(algunes) Eines Kali

Exploitation tools (eines d'explotació)

DNSMap. Es un mapejador de la xarxa, normalment es coneix com Força Bruta per a Subdominis, originàriament publicat en el 2006, utilitzat per pentesters durant la recopilació d'informació/enumeració en la fase d'avaluació de la seguretat de la infraestructura. És una eina programada en Python de codi obert.

Metasploit. És una eina per trobar, validar i explotar vulnerabilitats en equips d'una xarxa. Proporciona les eines per realitzar proves de penetració i auditories de seguretat, i ens retorna la informació dels ports oberts i també les vulnerabilitats que puguin tenir els serveis trobats en aquests ports. Es un framework que està molt actualitzat, per tal que estigui sempre al dia de les últimes vulnerabilitats. Com a framework té moltes possibilitats i val la pena conèixer moltes de les funcionalitats que té.

Sqlmap. És una eina per realitzar injecció sql automatitzada i s'usa per detectar i aprofitar les vulnerabilitats en aplicacions web i la presa de control dels servidors de bases de dades. Les opcions que té l'usuari són enumerar els usuaris, els hashes de contrasenyes, els privilegis, les bases de dades, fer bolcat de taules ...

Forensics tools

Binwalk: xafardejar firmware
Bulk-extractor: per targetes de crèdit, email ….

Information gathering (recollida d'informació)

Nikto. Es una aplicació tipus escaner de servidor web, de codi obert, amb llicència tipus GPL i serveix per a realitzar proves exhaustives contra servidors web. Detecció de programes potencialment perillosos, verificació de versions desactualitzades i problemes específics. Provarà un servidor web en el menor temps possible, i es mostra en els fitxers de registre o en un IPS/IDS.

Xplico. Extreu d'una captura de trànsit d'internet les dades contingudes referents a aplicacions. Com a exemple, és capaç d'extreure d'un arxiu pcap cadascun els protocols de correu usats, els continguts HTTP, trucadees VoIP, FTP, TFTP, entre moltes altres. És una eina de codi obert classificada com a Network Forensics Analisis Tool (NFAT) tot i que el mateix programa es defineix com a Internet Traffic Decoder.
https://tools.kali.org/information-gathering/xplico
https://www.xplico.org/about

apache-users. És un script escrit en Perl que serveix per enumerar els noms d'usuari de qualsevol sistema que utilitzi el mòdul UserDir d'Apache.
Exemple:
apache-users -h 192.168.1.202 -l /usr/share/wordlists/metasploit/unix_users.txt -p 80 -s 0 -e 403 -t 10

Mitmproxy. Aplicació de codi obert proxy que permet l'interceptació (lectura, modificació i gravació per anàlisi) de connexions HTTP i HTTPS entre qualsevol client HTTP (S) (mòbil, ordinador) i un servidor web.
Font: Ciberlider Blogspot: https://cyberlider.blogspot.com/2016/03/como-utilizar-mitmproxy-para-leer-y.html
Altra font: Document descriptiu d'us de Mitmproxy
https://buildmedia.readthedocs.org/media/pdf/mitmproxy/v2.0.2/mitmproxy.pdf

adicionalmente
https://tools.kali.org/sniffingspoofing/mitmproxy

mitmproxy es un proxy HTTP man-in-the-middle con capacidad SSL. Proporciona una interfaz de consola que permite que los flujos de tráfico sean inspeccionados y editados sobre la marcha.

caracteristicas:

- interceptar y modificar el tráfico HTTP sobre la marcha
- guardar conversaciones HTTP para su posterior reproducción y análisis
- reproducir tanto clientes como servidores HTTP
- hacer cambios en el script al tráfico HTTP usando Python
- Certificados de intercepción SSL generados sobre la marcha

Nmap. És una eina per a l'exploració de vulnerabilitats i la detecció de xarxes. Permet identificar quins dispositius s'estan executant en els seus sistemes, descobrir els hosts disponibles i els serveis que ofereixen, trobar ports oberts i detectar riscos de seguretat. També disposa d'una interfície gràfica d'usuari anomenada Zenmap.

SSLyze. Eina escrita en python que analitza la configuració SSL d'un servidor connectant-se a ell. Permet detectar configuracions errònies que puguin afectar als servidors (cyphersuites vulnerables, renegociacions insegures, vulnerabilitats dels exploits CRIME, Heartbleed, etc.) i fer proves de rendiment. Compatible amb versions 2.0/3.0 d'SSL i 1.0/1.1/1.2 de TLS.

