



Faculdade de Tecnologia SENAC Goiás

Segurança da Informação

Aldo Brito da Costa Filho

Levi Souza

Matheus Marçal

Matheus Oliveira

## **HARDENING CONTRA MITM EM LINUX E WINDOWS SERVER**

Goiânia

2015

Aldo Brito  
Levi Souza  
Matheus Marçal  
Matheus Oliveira

## **HARDENING CONTRA MITM EM LINUX E WINDOWS SERVER**

Hardening contra o ataque MITM em servidores Linux e Windows Server desenvolvido no curso de Segurança da Informação, da Faculdade de Tecnologia SENAC Goiás para o Projeto Integrador do 2º Período

Goiânia

2015

## **Sumário**

<b>1. Introdução .....</b>	<b>4</b>
<b>2. Hardening.....</b>	<b>5</b>
<b>3. MITM.....</b>	<b>5</b>
<b>4. Como se proteger do MITM.....</b>	<b>6</b>
<b>4.1. Servidor Linux.....</b>	<b>6</b>
<b>4.2. Servidor Windows.....</b>	<b>7</b>
<b>5. Configurações.....</b>	<b>7</b>
<b>5.1. Fixação de endereço MAC no switch.....</b>	<b>7</b>
<b>5.2. Configuração do ArpON .....</b>	<b>7</b>
<b>5.3. Configuração ArpFreezeNG .....</b>	<b>9</b>

## **1. Introdução**

Neste relatório iremos ver como fazer um Hardening contra o ataque MITM (Man-in-the-middle) nos servidores Linux e Windows.

## 2. Hardening

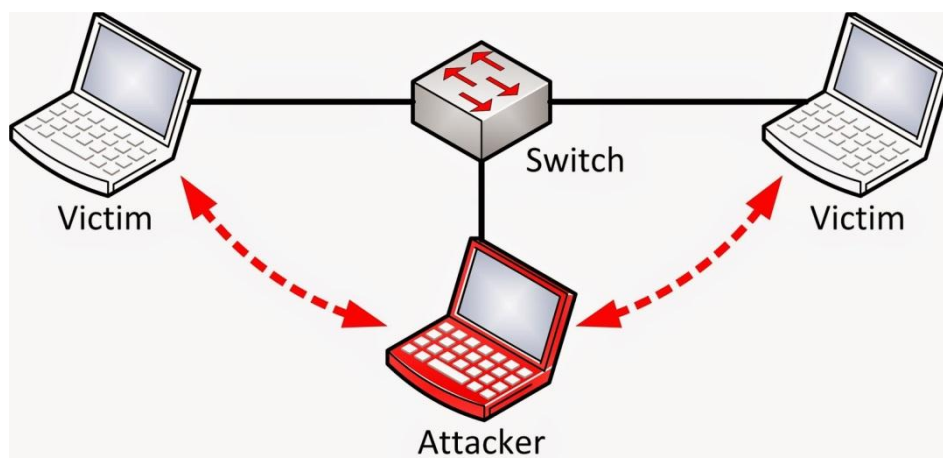
A definição de hardening (Técnica de blindagem do sistema): Hardening é o processo de mapeamento de ameaças, mitigação dos riscos e execução de correções no sistema para prepara-lo para possíveis ataques e invasões.

## 3. MITM

Man-in-the-middle (Homem no meio) é o tipo de ataque em que o invasor intercepta dados entre dois interlocutores e falsifica as trocas a fim de fazer-se passar por uma das partes, em uma comunicação normalmente as vítimas comunicam entrem si sem a interferência do invasor, este tipo de ataque ocorre na camada 2 (enlace) do Modelo TCP e só pode ser realizada caso o atacante esteja na sua rede local.

O ataque ARP Poisoning ou ARP Spoofing são os tipos de ataques mais eficientes de executar o MITM,

O ataque ARP Spoofing consiste em adicionar uma entrada que diz o IP da máquina alvo que está fazendo a comunicação e o endereço MAC do atacante. Quando a máquina alvo for montar um pacote para envio ela vai montar com o IP real do servidor de destino que ela quer acessar porem utilizará o MAC do atacante.



