GTER 32

GTS 18

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de Vulnerabilidades no Protocolo SIP com o Uso de Softwares Livres

Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardo.galvao@ifrn.edu.br
www.twitter.com/ricardokleber

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
1909-2009

Grupo de Pesquisa no IFRN

Pesquisas em Andamento...

Grupo de Pesquisa em

Segurança da Informação e Software Livre

SEGURANÇA DE REDES

www.segurancaderedes.org

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Foco da Apresentação

- Visão Geral do SIP
- Principais Problemas de Segurança no Uso do SIP
- Contramedidas/Soluções
- Ferramentas (FOSS) para Análise de Vulnerabilidades no SIP

Foco da Apresentação

Layer	Call Process.	User Audio or Video	User Data	Support	Routing	Signal Transport
5	H.323 Megaco MGCP SIP	RTP	T.120	RTCP RTSP NTP SDP	ENUM TRIP	SIGTRAN†
4	TCP UDP	UDP	TCP	TCP UDP		SCTP
3	IP, RSVP, and IGMP					

Voip / SIP

Por que SIP?

Protocolo de Sinalização e Controle

mais utilizado em Sistemas VoIP

SIP :: Session Initialization Protocol

Histórico

- Desenvolvido em meados da década de 90
  IETF (Internet Engineering Task Force) MMUSIC Working Group;
- **1996:** primeira versão do SIP(SIPv1);
- **1997:** segunda versão do SIP(Mescla do SIPv1 e o SCIP);
- **1999:** relatório técnico RFC2543 (Request For Comments): SIP como padrão (IETF);
- **2000:** aceito como 3GPP (3rd Generation Partnership Project) e elemento permanente da arquitetura IMS (IP Multimedia Subsystem);
- **2002:** RFC3261: consolidada a arquitetura, estrutura, organização e métodos do SIP.

SIP :: Session Initialization Protocol

Visão Geral do Protocolo (Serviços Oferecidos)

- *Localização do usuário;*
- *Disponibilidade do usuário;*
- *Recursos do usuário;*
- *Características da negociação;*
- *Gestão da sessão;*
- *Modificar sessão*

SIP :: Session Initialization Protocol

Elementos (Arquitetura)

- *SIP User Agents;*
- *SIP Proxy Servers;*
- *SIP Redirect Server;*
- *SIP Registrar Server.*

SIP :: Session Initialization Protocol

Métodos

- *Register – usado para registra o usuário*
- *Invite – convidar alguém para uma sessão*
- *Ack – confirmação de uma requisição de estabelecimento de sessão*
- *Cancel – cancelamento de uma transação*
- *Bye – encerramento de uma sessão ou transação*
- *Options – Consulta de compatibilidades*
- *Info – usado para troca de informações intermediárias como dígitos discados*
- *Messages – usado para mensagens curtas de serviço e mensagem instantânea*
- *Notify – usado para notificar eventos e atualização de registro*
- *Subscribe – usado para a subscrição de notificação de eventos*
- *Update – usado para atualização das informações de uma sessão*

SIP :: Session Initialization Protocol

Códigos de Resposta (Classes Principais):

- *1xx*
- *2xx*
- *3xx*
- *4xx*
- *5xx*
- *6xx*

Derivadas do HTTP

SIP :: Session Initialization Protocol

Cabeçalhos (principais)

- *Call-ID(i)*

  Ex.: `i:34d93422afdd5676@200.1.2.3`

- *From(f)*

  Ex.: `From:<sip:ricardo.kleber@meupbx.com>`

- *Date*

  Ex.: `Date: Fri, 11 Jun 2011 22:15:00 GMT`

- *Cseq*

  Ex.: `CSeq: 3 OPTIONS`

- *Proxy-Authorization*

SIP :: Session Initialization Protocol

Endereçamento

- *Cada usuário possui uma URI (Uniform Resource Identifier)*
- *Formato:* `<sip://usuario@servidor>;`
- *URI's endereçam recursos dentro de uma rede;*
- *SIP utiliza Three-way Handshake para estabelecer uma sessão.*

http://www.3com.com/voip/assets/sip.jpg

Interrupção e Abuso de Serviço

Ameaças que Afetam a disponibilidade do serviço

- *SIP Flooding*
  - Inundação de mensagens INVITE enviadas a um usuário SIP
    - Degradação de desempenho de SIP Proxies
    - Impedimento de efetuar ligações (usuário atacado)
- *SIP Signalling Loop*
  - Registro de dois usuários em domínios SIP distintos
  - Com dois valores cabeçalho de contato
  - Cada um apontando para o usuário no domínio contrário
  - SIP Proxy recebe INVITE e gera duas mensagens INVITE
  - O outro SIP Proxy recebe 2 e envia 4...
  - Número de mensagens cresce exponencialmente

Interrupção e Abuso de Serviço

Ameaças que Afetam a disponibilidade do serviço

- *VoIP Packet Replay Attack*
  - Captura e reenvio de pacotes VoIP fora de sequência
  - Geração de atraso e progressiva degradação de qualidade das chamadas
- *QoS Modification Attack*
  - Modificação dos campos referentes a QoS (VLAN Tags ou ToS bits)
  - Anula o controle de QoS na rede (comprometendo o serviço)
- *VoIP Packet Injection*
  - Envio de pacotes VoIP falsificados para terminais
  - Injeção de sons (falas, ruídos, lacunas) nas chamadas ativas.

