

Wydział Fizyki, Matematyki i Informatyki	Zarządzanie projektem informatycznym	04.02.2019r.
Informatyka Stosowana II semestr	Projekt zaliczeniowy	Autorzy: <ul style="list-style-type: none"> • Kurdziel Kordian • Maciejak Mateusz • Mikołajczyk Mariusz • Milanović Aleksander • Uryga Marcin

1. Cel projektu

Zadaniem projektu było spreparowanie plików z logami w celu zasymulowania wystąpienia ataków na bezpieczeństwo systemu lub sieci. Ponadto, kolejnym zadaniem było zbudowanie sztucznej sieci neuronowej, której zadaniem było odczytywanie przygotowanych plików z logami i próba wykrycia jak największej liczby ataków na podstawie tych danych.

2. Przygotowanie plików logów

W naszym projekcie wybraliśmy dwa proponowane pliki z logami:

- 1) Plik flows.txt – zawierający dane nt. przesyłanych danych pomiędzy komputerami w danej sieci. Plik ten zawierał informacje nt. czasu wystąpienia, czasu trwania transmisji, komputera źródłowego, portu źródłowego komputera, komputera docelowego, portu komputera docelowego, rodzaju protokołu, liczby pakietów oraz liczby przesyłanych bajtów.

W pliku tym ukryliśmy dwa ataki:

- a) **Man-in-the-middle (MITM)** – atak polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy
- b) **MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution** – luka w bezpieczeństwie systemu operacyjnego Windows pozwalająca na zdalnym przejęciem kontroli na komputerem za pomocą wysłania spreparowanego żądania RPC.

- 2) plik procs.txt – plik zawierający logi ze zdarzeń uruchomienia i zakończenia wykonywania procesów na komputerach w danej sieci. Plik ten zawierał informacje nt. czasu wystąpienia, użytkownika oraz nazwy komputera, na którym był uruchomiony proces, nazwy procesu oraz informacji, czy dany proces był wówczas uruchomiony czy zatrzymany, reprezentowaną za pomocą ciągów znaków *Start* oraz *End*.

Plik ten został spreparowany tak, aby zawierał logi jak podczas ataku **Remote Code Execution**. Atak tego typu pozwala atakującemu na zdalne kontrolowanie komputera

swojej ofiary bez względu na lokalizację jej urządzenia. Atak tego typu jest możliwy poprzez wykorzystanie różnych luk bezpieczeństwa w systemie operacyjnym.

