

# **Sızma Testlerinde Pratik Programlama**

Gökhan ALKAN  
Tübitak/Siber Güvenlik  
Enstitüsü

# İçerik

- Sızma Testi Nedir ?
- Genel Sızma Testi Kategorileri Nelerdir ?
- Sızma Testi Türleri
- Sızma Testi Adımları
- Sızma Testlerinde Yaşanan Problemler
- Sızma Testlerinde Tercih Edilen Linux Dağıtımları
- Sızma Testlerinden En Çok Tercih Edilen Açık Kaynak Kodlu Yazılımlar
- Sızma Testlerinden Tercih Edilen Yazılım Dilleri
- Örnek Uygulama

# Sızma Testi Nedir ?

- Penetrasyon testi, kurumların Bilişim Sistemleri'nin saldırgan öngörüsü ile güvenlik açıklarının tespit edilip bulunan zafiyetlerin kullanılarak sistemlere sızılmaya çalışılması ve raporlanmasıdır.

# Sızma Testi Nedir-2 ?



# Genel Sızma Testi Kategorileri

- Ağ Sızma Testleri
- Web Uygulama Sızma Testleri
- Veritabanı Sistemleri Sızma Testleri
- İşletim Sistemleri Sızma Testleri
- Sosyal Mühendislik
- DDOS
- Kablosuz Ağ Sızma Testi

# Sızma Testi Türleri

- **White Box**

Her türlü bilgi açık. Kolay

- **Black Box**

Hiçbir bilgi yok. Zor

- **Grey Box**

İç ağ içerisinde yetkisiz bir kullanıcı bakış açısı. Black Box > Grey Box > White Box



# Sızma Testi Adımları

- Bilgi Toplama
- Ağ Keşif Çalışmaları
- Zaafiyet Taraması
- Sisteme Sızma
- Erişimi Koruma
- Erişimleri Temizleme

# Sızma Testlerinde Yaşanan Problemler

- Kaynak (İş gücü, Donanım vb)
- **Zaman**
- Çözüm
  - Otomatize işlerin programlı olarak yapılması yolu ile koterılması.





# Sızma Testlerinde En Çok Tercih Edilen Linux Dağıtımları

- Backtrack
- NodeZero
- BackBox Linux
- BlackUbuntu

vb ...

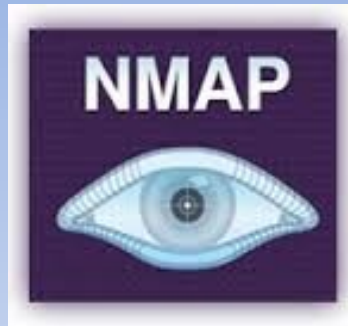


```
done.  
Activating swapfile swap...done.  
Setting up networking...  
Configuring network interfaces...Internet Systems Consortium DHCP Client  
U3.0.4  
Copyright 2004-2006 Internet Systems Consortium.  
All rights reserved.  
For info, please visit http://www.isc.org/sw/dhcp/  
-> gelic_net open:1386  
Listening on LPP/eth0/00:19:c5:17:9d:6c  
Sending on LPP/eth0/00:19:c5:17:9d:6c  
Sending on Socket/Fallback  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5  
DHCPOFFER from 192.168.88.129  
DHCPREQUEST on eth0 to 255.255.255.255 port 67  
DHCPACK from 192.168.88.129  
bound to 192.168.88.197 -- renewal in 1535 seconds.  
done.  
Starting portmap daemon...  
Setting console screen modes and fonts.  
INIT: Entering runlevel: 2  
Starting system log daemon: syslogd.  
Starting kernel log daemon: klogd.  
Starting portmap daemon...Already running..  
Not starting internet superserver: no services enabled.  
Starting OpenBSD Secure Shell server: sshd.  
Starting NFS common utilities: statd.  
Starting periodic command scheduler: crond.  
Debian GNU/Linux 4.0 ps3 tty1  
ps3 login:
```

<http://www.concise-courses.com/security/top-ten-distros/#>

# Sızma Testlerinde En Çok Tercih Edilen Açık Kaynak Kodlu Yazılımlar

- Nessus
- Metasploit
- Nmap



# Sızma Testlerinde En Çok Tercih Edilen Yazılım Dilleri

- Perl
- Python
- Bash Script
- Ruby
- Power Shell
- ...

