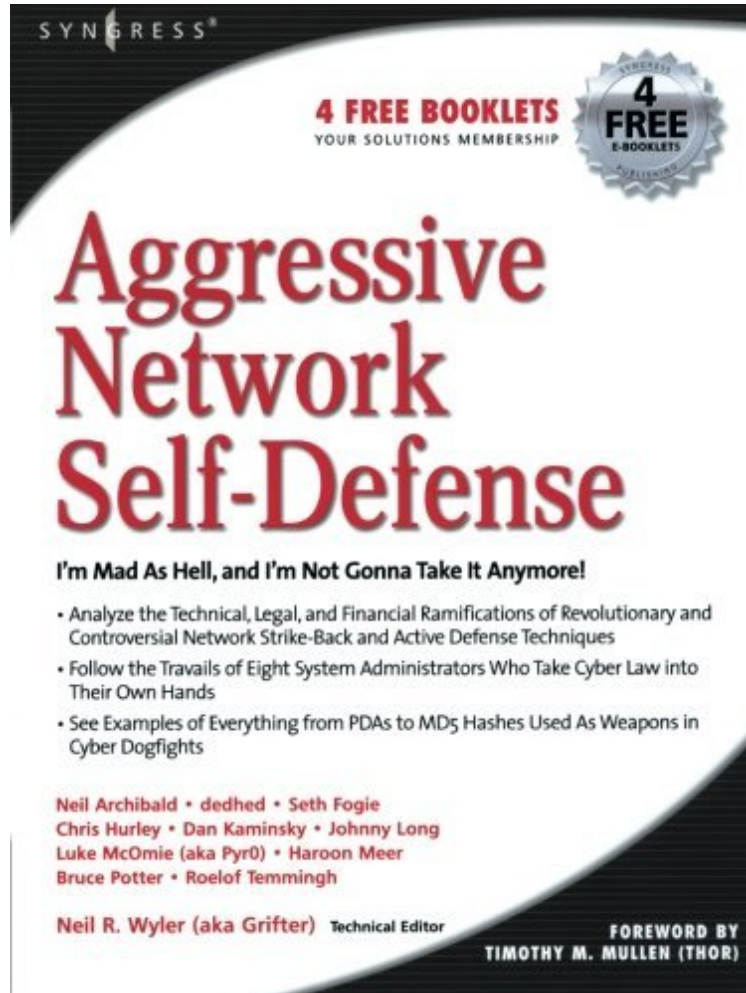


Aggressive Network Self-Defense

Von Neil R. Wyler

audiobook / *ebooks / Download PDF / ePub / DOC



Produktinformation Veröffentlicht am: 2005-04-12 Erscheinungsdatum: 2005-04-12 File Name: B001J54VB4 | File size: 50.Mb

Von Neil R. Wyler : Aggressive Network Self-Defense before purchasing it in order to gage whether or not it would be worth my time, and all praised Aggressive Network Self-Defense:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. Als Fachbuch getarnter RomanVon DaFuxWer hier konkretes Material fr Strike-Back-Szenarien sucht, wird eher enttäuscht sein: Die vielen Autoren dieses Buchs haben eher eine Reihe unterhaltsamer Aufstze in Buchform zusammengefasst, die sich mit hypothetischen und mehr oder weniger realistischen Angriffsszenarien und entsprechenden Verteidigungsmöglichkeiten befassen.Andererseits ist das auch nicht wirklich verwunderlich, denn erstens sind aktive Verteidigungsmaßnahmen in Form eines Gegenschlags rechtlich umstritten (Grenze zwischen Notwehr und Gesetzesverletzung) und zweitens sind sie technisch meist nur in der Theorie a) erfolgreich und b) in der gebotenen Geschwindigkeit ausführbar.Insofern sollte das Buch als das gelesen werden, was es ist: Eine unterhaltsame Sammlung

von Aufstzen, in denen der Verteidiger der Held und dem Angreifer immer um eine Nasenlnge voraus ist (in der Praxis ist es leider meist umgekehrt).

Kurzbeschreibung Over the past year there has been a shift within the computer security world away from passive, reactive defense towards more aggressive, proactive countermeasures. Although such tactics are extremely controversial, many security professionals are reaching into the dark side of their tool box to identify, target, and suppress their adversaries. This book will provide a detailed analysis of the most timely and dangerous attack vectors targeted at operating systems, applications, and critical infrastructure and the cutting-edge counter-measures used to nullify the actions of an attacking, criminal hacker. *First book to demonstrate and explore controversial network strike back and countermeasure techniques. *Provides tightly guarded secrets to find out WHO is really attacking you over the internet. *Provides security professionals and forensic specialists with invaluable information for finding and prosecuting criminal hackers.

Kurzbeschreibung Over the past year there has been a shift within the computer security world away from passive, reactive defense towards more aggressive, proactive countermeasures. Although such tactics are extremely controversial, many security professionals are reaching into the dark side of their tool box to identify, target, and suppress their adversaries. This book will provide a detailed analysis of the most timely and dangerous attack vectors targeted at operating systems, applications, and critical infrastructure and the cutting-edge counter-measures used to nullify the actions of an attacking, criminal hacker. *First book to demonstrate and explore controversial network strike back and countermeasure techniques. *Provides tightly guarded secrets to find out WHO is really attacking you over the internet. *Provides security professionals and forensic specialists with invaluable information for finding and prosecuting criminal hackers.

Synopsis Over the past year, there has been a shift within the computer security world away from passive, reactive defense towards more aggressive, proactive countermeasures. Although such tactics are extremely controversial, many security professionals are reaching into the dark side of their tool box to identify, target, and suppress their adversaries. This book will provide a detailed analysis of the most timely and dangerous attack vectors targeted at operating systems, applications, and critical infrastructure and the cutting-edge counter-measures used to nullify the actions of an attacking, criminal hacker. This is the first book to demonstrate and explore controversial network strike back and countermeasure techniques. It provides tightly guarded secrets to find out WHO is really attacking you over the internet. It provides security professionals and forensic specialists with invaluable information for finding and prosecuting criminal hackers.