

# Özgür Yazılımlar ile VoIP Denetimi

Fatih Özavcı

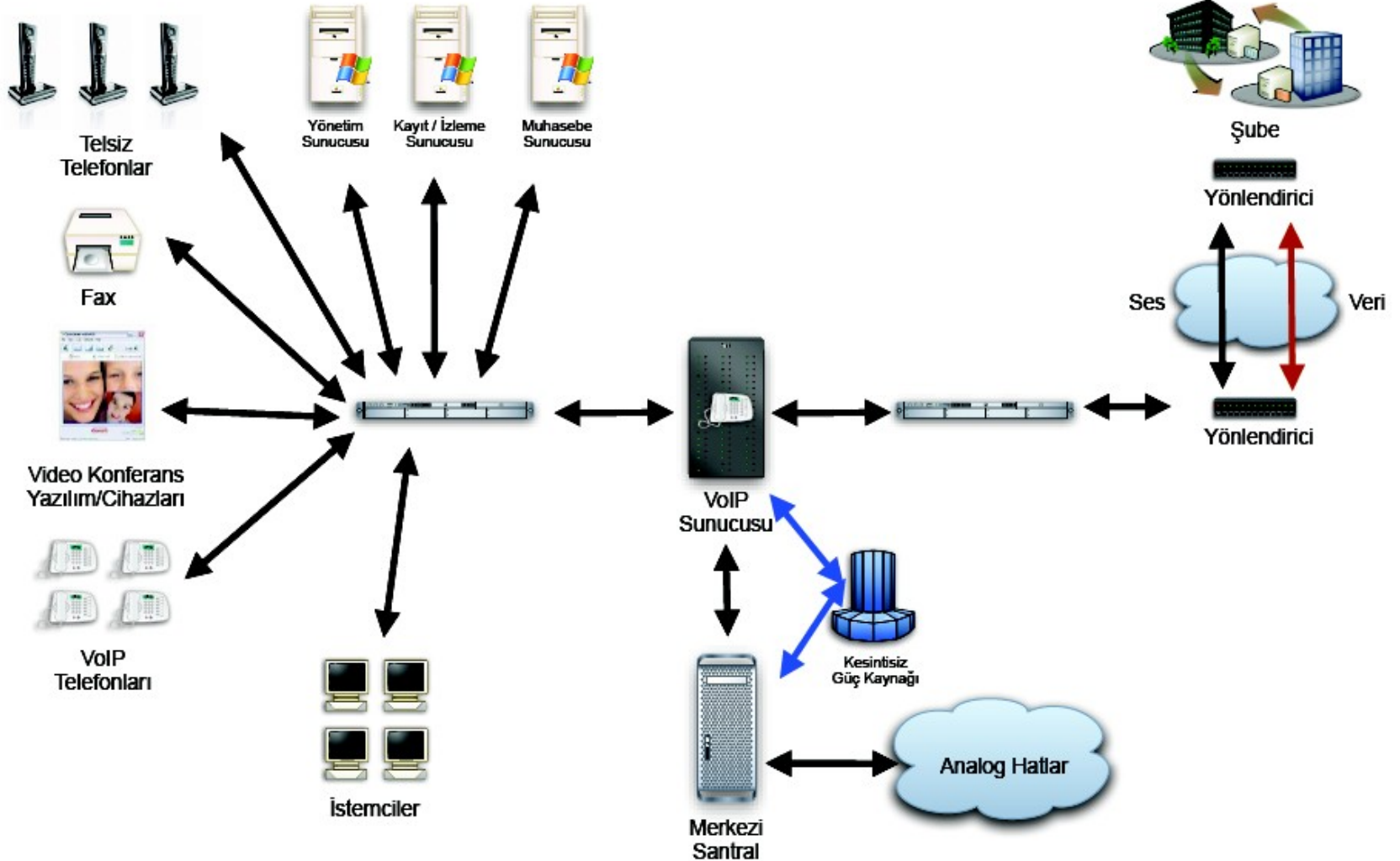
Bilgi Güvenliği Danışmanı

[fatih.ozavci@gamasec.net](mailto:fatih.ozavci@gamasec.net)

