

УДК 004.382
ББК 32.973-018
Д94

Дэвис Р.

Д94 Искусство тестирования на проникновение в сеть / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2021. – 310 с.: ил.

ISBN 978-5-97060-529-5

Автор книги, специалист по наступательной безопасности, делится с читателями секретами пентестинга – проникновения во внутреннюю сеть компании с целью выявления слабых мест в ее защите. Опираясь на опыт многолетней работы и успешных взломов сетей, он предлагает свою методологию тестирования на проникновение и предоставляет набор практических инструкций, которым может воспользоваться новичок в этой отрасли.

В начале книги изучаются хакерские приемы и инструменты пентестинга; затем поэтапно описываются действия, которые злоумышленник предпринимает для захвата контроля над корпоративной сетью. Имитация этих действий (обнаружение сетевых служб и уязвимостей, проведение атак, постэксплуатация) позволит выявить критические проблемы безопасности и представить заинтересованным лицам в компании результаты пентеста, показывающие, в каком направлении двигаться, чтобы лучше защитить корпоративную сеть.

Читателю предлагается ряд упражнений, ответы на которые приводятся в конце книги.

Издание адресовано техническим специалистам, не имеющим опыта работы в сфере безопасности.

УДК 004.382
ББК 32.973-018

Original English language edition published by Manning Publications USA, USA. Russian-language edition copyright © 2021 by DMK Press. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-6172-9682-6 (англ.)
ISBN 978-5-97060-529-5 (рус.)

© Manning Publications, 2020
© Перевод, оформление, издание, ДМК Пресс, 2021

Содержание

Оглавление.....	5
Предисловие.....	12
Благодарности.....	15
О чем эта книга.....	16
Об авторе.....	20
Изображение на обложке.....	21

1	Тестирование сетей на проникновение.....	22
1.1	Утечки корпоративных данных.....	23
1.2	Как работают хакеры.....	24
1.2.1	Что делает защитник.....	24
1.2.2	Что делает злоумышленник.....	25
1.3	Моделирование состязательной атаки: тестирование на проникновение.....	25
1.3.1	Типичные этапы вторжения.....	26
1.4	Когда тест на проникновение наименее эффективен.....	28
1.4.1	Доступные мишени.....	28
1.4.2	Когда компании действительно нужен тест на проникновение?.....	29
1.5	Проведение теста на проникновение в сеть.....	30
1.5.1	Этап 1: сбор информации.....	31
1.5.2	Этап 2: целенаправленное проникновение.....	32
1.5.3	Этап 3: постэксплуатация и повышение привилегий.....	33
1.5.4	Этап 4: документирование.....	34
1.6	Настройка лабораторной среды.....	35
1.6.1	Проект Capsulecorp Pentest.....	35
1.7	Создание собственной виртуальной платформы для пентеста.....	36
1.7.1	Начните с Linux.....	36

1.7.2	Проект Ubuntu	37
1.7.3	Почему бы не использовать пентест-дистрибутив?.....	38
1.8	Заключение.....	39

Этап 1 СБОР ИНФОРМАЦИИ 40

2	Обнаружение сетевых хостов	41
2.1	Оценка объема вашего задания	43
2.1.1	Область видимости черного, белого и серого ящиков	44
2.1.2	Корпорация Capsulecorp	45
2.1.3	Настройка среды Capsulecorp Pentest.....	46
2.2	Протокол управляющих сообщений интернета.....	47
2.2.1	Использование команды ping	48
2.2.2	Использование bash для проверки диапазона сети	49
2.2.3	Ограничения использования команды ping	51
2.3	Обнаружение хостов с помощью Nmap	52
2.3.1	Основные выходные форматы	54
2.3.2	Использование портов интерфейса удаленного управления.....	55
2.3.3	Повышение производительности сканирования Nmap.....	57
2.4	Дополнительные методы обнаружения хостов.....	58
2.4.1	Сканирование DNS прямым перебором	59
2.4.2	Захват и анализ пакетов	59
2.4.3	Поиск подсетей	60
2.5	Заключение.....	62

3	Обнаружение сетевых служб	63
3.1	Сетевые службы с точки зрения злоумышленника	64
3.1.1	Что такое сетевые службы	65
3.1.2	Поиск прослушивающих сетевых служб.....	67
3.1.3	Баннеры сетевых служб	68
3.2	Сканирование портов с помощью Nmap	69
3.2.1	Часто используемые порты.....	70
3.2.2	Сканирование всех 65 536 TCP-портов	73
3.2.3	Сортировка вывода сценария NSE.....	75
3.3	Анализ данных в формате XML с помощью Ruby.....	78
3.3.1	Создание целевых списков для конкретных протоколов	84
3.4	Заключение.....	85

