Analiza nieszyfrowanego ruchu sieciowego pod kątem obecności danych logowania

Teoria i inżynieria ruchu teleinformatycznego

Michał Kowalczyk 196858, Arkadiusz Klimkiewicz 180003

# Struktura komunikacji w aplikacji



# Dane przesyłane między usługami

#### MySnifferService.py ---> [21003] SelectorService.py

{

'data': http\_data,

'header': http\_header

}

#### SelectorService.py ---> [21002] MyPassFinderService.py

{

'header': msg['header'], # raw header

'fields': h.fields, # header fields

'request\_line': h.request\_line, # request line

'data': HeaderParser.data\_to\_string(msg['data']) # data

}

#### MyPassFinderService.py ---> [21000] StorageService.py

{

'pass': pass\_grdic['pass'], # post data with pass

'addr': url

}

# Opis usług

#### MySnifferService

Usługa zajmuje się przechwytywaniem pakietów TCP, które są adresowane na port 80 lub zostały wysłane z tego portu.

#### MyTcpAndHttpReassemblerService

Usługa ta dokonuje składania strumienia pakietów TCP a następnie składanie strumienia pakietów HTTP (wybranych metod).

Składanie strumienia TCP:

* Podczas składania strumienia brane są pod uwagę flagi przesyłane w pakietach tcp
* Strumie tcp są składane zgodnie z kolejnością (numerem sekwencyjnym). Jeśli pakiety przyjdą w niewłaściwej kolejności to czekają one na wcześniejsze pakiety(te z wcześniejszym numerem sekwencyjnym)
* Dla każdego strumienia składanie odbywa się niezależnie.
* Składane są tylko te strumie, które zostały podsłuchane od początku, czyli od momentu ustawienia połączenia.
* W przypadku zakończenia połączenia bądź resetu składanie zostaje przerwane.
* W razie braku komunikacji na danym strumieniu przez dłuższy czas składanie zostaje przerwane

Składanie pakietów HTTP:

* Składaniu strumienia HTTP poddawane są pakiety transmitowane w trybie Chunk oraz pakiety, które w nagłówku mają zadeklarowany rozmiar ładunku, jaki niesie.
* W razie braku kontynuacji pakietu przez dłuższy czas, jego składanie zostaje przerwane.

#### SelectorService

Usługa stara się odfiltrować pakiety HTTP, które w dalszym procesie przetwarzania nie będą przydatne. Pakiety, które zostaną przekazane dalej to takie pakiety, które są wysłane metodą POST, są w nieskompresowanej formie i są oznaczone, jako dane formularza (Content-Type: application/x-www-form-urlencoded).

#### MyPassFinderService

Usługa ta stara się analizować otrzymany pakiet HTTP pod kątem obecności słów kluczowych (‘pass’, ‘secret’). Jeśli pakiet zostanie zakwalifikowany, jako pakiet niosący dane logowania to dane w nim zawarte zostają przekazane do kolejnej usługi w celu zapisania.

#### StorageService

Usługa zajmuje się zapisywaniem do pliku otrzymanej struktury danych w postaci JSON.

#### MyPrinter

Usługa wyświetla dane statystyczne wysyłane przez inne usługi.

# Przykład przechwyconych danych

#### elektroda.pl

{

"addr": "www.elektroda.pl/rtvforum/login.php",

"pass": "username=Zaaaaap&password=ASDFASDFASDFASDFASDF&redirect=&login=Zaloguj"

}

#### electropark.pl

{

"addr": "electropark.pl/logowanie",

"pass": "email=asdFASDF&passwd=ASDFASDF&SubmitLogin=Zaloguj"

}

Jak widać oba te serwisy pozwalają na przesyłanie danych logowania w postaci niezaszyfrowanego tekstu.