Esercitazione W10D1 - Pratica 2

Info Gathering

Fabio Benevento - 10/01/2024

Traccia

Nell'esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta.
Lo scopo di questo esercizio è più che altro familiarizzare con i tool principali della fase di information gathering, quali:
- Google, per la raccolta passiva delle info
- dmirty
- Recon-ng
- Maltego

Alla fine dell'analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato:
- Il target
- Le query utilizzate (dove applicabile)
- I moduli utilizzati (dove applicabile)
- I risultati ottenuti

Implementazione

Per esercitazione ho continuato con la raccolta di informazioni relativamente al sito della precedente esercitazione (offuscato per motivi di privacy) utilizzando tool alternativi come dmirty, Recon-ng e Maltego.
La seguente tabella riporta i risultati ottenuti dallo scanning.

Tool	Versione	Strumento/Modulo	Risultati
Maltego	4.6.0 CE	Transform To DNS Name - MX (mail server)	Ritrovati info sui server mail dell'organizzazione

Maltego	4.6.0 CE	Transform To IP Address	Ricavato IP address del server mail precedente
Maltego	4.6.0 CE	Transform To Entities From WHOIS [IBM Watson]	Ricavate info come Location/Phone number/Email address
Maltego	4.6.0 CE	Transform To CPE	Ricercate vulnerabilità
Maltego	4.6.0 CE	Transform To CVE	Ricercate vulnerabilità
Dmirtry	1.3a	-w	loockup dominio
Dmirtry	1.3a	-i	lookup IP address
Dmirtry	1.3a	-n	informazioni dell'host tramite Netcraft
Dmirtry	1.3a	-s	ricerca sottodomini
Dmirtry	1.3a	-e	ricerca indirizzi email
Dmirtry	1.3a	-p	ricerca porte TCP aperte
Recon-ng		brute_hosts	ricerca dei record DNS e indirizzi IP tramite brute-force di possibili nomi a partire dal dominio
Recon-ng		mx_spf_ip	hostname e dominio email server
Recon-ng		hackertarget	ritrovati gli hostname e le info relative mediante le API di HackerTarget.com
Recon-ng		interesting_files	trovate informazioni su file robots.txt e phpinfo.php

Fare riferimento alla versione estesa per maggiori informazioni