Segurança Informática e nas Organizações

Guiões das Aulas Práticas

João Paulo Barraca[1] e Hélder Gomes[2]

[1]Departamento de Eletrónica, Telecomunicações e Informática
[2]Escola Superior de Tecnologia e Gestão de Águeda
Universidade de Aveiro

2015–2016

Conteúdo

2

ARP Poisoning

Resumo:

- Manipulação de *caches* ARP
- Ataques de envenenamento de *caches* ARP
- Ataques por interposição (*Man-in-the-Middle*)
- Observação de tráfego alheio

2.1 Introdução

A aplicação `ettercap`[1] é uma ferramenta para análise de protocolos de rede e quebras de segurança. Tem a capacidade de intercetar tráfego num segmento de rede, de capturar senhas e de realizar ataques contra vários protocolos.

Um dos ataques possíveis de realizar com o `ettercap` consiste na manipulação das *caches* ARP (*Address Resolution Protocol*), o que é conhecido como um ataque de envenenamento das *caches* ARP (ARP *Poisoning*). O princípio deste tipo de ataque é o envio de mensagens ARP falsas para a rede, para provocar alterações nas *caches* ARP das máquinas vítimas de modo a que todo o tráfego entre as máquinas vítimas sofra um reencaminhamento (por exemplo, passe pelo atacante).

No caso em que o atacante se coloca no meio do tráfego entre dois quaisquer nós ele concretiza um ataque de interceção conhecido como *homem no meio* (*Man-in-the-Middle*, ou MitM). Este ataque implica a associação, na tabela ARP de cada máquina vítima, do endereço MAC do atacante com os endereços IP das restantes máquinas vítima. O atacante, ao receber os pacotes trocados pelas máquinas vítimas, pode optar por encaminhá-los normalmente entre elas (limitando-se o ataque a uma escuta passiva), ou modificar os dados antes de os enviar. O atacante pode também optar por fazer um ataque de negação de serviço (*Denial of Service* – DoS) contra uma vítima ao associar um endereço MAC inexistente ao endereço IP de um interlocutor dessa vítima (por exemplo, o endereço IP do seu `gateway` por omissão). Este ataque é conhecido como ARP *Black Hole*.

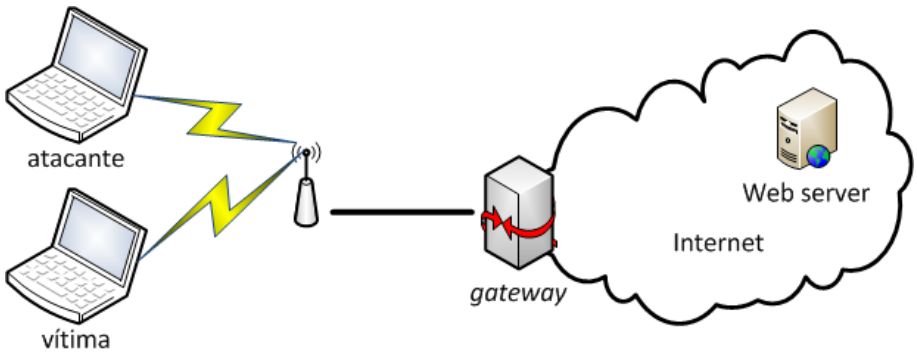

Figura 2.1: Arquitetura da rede para a demonstração do ataque.

Para a realização deste trabalho, cada grupo irá usar a rede da figura 2.1 utilizando o material de rede disponibilizado pelo docente. A máquina atacante deve ser Linux e a máquina vítima pode ser Windows ou Linux, à

[1] `http://ettercap.github.io/ettercap`

escolha. Pode usar máquinas físicas ou máquinas virtuais, tanto para a máquina vítima como para a máquina atacante. A máquina atacante pode ser por exemplo uma distribuição Linux LiveUSB, tal como a Kali[2].

Antes de começar a instalar a rede, garanta que o analisador de protocolos `wireshark` está instalado tanto na máquina vítima como na máquina atacante.

2.2 Montagem da rede

Ligue tanto o computador atacante como a vítima à rede WiFi fornecida pelo docente; pormenores sobre a mesma serão fornecidos na aula. A rede WiFi possui servidor DHCP, pelo que ambos os computadores ficarão com as configurações de rede corretas. Esta configuração permite que os computadores se liguem à rede da UA e à Internet em geral. Verifique que a rede fica a funcionar corretamente e que consegue aceder a páginas Web na Internet.

2.3 Preparação do ataque

Verifique a cache ARP da máquina vítima (através do comando `arp -n`) e **registe o endereço MAC associado ao endereço IP do seu gateway por omissão** (obtido através do comando `route -n`).

