Л33. Стандартное проведение тестов на проникновение

Стандарт выполнения тестирования на проникновение состоит из семи основных разделов. Они охватывают все требования, условия и методы проведения испытаний на проникновение: от разведки и до попыток проведения пентестов; этапы сбора информации и моделирования угроз, когда, чтобы добиться лучших результатов проверки, испытатели работают инкогнито; этапы исследования уязвимостей, эксплуатации и пост-эксплуатации, когда практические знания испытателей в области безопасности соединяются с данными, полученными в ходе проведения тестов на проникновение; и как заключительный этап — отчетность, в которой вся информация предоставляется в виде, понятном клиенту.

Сегодня действует первая версия, в которой все стандартные элементы испытаны в реальных условиях и утверждены. Вторая версия находится в стадии разработки. В ней все требования будут детализированы, уточнены и усовершенствованы. Поскольку план каждого теста на проникновение разрабатывается индивидуально, в нем могут быть применены разные тесты: от тестирования веб-приложений до проведения испытаний, предусмотренных для тестирования методом «черного ящика». С помощью этого плана сразу можно определить ожидаемый уровень сложности конкретного исследования и применить его в необходимых, по мнению организации, объемах и областях. Предварительные результаты исследования можно увидеть в разделе, отвечающем за сбор разведданных.

Ниже в качестве основы для выполнения тестов на проникновение приведены основные разделы рассматриваемого нами стандарта.

- Предварительное соглашение на взаимодействие.
- Сбор разведданных.
- Моделирование угроз.
- Анализ уязвимостей.
- Эксплуатация.
- Пост-эксплуатация.
- Составление отчета.

NIST 800-115

Специальное издание *Национального института стандартов и технологий* (National Institute of Standards and Technology Special Publication, NIST SP 800-115) является техническим руководством по тестированию и оценке информационной безопасности. Публикация подготовлена *Лабораторией информационных технологий* (Information Technology Laboratory, ITL) в NIST.

В руководстве оценка безопасности трактуется как процесс определения того, насколько эффективно оцениваемая организация отвечает конкретным требованиям безопасности. При просмотре руководства вы увидите, что в нем содержится большое количество информации для тестирования. Хотя документ редко обновляется, он не устарел и может послужить в качестве справочника для построения методологии тестирования.

В этом справочнике предлагаются практические рекомендации по разработке, внедрению и ведению технической информации, тестам безопасности и процессам и процедурам экспертизы, охватывая ключевой элемент или техническое тестирование на безопасность и экспертизу. Данные рекомендации можно использовать для нескольких практических задач. Например, поиск уязвимостей в системе или сети и проверка соответствия политике или другим требованиям.

Стандарт NIST 800-115 предоставляет большой план для испытаний на проникновение. Он позволяет убедиться, что программа тестирования на проникновение соответствует рекомендациям.

Руководство по методологии тестирования безопасности с открытым исходным кодом

OSSTMM — документ, довольно сложный для чтения и восприятия. Но он содержит большое количество актуальной и очень подробной информации по безопасности. Это также самое известное руководство по безопасности на планете с примерно полумиллионом загрузок ежемесячно. Причина такой популярности в следующем: эти инструкции примерно на десятилетие опережают все остальные документы в индустрии безопасности. Цель OSSTMM — в развитии стандартов проверки безопасности Интернета. Данный документ предназначен для формирования наиболее подробного основного плана для тестирования, что, в свою очередь, обеспечит досконального и всестороннее испытание на проникновение. Независимо от других организационных особенностей, таких как корпоративный профиль поставщика услуг по тестированию на проникновение, это испытание позволит клиенту убедиться в уровне технической оценки.

Фреймворк: общее тестирование на проникновение

Несмотря на то что стандарты различаются по количеству условий, тестирование на проникновение можно разбить на следующие этапы.

1. Разведка.
2. Сканирование и перечисление.
3. Получение доступа.
4. Повышение привилегий.
5. Поддержание доступа.

6. Заметание следов.
7. Составление отчета.

Рассмотрим каждый этап более подробно.

Разведка

Это первый и очень важный этап в тесте на проникновение. На него может уйти немало времени. Многие испытатели делят данный этап на две части: активную и пассивную разведку. Я же предпочитаю эти два этапа объединить, так как полученные результаты скажут сами за себя.

Разведка (рекогносцировка) — это систематический подход, когда вы стараетесь обнаружить расположение и собрать максимально возможное количество информации о целевой системе или машине. Это еще называется *сбором следов*.

