Sequestro de Conexão TCP: Uma Abordagem Contemporânea

Felipe Gonçalves dos Santos (UFPI. fgs4ntos@gmail.com),
Prof. Rayner Gomes Sousa (Orientador. UFPI. rayner@ufpi.br)

RESUMO EXPANDIDO

O protocolo de rede TCP, parte essencial da Arquitetura TCP/IP usada pela *Internet,* por décadas vem sendo estudado e avaliado em relação à segurança. Desde 1985 a comunidade científica vem execrando este protocolo e mostrando a facilidade de se quebrar requisitos mínimos de segurança dele. Em 1995, Paul Watson apresenta a comunidade científica a facilidade de se quebrar uma conexão TCP, através de uma técnica simples conhecida como Sequestro de Conexão, deixando ainda mais evidente que os 10 anos não foram suficientes para melhorar a segurança em relação ao protocolo TCP. Em 2005 Christoph Wegener e Wilhelm Dolle apresentaram um novo artigo mostrando, novamente, que mais 10 anos não foram suficientes para solucionar o problema de Sequestro de Conexão.

A quebra de uma conexão para algumas aplicações apresenta apenas um incomodo passageiro, porém para outras pode ser severamente prejudicial, ocasionando prejuízos financeiros elevadíssimos. Há uma relação diretamente associada a confiabilidade da rede. Se este problema ainda persistir a segurança se torna totalmente questionável e todas as aplicações fundamentadas na arquitetura TCP/IP, entre elas a nova gama de soluções para Computação em Nuvem, ficarão reféns do problema do Sequestro de Conexões.

Este trabalho refaz alguns dos testes feitos por Paul Watson orientado por uma metodologia próxima ao dele porém com Sistemas Operacionais recentes para descobrir se ainda o problema de quebra de conexão se apresenta como uma vulnerabilidade atual apesar de um quarto de século passado deste o início dos testes de segurança que o TCP vem sofrendo ao longo do tempo, ao tipo de ataque de Sequestro de Conexões.

Palavras-chave: Redes de Computadores, Ataque TCP/IP, Segurança.

Apoio:

Universidade Federal do Piauí - UFPI

Pró-Reitoria de Pesquisa e Pós-Graduação - PRPPG

Referências

[1] Géssica vereiro Hellmann. Crescimento da internet x crescimento da economia global. Fev 2011. http://gehspace.com/midias-sociais-blogs-corporativos/2011/02/14/crescimento-da-internet-x-crescimento-da-economia-global/.

[2] Open Source Vulnerability Database. Slipping in the windows. tcp reset attacks. Julho 2010. http://osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.doc.

[3] RFC 793. Transmission control protocol. julho 2010. http://tools.ietf.org/html/rfc1323.

[4] RFC 1323. Tcp extensions for high performance. julho 2010.

[5] Paul Watson. Open source vulnerability database.http://tools.ietf.org/html/rfc1323. julho 2010. http://osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.doc.

[6]Frsirt.Tcp connection reset remote exploit.julho 2010. www.frsirt.com/exploits/04232004/tcpexploit.

[7] Christph Wegener e Wilhelm Dolle. Entendendo e evitando ataques ao protocolo tcp. Pages 66-73, Outubro 2005. www.linuxmagazine.com.br/.../LM13_TCPhijack.pdf.

[8] PUC-RIO. Apostila de internet e arquitetura tcp/ip. 2. http://www.rjunior.com.br/download/tcp.pdf.

[9] Andrew S. Tanenbaum. Redes de computadores. 4, 2003.

[10] Internet world stats. Março 2011. http://www.internetworldstats.com/.

[11] Edson Furmankiwicz e Rogério Rodrigues. Tcp a bíblia tradução. 7, 2002.

[12] Luiz P. Maia. Arquitetura de redes de computadores. 1, 2009.

[13] Júlio Battisti. Tcp, udp e portas de comunicação. Setembro 2006. http://www.juliobattisti.com.br/artigos/windowstcpip_p11.asp.

[14] Larry L Peterson e Bruce S. Davie. Redes de computadores uma abordagem de sistemas. 2004.

[15] forcehacker. Definição de sniffer by thorking. 2006.http://www.forcehacker.kit.net/snif.html.