Özgür Yazılımlarla VoIP Güvenlik Denetimi

Fatih Özavcı - Linux Kullanıcıları Derneği

VoIP Servislerinin ve Cihazların Saptanması

VoIP analizlerinin ilk adımı kapsamda yer alan VoIP cihazlarının ve servislerinin saptanmasıdır. Ağ haritalama aşamasında saptanan cihazlar üzerinde çalışan servisler analiz edilerek SIP, IAX veya H.323 temelli servislerin varlığı doğrulanabilir. VoIP temelli servislerin saptanması için standart ağ haritalama yazılımlarına ek olarak VoIP analizi için hazırlanmış özel araçlarda kullanılabilir.

VoIP temelli sistemlerin saptanmasına ek olarak ilgili sistemler üzerinde çalışan VoIP servislerinin türü, işletim sistemi, servisleri sunan yazılımlar ve sürümleri de toplanması gereken bilgiler arasındadır. Birçok VoIP ağı SIP veya IAX protokollerini tercih etmekte, ağırlıklı olarak uzak erişimler ve çağrı yönetiminde SIP tercih edilmektedir. IAX ise Asterisk için geliştirilmiş özel bir protokoldür; Asterisk'in PBX olarak kullanıldığı durumlarda veya IAX üzerinden VoIP servisleri sunulması amacıyla tercih edilmektedir. H.323 ise görüntü ve ses akışı gerekli olan konferans ortamlarında sıklıkla tercih edilmektedir. Saptanan cihaz ile ilgili servis türü ve yazılımsal bilgiler, denetimin analiz aşamalarında sıklıkla kullanılacaktır.

Sipvicious araç seti ile SIP temelli VoIP servislerinin saptanabilmekte ve analizi yapılabilmektedir. Sipvicious'un parçası olan “svmap.py” kullanılarak bir ağ veya IP adresi üzerinde çalışan SIP servislerinin listelenmesi ve servisi çalıştıran yazılım hakkında bilgi alınması mümkündür.

```
# ./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 (0.2.91.0616) | T-Com Speedport W500V / Firmware v1.37
MxSF/v3.2.6.26 |
```

Sipvicious ile SIP Sunucusu/Cihazları Saptanması

Asterisk IAX2 servislerinin araştırılması için ise iaxscan ve enumiax araçları kullanılabilir. IAX2 temelli servisler SIP servislerine göre daha az yaygındır; ancak birçok SIP servisi sunan cihazda yazılım olarak Asterisk kullanılmaktadır. Bu nedenle temelde SIP servisi sunmak üzere hazırlanmış bir sunucu veya sistemde de IAX2 servisinin etkin olması sözkonusu olabilmektedir.

Referanslar

Araçlar ve Uygulamalar

1. Sipvicious - http://sipvicious.org
2. Enumiax - http://sourceforge.net/projects/enumiax
3. Iaxscan - http://code.google.com/p/iaxscan

SSL/TLS Kullanımının Analizi

Açıklama

IP telefon servisi için kullanılan protokollerin düz metin olması durumunda, ağ temelli paket yakalama saldırıları kullanılarak iletişim içerikleri çözümlenebilir. Bu nedenle düz metin temelli protokoller yerine SSL/TLS destekli protokoller tercih edilmelidir. SIP, RTP ve H.323 protokollerinin tamamı SSL/TLS üzerinden akabilmekte ve iletişimi kriptolu olarak sağlayabilmektedir. SSL/TLS kullanımı kimlik doğrulama aşamasında kullanılıyor ise iletişimin devamı içinde kullanılabilir ve bu doğrultuda iletişimin kriptolu olarak korunması sağlanabilir. Ağ temelli birçok saldırıdan korunabilmek adına tüm servislerde SSL/TLS desteğinin etkin olduğu doğrulanmalıdır.

İstemciler ile sunucular arasında akmakta olan, kimlik doğrulama, çağrı işletimi, çağrı akışı ve diğer iletişim istekleri düz metin olarak akmaktadır. VoIP istemcileri ile sunucuları arasında yer alan iletişim kriptolanmamaksı durumunda; VOIP iletişimleri yakalanabilir, ortadaki adam saldırıları düzenlenerek çağrılar yakalanabilir veya değiştirebilir.