Do preparowania ww. plików zostały wykorzystane dwie maszyny wirtualne z systemami operacyjnymi Kali Linux oraz Windows Server 2003. Kali Linux zawierał w sobie potrzebne narzędzia do testowania ataków oraz do podsłuchu ruchu sieciowego podczas wykonywania wybranych ataków. Dzięki takiemu podejściu przygotowane przez nas pliki logów były bardziej precyzyjne i wiarygodne, ponieważ spreparowane dane były dodawane na podstawie wyników rzeczywistych eksperymentów. Podsłuchany ruch sieciowy był podstawą do odwzorowania pierwszego etapu ataku w logach. Poniżej umieszczono kilka zrzutów ekranu prezentujące proces testowania ataków za pomocą ww. narzędzi:

```

[6e18157-325820] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 150385, win 64240, length 0
[6e18157-326071] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 177941779796, win 3, win 3200, length 4039
[6e18157-326242] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 177941779796, win 3, win 3200, length 0
[6e18157-326466] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 184235, win 64240, length 0
[6e18157-326690] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 193149, win 64240, length 0
[6e18157-326723] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 1400260, win 64240, length 0
[6e18157-326885] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 146889, win 64240, length 0
[6e18157-327036] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 147939, win 64240, length 0
[6e18157-327187] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 147939, win 64240, length 0
[6e18157-327343] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 173745, win 64240, length 0
[6e18157-327498] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 176655, win 64240, length 0
[6e18157-327657] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 179618, win 64240, length 0
[6e18157-327892] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 179794, win 64240, length 0
[6e18157-328137] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 179794180355, win 3, win 3200, length 371
[6e18157-328383] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 11424, seq 180355, win 43470, length 423
[6e18157-328629] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 180355180355, ack 426, win 30016, length 128
[6e18157-328875] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 426160, ack 180352, win 31872, length 0
[6e18157-329121] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 4004, win 30016, length 144
[6e18157-329367] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 4004760, ack 104247, win 3139, length 146
[6e18157-329613] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 4004760, ack 104247, win 3139, length 146
[6e18157-329859] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 4004761133567, ack 740, win 32160, length 280
[6e18157-330105] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 400476136647, ack 740, win 32160, length 280
[6e18157-330351] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 184447180387, ack 740, win 32160, length 280
[6e18157-330597] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 184447180387, ack 740, win 32160, length 280
[6e18157-330843] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 182307180227, ack 740, win 32160, length 280
[6e18157-331089] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 182307180227, ack 740, win 32160, length 280
[6e18157-331335] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 180172101567, ack 740, win 32160, length 280
[6e18157-331581] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 180172101567, ack 740, win 32160, length 280
[6e18157-331827] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 20350718033097, ack 740, win 32160, length 280
[6e18157-332073] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 187929, win 64240, length 0
[6e18157-332319] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 2038071804007, ack 740, win 32160, length 280
[6e18157-332565] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 187929, win 64240, length 0
[6e18157-332811] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 180387, win 64240, length 0
[6e18157-333057] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 208027212747, ack 740, win 32160, length 280
[6e18157-333303] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 1923207, win 63339, length 3
[6e18157-333549] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 212747212647, ack 740, win 32160, length 280
[6e18157-333795] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 212647212647, ack 740, win 32160, length 280
[6e18157-334041] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 180237, win 58400, length 0
[6e18157-334287] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 212507212647, ack 740, win 32160, length 280
[6e18157-334533] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 212507212647, ack 740, win 32160, length 280
[6e18157-334779] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-335025] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-335271] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-335517] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-335763] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-336009] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-336255] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-336501] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-336747] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-336993] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-337239] P 192.168.0.224:1040 > wall.3389 Flags [P], seq 224472127397, ack 740, win 32160, length 280
[6e18157-337485] P 192.168.0.224:1040 >
```

[illegible]

3. Wykrywanie ataków za pomocą sztucznej sieci neuronowej

Kolejnym etapem wykonania projektu było przygotowanie i utworzenie sztucznej sieci neuronowej, której zadaniem było wykrycie wystąpienia ataków na bezpieczeństwo w systemie poprzez wykonanie analizy plików z logami. W tym celu wykorzystaliśmy bibliotekę języka Python – Tensorflow, która zawiera pełny zestaw gotowych implementacji narzędzi do budowania sieci neuronowych.

Przed przystąpieniem do prac zostały przygotowane dane trenujące z plików logów. Dane trenujące były pewnym wycinkiem logów, zawierającym badany atak. Dane te były konieczne do procesu trenowania sieci, aby podczas analizy całych plików z logami mogła poprawnie wykrywać ataki.

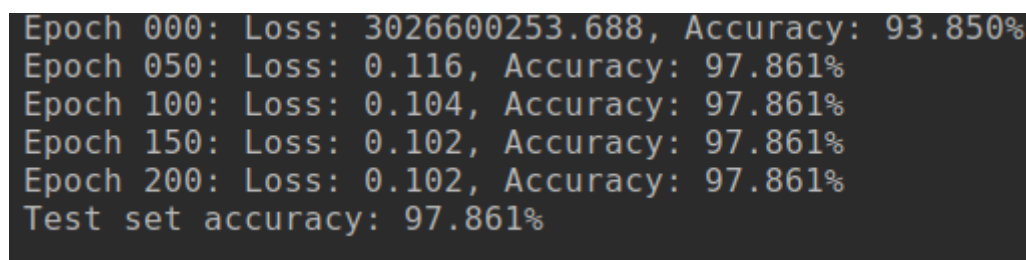
Przygotowana przez nas sieć neuronowa została zbudowana wraz z następującymi parametrami:

- Liczba warstw ukrytych: 2
- Algorytm uczenia: stochastic gradient descent (SGD)
- Funkcja aktywacji: Rectified Linear Unit (ReLU)
- Liczba epok trenowania: 201

4. Wyniki wykrywania ataków z wykorzystaniem SSN

Podczas testowania utworzonej przez nas sieci neuronowej nie udało się wykryć ataków. Niska wydajność wykrywania była spowodowana specyfiką ataków zawartych w plikach logów. Ataki te były zawarte w kilku rozdzielonych od siebie wpisach, co utrudniało skuteczną ich analizę. Ponadto, jako dane trenujące sieć został wybrany mały podzbiór dużego pliku logów. Powodem doboru takich danych trenujących była ograniczona wydajność komputera, na których trenowano sieć; wybór zbyt dużego pliku do trenowania mógłby pochłoniąć bardzo dużo czasu przy jednoczesnym wykorzystaniu słabej jednostki obliczeniowej.

Poniżej zamieszczono zrzuty ekranu prezentujące osiągniętą dokładność podczas testowania sieci:



```
Epoch 000: Loss: 3026600253.688, Accuracy: 93.850%
Epoch 050: Loss: 0.116, Accuracy: 97.861%
Epoch 100: Loss: 0.104, Accuracy: 97.861%
Epoch 150: Loss: 0.102, Accuracy: 97.861%
Epoch 200: Loss: 0.102, Accuracy: 97.861%
Test set accuracy: 97.861%
```

Rysunek 1. Zrzut ekranu prezentujący osiągniętą dokładność podczas testowania sieci na pliku logów procs.txt

```
Epoch 100: Loss: 0.351, Accuracy: 89.144%  
Epoch 150: Loss: 0.342, Accuracy: 89.144%  
Epoch 200: Loss: 0.343, Accuracy: 89.144%  
Test set accuracy: 89.144%
```

Rysunek 2. Zrzut ekranu prezentujący osiągniętą dokładność podczas testowania sieci na pliku logów flows.txt

5. Wnioski

Podsumowując wykonane prace udało się przygotować pliki z logami, w których zawarto kilka ataków na bezpieczeństwo systemu. Dzięki wykorzystaniu dwóch maszyn wirtualnych oraz profesjonalnych narzędzi do wykrywania i testowania luk bezpieczeństwa spreparowane pliki z logami zawierały jak najlepsze dane, odzwierciedlające możliwe, rzeczywiste ataki.

Dzięki wykorzystaniu narzędzi sztucznej inteligencji możliwe jest zbudowanie modelu sztucznej sieci neuronowej, której zadaniem jest wykrywanie ataków na bezpieczeństwo na podstawie analizy dostarczonych plików z logami. Dzięki oddzieleniu procesów trenowania sieci i jej rzeczywistego działania na danych możliwe jest jej wcześniejsze przygotowanie do właściwego wykrywania ataków. Narzędzie to efektywnie i szybko może posłużyć do detekcji i monitorowania sieci w celu wykrycia szkodliwego działania przez niepowołane osoby.

Jak wspomniano wcześniej stworzonej przez nas sieci nie udało się wykryć ataków. Było to spowodowane przez opisane powyżej różne czynniki, nie do końca od nas zależne. Jednakże przy wystarczającej ilości danych i większych zasobach obliczeniowych skuteczność wykrywania ataków zwiększyłaby się. W dzisiejszych sztuczna inteligencja jest coraz częściej wykorzystywana w tych celach. Coraz bardziej popularne staje się jej wykorzystywanie w celu wykrywania potencjalnych ataków na sieci i systemy.