Violação de Acesso

Ameaças em que serviços e elementos da rede são acessados sem a devida permissão

- *Métodos Utilizados*
  - **Impersonificação**
    - Descoberta ou roubo de senha e uso para acesso
  - **Ataque "man-in-the-middle"**
    - Interceptação de sessão válida e apropriação após a autenticação
  - **Comprometimento Total**
    - Acesso total ao sistema por comprometimento via métodos tradicionais

Violação de Acesso

Ameaças em que serviços e elementos da rede são acessados sem a devida permissão

- *Ataque de Dicionário na Autenticação SIP*
  - Ataque "força bruta" p/ obtenção de credenciais de acesso de usuário válido
  - Envio de várias requisições de registro (método REGISTER do SIP) com Identificadores (ID) e senhas sugestivas (utilizadas a partir de um "dicionário")
- *Escuta e Análise de Tráfego*
  - Ameaças que afetam a confidencialidade do serviço
  - Utilização de escutas (sniffers) para captura específica e análise posterior
  - Monitoramento da sinalização e tráfego (sem alteração) e ataque off-line
  - Necessidade de posicionamento "estratégico" da escuta
    - ARP Poisoning, VLAN hopping, ...

Violação de Acesso

Ameaças em que serviços e elementos da rede são acessados sem a devida permissão

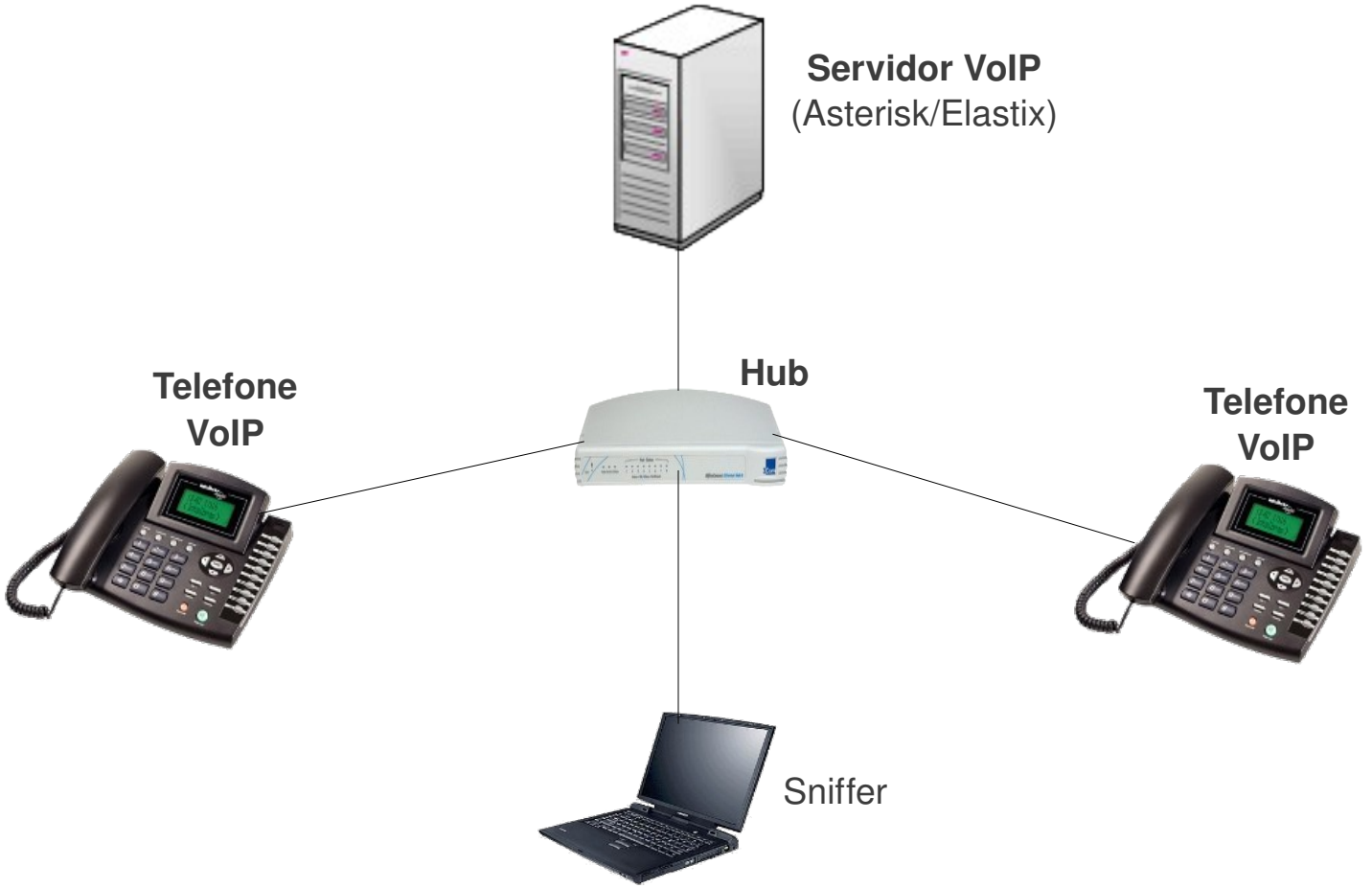
- *Mascaramento*
  - Técnica também utilizada como complemento de outras (como violação de acesso, interrupção dos serviços e fraudes)
  - Atacante se faz passar por usuário, dispositivo, serviço e/ou aplicação
  - Além da tentativa de manipulação de mensagens de sinalização, também são exemplos destas ameaças clonagem de IPs e MACs e IP Spoofing.
    - Ex.: Sequestro de Chamada
      - Alteração do CONTACT no cabeçalho da requisição REGISTER
      - Alteração do IP contido neste registro
      - Desvio do encaminhamento das ligações para outro dispositivo

Recomendações

- *Uso de VLANs para Rede VoIP*
- *Uso de Firewall, IDS e IPs (identificação e bloqueio de ataques)*
- *Uso de QoS (identificação e priorização de tráfego VoIP)*
- *Segurança na Sinalização (SIP)*
  - *Autenticação nos métodos REGISTER e INVITE (que é opcional)*
    - *Utilização do MD5 não disponível para métodos BYE e CANCEL*
  - *Melhor solução: Uso de criptografia para todas as Mensagens de identificação* **(TLS, IPSec e S/MIME)**.