4	Обнаружение сетевых уязвимостей.....	86
4.1	Что такое обнаружение уязвимостей	87
4.1.1	По пути наименьшего сопротивления	88
4.2	Обнаружение уязвимостей, связанных с исправлениями...89	

4.2.1	Поиск MS17-010 Eternal Blue	91
4.3	Обнаружение уязвимостей аутентификации	93
4.3.1	Создание списка паролей для конкретного клиента	93
4.3.2	Подбор паролей локальных учетных записей Windows.....	96
4.3.3	Подбор паролей баз данных MSSQL и MySQL	98
4.3.4	Подбор паролей VNC	101
4.4	Обнаружение уязвимостей конфигурации	103
4.4.1	Настройка Webshot.....	104
4.4.2	Анализ вывода Webshot	106
4.4.3	Подбор паролей веб-сервера вручную	107
4.4.4	Подготовка к целенаправленному проникновению	109
4.5	Заключение.....	110

Этап 2 ЦЕЛЕНАПРАВЛЕННОЕ ПРОНИКНОВЕНИЕ..... 111

5 Атака на уязвимые веб-сервисы..... 112

5.1	Описание фазы 2 – целенаправленного проникновения	113
5.1.1	Развертывание веб-оболочек бэкдора	114
5.1.2	Доступ к службам удаленного управления	115
5.1.3	Эксплуатация отсутствующих программных исправлений.....	115
5.2	Захват исходного плацдарма.....	115
5.3	Взлом уязвимого сервера Tomcat	116
5.3.1	Создание вредоносного файла WAR	117
5.3.2	Развертывание файла WAR	118
5.3.3	Доступ к веб-оболочке из браузера	119
5.4	Интерактивные и неинтерактивные оболочки.....	121
5.5	Обновление до интерактивной оболочки	122
5.5.1	Резервное копирование sethc.exe	123
5.5.2	Изменение списков управления доступом к файлам с помощью cacls.exe	124
5.5.3	Запуск залипания клавиш через RDP	125
5.6	Взлом уязвимого сервера Jenkins	127
5.6.1	Запуск консоли с помощью Groovy Script.....	128
5.7	Заключение.....	129

6 Атака на уязвимые службы баз данных..... 130

6.1	Взлом Microsoft SQL Server.....	131
6.1.1	Хранимые процедуры MSSQL	133
6.1.2	Перечисление серверов MSSQL с помощью Metasploit	133
6.1.3	Включение xp_cmdshell	134
6.1.4	Запуск команд ОС с помощью xp_cmdshell.....	137

6.2	Кража хешей паролей учетной записи Windows.....	138
6.2.1	Копирование кустов реестра с помощью reg.exe.....	140
6.2.2	Загрузка копий куста реестра	142
6.3	Извлечение хешей паролей с помощью creddump	144
6.3.1	Что такое вывод rwdump	145
6.4	Заключение.....	146

7	Атака на непропатченные службы	147
7.1	Что такое программные эксплойты.....	148
7.2	Типичный жизненный цикл эксплойта	149
7.3	Взлом MS17-010 с помощью Metasploit.....	151
7.3.1	Проверка отсутствия патча	152
7.3.2	Использование модуля эксплойта ms17_010_psexec	153
7.4	Полезное действие – запуск оболочки Meterpreter	155
7.4.1	Полезные команды Meterpreter.....	157
7.5	Предостережения относительно общедоступной базы данных эксплойтов	160
7.5.1	Создание собственного шелл-кода	161
7.6	Заключение.....	163

