М.А. Баймяшкин

ОБЗОР УТИЛИТ, ОСУЩЕСТВЛЯЮЩИХ СЕТЕВЫЕ АТАКИ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ИМ

(Самарский университет)

Аннотация

Настоящая работа посвящена анализу наиболее популярных утилит для проведения сетевых атак. Конечной задачей хакера является дестабилизация сайтов и серверов, вывод их из строя, получение личных данных каждого пользователя сети. В работе описаны особенности атак на реальный сервер утилитами Nmap, Hping3, LOIC и по ответным пакетам сформулированы квалификационные признаки, позволяющие выявить начало атаки. В дальнейшем указанные признаки могут быть внедрены на SDN оборудовании для затруднения начального этапа атаки, проводимой злоумышленниками.

Введение

Сетевая атака — разрушающее воздействие на информационный ресурс, осуществляемое программно по каналам связи. Для её осуществления применяются различные утилиты.

Данная работа посвящена обзору утилит для проведения сетевых атак, с целью формирования методов противодействия им. При любой атаке главная цель злоумышленника, как правило – это получение несанкционированного доступа к информации. С этой целью хакер использует различные программы, которые осуществляет воздействие на атакуемого. Далее будет рассказано о некоторых из них.

Список утилит и их обзор

Существует множество программ, которые используются злоумышленниками, рассмотрим наиболее популярные из них.

1) Nmap

Nmap является стандартной утилитой для сканирования портов. Она может быть использована для проверки безопасности, или же просто для определения сервисов запущенных на узле, для идентификации ОС и приложений, определения типа фаервола используемого на сканируемом узле.

2) Hping3

Hping3 – генератор пакетов и анализатор для TCP/IP протокола. Он поддерживает протоколы TCP, UDP, ICMP, имеет режим traceroute, возможность отправки файлов между закрытым каналом и многими другими функциями.

3) LOIC

LOIC - утилита, предназначенная для осуществления DDoS-атак, написанная на языке программирования C#. Осуществляет атаки по протоколам TCP, UDP или HTTP.

Экспериментальное применение утилит

1) Nmap

Команда запуска Nmap очень проста для этого достаточно передать ей в параметрах целевой IP адрес или сеть, а также указать опции при необходимости:

$ nmap опции адрес

Теперь давайте рассмотрим основные опции, которые понадобятся нам в этой статье.

- -sP - проверка доступности хоста с помощью ping;
- -sS/sT/sA/sW/sM - TCP сканирование;
- -sU - UDP сканирование;
- -sN/sF/sX - TCP NULL, FIN и XMAS сканирование.

2) Hping3

Также, как и в nmap, запуск утилиты осуществляется с помощью команды с указанием опций и адреса:

$ hping3 опции адрес

Hping3 по умолчанию (без параметров) отправляет нулевой пакет с заголовком TCP на порт 0.

Возможен выбор другого протокола с помощью числовой опции, доступной для каждого из них:

- -0 (режим Raw IP)
- -1 (режим ICMP)
- -2 (режим UDP)
- -8 (Режим сканирования)
- -9 (Режим прослушивания)

Поскольку hping3 использует TCP по умолчанию, отсутствие указанных ниже параметров отправит сегмент TCP.

При использовании TCP мы можем решить либо опустить флаги (по умолчанию), либо установить флаг, используя один из следующих параметров: -S (SYN), -A (ACK), -R (RST), -F (FIN), -P (PUSH), -U (URG), -X (XMAS), -Y (YMAS).

3) LOIC

Главной задумкой LOIC было то, что любой пользователь, даже если у него нет ни малейшего представления о проведении атак, может поучаствовать в процессе. Для использования утилиты достаточно указать адрес жертвы и выбрать тип атаки.

Квалификационные признаки для противодействия

При использовании утилит, атакуемый сервер даёт отклики. Эти отклики были записаны во время атаки и проанализированы. Как результат этого анализа, были сформулированы квалификационные признаки.

Для портов UDP таким квалификационным признаком является отклик, содержащий пакет ICMP типа 3.3(порт недостижим). При повторном появлении такого пакета на SDN коммутатора с одного и того же внешнего IP адреса, получение пакетов с этого IP адреса должно быть блокировано.

