Temel Network Pentest'e Giriş

Ahmet GÜREL
www.gurelahmet.com

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

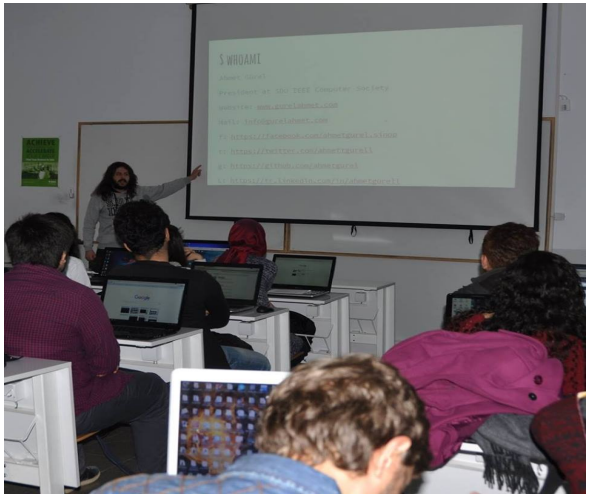
HAKKIMDA

Ahmet GÜREL

Cyber Security Researcher

President at SDU IEEE Computer Society

Suleyman Demirel University Computer Engineering



LinkedIn : www.linkedin.com/in/ahmetgurell

@ahmettgurell

MAIL

info@gurelahmet.com

ahmetgurel.yazilim@gmail.com

Blog: www.gurelahmet.com

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

Eğitim 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

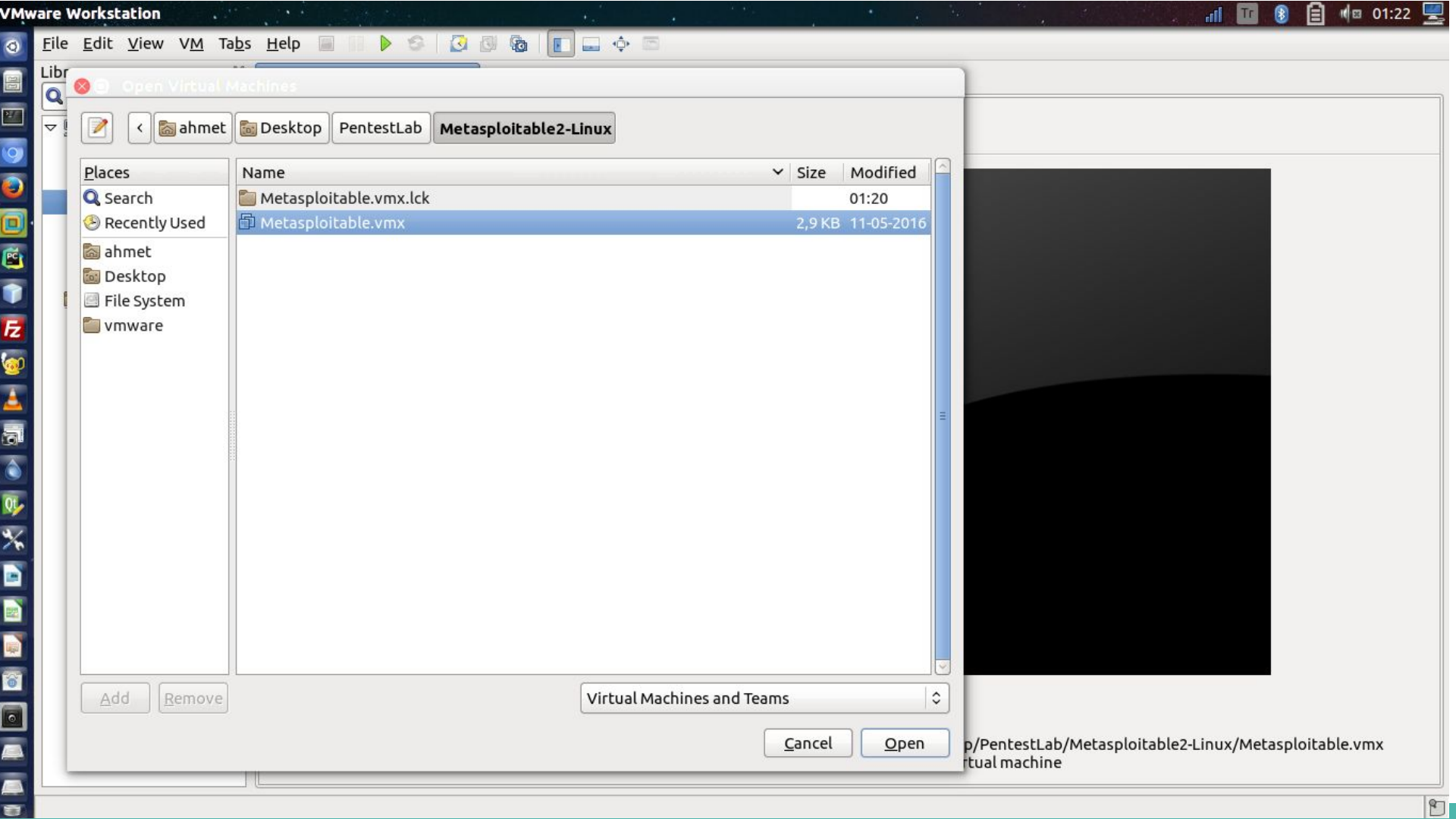
-Temel Metasploit Kullanımı

-Açıklık Tarama Araçları Kullanımı

-Uygulamalı Sızma Testi Örnekleri

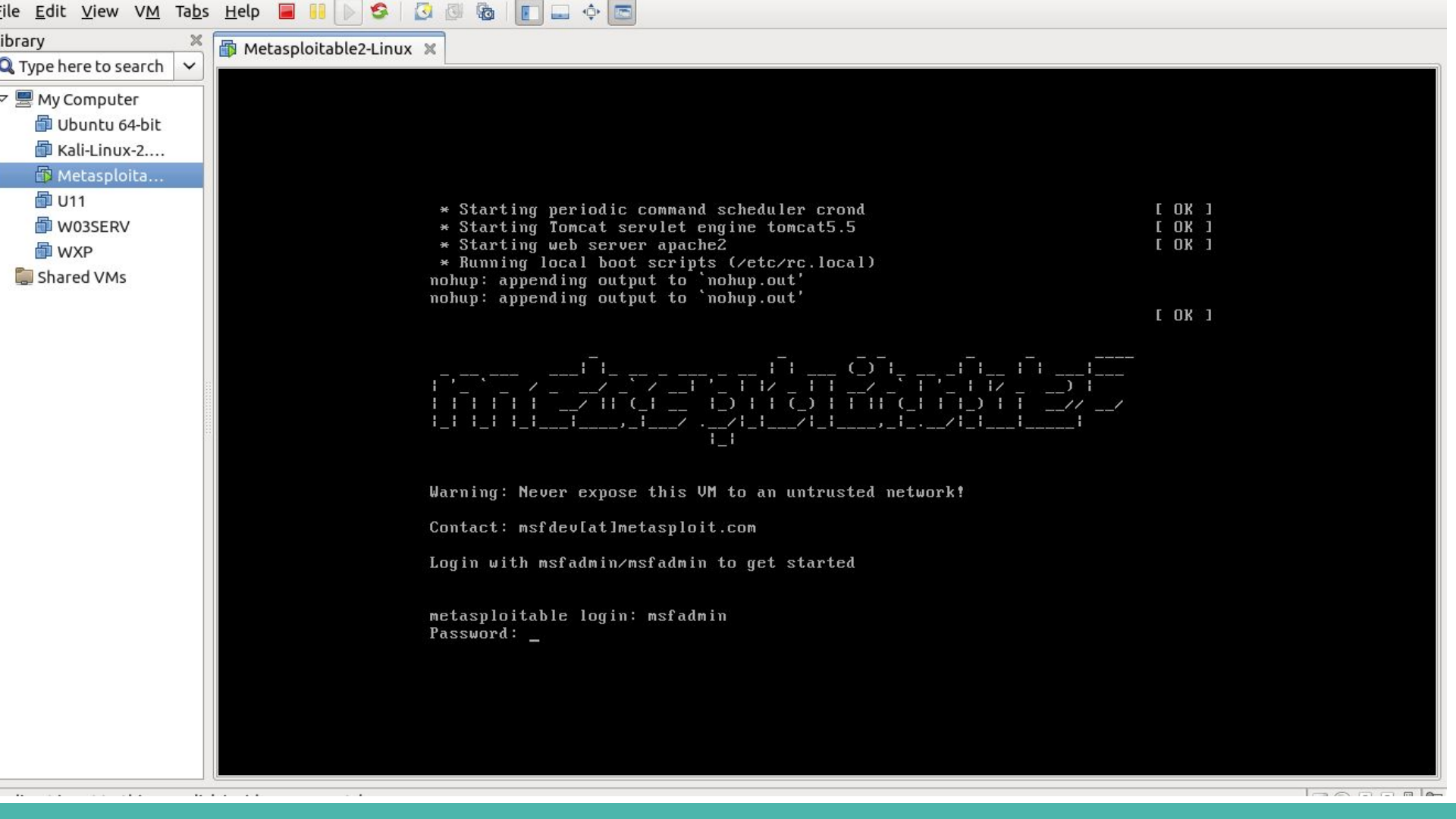
VMware Üzerine Kali ve Metasploitable2 Kurulumu