- VoIP Güvenliđi
- VoIP Güvenlik Denetim Süreci
  - Denetim Kapsamının Belirlenmesi
  - Ağ Altyapısı Analizi
  - SIP Sunucuları Analizi
    - Kimlik Doğrulama ve Yetkilendirme
    - Programlama Sorunları
    - Ek Uzantılar ve Özel İşlemler
  - SIP İstemcileri Analizi
- Denetim Sürecinde Kullanılabilecek Araçlar
  - Araçlar ve Özellikleri
  - Kullanım Amaçları

- Kurumlar ucuz iç haberleşme amacıyla veri ağları üzerinden ses iletişimini aktarmaya ihtiyaç duymaktadır
  - VoIP, Veri Ağlarından Ses İletişiminin Genel Adıdır
  - SIP, H.323, IAX
  - Analog Telefon Hatları ile Beraber Çalışmaları Gereklidir
- VoIP Yapılarında Güvenlik Sorunları
  - Kimlik doğrulama ve yetki sorunları
  - Servis engelleme
  - Ortadaki adam saldırısı
  - Çağrı yakalama, yönlendirme
  - IP/Çağrı sahteciliği
  - Tekrarlama saldırısı

# VoIP Denetim Süreci



# VoIP Denetim Süreci (SIP Odaklı)



- Denetim kuruma/sisteme/yazılıma özel olmalıdır, bu nedenle her bir testin özelleştirilmesi gerekmektedir
- Farklı denetim adımlarında alınan çıktıların birleştirilmesi ve beraber değerlendirilmesi gerekmektedir
- Bazı özel testlerin tanımlanabilmesi, kullanılacak test şekillerinin döngülere sokulabilmesi gerekmektedir
- Basit, hızlı ve amaca hizmet eden yazılımlar denetim sürecinin verimini arttırmaktadır
- Kaynak kodu açık, yapılan işlemin net olarak görülebileceği araçlar tercih edilmelidir
- Özgür yazılımlar genellikle bu şartları veya fazlasını sunmaktadır

- Denetim bilgilerinde verilenler her zaman yeterli değildir
  - Sunucular (SIP, SIP Proxy, RTP Proxy)
  - İstemciler (Yazılım, Özel Donanım)
  - Ağ Altyapısının Yerleşimi
- Denetim Öncesi Gerekli Bilgiler
  - Donanım ve Yazılımların Türü, Sürümü
  - Seçilen Protokoller ve Seçenekler
  - Yönetim veya Destek Amaçlı Servisler
  - SSL/TLS Kullanımı
- Araçlar
  - Sipvicious, Sipsak, Sip Forum Testing Framework, Nmap, OpenVAS, Metasploit Framework, Wireshark, Ettercap, Netcat

## Sipvicious

- <http://sipvicious.org>
- Python temelli, çok sayıda platformda çalışabilir
- Modüller
  - Svmap – SIP Servislerini Doğrulama ve Sürüm Bilgisi Alma
  - Svcrack – Kullanıcı/Şifre Doğrulaması
  - Svwar – SIP Servisindeki Uzantıların Doğrulanması
  - Svreport – SIP Analizleri Sonucunda Rapor Oluşturma
  - Svlearn – SIP Servisi Parmak İzinin Öğretilmesi ve Kaydedilmesi
- Haritalama ve bilgi toplama için elverişlidir, ancak servis analizlerinde kullanılamamaktadır
- Servis parmak izi veritabanı oldukça geniş ve kalitelidir
- Uzanti ve kullanıcı analizleri yapabilmektedir
- Araçların seçenekleri çok geniştir, analiz esnek yapılabilmektedir

## Sipsak

- <http://sipsak.org>
- Linux/Unix/Windows'ta Çalışabilmektedir
- Haritalama ve bilgi toplama için elverişlidir, ayrıca özel analizler veya ham iletişimlerin kullanımını desteklemektedir
- SIP isteği ham olarak hazırlanıp doğrudan girdi olarak verilebilmektedir
- Kullanım Amaçları
  - SIP Servislerinin Keşfi
  - Kullanıcı / Şifre Denemeleri
  - Çağrı Yönlendirme
  - Uzantıların Analizi
  - Özel Zaafiyet Analizleri

## Nmap

- <http://insecure.org/nmap>
- Linux/Unix/Windows'ta Çalışabilmektedir
- Haritalama ve bilgi toplama için elverişlidir

