Segurança de redes de computadores

Roberto Sadao Yokoyama

UTFPR-CP

Setembro, 2016

Aula de hoje: [1]

1. Protocolo ARP
   - Ataques
     - MAC spooging
     - MAC flooding
     - ARP spoofing
     - Man-in-the-middle
2. DoS (Denial of Service)
   - IP spoofing
   - Ataques de inundação
   - Fragmentação de pacotes IP
3. Prática: Ataque homem no meio
4. Demonstrações

[1] Slides baseados no material do livro: Goodrich [2], Mota Filho [4] e Forouzan [1]

ARP

ARP (Address Resolution Protocol): a entrega de um pacote IP para um host ou um roteador requer dois níveis de endereçamento: lógico e físico. O ARP cria o mapeamento entre os endereços lógicos e físicos. Os pacotes IP usam endereços lógicos (host-to-host). Esses pacotes, porém, devem ser encapsulados em frames, que requerem endereços físicos (nó-a-nó).

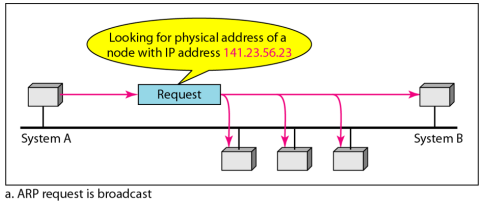
MAC Addresses:

- Os hosts e roteadores são identificados por seus endereços físicos. Endereço físico é local e precisa ser exclusivo localmente, mas não necessariamente exclusivo globalmente.
- Exemplo: MAC de 48 bits representado por 6 hexadecimais 00-1A-92-D4-BF-86. Os 3 primeiros identificam o fabricante: Ex. Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92

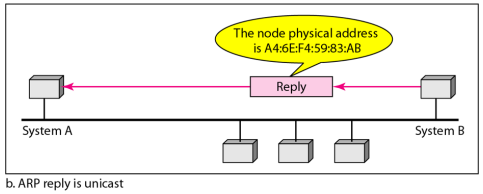
ARP

Operação ARP (Address Resolution Protocol):

- Uma solicitação ARP é transmitida em broadcast e uma resposta ARP é transmitida em unicast (unicast)



a. ARP request is broadcast

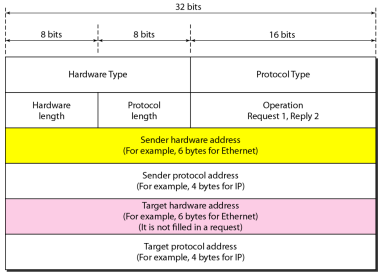


b. ARP reply is unicast

ARP

Campos do ARP:

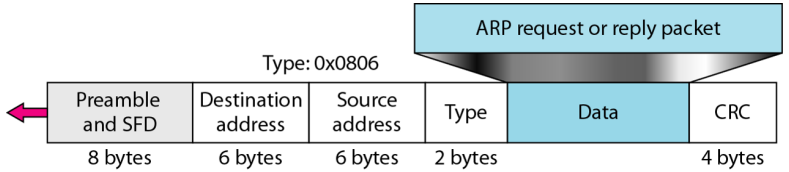
- **Hardware Type**: tipo de rede. Ethernet=0001
- **Protocol Type**: protocolo que deseja a informação. IPv4=0800
- **Hardware Length**: tamanho do endereço de hardware. MAC=06
- **Protocol Length**: tamanho do endereço de rede. IPv4=04
- **Operation**: tipo de ARP. ARP resquest=0001; ARP reply=0002
- **Sender Hardware Address**: endereço físico do emissor. MAC
- **Sender Protocol Address**: endereço lógico do emissor. IP
- **Target Hardware Address**: endereço físico do destinatário. MAC
- **Target Protocol Address**: endereço lógico do destinatário. IP



ARP

Encapsulamento (campos Ethernet):

- **MAC Destino**
- **MAC Origem**
- **Type**: protocolo que está no payload (ARP=0806, IP=0800)
- **Payload**: dados (usualmente, 46 a 1500 bytes)
- **Checksum**: CRC