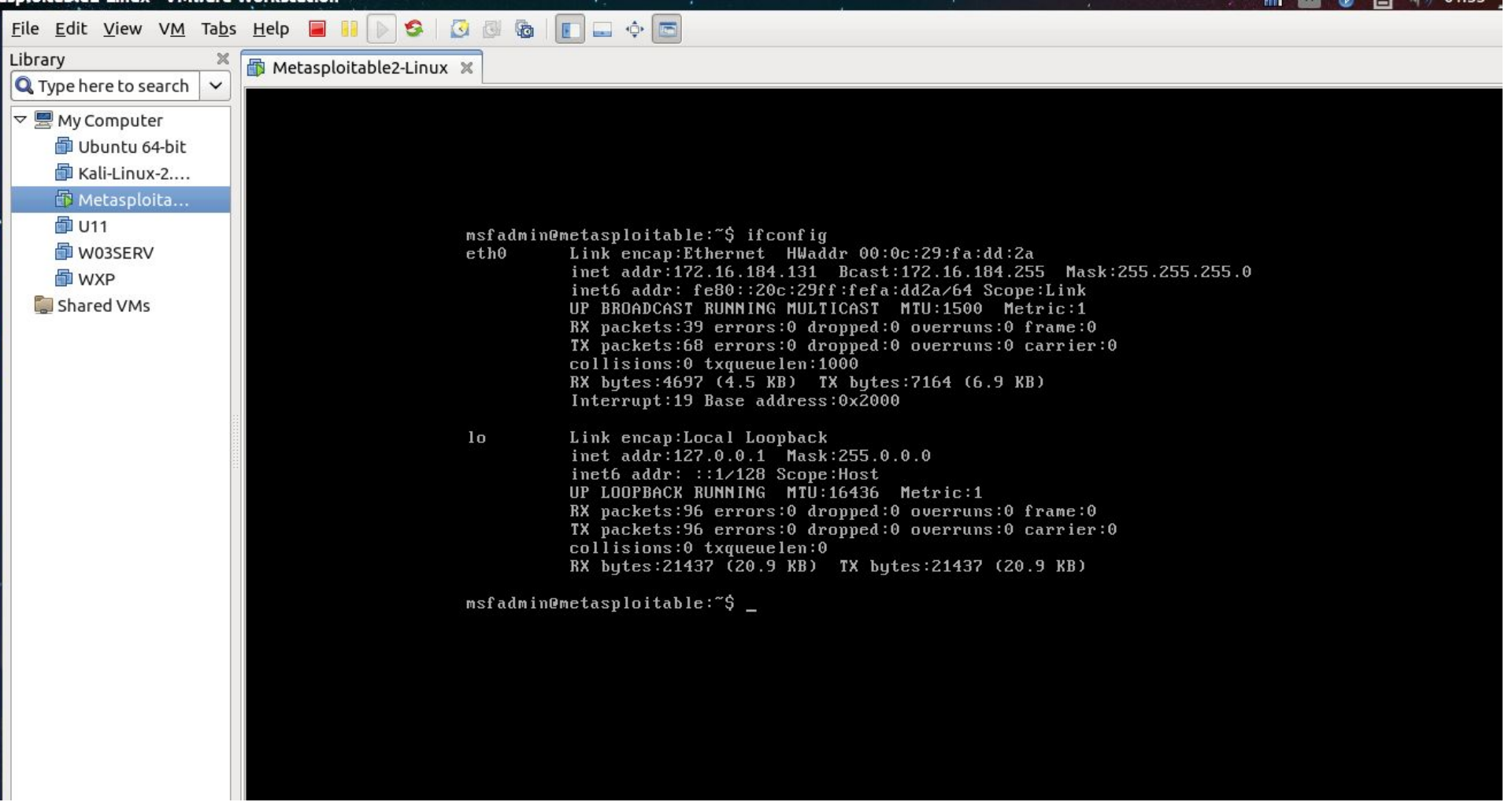
Öncelikle Metasploitable2 de kuracağımız için VMware sanallaştırma yazılımını kullanmanız gerekmekte.Ücretsiz versiyonu Playerin setupını googledan rahatlıkla bulunabilmekte.İndirip VMware i kurduktan sonra https://www.kali.org/downloads/ adresinden Kalinin iso dosyasını indirmeniz gerekmektedir.Bundan 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.


VMware Workstation
01:22
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

WMware üzerine Metasploitable2 yi import ettikten sonra çalıştırıyoruz ve gelen terminalde username kısmına **msfadmin** ve password kısmınada **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.


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
Metasploitable2-Linux
* Starting periodic command scheduler crond [OK]
* Starting Tomcat servlet engine tomcat5.5 [OK]
* Starting web server apache2 [OK]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
[OK]
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:


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
Metasploitable2-Linux
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a
inet addr:172.16.184.131 Bcast:172.16.184.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:39 errors:0 dropped:0 overruns:0 frame:0
TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4697 (4.5 KB) TX bytes:7164 (6.9 KB)
Interrupt:19 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$ _

Warning: Never expose this VM to an untrusted network!

Contact: 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 çalışacaz bunun içinde bir adet saldırgan makina yani Kali Linux kurmamız gerekmekte.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.