## 4. Como se proteger do MITM

Uma das formas de se proteger contra este tipo de invasão é habilitando o MAC binding ou fazendo uma ACL, ACL é uma lista de controle de acesso que pode ser feita em alguns switches. MAC binding é uma característica encontrada em switches que não permite que os endereços associados sejam alterados após a sua configuração, esta é a maneira mais prática de se proteger, outra defesa é colocar os endereços físicos de forma estática mas em redes grandes isso é inviável por ser muito trabalhoso ter que configurar host a host e levaria muito tempo.

### 4.1. Servidor Linux

No servidor Linux vamos utilizar a ferramenta chamada ArpON, ArpON(ARP handler inspection) é um manipulador daemon que torna o protocolo ARP seguro a fim de evitar o ataque MITM através dos ataques ARP Spoofing, ARP Cache Poisoning ou ARP Poison Routing(APR). Esta ferramenta bloqueia também ataques derivados: Sniffing, Hijacking, Injection, Filtering e ataques mais complexos ou derivados, como: falsificação de DNS, Web Spoofing, Session Hijacking

Esta ferramenta consegue fazer o bloqueio através de três tipos de técnicas anti ARP spoofing: a primeira é baseada no SARPI (Static ARP Inspection) em redes que estão configuradas como estática, a segunda baseada no DARPI (Dynamic ARP Inspection) em redes configuradas dinamicamente com DHCP e a terceira é baseado no HARPI (Hybrid ARP Inspection) com uma rede que possui configuração estática e dinâmica.

Outra ferramenta é a ArpWatch, *Arpwatch* é uma ferramenta que monitora a atividade em uma rede ethernet, mantendo atualizada uma tabela com endereços ethernet(MAC) e seus respectivos endereços IP. Essa ferramenta tem a capacidade de reportar via email certas mudanças.

O Arpwatch é uma ferramenta importante na monitoração da rede contra ataques de Arp Poisoning ou Arp Spoofing esta ferramenta apenas alerta o administrador da rede sobre as mudanças de IP e MAC dos hosts.

## **4.2. Servidor Windows**

A ferramenta utilizada no Windows Server foi a ARPFreezeNG, uma ferramenta bastante simples de se utilizar, A ferramenta deixa você configurar sua tabela ARP de forma estática de uma maneira bastante simples para que os atacantes (usando ArpSpoof, Ettercap ou outra ferramenta) não consigam realizar o ataque.

## **5. Configurações**

### **5.1. Fixação de endereço MAC no switch**

No switch da Cisco basta entrar na configuração das interfaces, verificar se estão no modo de acesso e usar os seguintes comandos:

```
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport port-security
```

```
Switch(config-if)# switchport port-security maximum 1
```

```
Switch(config-if)# switchport port-security mac-address stick
```

```
Switch(config-if)# switchport port-security violation shutdown
```

### **5.2. Configuração do ArpON**

O ArpON pode ser instalado de uma maneira bem simples através do repositório digitando apt-get install arpon ou você pode baixa-lo do site oficial da ferramenta <<http://arpon.sourceforge.net/>>. O arquivo de configuração do ArpON fica em /etc/default/arpon nele você habilita de que modo a ferramenta vai funcionar, se vai ser pelo SARPI ou DARPI

```
root@PC-XXXX: ~
GNU nano 2.2.6      Arquivo: /etc/default/arpon

# Defaults for arpon initscript
# sourced by /etc/init.d/arpon
# installed at /etc/default/arpon by the maintainer scripts

# You must choose between static ARP inspection (SARPI) and
# dynamic ARP inspection (DARPI)
#
# For SARPI uncomment the following line (please edit also /etc/arpon.sarpi)
#DAEMON_OPTS="-q -f /var/log/arpon/arpon.log -g -s"

# For DARPI uncomment the following line
DAEMON_OPTS="-q -f /var/log/arpon/arpon.log -g -i eth0 -d"

# Modify to RUN="yes" when you are ready
RUN="yes"
```