Apresentando... Ferramentas FOSS

Cenário (Laboratório)



Apresentando... Ferramentas FOSS

Capturando e Analisando (Grampo SIP for Dummies)

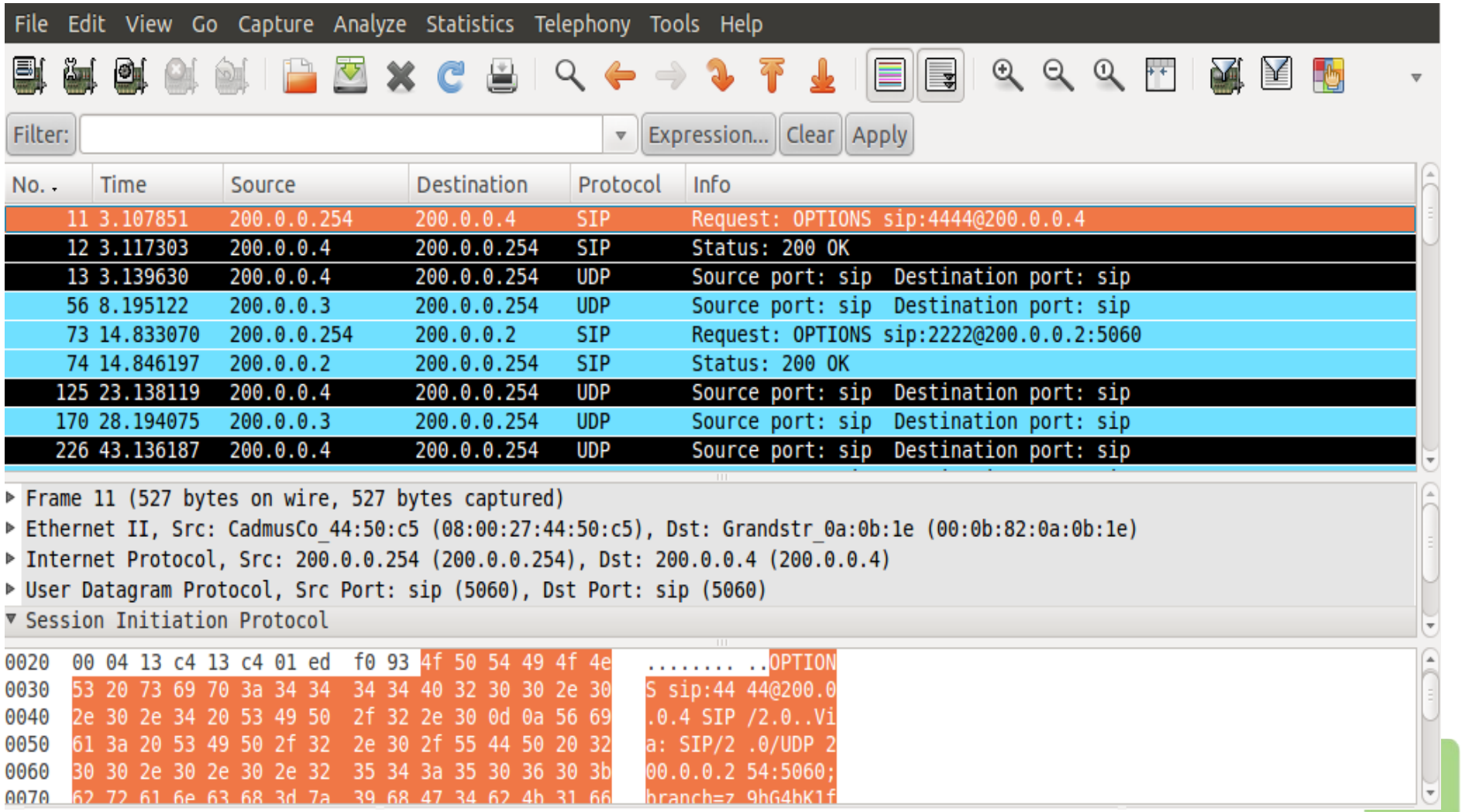
- **Grampeando a porta 5060/UDP c/Tcpdump**

```
# tcpdump -vvv udp port 5060 -w 5060udp.pcap
```

- **Analisando com Wireshark**
  - *Abrir arquivo pcap no Wireshark*
  - *Analisar protocolo SIP (filter sip)*
  - *Verificar Cabeçalhos de Sinalização SIP (Follow UDP Stream)*
  - *Separar e Analisar Chamdas (Telephony / VoipCalls)*

