Prowadzący: Wojciech Mazurczyk 2018.02.28

Projekt BEST – wytyczne v.1.5

Grupy projektujące vs. grupy detekujące

1. Wprowadzenie

Celem projektu jest przybliżenie zagadnień i wyzwań związanych z bezpieczeństwem sieciowym. Ważnym rezultatem projektu jest uświadomienie uczestnikom BEST jak (stosunkowo) łatwo jest zaprojektować i zrealizować prototyp złośliwego oprogramowania, a z drugiej strony jaką wiedzą, podejściem i umiejętnościami trzeba się wykazać, żeby takie zagrożenie wykryć.

W ramach projektu studenci dzieleni są na dwie grupy i wewnątrz nich formują 2 osobowe zespoły. Pierwsza połowa uczestników BEST to grupy projektujące odpowiedzialne za realizację prototypu złośliwego oprogramowania, natomiast druga połowa to grupy detekujące, których rolą jest jego wykrycie.

Forma projektu ma charakter **konkursu** tj. grupy projektujące rywalizują z grupami detekującymi. Innymi słowy celem grup projektujących jest realizacja niewykrywalnej komunikacji pomiędzy zainfekowaną maszyną, a serwerem zewnętrznym. Natomiast grupy detekujące mają za zadanie wykrycie i odgadnięcie użytego sposobu komunikacji dla jak największej liczby zespołów projektujących.

Grupy projektujące pracują przez pierwsze pół semestru i w rezultacie przekazują dane, na bazie których analizę rozpoczynają grupy detekujące (trwającą przez drugą połowę semestru).

2. Założony scenariusz projektu

W ramach projektu zakładamy następujące role:

- **grupy projektujące:** cyberprzestępcy/szpiedzy przemysłowi,
- **grupy detekujące:** specjaliści ds. bezpieczeństwa firmy XYZ/zewnętrznej firmy bezpieczeństwa.

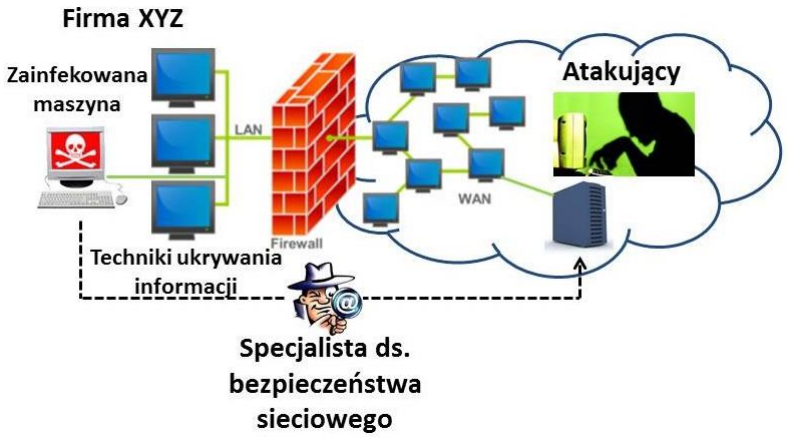
Scenariusz realizowany w projekcie jest nastepujący: firma XYZ jest wschodzącą gwiazdą innowacyjnych firm technologicznych i posiada w swoich zasobach/produktach rozwiązania i informacje, które zmienią oblicze sektora ICT (Information and Communication Technologies) na najbliższą dekadę.

Na rynku firma XYZ posiada (nie do końca uczciwą) konkurencję, która jest zmotywowana do pozyskania tych wartościowych rozwiązań/informacji oraz posiada odpowiednie zasoby

finansowe i znajomości w świecie cyberprzestępców[1]. Konkurencyjna firma wynajmuje zespół kompetentnych osób (grupy projektujące) w celu pozyskania w sposób nielegalny tych danych.

