Fasi dell'hacking

1.Fase di Ricerca/ Ricognizione

Ricognizione Passiva

-utilizzo di motori di ricerca
-utilizzo di social media (es linkedin/ facebook ecc
-Utilizzo di Shodan
-dnsdumpster.com
-Utilizzo di Record Dns

Lista comandi

nslookup (record AAAA, A , TXT , MX ,) TYPE

dig ,

whois

Ricognizione Attiva

L'HACKER PUÒ LASCIARE DELLE TRACCIE CHE SONO RILEVATE DAI SISTEMI DI DIFESA DEL DIFENSORE (IDS / IPS)

PING (USA ICMP) PER CONTROLLARE SE UN HOST È ATTIVO. NOTA UN HOST PUÒ ESSERE ATTIVO MA NON RISPONDERE AI PACCHETTI ICMP

TRACEROUTE/TRACERT-> questo comando traccia tutto il percorso, quindi tutti i router che sono coinvolti dalla sorgente(l'hacker) , fino al destinatario(vittama) , usato per scoprire se ci sono dei FIREWALL

NMAP , PER SAPERE AD ESEMPIO QUALI PORTE/SERVIZI SONO ATTIVI SULLA VITTIMA . ESEMPIO PORTA 3389 ,22 ,25 , ECCC
POSSO UTILIZZARE L'OPZIONE -sS per cercare di eludere gli IPS

2- BANNER GRABBING (SIGNIFICA CHE UNA VOLTA CHE HO COMPLETATO LA RICOGNIZIONE ATTIVA , DEVO SAPERE QUALI PROGRAMMI E QUALI VERSIONI SONO IN ESECUZIONE SUL PC VITTIMA

ESEMPIO : POSSO AVERE NGINX , COME POTREI AVERE APACHE , ECC , VOGLIO SAPERE ANCHE LA LORO VERSIONE.
POSSO USARE nmap -sV

ALTRI TOOLS :
NETCAT (COMANDO nc)
TELNET

3-ANALISI DELLE VULNERABILITÀ

IN BASE HAI RISULTATI DEL BANNER GRABBING CERCO SE ESISTONO DELLE VULNERABILITÀ

nmap utilizzando --script vuln
OPPURE

DATABASE ONLINE / TOOL DI RICERCA DI VULNERABILITÀ (ESSEMPIO NESSUS/ OPENVAS)

ATTACCO/ACCESSO A QUESTE VULNARIBILITÀ - UTILIZZO DEGLI EXPLOIT .

UTILIZZO DI METASPLOIT

FASE DI POST EXPLOITATIONS

CANCELLAZIONE DELLE TRACCIE , INSTALLAZIONE DI MALWWARE , DUMP DI DATABASE , CREDENZIALI ECC