АНАЛИЗ МЕТОДА СКАНИРОВАНИЯ ЛВС

Савик К. В.
Факультет информационных технологий и управления, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: zahariev@bsuir.by, hootkich@gmail.com

Сетевая безопасность состоит из аппаратных и программных компонентов, предназначенных для защиты данных и информации, обрабатываемой в сети. Кроме того, эти компоненты обеспечивают установку профилактических мер для защиты сетевой инфраструктуры и ее данных от несанкционированного доступа, изменения данных, повреждения и несанкционированного раскрытия. В конечном счете, сетевая безопасность предназначена для создания безопасной среды, в которой пользователи компьютеров, программ и мобильных приложений могут выполнять компьютерные или цифровые действия без сетевых уязвимостей.

Введение

Надежность и безопасность сети крайне важны в мире, где компьютерные сети являются ключевым элементом в коммуникациях и транзакциях между объектами. Сетевые администраторы, правительство, консультанты по безопасности и хакеры использовали различные инструменты для проверки уязвимостей целевых сетей, таких как, например, возможность удаленного доступа к компьютерам в сети и управления ими без авторизации. Благодаря этому интенсивному тестированию целевая сеть может быть «защищена» от распространенных уязвимостей и эзотерических атак. Однако существующие системы тестирования дают противоречивые результаты, используют недоказанные методы или наносят ущерб целевой сети.

Таким образом, целью данной работы является исследование метода сканирования узлов в сети, частности на открытые порты, на примере утилиты "nmap"(Network Mapper).

I. NMAP

NMAP (Network Mapper) — это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Nmap использует "сырые"IP пакеты оригинальным способом, чтобы определить какие хосты доступны в сети, какие службы (название приложения и версию) они предлагают, какие операционные системы (и версии ОС) они используют, какие типы пакетных фильтров/брандмауэров используются и еще множество других характеристик. В то время, как Nmap обычно используется для проверки безопасности, многие системные администраторы находят ее полезной для обычных задач, таких как контролирование структуры сети, управление расписаниями запуска служб и учет времени работы хоста или службы.

Выходные данные Nmap это список просканированных целей с дополнительной информацией по каждой из них в зависимости от заданных опций. Ключевой информацией является «таблица важных портов». Эта таблица содержит номер порта, протокол, имя службы и состояние. Состояние может иметь значение open (открыт), filtered (фильтруется), closed (закрыт) или unfiltered (не фильтруется). Открыт означает, что приложение на целевой машине готово для установки соединения/принятия пакетов на этот порт. Фильтруется означает, что брандмауэр, сетевой фильтр, или какая-то другая помеха в сети блокирует порт, и Nmap не может установить открыт этот порт или закрыт. Закрытые порты не связаны ни с каким приложением, но могут быть открыты в любой момент. Порты расцениваются как не фильтрованные, когда они отвечают на запросы Nmap, но Nmap не может определить открыты они или закрыты. Nmap выдает комбинации открыт|фильтруется и закрыт|фильтруется, когда не может определить, какое из этих двух состояний описывает порт. Эта таблица также может предоставлять детали о версии программного обеспечения, если это было запрошено. Когда осуществляется сканирование по IP протоколу (-sO), Nmap предоставляет информацию о поддерживаемых протоколах, а не об открытых портах.

II. Методы сканирования

Синтаксис запуска программы следующий: Nmap [Scan type(s)] [options] target specification, где вместо Scan type указывается тип сканирования (по умолчанию, если это место оставить пустым, Nmap будет открыто сканировать доступные порты). В качестве options вводятся всевозможные ключи и параметры сканирования, а вместо target specification — либо IP-адрес компьютера, либо диапазон IP-адресов (который определяется маской подсети), либо название хоста.

Когда запускается сканер Nmap, и начинается скнирование портов, сначала идёт запрос

пингом, а затем поэтапно сканируются и порты. Следовательно, не ответив на пинг, хост сканироваться не будет. Этот подход можно считать одним из методов защиты от сканирования.

Пример работы nmap:

nmap -v scanme.nmap.org - сканер проверит хост на наличие открытых портов и служб, которые слушают эти порты.

Nmap scan report for scanme.nmap.org (45.33.32.156) Not shown: 994 closed ports PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 139/tcp filtered netbios-ssn 445/tcp filtered microsoft-ds 9929/tcp open nping-echo 31337/tcp open Elite

Nmap done: 1 IP address (1 host up) scanned in 7.00 seconds

Из показанного вывода можно увидеть, что открыты 22, 80, 9929, 31337 порты и т.к они имеют состояние open, то это означает, что приложение на целевой машине готово к принятию пакетов на указанный порт. Порты 139 и 445 с состоянием filtered показывают, что брандмауэр, фильтр, или что-то другое в сети блокирует порт, так что Nmap не может определить, является ли порт открытым или закрытым.

III. Пример использования Nmap

В эффективной атаке необходимо проанализировать цель и используемые технологии, чтобы знать, какой тип атаки следует запустить. Запускать атаки, относящиеся к уязвимостям UNIX, если цель работает только на серверах Microsoft, не имеет смысла. Небольшое время, затрачиваемое на исследования, экономит много времени при атаке проникновения.

Цель сканирования узлов - найти следующую информацию:

- IP-адреса хостов в целевой сети;
- операционные системы на целевых системах;
- доступные порты протокола пользовательских дейтаграмм (UDP) и протокола управления передачей (TCP) в целевых системах.

В качестве примера, возмьмем последнюю цель сканирования узлов для получения несанкцианированного доступа. В исследовательский целях, сканируется локальная машина.

nmap -p "*"localhost - сканирует localhost на все порты. Nmap scan report for localhost (127.0.0.1) Host is up (0.000065s latency). Not shown: 8287 closed ports PORT STATE SERVICE 22/tcp open ssh 139/tcp open netbios-ssn 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp open ppp 5432/tcp open postgresql

Из результата особо интересует 22 порт, доступный по ssh. Для получения доступа по ssh необходимо знать пользователя и пароль. В качестве пользователя можно испльзовать root (в качестве примера будет использован другой пользователь). Пароль будет получен с помощью утилиты hydra.

hydra -l k.savik -P ./pass.txt localhost -t 4 ssh [DATA] max 4 tasks per 1 server, overall 4 tasks, 7 login tries, 2 tries per task [DATA] attacking ssh://localhost:22/ [22][ssh] host: localhost, login: k.savik password: 1111111 1 of 1 target successfully completed, 1 valid password found

Как видно из вывода, пароль - 1111111. И с помощью его можно получить удаленнуй доступ по ssh.

IV. Вывод

В ходе проведенной работы был проведен обзор сканирования узлов при помощи утилиты nmap, а так же ее практическое применение в связке с утилитой hydra для получения удаленного доступа по ssh протоколу. Исходя из проведенной работы, стало видно, насколько важен этап сбора информации о узлах в сети и насколько уязвимыми они могут быть.

1. Weir, Matt, et al. "Password cracking using probabilistic context-free grammars."Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009.
2. http://xgu.ru/downloads/mac2port
3. https://www.securitylab.ru/analytics/216229.php
4. Wang, K. C. SYSTEMS PROGRAMMING IN UNIX/LINUX. Springer, 2018.