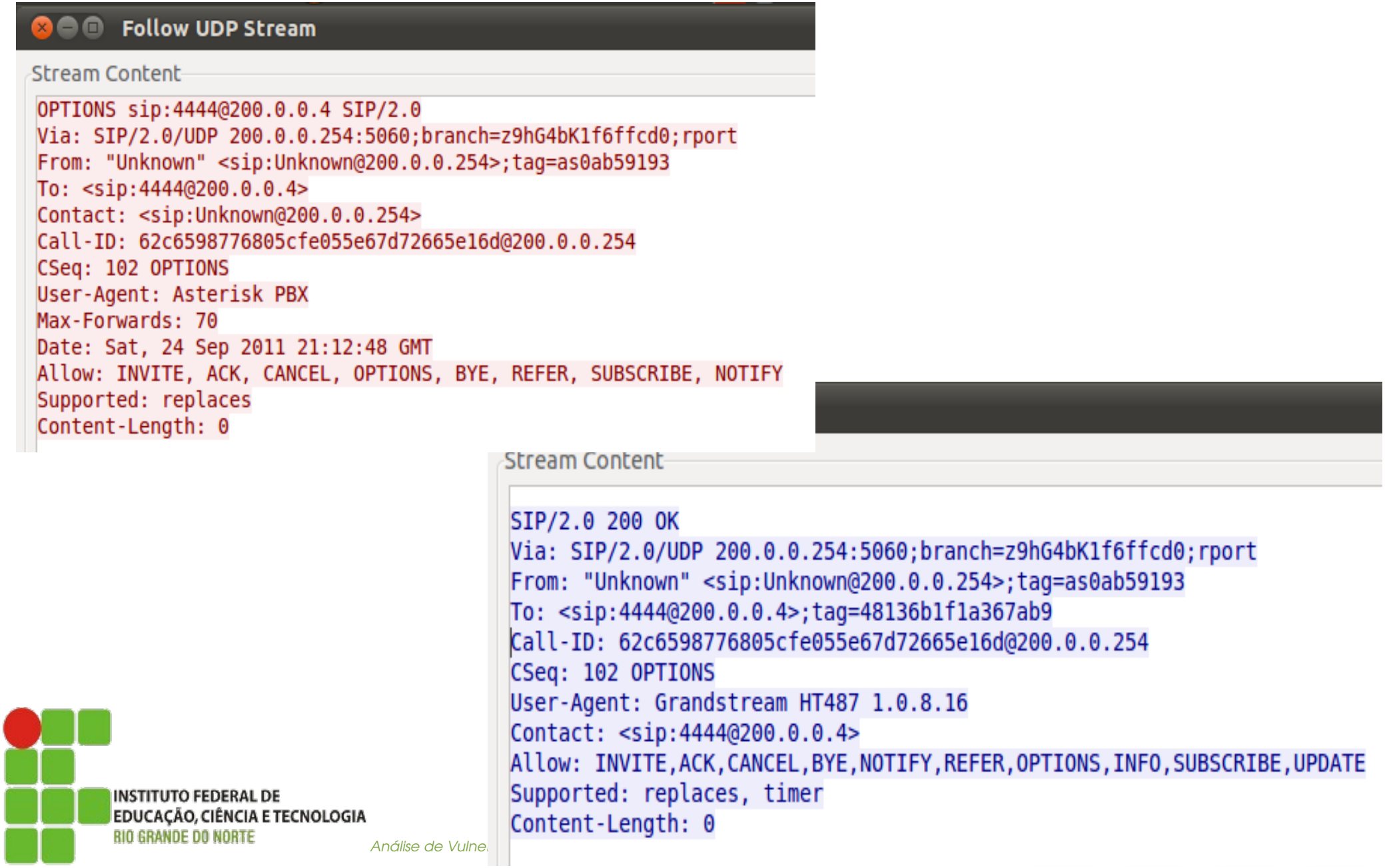
Apresentando... Ferramentas FOSS

Analisando Tráfego SIP com Wireshark



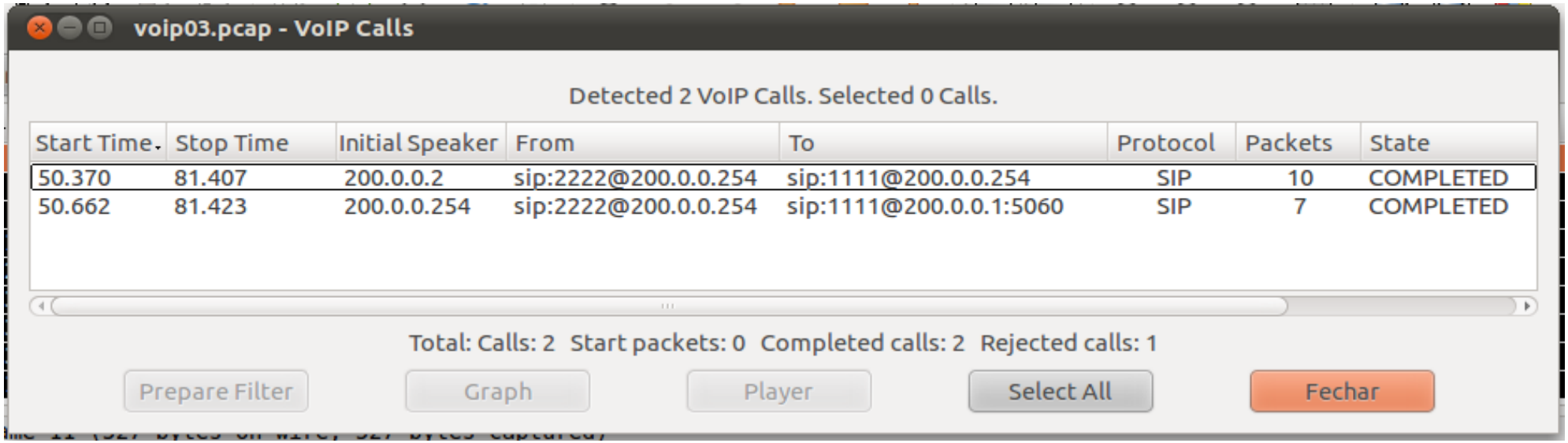
Apresentando... Ferramentas FOSS

Analisando Tráfego SIP com Wireshark



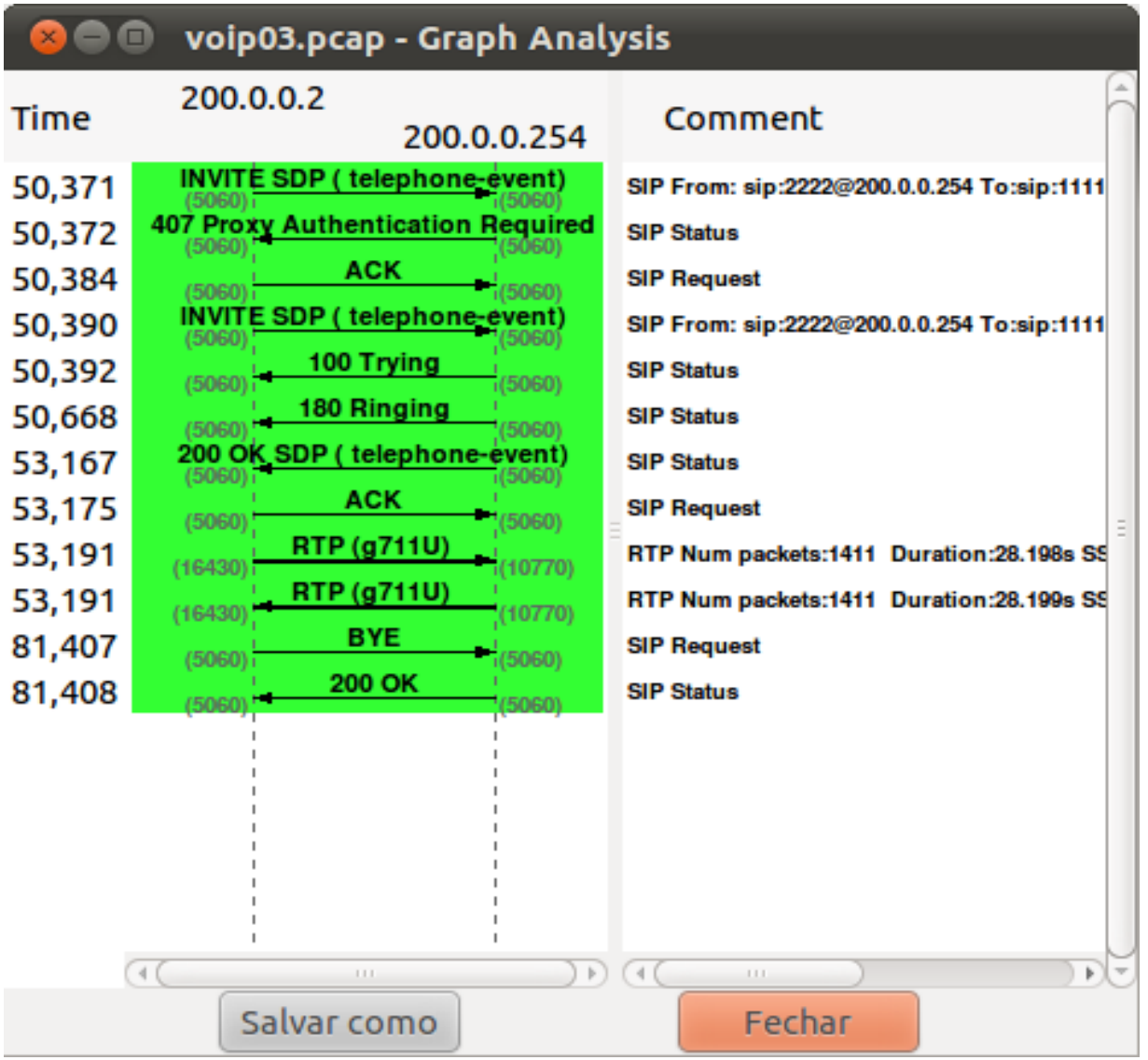
Apresentando... Ferramentas FOSS

Analisando Tráfego SIP com Wireshark



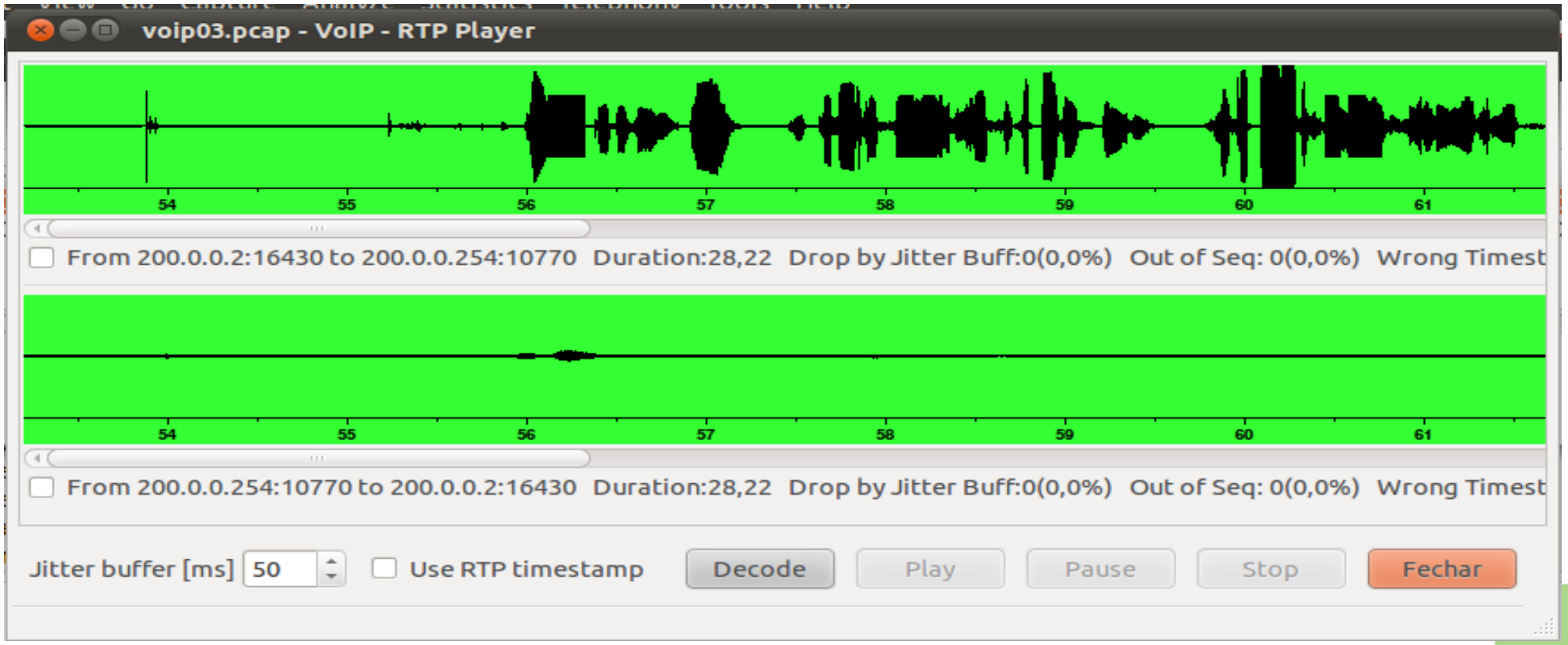
Apresentando... Ferramentas FOSS

Analisando Tráfego SIP com Wireshark



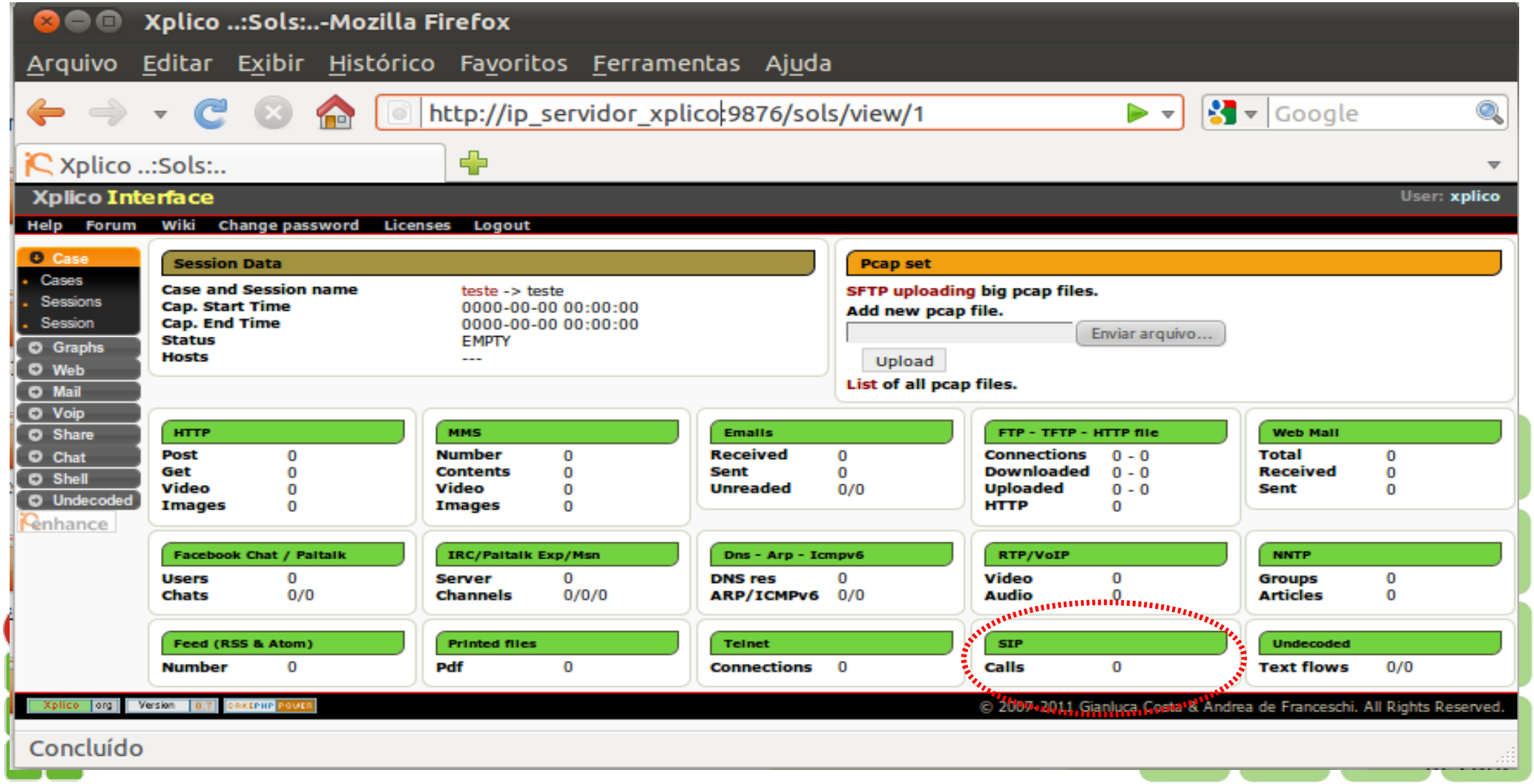
Apresentando... Ferramentas FOSS

Analisando (Além do) Tráfego SIP com Wireshark



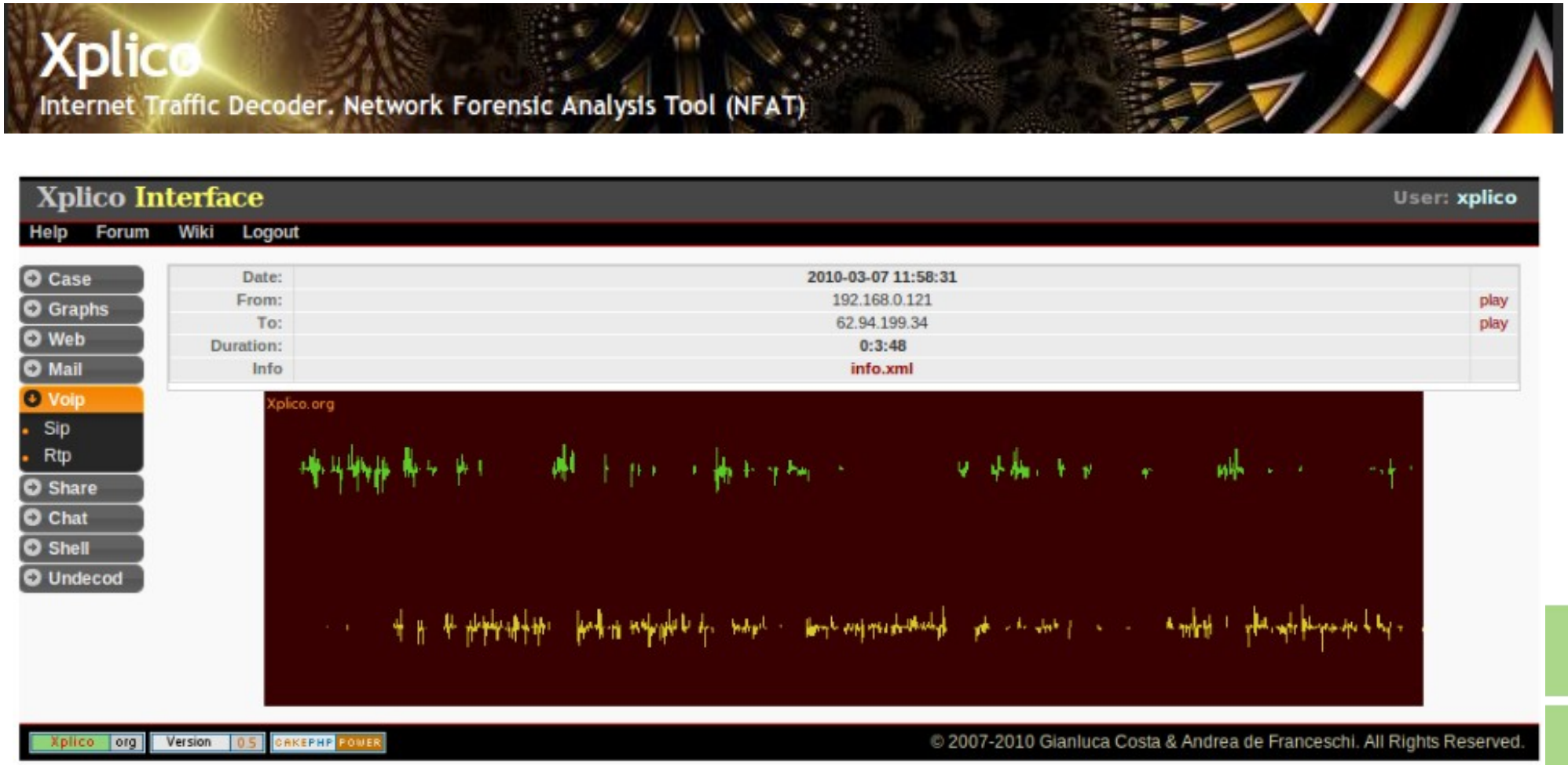
Apresentando... Ferramentas FOSS

Xplico (www.xplico.org)



Apresentando... Ferramentas FOSS

Xplico (www.xplico.org)



(Tentativa de) Quebra de Senha de Autenticação SIP