Neste exemplo foi utilizado o DARPI, depois disto basta iniciar o ArpON com `service arpon start`, o arquivo de log fica localizado em `/var/log/arpon/arpon.log`. É possível iniciar o arpon através de comandos como por exemplo `arpon -i eth0 -D` após digitar este comando seu ArpON vai começar a funcionar da seguinte forma.

```
root@PC-XXXX: ~
src IP = <192.168.1.120>
21:53:11 ARP cache, DENY
src HW = <50:e5:49:f7:a:93>
src IP = <192.168.1.120>
21:53:11 ARP cache, ACCEPT
src HW = <50:e5:49:f7:7:ba>
src IP = <192.168.1.120>
21:53:13 ARP cache, DENY
src HW = <50:e5:49:f7:a:93>
src IP = <192.168.1.120>
21:53:13 ARP cache, ACCEPT
src HW = <50:e5:49:f7:7:ba>
src IP = <192.168.1.120>
21:53:15 ARP cache, DENY
src HW = <50:e5:49:f7:a:93>
src IP = <192.168.1.120>
21:53:15 ARP cache, ACCEPT
src HW = <50:e5:49:f7:7:ba>
src IP = <192.168.1.120>
21:53:17 ARP cache, DENY
src HW = <50:e5:49:f7:a:93>
src IP = <192.168.1.120>
21:53:17 ARP cache, ACCEPT
src HW = <50:e5:49:f7:7:ba>
```