Password attacks

Mimikatz. És una eina post-explotació de codi obert que extreu informació del servei LSASS com poden ser contrasenyes, hashes y tickets de Kerberos i tb altres tipus d'atacs. Va ser escrit per el francés Benjamin Delpy l'any 2011.

John the Ripper. És un programa de criptografia que aplica força bruta per a desxifrar contrasenyes. És capaç de trencar diversos algorismes de xifrat o hash, com DES, SHA-1 i uns altres. És una eina de seguretat molt popular, ja que permet als administradors de sistemes comprovar que les contrasenyes dels usuaris són prou bones. John the Ripper és capaç de autodetectar el tipus de xifrat de molts disponibles, i es pot personalitzar el seu algorisme de prova de contrasenyes. Això ha fet que sigui un dels més usats en aquest camp.

Hydra. És un programa que permet realitzar de forma molt nombrosa i en paral·lel atacs de força bruta contra diferents serveis per aconseguir acces a un sistem remotament: Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

A la sintaxi per terminal es pot indicar el tipus de servei, el fitxer que conté els usuaris i/o contrasenyes a utilitzar, la quantitat de tasques que volem executar en paral·lel i el port entre d'altres.

Exemple: hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 ssh://192.168.1.123
-l: usuri root
-P fitxer que conte els password
-t: numero de tasques, 6
ssh://192.168.1.123 servei que es vol explotar (ssh al port per defecte, 22) i adreça ipv4 del servei

Vulnerability analysis (anàlisi de vulnerabilitats)

Cuckoo. És un sistema d'anàlisi de programari maliciós. Podeu llençar-hi qualsevol fitxer sospitós i, en qüestió de segons, Cuckoo us proporcionarà resultats detallats en què es descriu el que va fer aquest fitxer quan s'executava en un entorn aïllat.

Wapiti. És una eina de línia de comanda que permet automatitzar auditoria WEB (escàner de vulnerabilitats WEB), aquesta eina inclou mòduls per detectar diferents tipus de vulnerabilitats com són: file disclosure, injection, xss, ...

Web applications

Wpscan. És un software escrit en Ruby utilitzat per realitzar tests de vulnerabilitats en aplicacions fetes amb Wordpress. Entre altres funcions escaneja plugins, temes,usuaris o atacs de força bruta contra la password dels usuaris.

KALI Nethunter. És una plataforma de prova de penetració d'Android de codi obert per a dispositius Nexus, creada entre el membre de la comunitat de Kali "BinkyBear" i Offensive Security. NetHunter admet la injecció de paquets 802.11, configuracions MANA Evil Access Point, el teclat HID (atacs tipus Teensy), així com els atacs BadUSB MITM

Soportada en dispositius Nexus 5, Nexus 6, Nexus 7, Nexus 9, Nexus 10 o OnePlus One.

Reaver. Implementa un ataque de fuerza bruta contra los PINs de los registradores de Wifi Protected Setup (WPS) para recuperar las frases de contraseña WPA/WPA2, como se describe en este documento.

Reaver ha sido diseñado para ser un ataque robusto y práctico contra WPS, y ha sido probado contra una amplia variedad de puntos de acceso e implementaciones de WPS.

En promedio, Reaver recuperará la frase de contraseña WPA/WPA2 de texto plano del AP de destino en 4-10 horas, dependiendo del AP. En la práctica, generalmente toma la mitad de este tiempo adivinar el pin WPS correcto y recuperar la frase de contraseña.

SlowHTTPTest. És una eina altament configurable que simula alguns atacs de denegació de serveis de la capa d'aplicacions. Funciona a la majoria de plataformes Linux, OSX i Cygwin: un entorn similar a la interfície i línia de comandes per a Microsoft Windows.

W3AF. 'W3AF' (**Web Application Attack and Audit Framework**) és una eina per identificar i explotar vulnerabilitats a aplicacions web. Es pot usar des d'una consola o amb una interfície gràfica. Tant el seu nucli com a tots els seus complements (més de 130) estan escrits en Python. Algunes de les seves funcions són: SQL injection, cross site scripting, inclusió remota d'arxius, etc.

https://tools.kali.org/sniffingspoofing/mitmproxy

mitmproxy es un proxy HTTP man-in-the-middle con capacidad SSL. Proporciona una interfaz de consola que permite que los flujos de tráfico sean inspeccionados y editados sobre la marcha.

caracteristicas:

- interceptar y modificar el tráfico HTTP sobre la marcha
- guardar conversaciones HTTP para su posterior reproducción y análisis
- reproducir tanto clientes como servidores HTTP
- hacer cambios en el script al tráfico HTTP usando Python
- Certificados de intercepción SSL generados sobre la marcha