SSL/TLS'in Gerekli Olduğu VoIP Süreçleri

- SIP El Sıkışmaları
  - Kullanıcı Doğrulama
  - Oturum Başlatma, Durdurma ve Diğer İşlemler
- RTP İletişimi
- IAX2 İletişiminin Tüm Aşamaları
- H.323 İletişiminin Tamamı
- İstemci Cihazlarının Güncellenme İşlemleri

SSL/TLS'in Varlığını Kontrol Yöntemleri

- Örnek bir bağlantı yaparak ve paket yakalama yazılımları aracılığıyla analiz
  - SIP/IAX2/H.323 İçeriğinin Çözümlenmesi
  - RTP İletişiminin Ses/Görüntü Dosyasına Aktarılması
- İstemci cihazların ilk güncelleme isteklerinin ve işlemlerinin analizi

Referanslar

Araçlar ve Uygulamalar

1. Vomit - http://vomit.xtdnet.nl
2. Voipong - http://www.enderunix.org/voipong
3. Wireshark - http://www.wireshark.org

Kimlik Doğrulama Analizi

VoIP sunucularına bağlanabilecek yazılımlar veya yazılımsal servisler için kullanıcı kimliği yönetim süreci kullanılıyor olmalıdır. Servise bağlanabilecek olan kullanıcıların tanımlamaları, merkezi kullanıcı yönetimi, şifre politikaları ve harici kimlik doğrulama yöntemleri analiz esnasında dikkate alınmalıdır. Kimlik doğrulama olmaksızın bir servis kullanımı tercih edilmiyor olmalıdır.

VoIP sunucularına bağlanabilecek donanımlar ve telefonlar için sertifika temelli kimlik yönetim süreci kullanılmalıdır. Servise bağlanabilecek olan cihazların tanımlamaları, merkezi sertifika yönetimi için gerekli yapılandırmalar uygulanmış olmalıdır. Hatalı yapılandırılmış cihaz yönetim süreci nedeniyle, yetkisiz cihazlar ile sunucuya erişim sağlanabilir.

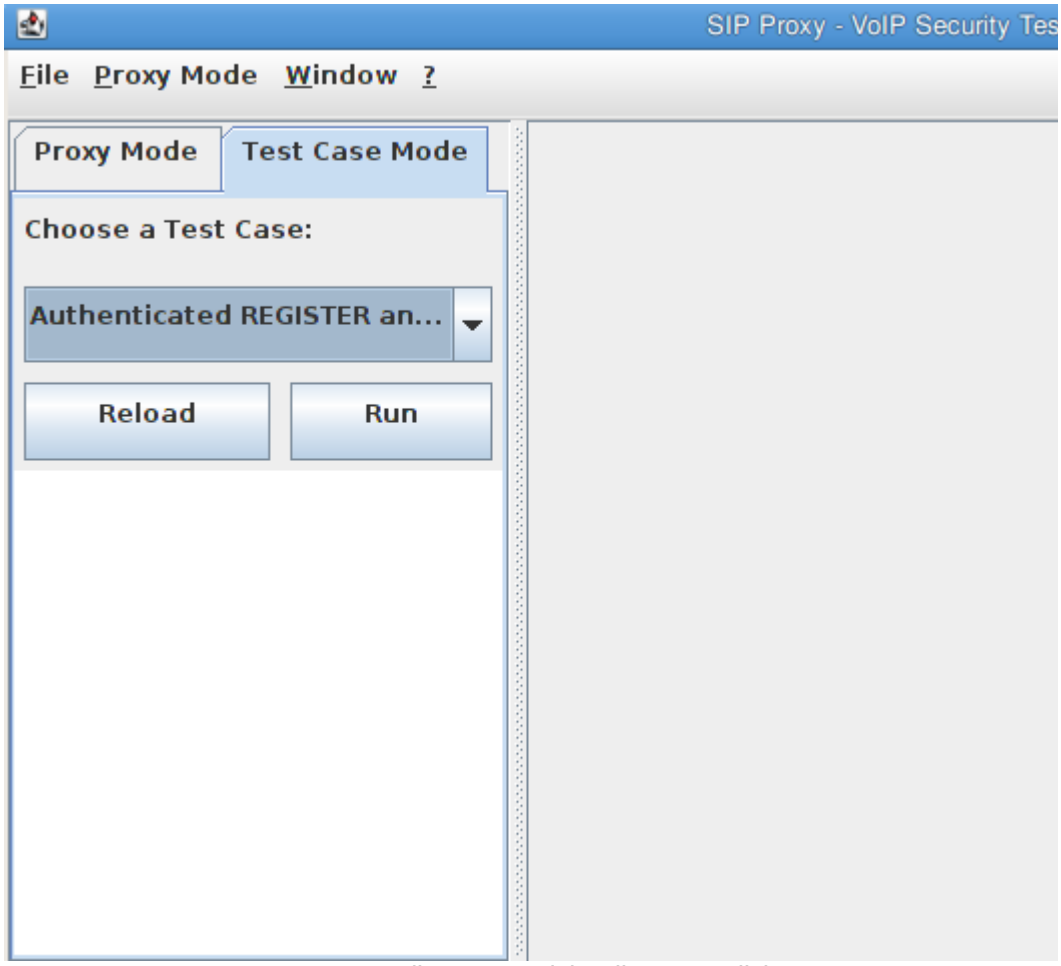
Analiz sürecinde kullanıcı/şifre denemeleri, servislere/yazılıma özel kullanıcıların denetimi, kimlik doğrulama olmaksızın kullanılabilecek işlemler ve cihazlar için sertifika kullanımının gerekli olduğu durumlar analiz edilmelidir.

