КОНЦЕПЦИЯ НА ГЕНЕТИЧНИЯ АЛГОРИТЪМ ЗА ОТКРИВАНЕ НА ПРОНИКВАНИЯ В КОМПЮТЪРНАТА МРЕЖА

Андон Лазаров, Петя Петрова

GENETIC ALGORITHM CONCEPTION OF INTRUSION DETECTION IN COMPUTER NETWORK

Andon Lazarov, Petia Petrova

***Abstract*:** The present work addresses main functionality and structure of the genetic algorithms. The sequence of characteristics of network connections is interpreted as a chromosome that defines an intrusion detection rule, whereas the very characteristics are considered as chromosome’s genies. The basic IP v-4 and IP-v6 network characteristics and their structure are provided and illustrated in examples of network connections with intrusion and without intrusion.

Key words: Genetic algorithm, network Intrusion Detection System (IDS), chromosome structure, intrusion detection rule,

1. Въведение

Съвременният свят е немислим без глобалната мрежа Internet и локалните компютърни мрежи, както и техните хардуерни и софтуерни компоненти, създаващи среда за комуникация, информационно и технологично осигуряване. Но, базирани на детерминираните механизми на тяхното функциониране, компютърните мрежи, с техните хардуерни и софтуерни компоненти представляват и обект на заплаха и агресия от злонамерени потребители, преследващи различни цели. Това определя особената актуалност в разработването на софтуерни технологии, противодействащи на тези агресивни действия. Известни са различни инструменти, използвани за защита на компютърната система от мрежови атаки, като защитна стена, антивирусен софтуер, защита с парола, криптиране на съобщение, криптиране на пароли и т.н., за да се преодолеят заплахите. Особено е актуален въпросът за разпознаване на атаките и откриване на проникванията в компютърната мрежа. Един от подходите в разработването на софтуерна технология за откриване и предотвратяване на проникванията е прилагането на генетични алгоритми [1-12].

Система за откриване на проникване в компютърните мрежи чрез прилагане на генетичен алгоритъм за ефективно откриване на различни видове мрежови проникванията и оценка на параметрите на генетичния еволюционния процес са представени в [1].

Софтуерна реализация на генетичен алгоритъм за откриване на проникване в компютърните мрежи е представена в [2]. В [3] се описва генетичен алгоритъм при използване на механизъм за селекция на хромозомите, базиращ се на тяхното устойчиво състояние. Направена е оценка на влиянието на броя итерации, различните функции на пригодност (Fitness функции) чрез вариране на началната дължина на хромозомата. Структурно описание на компонентите на генетичния алгоритъм, дефиницията на правилата за откриване на проникване и прилагането на различни Fitness функции е направено в [4].

Генетичен алгоритъм, използван за класификация и откривания на проникванията в мрежата на базата на пространствена (адресна) и времева информация в информационния пакет, неговите параметри и еволюционният процес за вземане на решения е представен в [5]. Генетичен алгоритъм за идентифициране на различни проникващи атаки, отчитащ различните характеристики в мрежовата комуникация, като тип протокол, продължителност, сервизна функция, с цел генериране на множество от класификационни правила за идентифициране и класифициране на различни видове атаки, е представен в [6].

За оценка на пригодността на хромозомата, структурна компонента на генетичния алгоритъм, се прилага функция за пригодност (Fitness функция). Чрез оценка на Fitness функцията на дадена хромозома се взема решение за откриване на проникване. Структурата на Fitness функция и резултати от експеримент за откриване на проникване се представят в [7]. Приложението на