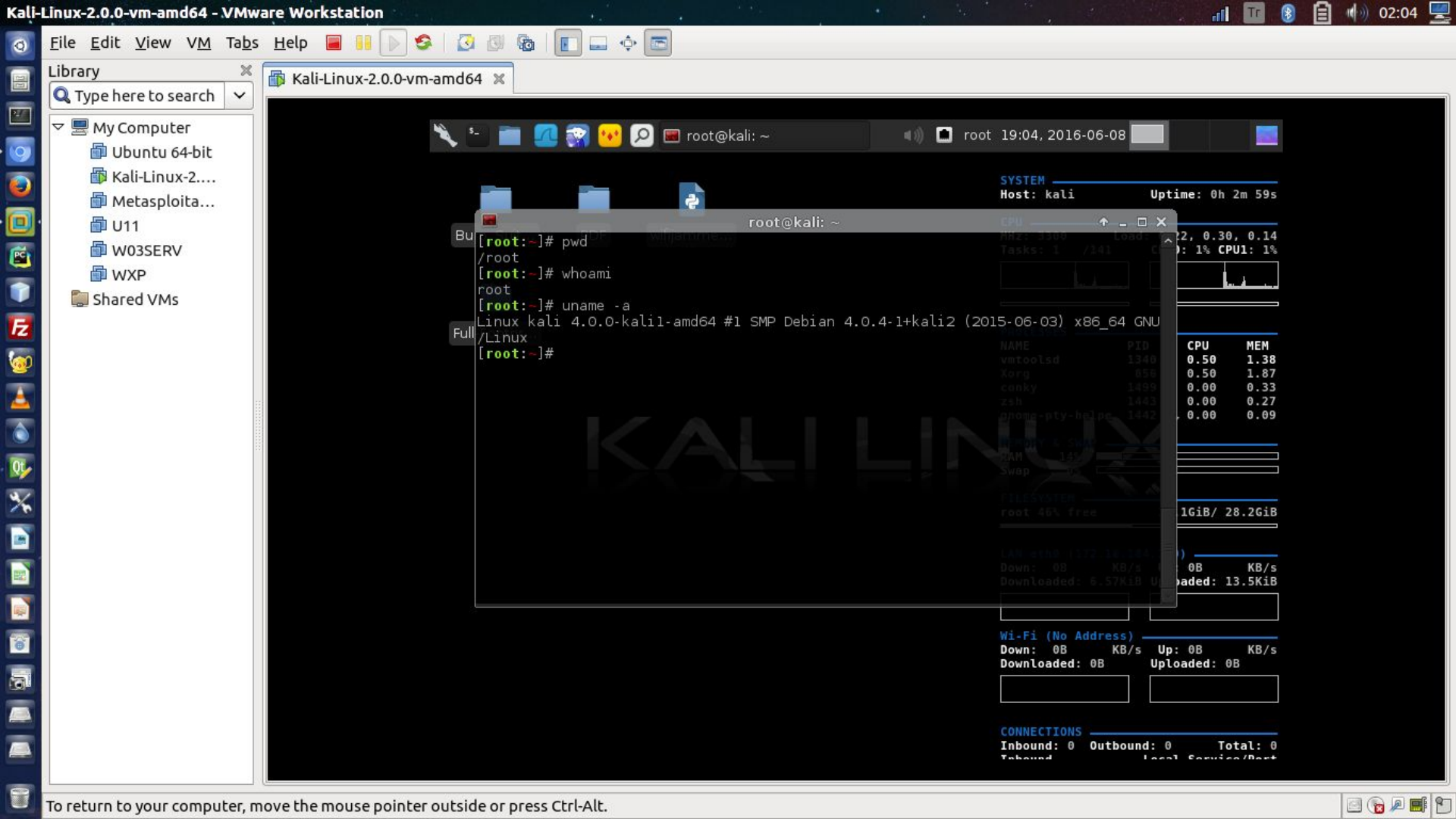
Temel Linux Sistem Bilgisi

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 : Bulunduğunuz dizini verir.

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

uname -a : Bulunduğunuz 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
root@kali: ~
root 19:04, 2016-06-08
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
MEM
vmtoolsd 0.50 1.38
Xorg 0.50 1.87
conky 0.00 0.33
zsh 0.00 0.27
0.00 0.09
Wi-Fi (No Address)
Down: 0B KB/s
Up: 0B KB/s
Downloaded: 0B
Uploaded: 0B
CONNECTIONS
Inbound: 0
Outbound: 0
Total: 0

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 gerçekleştirmek 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?

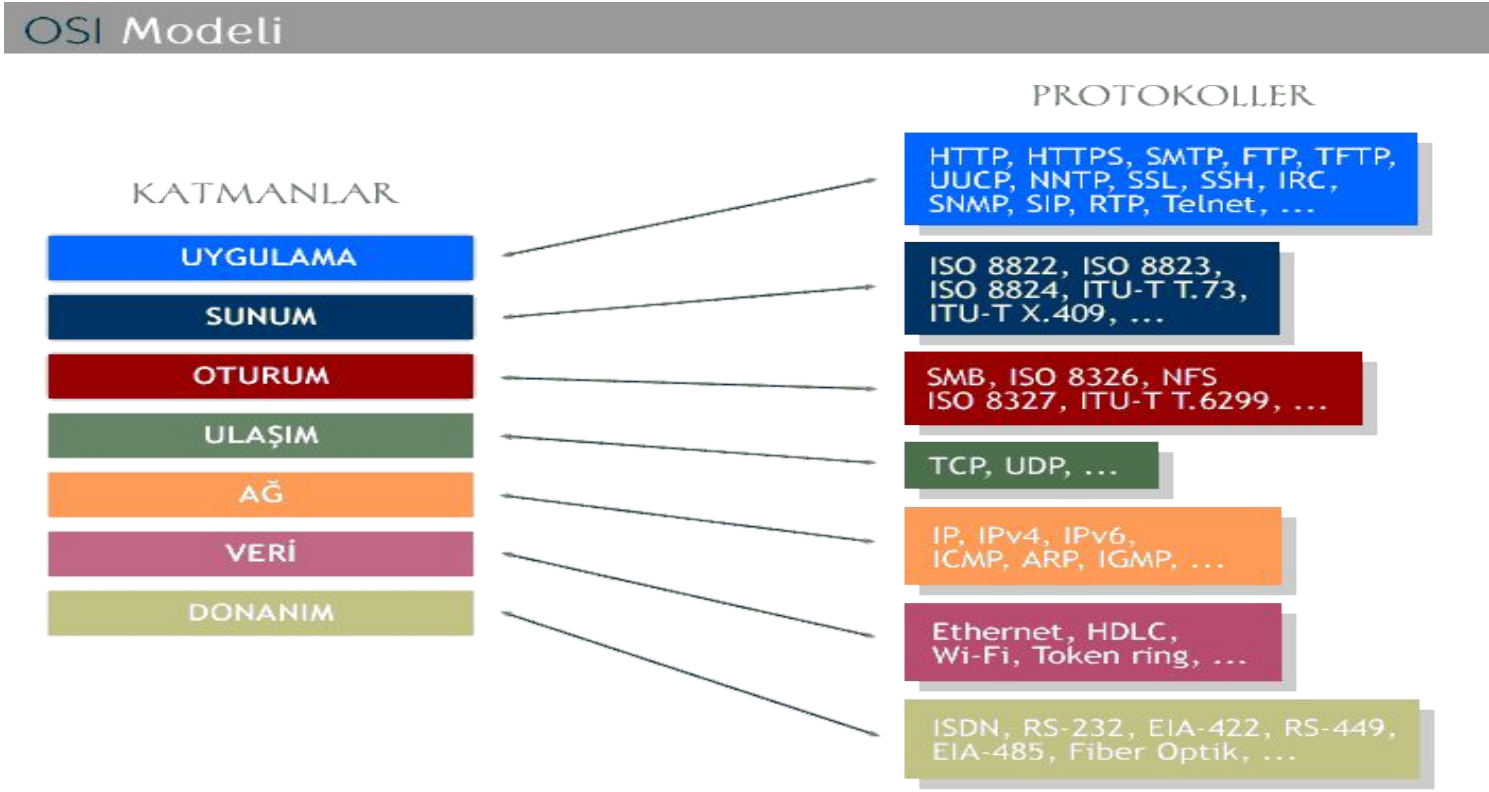
IP adresi (İngilizce: Internet Protocol Address), interneti ya da TCP/IP protokolünü kullanan diğer paket anahtarlamalı ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adres.

DNS Nedir?

