Gökhan ALKAN
Twitter: @cigalkan, Web Site: www.agguvenligi.net

SCRIPTING FOR PENTESTER

06.06.2013

Twitter: @cigalkan, Web Site: www.agguvenligi.net

İçerik

- En Çok Tercih Edilen Yazılımlar ve Geliştirme Ortamları?
- Hangi Yazılım Dilleri Tercih Ediliyor?
- Sectools.org
- Hangisi Tercih Edilmeli?
- Exploit-db Icerisinde En Cok Hangi Diller Tercih Edilmis
- Gerçek Hayatdan Betikler
  - LinkedinE-posta Toplama, Sees, Copten Karton Toplar, Otomatik Domain Admin
- C/C++ ve Betik Dilleri İçin Tercih Sebebi
- Bu Paragraftan Çıkacak Sonuç ?
- Demo - Bir Yerel Ağ Klişesi Arp Spoofing
- Kaynaklar

Kambersiz Düğün Olur mu ?

- Pentestlerin Mfö'sü - Metasploit,Nmap,Nessus
  - Metasploit - Ruby
  - Nessus - Nasl
  - Nmap - Lua

Nerelerde Kullaniliyor?

- Sizma Testleri
- Sosyal Muhendislik
- Exploit Gelistirme
- Zararli Yazilim Analizi
- DOS/DDOS
- …

Hangi Yazılım Dilleri Tercih Ediliyor?

Proje	Gelistirme Ortami
Metasploit	Ruby
Nmap	Lua
Nessus	Nasl
SqlMap, Wa3f, Scapy	Python
C/C++	Netcat, John The Ripper,Sysinternals
Nikto	Perl

http://sectools.org - Top 25

- **Perl/Python/Ruby (#23, 3)**
- While many canned security tools are available on this site for handling common tasks, scripting languages allow you to write your own (or modify existing ones) when you need something more custom. Many security tools use scripting languages heavily for extensibility. For example Scapy interaction is through a Python interpreter, Metasploit modules are written in Ruby, and Nmap's scripting engine uses Lua. Review this tool.

Peki Ama Hangisi ?

- Hızlı ve Öfkeli -> C/C++
- Evli ve Çocuklu -> Perl
- Hamarat ve Basit -> Python
- Yetenekli ama Nazlı –> Ruby
- Güçlü Ama Ağır -> Java
- Tehlike Anında Kırınız -> Lua, Nasl

…

Exploit-db


```
#!/bin/bash
for ext in c py rb sh pl
do
        result="`find /pentest/exploits/exploitdb/ -type f -name "*.$ext" | wc -l`"
        echo -e "$ext: $result"
done
```

c: 1575

py: 824

rb: 1442

sh: 95

pl: 1787

Hızlı ve Öfkeli


```
root@vps:~# cat dosya_oku.c
#include <stdio.h>

int main ( int argc, char *argv[] )
{
        char *filename = argv[1];
        FILE *file = fopen ( filename, "r" );

        if ( file != NULL )
        {
                char line [ 5 ];
                while ( fgets ( line, sizeof line, file ) != NULL )
                {
                        fputs ( line, stdout );
                }
                fclose ( file );
        }
        else
        {
                perror ( filename );
        }
        return 0;
}

root@vps:~# cat dosya_oku.py
#!/usr/bin/python

import sys

dosya_path = sys.argv[1]

for line in open(dosya_path,"r"):
        print line[:-1]
```

Hızlı ve Öfkeli


```
root@vps:~# wc -l dosya_oku.c
23 dosya_oku.c
root@vps:~# wc -l dosya_oku.py
9 dosya_oku.py
root@vps:~# gcc -o calistir dosya_oku.c
root@vps:~# for line in `seq 1 1000`; do echo "$line"; done > oku_beni.txt
root@vps:~# time ./calistir oku_beni.txt >/dev/null

real    0m0.001s
user    0m0.000s
sys     0m0.001s
root@vps:~# time ./dosya_oku.py oku_beni.txt >/dev/null

real    0m0.011s
user    0m0.008s
sys     0m0.003s
root@vps:~# cat /proc/cpuinfo | grep "model name"
model name      : Intel(R) Xeon(R) CPU           X3450   @ 2.67GHz
root@vps:~#
```