генетичен алгоритъм за постигане на сигурност в комуникационните мрежи и разработване на примерен криптиращ алгоритъм се разглеждат в [8].
Изграждане на генетичен алгоритъм и дървовидна структура за вземане на решение за проникване в компютърната мрежа и подход за откриване на проникване в мрежата чрез анализ на Sun данни, подлежащи на проверка, с прилагане на йерархичен генетичен алгоритъм се анализират в [9, 10]. Система за откриване на прониквания в мрежата чрез прилагане алгоритъм, базиран на размита логика е предложена в [11]. Същността на генетичния алгоритъм е да намери оптимално решение на проблема, откриване на проникване, чрез функция на пригодност (Fitness функция), която оценява до колко селектираните индивиди (хромозоми) оптимизират решението. В естествената еволюция свойството на пригодност (Fitness) е способността на организма да оцелее и да се възпроизведе. Генетичен алгоритъм, приложен за постигане самоорганизираща се гъвкава сигурност е представен в [12]. Модел на система за откриване на прониквания в компютърните мрежи чрез прилагане на подхода на линейното генетично програмиране и методите на изкуствения интелект са представени в [13, 14, 15]. Софтуерно осигуряване, тематичен обзор на методите, прилагащи генетични алгоритми за откриване на прониквания в компютърните комуникационни мрежи са анализирани в [16, 17].
Целта на настоящата статия е да се направи тематичен обзор на въздействията върху мрежовите комуникации. Да се систематизират основните характеристики на системите за откриване и превенция на прониквания в компютърните мрежи. Да се разкрие синтаксисът на генетичния алгоритъм и анализира мрежовата структура и характеристики (гените и техните кодове) на правилата (хромозомите) за определяне вида на комуникационния обмен.
В съответствие с така дефинираната цел, съдържанието на статията е организирано по следния начин. Във 2 част се прави обща характеристика на система за откриване на проникване в компютърните мрежи. В 3 част са разгледани видовете прониквания в компютърните мрежи. В 4 част е дадена характеристика и се дефинират параметрите на генетичния алгоритъм, използван за откриване и разпознаване на атаки в компютърните мрежи. Дефиниран е синтаксисът и структурата на различни правила (хромозоми) в генетичния алгоритъм. Подробно е описан и илюстриран с примери процесът на кодиране на мрежовите характеристики (гените). В 5 част са направени заключение и общи изводи, както и дадени насоки за бъдеща работа.

2. Основни характеристики на системите за откриване и превенция на прониквания в компютърните мрежи

Системата за откриване на проникване е система или софтуерно приложение, което следи мрежовите или системните функции за откриване на злонамерени действия или нарушения на правилата и изпраща съобщения до работната станция за управление на мрежовите комуникации. Някои системи са предназначени да възпрепятстват опити за проникване, което не се изисква за системи за наблюдение и статистически контрол на трафика. Съществуват два основни принципа на откриване на прониквания [4]:

А. Разпознаване на проникването на база на хост: хост-базирани IDS проследяват файлове и процеси, свързани със софтуерна среда на конкретен хост. Хост-базирани IDS наблюдават мрежовия трафик, за да идентифицират атаки срещу хост.
Б. Разпознаване на проникване в мрежа: Това са системи, които идентифицират прониквания чрез наблюдение на трафика чрез мрежови устройства, например, мрежова интерфейсна карта, NIC. NIDS оценяват информацията, получена от мрежовата комуникации, анализират потока от пакети, които се транспортират в мрежата.
Системата за откриване на проникване IDS прилага следните механизми за оценка и реакция на проникване в мрежата:

- Сигнатурно-базиран подход за откриване на злоупотреба и уязвимост на софтуера.
Системата открива злоупотреба и регистрира прониквания, които следват известни модели (сигнатури - последователности от мрежови характеристики, IP адреси, порт адреси и т.н.) на атаки, използващи определена уязвимост на софтуерните приложения. Сигнатурата може да бъде статичен низ или последователност в пакета от данни. Системните отговори се основават на

идентифициране на проникванията чрез сигнатура, които защитният софтуер търси и открива. Ограничение на този подход е, че IDS системата открива само известни злонамерени проникванията и е невъзможно откриване на неизвестни като сигнатури проникванията.