Türkçe olarak Alan Adı Sistemi olan DNS girdiğimiz sitelerin IP adresini tutan bir adres defteri gibidir.Girdiğimiz bir domain tıkladığımızda kullandığımız DNS bizi yönlendirdiği için bazen ulaşamama durumları oluyor farklı nedenlerden o IP yı engellıyorlar 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 geliştirimiştir. **Bu modelle, ağ farkındalığına sahip cihazlarda çalışan uygulamaların birbirleriyle nasıl iletişim kuracakları tanımlanır.**



Temel Network Bilgisi | OSI MODELİ

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

Network haberleşmelerinde OSI Referans modeli kullanılır.

Katmanlarda çalışan donanımlara ve protokollere iler ki sunumlarda bulunmaktadır.

Temel Network Bilgisi | OSI MODELİ

Terminal A

Terminal B

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

Temel Network Bilgisi | TCP/IP

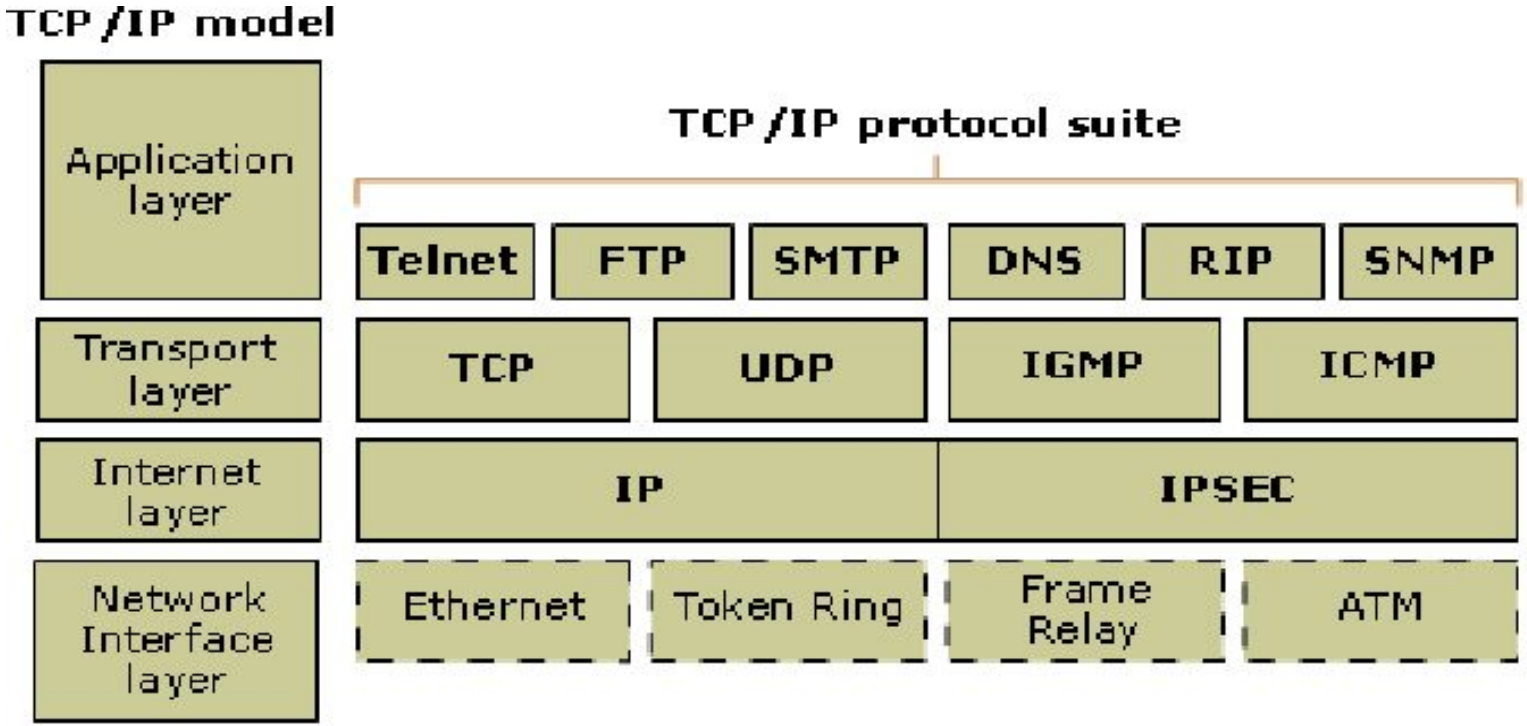
Tarihçe:

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



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?

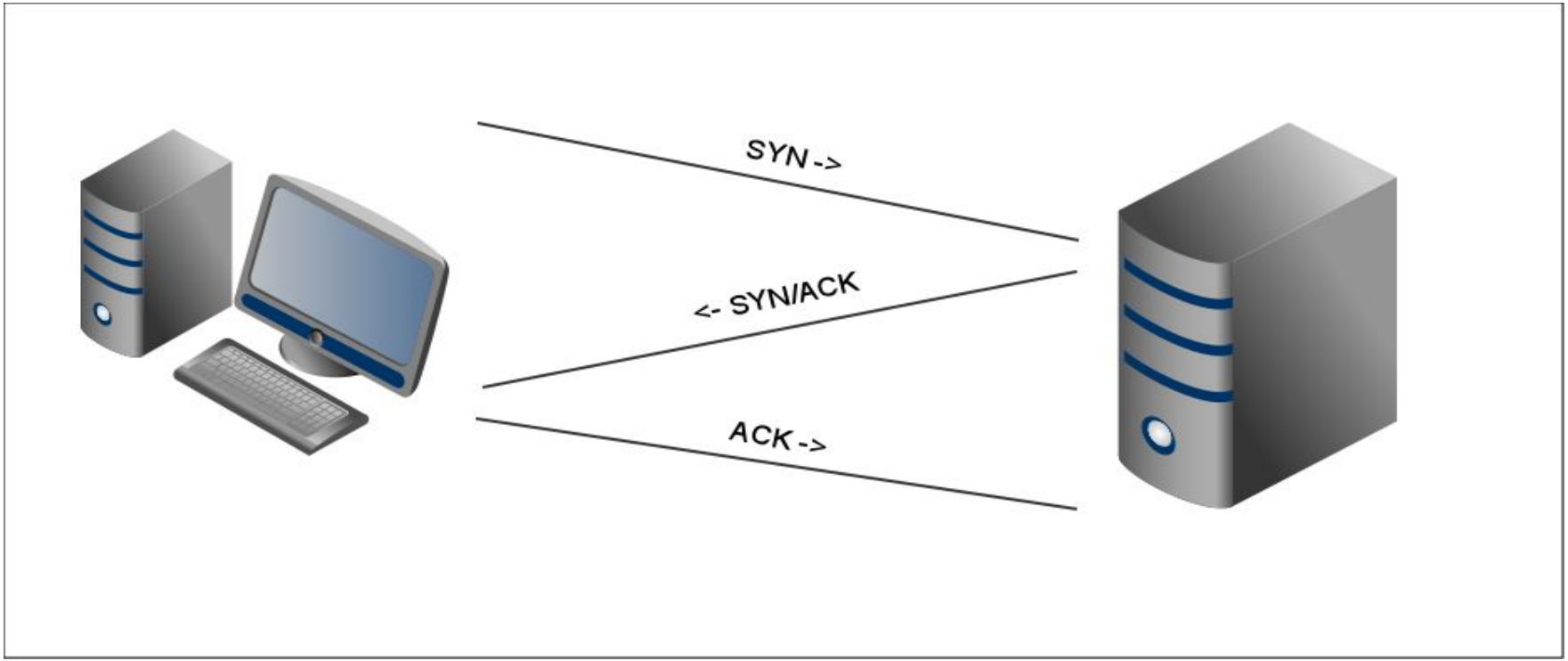
A bilgisayarı B bilgisayarına TCP yoluyla bağlanmak istediğinde şu yol izlenir:

- 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

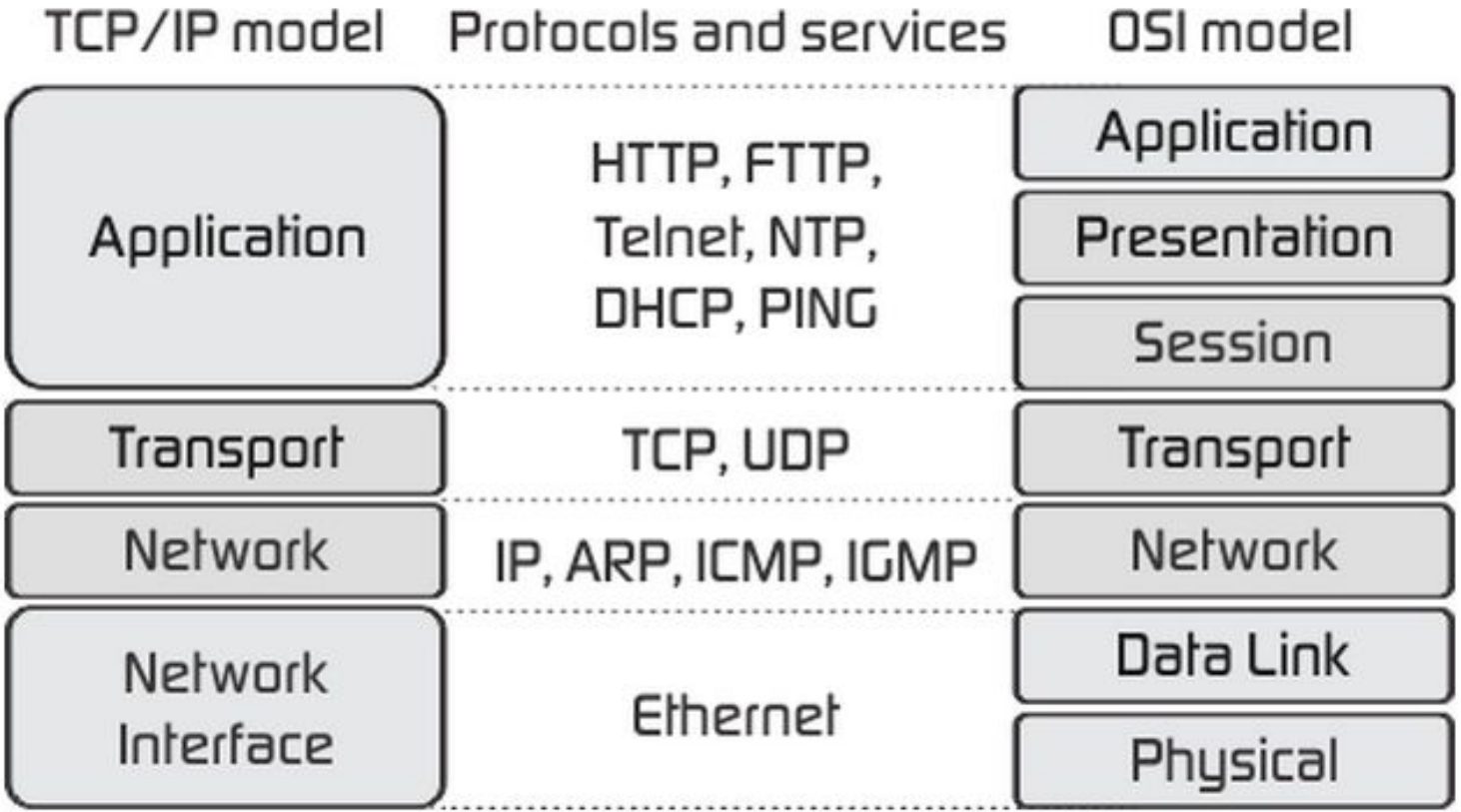
Veri iletişimi bitince bilgisayarlardan herhangi biri diğerine TCP kapatma mesajı yollar. Diğer bilgisayar, kapatmayı teyid etme paketi ve kapatma isteği yollar. Son olarak, diğer bilgisayar da kapatma teyidini yollar ve bağlantı kapatılmış olur.

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 ani 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 alabilir.

Temel Network Bilgisi | ÖNEMLİ PORTLAR

- 21 FTP
- 22 SSH
- 23 TELNET
- 25 SMTP
- 53 DNS
- 80 HTTP
- 110 POP3
- 115 SFTP
- 135 RPC
- 143 IMAP

194 IRC
443 SSL
445 SMB
1433 MSSQL
3306 MYSQL
3389 Remote Desktop

Temel Network Bilgisi | IP ADRESLEME

- 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

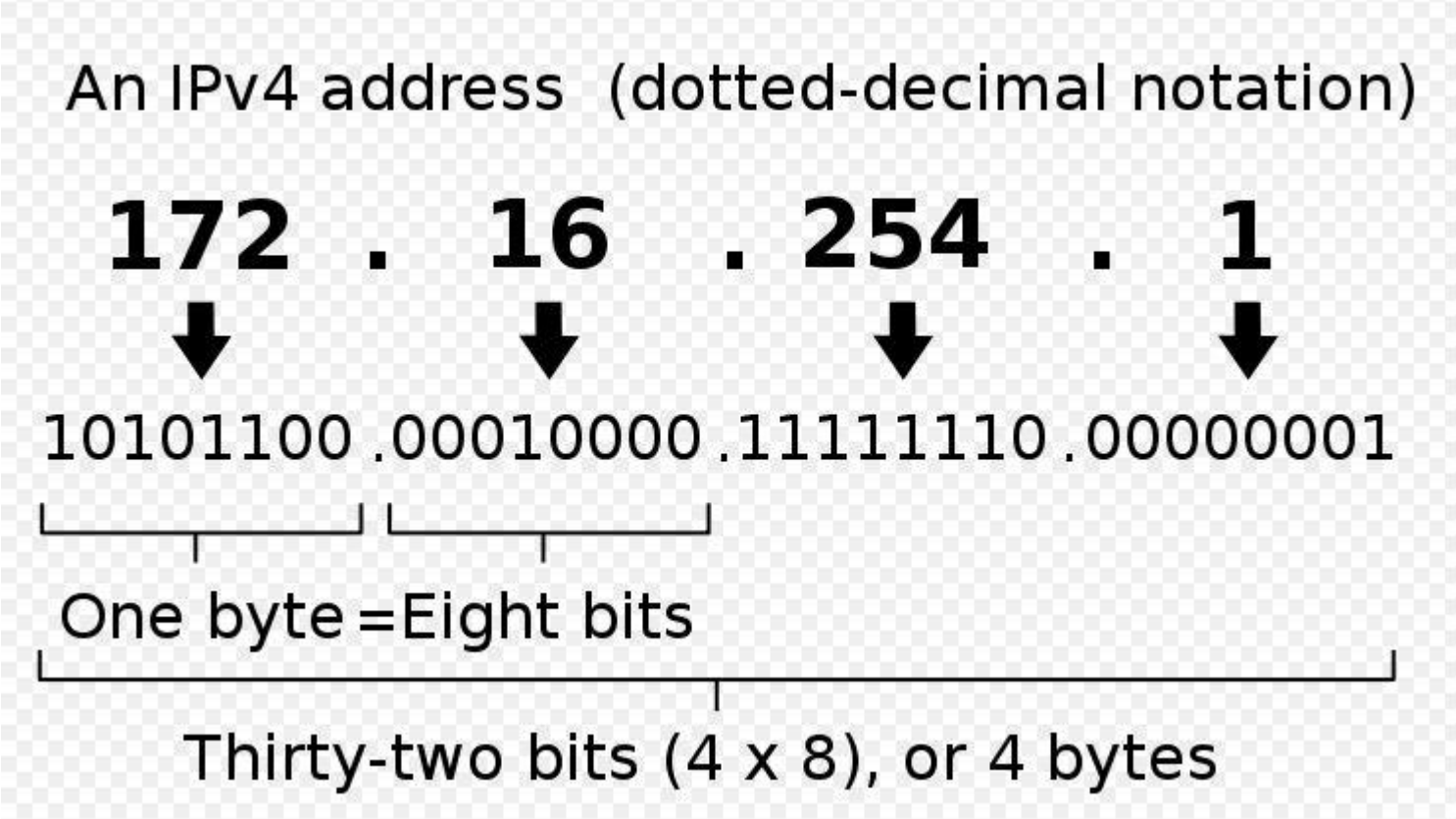
IPv4 Adresleme:

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:



Temel Network Bilgisi | IP ADRESLEME

IPv4 Adres Sınıfları:

A sınıfı adresler : 1-126

B sınıfı adresler : 128-191

C sınıfı adresler : 192-223

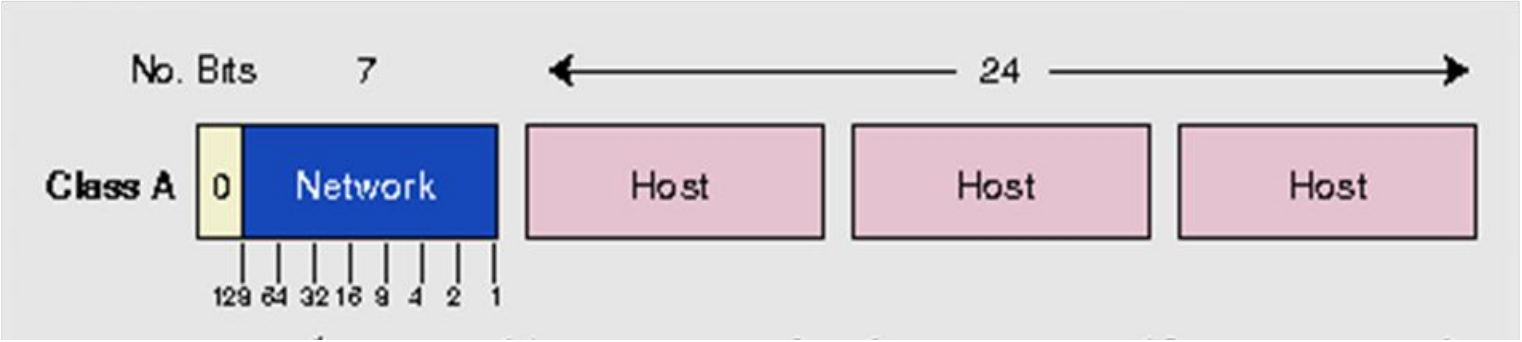
D sınıfı adresler : 224-239

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 Desteği	Opsiyonel	Zorunlu
Adres Çözümleme Protokolü	ARP, Broadcast kullanarak istekleri link-layer adresine çözümler.	ARP istek frame'leri, multicast Neigbor Solicitaion mesajları ile değişir.
IGMP	Lokal subnet grup üyeliklerini yönetir.	IGMP, MLD mesajları ile değişmiştir.
ICMP Router Discovery	Default Gateway'in IP adresini tespit eder.	ICMP Router Solicitation ve Router Advertisement mesajları ile değişmiştir.
Broadcast Adresleri	Subnet üzerindeki tüm düğümlere trafiği 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 değildir.
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 (boardcast) şeklinde iletir. Bu yüzden fiziksel katmana dahildir.

Temel Network Bilgisi | NETWORK CİHAZLARI

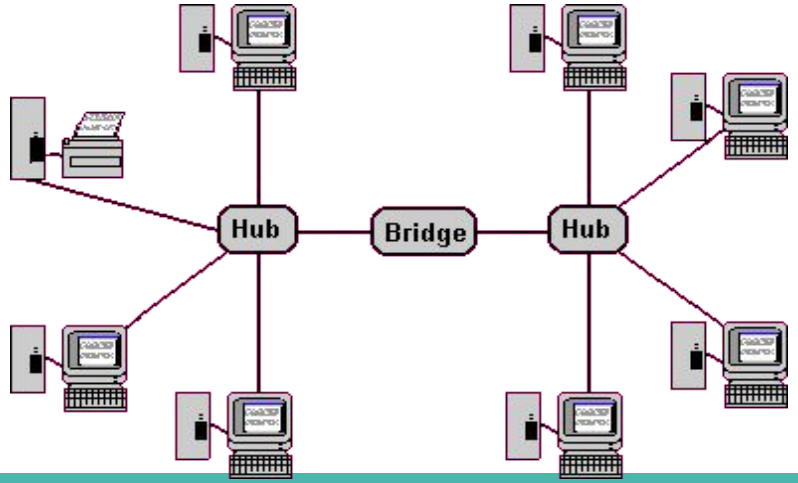
Switch (Network Anahtarı)

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 sağlanır.



Temel Network Bilgisi | NETWORK CİHAZLARI

Router (Yönlendirici)

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

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

Acces Point (Erişim Noktası)

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

Temel Network Bilgisi | NETWORK CİHAZLARI

Modem

Modem, bilgisayarların genel ağa bağlantısını sağlayan ve bir bilgisayarı uzak yerlerdeki bilgisayarlara bağlayan 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 dökumanını okuyabilirsiniz : https://drive.google.com/viewerng/viewer?url=http://alikoker.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.

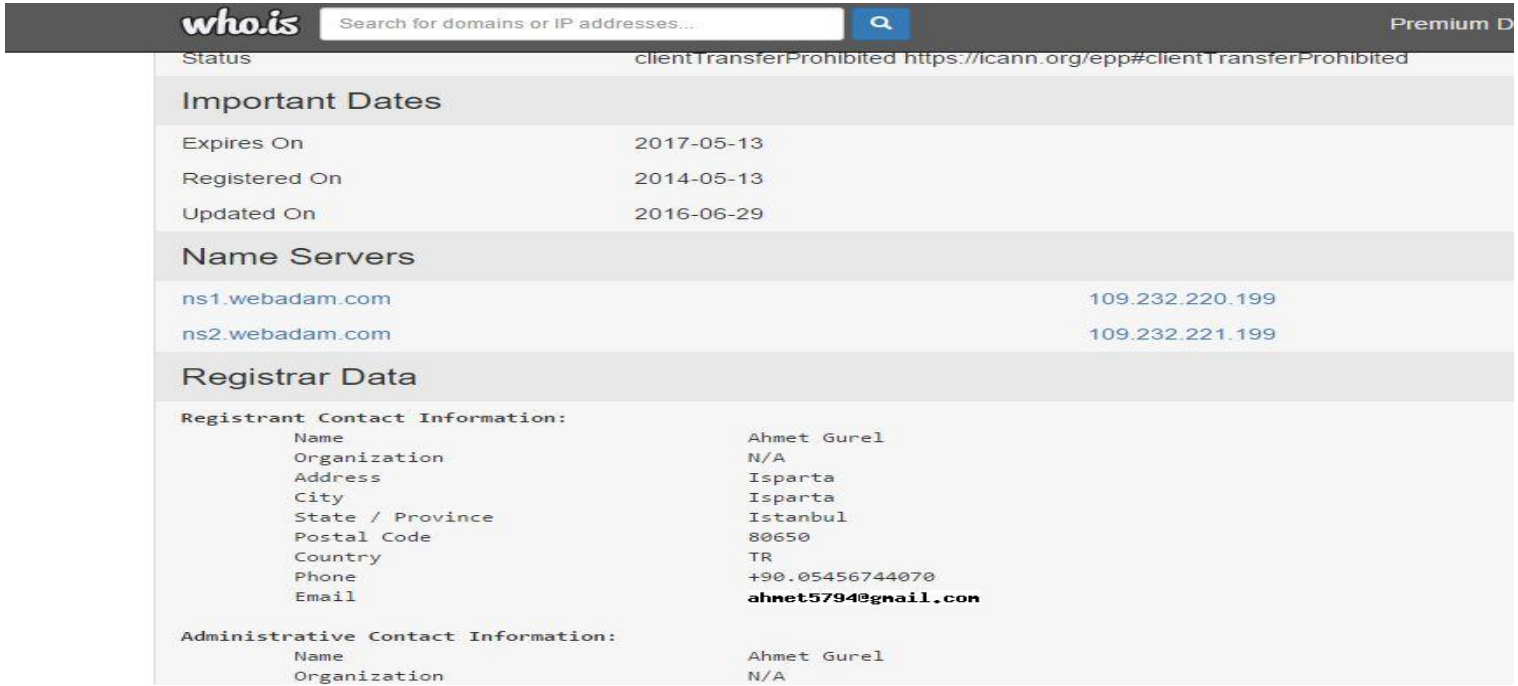
Şimdi bu bilgi toplama yöntemlerini ve toollarını beraber inceleyeceğiz.

