Escaneo

- Adquisitions
- AS
- bgp.he.net
- Whois
- Lookups
- Built With
- Git hub "api key palabras claves"
- Hakrawler
- Sublist3er
- SubDomainer
- gospaider
- HTTPprobe
- Eyewithnees
- port table
- Web Tecnology
- Wafwoof
- Ip4info
- Visualping
- Filebunty
- Grammaly
- Aplicacion en pre produccion (crt.sh busca subdominio (nslookup el subdominio si no sale nada es por que no a creado el registro dns de ese dominio)) luego ahi que bsucar en cencys.io el odminio o subdominio ahi que sacar la dirrecion ip luego modificar nuestro archivos nano /etc/host   meter la ip y el dominio intendificado
- Codigo 300 redi, 404 y 500 bay,goburter
- Navegadores.Google,Yahoo,Bing,Ask,DuckDuckGo,Startpage,Yandex,Gibiru,Microsoft Academic,
- Bru forzy
- Shodan,Zoomey
- Escaneo Historico
- Crt.sh
- Nslookup
- Wiew.dns
- Dns.dumpster busca sub dominio
- The harvester
- Metadatos
- Nmap -Script nmap http.vulner-regex.n (namp)-/usr/share/nmap/scripts -metodo.nse   (nmap -vv -Pn -sT -p 80 --script htt-methods.nse dominio)
- Abouthisite.com
- Archivo.org
- exif metadatos
- typo error de tipeo
- Metabuscadores-Zapmeta,Dogpile,Yippy,Metacrawler,iBoggie,Indeed
- robots.txt-sitemap.xml
- wget
- trace rout
- bloque de ip fuera de estados unidos
- ip verdadera detras de cloud-viewdns.info
- Copias de serudiad de diferentes archivos
- http-config-backup
- Censys

google haking
Hackredns
cache pag caidas
VPS
Aquatone
pester monkey shel diferentes etc
Saber la version server ACL.
IDS,IPS HARDERING
Versionde server nwes.nectcraft.com
gospaider
gobuaster,wfuzzw(secret.list)
Analisis de codigo fuente pagina estatica
Ficheros de las tecnogologias especificas
Mailineitor
Certificados -SSL-TLS-script en nmap
MXToolBox
Transferencia de zona (dig-dominio -t ns(dig axfr dominio servidor de nombre)) dnsnum (host -t ns dominio devuelve los servidores dns) host -l dominio el servidor dns nombre
Mala configuracion de proxy
Servidores smtp,ftp,dns,servidor web
TLD dnsrecon -t tld -d dominio (saca los diferentes extenciones de dominnio d ela empresa)
ICMP
ARP
Domdominio.com
whoxy.com saca los dominio registrado por la misma persona
amass (amasss intel --asn 9619)
subdomainer
inpecionar la consola
ISP empresa de internet cual es mi ip
Ciberchef
Malas praticas de programacion
Zap
dcode.fr/indetifica
hexaeditor
ping -c el dominio o la ip -R
snmwalk -c public -v seria la version y luego la ip
smb nmap script reconocer
theharvester -d dominio -b (nc)
Escaneo de redes no tan protegidas asn se busca en shodan net:la ip
Escaneo historico de red
dnsreconm -r el rango de ip -t rvl (esto es para scar y verificar si las ip pertenecen a la empresa)
dnsrecon -d dominio(enumera todos los campos de ahi se saca servidor de correo mx para hacer el atauqe smtp)