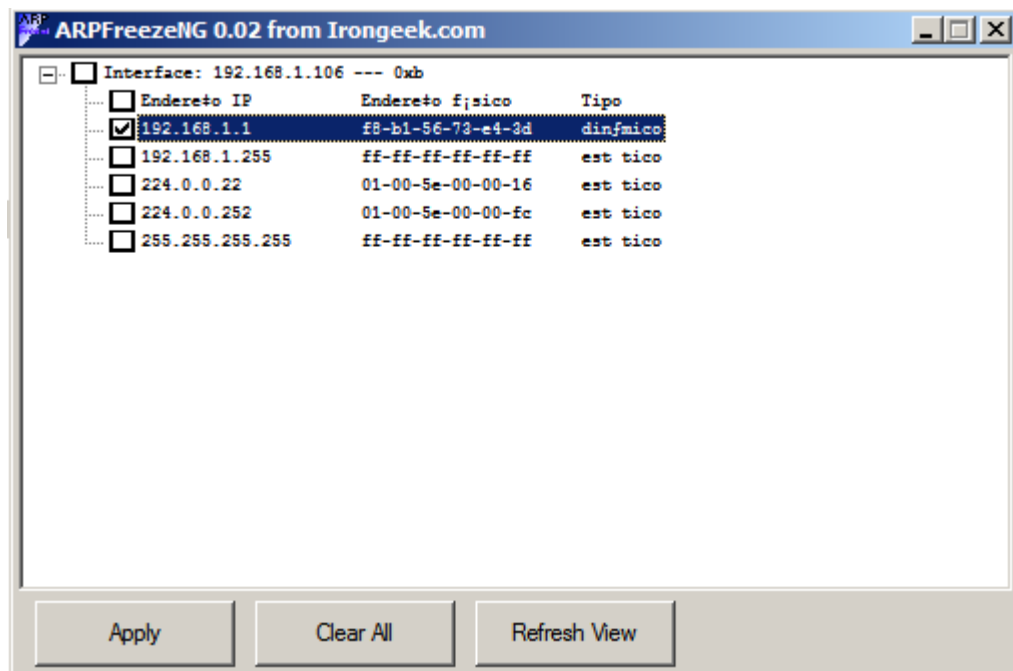


### 5.3. Configuração ArpFreezeNG

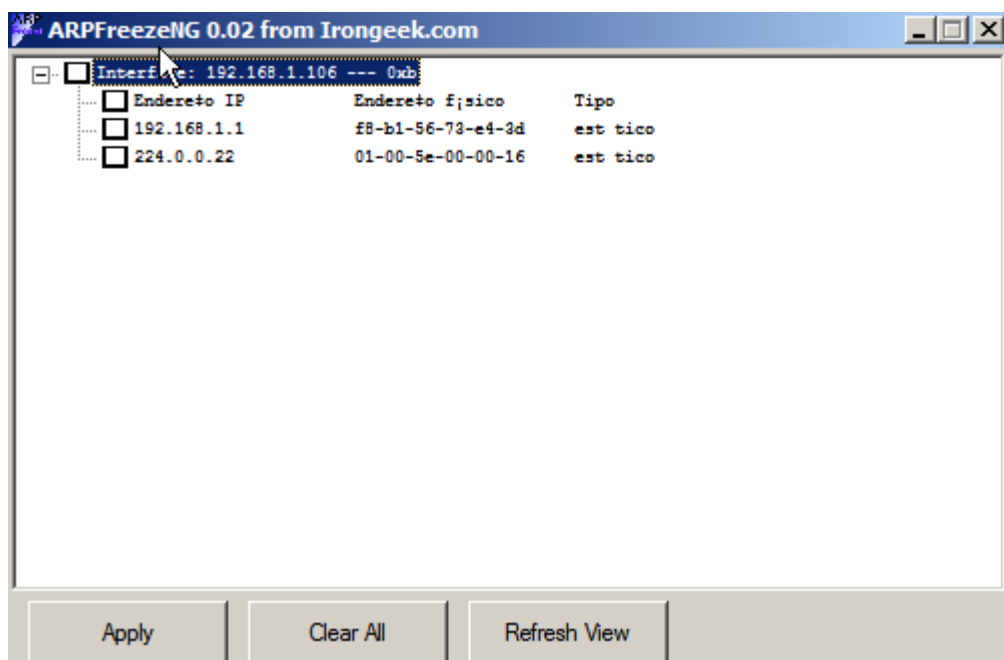
A utilização do ArpFreezeNG pode ser feita tanto em servidores como em clientes, a utilização desta ferramenta é simples, baixe-a no site oficial

<<http://www.irongeek.com/i.php?page=security/arpfreeze-static-arp-poisoning>>

depois descompacte-a e execute.

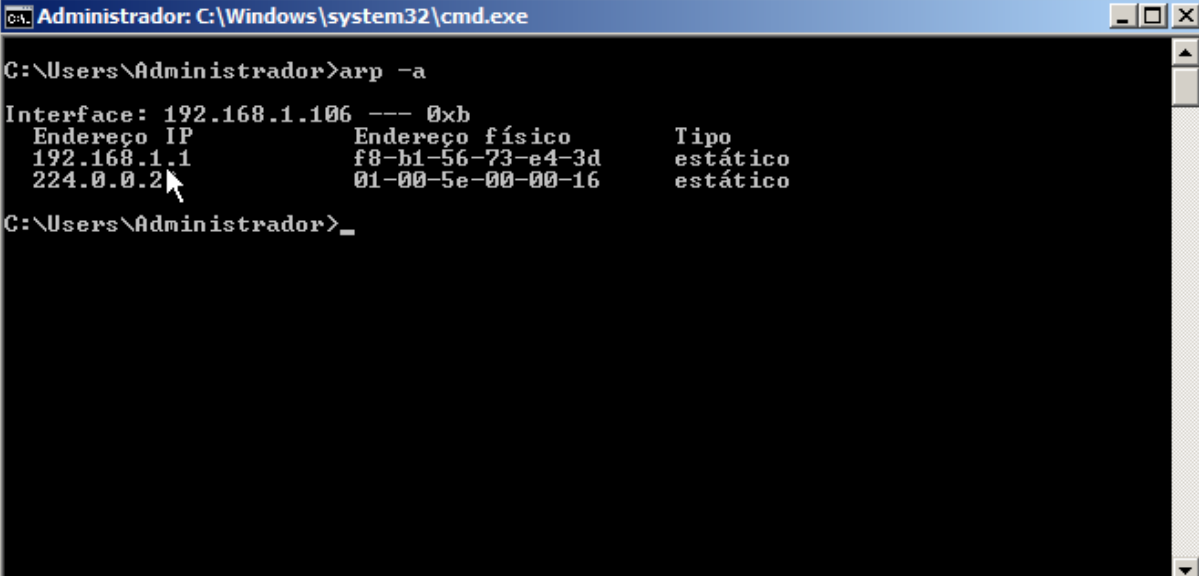


Essa é a tela do ArpFreeze, basta marcar a caixa do IP que deseja mudar para estático e clicarem Apply.



Após isso a ferramenta mostra suas mudanças e pronto você já está com seus endereços configurados de forma estática.

Caso queira conferir abra o prompt de comando e digite arp -a



```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>arp -a

Interface: 192.168.1.106 --- 0xb
Endereço IP      Endereço físico      Tipo
192.168.1.1      f8-b1-56-73-e4-3d    estático
224.0.0.2        01-00-5e-00-00-16    estático

C:\Users\Administrador>_
```