DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.2.3
УДК 004.775:004.491
ББК 32.972.53

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В ЗАЩИТЕ ВЕБ-ПРИЛОЖЕНИЙ

Марина Ивановна Ожиганова

Кандидат технических наук, доцент кафедры информационной безопасности,
Севастопольский государственный университет
vip.tapki@list.ru
ул. Университетская, 33, 299053 г. Севастополь, Российская Федерация

Эмиль Сейфуллаевич Куртаметов

Магистрант кафедры информационной безопасности,
Севастопольский государственный университет
emilkurtametov@gmail.com
ул. Университетская, 33, 299053 г. Севастополь, Российская Федерация

Аннотация. Целью данной статьи является исследование особенностей использования машинного обучения в защите веб-приложений. Были изучены методы защиты веб-приложения и способы обучения нейронных сетей.Результатом данной работы является теоретический обзор нейросетевой защиты веб-приложения.

Ключевые слова: сетевая система, информационная безопасность, машинное обучение, брандмауэр, веб-приложение, средства защиты, система обнаружения вторжений, сканер веб-приложения, брандмауэр веб-приложения, СОВ.

Введение

Безопасность сетевых системстало необходимостью, так как все больше важной информации хранится и используется в режиме онлайн. Распространение веб-приложений открывает новые векторы атаки. Традиционные механизмы защиты, такие как брандмауэры, не предназначены для защиты веб-приложений и поэтому не обеспечивают адекватной защиты. Текущие атаки не могут быть предотвращены только путем блокирования портов 80 (HTTP) и 443 (HTTPS).

Превентивные меры (например, правила брандмауэра веб-приложения) не всегда возможны. Сигнатурные методы для обнаружения всегда находятся позади фактического события.

Сетевые брандмауэры с принудительным применением протокола обычно обеспечивают первую линию защиты, задерживая большинство основных атак на периметре сети. Они, в основном, работают на сетевом, сессионном и транспортном уровнях эталонной модели сети (OSI).

Разработчики значительно расширили возможности сетевых брандмауэров для контроля целостности широкого спектра протоколов верхнего уровня, таких как DNS, FTP, HTTP, SMTP и TFTP.

Стандартные брандмауэры могут помочь ограничить или разрешить доступ к сетевым портам. Хотя брандмауэры прокси-сер-

© Ожиганова М.И., Куртаметов Э.С., 2020

вера приложений существуют, они не могут понять конкретное содержимое всех веб-приложений, запускаемых предприятием.

Существует два подхода защиты:

1. На основе сигнатурного анализа: брандмауэр веб-приложения идентифицирует атаки посредством проверки веб-запроса на соответствие сигнатуре атаки.

2. На основе аномального поведения: брандмауэр веб-приложения идентифицирует атаки путем обнаружения аномальных шаблонов трафика [9].

Защита веб-приложения

Защита веб-приложений – это отрасль информационной безопасности, которая обеспечивает защиту веб-сайтов и веб-приложений. Она отличается от других ветвей информационной безопасности тем, что защита веб-приложений сосредоточена на уязвимостях в коде приложения, которые обнаруживаются во время сеанса пользователя в интернете.

Большинство атак на веб-серверы осуществляются через сетевые брандмауэры и через порты http (80) или https (443). Некоторые из наиболее часто используемых методов взлома включают отказ в обслуживании, утечку, межсайтовый скриптинг, SQL-инъекции и раскрытие информации [8].

Для обеспечения безопасности веб-приложений помимо стандартных брандмауэров на прикладном уровне используются различные типы решений такие как: внешние инструменты – сканеры веб-приложений (WAS) и брандмауэры (WAF) и внутренние – само приложение должно быть самозащищенным [10].

Сканер веб-приложений (WAS) – это автоматизированная программа, которая проверяет веб-приложения на наличие определенных уязвимостей в системе безопасности. WAS использует алгоритм фильтрации для обнаружения уязвимостей в веб-приложениях основанный на отрицательной логике (черный список). Фильтрация отрицательной логики, построенная на сигнатурах известных атак, позволяет системам безопасности предотвратить попадание на защищенные серверы любых запросов, которые могут соответствовать сигнатурам атак [10].

Брандмауэры веб-приложений (WAF) – это аппаратные или программные устройства, предназначенные для мониторинга трафика веб-сайта, с возможность применения политики к транзакциям браузера сервера.Чтобы отличить обычные запросы от несанкционированных запросов, WAF используют набор правил фильтрации в виде белых списков, черных списков или их комбинации. Обычно WAF передает приложению только те запросы, которые классифицируются как обычные запросы. Запросы, классифицированные как мошеннические, обычно блокируются и, таким образом, не передаются в приложение. Создание наборов правил фильтра является сложной задачей, потому что с одной стороны, если WAF блокирует некоторые обычные запросы (ложное срабатывание), то приложение может больше не функционировать. С другой стороны, если WAF не блокирует все посторонние запросы (ложноотрицательные), то злоумышленник может обойти WAF и использовать уязвимость в приложении [4].