Для проведения данного процесса могут быть использованы следующие методы (в действительности список методов может быть значительно шире).

- Социальная инженерия (это увлекательный метод).
- Исследование в Интернете (с помощью поисковых машин Google, Bing, LinkedIn и т. д.).
- Путешествие по мусорным бакам (можно испачкать руки).
- Холодные звонки.

Вы можете выбрать любой из перечисленных методов для получения информации о целевой системе или машине. Но что же мы все-таки должны на данном этапе узнать?

Нам, конечно, может быть полезным каждый бит информации. Но у нас должна быть приоритетная цель. При этом учтите, что собранные данные, которые на текущем этапе могут показаться ненужными, позже могут пригодиться.

Сначала для нас будет очень важна следующая информация.

- Имена контактов в организации.
- Где располагается организация (если такие данные есть).
- Адреса электронной почты (эти данные можно использовать позже для фишинга, то есть сбора конфиденциальных данных).
- Номера телефонов важных персон, работающих в этой компании (пригодятся для фишинга).
- Операционные системы, используемые в компании, например Windows или Linux.
- Объявления о работе.
- Резюме сотрудников (прошлое и настоящее).

На первый взгляд все эти данные кажутся полезными (разве что смущают объявления о работе). Но представим, что вы встречаетесь с системным администратором. Зная основные требования, вы можете получить большое количество

информации о внутренней системе организации. Это можно использовать для разработки направления атаки.

Для этих же целей служат и резюме сотрудников. Зная, что люди умеют делать, легко можно определить, с какими системами они работают, а какие им недоступны.

Вам это может показаться утомительным. Но имейте в виду: чем больше информации вы соберете, тем больше у вас будет возможностей для принятия решений как сейчас, так и позже.

Мы считаем, что к разведке следует прибегать на протяжении всего взаимодействия.

Сканирование и перечисление

Без сомнения, почти каждый специалист по безопасности хочет сразу заняться эксплуатацией. Но без понимания основ, эксплойтов и, самое главное, среды, в которой они находятся, этот шаг не принесет никакой пользы и даже может спровоцировать ошибки или, что еще хуже, разрушение среды.

Сканирование и перечисление позволяют испытателю на проникновение понять среду целевой системы. Результат, полученный в ходе этих проверок, предоставит *красной команде* отправную точку для использования уязвимостей в разных системах.

Термин red team (красная команда) взят из военной среды и определяет «дружественную» атакующую команду. В противовес ей существует команда защитников — blue team (голубая команда). При работе красной команды снимаются все ограничения и производится реальная атака на инфраструктуру: от атак на внешний периметр до попыток физического доступа, «жестких» социотехнических тестов (тест с использованием методов социальной инженерии).

Сканирование — это поиск всех доступных сетевых служб (TCP и UDP), работающих на целевых узлах. Оно может помочь красной команде обнаружить, может ли быть на целевой машине открыт SSH/Telnet. В этом случае, используя систему грубой силы, можно попытаться войти через него. Тогда мы можем обнаружить файловые ресурсы для загрузки данных с уязвимых сайтов или принтеров, на которых могут храниться имена пользователей и пароли. *Перечисление* — это обнаружение служб в сети, что позволит нам лучше понять информацию, полученную от сетевых служб.

Сканирование

Если вы не знаете, включен ли брандмауэр, задействована ли система обнаружения вторжений и производится ли мониторинг целостности файлов, идеально подходит полный тест на проникновение. При сканировании можно обнаружить отдельные уязвимости. В этом случае при тестировании на проникновение будет предпринята

попытка проверить, можно ли обнаруженные уязвимости использовать в целевой среде. Рассмотрим все типы сканирования.

ARP-сканирование

С помощью широковещательного запроса мы можем получить преимущество в добыче информации об IP-адресе. Каждый широковещательный кадр ARP запрашивает, у кого какой IP-адрес. При этом запрашиваемый IP-адрес при каждом запросе увеличивается на единицу. После того как хост получит этот IP-адрес, он даст ответ, сопоставив запрошенный IP-адресом соответствующий ему MAC-адрес. ARP-сканирование является быстрым и эффективным методом и обычно не вызывает никаких аварийных сигналов. Только есть проблема: ARP — протокол второго уровня и поэтому не может перейти границы сети. То есть, если красная команда находится в сети, например, по адресу 192.100.0.0/24, а ваша цель (цели) — в сети 10.16.X.0/24, вы не сможете отправлять ARP-запросы для 10.16.X.0/24.

