SSC0547 - Engenharia de Segurança

Professora : Kalinka Castelo Branco

Aluno : Ubiratan Soares (5634292)

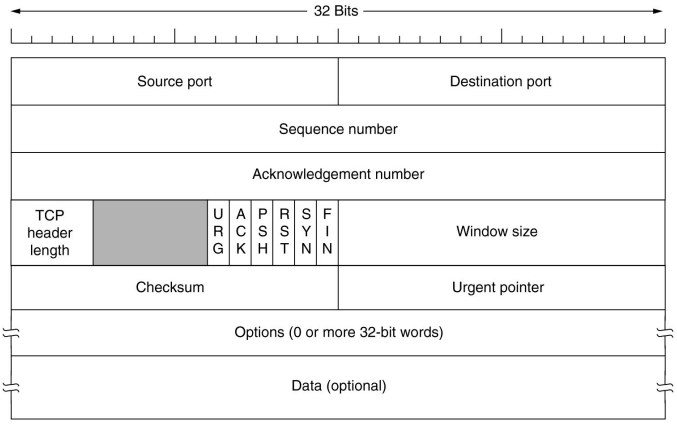
Exercício para Entregar

O ataque "TCP Sequence Prediction"

Data : 12/11/2010

O ataque **TCP Sequence Prediction** está relacionado à identificação dos números de sequência associados a segmentos transmitidos pelo protocolo TCP, de maneira que alguns desses possam ser falsificados e injetados na conexão pelo atacante[2].

Esse ataque deriva diretamente do mecanismo de *three-way handshake* para estabelecimento de conexões entre dois *peers* no protocolo TCP[3]. Esse mecanismo é descrito a seguir, envolvendo duas máquinas, cliente e servidor. Assume-se que esse está com a porta associada à comunicação aberta para novas conexões (*passive open*).



Cabeçalho TCP (IPv4)

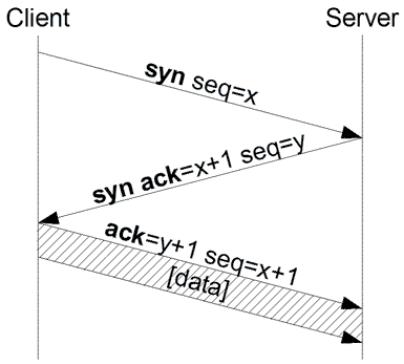


Diagrama de Sequência da Conexão TCP

1) O cliente solicita abertura de uma nova conexão (*active open*) com o servidor, enviando um segmento tipo **SYN** - ou seja, que contém o bit SYN ativo nos bits de flag - contendo um número de sequência gerado aleatoriamente **x** no campo *Sequence Number*.

2) O servidor responde ao cliente com um segmento tipo **SYN + ACK**, aceitando a conexão. Além das flags, ele responde com o campo *Acknowledgement Number* valendo **x + 1** e com com seu próprio número de sequência aleatório **y** no campo *Sequence Number*.

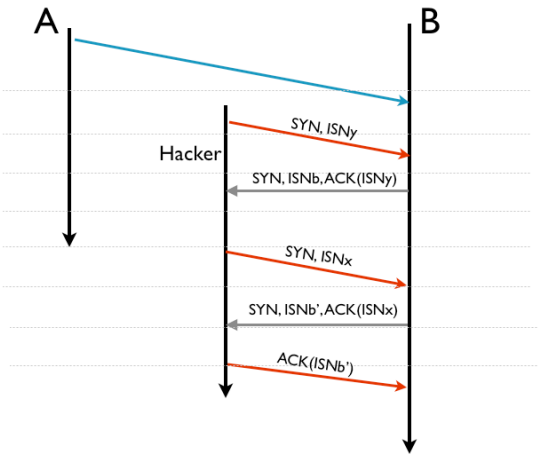
3) O cliente responde ao servidor, incrementando o campo *Acknowledgement Number* para **y + 1** no segmento de respota. Isso estabelece o *three-way handshake*. Os dados então já podem ser enviados entre as partes, com os números de sequência sincronizados entre os peers, estabelecendo o fluxo da conexão.

O ataque de Previsão do Número de Sequência consiste em explorar as fraquezas dos mecanismos de conexões TCP. Em especial, uma das fraquezas está na geração dos números de sequência **x** e **y** no processo de three-way handshake. O estabelecimento de tais parâmetros está vinculado à implementação dos protocolos pilha TPC/IP nos hosts envolvidos, com cada sistema apresentando suas peculiaridades.