- Статистически подход за откриване на аномалия в комуникационния трафик
Системата открива аномалия, като търси и открива нещо извънредно в пакета от данни при комуникацията, чиито характеристики не са известни. Анализират се потоците от системни събития, като се прилагат статистически техники за намиране на модели на поведение, които изглеждат аномални. Това са техники, които проследяват, определят и характеризират естествени или приемливи поведения на компютърната система като използване на процесора, време за изпълнение на заданието, системни извиквания [1, 2]. Мрежови състояния, които се отклоняват от очакваното и естествено поведение на мрежата, се считат за проникванията. Недостатъци на тази система са, че е скъпа и съществува вероятност злонамерено проникващо поведение да бъде оценено като нормално поведение поради липса на данни.

- Реакция на системата при откриване на проникване чрез мениджъра за ответно действие (реакция-отговор).
Мениджърът на ответното действие се активира тогава, когато се открият несъответствия (евентуално проникващи действия срещу системата), като се извежда информация за събитието и действието, предприето спрямо него.

3. Видове мрежови атаки
Компютърните мрежи са подложени на различни видове несанкционирани проникванията, известни като мрежови атаки, които целят компроментиране на даден компютърен възел, работна машина или мрежа чрез достъп до данни или възпрепдстване на нормалното протичане на комуникационния обмен. Известни са следните основни атаки в компютърните мрежи [3, 4, 5]:

3.1. Отказ от обслужване (Denial of Service - DoS)
DoS атаката е вид проникване, при което хакерът прави компютърните ресурси или ресурсите на паметта твърде заети или прекалено пълни, за да обслужват легитимни мрежови заявки и по този начин отказват на потребителите достъп до машина. Пример на такива атаки, apache, smurf, neptune, pingof death, back, mail bomb, UDP storm и др.

3.2. Отдалечени от потребителя атаки (Remote to User Attacks - R2L)
Атака за отдалечен потребител е атака, при която потребителят изпраща пакети до машина по интернет, която няма достъп до тях, за да разкрие уязвимостта на машините и да използва права, които местният потребител има на компютърния мрежови възел.

3.3. Потребителски коренови атаки (User to Root Attacks - U2R)
При тези атаки хакерът се включва в мрежата (системата) с нормална потребителска регистрация (account) и се опитва да злоупотреби със защитата и открие уязвимост в системата, за да получи статут за привилегирован потребител.

3.4. Сондиране (Probing)
Сондирането е атака, при която хакерът сканира работна станция, сървър или друго мрежово устройство, за да определи слабости или уязвимостта, които по-късно могат да бъдат използвани, за да компрометират комуникационната система. Тази техника се използва често при извличане на данни.

4. Обща характеристика и дефиниране на параметрите на генетичния алгоритъм

Генетичният алгоритъм е еволюционен изчислителен процес за търсене и оптимизация, който се прилага за откриване на злонамерено проникване. Този алгоритъм оперира с последователности

от мрежови характеристики - индивиди, наречен хромозоми и имитира биологични генетични процеси. Откриването на злонамерено проникване е процес на генериране на качествена хромозома с гени, т.е. мрежови характеристики, максимално съответстващи на въздействие върху компютърната мрежа или качествена популация от хромозоми, отново съответстваща на компютърно въздействие, на базата на начална група от хромозоми чрез прилагане на основните биологични операции: селекция, кръстосване и мутация. Оценка на качеството на всяка популация от хромозоми е чрез т.н. Fitness функция (функция на пригодност), която има смисъл на целева функция в евристичния изчислителен процес.
В действителност, алгоритъмът за откриване работи с мрежови последователности от данни, които представляват характеристиките на всяка мрежово съобщение (IP адреси, порт-адреси, параметри на свързването, съдържание и т.н.). Именно, тези последователности от данни се интерпретират с хромозоми, а тяхното съдържание се интерпретира като гени. Формално, последователностите се наричат още правила. С други думи, генетичният алгоритъм работи върху правила, като развива начална група от правила, произволно подбрани, до съвкупност (популация) от качествени правила, оценени с високи стойности на Fitness функцията (функцията на пригодност).