Сетевой картограф (Nmap)

Nmap является главной ищейкой в сканировании портов и перечислении. Мы не сможем в данной книге описать все параметры и модули Nmap. Вместо этого мы рассмотрим сканы, которые чаще всего используют при тестировании.

Но сначала расскажем, в каком состоянии может быть порт.

- *Открыт*. Приложение на целевом компьютере прослушивает соединения/пакеты на этом порту.
- *Закрыт*. Порт в данное время не прослушивает ни одно из приложений, но может быть открыт в любое время.
- *Фильтр*. Брандмауэр, фильтр или другое сетевое препятствие блокирует порт таким образом, что Nmap не может определить, открыт он или закрыт.

В Nmap нам доступны следующие параметры:

- `O` — обнаружение ОС;
- `p` — сканирование порта;
- `p-` — сканирование всех портов (от 1 до 65 535);
- `p 80,443` — сканирование портов 80 и 443;
- `p 22-1024` — сканирование портов от 22 до 1024;
- `top-ports X` — здесь в качестве `X` указывается число наиболее используемых портов, которые мы будем сканировать. Чтобы ускорить сканирование, мы обычно указываем значение `100`;
- `sV` — обнаружение служб;
- `Tx` — определение скорости сканирования;
- `T1` — очень медленное сканирование портов;
- `T5` — очень быстрое сканирование портов (с большим шумом);

- `sS` — скрытное сканирование;
- `sU` — сканирование UDP;
- `A` — определения версии ОС, сканирование с использованием сценариев и трассировка.

Сканирование портов/TCP-сканирование в Nmap. Эта служба запускается путем активации соединения (`SYN`) на каждом порте целевого хоста. Если порт открыт, хост ответит (`SYN, ACK`). Соединение закрывается (`RST`), если команда отправлена инициатором (рис. 3.1).

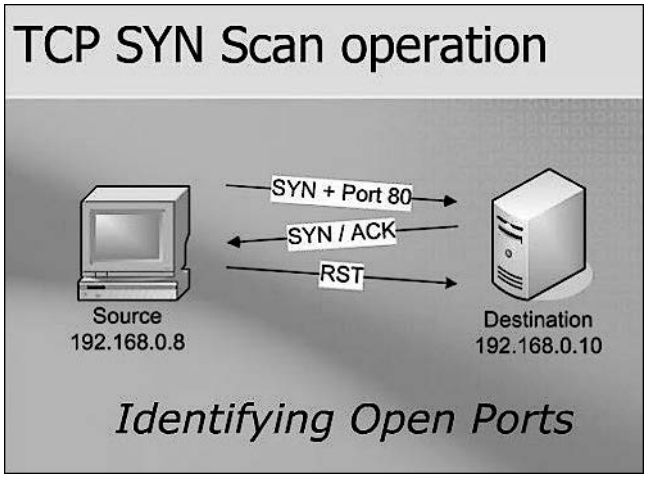

Рис. 3.1. Операция сканирования TCP SYN

Полуоткрытое/скрытое сканирование в Nmap. Этот параметр запускается путем отправки соединения (`SYN`) на каждый порт целевого хоста. Если порт открыт, хост на запрос ответит (`SYN, ACK`). Если порт закрыт, хост ответит сбросом соединения (`RST`). Если ответ не получен, можно предположить, что порт фильтруется. Разница между TCP- и скрытым сканированием заключается в том, что инициатор соединения не возвращает пакет подтверждения (`ACK`). Эффективность такого сканирования в том, что регистрируется только полностью установленное соединение.

Обнаружение OS в Nmap. Данный параметр использует различные методы для определения типа и версии операционной системы. Это очень полезно для обнаружения уязвимостей. Поиск версии ОС покажет в операционной системе известные уязвимости и эксплойты. Для этого введите следующую команду:

```
nmap 172.16.54.144 -O
```

Обнаружение служб в Nmap. Как и при обнаружении ОС, этот параметр пытается определить службу и версию, как показано на рис. 3.2:

```
nmap 172.16.54.144 –sV
```