## Metasploit Framework

- <http://www.metasploit.org>
- Linux/Unix/Windows'ta Çalışabilmektedir
- Yardımcı modüller arasında SIP servisi arama ve uzantı analizi yer almaktadır, Exploit'lerde ise sipXphone açığı bulunmaktadır

## OpenVAS

- <http://www.openvas.org>
- Linux/Unix'lerde Çalışabilmektedir
- Otomatize zaafiyet eklentilerinde SIP analizleri de bulunmaktadır

## Sipvicious

```
# ./svmap.py 192.168.2.0/24
| SIP Device      |User Agent| Fingerprint          |
|192.168.2.97:5060|unknown  |3CXPhoneSystem/AVM FRITZ!Box Fon WLAN 7170 29.04.22|
|                |          |6 2006) / T-Com Speedport W500V / Firmware v1.37 |
|                |          |MxSF/v3.2.6.26      |
|192.168.2.105:5060|LRSTD XTP8886 2008.06.05|T-Com Speedport W500V / Firmware v1.37
MxSF/v3.2.6.26 |
| 192.168.2.104:5060 | Nortel IP Phone 1535 (0.291.0616) | T-Com Speedport W500V / Firmware
v1.37 MxSF/v3.2.6.26 |
```

## Sipsak

```
# sipsak -s sip:1000@192.168.2.1 -vv
```

message received:

SIP/2.0 200 OK

To: <sip:1000@192.168.2.1>;tag=472a8800

From: <sip:sipsak@127.0.11:45431>;tag=2dc0184a

Via: SIP/2.0/UDP

127.0.11:45431;branch=z9hweveG4bK65f08cbb;rport=45431;received=94.122.9.4.49;alias

Call-ID: 767563850@127.0.11

CSeq: 1 OPTIONS

Contact: <sip:192.168.2.1:5060>

Content-Length: 0

\*\* reply received after 38.297 ms \*\*

SIP/2.0 200 OK

final received

## ➤ SIP Yapısının Yerleşim Analizi

- Ses ve Veri Ağı Ayırıştırması
- SIP Sunucusunun Servislerine Erişim Hakları
- Destek Servislerinin Konumları
  - DHCP, DNS, TFTP
- SSL/TLS Kullanımı

## ➤ İletişim Analizi

- SIP İstek ve Cevapları Analizi
- Ortadaki Adam Saldırıları ve Proxy Kullanımı
- Çağrı Yakalama, Çözümleme ve Yönlendirme
- Ağ Temelli Servis Engelleme