Linkedin E-posta Toplama

- Geliştirme ortamı ruby
- Oauth kütüphanesi
- 1 Adet ruby yuklu tercihcen Linux dagitimi

- # ./linkedin.rb

  -s Aranacak_Kisi_Sayisi -k Aranacak_Kurum_Adi -e Eposta_Domain_Bilgisi -o Cikti_Format_Degerleri[1,2,3] -f Yapilandirma_Dosyasi

Linkedin E-posta Toplama

Muhtemel E-posta formati:

- Ilk_Harf[Isim].SoyIsim -> g.alkan
- Ilk_Harf[SoyIsim].Isim -> a.gokhan
- Isim.SoyIsim -> gokhan.alkan

- # ./linkedin.rb -s 10 -k microsoft -e microsoft.com -o 1,2,3 -f config.txt

l.calderon@microsoft.com

lisa.c@microsoft.com

lisa.calderon@microsoft.com

…

Sees - Social Engineering Email Sender

- Geliştirme ortamı python
- Ekli e-posta (Çoklu) gönderme
- Html içerikli e-posta gönderme
- Aynı anda çoklu olarak e-posta gönderme
- Smtp auth gereksinimi yok
- Geçerli bir domain ve smtp sunucu yeterli

```
# ./sees.py
Usage: ./sees.py  (-a attach_file |-n html_file) (-f mail_user_file) (-c
    config_file)
```

