Sprawozdanie - Analiza podatności opragromwania

Patryk Kaniewski

9 grudnia 2021

Spis treści

1 Skaner podatności oprogramowania

Skanery podatności oprogramowania to zautomatyzowanie narzędzia które skanują programy (aplikacjie sieciowe itp.) by wyszukać najczęsciej spotykane wektory ataku. Nazywane sa dynamicznymi gdyż głownie operują na podstawie wykonania ataku na działająca usługe lub system. Do tego typu często używanych ataków należa m.in:

- SQL injection
- XSS (cross site scripting)
- XSRF (cross site request forgery)
- Command Injection

1.1 Licencjowanie

Zwykle jest to oprogramowanie wspomagane poprzez społeczeństwo używające licencji otwartego oprogramowania (apache, MIT) lub *copyleftowych* licencji wolnego oprogramowania (GPL,BSD 3 clause) albo sa wspierane jako produkt przez firme oferujące usługi zawarte w takim skanerze. Część tych produktów ma również darmową wersję (czasami rozwijane jako *community* używając powyższych licencji).

1.2 Funkcjonalność

Skanery te można podzielić na takie które

2 Metasploit Framework

2.1 Instalacja

Moja dystrybucja systemu GNU/linux (ArchLinux) oferuje paczkę Metasploit w repozytorium. Metasploit wymaga tylko konfiguracji rvm (ruby) oraz założenia bazy danych postgres.

2.2 Bruteforce ssh

W tym przypadku spreparowalem konto na systemie który bedzie celem penetracji.

```
#useradd msfexploit
#passwd   #hasło zostało ustawione na password1
```

Na maszyne z metasploit pobrałem również popularny plik słownikowy rockyou.txt zawierający najczęsciej pojawiające się hasła.

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting          Required  Description
   ----              ---------------          --------  -----------
   BLANK_PASSWORDS   false                    no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                        yes       How fast to bruteforce, from 0 to 5
```

```
   DB_ALL_CREDS       false                     no        Try each user/password couple stored in the current database
   DB_ALL_PASS        false                     no        Add all passwords in the current database to the list
   DB_ALL_USERS       false                     no        Add all users in the current database to the list
   DB_SKIP_EXISTING   none                      no        Skip existing credentials stored in the current database (Acc
                                                          epted: none, user, user&realm)
   PASSWORD                                     no        A specific password to authenticate with
   PASS_FILE          ~/Downloads/rockyou.txt   no        File containing passwords, one per line
   RHOSTS             servbuntu.lan             yes       The target host(s), see https://github.com/rapid7/metasploit-
                                                          framework/wiki/Using-Metasploit
   RPORT              22                        yes       The target port
   STOP_ON_SUCCESS    true                      yes       Stop guessing when a credential works for a host
   THREADS            1                         yes       The number of concurrent threads (max one per host)
   USERNAME           msfexploit                no        A specific username to authenticate as
   USERPASS_FILE                                no        File containing users and passwords separated by space, one p
                                                          air per line
   USER_AS_PASS       false                     no        Try the username as the password for all users
   USER_FILE                                    no        File containing usernames, one per line
   VERBOSE            false                     yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) >
```