## ➤ Araçlar

- Ucsniff, Voipong, RTPBreak, VNAK, Wireshark, Ettercap, Nmap

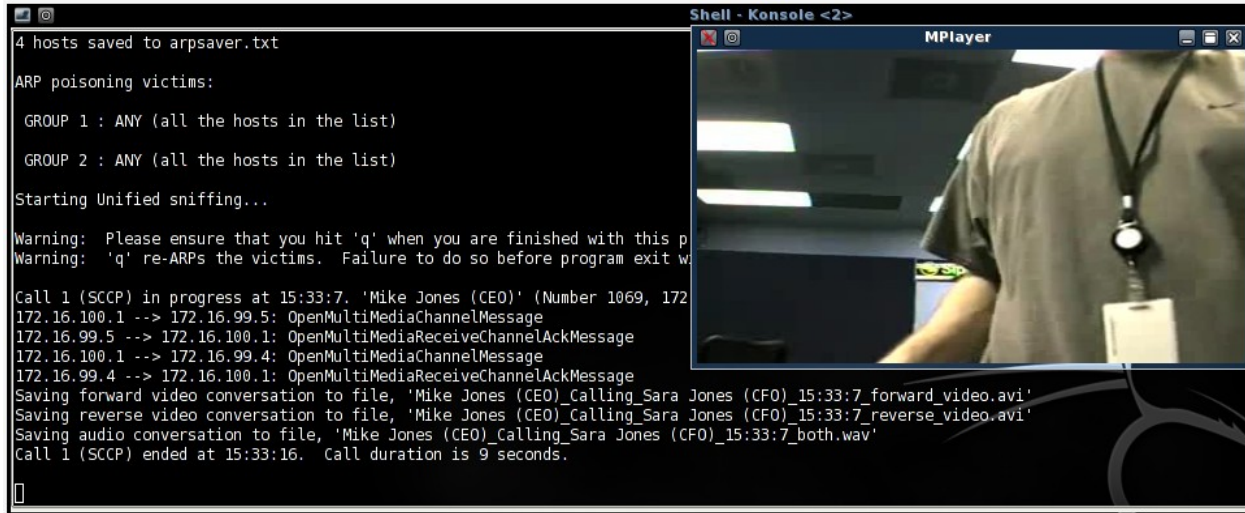
## Ucsniff

- <http://ucsniff.sourceforge.net>
- Linux/Unix'lerde Çalışabilmektedir
- Ağda paket yakalama ve iletişimi çözümleme için kullanılır
- Kullanım Amaçları
  - ARP Analizleri, VLAN Atlamaları ve Analizleri
  - RTP Ayıklama ve Kayıt Etme
  - Çağrı Kaydı ve Çözümleme (Video: H.264, Ses: G-711 ve G.722)
  - SIP, Skinny Desteği

## Voipong

- <http://www.enderunix.org/voipong>
- Linux/Unix'lerde Çalışabilmektedir
- Ağda paket yakalama ve iletişimi çözümleme için kullanılır

## Ucsniff



```
4 hosts saved to arpsaver.txt
ARP poisoning victims:
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
Warning: Please ensure that you hit 'q' when you are finished with this p
Warning: 'q' re-ARPs the victims. Failure to do so before program exit w

Call 1 (SCCP) in progress at 15:33:7. 'Mike Jones (CEO)' (Number 1069, 172
172.16.100.1 --> 172.16.99.5: OpenMultiMediaChannelMessage
172.16.99.5 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
172.16.100.1 --> 172.16.99.4: OpenMultiMediaChannelMessage
172.16.99.4 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
Saving forward video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_forward_video.avi'
Saving reverse video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_reverse_video.avi'
Saving audio conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_both.wav'
Call 1 (SCCP) ended at 15:33:16. Call duration is 9 seconds.
```

## Voipong

```
efer:[voipong]# voipong -d4 -f
EnderUNIX VOIPONG Voice Over IP Sniffer starting...
Release 2.0-DEVEL, running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE #0: Thu Dec i386]

(c) Murat Balaban http://www.enderunix.org/
19/11/04 13:32:10: EnderUNIX VOIPONG Voice Over IP Sniffer starting...
19/11/04 13:32:10: Release 2.0-DEVEL running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE
19/11/04 13:32:10: fxp0 has been opened in promisc mode, data link: 14 (192.168.0.0/255.255.255.248)
19/11/04 13:32:10: [8434] VoIP call detected.
19/11/04 13:32:10: [8434] 10.0.0.49:49606 <-> 10.0.0.90:49604
19/11/04 13:32:10: [8434] Encoding: 0-PCMU-8KHz
19/11/04 13:38:37: [8434] maximum waiting time [10 sn] elapsed for this call, call might have been ended.
19/11/04 13:38:37: .WAV file [output/20041119/session-enc0-PCMU-8KHz-10.0.0.49,49606-10.0.0.90,49604.wav] has l
```

## SIPProxy

- <http://sourceforge.net/projects/sipproxy>
- Java Temellidir, Birçok Platformda Çalışabilmektedir
- Proxy Özellikleri ve İstek Analizi İçin Kullanılabilmektedir
- Proxy Özellikleri
  - SIP Çağrısı İzleme ve Çözümleme
  - Çağrılar Üzerindeki Belirli Bölümleri Sürekli Değiştirme

## RTPProxy, RedirectRTP

- <http://skora.net/uploads/media/>
- Perl ve Iptables'a İhtiyaç Duymakta ve Linux'ta Çalışabilmektedir
- RTPProxy'ye istekleri yönlendirme ve değiştirebilme imkanı sunmaktadır

# Ekran Görüntüleri



## SIPProxy

The screenshot displays the SIP Proxy - VoIP Security Test Tool interface. The left pane shows a list of SIP messages with status indicators. The right pane shows the details of a selected NOTIFY message.