Ataques

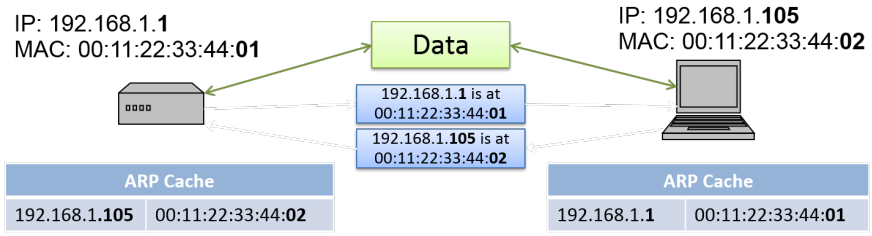
- **MAC spooging**: é o ato de trocar, via software, o endereço MAC de um adaptador de rede. Por exemplo, o atacante pode trocar o endereço para entrar em sistemas que usam autenticação via endereço MAC. Ex. no Linux: *ifconfig eth0 hw ether 00:11:22:33:44:55*
- **MAC flooding**: inunda a rede com associações diversas de MACs com IPs, de forma totalmente descasada e irreal, forçando o switch a reaprender em que porta está cada MAC. O switch para não parar o tráfego da rede, irá deixar passar todo o tráfego, por todas as portas.
- **ARP spoofing**[2]: falsificação de ARP o atacante manipula a tabela ARP (cache ARP) dos alvos, normalmente, o host e o *gateway*. Por exemplo, o atacante pode ficar entre a comunicação aplicando um ataque man-in-the-middle.

[2] https://net.educause.edu/ir/library/powerpoint/SEC08078.pps

Ataques

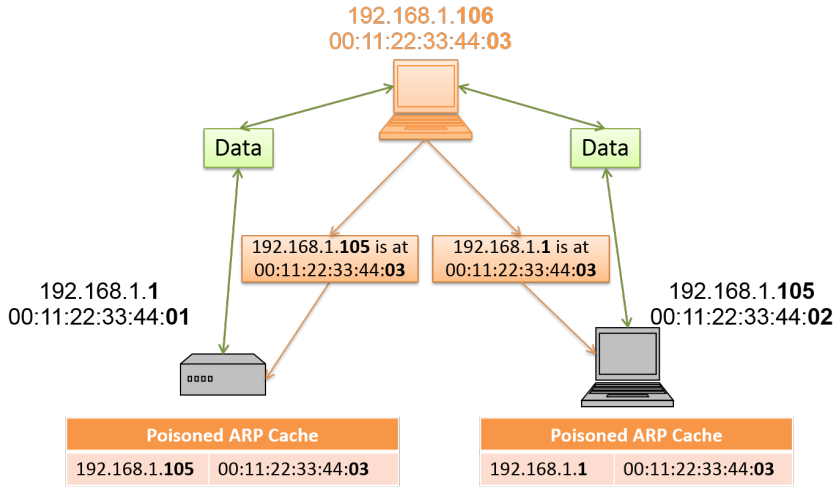
ARP spoofing

- Protocolo ARP não tem esquema de **autenticação**. Qualquer computador na rede pode afirmar que tem um endereço requisitado
- **Gratuitous ARP reply** é um ARP reply sem uma requisição ARP prévia. Normalmente, para informar a troca de endereço IP do host implemenatado em alguns SO.



Ataques

Man-in-the-midlle



Ataques de negação de serviço

DoS (Denial of Service)

é uma tentativa de comprometer a *disponibilidade*, impedindo ou bloqueando completamente o fornecimento de um serviço.

- **DoS** não estão preocupados com recebimento de respostas. Usam IP spoofing para obscurecer a identidade do atacante, bem como dificultar abrandar o ataque.
- **Categorias**:
  - *Largura de banda da rede*: sobrecarrega o enlace de rede
  - *Recursos do sistema*: sobrecarrega o software de tratamento de rede. Ex. falsificação de SYN; Ping da morte
  - *Recursos da aplicação*: sobrecarrega um servidor WEB. Por exemplo, construir uma consulta grande e custosa, o atacante pode gerar um grande número de requisições com essa consulta.

Falsificação IP

- **IP spoofing**: o atacante falsifica o endereço de origem do pacote IP. Contudo, não permite que o atacante assuma um novo endereço, pois o IP real permanece o mesmo do host.
- Protocolo IP não limita o uso da largura de banda. Um grande número de pacotes podem ser injetados na rede para iniciar um DoS
- Um maneira de proteção é por meio de filtro de pacotes IP o mais próximo possível do sistema originador