Ferramentas FOSS

- **Sipcrack**
  - No Linux/Ubuntu: apt-get install sipcrack
    - Sipdump :: Captura tráfego durante processo de autenticação
      - `sipdump -i interface arquivo.pcap`
    - Sipcrack :: Tenta quebrar senha de Autenticação SIP (Algoritmo MD5)
      - `sipcrack -s arquivo.pcap` :: Utiliza dicionário padrão
      - `sipcrack -w dicionario.txt arquivo.pcap` :: Utiliza dicionário específico

(Tentativa de) Quebra de Senha de Autenticação SIP
Ferramentas FOSS

- **Sipcrack**

```
192.168.4.41"192.168.4.21"5002"asterisk"REGISTER"sip:192.168.4.21"587d1987""""MD5"543ac5000fb278d4398fa42da13bcf6c
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"1e7e4a08""""MD5"b47ed58c11c75ff905f6b766a68081a4
192.168.2.1"192.168.2.21"5001"asterisk"INVITE"sip:5001@192.168.2.21"37e31a74""""MD5"523ab0ce1c8243ed88405477f0a837d2
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"36abdf3d""""MD5"72b35deaea4a6cc18d3d57e19bb29fd9
192.168.4.41"192.168.4.21"5002"asterisk"REGISTER"sip:192.168.4.21"297c757d""""MD5"b6e1eb90f40958a7a6ab617eb2cf825a
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"385ac36e""""MD5"f73c2cfe861b1e44e000667bb93ca3f4
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"3a464653""""MD5"1e61d0369e6fd944d850fd3a0c589b4f
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"64730a5e""""MD5"ae523f0da4d20a8b78b36580fc497fe7
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"1071bac1""""MD5"f9930d8d9f84a1b587ef9a1c8d426f4f
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"174384e5""""MD5"46aeedb459b625ed14d4ac92f0bff0fc
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"0f079b31""""MD5"65de0720b1b43380de47b6f6f5a1e056
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"4ebb979f""""MD5"d2856016f1803b0a4a4333af7abfc0c1
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"789f8521""""MD5"9cde6bdd76c48c5a5883e8795e3b79b6
192.168.1.13"192.168.1.21"5001"asterisk"REGISTER"sip:192.168.1.21"33f0fcc6""""MD5"7a4c09c1fc935ab58b4be0dd06b23f98
192.168.1.13"192.168.1.21"5001"asterisk"REGISTER"sip:192.168.1.21"6f1d51db""""MD5"570aea21cf85d76c46db0c6d4d520e5f
192.168.1.13"192.168.1.21"5001"asterisk"REGISTER"sip:192.168.1.21"18b8cd9a""""MD5"adb04604c6d802a80d9ebe613b0e0158
192.168.2.1"192.168.2.21"5001"asterisk"INVITE"sip:5001@192.168.2.21"46bd1b79""""MD5"f7939ddebcdc9b1340bd96f062bccea8
```