Denetim Kontrolleri

- Kimlik Kullanılabilecek Her İstemci İçin Kullanıcı Kimliği Kullanılıyor Olmalı
- Merkezi Kimlik Yönetim Servisleri Kullanılıyorsa, VoIP Kullanıcıları Ayrı Bir Grupta Tanımlanarak Özel Yetkilere Atanmış Olmalı
- IP Telefon Sunucusu veya Kullanıcı Kimliklerini Yöneten Sunucu Üzerinde, Kalite ve Süre Kriterleri İçeren Şifre Politikası Uygulanıyor Olmalı
- Ön Tanımlı Kullanıcılar ve Kimlikler Devre Dışı Bırakılmış veya Şifreleri Değiştirilmiş Olmalı
- Şifre Girmesi Mümkün Olmayan ve Uzun Süreli Kalıcı Bağlantı Kuran Sistemlerde, Kullanılabiliyorsa Harici Kimlik Doğrulama Tercih Edilmeli (Tek Kullanımlık Şifre, Sertifika)

SIP servisinde REGISTER, INVITE, BYE ve CANCEL gibi çok sayıda istek türü kullanılmaktadır. Her bir komut için kimlik doğrulama ve oturum takip yapılıyor olmalıdır, aksi durumda REGISTER sürecinden geçmemiş bir cihaz ile INVITE kullanılarak oturum açılabilir veya BYE ile açılmış bir oturum sonlandırılabilir.

SIPProxy yazılımı Proxy olarak çalışmakta ve bir SIP istemcisi ile sunucu arasındaki iletişimin analiz edilmesini sağlamaktadır. Test özellikleri arasında yetkisiz REGISTER, INVITE ve BYE istekleri gönderimi yer aldığı gibi hazırlanan özel testlerin kullanımı da mümkündür.



SIPProxy ile SIP Servisi Kullanıcı Analizi

Sipvicious araç seti içinde yer alan svcrack aracı, SIP sunucularına kullanıcı ve şifre denemeleri yapılması için kullanılabilmektedir. Kullanıcı denemelerini belirli bir dahiliyi veya özel yetkiyi kullanmak için de yapabilmektedir.
IAX2 protokolü için ise iaxscan ve enumiax araçları kullanılabilir, her iki aracın da kullanıcı/şifre doğrulama imkanları bulunmaktadır. Deneme/yanılma veya sözlük saldırıları aracılığıyla IAX2 kullanıcılarını analiz etmektedirler.

Referanslar

Araçlar ve Uygulamalar

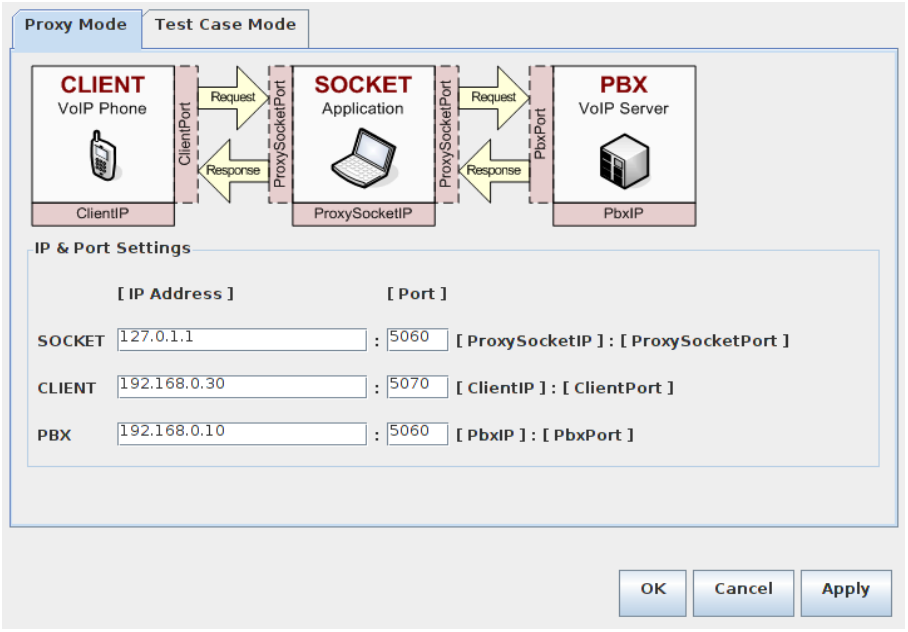
1. SIP Proxy - http://sourceforge.net/projects/sipproxy
2. Sipvicious - http://sipvicious.org
3. Enumiax - http://sourceforge.net/projects/enumiax
4. Iaxscan - http://code.google.com/p/iaxscan