Bilgi Toplama | Pasif Bilgi Toplama

1-whois Bilgileri

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

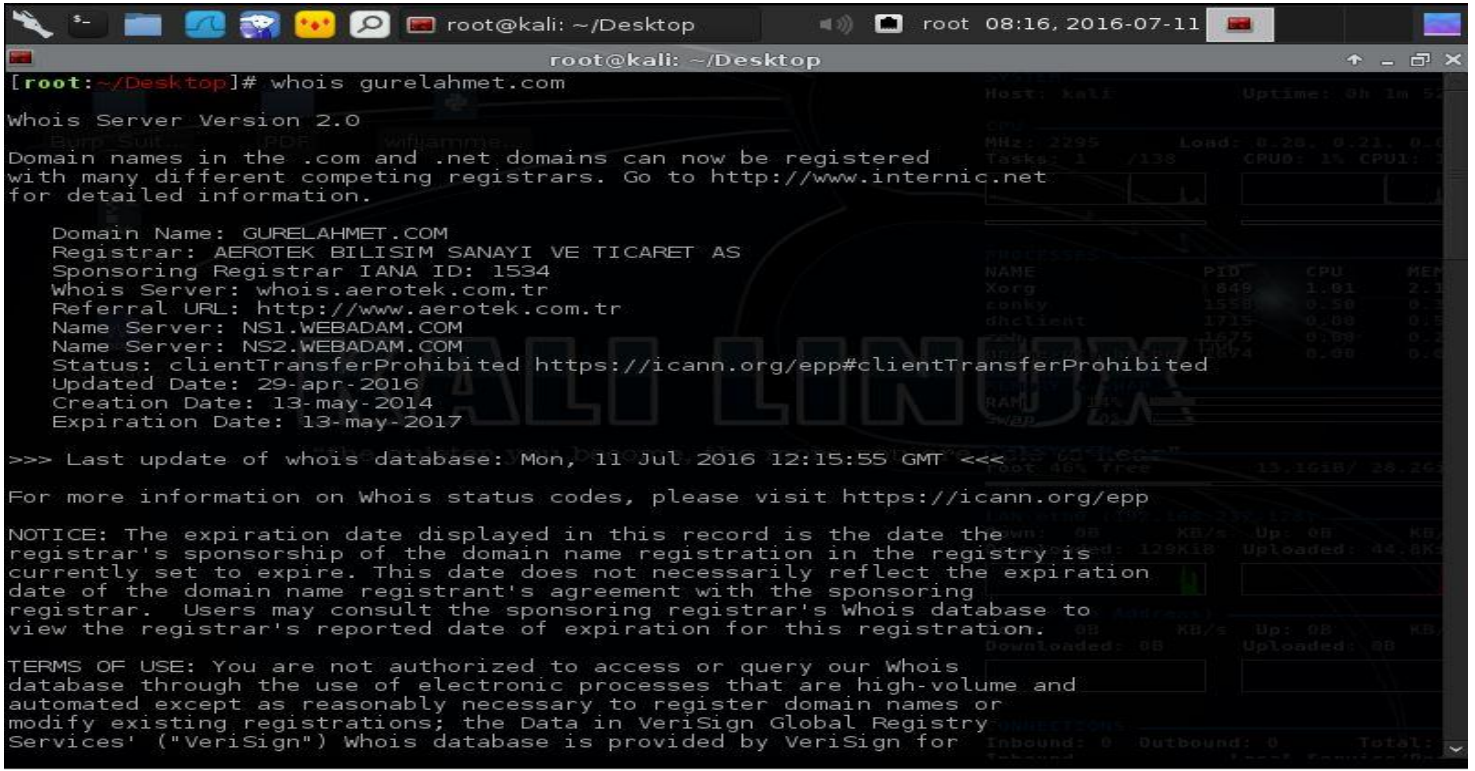
Bilgi Toplama | Pasif Bilgi Toplama



https://who.is/ sitesindewww.gurelahmet.com Sorgulaması

Bilgi Toplama | Pasif Bilgi Toplama

whois Komutu Kullanımı



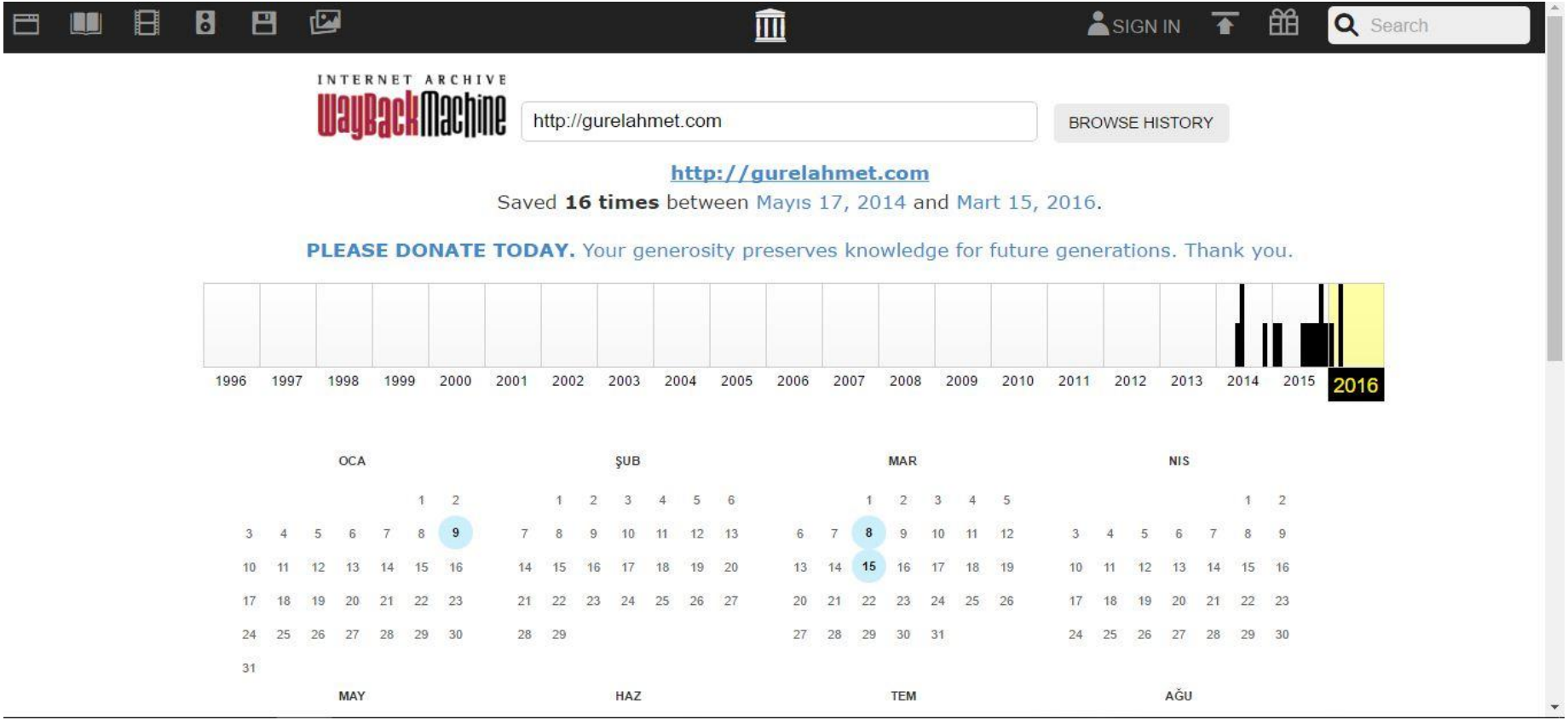
Bilgi Toplama | Pasif Bilgi Toplama

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



Bilgi Toplama | Pasif Bilgi Toplama

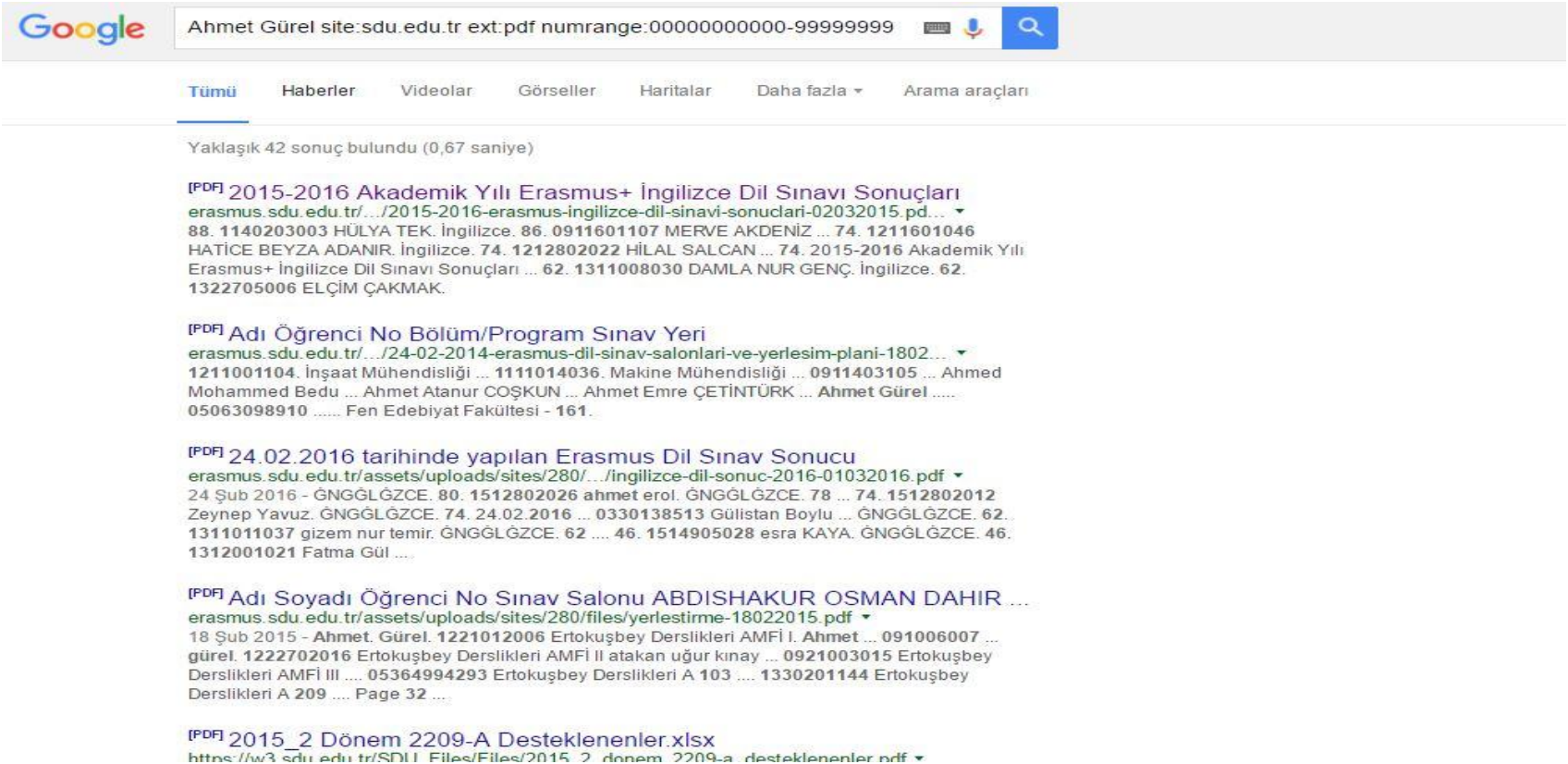
3-Arama Motorları:

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