4.1. Основни операции на генетичния алгоритъм

1. Към всеки индивид по време на процеса на генериране на правилата (хромозомите) се прилагат три генетични оператора: **селекция, кръстосване, мутация.**
2. Избира се група от хромозоми удовлетворяващи критерий за принадлежност, използвайки Fitness функция и се елиминират останалите индивиди.
3. Процесът продължава, като се избират няколко индивида и се формират двойки за нова популация. Хромозомната двойка генерира едно потомство, което приема гените в областта на точката на кръстосване на двете хромозоми.
4. Някои индивиди се идентифицират като потенциално пригодни и към тях се прилагат мутационните операции.
5. По дефинициите на атаката (smurf, mailbomb, saint, warezmaster и т.н.) се извършва разпознаване с прилагане на критериите за принадлежност (пригодност) и избор на най-пригодните хромозоми от всяка популация, способни да откриват атаките.

Генетичният алгоритъм, като правило, започва с произволно избрана популация от хромозоми. Тези хромозоми дефинират проблема, който трябва да бъде решен. В съответствие с атрибутите на проблема, позициите на мрежовите характеристики (полетата) на всяка хромозома се кодират като последователности от битове, символи или числа (десетични или шестнадесетични). Тези мрежови позиции се наричат гени, които се променят на случаен принцип в процеса на еволюцията [1,2,3].
Генетичният алгоритъм стартира с избор на първоначална популация от случайно генерирани индивиди. Популацията от първоначални индивиди итеративно се развива до популация от индивиди, където всеки индивид, който се състои от определен брой гени, представлява решение на проблема, ако удовлетворява целевата функция на пригодност (Fitness функция). Броят на възможните стойности на всеки ген се нарича мощност (кардиналност) на гена.
Развитието на популацията се състои в генериране на последователност от поколения, като качеството на индивидите в поколенията постепенно се подобрява. Fitness функцията за оценка на пригодността на всяка хромозома (индивид или правило) сравнява правилото с правила (хромозоми) в база от данни (знания) за комуникационни характеристики на известни прониквания (атаки) и нормални комуникационни характеристики. Към всеки индивид от поколението се прилагат последователно трите основни генетични оператора: селекция (на база стойността на Fitness функцията), кръстосване (рекомбинация) и мутация.
Първо, селекцията на най-подходящите индивиди се извършва въз основа на предварително дефинирана Fitness функция. Останалите индивиди се отстраняват.
Второ, обединяват се по двойки (кръстосване, рекомбинация) редица индивиди (хромозоми). Всяка индивидна двойка произвежда едно потомство (хромозома), като индивидите частично обменят гените си около една или повече случайно избрани пресечни точки.
Трето, избират се определен брой индивиди, към които се прилага операция-мутация, т.е. случайно избран ген на индивид рязко променя своята стойност, например от 0 на 1.

4.2. Дефиниране на синтаксиса и структурата на правилото (хромозомата) в генетичния алгоритъм

Генетичните алгоритми се прилагат за генериране на мрежови характеристики (правила) за оценка на трафика в компютърната мрежа. Тези правила се използват за определяне и диференциране на нормалните и аномалните мрежови свързвания. Аномални връзки са тези, които се отнасят до събития, оценени с висока вероятност като злонамерено проникване в мрежата. Правилата, съхранени в базата от правила (знания) на системата за откриване на проникване, са със синтаксис на клауза от предикатната логика [4,5]:

If {condition} then {act}

В частта *if* се дефинира състояние (условието), описано с мрежовите характеристики, като IP адреси на източник и местоназначение и номера на портове (използвани TCP/IP мрежови протоколи), продължителност на комуникацията и т.н., включително и индикация за вероятност от проникване. Тази част от правилото генетичният алгоритъм сравнява с мрежовите характеристики от правилата, съхранени в базата от правила на системата за откриване на проникване. Характеристиките в условната част са свързани чрез логически оператор AND. Частта *act* (действие) се отнася до действие, дефинирано от правилата за сигурност, като доклад за предупреждение към системния администратор, спиране на комуникацията, регистриране на съобщение в системни наблюдавани (проверявани) файлове или всички заедно, изброени по-горе. Някои мрежови характеристики имат по-голям относителен принос при дефиниране на мрежовите свързвания и комуникационен обмен.