# Neden C veya C++ Değil ???

- **Avantaj**
  - Hız, Performans
- **Dezavantaj**
  - Geliştirme Zamanı

# Neden C veya C++ Değil-2 ???

- **Lab**
  - Dosya okuma zamanları

# ExploitDb - Script Sayısı

```
#!/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**

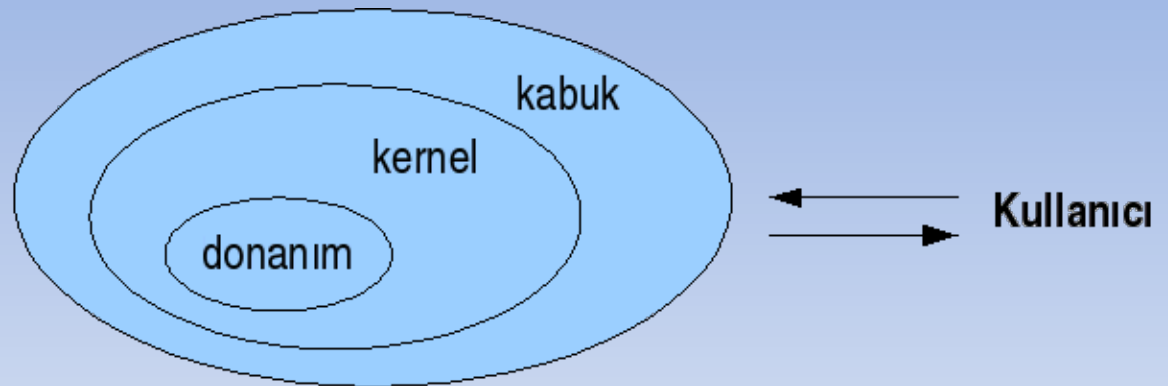


# Python

- Özgür
- Nesneye Yönelik Bir Dildir
- Yorumlamalı/Derlemeli
- Öğrenmesi Kolay
- Taşınabilirlik

# Kabuk Programlama (Bash Scripting)

- Kurulum Gerektirmez
- İnteraktif
- Kolay
- Basit





# Örnek Sızma Testi Senaryosu

- **Sızma Testi 1. Adımı -> BİLGİ TOPLAMA**
- **Lab**
  - Bash scripting ile multithread ping programı.
  - Ters DNS kayıtlarının tespit edilmesi.

# Sonuç - 1

- En iyi yazılım dili, en çok hakim olunan yazılım dilidir.
- Yapılabilecekler hayal gücüne bağlıdır.
- Sızma testleri için pratik programlama ile kısa sürede bir çok iş otomatize olarak gerçekleştirilebilir.

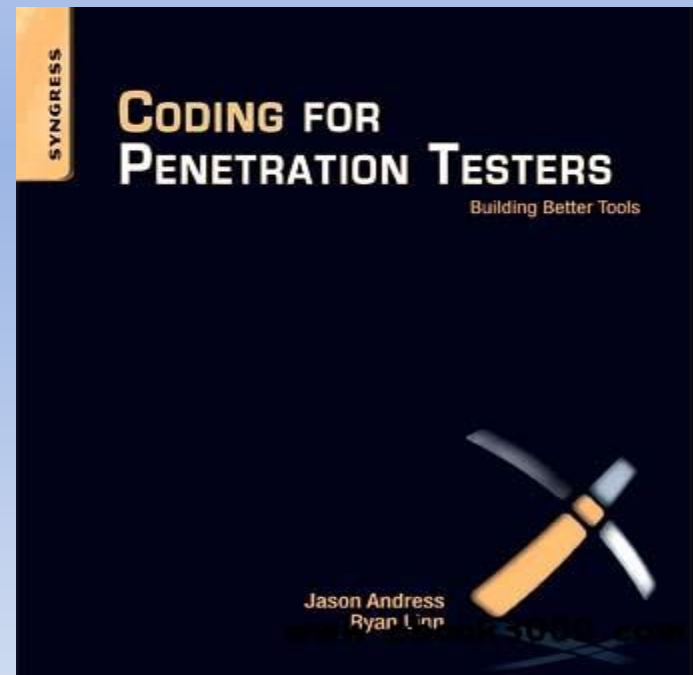
# Sonuç - 2

- Çözümler ihtiyaçlardan doğar.



# Kaynak

- <http://www.syngress.com/hacking-a>



# Sorular ???

## Teşekkürler

Gökhan ALKAN

2013/03/06

<http://www.galkan.net/>