VAJA: Vdor v informacijski sistem z grobo silo

Namen

Vaja je namenjena učenju tehnik grobe sile (ang. brute force) za vdor v informacijski sistem. Skozi praktično uporabo orodja Hyrdra boste spoznali, kako poteka avtomatizirano ugibanje gesel ter se seznanili z etičnimi in pravnimi okvirji uporabe takšnih orodij v kontekstu kibernetske varnosti. Cilj je osvestiti učinkovitost in potencialne nevarnosti takšnih napadov ter poudariti pomen ustrezne zaščite informacijskih sistemov.

Uvod

V okviru vaj se bomo osredotočili na praktično uporabo orodja Hydra, ki je eno izmed najmočnejših orodij za izvajanje napadov grobe sile. Hydra omogoča avtomatizirano preizkušanje kombinacij uporabniških imen in gesel za različne protokole, ključno s SSH, FTP ,http in mnoge druge. Vaja bo potekala v kontroliranem okolju, kjer bomo na testnem SSH strežniku na naslovu 212.101.137.92 preizkusili tehniko grobe sile za vdor v sistem. Na druge sisteme vdor v okviru navodil ni dovoljen!

Naloge izvajajte v operacijskem sistemu Kali Linux.

Naloge:

1. Priprava okolja: Prepričajte se, da imate dostop do testnega okolja in da je orodje Hydra pravilno nameščeno na vašem sistemu.

2. Razumevanje osnov: Pred začetkom se seznanite z osnovnimi opcijami, ki jih Hydra ponuja. Za to lahko uporabite ukaz »`hydra -h`«, ki prikaže seznam vseh možnih ukazov in opcij. Opišite osnovne možne parametre.

3. Izvedba brute force napada:
   3.1. Za izvedbo napada uporabite ukaz v sledeči obliki:

```
hydra -l <uporabniško_ime> -P <pot_do_datoteke_z_gesli>
212.101.137.92 ssh -v
```

   3.2. Pri tem `<uporabniško_ime>` nadomestite z uporabniškim imenom, ki ga želite preizkusiti, `<pot_do_datoteke_z_gesli>` pa z lokacijo datoteke, ki vsebuje seznam možnih gesel.

4. Izbira uporabniškega imena in seznama gesel:

Uporabniško ime in geslo predvidevamo s socialnim inženiringom. Običajno za uporabniško ime preizkusimo »admin«. Lahko pa bi uporabili datoteko s seznamom najbolj pogostih uporabniških imen.

Gesla, ki jih preizkušamo morajo biti smiselna glede na kontekst.

Kali vključuje osnovne sezname (wordlists | Kali Linux Tools), lahko pa prenesete lastni seznam iz željene spletne strani z ukazom:

```
wget https://raw.githubusercontent.com/andrazjelenc/Slovenian-wordlist/master/wordlist.txt
```

5. Analiza rezultatov

Po izvedenem napadu analizirajte rezultate. Hydra bo izpisala uspešna gesla skupaj z uporabniškimi imeni. Kakšno uporabniško ime in geslo ste dobili?

6. Nadaljevanje

Na podoben način lahko izvedete vdor v napravo na naslovu 212.101.137.93. Začnite s poizvedovanjem in nadaljujte z izkoriščanjem najdenih ranljivosti.