4.3. Кодиране на мрежови характеристики (гените) на правилата (хромозомите)

Гените в хромозомите могат да бъдат представени с различни типове данни, двоични числа (байтове) десетични числя или числа с плаваща запетая. Това се обуславя от различния формат и диапазон от стойности на данните за различните мрежови характеристики. В Таблица 1 се привежда названието на мрежовите характеристики - атрибути на хромозомите, броят на гените, дефиниращи атрибутите на хромозомите и техните формати, съответно в първата, втората и третата колона.

Например, характеристиката „Duration“ има три компонента (часове, минути и секунди), всеки от които е представен от един ген от тип байт (Табл. 1). По същия начин, всяка от характеристиките “Protocol” („Протокол“), “Source Port Number”, „Порт за източник“, „Destination port number“ е кодирана с помощта на един ген от тип цяло число, а всяка от характеристиките „Source IP-v4“ и „Destination IP-v4“ има четири компонента. (a, b, c и d), всеки от които е представен от един ген от тип байт, „Source IP-v6“ и „Destination IP-v6“ имат осем компонента. (a, b, c, d, e, f, g, h), всеки от които е представен от един ген от тип байт.

Наименование на атрибутите на хромозомата	Брой на гените	Формат на кода
Source IP-v 4 address	4	a.b.c.d
Source IP-v 6 address	8	a.b.c.d.e.f.g.h
Destination IP -v 4 address	4	a.b.c.d
Destination IP -v 6 address	8	a.b.c.d.e.f.g.h
Source Port Number	1	Integer
Destination Port Number	1	Integer
Duration	3	h:m:s
State	1	Integer
Protocol	1	Integer
Number of Bytes Sent by Originator	1	Integer
Number of Bytes sent by Responder	1	Integer
Attack_name	1	Integer

Таблица 1. Атрибути, генна структура и кодове на мрежовите характеристики на хромозомата (правилото) в генетичния алгоритъм.

Атрибутът “Attack_name” (име на атака) се намира в частта на правилото (*act*) – *действие*, която класифицира мрежовите характеристики на етап обучение или определя характера на комуникацията на етап откриване на проникване, когато (*condition*) – *състоянието* или *условието* на дадено правило съвпада с това от етап обучение.

Пример на правило, което класифицира мрежова комуникация като атака Denial of Service - DoS (отказ на услуга) *Neptune* е следната хромозома [2]:

if (duration=“0:0:1” and protocol=“finger” and source_port=18982 and destination_port=79 and source_ip=“9.9.9.9” and destination_ip=“172.16.112.50”) then (attack_name=“neptune”).

Правилото показва, че ако мрежовият пакет произхожда от IP адрес 9.9.9.9 и порт 18982, и се изпраща на IP адрес 172.16.112.50 и порт 79 с помощта на протокола *finger*, а продължителността на комуникацията е 1 секунда, тогава най-вероятно е мрежова атака от тип neptune, която може да доведе до изключване на хоста на дестинацията (местоназначението на пакета). Всяко правило се кодира като хромозома, като се използва вектор с фиксирана дължина, където всяка мрежова характеристика се кодира, използвайки един или повече гени от различни типове (втората и третата колона от Таблица 1). Кодираната хромозома на правилото от горния пример получава вида

{0, 0, 1, 2, 18982, 79, 9, 9, 9, 9, 172, 16, 112, 50, 1}

Пример на правило, което извежда действие - спиране на комуникацията:

if {the connection has following information: source IP address 124.12.5.18; destination IP address: 130.18.206.55; destination port number: 21; connection time: 10.1 seconds} then {stop the connection}

