ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА UNIX

Денисов Роман Андреевич

студент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, РФ, г. Санкт-Петербург

Бакур Фатех Юсефович

студент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, РФ, г. Санкт-Петербург

Мухаметдинов Тимур Русланович

студент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, РФ, г. Санкт-Петербург

Аннотация. Надежность функционирования программного обеспечения и работы ОС в целом является ключевой задачей разработчиков. Для создания, соответствующего ПО были разработаны различные способы слежения за состоянием вычислительной машины: физические (например, отдельный, встроенный в плату модуль) и виртуальные (в виде установленной на ОС программы). Более актуальным и продвинутым будет виртуальный способ контроля функционирования. Следующей частью составной частью надежной ОС является ее защищенность. В это же время количество уязвимостей может говорить, как и о уязвимости системы так и о ее возможной простоте и функционале. В этой работе мы хотели рассмотреть и проанализировать уязвимости различных операционный систем, в частности их количество и весомость для каждой системы отдельно.

Ключевые слова: Linux, семейство UNIX, nmap, руткиты.

Введение

Особый вклад в процесс эволюции защитных ОС внесли ведущие разработчики и испытательные лаборатории систем обеспечения сетевой безопасности и средств защиты от несанкционированного доступа, которые на основании проводимых испытаний подтвердили отсутствие недекларированных возможностей, высокую отказоустойчивость встроенных механизмов защиты ОС.

Правила реализации парольной политики и типовые настройки базовых встроенных механизмов управления доступом известны, однако вопрос анализа сложных и временных характеристик успешного получение несанкционированного доступа к пользовательским и системным данным ОС на настоящий момент не подтверждены единым математическим доказательством.

Рассмотрим некоторые статистические данные, рассказывающие какие ОС самые уязвимые.

Таблица 1.

Статистические сведения о уязвимостях в ОС семействах Unix

Название ОС	Производитель	Общее число уязвимостей за 2017 год	Общее число уязвимостей за 2016 год	уязв вед
LinuxKernel	Linux	381	217	
Windows 10	Microsoft	226	172	
Windows Server 2016	Microsoft	212	39	
Windows 7	Microsoft	197	134	
Windows 8.1	Microsoft	192	154	
Windows Vista	Microsoft	64	125	
DebianLinux	Debian	95	327	
UbuntuLinux	Canonical	66	279	

Основные виды уязвимостей, которые рассматриваются в нашем анализе:

1). DoS (DenialofService / отказ в обслуживании) (эксплойт уязвимости приводит к DoS устройства);

2). Обход чего-либо (например, пароля для входа в систему);

3). Исполнение кода (возможность злоумышленником выполнить какую-то команду на устройстве жертвы);

4). Повреждение памяти;

5). Доступ к информации (имеется в виду секретная информация, полученная за счет уязвимости);

6). Увеличение привилегий (в частности для вредоносного ПО);

7). Переполнение буфера;

Использование уязвимостей

Как можно увидеть, количество уязвимостей у большинства ОС только за один 2016 год переваливает за 100. Если у ОС так много уязвимостей, то ими можно воспользоваться.

Получив доступ оп одной их подобных уязвимостей, злоумышленник может сделать многое:

-Установить бесполезную программу и позже потребовать оплатить “подписку”, которую вы естественно не оформляли.

-Загрузить вирус пользующийся ресурсами вашего ПК для собственной выгоды.

-Узнать вашу личную информацию.

-Получить доступ к данный расположенным и привязанным к вашей системе.

-И т.п.

Первое что потребуется сделать перед взломом, это узнать используемую операционную систему. Подробные способы по определению ОС описаны в [1].

Таблица 2.

Краткое описание способов определения операционной системы

Халатность администратора	**PING**
В данном случае при подключении по telenet вполне вероятно сразу же узнать операционную систему жертвы. Например: RED HAT 6.2 Login: Значит мы имеем дело с операционной системой RAD HAT 6.2	Самый простой способ определить, какая OS помощью ping. Ответ сервера на запрос ping содержать значение TTL – время жизни паке помощью которого, можно определить OS. PingIP_жертвы определяем по TTL (время жизни) linux 2.0.x Win 95 OSR/2 – 32 NowellNetware – 128
ShadowScan и другие программы	**Использование открытых порт**
В сети можно найти огромное количество всевозможных сканеров, которые находятся в открытом доступе и скачать их может абсолютно каждый. Также для пользования данными программами особых навыков не требует. Поэтому ими пользуются как администраторы, так и злоумышленники. Одна из таких программ: ShadowScan – программа позволяющая получить большую часть информации о хосте просто после ввода адреса. Установить фильтр (netfilter). Например, случае Linux системы помогут несколько подобных правил: *iptables -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j LOG --log-prefix «Stealth scan»* *iptables -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j DROP* Первое правило служит для обязательной записи события в журнал. После цели LOG пакет продолжает движение по цепочке условий (в отличие от целей DROP и ACCEPT. Принятые или отклоненные пакеты на дальнейшую проверку не пойдут). Подобные команды настройки фильтров можно так же найти и интернете для любой системы.	Используя telenet, подключится по открытым жертве и проверить версии серверов. Некоторые сервисы являются специфичными определенного вида OS, а по их версии можн определить с какой OS имеешь дело. Кроме того, версию ОС иногда можно опреде баннеру сервиса (надписи, которую ты видиш соединяешься с данным сервисом). Если буде sendmail, Apache, QPOP то это UNIX. ЕслиIIS, FTP и т.д. то это Win NT. Поверхность атаки каждого сервера, подклю сети, можно уменьшить, отключив все необя сетевые службы.
Социальная инженерия	**Суперпользователь**

