #2
Created 30 March 2026 14:12:43 by Raphaël
Updated 30 March 2026 15:20:43 by Raphaël