**Message List (Left Pane):**

- REGISTER sip:192.168.0.18 SIP/2.0
- SIP/2.0 100 Trying
- SIP/2.0 401 Unauthorized
- REGISTER sip:192.168.0.18 SIP/2.0
- SIP/2.0 100 Trying
- SIP/2.0 200 OK
- NOTIFY sip:2222@192.168.0.19:5070 SIP/2.0**
- SIP/2.0 481 Call/Transaction Does Not Exist
- INVITE sip:\*98@192.168.0.19 SIP/2.0
- SIP/2.0 407 Proxy Authentication Required
- ACK sip:\*98@192.168.0.18 SIP/2.0
- INVITE sip:\*98@192.168.0.19 SIP/2.0
- SIP/2.0 100 Trying
- SIP/2.0 200 OK
- ACK sip:\*98@192.168.0.18 SIP/2.0
- BYE sip:\*98@192.168.0.19 SIP/2.0
- SIP/2.0 200 OK

**Message Details (Right Pane):**

```
NOTIFY sip:2222@192.168.0.19:5070 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.19:5060;branch=z9hG4bK408fa87d
From: "Unknown" <sip:Unknown@192.168.0.19>;tag=as4b298183
To: <sip:2222@192.168.0.19:5060>
Contact: <sip:Unknown@192.168.0.19>
Call-ID: 0b0b53bb504b7e0044edaec249a618b0@192.168.0.19
CSeq: 102 NOTIFY
User-Agent: Asterisk PBX
Max-Forwards: 70
Event: message-summary
Content-Type: application/simple-message-summary
Content-Length: 92

Messages-Waiting: no
Message-Account: sip:asterisk@192.168.0.19
Voice-Message: 0/0 (0/0)
```

**Add Rule Table:**

Active	Direction	Regular Expression	Replacement	Edit	Delete
<input type="checkbox"/>	CLIENT to PBX	(Max-Forwards:)(\d*)	\$1 100		
<input checked="" type="checkbox"/>	CLIENT to PBX	^(User-Agent:)(.*)	\$1 SIP Proxy Application		
<input type="checkbox"/>	PBX to CLIENT	(Allow:)(.*)*(.*)	\$1 INVITE, ACK		

- **SIP Sunucu Yazılımının Analizi**
  - İşletim Sistemi ve Yazılım Güncellemeleri
  - Ön Tanımlı Yapılandırma, Yönetim Servisleri ve Şifreler
  - Bilinmeyen Programlama Sorunları
- **SIP Servisi Analizi**
  - Kullanıcı Doğrulama ve Şifre Analizi
  - İsteklerde ve Dahililerde Yetki Analizi
  - Özel Çağrılar ve Uzantılara Erişim Hakları
  - Çağrı Sahteciliği, Yönlendirme ve Posta Kutusu İşlemleri
  - Özel Testler
- **Araçlar**
  - SIPProxy, Sipsak, Sipvicious, OpenVAS, Nmap

## SIPProxy

- <http://sourceforge.net/projects/sipproxy>
- Java Temellidir, Birçok Platformda Çalışabilmektedir
- Özel Test Desteği
  - Hazır Testler
    - Doğrulasız REGISTER, Doğrudan INVITE, INVITE ile Yetki Analizi
    - Servis Engelleme için Ardışık Paket Desteği
  - Özel Testler İçin Destek
    - XML Temelli Test İçeriği, Farklı Girdi Türleri, Döngü ve Uyarı Desteği

## Nmap

- <http://insecure.org/nmap>
- Linux/Unix ve Windows'larda Çalışabilmektedir
- Servis Analizinde ve Cihaz Doğrulamada Kullanılmaktadır

## SIPProxy

```
<TestCase cycles="10" initialRequestMessageID="1" name="Unauthenticated REGISTER Attempt" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="TestCaseSchema.xsd">
```

```
<Variables>
```

```
<Var name="attackerNr">
```

```
<ClearText><![CDATA[||||]></ClearText>
```

```
</Var>
```

```
<Var name="attackerIP">
```

```
<ConfigValue paramName="TestCaseSocketIP"/>
```

```
</Var>
```

```
<Var name="attackerPort">
```

```
<ConfigValue paramName="TestCaseSocketPort"/>
```

```
</Var>
```

```
<Var name="targetIP">
```

```
<ConfigValue paramName="TargetIP"/>
```

```
</Var>
```

```
<Var name="call_ID">
```