Това правило може да се интерпретира по следния начин: ако съществува заявка за мрежова комуникация с IP адрес на източника 124.12.5.18, IP адрес на местоназначение (дестинация) 130.18.206.55, целеви порт на дестинацията с номер 21 и време за комуникация 10.1 секунди, тогава се спира създаването на това комуникационно свързване
С други думи, IP адресът 124.12.5.18 се разпознава от системата за идентификация на проникването като един от IP адресите в черния списък; следователно, всяка заявка за сервизна функция, инициирана от нея, се отхвърля.
Атрибутите на хромозомата, диапазона от стойности, примерни стойности на всеки атрибут и описание на атрибута са представени в следната последователност [5]:

Атрибут: IP адрес на източника
Диапазон на стойности: 0.0.0.0~255.255.255.255
Примерна стойност: d1.0b.**.** /209.11.??.??/
Описание: Подмрежа с IP адрес 209.11.0.0 до 209.11.255.255

Атрибут: IP адрес на дестинацията
Диапазон на стойности: 0.0.0.0~255.255.255.255
Примерна стойност: 82.12.b*.** /130.18.176+?.??/
Описание: Подмрежа с IP адрес 130.18.176.0 до 130.18.255.255

Атрибут: Номер порта на източника
Диапазон на стойности: 0~65535
Примерна стойност: 42335
Описание: Номер на порта на източника на комуникацията

Атрибут: Номер на порта на дестинацията (местоназначение)
Диапазон на стойности: 0~65535
Примерна стойност: 00080
Описание: Номер на порт на местоназначението, показва, че това е http услуга

Атрибут: Продължителност
Диапазон на стойности: 0~99999999
Примерна стойност: 00000482
Описание: Продължителност на комуникацията е 482 секунди

Атрибут: Състояние
Диапазон на стойности: 1~20
Примерна стойност: 11
Описание: Комуникацията се прекратява от инициатора, за вътрешна употреба

Атрибут: Протокол
Диапазон на стойности: 1~142
Примерна стойност: 9
Описание: Протоколът за тази комуникация е TCP

Атрибут: Брой байтове изпратени от подателя
Диапазон на стойности: 0~9999999999
Примерна стойност: 0000007320
Описание: Инициаторът изпраща 7320 байта данни

Атрибут: Брой байтове изпратени от приемащия кореспондент
Диапазон на стойности: 0~9999999999
Примерна стойност: 0000038891
Описание: Приемащият кореспондент изпраща 38891 байта данни

Пример на правило, което използва примерните стойности на атрибутите на хромозомата

if {the connection has following information: source IP address 209.11.??.??; destination IP address: 130.18.176+?.??; source port number: 42335; destination port number: 80; connection time: 482 seconds; the connection is stopped by the originator; the protocol used is TCP; the originator sent 7320 bytes of data; and the responder sent 38891 bytes of data} then {stop the connection}

В този случай кодираната хромозома има вида [5]:

/d, 1, 0, b, -1, -1, -1, -1, 8, 2, 1, 2, b, -1, -1, -1, 4, 2, 3, 3, 5, 0, 0, 0, 8, 0, 0, 0, 0, 0, 0, 0, 4, 8, 2, 1, 1, 9, 0, 0, 0, 0, 0, 0, 7, 3, 2, 0, 0, 0, 0, 0, 0, 3, 8, 8, 9, 1/

Правилото може да бъде интерпретирано по следния начин: ако мрежова комуникация с изходния IP адрес 209.11. ??. ?? (209.11.0.0 ~ 209.11.255.255), IP адрес на местоназначение 130.18.176. ?? (130.18.176.0 ~ 130.18.255.255), номер на порта на източника 42335, номер на порт за местоназначение 80, времетраене 482 секунди, завършва с състояние 11 (комуникацията е прекратена от създателя), използва протокол тип 9 (TCP), а източникът изпраща 7320 байта данни, отговарящите изпращат 38891 байта данни, тогава това е подозрително поведение и може да бъде идентифицирано като потенциално проникване.
Валидността на това правило се оценява чрез съвпадение на предварителен набор от данни, съставен от свързвания (комуникации), маркирани като аномални или нормални. Ако правилото е в състояние да намери аномално поведение, „награда” ще бъде даден на текущата хромозома. Ако правилото отговаря на нормална комуникация, ще бъде наложено „наказание“ върху хромозомата. Очевидно нито едно правило не може да се използва за разделяне на всички