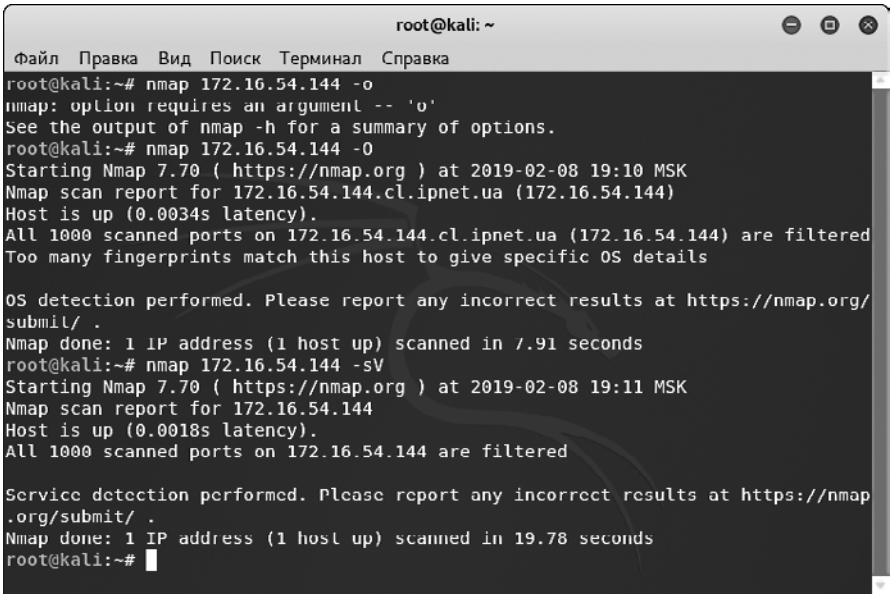

Рис. 3.2. Обнаружение служб

Nmap ping sweeps (Пинг-разведка Nmag). Этот параметр обрабатывает каждый IP-адрес в заданном диапазоне. Если узел подключен и настроен для ответа на запросы ping, он выдаст ICMP-ответ (рис. 3.3).

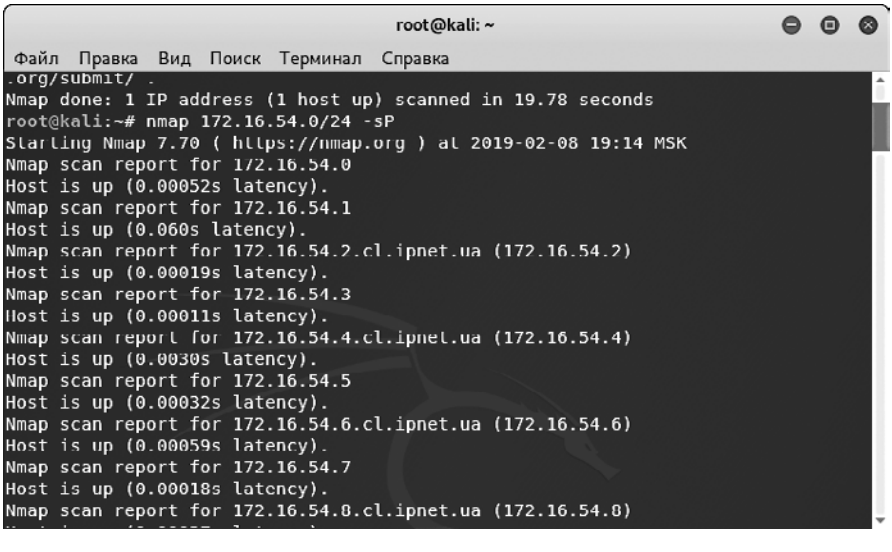

Рис. 3.3. Сканирование узла

Перечисление

Метод перечисления — это плацдарм для всех атак на слабые места, которые обнаруживаются в веб-приложениях. Все атаки на слабые места можно классифицировать по уязвимостям, которые появляются на разных этапах развития. Это может быть этап разработки, реализации или развертывания. Существует несколько методов перечисления. С некоторыми из них мы и познакомимся.

Совместное использование SBM

Server Message Block (SMB) обозначает блок сообщений сервера. Этот протокол обмена файлами был изобретен IBM в середине 1980-х годов и существует до сих пор. Назначение данного протокола — дать возможность компьютерам читать и записывать файлы на удаленный хост по *локальной сети (LAN)*. Каталоги на удаленных узлах SMB называются *акциями*.

Этот метод передачи данных имеет несколько преимуществ, которые мы и обсудим.

Передача зоны DNS. Протокол DNS — мой любимый протокол, потому что это просто кладезь информации. Данный протокол определяет связь имени хоста с IP-адресами всех хостов в сети. Если злоумышленнику известна схема сети, с помощью этого протокола он может быстро обнаружить все узлы в сети. С помощью DNS также можно создавать службы, работающие в сети, например почтовые серверы.

