ДЖОН ЭРИКСОН

ХАКИНГ
ИСКУССТВО ЭКСПЛОЙТА

2-е ИЗДАНИЕ

ПИТЕР®
Санкт-Петербург · Москва · Екатеринбург · Воронеж
Нижний Новгород · Ростов-на-Дону · Самара · Минск
2020

ББК 32.973.23-018-07
УДК 004.56.53
Э77

Эриксон Д.

Э77 Хакинг: искусство эксплойта. 2-е изд. — СПб.: Питер, 2020. — 496 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-0712-4

Каждый программист по сути своей — хакер. Ведь первоначально хакингом называли поиск искусного и неочевидного решения. Понимание принципов программирования помогает находить уязвимости, а навыки обнаружения уязвимостей помогают создавать программы, поэтому многие хакеры занимаются тем и другим одновременно. Интересные нестандартные ходы есть как в техниках написания элегантных программ, так и в техниках поиска слабых мест.

С чего начать? Чтобы перезаписывать память с помощью переполнения буфера, получать доступ к удаленному серверу и перехватывать соединения вам предстоит программировать на Си и ассемблере, использовать шелл-код и регистры процессора, познакомиться с сетевыми взаимодействиями и шифрованием и многое другое.

Как бы мы ни хотели верить в чудо, программное обеспечение и компьютерные сети, от которых зависит наша повседневная жизнь, обладают уязвимостями.

Мир без хакеров — это мир без любопытства и новаторских решений. (*Джон Эриксон*)

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.973.23-018-07
УДК 004.56.53

ISBN 978-1593271442 англ.

ISBN 978-5-4461-0712-4

ОГЛАВЛЕНИЕ