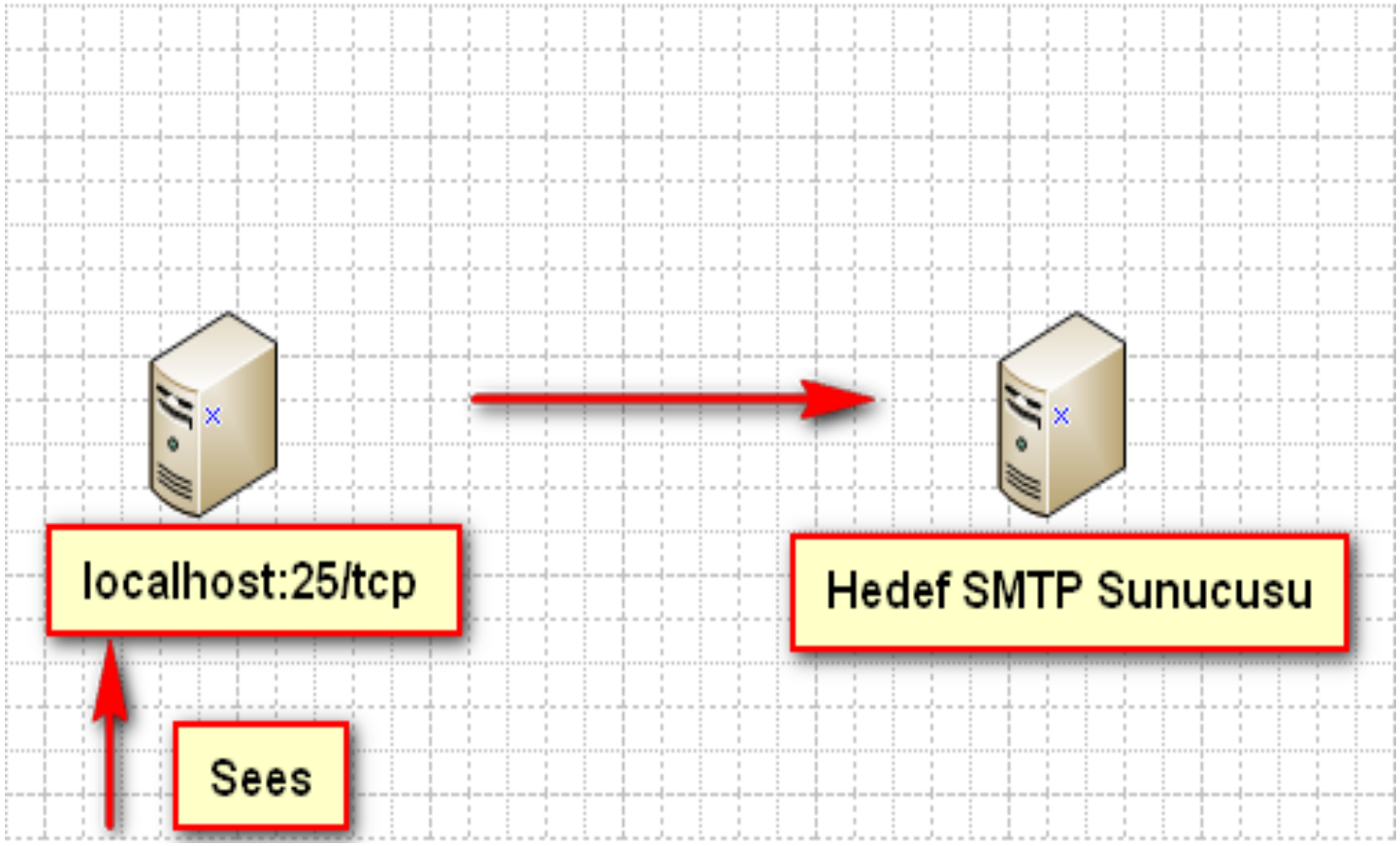
Sees - Social Engineering Email Sender

- config_file

```
# cat config
[mail]
domain = XXX.com   # görünen domain bilgisi

[smtp]
server = 127.0.0.1   # E-posta gönderecek smtp sunucu
time = 2  # Bir sonraki e-posta göndermek için beklenecek süre
port = 25 # smtp sunucu porte bilgisi
```

Sees - Social Engineering Email Sender



Sees - Social Engineering Email Sender

- mail_config_file

cat mail_user_file

mudur@XXX.com:Mudur Bey:Maas Zammi Hakkinda:user@XXX.com

exit

Çoklu E-posta Gönderimi

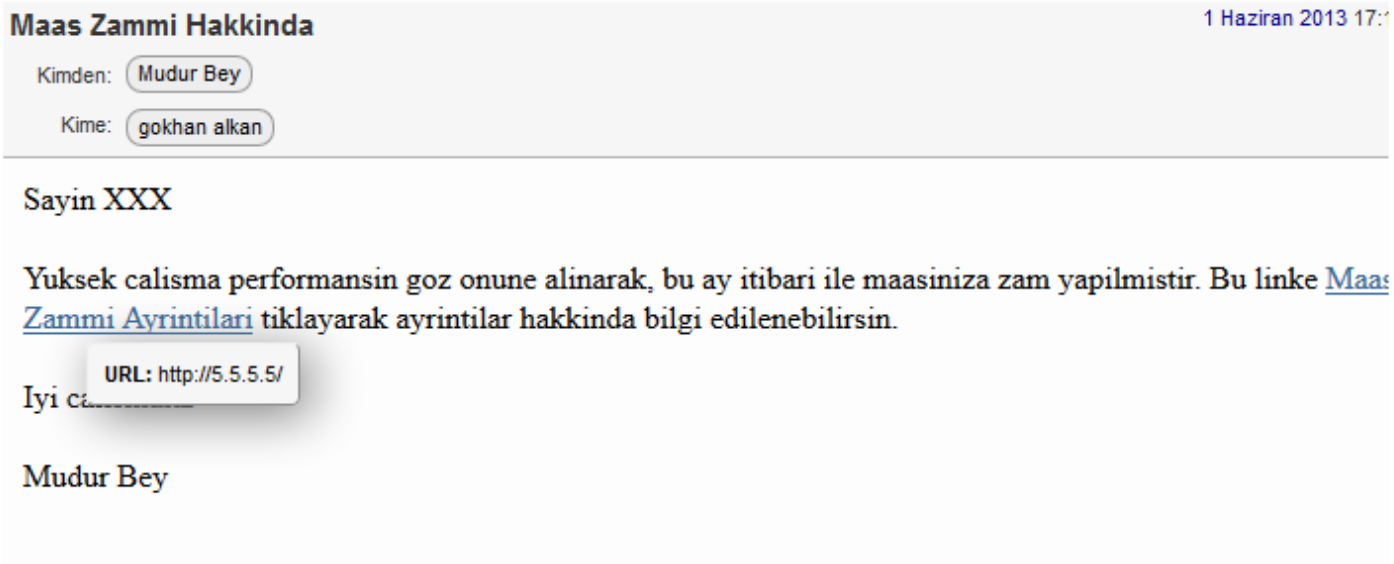
mudur@XXX.com:Mudur Bey:Maas Zammi Hakkinda:user1@XXX.com

