Álvaro Vilobaldo Rios da Silva

Antiforense com uso de rootkits

São Paulo

2013

Álvaro Vilobaldo Rios da Silva

Antiforense com uso de rootkits

Monografia de Conclusão de Curso apresentada à Universidade Presbiteriana Mackenzie de São Paulo como requisito parcial à obtenção do título de Especialista em Computação Forense do Curso Lato Sensu em Computação Forense

Orientador:
Ivete Irene dos Santos

UNIVERSIDADE PRESBITERIANA MACKENZIE

São Paulo

2013

Monografia sob o título Antiforense com uso de rootkits, desenvolvida por Álvaro Vilobaldo Rios da Silva, e aprovada em 11 de novembro de 2012, São Paulo capital, pela banca constituída por:

Ivete Irene dos Santos
Orientador

Epígrafe

"Se você conhecer o inimigo e a si mesmo, não precisa temer o resultado de uma centena batalhas. Se você se conhecer a si mesmo, mas não o inimigo, para cada vitória você também sofrerá uma derrota. Se você não conhecer nem o inimigo, nem a si mesmo, você sucumbirá em todas as batalhas." (TZU, IV a.C)

Resumo

Monografia foi desenvolvida como trabalho de conclusão de curso *Latu sensu* em computação forense pela Universidade Presbiteriana Mackenzie de São Paulo. Sendo este trabalho um estudo elaborado cujo tema central é antiforense com utilização de rootkits, ele acaba por apresentar definições de antiforense e rootkits junto com suas práticas mais comuns e históricos de utilização respectivamente. Durante o avanço do texto, no entanto, poderá se notar diversas formas de detecção de rootkits além de indicios de seu uso em analises.

Abstract

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

O autor entende que o leitor será convencido a precave-se de supor que situações mais corriqueiras tenham só e apenas a resposta mais obvia, desse modo evitando que sejam subestimadas. Além do conhecimento técnico e de foro que se espera de um perito, compreender que existem técnicas sofisticadas para destruir e/ou dificultar acesso a provas no ambito computacional é de fundamental necessidade para qualquer perito. A combinação do uso de diversas técnicas avançadas com maestria se mostra realmente desafiadora.

O objetivo desse texto não é de forma alguma desencorajar peritos em sua nobre luta diária superestimando todas as suas próximas empreitadas tão utéis para a sociedade. Definitivamente esse não é o caso e sim mostrar que o perito pode se deparar com algum artefato que tenham sido usado por alguém com o mesmo ou um maior conhecimento sobre o corpo de delito.

É claro que essa monografia apresenta apenas uma limitada incursão na antiforense focada na utilização de rootkits ciente que ninguém abordaria de forma completa tais assuntos. Portando em assuntos que fojem da mediocridade cotidiana e adentram nesse mundo instigante e revelador da análise de artefatos únicos, se faz necessário que quanto maior o desafio maior deverá ser a dedicação e paixão do perito.

1 Forense Computacional

2 AntiForense Computacional

3 Rootkits

Expor o que é um rootkit; Como o rootikit pode impedir a formação de provas; Mostrar o que ele pode fazer usando se possível com exemplos reais;

4 Análise

Desenvolver em cima da análise do funcionamento do rootkit e do seu potencial fatores que devem ser levados em conta antes de qualquer análise; e Contemplar o trabalho com um estudo de caso.

Referências Bibliográficas

TZU, S. *A Arte da Guerra*. Tradução de Candida de Sampaio Bastos. 1ª. ed. [S.l.]: Golden Books, IV a.C. 47 p. ISBN 978-85-7501-272-7.