Позитивная логическая фильтрация позволяет выполнять допустимые запросы, основанные на наборе сигнатур (белый список), определяющие, какие типы коммуникаций защищенный сервер знает как обрабатывать; это предотвращает любые запросы, не определенные как допустимые, от достижения защищенных серверов [7].

Фильтрация на основе сеанса использует правила на основе положительной логики, но позволяет включать переменные в набор правил. Значения переменных задаются динамически во время пользовательских сеансов.

Недостатки положительной логической фильтрации – это требование большой базы данных уязвимостей, основанной на правилах регулярных выражений. Это вызывает плохую пропускную способность, требует больше ресурсов, с трудом адаптируется к большим веб-системам [5].

За счет уменьшения количества правил, для улучшения пропускной способности, снижается качество обнаружения уязвимостей. С целью повышения производительности WAF, пропускной способности, WAF разрабатываются с использованием методов искусственного интеллекта (искусственные нейронные сети, нечеткая логика).

Для обнаружения атак используются два способа: сигнатурный и аномальный. Первый используется для идентификации известных атак и требует регулярное обновление сигнатур, в то время как второй используется для идентификации неизвестных или новых атак, что будет являться отклонением модели, построенной на начальном этапе обучения без атак. Оба способа будут определять атаку вместолегитимных вебзапросов [6].

Существуют различия между обычным брандмауэром и брандмауэром веб-приложений. Обычный брандмауэр имеет дело с сетевым уровнем, а брандмауэр веб-приложения имеет дело с прикладным уровнем.

Искусственная нейронная сеть состоит из группы обрабатывающих элементов (нейронов), которые тесно связаны между собой и преобразуют набор входных данных в набор предпочтительных выходных [2].

Искусственные нейронные сети являются альтернативами. Первое преимущество в использовании нейронной сети при обнаружении атак будет заключаться в гибкости, которую эта сеть обеспечит. Нейронная сеть была бы способна анализировать данные из этой сети, даже если эти данные являются неполными или неясными. Аналогичным образом, сеть будет обладать способностью к анализуданных нелинейным образом. Кроме того, поскольку некоторые атаки могут быть проведены против сети в скоординированной атаке несколькими злоумышленниками, способность обрабатывать данные из нескольких источников в нелинейнойформе особенно важна [3].

Проблема частого обновления традиционного детектора атак также сведена к минимуму. Нейросеть обладает свойством обобщения и, следовательно, способна обнаруживать неизвестные атаки и даже вариации известных атак. Еще одна причина использовать СОВ на основе нейронной сети заключается в том, что система может кластеризировать шаблоны, которые имеют схожие черты, таким образом, проблема классификации в обнаружении атаки может быть решена. Естественная скорость работы нейронных сетей является еще одним преимуществом [1].

Заключение

Система, созданная на основе машинного обучения, обладает возможностью обнаружения новых видов атак, не требующих обновления сигнатур. Также нейронная сеть обеспечивает возможность прогнозирования для обнаружения случаев вторжения, что проявляется в способности определять что и где может произойти в процессе атаки. Поскольку нейросеть обучается на аномалиях поведения пользователя, неоднократно совершавшего попытки взлома, она полностью адаптирована к особенностям защищаемого WEB-приложения.

СПИСОК ЛИТЕРАТУРЫ

1. Белоглазов, Д. А. Особенности нейросетевых решений, достоинства и недостатки, перспективы применения / Д. А. Белоглазов // Известия ЮФУ. Технические науки. – 2008. – № 7. – Электрон. текстовые дан. – Режим доступа: https://cyberleninka.ru/article/n/osobennosti-neyrosetevyh-resheniy-dostoinstva-i-nedostatki-perspektivy-primeneniya (дата обращения: 02.02.2020). – Загл. с экрана.

2. Искусственные нейронные сети (ИНС). – Электрон. текстовые дан. – Режим доступа: https://www.it.ua/ru/knowledge-base/technology-innovation/iskusstvennye-nejronnye-seti-ins (дата обращения: 02.02.2020). – Загл. с экрана.

3. Фимичев, Н. Н. Применение нейронных сетей в обнаружении вторжений / Н. Н. Фимичев / / Современные научные исследования и инновации. – 2015. – № 10. – Электрон. текстовые дан. – Режим доступа: http://web.snauka.ru/issues/2015/10/58404 (дата обращения: 02.02.2020). – Загл. с экрана.

4. Чем защищают сайты, или Зачем нужен WAF? – Электрон. текстовые дан. – Режим доступа: https://habr.com/ru/company/pt/blog/269165/ (дата обращения: 02.02.2020). – Загл. с экрана.

5. Schmitt, I. WAFFle: Fingerprinting Filter Rules of Web Application Firewalls / I. Schmitt and S. Schinzel. – University of Engineering and Technology, Taxila, Jule 2012.

