Bezpieczeństwo Systemów i Usług Informatycznych

Laboratorium 6. Patch_me_sr

1. Treść zadania.

Na zajęciach dostaliśmy do pracy plik binarny o nazwie "patch_me_sr". Uruchomiony program prosi nas o hasło i na jego podstawie przepuszcza nas (bądź nie) dalej. Naszym zadaniem było "spatchowanie" pliku za pomocą ingerencji w kod tak, aby logowanie wyłączyć, bądź sprawić, że poprawne będzie każde wprowadzone hasło. Mieliśmy wykonać to zadanie na dwa różne sposoby.

Do pracy nad kodem użyliśmy programu objdump oraz vim.

1. Sposób pierwszy.

Pierwszym krokiem jest unieszkodliwienie funkcji time_guard(), która za zadanie ma utrudnić nam ingerencję w plik. Analiza kodu wykazała, że funkcja ta w przypadku wykrycia "oszusta" zwraca wartość -1. Aby wyłączyć to zabezpieczenie możemy zmienić kod tak, aby zawsze zwracane było 0.

```
80484c3:       b8 ff ff ff ff          mov    $0xffffffff,%eax
```

Rysunek 1. Miejsce przypisania wartości -1.

Fragment ten możemy zmodyfikować otwierając plik binarny programem vim i znajdując go.

```
00004c0: 027e 07b8 ffff ffff eb16 c704 2400 0000  .~..........$...
```

Rysunek 2. Fragment z wartością "-1". Program vim.

Następnym krokiem jest zmodyfikowanie funkcji init tak, żeby we wszystkie pola tabeli którą wypełnia, wpisywane były wartości "winner". Wystarczy podmienić adres, z którego wartość przypisywana jest do rejestru edx.

```
804858c:       ba 52 85 04 08          mov    $0x8048552,%edx
```

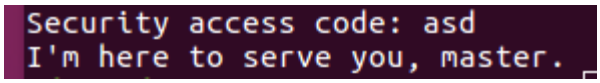
Rysunek 3. Fragment funkcji init z adresem dla wartości "looser".

Wyszukujemy ten fragment funkcji za pomocą programu vim i podmieniamy adres pod którym znajduje się wartość "looser" na adres z wartością "winner".

```
00000580: c745 f400 0000 00eb 138b 45f4 ba66 8504  .E........E..R..
00000590: 0889 1485 60a0 0408 8345 f401 837d f429  ....`....E...}.)
```

Rysunek 4. Podmieniony adres do łańcucha znaków.

Teraz możemy wypróbować naszą przeróbkę w działaniu. Po podaniu jakiegokolwiek hasła program zezwala nam dostęp.



Rysunek 5. Wynik działania przeróbki 1.

2. Sposób drugi.

Sposób drugi wykorzystuje pierwszy fragment sposobu pierwszego, czyli unieszkodliwienie time_guarda(). Następnie podmieniamy kod tak, aby dla pierwszego elementu tablicy przypisana została wartość "winner". Aby osiągnąć ten cel funkcja generate_code musi zwracać 0.

Rysunek 6. Końcowy fragment funkcji generate_code().

Po tej modyfikacji program bezproblemowo przepuszcza nas przez logowanie.