UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

DAVID BARROS HULAK

ANÁLISE DE VIGILÂNCIAS ELETRÔNICAS E TÉCNICAS PARA MANUTENÇÃO DA PRIVACIDADE

PROPOSTA DE TRABALHO DE GRADUAÇÃO

RECIFE
2013

DAVID BARROS HULAK

ANÁLISE DE VIGILÂNCIAS ELETRÔNICAS E TÉCNICAS PARA MANUTENÇÃO DA PRIVACIDADE

Trabalho de Graduação a ser apresentado junto ao
curso de Ciência da Computação da
Universidade Federal de Pernambuco
como requisito à obtenção do título de Bacharel

Orientador: Prof. Ruy de Queiroz

RECIFE
2013

Sumário

1 INTRODUÇÃO 3
2 OBJETIVOS 4
3 CRONOGRAMA 5
4 BIBLIOGRAFIA 6

1 INTRODUÇÃO

A vigilância eletrônica consiste no monitoramento de informações e dados de computadores, armazenados em discos rígidos ou sendo transferidos por uma rede como a Internet. Tal monitoramento é frequentemente feito de modo clandestino, podendo ser realizado por corporações, organizações criminosas, indivíduos ou entidades governamentais. Essas vigilâncias são executadas de modo bastante difundido e quase todo o tráfego da Internet pode potencialmente ser monitorado [1].

O aumento no número de aparelhos eletrônicos, na última década, como computadores, câmeras, sensores, dispositivos sem fio, GPS, sistemas biométricos e outras tecnologias, vem contribuindo para que tais monitoramentos se intensifiquem. Com isso surgem sempre novas maneiras para invasão de privacidade, junto com a criação de infraestruturas poderosas para pô-las em prática. Quando várias tecnologias e técnicas de monitoramento são combinadas, elas podem criar uma rede de vigilância ainda mais poderosa [2].

Recentemente, o tema vem ganhando destaque por conta de monitoramentos realizados pela National Security Agency (NSA), uma das principais agências de inteligência dos Estados Unidos. Esse monitoramento de informações foi realizado em escala internacional, causando diversos conflitos políticos [3]. Com isso, técnicas e estratégias para prevenção e amenização dessa análise massiva de dados vêm sendo buscadas, muitas vezes com soluções dispendiosas ou impraticáveis para o problema, como foi o caso de algumas alternativas propostas pelo governo brasileiro [4].

Entretanto, apesar de tais monitoramentos serem tão comuns no dia-a-dia, pouco se é feito para tentar contornar esses ataques à privacidade. Porém, há muito que se pode fazer, tanto em nível de uma organização quanto em nível individual. Medidas como criptografar comunicações, utilizar redes como Tor e utilizar de sistemas de código aberto são alguns exemplos [5]. Porém, toda rede tem suas restrições nas técnicas que conseguem implementar para manutenção de privacidade, além de que pode ser impraticável para um usuário comum utilizar tantas medidas que muitas vezes até um profissional da área desconhece.

2 OBJETIVOS

Este trabalho tem como objetivo realizar uma análise dos possíveis pontos de ataque quando se quer realizar um monitoramento de um computador ou rede de computadores, bem como utilizar exemplos já realizados para demonstração da teoria na prática. A partir disso, serão apresentadas técnicas que podem ser executadas para se defender de tais ataques, ferramentas e recursos existentes voltados a esta finalidade e investigar suas limitações.

3 CRONOGRAMA

Atividade	Novembro	Dezembro	Janeiro	Fevereiro	Março
Levantamento bibliográfico					
Estudo do material pesquisado					
Escrita do TG					
Apresentação					

4 BIBLIOGRAFIA

[1] *Computer and network surveillance*. Wikipedia. Disponível em <http://en.wikipedia.org/wiki/Computer_surveillance>. Acesso em: 16 nov. 2013.

[2] STANLEY, Jay; STEINHARDT, Barry. *Bigger Monster, Weaker Chains*: The Growth of an American Surveillance Society. Nova Iorque: American Civil Liberties Union, 2013. Disponível em: <https://www.aclu.org/technology-and-liberty/bigger-monster-weaker-chains-growth-american-surveillance-society>. Acesso em: 17 nov. 2013.

[3] SHANE, Scott. No Morsel Too Minuscule for All-Consuming N.S.A. The New York Times. Nova Iorque, p. 1-1. 02 nov. 2013. Disponível em: <http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?_r=0>. Acesso em: 17 nov. 2013.

[4] ESTES, Adam Clark. *Brazil's Wild Plan to Purge America From Its Internet*. Gizmodo. Nova Iorque, p. 1-1. 17 set. 2013. Disponível em: <http://gizmodo.com/how-brazil-wants-to-purge-america-from-its-internet-aft-1333914046>. Acesso em: 17 nov. 2013.

[5] SCHNEIER, Bruce. *NSA surveillance*: A guide to staying secure. The Guardian. Londres, p. 1-1. 06 set. 2013. Disponível em: <http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>. Acesso em: 17 nov. 2013.