exit

mudur@XXX.com:Mudur Bey:Maas Zammi Hakkinda:user2@XXX.com

mudur@XXX.com:Mudur Bey:Maas Zammi Hakkinda:user3@XXX.com

Sees - Social Engineerin Email Sender



Sees - Social Engineering Email Sender

MAIL FROM:<legal_user@XXX.com>

…

DATA

…

Content-Type: multipart/alternative;

boundary="X.X.X.X.0.3655.13700981 20.489.1"

To: gokhan.alkan@XXX.com

From: Mudur Bey <mudur@XXX.com>

Subject: Maas Zammi Hakkinda

MIME-Version: 1.0

Message-Id: <20130601144840.781A96013C3@sunucu_hostname_bilgisi>

Date: Sat, 1 Jun 2013 17:48:40 +0300 (EEST)

Paylasımları Tarama

- Geliştirme ortamı bash
- #./ckt.sh subnet_bilgisi “domain_adi\username%sifre"” -f config

cat config

string = “password,db_connection,sifre,kullanıcı_adı”

file_size = 10Mb

  - 192.168.1.37 -> password = 123456
  - 192.168.1.34 -> db_connection = “cok_gizli”

Otomatik Domain Admin

- Geliştirme ortamı python
- #./domain_admin.py -f config_file
  - 192.168.1.37 -> dbadmin

- # cat config_file
  - subnet = 192.168.1.0/24
  - username = username
  - hash = XXX
  - admin_names = admin1,admin2,admin3