Firma XYZ podejrzewa, że ze względu na istotę wynalazków może stać się obiektem ataków sieciowych w związku z tym zatrudnia odpowiedni personel (bądź firmę zewnętrzną) odpowiedzialny za monitorowanie i zapewnienie bezpieczeństwa jej infrastruktury sieciowej oraz instaluje odpowiednie zabezpieczenia.

Niestety mimo najszczerszych starań i nowoczesnych zabezpieczeń atakujący w końcu znajdują i wykorzystują dziurę bezpieczeństwa, co prowadzi do infekcji jednej z maszyn. Po „dostaniu się do środka" cyberprzestępcy muszą zachowywać się jednak bardzo ostrożnie, żeby nie wzbudzić podejrzeń. Udaje im się w końcu zlokalizować miejsce przechowywania cennych danych, jednak ze względu na mocne zabezpieczenia (monitorowanie ruchu, systemy IDS/IPS, etc.) ich wyciek musi zostać zrealizowany tak, aby nie został wykryty. W tym celu atakujący chcą wykorzystać *techniki ukrywania informacji w ruchu sieciowym*[2], czyli sposoby pozwalające na ukrycie tajnych danych w odpowiednio wybranym nośniku – ruchu sieciowym związanym z konkretną usługą/protokołem (Rys. 1).



Rys. 1 Scenariusz projektu BEST

Zadaniem atakujących (grup projektujących) jest zatem zaprojektowanie i zrealizowanie prototypu malware'u, a następnie wykorzystanie go do przesłania w sposób ukryty wskazanych danych.

Zadaniem specjalistów ds. bezpieczeństwa firmy XYZ (grup detekujących) jest natomiast wykrycie przesyłanych danych i zidentyfikowanie wykorzystanych sposobów ukrywania informacji w ruchu sieciowym.

3. Grupy projektujące – wytyczne

[1] Więcej informacji nt. wykradania poufnych informacji z firm: http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

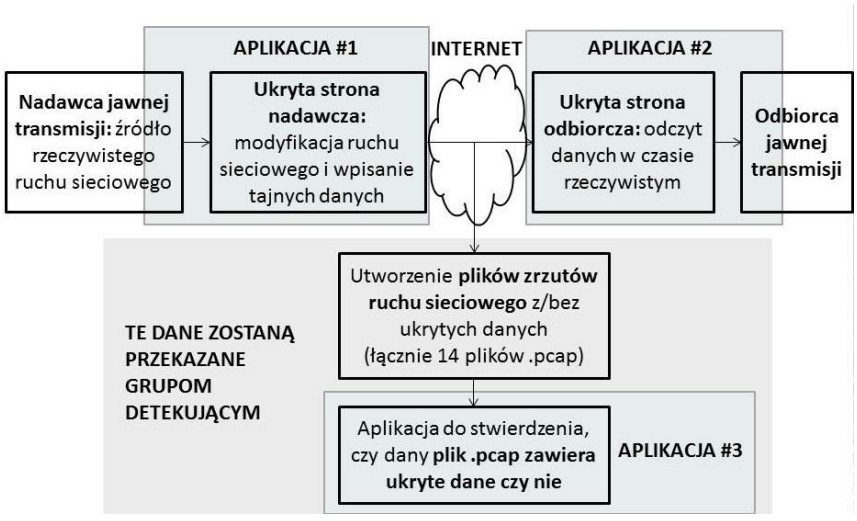
[2] Więcej o tym jak obecny malware wykorzystuje techniki ukrywania informacji można się dowiedzieć np. tu: http://arxiv.org/ftp/arxiv/papers/1504/1504.04867.pdf