Этап 3	ПОСТЭКСПЛУАТАЦИЯ И ПОВЫШЕНИЕ ПРИВИЛЕГИЙ.....	164
---------------	---	------------

8	Постэксплуатация Windows	165
8.1	Основные цели постэксплуатации.....	166
8.1.1	Обеспечение надежного повторного входа	167
8.1.2	Сбор учетных данных.....	167
8.1.3	Движение вбок.....	167
8.2	Обеспечение надежного повторного входа с помощью Meterpreter	168
8.2.1	Установка бэкдора Meterpreter с автозапуском	169
8.3	Получение учетных данных с Mimikatz	171
8.3.1	Использование расширения Meterpreter.....	172
8.4	Извлечение кешированных учетных данных домена	173
8.4.1	Использование постмодуля Meterpreter.....	174
8.4.2	Взлом кешированных учетных данных с помощью John the Ripper	175
8.4.3	Использование файла словаря в John the Ripper	177
8.5	Извлечение учетных данных из файловой системы.....	178
8.5.1	Поиск файлов с помощью findstr и where	179
8.6	Движение вбок с Pass-the-Hash	180
8.6.1	Использование модуля Metasploit smb_login.....	181
8.6.2	Передача хеша с помощью CrackMapExec	183
8.7	Заключение.....	185

9	Постэксплуатация Linux или UNIX	186
9.1	Обеспечение надежного повторного входа с помощью заданий cron	187
9.1.1	Создание пары ключей SSH	189
9.1.2	Настройка аутентификации с открытым ключом	190
9.1.3	Туннелирование через SSH	192
9.1.4	Автоматизация SSH-туннелирования с помощью cron	194
9.2	Сбор учетных данных	195
9.2.1	Извлечение учетных данных из истории bash	197
9.2.2	Получение хешей паролей	198
9.3	Эскалация привилегий с помощью двоичных файлов SUID	199
9.3.1	Поиск двоичных файлов SUID с помощью команды find	200
9.3.2	Добавление нового пользователя в /etc/passwd	202
9.4	Передача SSH-ключей	204
9.4.1	Похищение ключей от взломанного хоста	205
9.4.2	Сканирование нескольких целей с помощью Metasploit	205
9.5	Заключение	207

10	Доступ к управлению всей сетью	209
10.1	Определение учетных записей пользователей – администраторов домена	212
10.1.1	Использование команды net для запроса gwynn Active Directory	212
10.1.2	Поиск авторизованных пользователей – администраторов домена	213
10.2	Получение прав администратора домена	214
10.2.1	Как выдать себя за других пользователей при помощи Incognito	216
10.2.2	Получение учетных данных в виде открытого текста с помощью Mimikatz	217
10.3	База данных ntds.dit и ключи от королевства	219
10.3.1	Обход ограничений доступа к VSC	220
10.3.2	Извлечение всех хешей с помощью secretsdump.py	223
10.4	Заключение	225

Этап 4	ДОКУМЕНТИРОВАНИЕ	226
---------------	-------------------------	-----

11	Очистка среды после проникновения	227
11.1	Удаление активных соединений оболочки	229
11.2	Деактивация локальных учетных записей пользователей	229
11.2.1	Удаление записей из /etc/passwd	230

11.3	Удаление оставшихся файлов из файловой системы	231
11.3.1	Удаление копий куста реестра Windows	232
11.3.2	Удаление пар ключей SSH	233
11.3.3	Удаление копий ntds.dit	233
11.4	Отмена изменений конфигурации	234
11.4.1	Отключение хранимых процедур MSSQL	235
11.4.2	Отключение анонимных общих файловых ресурсов	235
11.4.3	Удаление записей crontab	236
11.5	Заккрытие бэкдоров	237
11.5.1	Отмена развертывания файлов WAR из Apache Tomcat	237
11.5.2	Заккрытие бэкдора залипания ключей	239
11.5.3	Удаление постоянных обратных вызовов Meterpreter	239
11.6	Заклучение	241

12 Написание качественного отчета о проникновении

12.1	Восемь компонентов хорошего отчета о тестировании на проникновение	243
12.2	Сводное резюме	245
12.3	Методика проникновения	246
12.4	Описание атаки	247
12.5	Технические замечания	247
12.5.1	Рекомендации	249
12.6	Приложения	250
12.6.1	Определения значимости	250
12.6.2	Хосты и службы	251
12.6.3	Список инструментов	252
12.6.4	Дополнительные ссылки	252
12.7	Заключительная часть	252
12.8	Что дальше?	254
12.9	Заклучение	255

Приложение А. Создание виртуальной платформы для пентеста	256
---	-----

Приложение В. Основные команды Linux	276
--	-----

Приложение С. Создание лабораторной сети Capsulecorp Pentest	283
--	-----

Приложение D. Отчет о тестировании на проникновение во внутреннюю сеть Capsulecorp	290
--	-----

Приложение Е. Ответы на упражнения	303
--	-----

Предметный указатель	308
----------------------------	-----