Один из самых интересных\простых способов, чтобы узнать тип используемой OS. Можно пойти совершено разными способами: • Совершить звонок жертве, если имеется номер, и сказать, что для новый программы требуется указание OS • Отправить письмо на электронную почту • Назваться программистом, компьютерным экспертом или администратором Данный способ использует серьёзную уязвимость - человеческий фактор. Защититься от этого достаточно просто и одновременно тяжело, так как многим не захочется или не найдётся времени проверить информацию.	Злоумышленник может попытаться создать с пользователя, но при этом его можно будет с логах системы. Либо его могут заметить спец программы нацеленные на выявление появле несанкционированных пользователей. В таки злоумышленник в очередной раз может восп набором утилит Rootkit. Защититься от этого можно настроив брандм вручную, но это будет не эффективно и не бе Проще всего установить хороший антивирус возможности которого будет входить защита Rootkit’ов.

Предположим злоумышленник все-таки узнал вашу OS. Второе, что он должен сделать - это просканировать все порты. Это также можно сделать программами ShadowScan и nmap. Особенно обратите внимание на sendmail, qpop, imap, rlogin, ssh, mount, named, amd, talk. Теперь ему/вам понадобиться эксплоит. **Эксплоит** - это утилита, реализующия в программе недокументированные или закрытые функции. Можете досать эксплоит на rootshell и technotronic. Также советуем вам посетить BUGTRAQ. Найдите эксплоиты именно для вашей версии. После этого найти противодействие им будет проще. Например, если на хосте злоумышленника стоит sendmail, 9.8.9./9.8.9, то эксплоит под версию sendmail 3.4.3./3.4.3 не сработает. Версии должны полностью совпадать (это для Unix, но есть эксплоиты и под NT). После того, как нашли эксплоит, его нужно привести в рабочее состояние. Для этого нужно его скомпилировать. Все достаточно просто. Обычно эксплоиты написаны на SI,поэтому пользуемся командой gcc (Так же множество способов защиты на этом этапе можно реализовать на уровне компилятора, написав к нему расширение. Подходящие вам расши рения находятся в открытом доступе в интернете). Например вы скачали эксплоит sux.c. Самый простой вариант компиляции:

gcc -o suxsux.c

Теперь запускаете его командой:

./suxимя_жертвы

Также могут потребоваться дополнительные опции в команде. При успехе вы получите shell и ваш UID и GID будет равен 0(root). Теперь вы суперпользователь. Но эксплоиты - это еще не все. Вам еще может помочь NFS. Посмотрите камандойshowmountрасшаренные ресурсы атакуемого хоста. Например:

showmount -e

имя_атакуемого_хоста

Допустимвывидите:

/usr

/var (everyone)

/home (everyone)

Теперь пора монтировать home((everyone) говорит о том, что каталог доступен любому по NFS). Монтируем:

mount

имя_атакуемого_хоста:/home /mnt

Где /mnt -имя вашей папки на компьютере для монтажа. Теперь можно создать в папке какого-нибудь пользователя файл .rhosts с содержанием '+ +'. Теперь можете логиниться в сеть с помощью rlogin.

Заключение

Анализ уязвимостей программного обеспечения в настоящее время является обязательным видом деятельности, выполняемым экспертами испытательных лабораторий отечественных систем сертификации средств защиты информации.

Любой компьютер или сервер нуждается, для полного функционирования, не только в качественных комплектующих, но и в не менее качественном, а главное, безопасном программном обеспечении.

Список литературы:

1. Взлом Unix: пособие хакера [Электронный ресурс] // «Хакер» - Безопасность, разработка, DevOps: электронный научный журнал. URL: https://xakep.ru/2000/08/11/10443/

2. Методика оценки эффективности средств алгоритмизации, используемых для поиска уязвимостей / Израилов К.Е. // Информатизация и связь. 2014. № 3. С. 44-47

3. Метод и модель анализа безопасности операционной системы от атак типа руткит / Милушков В.И., Митрушин А.А., Люльченко А.Н., Менщиков А.А., Швед В.Г. // Перспективы науки. 2015. № 10 (73). С. 100-103.