Herramientas para Osint Ofensivo – Pentesting Web

ReadMe: En este documento se presenta una lista de herramientas OSINT utilizadas para realizar tareas de reconocimiento en pruebas de penetración orientadas a servicios web. El uso de estas herramientas, junto con el procesamiento y análisis de la información obtenida, permite desarrollar una fase de reconocimiento eficiente como base para la posterior etapa de penetración en la infraestructura.

🌐 Whois

👉 https://www.kali.org/tools/whois/

👉 https://centralops.net/co/

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/domain/<domain>/whois

🌐 DNS

👉 https://search.dnslytics.com

👉 https://dnsdumpster.com/

👉 https://www.kali.org/tools/dnsrecon/

👉 https://dnschecker.org/all-dns-records-of-domain.php

👉 Dig Linux Tools (*sudo apt install dnsutils*)

👉 Nslookup Linux Tool (*sudo apt install dnsutils*)

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/domain/<domain>/passive_dns

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/IPv4/<ip >/passive_dns

🌐 IP

👉 Nslookup Linux Tool (*sudo apt install dnsutils*)

👉 Mtr Linux Tools (*sudo apt install mtr*)

👉 Traceroute (*sudo apt install traceroute*)

👉 https://ip-api.com

👉 https://domaintoipconverter.com/

🌐 GEO

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/domain/<domain>/geo

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/IPv4/<ip>/geo

👉 curl -sX GET https://api.hackertarget.com/geoip/?q=<ip>

🌐 Technologies

👉 https://www.kali.org/tools/whatweb/

👉 https://www.wappalyzer.com/ (Wappalyzer - Technology profiler)

🌐 URLS List

👉 curl -sX POST https://utlscan.io/api/v1/scan/ \

-H “Content-Type: application/json” \

-H “API-Key: YOUR-API-KEY-HERE“ \

-d “{\”url\”: \”DOMAIN-HERE\”, \”visibility\”: \”public\”, \”tags\”: [\”demotag1\”, \”demotag2\”]}” \

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/domain/<domain>/url_list

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/IPv4/<ip>/url_list

👉 curl -sX GET https://web.archive.org/cdx/search/cdx?url=<domain>/*&collapse=urlkey&output=text&fl=original

👉 site:*.domain.com inurl:domain.com

🌐 Subdomains

👉 https://crt.sh

👉 https://osint.sh/subdomain/

👉 https://www.merklemap.com/search?query=<domain>&page=0

👉 curl -N -G https://api.merklemap.com/search -d query=<domain> -d page=0

👉 https://sslmate.com/ct_search_api/

👉 https://github.com/UnaPibaGeek/ctfr

👉 curl -sX GET https://otx.alienvault.com/api/v1/indicators/domain/<domain>/passive_dns

👉 https://www.kali.org/tools/theharvester/

👉 https://www.nmmapper.com/

👉 site:*domain.com, site:domain.com -www, site:*.pagina.*

🌐 Dorks (Google - Duckduckgo)

👉 [GOOGLE] https://ahrefs.com/blog/google-advanced-search-operators/

👉 [DUCKDUCKGO] https://duckduckgo.com/duckduckgo-help-pages/results/syntax

👉 https://dorksearch.com/

🌐 Emails

👉 https://github.com/FeathersMcgr4w/emails-from-domain

👉 https://www.zoominfo.com/s/search

👉 https://rocketreach.co/

👉 https://www.apollo.io/

👉 https://intelx.io/tools?tab=email

👉 https://snov.io/es/buscador-de-correo-electronico

👉 https://emailrep.io/free

👉 https://www.predictasearch.com/

👉 https://github.com/megadose/holehe

👉 site:dominio.com “@dominio.com”, "email" “@dominio.com”, "contacto" “@dominio.com”, "correo electrónico" “@dominio.com”

👉 https://emkei.cz/

🌐 Linkedin

👉 https://github.com/FeathersMcgr4w/find-linkedin-employees

👉 https://github.com/m8sec/CrossLinked

👉 "founder" "domain.com" "linkedin", “ceo” “dominio.com”

🌐 Directory Listing

👉 https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files

👉 https://www.kali.org/tools/wfuzz/ (*sudo apt install wfuzz*)

👉 https://www.kali.org/tools/ffuf/ (*sudo apt install ffuf*)

🌐 Port Scan

👉 https://www.kali.org/tools/nmap/ (*sudo apt install nmap*)

👉 https://pentest-tools.com/network-vulnerability-scanning/port-scanner-online-nmap

🌐 SSL Scan

👉 https://www.websiteplanet.com/webtools/ssl-checker

👉 echo | openssl s_client -connect <domain:443> -servername <domain> 2>/dev/null | openssl x509 -noout -subject -issuer -dates -ubjectAltName

🌐 Search Engines

👉 https://www.shodan.io/

👉 https://en.fofa.info/

👉 https://search.censys.io/

🌐 Proxys

👉 https://portswigger.net/burp/communitydownload

👉 https://www.mitmproxy.org/

🌐 Metadata

👉 https://exiftool.org/ (*sudo apt install exiftool*)

👉 https://fotoforensics.com/

🌐 WordPress

👉 https://www.kali.org/tools/wpscan/ (*sudo apt install wpscan*)

🌐 Leaks

👉 https://leak-lookup.com

👉 https://www.snusbase.com

👉https://breachdirectory.org

👉https://leaked.domains

👉https://es.scribd.com/document/606059745/Cuentas-Comprometidas-04-2022-Informe-Argentina

🌐 OsintTool

👉 https://github.com/FeathersMcgr4w/osintTool

👉 https://osint-ui.com/

👉 https://www.kali.org/tools/recon-ng/ (*sudo apt install recon-ng*)

👉 https://www.maltego.com/

👉 https://www.kali.org/tools/sherlock/ (*sudo apt install sherlock*)

🌐 Cheat Sheets

👉 https://github.com/coffinxp/payloads/tree/main

👉 https://github.com/kongsec/Wordpress-BruteForce-List/blob/main/

👉 https://github.com/H4ckD4d/FOFA-Syntax-Guide-for-OSINT-Queries

👉 https://www.stationx.net/how-to-use-shodan/

👉 https://github.com/lanmaster53/recon-ng-marketplace/wiki/API-Keys

🌐 Converter online

👉 https://codebeautify.org/ascii-to-text

👉 https://codebeautify.org/hex-decimal-converter

👉 https://cyberchef.org/

🌐 Word, excel, pdf viewer

👉 https://products.aspose.app/words/viewer

👉 https://products.aspose.app/cells/viewer

👉 https://products.aspose.app/pdf/viewer

🌐 Osint resources

👉 https://github.com/jivoi/awesome-osint

👉 https://ohshint.gitbook.io/oh-shint-its-a-blog/osint-web-resources/digital-network-intelligence-dnint

🌐 Payloads 4Pentest

👉 https://github.com/swisskyrepo/PayloadsAllTheThings/

🌐 Cuit Online

👉 https://www.cuitonline.com/

👉 https://www.dateas.com/es/consulta_cuit_cuil

🌐 Cracking online

👉 https://crackstation.net/

[📡] Contacto

[📎] https://www.linkedin.com/in/david-padron-9a74aa323/

[📎] https://github.com/FeathersMcgr4w

[📎] https://feathersmcgr4w.github.io/cyber-portfolio/