3.1 Wymagania

Grupy projektujące realizują komunikacyjną część prototypu złośliwego oprogramowania, którym została zainfekowana jedna z maszyn firmy XYZ. Zakładamy, że pozostała część malware'u już jest tam zainstalowana i funkcjonuje. W związku z tym zadaniem grup projektujących jest wybór, zaprojektowanie i realizacja metody ukrywania informacji, która pozwoli na niewykrywalne przesłanie tajnych danych z firmy XYZ na serwer kontrolowany przez atakującego. Wybrana metoda ma być techniką **steganografii sieciowej**, czyli powinna ukrywać dane w wybranym ruchu sieciowym (innymi słowy ukrywanie np. w najmniej znaczących bitach obrazków nie jest akceptowalne – w razie wątpliwości co do wybranej metody proszę skonsultować się z prowadzącym przedmiot!). Jako nośnik ukrytych danych ma być wykorzystany jeden z popularnych protokołów/usług znanych z sieci Internet – nie jest zatem możliwe generowanie sztucznie wytworzonego ruchu sieciowego poprzez formowanie pakietów, których typowo nie można by znaleźć w sieci Internet. Wskazane jest natomiast użycie aplikacji pozwalających generować prawdziwy ruch sieciowy np. klienta/serwera FTP, HTTP, klienta telefonii IP, itp. a następnie wpisanie w ten ruch tajnych danych. Należy pamiętać, że zmodyfiowany przez grupy projektujące ruch sieciowy ma nie wzbudzać podejrzeń, czyli ma nie odróżniać się znacząco od ruchu, który typowo jest przesyłany w sieci korporacyjnej (jednocześnie transmisja jawna ma przebiegać bez zakłóceń!). Dane powinny być jak najlepiej ukryte, co jest istotą steganografii.

W ramach projektu niezbędna będzie realizacja łącznie 3 aplikacji (Rys. 2):

- **Ukrytej strony nadawczej** (rezydującej na zainfekowanej maszynie) modyfikującej rzeczywisty ruchu sieciowy tak, aby zawierał tajne dane i wysyłającej je poza sieć lokalną
- **Ukrytej strony odbiorczej**, która ten ruch zaakceptuje (serwer będący pod kontrolą atakującego) oraz będzie w stanie w czasie rzeczywistym odczytać ukryte dane.
- Aplikacji będącej w stanie stwierdzić, czy ukryte dane są zapisane zrzutach ruchu sieciowego.



Rys. 2 Scenariusz projektu BEST

Każda grupa projektująca ma te same tajne dane do przesłania. Jest to treść „Antygony" Sofoklesa zawartej w pliku tekstowym o rozmiarze ok. 55 kB (plik dostępny na stronie przedmiotu: http://www.tele.pw.edu.pl/best/Sofokles%20-%20Antygona.txt).

W dokumentacji projektowej należy zawrzeć także oszacowanie przepływności zaprojektowanej metody steganografii sieciowej (w bit/s), ocenę niewykrywalności oraz jej elastyczności (robustness).

Rezultatem końcowym realizacji projektu przez grupy projektujące, który zostanie przekazany grupom detekującym są:

- **Zrzuty ruchu sieciowego** zapisanego za pomocą programu WireShark (pliki .pcap). Należy nagrać razem 14 połączeń z czego 7 połączeń ma zawierać komunikację steganograficzną, a 7 połączeń ma być „czystych" (wygenerowanych tą samą aplikacją bez dodawania ukrytych danych). UWAGA: w każdym zrzucie ma być *co najmniej* 10kB tajnych danych (ok. 20% całości).
- **Aplikacja** (.exe) **będąca w stanie stwierdzić, czy ukryte dane są zapisane w ruchu sieciowym** (plikach .pcap). Aplikacja ma działać w następujący sposób: można wywołać aplikację podając jako argument plik .pcap np. *aplikacja.exe 123.pcap* i w rezultacie działania aplikacja poinformuje użytkownika czy plik zawiera ukryte dane czy nie. Najlepiej razem z aplikacją przekazać także krótką instrukcję jej uruchomienia i jeśli jest to wymagane, co należy doinstalować, żeby ona zadziałała. Za jakość instrukcji i jej kompletność odpowiada grupa projektująca – jeśli okaże się, że jest problem w uruchomieniem dostarczonej aplikacji to grupa detekująca zgłasza ten fakt poprzez grupę mailinową BEST, a grupa projektująca jest zobowiązana problem jak najszybciej rozwiązać. Jeśli rozwiązanie problemu będzie się przedłużać, to będzie to w konsekwencji skutkowało obniżeniem punktacji końcowej grupy projektującej.