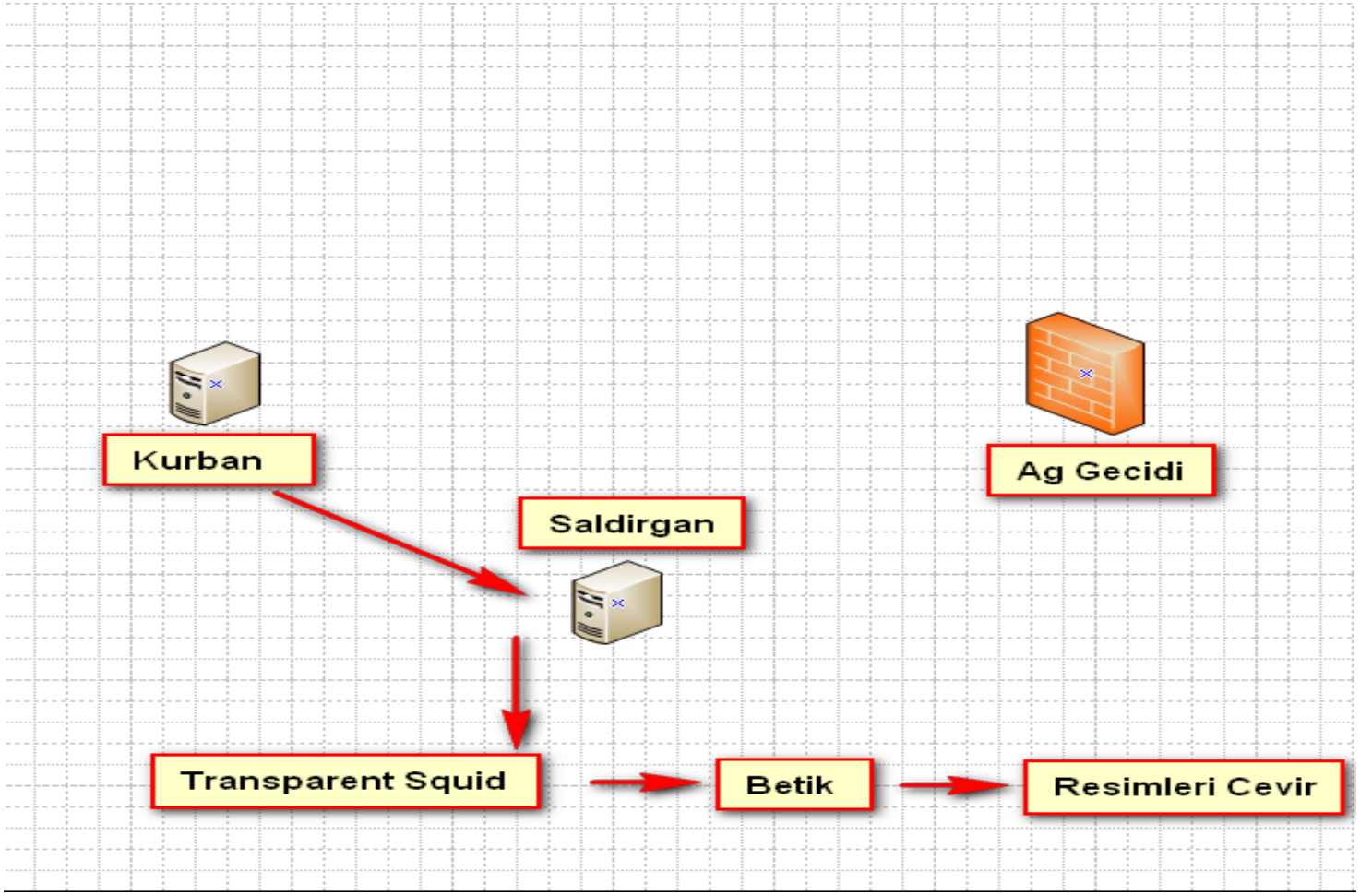
Bu Paragraftan Cikacak Sonuc

Metasploit staff say …

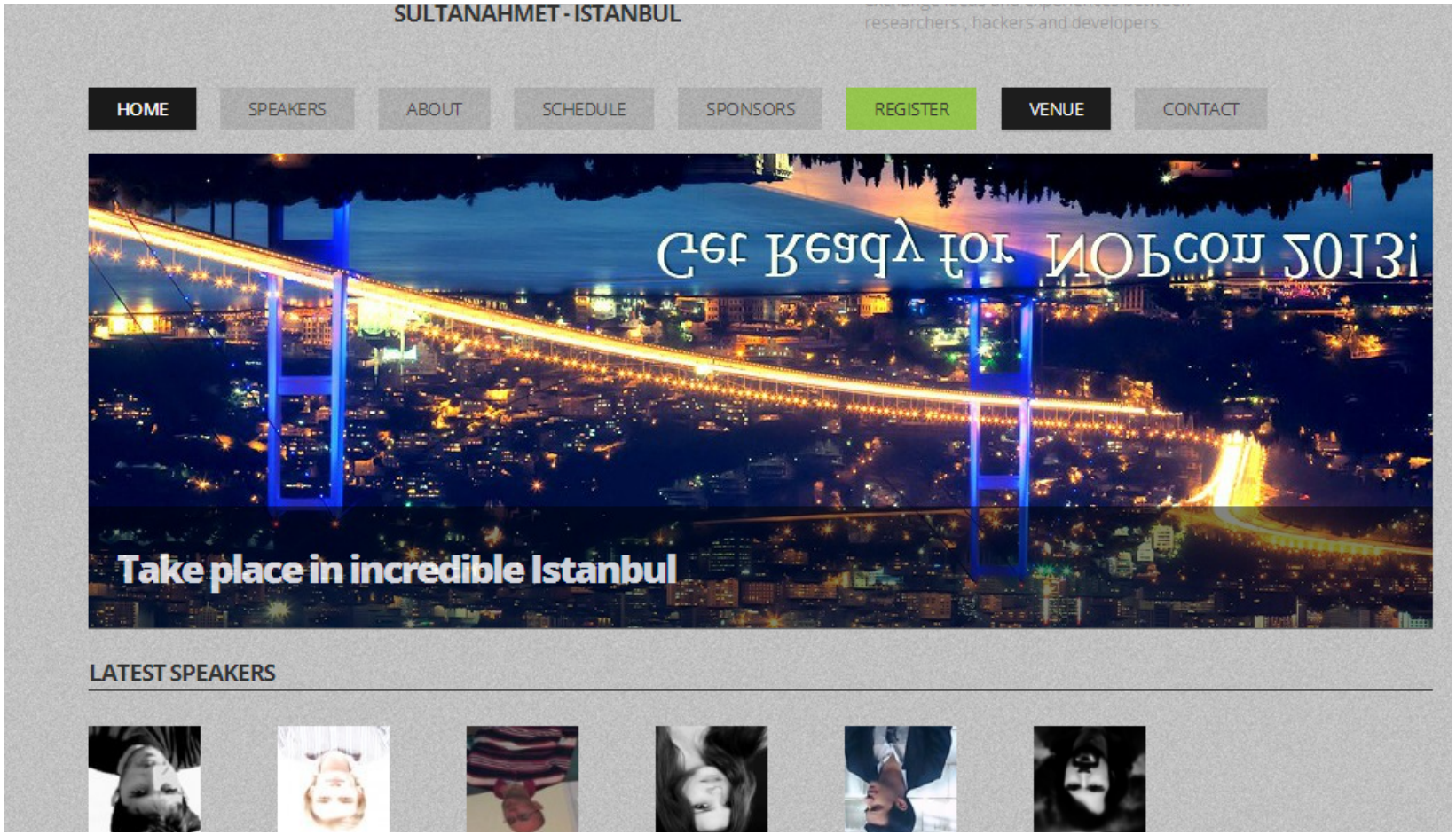
- The first (and primary) reason that Ruby was selected was because it was a language that the Metasploit staff enjoyed writing in.

- The reason is a general distaste for some of the syntactical annoyances forced by python, such as block-indention.

