Auditoria de seguridad Cheat Sheet

by Davomeist via cheatography.com/208487/cs/44676/

Reconociemiento DNS

nslookup	ip o dominio	realiza la traduccion de nombre a ip y vicebersa
dig	ip o dominmio	obtener inform-ación sobre los servidores de nombres, direcc-iones de host, puertas de enlace
whois	ip o dominmio	btener inform-ación de cualquier nombre de dominio del mundo
tracert	ip o dominio	lista los nodos atravesados para llegar al destino

Comandos de descubrimiento NMAP

Escaneo de ping	nmap -sP [objetivo]
Sin ping	nmap -PN [objetivo]
TCP SYN Ping	nmap -PS [objetivo]
TCP ACK ping	nmap -PA [objetivo]
UDP ping	nmap -PU [objetivo]
SCTP Init Ping	nmap -PY [objetivo]
ICMP echo ping	nmap -PE [objetivo]
ICMP Timestampnmap -PP ping	nmap -PP [objetivo]
ICMP addressnmap -PM mask ping	nmap -PM [objetivo]
IP protocol ping	nmap -PO [objetivo]
ARP ping	nmap -PR [objetivo]

Herramientas SMB

istar recursos compartidos en un host específico	smbmap -H [objetivo]
con autenticacion	smbmap -H [objetivo] -u [usuario] -p [contr-asena]
enumerar usuarios	smbmap -H [objetivo] -u [usuario] -p [contr-asena] -e
listar recursos compartidos	smbclient -L //SERVER -N

Webs de reconociemiento pasivo

dumpst-er.com	descubrimiento de servidores en base al dominio
shodan.io	motor de busqueda de dispositivos de red
phoneb-ook.cz	lista dominios y correos asociados a un dominio principal
hunter.io	buscador de direcciones de mail
verifyema-iladdr-ess.org	verificador de direcciones de email
email-che-cker.net	verificador de direcciones de email
dashed.com	credenciales y brechas de seguridad

Deteccion de versiones con NMAP

Sistema operativo	nmap -O [objetivo]
Intentar adivinar el sistema operativo	nmap -O --ossca n-guess [objetivo]
Version de los servicios	nmap -sV [objetivo]
Troubleshooting de version de servicios	nmap -sV --vers-ion-trace [objetivo]
Escaneo RCP	nmap -sR [objetivo]

Tecnicas de evasion de firewall NMAP

Fragmentacion de paquetes	nmap -f [objetivo]
Especificar el MTU	nbmap -mtu [MTU] [objetivo]
Usar un decoy	nmap -D RND [numero] [objetivo]
Escaneo zombie	nmap -sl [zombie] [objetivo]
Especificacion manual de puerto	nmap --source-port [port] [target]
Spoofing de MAC	nmap --spoof-mac [mac] [objetivo]

Herramientas de reconocimiento

Clearbit connect	extension de chrome para la busqueda de emails
Wapalyzer	extension de firefox para el analisis web
CTRF (github)	programa de busqueda de subdominios basado en transparencia de certificados
Motores de busqueda	Google, firefox etc..

Comandos basicos de hidra

ataque de fuerza bruta a ssh	hydra -l usuario -P /ruta/a/list-a_de_contraseñas.txt ssh://-ip_del_objetivo
ataque de fuerza bruta a ftp	hydra -l usuario -P /ruta/a/list-a_de_contraseñas.txt ftp://ip_-del_objetivo
ataque con lista de usuarios	hydra -L /ruta/a/lista_de_u-suarios.txt -P /ruta/a/lista_d-e_contraseñas.txt

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

Comandos basicos de hidra (cont)

ataque con conexiones concurrentes	hydra -l usuario -P /ruta/-a/lista_de_contraseña-s.txt -t 4
ataque con timeout	hydra -l usuario -P /ruta/-a/lista_de_contraseña-s.txt -s 5

Uso basico de gobuster

busqueda de subdir-ectorios	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt
enumer-acion de archivos por directorio	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -x php,html
enumer-acion de subdom-inios	obuster dns -d dominio.com -w /ruta/a/lista_de_subdomi-nios.txt
filtrar por codigo de estado http	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -s "200,204,3-01,302"
escaneo recursivo	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -r
con uso de proxy	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -p http://12-7.0.0.1:8080

Uso basico de gobuster

busqueda de subdir-ectorios	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt
enumer-acion de archivos por directorio	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -x php,html
enumer-acion de subdom-inios	obuster dns -d dominio.com -w /ruta/a/lista_de_subdomi-nios.txt
filtrar por codigo de estado http	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -s "200,204,3-01,302"
escaneo recursivo	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -r
con uso de proxy	gobuster dir -u http://ip_de-l_objetivo -w /ruta/a/lista_d-e_palabras.txt -p http://12-7.0.0.1:8080

By **Davomeist**
cheatography.com/davomeist/

Not published yet.
Last updated 15th October, 2024.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com