Za jakość przygotowanych zrzutów ruchu (plików .pcap) oraz działanie aplikacji odczytującej ukryte dane z tych plików odpowiadają grupy projektujące. UWAGA: pliki ze zrzutami ruchu mają zawierać jedynie wyfiltrowany ruch steganograficzny/niesteganograficzny, czyli nie jest akceptowalne celowe zaciemnianie i zaśmiecanie plików .pcap innymi rodzajami ruchu (tj. celowe uruchamiane innych połączeń w trakcie zgrywania steganograficznego/niesteganograficznego ruchu sieciowego). Dostarczenie nie działającej aplikacji lub nieprawidłowych plików .pcap będzie wpływało na opóźnienie prac grup detekujących i będzie skutkować ujemnymi punktami z oceny projektu.

Pliki ze zrzutami ruchu (.pcap) jak i aplikację odczytującą z nich ukryte dane należy wgrać w terminie wyznaczonym przez prowadzącego na wspólne konto Dropbox dla BEST (https://www.dropbox.com/login):

Login: oins@oins.pl

Password: BESTrulezzz

Każda z grup projektujących zakłada na powyższym koncie katalog zawierający nazwiska członków grupy. W przypadku, gdy zrzuty ruchu zajmują bardzo dużo miejsca, bądź dostępne miejsce na ww. koncie Dropbox się skończy należy do katalogu wgrać plik tekstowy zwierający link (np. do własnego konta Dropbox itp.), pod którym dostępne będą pliki pcap i aplikacja odczytująca.

Udostępnienie aplikacji pozwalającej stwierdzić, które pliki .pcap zawierają ukryte dane ma na celu **wyrównać szanse grup projektujących i wykrywających** – bez tego grupy detekujące byłyby w bardzo trudnej sytuacji.

Tydzień po terminie wgrania niezbędnych danych na konto Dropbox dla grup detekujących, grupy projektujące zobowiązane są przesłać link do wysharowanego katalogu na Dropbox (lub innej tego typu usłudze – nie mylić z kontem indywidualnym dla celów sprawozdań z laboratoriów!), w którym znajdować się będzie dokumentacja projektu oraz kody zaimplementowanych aplikacji realizujących ukrytą transmisję (aplikacja nadająca – ukrywająca dane w ruchu sieciowym oraz aplikacja odbiorcza, której zadaniem jest poprawne odczytanie danych z ruchu sieciowego w czasie rzeczywistym). Dokumentacja ma mieć postać pliku w formacie .pdf o nazwie "*Nazwiska_autorow_dok*". Podobnie inne załączane pliki np. spakowane zipem zródła mają posiadać adekwatne nazwę *Nazwiska_autorow_source.zip*.

3.2 Informacje dodatkowe: inspiracje i kryteria oceny

Inspirację dla projektowanej metody można czerpać z wielu źródeł np.:

- Przegląd metod steganografii sieciowej do 2007 roku: http://caia.swin.edu.au/cv/szander/publications/szander-ieee-comst07.pdf
- Informacje o metodach zamieszczone na stronie http://stegano.net

Inwencja własna mile widziana ☺

Na ocenę końcową projektu wpływać będą:

- Dobór metody ukrywania informacji i jej (nie)wykrywalność przez grupy detekujące,
- Sposób i jakość implementacji metody,
- Terminowość i jakość dostarczonych plików .pcap oraz aplikacji odczytującej tajne informacje ze zrzutów ruchu sieciowego,
- Jakość dostarczonej dokumentacji projektu (do 8 pkt.).

Grupy nie ujawniają sobie nawzajem jaką metodę steganograficzną wykorzystały. Najlepsza metoda ukrywania (najmniej wykrywalna przy dobrej przepływności) uzyska +8 punktów bonusowych. W przypadku remisu o podziale punktów decyduje prowadzący.