При атаке пакетами TCP SYN, TCP NULL, TCP FIN и TCP XMAS отправляется пакет TCP с флагами ACK и RST, сбрасывающим соединение. При атаке пакетами TCP ACK в ответ посылались TCP пакеты с флагами RST. Фактически при любой атаке пакетами TCP квалификационным признаком атаки является пакет с флагом RST. При повторном получении этого пакета, адрес должен быть заблокирован.

Для ICMP пакетов мы не стали формулировать квалификационные признаки так как их достаточно трудно сформулировать, а полное перекрытие может привести к полному блокированию проверок по работоспособности сети.

Как показал эксперимент, сканирование портов и сетевые атаки, вызывающие отказ в обслуживании, дают одинаковые квалификационные признаки.

Заключение

В настоящей работе были рассмотрены и проанализированы наиболее популярные утилиты для сетевых атак. Конечной задачей хакера является дестабилизация сайтов и серверов, вывод их из строя, получение личных данных каждого пользователя сети. Наша задача состоит в том, чтобы противодействовать атакам злоумышленника. Для этого мы описываем особенности сетевых атак проводим эксперимент на реальном сервере при помощи утилит для их реализации, на основании этого эксперимента формулируются квалификационные признаки для определения адреса с которого осуществляется вторжение.

Литература

1. Котенко И. В., Карсаев О. И. Использование многоагентных технологий для комплексной защиты информационных ресурсов в компьютерных сетях //Известия Южного федерального университета. Технические науки. – 2001. – Т. 22. – №. 4.

2. Сагатов Е.С., Шкирдов Д.А., Сухов А.М. и др. Обнаружение источников сетевых вторжений с помощью метода ловушек // Защита информации. Инсайд. — 2018. — № 5 (83). — С. 16-21

3. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия //Труды Института системного анализа Российской академии наук. – 2009. – Т. 41. – С. 104-146.

4. Orebaugh A., Pinkard B. Nmap in the enterprise: your guide to network scanning. – Elsevier, 2011.

5. Buchanan B. et al. A methodology to evaluate rate-based intrusion prevention system against distributed denial-of-service (DDoS) //Cyberforensics 2011. – 2011.

6. Dayal N., Srivastava S. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN //2017 9th International Conference on Communication Systems and Networks (COMSNETS). – IEEE, 2017. – С. 274-281.

7. Zegzhda P. D., Lavrova D. S., Shtyrkina A. A. Multifractal analysis of Internet backbone traffic for detecting denial of service attacks //Automatic Control and Computer Sciences. – 2018. – Т. 52. – №. 8. – С. 936-944.

К.О. Володина

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ МУП ПАТП№2 ПРИ ПОМОЩИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

(КНИТУ-КАИ им. А.Н. Туполева, Казань)

Аннотация

В данной статье рассматривается обеспечение безопасности предприятия при помощи установки системы видеонаблюдения, а так же проводится анализ выбора аппаратной и программной части системы видеонаблюдения.

В настоящий момент установка и доработка системы видеонаблюдения является приоритетной задачей компаний, в особенности больших предприятий. Несанкционированное проникновение или кража влияет как на финансовую составляющую предприятия, так и на производство в целом. Грамотно проанализировать исходные данные, такие как: квадратура помещений, имеющиеся оборудование, обслуживающий персонал, выявить уязвимости и возможные угрозы, а также предложить решения по ликвидации выявленных уязвимостей и угроз – основная задача специалиста. Также необходимо оценить рентабельность и эффективность предложенных решений по усовершенствованию и установке системы. А так как количество угроз кражи и несанкционированных проникновений постоянно растет, то постоянный анализ и своевременная модернизация системы является перманентными событиями.

Защита предприятия должна включать в себя физические, внутренние, информационные, технические и экономические компоненты. Все эти комплексы должны быть тесно связаны и дополнены друг другом. Обеспечение безопасности способствует защите от несанкционированного проникновения, своевременное реагирование на внештатные ситуации, выявление неправомерных действий персонала. В настоящее время выделяют следующие построение системы безопасности:

- Охранная сигнализация;
- Противопожарная сигнализация;
- Видеонаблюдение;
- Система контроля и управления доступом;
- Механизмы защиты информационной безопасности.