6. Kazanavicius, E. Securing Web Application By Embedded Firewall, Electronics And Electrical Engineering / E. Kazanavicius, V. Kazanavicius, and A. Venckauskas // Elektronika ir elektrotechnika. – 2012. – № 3. – P. 119.

7. Khochare, N. Web Application Vulnerabilities Detection Techniques Survey / N. Khochare, S. Chalurkar,

and B. B. Meshram // IJCSNS International Journal of Computer Science and Network Security. – 2013. – Vol. 13, № 6. – June 2013.

8. Panella, J. «Web Application Security» the OWASP Top 10 / J. Panella. – Sapient Corporation, SapientNitro, March 22, 2011.

9. Web Application Security, Top Ten Project Theme Page of the OWASP Website, OWASP_ Top _Ten Project. – (February 2008). – Electronic text data. – Mode of access: http://www.infosec.gov.hk/english/technical/files/web_app.pdf (date of access: 02.02.2020). – Title from screen

10. Web Application Scanner. – Electronic text data. – Mode of access: https://www.veracode.com/security/web-application-scanner (date of access: 02.02.2020). – Title from screen

REFERENCES

1. Beloglazov D.A. Osobennosti neirosetevih resheniy, dostoinstva i nedostatki, perspective primeneniya. *News SFU. Technicalscience*, 2008, no. 7. URL: https://cyberleninka.ru/article/n/osobennosti-neyrosetevyh-resheniy-dostoinstva-i-nedostatki-perspektivy-primeneniya (accessed: 02.02.2020).

2. *Iskysstvenie neironnie seti (INS)*. URL: https://www.it.ua/ru/knowledge-base/technology-innovation/iskusstvennye-nejronnye-seti-ins (accessed: 02.02.2020).

3. Fimichev N.N. Primenenie neironnih setei v obnaruzhenii vtorzheniy. *Modern research and innovation*, 2015, no. 10. URL: http://web.snauka.ru/issues/2015/10/58404 (accessed: 02.02.2020).

4. *Chem Zashishayut saiti, ili Zachem nyzhen WAF?* URL: https://habr.com/ru/company/pt/blog/269165/ (accessed: 02.02.2020).

5. Schmitt I. and Schinzel S. *WAFFle: Fingerprinting Filter Rules of Web Application Firewalls*. University of Engineering and Technology, Taxila, Jule 2012.

6. Kazanavicius E., Kazanavicius V., and Venckauskas A. Securing Web Application By Embedded Firewall, Electronics And Electrical Engineering. *Elektronika ir elektrotechnika*, 2012, no. 3, pp. 119.

7. Khochare N., Chalurkar S., and Meshram B.B. Web Application Vulnerabilities Detection Techniques Survey. *IJCSNS International Journal of Computer Science and Network Security*, vol. 13, no. 6, June 2013.

8. Panella J. *«Web Application Security» the OWASP Top 10*. Sapient Corporation, SapientNitro, March 22, 2011.

9. *Web Application Security, Top Ten Project Theme Page of the OWASP Website, OWASP_ Top _Ten Project*. (February 2008). URL: http://www.infosec.gov.hk/english/technical/files/web_app.pdf (accessed: 02.02.2020).

10. *Web Application Scanner*. URL: https://www.veracode.com/security/web-application-scanner (accessed: 02.02.2020).

USING NEURAL NETWORKS TO PROTECT WEB APPLICATIONS

Marina I. Ozhiganova

Candidate of Sciences (Engineering), Associate Professor,
Information Security Department,
Sevastopol State University
vip.tapki@list.ru
Universitetskaya St, 33, 299053 Sevastopol, Russian Federation

Emil S. Kurtametov

Student, Department of Information Security,
Sevastopol State University
emilkurtametov@gmail.com
Universitetskaya St, 33, 299053 Sevastopol, Russian Federation

Abstract. Security of network systems has become a necessity, as more and more important information is stored and used online. The spread of web applications opens up new attack vectors. Traditional security mechanisms, such as firewalls, are not designed to protect web applications and therefore do not provide adequate protection. Current attacks cannot be prevented only by blocking ports 80 (HTTP) and 443 (HTTPS). Preventative measures (such as web application firewall rules) are not always possible. Signature methods for detection

are always behind the actual event. Protocol-enforced network firewalls usually provide the first line of defense, delaying most major attacks on the network perimeter. They mainly work on the network, session, and transport layers of the reference network model (OSI). Developers have significantly expanded the capabilities of network firewalls to control the integrity of a wide range of top-level protocols, such as DNS, FTP, HTTP, SMTP, and TFTP. Standard firewalls can help restrict or allow access to network ports. Although application proxy firewalls exist, they cannot understand the specific content of all web applications run by an enterprise. The purpose of this article is to study the features of using machine learning in web application protection. Methods of web application security and learning neural networks were studied. The result of this work is a theoretical overview of the neural network security of a web application.

Key words: network system, information security, machine learning, firewall, web application, security tools, intrusion detection system, WAS, WAF, IDS.