аномални връзки от нормални връзки. Популацията се развива, за да намери оптималният набор от правила.
Използват се символите (‘*‘ и ,?‘) за означение на wildcards (мрежови части на IP адресите), като съответните гени в хромозомата са представени с -1. Тези wildcards се използват за представяне на диапазон от специфични мрежови адреси, т.е. представяне на мрежов блок (диапазон от IP адреси или номера на портове) в правило. След като информацията за полето на характеристиките е включена в правилата, способността на системата за откриване на проникване може да бъде подобрена, тъй като проникването може да започне от много различни адреси [5]. Включването на времетраенето на мрежовата комуникация в хромозомата осигурява включване на времева информация за мрежови връзки. Максималната стойност на продължителността е 99999999 секунди, което е повече от една година. Това е необходимо за идентифициране на сложни проникванията, които могат да обхванат часове, дни или дори месеци. Ще се подчертае още веднъж, че генетичният алгоритъм стартира с начална популация, която се състои от произволно избрани правила и се развива чрез използване на операторите на кръстосване и мутации. В съответствие с ефективността на оценъчната Fitness функцията, следващите популации са подчинени на правилата, които съответстват на проникващите свързвания. При **end** (край) на генетичния процес, алгоритъмът спира, правилата се селектират и добавят в базата на системата за откриване на проникващи свързвания.

Правилата за класифициране на атаки DoS (Smurf, Mailbomb), R2L Warezmaster, multihop), U2R (Snmpguess, Buffer-overflow), Probing (ip-sweep, saint), изведени от базата с данни за проникванията на DARPA-USA, имат следната структура [6]:

DOS:
Rule 1 – *if duration = 0 and protocol_type = tcmp and dst_host_srv_count = 255 and then Smurf*

Rule 2 – *if duration = 1 V 5 V 11 and protocol_type-tcp and dst_host_srv_count >= 2^ <= 247 and then Mailbomb*

R2L:
Rule 3 – *if duration = 0v duration <=289 and protocol_type = tcp and dst_host_srv_count >=1^ <= 128 and then waremaster*

Rule 4 – *if duration = 0 and protocol_type = icmp V top V udp and dst_host_srv_count >= 1^ <= 20 and then multihop*

U2R:
Rule 5 – *if duration = 0 V duration <= 289 and protocol_type = udp and src_bytes-I > and then Snmpguess*

Rule 6 – *if 1 and = 0 and protocol_type = tcp and dst_host_srv_count <= 100 and then buffer–overflow*

Probe:

Rule 7: *if duration = 0 and protocol_type – icmp and dst_host_srv_count >= 1^ <=255 and then ipsweep*

Rule 8: if duration = 0 and duration <= 11 and protocol_type – icmp V tcp V udp and dst_host_srv_count >=1^ <=255 and then saint

В дефиницията на горните правила са използвани следните означения „<=“ (по-малко или равно), „=>“ (равно или по-голямо), ^ (логическо „и“).

5. Заключение

В настоящата статия е направена обща характеристика на система за откриване на проникване в компютърните мрежи. Приведени са видове категории прониквания в компютърните мрежи и е дадено кратко описание на всяка една категория. Дефинирани са параметрите на генетичния алгоритъм, използван за откриване и разпознаване на атаки в компютърни мрежи. Разкрити са синтаксисът и структурата на различни правила (хромозоми) в генетичния алгоритъм, както и кодирането на мрежовите характеристики (гените).
Като активност на авторите в областта на откриване на злонамерени прониквания в компютърните мрежи чрез прилагане на подхода на генетичните алгоритми се предвижда изграждане на база от данни (правила, знания) за нови неизследвани структури от мрежови характеристики на компютърни атаки, както и методи за тяхното противодействие и превенция.