UWAGA: oddanie projektu jest warunkiem niezbędnym do zaliczenia przedmiotu. W przypadku nie oddania projektu albo oddania projektu drastycznie odbiegającego od wymagań – nie będą prowadzone żadne negocjacje na temat zaliczenia przedmiotu. Za każdy

dzień spóźnienia po ostatecznym dniu oddania projektu naliczane są karne punkty tj. -5 (pięć) pkt/dzień.

4. Grupy detekujące – wytyczne

4.1 Wymagania

Grupy wykrywające są personelem bezpieczeństwa firmy XYZ próbującym zdetekować ukrytą transmisję prowadzoną przez złośliwe oprogramowanie i odkryć jej dokładny sposób działania. Będą one dokonywały analizy w oparciu o dane dostarczone przez grupy projektujące. Dane będą dostępne na wspólnym koncie Dropbox dla BEST (https://www.dropbox.com/login):

Login: oins@oins.pl

Password: BESTrulezzz.

Do analizy, jako rezultat końcowy realizacji projektu przez grupy projektujące, grupy detekujące otrzymają:

- **Zrzuty ruchu sieciowego** zapisanego za pomocą programu WireShark (pliki .pcap). Razem 14 połączeń z czego 7 połączeń zawierać będzie komunikację steganograficzną, a 7 połączeń będzie „czystych" (wygenerowanych tą samą aplikacją bez dodawania ukrytych danych).
- **Aplikacja** (.exe) **będąca w stanie stwierdzić, czy ukryte dane są zapisane w ruchu sieciowym** (plikach .pcap).

Zespoły wykrywające mogą stosować wybrany przez siebie zestaw narzędzi/sposobów analiz. Inwencja własna mile widziana ☺. W szczególności podejścia niestandardowe: „nie chodzi o to, żeby walić głową w mur tylko żeby go obejść". Lepiej jest pokazać szerokie spektrum wykorzystanych podejść niż skupić się jedynie na jednym rozwiązaniu.

W celu wykrywania zastosowania technik ukrywania informacji można wykorzystać manualną/automatyczną/półautomatyczną metodę analizy ruchu sieciowego (implementacja własnych narzędzi lub skorzystanie z istniejących np. Wireshark – polecam prezentację Laury Chapel pt. *Wireshark Network Forensics* dostępną tu: https://www.youtube.com/watch?v=UXAHvwouk6Q). Nie należy jednak koncentrować się jedynie na analizie ruchu sieciowego tylko podejść do zagadnienia szeroko.

Informacje na temat dostępnych metod wykrywania można czerpać z wielu źródeł np.:

- Przegląd metod steganografii sieciowej i jej wykrywania do 2007 roku: http://caia.swin.edu.au/cv/szander/publications/szander-ieee-comst07.pdf,
- Informacje o metodach zamieszczone na stronie http://stegano.net.

Ważne jest przede wszystkim zaprezentowanie (najlepiej) jak największej liczby różnorodnych sposobów podejścia do detekcji (z niestandardowymi podejściami włącznie) wraz z uzasadnieniem ich wyboru oraz dokumentacją uzyskanych rezultatów. Istotne jest także odpowiednie udokumentowanie prób podejść do detekcji (także nieudanych), gdyż świadczy to o rozumowaniu podjętym przez grupę oraz sposobie podejścia do postawionego problemu.

W dokumentacji projektu (szczegółowe wytyczne w kolejnym rozdziale) ważne jest także określenie efektywności grupy wykrywającej co zależy od liczby prawidłowo zdetekowanych metod steganograficznych. W tym celu na końcu dokumentacji niezbędne jest umieszczenie tabeli podsumowującej metody (autorów) i sposoby detekcji w następujący sposób:

Metoda/Grupa projektująca	**Domniemana zasada działania (zwięźle)**	**Zastosowany sposób detekcji**
Metoda 1 - autorzy	Np. ukrywanie w polu X	Analiza manualna
Metoda 2 - autorzy	Np. ukrywanie poprzez modyfikację Y	Analiza automatyczna
...	...	...

