Audit du dˆ'pˆ·t ManInTheMiddle

Date: 2025-02-XX

1) Inventaire complet des fichiers (classˆ's par domaines/fonctions)

Scripts (shell)
- ‘client_traffic_capture.sh‘
- ‘fw.sh‘
- ‘fw_diagnostic.sh‘
- ‘mitm-sourcesvr.sh‘

Documentation
- ‘README.md‘

Frontend / statique (HTML)
- ‘linkedin_mitm_post.html‘
- ‘wifi-channels-guide.html‘
- ‘wifi-channels-guide-en.html‘

Configuration
- ‘.gitignore‘

Infra
- (aucun)

Backend
- (aucun)

Data
- (aucun)

Tests
- (aucun)

2) Fichiers clˆ's par domaine + usage

Scripts (shell)
- ‘mitm-sourcesvr.sh‘: script principal qui configure le routeur MITM (iptables, dnsmasq, hostapd), sauvegarde/restaure lâ ˆ'tat s
- ‘fw.sh‘: script â firewall strictâ pour iptables avec logging, rˆ¤gles de sˆ'curitˆ' restrictives, et support pour hotspot WiFi MITM.
- ‘fw_diagnostic.sh‘: script de diagnostic pour vˆ'rifier les rˆ¤gles iptables, lâ ˆ'tat des interfaces, la prˆ'sence de dnsmasq/hostap
- ‘client_traffic_capture.sh‘: script de capture rapide du trafic dâ un client, avec analyse basique (protocoles, ports, IPs) aprˆ¤s

Documentation
- ‘README.md‘: documentation trˆ¤s complˆ¤te orientˆ'e Kali Linux, avec prˆ'requis, explications techniques, ˆ'tapes dâ usage

Frontend / statique (HTML)
- ‘wifi-channels-guide.html‘: guide visuel complet (FR) sur les canaux WiFi.
- ‘wifi-channels-guide-en.html‘: guide visuel complet (EN) sur les canaux WiFi.
- ‘linkedin_mitm_post.html‘: page de prˆ'sentation (style â postâ) sur le projet.

Configuration
- ‘.gitignore‘: ignore des artefacts de logs, outputs, archives, etc.

3) Structure globale du projet

Points dâ entrˆ'e

- Principal: ‘mitm-sourcesvr.sh‘ (setup/restore MITM, DHCP, DNS, iptables).
- Complˆ'ments: ‘fw.sh‘ (firewall), ‘fw_diagnostic.sh‘ (diagnostic), ‘client_traffic_capture.sh‘ (capture ponctuelle).

Modules principaux (logiques)
- **Routage + NAT + DNS**: gˆ'rˆ' par iptables dans ‘mitm-sourcesvr.sh‘ et renforcˆ' par ‘fw.sh‘.
- **DHCP**: gˆ'rˆ' via ‘dnsmasq‘ (config gˆ'nˆ'rˆ'e ˆ la volˆ'e).
- **Hotspot WiFi**: gˆ'rˆ' via ‘hostapd‘ (config gˆ'nˆ'rˆ'e ˆ la volˆ'e).
- **Logging & sauvegarde dâ ˆ'tat**: crˆ'ation de logs et backups pour restauration.

Flux de donnˆ'es (haut niveau)
1. Lâ opˆ'rateur lance ‘mitm-sourcesvr.sh --exec‘ pour initialiser le MITM.
2. Le script configure les interfaces (LAN/WIFI), iptables (NAT + FORWARD), et lance dnsmasq/hostapd.
3. Le trafic des clients est routˆ' vers le WAN, avec redirection DNS transparente.
4. Les logs et captures (manuelles) sont stockˆ's localement dans ‘logs/‘ et ‘results/‘.
5. Sur arrˆ“t (‘--stop‘), le script restaure lâ ˆ'tat systˆ¤me.

Dˆ'pendances majeures
- Systˆ¤me/rˆ'seau: ‘iptables‘, ‘iproute2‘, ‘sysctl‘, ‘dnsmasq‘, ‘hostapd‘, ‘iw‘, ‘rfkill‘, ‘tshark‘ (recommandˆ'), ‘tcpdump‘.
- Utilitaires: ‘curl‘, ‘jq‘, ‘dig‘ (pour ‘fw.sh‘), ‘systemd‘ pour logging.

4) API & endpoints
- Aucune API web (FastAPI/Flask/Express/etc.) dˆ'tectˆ'e.

5) Scripts .sh (dˆ'tails dâ usage)

‘mitm-sourcesvr.sh‘
- Usage principal: ‘sudo ./mitm-sourcesvr.sh --exec‘ (ou ‘--start‘), ‘sudo ./mitm-sourcesvr.sh --stop‘.
- Rˆ·le: configuration complˆ¤te du MITM (iptables, DNS, DHCP, WiFi hotspot).
- Gˆ'nˆ¤re: configs temporaires ‘dnsmasq‘/‘hostapd‘, backups dâ ˆ'tat, logs.

‘fw.sh‘
- Usage: ‘sudo ./fw.sh‘.
- Rˆ·le: firewall strict avec journalisation, gestion DNS/HTTPS/NTP/SSH, rˆ¤gles spˆ'cifiques pour hotspot WiFi MITM.
- Dˆ'pendances: iptables, curl, jq, dig.

‘fw_diagnostic.sh‘
- Usage: ‘sudo ./fw_diagnostic.sh <IP_IPTV>‘.
- Rˆ·le: diagnostic complet des politiques iptables, NAT, interfaces, services et logs.

‘client_traffic_capture.sh‘
- Usage: ‘sudo ./client_traffic_capture.sh <IP_CLIENT>‘.
- Rˆ·le: capture tcpdump 30s + analyse rapide du trafic (protocoles/ports/IP).

6) Scripts .py
- Aucun fichier ‘.py‘ dˆ'tectˆ'.

7) Duplications, conflits potentiels, obsolescence
- **README vs script rˆ'el**: le README fait rˆ'fˆ'rence ˆ ‘mitm-clientmitm-capture.sh‘ alors que le dˆ'pˆ·t contient ‘mitm-source
- **Nom dâ usage incohˆ'rent**: ‘client_traffic_capture.sh‘ mentionne ‘./capture-client.sh‘ dans lâ usage, ce qui ne correspond p
- **.gitignore**: le pattern ‘*.html‘ ignore potentiellement des pages statiques utiles qui sont dˆ'jˆ versionnˆ'es dans le dˆ'pˆ·t.
- **Redondance**: deux guides WiFi (FR/EN) ont un contenu similaire (acceptable si ciblage multi-langues).

8) Tableau synthˆ'tique des fichiers

Fichier	Usage
‘README.md‘	Documentation complˆ¤te dâ installation, usage, et dˆ'pannage MITM.

‘mitm-sourcesvr.sh‘	Script principal: configure NAT/DHCP/DNS/hotspot pour MITM.
‘fw.sh‘	Script firewall strict avec logging et exceptions contrˆ·lˆ'es.
‘fw_diagnostic.sh‘	Diagnostic iptables/services/rˆ'seau.
‘client_traffic_capture.sh‘	Capture courte du trafic client + analyse rapide.
‘linkedin_mitm_post.html‘	Page statique de prˆ'sentation du projet.
‘wifi-channels-guide.html‘	Guide FR des canaux WiFi.
‘wifi-channels-guide-en.html‘	Guide EN des canaux WiFi.
‘.gitignore‘	Ignore logs/outputs/archives/fichiers gˆ'nˆ'rˆ's.

9) Tableau des endpoints
- N/A (aucune API dˆ'tectˆ'e).