Литература

1. M. Sazzadul Hoque, Md. A. Mukit, Md. A. N. Bikas. An implementation of intrusion detection system using genetic algorithm, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012, pp. 109-119.
2. R. H. Gong, M. Zulkernine, P. Abolmaesumi, ”A software implementation of a genetic algorithm based approach to network intrusion detection”, in Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks, SNPD/SAWN’05), 0-7695-2294-7/05, 2005.
3. Omprakash Chandrakar, Rekha Singh, Lal Bihari Barik. Application of Genetic Algorithm in Intrusion Detection System, Control Theory and Informatics, Vol.4, No.1, 2014, pp. 50-57.
4. Vr. Yewale, V. Jethani, T. Ghorpade. Applying Genetic Algorithm to Intrusion Detection System, International Journal of Science and Research (IJSR), Volume 4 Issue 4, April 2015, pp. 524-529.
5. Ehab Talal Abde-Ra'of Bader, Hebah H. O. Nasereddin. Using genetic algorithm in network security, IJRRAS vol. 5 (2), Nov. 2010, pp. 148-154.
6. B. Uppalaiah, K. Anand, B. Narsimha, S. Swaraj, T. Bharat. Genetic Algorithm Approach to Intrusion Detection System, International Journal of Computer science e and techhnology IJCST Vol. 3, Issue 1, Jan. - March 2012, pp. 156-160.
7. F. Alabsi, R. Naoum, Fitness Function for Genetic Algorithm used in Intrusion Detection System, International Journal of Applied Science and Technology, Vol. 2 No. 4; April 2012, pp. 129-134.
8. S. Chowdhury, S. Kumar Das, Ann. Das. Application of genetic algorithm in communication network security, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2015, pp. 274-280.
9. Ch. Sinclair, L. Pierce. An application of machine learning to network intrusion detection, published in: Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99), 6-10 Dec. 1999. DOI: 10.1109/CSAC.1999.816048.
10. P. A. Diaz-Gomez, D. F. Hougen. Improved off-line intrusion detection using genetic algorithm, in Proceedings of the Seventh International Conference on Enterprise Information Systems, 2005. http://www.cameron.edu/~pdiaz-go/Art_ICEIS.pdf
11. R. Shanmugavadivu, Dr. N. Nagarajan. Network intrusion detection system using Fuzzy logic. Indian Journal of Computer Science and Engineering (IJCSE), vol. 2, No1, 2011, pp. 101-111.
12. R. Messenger R. Dove. Basic genetic algorithm pattern for use in self-organizing agile security, IEEE International Carnahan Conference on Security Technology (ICCST), Boston, MA, USA, 15-18 Oct. 2012, 2 Aug. 2012.
13. S. Mukkamala, A. Sung, A. Abrham. (2004), Modeling Intrusion Detection System using Linear Genetic Programming Approach, Proceeding IEA/AIE 17th International Conference on Innovations in Applied Artificial Intelligence, pp. 633-642, ISBN: 3-540-22007-0.
https://www.researchgate.net/publication/221049814_Modeling_Intrusion_Detection_Systems_Using_Linear_Genetic_Programming_Approach

http://www.rmltech.com/doclink/LGP%20Based%20IDS.pdf.

14. V. Bapuji, R. N. Kumar, A. Goverdan, and S. Sharma, “Soft Computing and Artificial Intelligence Techniques for Intrusion Detection System,” Networks and Complex Systems, vol. 2, no. 4, 2012.
15. An. Goya, Ch. Kumar. GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System, 2007.
https://pdfs.semanticscholar.org/6c8e/6708a1a737a9a5509de2fba46f8de1aff7e3.pdf
16. Wei Li, Using Genetic Algorithm for Network Intrusion Detection,
https://pdfs.semanticscholar.org/9175/54c7cce69e6ee9708020863f2bd27fa986a6.pdf
17. Sh. Devi, R. Nagpal. Intrusion Detection System Using Genetic Algorithm - A Review, International Journal of Computing & Business Research, Proceedings of ‘I-Society 2012’atGKU,Talwandi Sabo Bathinda (Punjab). ISSN (Online): 2229-6166