SIP Servisi İç Yetkilendirme ve Özel Analiz

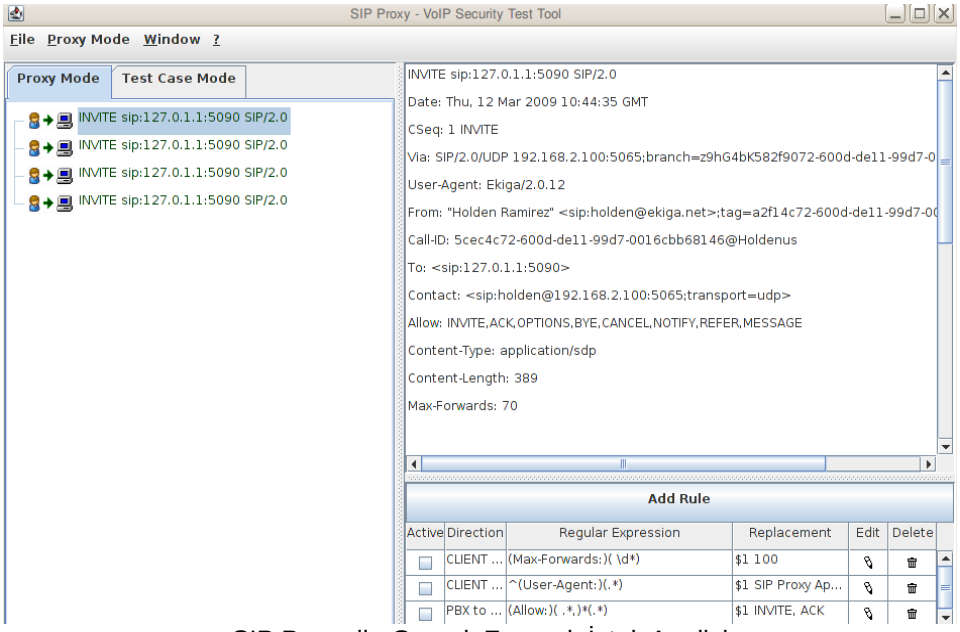
SIP servisi bir telefon yönlendirme yapısı gibi çalışmaktadır, birçok karasal hat, analog hat, diğer sunucular veya GSM şebekeleri için geçiş uzantıları bulunabilmektedir. Kullanıcılar sadece kendi aralarında değil, diğer hatlarla da iletişime geçebilmektedirler. Alan kodları veya ön ekler olarak bilinen kısa numaraların girilmesi sonrasında ilgili yetki kazanılır ve çağrı yapılır. Standart telefon hatlarındaki ön eklerin kullanımına benzer ön eklerin saptanması, bu ön eki kullanabilecek kullanıcıların saptanabilmesi veya diğer kullanıcıların listesinin alınabilmesi gibi analizler yapılabilmektedir.

Belirli bir kullanıcı veya anonim durumda iken yetkili bir kullanıcının doğrulanması, çağrı yapılabilecek olan ön eklerin veya uzantıların saptanması gibi amaçlarla özel testlerin yapılabilmesi gerekmektedir. Özel testler yapılabilecek yazılımlar ile test şablonu belirtilerek analizler yapılabilir, sunucuya özel yetkilendirme veya diğer zaafiyetler saptanabilir.

SIP Proxy yazılımını ise özel testler için veya Proxy özelliği ile gerçek zamanlı analizlerde kullanılabilmektedir. Özel testler XML olarak hazırlanabilir ve yazılım tarafından işlenebilmektedir. Test için hazırlanmış farklı girdi biçimleri ve hazır fonksiyonlar önemli kolaylıklar sağlamaktadır. Ayrıca varolan bir istemci/sunucu iletişiminin ortasına girmek veya gerçek zamanlı analiz için de arayüzü bulunmaktadır. SIP Proxy testleri için hazırlanan XML içerikte öncelikle değişkenler hazırlanmakta, sonrasında ise tanımlanan değişkenler standart SIP isteklerinin uygun değerlerine yerleştirilebilmektedir.