Demo - Arp Spoofing ve Resimleri Ters Cevirmek

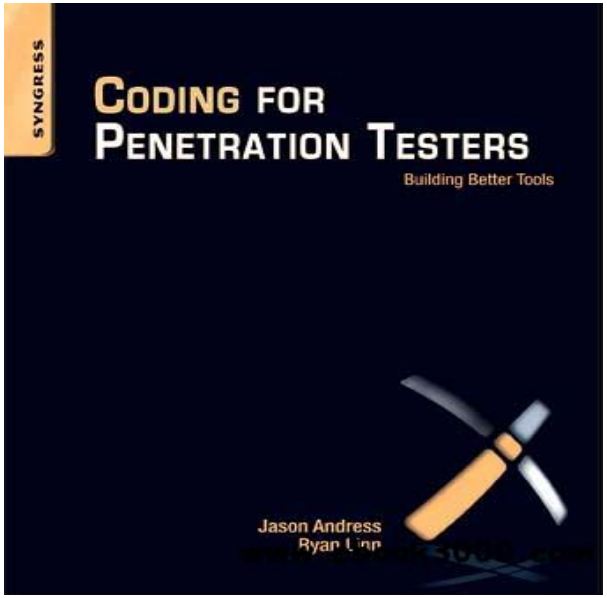


Demo - Arp Spoofing ve Resimleri Ters Cevirmek



Kaynaklar

- **Coding for Penetration Testers: Building Better Tools**



- **http://www.agguvenligi.net**

Sorular

Twitter: @cigalkan, Web Site: www.agguvenligi.net