(Tentativa de) Quebra de Senha de Autenticação SIP
Ferramentas FOSS

- **Sipcrack**

```
192.168.4.41"192.168.4.21"5002"asterisk"REGISTER"sip:192.168.4.21"587d1987""""PLAIN"5002
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"1e7e4a08""""PLAIN"5002
192.168.2.1"192.168.2.21"5001"asterisk"INVITE"sip:5001@192.168.2.21"37e31a74""""PLAIN"5001
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"36abdf3d""""PLAIN"meusegredo
192.168.4.41"192.168.4.21"5002"asterisk"REGISTER"sip:192.168.4.21"297c757d""""PLAIN"5002
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"385ac36e""""PLAIN"meusegredo
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"3a464653""""PLAIN"meusegredo
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"64730a5e""""PLAIN"meusegredo
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"1071bac1""""PLAIN"5002
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"174384e5""""PLAIN"5002
192.168.1.13"192.168.1.20"5001"asterisk"REGISTER"sip:192.168.1.20"0f079b31""""PLAIN"meusegredo
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"4ebb979f""""PLAIN"5002
192.168.5.41"192.168.5.21"5002"asterisk"REGISTER"sip:192.168.5.21"789f8521""""PLAIN"5002
192.168.1.13"192.168.1.21"5001"asterisk"REGISTER"sip:192.168.1.21"33f0fcc6""""PLAIN"meusegredo
192.168.1.13"192.168.1.21"5001"asterisk"REGISTER"sip:192.168.1.21"6f1d51db""""PLAIN"meusegredo
192.168.1.13"192.168.1.21"5001"asterisk"REGISTER"sip:192.168.1.21"18b8cd9a""""PLAIN"meusegredo
192.168.2.1"192.168.2.21"5001"asterisk"INVITE"sip:5001@192.168.2.21"46bd1b79""""PLAIN"5001
```

(Tentativa de) Quebra de Senha de Autenticação SIP
Ferramentas FOSS

- **Quebrando "no braço"**
  - Composição do Hash MD5 do Cabeçalho
    - **`Hash = MD5(MD5(USER:REALM:PASSWORD):NONCE:MD5(METHOD:URI)`**
    - Exemplo:
      - USER = 1111
      - REALM = asterisk
      - PASSWORD = Aqui entra o dicionário
      - NONCE = 1c305a2f
      - METHOD = REGISTER
      - URI = sip:200.1.2.3

Thanks: André Landim / Fred Costa (CAIS/RNP)

(Tentativa de) Quebra de Senha de Autenticação SIP
Ferramentas FOSS

- **O que temos no BackTrack (5) ?**
  - SIPSAK :: Levantamento de Informações
    - Também disponível no repositório APT do Debian/Ubuntu
  - SMAP :: Injetor de requisições SIP para alvo específico
  - SIPVicious :: Conjunto de Scripts em Python
    - SVMAP :: Levantamento de Informações
    - SVWAR :: Identificação de extensões ativas
    - SVCRACK :: Ataques de força bruta
    - SVREPORT :: Relatórios do SVMAP

Captura e Análise de Tráfego VoIP (RTP)

Ferramentas FOSS (complementares)

- **VOMIT (Voice Over Misconfigured Internet Telephones)**
  (http://vomit.xtdnet.nl/)
  - Tráfego capturado com o Sniffer (padrão tcpdump)
  - Conversão para arquivo wave com o VOMIT
  - Reprodução em qualquer player
  - Somente para tráfego não encriptado (misconfigured)
  - Trabalha somente com **G.711** (padrão utilizado por telefones IP Cisco e Microsoft® Netmeeting)

```
vomit -r trafego.dump | waveplay -S8000 -B16 -C1
```

Captura e Análise de Tráfego VoIP (RTP)
Ferramentas FOSS (complementares)

- **Voipong (http://www.enderunix.org/voipong)**
  - Escrito em C
  - Detecta e captura tráfego VoIP e separa em arquivos WAV distintos

```
estacaopericial# ./voipctl
Connected to VoIPong Management Console
System: efe.enderunix.org

voipong> help
Commands:
help                    : this one
quit                    : quit management console
uptime                  : Server uptime
logrotate               : rotate server's logs
shutdown                : shutdown server
rusage                  : CPU usage statistics for the server
loadnets                : Reload voipongnets file
info                    : General server information
shcall                  : Show currently monitored calls
shrtcp                  : Show currently RTCP cache
killcall [id]           : end monitoring session with [id]
```

Perguntas

GTER 32

GTS 18

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de Vulnerabilidades no Protocolo SIP com o Uso de Softwares Livres

Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardo.galvao@ifrn.edu.br
www.twitter.com/ricardokleber

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
1909-2009