SIP Proxy ile Proxy Yapılandırması



SIP Proxy ile Gerçek Zamanlı İstek Analizi

Referanslar

Araçlar ve Uygulamalar

1. SIP Proxy - http://sourceforge.net/projects/sipproxy
2. Sipvicious - http://sipvicious.org
3. Enumiax - http://sourceforge.net/projects/enumiax
4. Iaxscan - http://code.google.com/p/iaxscan

VoIP Cihaz ve Servislerinde Yayınlanmış Güvenlik Açıkları Analizi

IP telefonlar ve VoIP cihazları gömülü işletim sistemi barındırırlar, genellikle özel bir işletim sistemi veya Linux temelli bir sistem bu amaçla kullanılmaktadır. Gömülü işletim sisteminin üzerinde ise VoIP, web ve snmp gibi servisleri sağlayan çeşitli uygulamalar da çalışır. Bu uygulamalar servis engelleme saldırılarına karşı zaafiyet barındırabilecekleri gibi uzaktan yönetim servisi devre dışı bırakılabilir veya servisin/cihazın kontrolü tamamen ele geçirilebilir.

VoIP cihazlarının ve servislerinin saptanması aşamasında elde edilen bilgiler analiz edilerek, denetlenen sistemin türü ve yayınlanmış güvenlik açıkları araştırılabilir. Yayınlanmış güvenlik açıkları otomatize araçlar veya güvenlik açığı veritabanlarından araştırılabilir.

Denetim Kontrolleri

- Cihaz Yazılımları Güncelleniyor Olmalı
- Cihazlar Üzerinde Gerekli Olmayan Ağ Temelli Servisler Bulunmamalı
  - Web Servisi, SNMP Servisi, Telnet Servisi, Secure SHell Servisi
- Cihazlar Üzerindeki Servislerin Tahmini Zor Şifre ile Korumalı Olduğu Doğrulanmalı

Nmap kullanılarak örnek cihazlar üzerinde yer alan görev dışı servisler veya alt servisler hakkında bilgi alınabilir. Birçok VoIP sunucu cihazı yönetsel ve bilgi edinme amaçlı servisler kullanmaktadır. VoIP istemcisi olarak kullanılan telefon ve cihazlar ise merkezi yönetim amaçlı servisler çalıştırmaktadır. Saptanan servisler analiz edilerek yayınlanmış güvenlik açıkları araştırılabilir, kullanıcı ve şifre denemeleri yapılabilir. Birçok istemci cihaz ön tanımlı şifreleri kullanmaktadır, belirtilen şifreler cihaz modeli ile araştırma yapıldığında birçok kaynaktan edinilebilir.

Nmap kullanılarak, Nortel IP Phone 1535 modeli için yapılmış olan bir servis analizi örnekte görülmektedir.

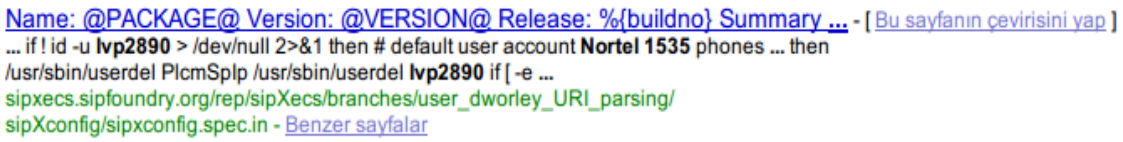
```
# nmap -sS -sV -O -F -n -P0 192.168.2.104

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
```

Nmap ile Nortel IP Phone 1535 için Servis Analizi

Örnekte Nortel IP Phone 1535 modeli için fabrika ayarlarında tanımlanmış şifreler denenerek erişim sağlanmıştır. Giriş sonrası cihaz üzerinde her türlü değişiklik, ekran görüntüsü alma veya çağrı yönlendirme/kayıt işlemleri yapılabilmektedir.



Nortel IP Phone 1535 için Ön Tanımlı Yönetici Şifresi Araştırması

```
# telnet 192.168.2.104
Trying 192.168.2.104...
Connected to 192.168.2.104.
Escape character is '^]'.

lgvp login: root
Password: lvp2890

BusyBox v1.00 (2006.04.10-06:46+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
#
```

Nortel IP Phone 1535 için Ön Tanımlı Şifre Girişi

Referanslar

Araçlar ve Uygulamalar

1. Nmap - http://www.insecure.org/nmap