Capítulo 4 – Vulnerabilidades na Arquitetura TCP/IP

- ✔ 4.1 – Introdução
- ✔ 4.2 – Problemas de segurança inerentes ao TCP/IP
  - 4.2.1 – *Sniffers*
  - 4.2.2 – *Source routing*
  - 4.2.3 – *Spoofing*
  - 4.2.4 – *Syn flood*
  - 4.2.5 – *Smurf*
  - 4.2.6 – *Port scan*
  - 4.2.7 – *Distributed denial of service (DDoS)*

- ✔ 4.3 – Vulnerabilidades em implementações específicas
  - 4.3.1 – Ping da morte (*ping o'death*)
  - 4.3.2 – *IP denial of service (land e teardrop)*
  - 4.3.3 – *Teardrop*
  - 4.3.4 – *Land*

4.1 – Introdução

- ✔ Neste capítulo, são apresentados alguns ataques conhecidos que são inerentes ao projeto do protocolo TCP/IP
- ✔ Também são apresentados ataques que são problemas de uma implementação específica

4.2 – Problemas de segurança inerentes ao TCP/IP

4.2.1 – *Sniffers*

- São programas capazes de “escutar” a rede em busca de informações importantes
- Coleta informações em um determinado segmento de rede
  - comparado a um grampo telefônico, mas permite “escutar” diversas “conversas” ao mesmo tempo
- A maior parte do tráfego numa rede ainda não é criptografado
- Exemplos de *sniffers*: Wireshark e tcpdump

- Podem ser usados para o bem e/ou para o mal
  - bem: análise de tráfego, diagnóstico de problemas
  - mal: coleta de senhas, espionagem
- *Sniffer* utiliza de um recurso presente nas maiorias das placas ethernet: ***modo promíscuo***
- Uma NIC geralmente recusa quadros cujo endereço MAC de destino não seja o seu ou um endereço de *broadcast*
- Em modo promíscuo, a NIC passa a aceitar qualquer quadro, inclusive os que têm destino a outras máquinas da rede
- ***Hub***: repassa todos os quadros que recebe para todas as portas
- ***Switch***: só repassa os quadros para as portas certas

- Uma máquina rodando um *sniffer* não conseguirá ouvir o tráfego presente em outras portas do *switch*
  - ouve somente o tráfego local e os pacotes de *broadcast*
- Existem técnicas que permitem que o tráfego seja observado mesmo em *switchs*
- *switchs* possuem *buffer* para armazenar a CAM (tabela de correlações entre endereços MAC e portas do *switch*)
- *buffer* possui tamanho limitado → CAM terá tamanho fixo com número limitado de entradas

- Ataque *CAM Table Flooding*: consiste em enviar uma série de requisições ARP falsas, contendo endereços MAC randômicos e distintos
  - essas requisições encherão a tabela CAM do *switch*, fazendo com que novas requisições sejam repassadas para todas as portas
- Ataque *MAC Spoofing*: falsificação de endereços MAC em quadros ethernet
- Prevenção: ???
  - configurar manualmente as entradas da tabela CAM para todas as portas do *switch*
  - problemas: estações que se movem com frequência

4.2.2 – *Source routing*

- *Source routing*: opção especial do pacote IP, em que o originador do pacote pode indicar explicitamente a rota por onde um pacote deve passar
  - opção criada para diagnóstico de rede
- Usuários maliciosos podem usar o *souce routing* para se fazer passar por outras máquinas na rede
- Alguns sistemas operacionais já vem com esta opção desabilitada
- Prevenção: ???
  - configurar todos os roteadores da sua rede para rejeitarem (descartarem) pacotes com essa opção habilitada

4.2.3 – Spoofing

- *Spoofing* consiste em falsificar identidade na rede
  - é qualquer procedimento que envolva personificação de usuários ou máquinas, incluindo endereços IP e consultas em servidores de nomes
- Usado para obter acesso não autorizado, ou para esconder tentativas de ataque
- Existem diversos tipos de *spoofing*:
  - IP
  - DNS
  - Web
  - e-mail
  - roteamento
  - etc

E-mail spoofing

- O SMTP não possui nenhum sistema de autenticação padrão que comprove a autenticidade do remetente
- Forma simples de realizar um ataque de engenharia social
- Forma mais simples e utilizada para realizar um *spoofing*
- Como fazer ???
  - basta informar ao SMTP, no momento do envio do e-mail, um remetente diferente
  - SMTP não confere a identidade do remetente, assim como no correio convencional :(
- Como evitar ???
  - Configurar o MTA para que ele exija autenticação
- Recomendações sobre e-mail *spoofing*:
  - http://www.cert.org/tech_tips/email_spoofing.html

IP spoofing

- *IP spoofing* consiste em falsificar o endereço IP de origem para tentar enganar regras de filtragem por IP, ou sistemas de autenticação baseados em IP
- O roteamento na Internet se baseia no IP de destino
- O IP de origem é usado apenas para o retorno da informação
- Pacote com IP de origem falso chegará ao destino, mas sua resposta será enviada para outra origem
- Parece uma prática inútil, uma vez que o pacote nunca retornará para o próprio atacante
- Por que fazer ???

- Sequestro de conexão: em conexões em andamento, o atacante pode conseguir “sequestrar” a conexão, através da manipulação dos números de sequência do TCP
  - utilizar um *sniffer* e capturar as respostas
  - necessário que o atacante esteja na mesma sub-rede que a vítima
- Ataque cego: o atacante é capaz de “advinhar” qual seria a resposta e envia o próximo pacote de acordo
  - necessário “advinhar” os números de sequência do servidor
- Negação de serviço (DoS): o atacante enviará pacotes mal-formados com a intenção de negar o serviço remoto através de uma vulnerabilidade ou inundação

- ✔ Como se proteger ???
- ✔ Usar filtros ***ingress*** e ***egress***: nenhum pacote deve sair de sua rede com um endereço IP que não pertença à sua rede; e nenhum pacote deve entrar com endereço de origem de dentro da sua rede
- ✔ Números de sequência randômicos
- ✔ Criptografia e autenticação: sistemas seguros devem criptografar a informação e exigir meios de autenticação entre as partes

Roteamento

- **Roteamento estático**: definido manualmente pelo administrador da rede
- **Roteamento dinâmico**: definido através de protocolos específicos de roteamento
- Rotas dinâmicas são propagadas pelos próprios roteadores que compõem a rede
- Atualizações de tabelas de roteamento podem ser falsificadas
- Como fazer ???
  - qualquer elemento na rede poderia se passar por um roteador e enviar atualizações de rota falsas para outros roteadores da rede
- Como evitar ???
  - utilizar protocolos modernos, como o RIPv2 e o OSPF, que dispõem de esquemas de autenticação

4.4 – Atividades

1. Usar o tcpdump no roteador de sua bancada para capturar todo o tráfego da rede interna.
2. Analisar o tráfego capturado na atividade 1 dentro do Wireshark.
3. Utilizar o Wireshark para analisar o tráfego interno da rede usando um hub e depois um switch.
4. Configurar, manulamente, a placa de rede de uma estação para operar em modo promíscuo
5. Pesquisar na Internet uma forma de se fazer um ataque CAM Table Flooding no switch de sua bancada. Comprovar o sucesso desse ataque com o Wireshark.
6. Realizar um ataque MAC Spoofing e comprovar o sucesso desse ataque utilizando o tcpdump no roteador de sua bancada.