Ative o analisador de pacotes `wireshark` na máquina vítima e na máquina atacante. Na máquina vítima faça um `ping` para um endereço na Internet (por exemplo `www.ua.pt`) e compare os pacotes capturados pelo `wireshark` nas máquinas vítima e atacante. Comente estas capturas.

Se necessário, instale o pacote `ettercap-graphical` (com `apt-get install`) na máquina atacante. Uma vez instalado, altere o respetivo ficheiro de configuração `/etc/etter.conf` para colocar as variáveis `ec_uid` e `ec_guid` de acordo com o excerto abaixo:

```
[privs]
ec_uid = 0 # nobody is the default
ec_gid = 0 # nobody is the default
```

Recorrendo ao manual do `ettercap` (`man ettercap`), explique a razão desta alteração.

[2] `http://www.kali.org`

2.4 Realização do ataque de interceção

Neste trabalho pretende-se envenenar as *caches* ARP da máquina vítima e do `gateway` da rede, de modo que a vítima reencaminhe para o atacante todo o tráfego dirigido ao seu `gateway` e que o `gateway` reencaminhe para o atacante todo o tráfego dirigido à vítima. Desta forma, o atacante interceta todo o tráfego entre a vítima e o `gateway`. Para o efeito siga os seguintes passos:

- Inicie o `ettercap` com o comando

  ```
  ettercap -G
  ```

  Coloque-o em modo *Unified Sniffing* (menu *Sniff/Unified Sniffing*) e selecione a interface a usar (no nosso caso, a WiFi, ou WLAN)). Neste modo o `ettercap` irá reencaminhar todos os pacotes que cheguem à interface de rede selecionada e que possuam como destino o seu endereço MAC e um endereço IP de diferente do seu.

- Selecione as máquinas vítima. Para o efeito, faça primeiro uma procura de máquinas na rede (menu *Hosts/Scan for hosts*). Com base na lista de máquinas descobertas (uma vez mais, através do menu *Hosts/Host list*), selecione a máquina vítima e pressione no botão *Add to Target 1* e depois selecione o `gateway` e pressione no botão *Add to Target 2*.

- Lance o ataque de envenenamento das *caches* ARP das duas máquinas escolhidas (menu *Mitm/Arp poisoning*). Na janela de parâmetros opcionais que se abre, selecione a opção *Sniff remote connections* e pressione Ok.

  O ataque para o envenenamento das *caches* AP já está a decorrer. No entanto, é ainda necessário o passo seguinte.

- Dê início à escuta de pacotes (menu *Start/Start sniffing*). Sem este passo, os pacotes que a vítima pretende enviar ao `gateway`, e vice-versa, não seriam reencaminhados pelo atacante, ou seja, a vítima ficaria sem comunicação com o seu `gateway` (o atacante atuaria como um buraco negro para a comunicação entre ambos).

Verifique a cache ARP da máquina vítima e registe o endereço MAC associado ao endereço IP do seu `gateway` por omissão. Utilizando o `wireshark`, inicie capturas de tráfego na máquina cliente e na máquina atacante, e faça `ping` da vítima para o `gateway`. Comente e justifique as diferenças entre o observado agora, na tabela de ARP da vítima e nas capturas de tráfego, e o observado na secção 2.3.

2.5 Observação do tráfego intercetado

Neste momento, como todo o tráfego entre a máquina vítima e o seu `gateway` passa pela máquina atacante, ela está em condições de lançar ataques de inspeção do tráfego intercetado. Como exemplo, o atacante irá observar as páginas Web a que a vítima acede. Para o efeito, siga os passos seguintes:

- Termine o ataque de ARP Poisoning e feche o `ettercap`.
- Inicie, com permissões de administrador, o navegador configurado como navegador principal no seu sistema (aquele que se inicia quando acede a uma página web a partir de um link)
- Inicie o `ettercap`, tal como na Secção 2.4.
- Inicie o *plugin* que permite visualizar as páginas Web a que a vítima acede (menu *Plugins/Manage plugins*, faça duplo clique sobre o *plugin* `remote_browser` e depois feche a janela).
- Na máquina da vítima, aceda a uma página Web, como por exemplo a da UA (`http://www.ua.pt`). Comente o resultado.

Consegue visualizar páginas Web acedidas através de ligações seguras (https)? Porquê?

2.6 Desafio

Analise os vários plugins disponibilizados pelo Ettercap. Usando a ajuda disponibilizada pelo Ettercap, lance um ataque de DNS Spoofing.

2.7 Bibliografia

- ARP *poisoning*, `http://en.wikipedia.org/wiki/ARP_spoofing`.
- `ettercap`, `http://en.wikipedia.org/wiki/Ettercap_%28computing%29`.