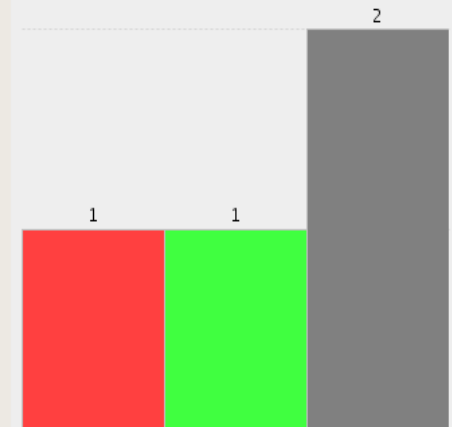
```
<StringMutationFuzzer length="10">
```

```
<CharacterSet><![CDATA[a-z,0-9]]></CharacterSet>
```

```
</StringMutationFuzzer>
```

### Test Case Report

■ WARNING ■ OKAY ■ UNKNOWN



Status: COMPLETED  
Test Case Name: TT- OPTS  
Executed Cycles: 1  
Target Address: 192.168.2.130:5060  
Target UA: LRSTD XTP8886 2008.06.05  
Start Time: 22.08.2008 15:20:32:750  
End Time: 22.08.2008 15:20:35:351

## Nmap

```
# nmap -sS -sV -O -F -n -PO 192.168.2.104
```

```
Starting Nmap 4.62 ( http://nmap.org ) at 2009-03-12 14:22 EET
```

```
Interesting ports on 192.168.2.104:
```

```
Not shown: 1275 closed ports
```

```
PORT      STATE SERVICE VERSION
```

```
21/tcp open  ftp      Trolltech Troll-FTPd
```

```
23/tcp open  telnet   NASLite-SMB/Sveasoft Alchemy firmware telnetd
```

```
MAC Address: 00:40:5A:17:DF:49 (Goldstar Information & COMM.)
```

```
Device type: switch
```

```
Running: Cisco embedded
```

```
OS details: Cisco MDS 9216i switch
```

```
Uptime: 0.085 days (since Thu Mar 12 12:21:16 2009)
```

```
Network Distance: 1 hop
```

```
Service Info: Host: lgvp; OS: Linux
```

```
OS and Service detection performed. Please report any incorrect results at  
http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 18.623 seconds
```

## ➤ SIP İstemcisi Analizi

➤ Sunucu Testlerinin Tamamı Uygulanmalıdır

➤ Test Bakış Açılarında Küçük Değişiklikler Yapılmalıdır

- Doğrudan Çağrı → Faturalamanın Ortadan Kalkması
- Kayıt Desteği Olması → SIP Ağına Yönelik Çağrı Açabilme
- Şifre Kaydetme → Kullanıcı Kimlikleri
- Ön Tanımlı Yönetim → Şifreler, TFTP Güncelleme
- Merkezi Güncelleme → Toplu Ele Geçirme
- Gömülü Yazılım → Harici Yazılımların Yan Etkileri (Netcat?)

## ➤ Araçlar

- SIPProxy Testleri Kullanılmalı, Bolca Özel Test Hazırlanmalı
- Yönetim/SIP/Destek Servislerine Yönelik Analiz Yapılmalı
- SIPProxy, Sipsak, Sipvicious, OpenVAS, Nmap

## Ekiga

- <http://www.gnomemeeting.org>
- Linux/Unix/Windows için SIP/H.323 Telefonu
- Sunuculara bağlantı ve istemci örnekleme için sıklıkla ihtiyaç duyulacaktır

## AsteriskNOW

- <http://www.asterisknow.org>
- Asterisk Projesinin Kurulum/Kullanımı Kolay Özel Sürümü
- Örnek sunucular oluşturmak ve denetim senaryolarını gerçekleştirmek için ihtiyaç duyulacaktır

- VOIPSA  
<http://www.voipsa.org>
- VOIPSA Araçlar  
<http://www.voipsa.org/Resources/tools.php>
- OSSTMM - Open Source Security Testing Methodology Manual  
<http://www.isecom.org/projects/osstmm.htm>
- ISSAF Penetration Testing Framework  
[http://www.oisssg.org/wiki/index.php/ISAAF-PENETRATION\\_TESTING\\_FRAMEWORK](http://www.oisssg.org/wiki/index.php/ISAAF-PENETRATION_TESTING_FRAMEWORK)
- How To Set Up a VoIP Lab  
<http://resources.enablesecurity.com/resources/voiplab.pdf>
- Siyah Şapka  
<http://siyahsapka.blogspot.com>

*Teşekkürler....*