4.2 Informacje dodatkowe: kryteria oceny

Na ocenę końcową projektu wpływać będą:

- Zaprezentowanie różnorodnych sposobów podejścia do detekcji (z niestandardowymi podejściami włącznie) wraz z uzasadnieniem ich wyboru oraz dokumentacją uzyskanych rezultatów,
- Odpowiednie udokumentowanie prób podejść do detekcji (nawet nieudanych),
- Liczba wykrytych technik ukrywania informacji,
- Jakość dostarczonej dokumentacji projektu (do 8 pkt.).

Grupy nie ujawniają sobie nawzajem jakie sposoby detekcji wykorzystały. Najbardziej skuteczna grupa (czyli ta, która wykryje najwięcej metod) uzyska +8 punktów bonusowych. W przypadku remisu o podziale punktów decyduje prowadzący.

UWAGA: oddanie projektu jest warunkiem niezbędnym do zaliczenia przedmiotu. W przypadku nie oddania projektu albo oddania projektu drastycznie odbiegającego od wymagań – nie będą prowadzone żadne negocjacje na temat zaliczenia przedmiotu. Za każdy dzień spóźnienia po ostatecznym dniu oddania projektu naliczane są karne punkty tj. -5 (pięć) pkt/dzień.

5. Dokumentacja projektowa – wymagania

Dokumentacja projektu stanowi jego istotną i integralną część i można uzyskać za nią od 0 do 8 pkt. Dokumentacja projektu ma spełniać wymogi publikacji naukowo-technicznej, czyli:

- Powinna być napisana językiem technicznym (bez sformułowań potocznych) i logicznie ułożona.
- Powinna odzwierciedlać sposób podejścia zespołu do problemu projektowego: analizę dostępnych możliwości rozwiązania problemu, uzasadnienie podejmowanych decyzji np. co do wyboru oprogramowania, bibliotek itp.
- Powinna zawierać m.in. takie elementy jak: szczegółową treść projektu, cele projektu, ogólne założenia projektu, opis architektury rozwiązania, opis sposobu działania (w przypadku aplikacji), opis najważniejszych funkcji/metod itp. wykonanej implementacji oraz bibliografię,
- Powinna zawierać referencje do pozycji literatury naukowej, standardów itp. (które zostaną umieszczone w bibliografii).
- Powinna "wyglądać" jak publikacja naukowo-techniczna pod względem estetycznym (formatowanie, justowanie, akapity itp. itd.).

Dokumentacja ma być "przetarciem" przed pisaniem prac dyplomowych, więc ma spełniać takie standardy jak praca dyplomowa. Więcej informacji o tym jak dokumentacja/praca dyplomowa powinna wyglądać można znaleźć w prezentacji prof. Kraśniewskiego – przede wszystkim: Sformułowanie problemu, "Filozofia" pisania pracy, Struktura tekstu, styl i forma oraz Ogólna struktura, która jest dostępna tu: http://zpt2.tele.pw.edu.pl/~andrzej/TP/wyklad/wyklad-pdf/TP-praca_dypl.pdf.

Grupy detekujące zobowiązane są przesłać prowadzącemu projekt link do wysharowanego katalogu na Dropbox (lub innej tego typu usłudze – nie mylić z kontem indywidualnym dla celów sprawozdań z laboratoriów!), w którym znajdować się będzie dokumentacja projektu i np. ew. narzędzia stworzone na potrzeb detekcji ukrytej komunikacji. Dokumentacja ma mieć postać pliku w formacie .pdf o nazwie "*Nazwiska_autorow_dok*". Podobnie inne załączane pliki np. spakowane zipem zródła mają posiadać adekwatne nazwę *Nazwiska_autorow_source.zip*.