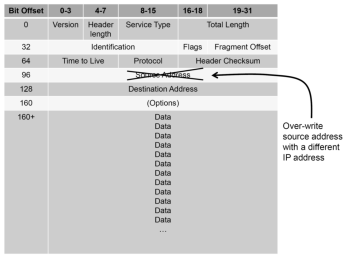
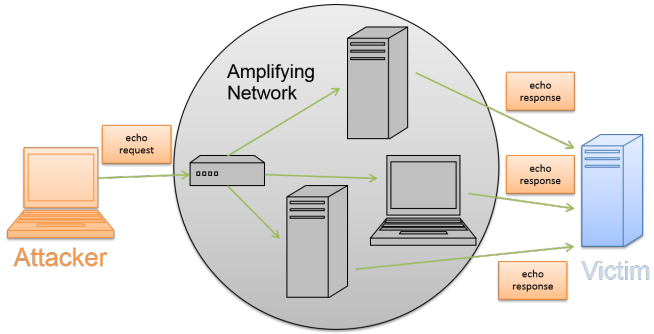


Figure 5.12: How IP spoofing works. The source address in the header of an IP packet is simply overwritten with a different IP address from the actual source. Note the header checksum field also needs to be updated.

Ataques de inundação

- **Ataque Smurf**: envia ICMP echo request para endereço IP de broadcast da rede, tendo como origem o endereço IP da vítima.



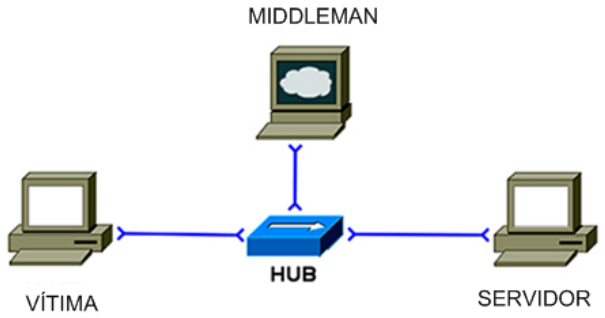
Fragmentação de pacotes IP

Fragmentação de pacotes IP

- Está relacionada à quantidade máxima de dados (MTU – Maximum Transfer Unit) que podem passar em um pacote por um meio físico da rede
- Pacotes maiores que a MTU são fragmentados. Os fragmentos trafegam pela rede e são reagrupados quando chegam ao destino final
- O reagrupamento possibilita o atacante manipular os fragmentos e enviar um pacote maior que o buffer do receptor, ocorrendo um overflow. Ex. Ping o'Death.

Netkit: Ataque homem no meio[3]

- A figura abaixo representa a topologia de rede sendo estudada. Temos uma rede simples em LAN com 3 computadores. Um servidor, a vítima e o atacante, middleman.
- O uso do hub neste cenário é importante para simplificar o ataque. O mesmo ataque seria possível no entanto se fosse um switch, de modo que seria necessário atacar o switch também, no entanto.



[3] Laboratório do livro: Gurgel [3]

Sugestões de demonstrações

- **Implementar um cavalo de troia** (preferencialmente sem utilizar a ferramenta *msfvenon*). O cavalo de troia deve ser embutido em um jogo (ex. jogo da velha, campo minado etc). A ação maliciosa do cavalo de troia será a cópia dos arquivos que estão no diretório de execução do jogo e transmitir via rede para a máquina do atacante [médio].
- **Implementar um screenlogger**. O screenlogger deve capturar a tela (print screen) sempre que a vítima executar um aplicativo alvo (por exemplo, firefox). Os dados capturados podem ser armazenados localmente ou enviados ao atacante. O screenlogger deve ser executado em background (segundo plano, como um daemon) [difícil].

Sugestões de demonstrações

- Apresentar como utilizar os **sistemas de segurança do Windows** moderno. Autenticação, controle acesso, permissões de arquivos, recuperação de dados, backup, criptografia do disco, compartilhamento de arquivos, etc [fácil].
- Realizar um **ataque de *buffer overflow*** em um aplicativo real do Windows com essa vulnerabilidade conhecida (ex. War-FTP). Explicar o sistema de memória do Windows, o endereço da memória onde ocorre o estouro da memória e injetar um *payload* malicioso [difícil].
- Realizar um ataque **man-in-the-middle** em uma rede sem fio desprotegida (sem criptografia) para filtrar e substituir uma mensagem da vítima para o servidor (tentar utilizar outro serviço diferente de FTP) [fácil].

Referências

[1] B. A. Forouzan. *Comunicação de Dados e Redes de Computadores*. McGrawHill e Bookman, 2008.

[2] M. T. Goodrich and R. Tamassina. *Introdução à Segurança de Computadores*. Bookman, 2013.

[3] P. Gurgel, K. R. L. C. Branco, L. H. C. Branco, F. E. Barbosa, and M. M. Teixeira. *Redes de Computadores Da teoria à prática com Netkit*. Elsevier, 1ed, 2015.

[4] J. E. Mota Filho. *Análise de tráfego em redes TCP/IP*. Novatec, 2013.