DNSRecon. Содержит инструменты разведки и перечисления. В этом примере мы запросим перенос зоны из домена domain.foo. DNS-сервер, работающий в домене domain.foo, вернет все записи, относящиеся к этому домену и ко всем связанным с ним поддоменам. Благодаря этой операции мы получим имена серверов, соответствующие им имена хостов и IP-адреса для домена. Будут возвращены все имеющиеся записи DNS: TXT-записи (4), PTR-записи (1), MX-записи для почтового сервера (10), записи протоколов IPv6 (2) и IPv4 (12). Эти записи действительно предоставляют пикантную информацию о сети. Одна запись показывает IP-адрес офиса DC, во второй записи вы увидите IP-адрес брандмауэра, в третьей — VPN и IP-адрес, и еще одна запись показывает IP-адрес почтового сервера и логин портала (рис. 3.4).

```
dnsrecon -d zonetranfer.zone -a
```

Здесь `-d` — домен; `-a` — выполнить перенос зоны.

SNMP-устройства

Простой протокол сетевого управления (Simple Network Management Protocol), сокращенно **SNMP**, используется для регистрации сетевых устройств и приложений и управления ими. SNMP можно применять для удаленной настройки устройств и приложений, но, если оставить его незащищенным, он также мо-

жет быть использован для извлечения информации об указанных приложениях и устройствах. Эта информация пригодится для лучшего понимания сети:

```
snmpwalk 192.16.1.1 -c PUBLIC
```

-c — это строка аутентификации устройства.

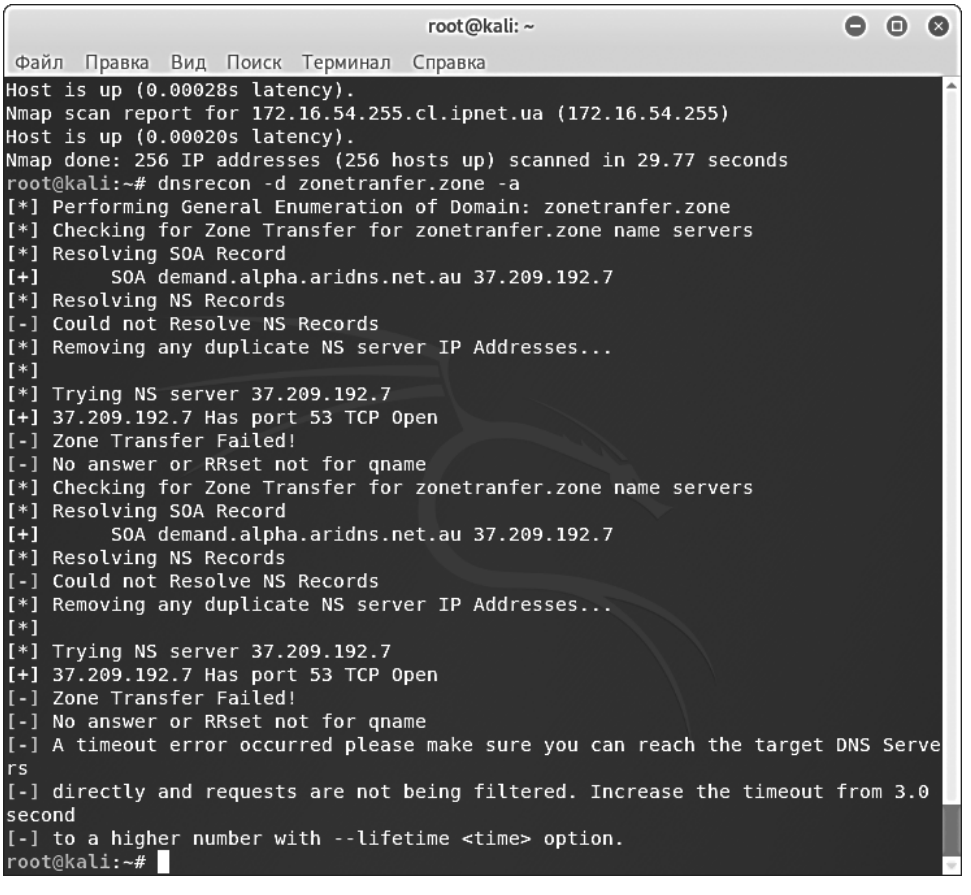

Рис. 3.4. Передача зоны DNS с помощью команды dnsrecon -d zonetranfer.zone -a