A necessidade de mecanismos mais seguros para o estabelecimento de tais números foi inicialmente abordada por Morris, pesquisador da AT&T que demonstrou o mecanismo de previsão para a implementação TCP/IP do UNIX de Berkeley em 1985[4]. Essa falha foi detalhada por S.M. Bellovin na RFC1948, juntamente com possíveis mecanismos de corretivos para as implementações TCP, em 1996[5].

A falha desses sistemas permitia que o atacante, ao abrir uma conexão com um host, soubesse com grande grau de precisão qual o número de sequência que esse host usaria na próxima conexão. Um estudo de caso de como o ataque é realizado nessas condições está ilustrado a seguir [5] :

Inicialmente, o host A mantém uma comunicação TCP com o host B. Então, o hacker abre uma conexão com B, obtendo assim o número de sequência inicial **ISNb**.



Agora, o hacker abre uma nova conexão com B, dessa vez enviando um segmento falsificado como se fosse o host A, acompanhando pelo seu número de sequência inicial **ISNx**. O host B responde com um novo número de sequência, **ISNb'**, assumindo que é o host A que está abrindo uma nova conexão.

Apesar de agora o hacker não ter acesso explicíto ao número ISNb´, ele pode fazer a previsão do valor desse número e responder ao servidor com o segmento **ACK(ISNb')**. Se esse valor estiver corretamente previsto, o atacante consegue estabelecer uma conexão com o host B (que entende essa como estabelecida com o host A).

Uma vez estabelecida a conexão entre o host B e o atacante, esse é capaz de enviar segmentos para a vítima, solicitando por exemplo a execução de comandos remotos.

Um caso famoso desse tipo de ataque ocorreu na noite de Natal de 1994[6]. O atacante, Kevin Mitnick, lançou uma série de ataques sobre a rede de responsabilidade de Tsutomu Shimomura no *San Diego Supercomputer Center*, da Universidade de San Diego, EUA. Esses ataques contemplaram práticas como *IP spoofing*, *DoS* e *sequestro de sessão* combinadas.

Inicialmente, Mitnick lançou um ataque de **DoS** - Denial of Service - baseado em *SYN flood* contra um dos servidores da rede alvo. Esse rapidamente ficou indisponível para responder a novas conexões (fazendo aqui o papel do host A).

Mitnick então executou o **IP spoofing** para se camuflar como o servidor *offline* e a seguir, o alvo foi uma estação de trabalho tipo *x-term* da rede (a qual faz o papel do host B), que recebeu uma série de segmentos falsificados.

A resposta a esses segmentos deu ao hacker o conhecimento de como a máquina *x-term* gerava os números de sequência, e por consequência, permitiu ao atacante estabelecer uma conexão legítima e executar comandos no alvo, que tinha o servidor *offline* na lista de conexões confiáveis para comandos remotos. Mitnick instalou um módulo para **sequestro de sessão** na máquina alvo, e habilitou nessa a execução de comandos remotos a partir de qualquer máquina, de maneira que o *IP spoofing* não fosse mais necessário.

Para a infelicidade do hacker, Shimomura é engenheiro de redes e especialista em segurança, e manteve-se atento ao ataque durante todo o processo. Com as ferramentas de diagnóstico que possuía, colaborou com a operação do FBI para rastrear e prender Kevin Mitnick, que foi detido em 15 de fevereiro de 1995[7].

Referências :

1. *Computer Networks* - Tanembaum, A. S, 4th Edition. Prentice Hall, 2003.

2. *TCP Sequence Prediction Attack* - Wikipedia, the Free Encyclopedia http://en.wikipedia.org/wiki/TCP_sequence_prediction_attack - Acessado em 05/11/2010

3. *Transmission Control Protocol* - Wikipedia, the Free Encyclopedia http://en.wikipedia.org/wiki/Transmission_Control_Protocol - Acessado em 05/11/2010

4. *Security Problems in the TCP/IP Protocol Suite* - Bellovin, S. M. New Jersey, 1989.

5. *Defending Against Sequence Number Attacks* (RFC1948) http://tools.ietf.org/html/rfc1948 - Acessado em 05/11/2010

6. *Kevin Mitnick's Attack on Tsutomu Shimomura's Computers and How IDS Could Have Saved the Day* http://book.soundonair.ru/cisco/ch14lev1sec6.html - Acessado em 06/11/2010

7. *Kevin Mitnick* - Wikipedia, the Free Encyclopedia http://en.wikipedia.org/wiki/Mitnick - Acessado em 06/11/2010