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 Paylasım Siteleri

Facebook,Twitter,Linkedin,İnstagram,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.robtex.com

Online bilgi toplama araçları :

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

Bilgi Toplama | Aktif Bilgi Toplama

1-theharvester ile Mail ve Subdomain Tespiti

Kalinin 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

Bilgi Toplama | Aktif Bilgi Toplama

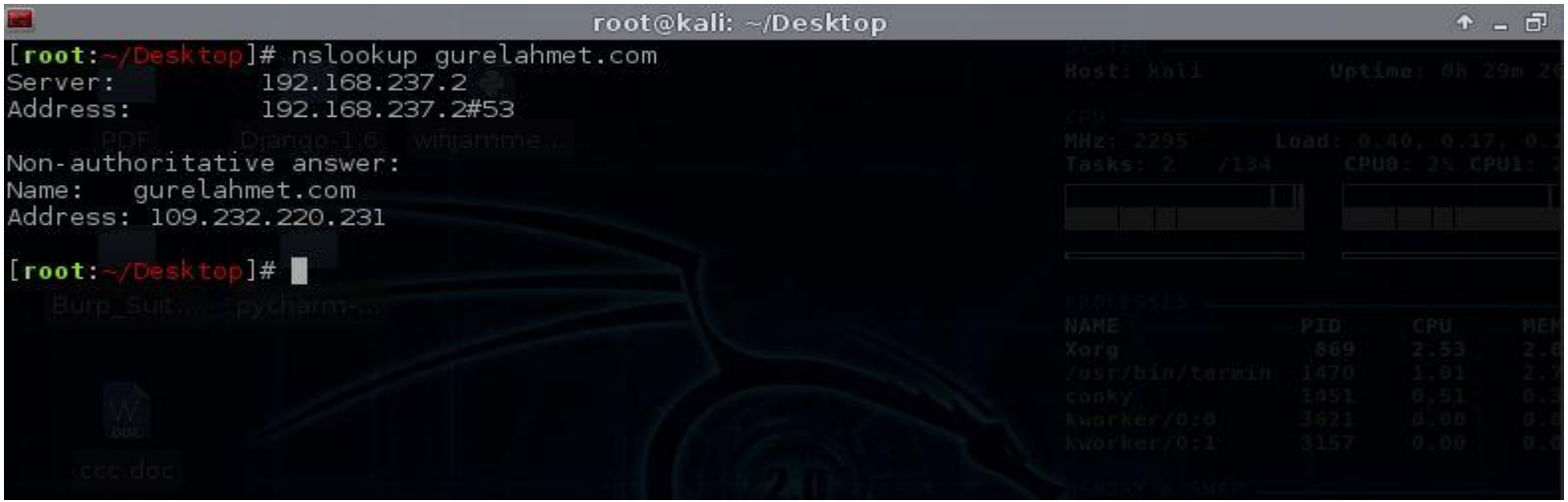
2-traceroute Kullanımı

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

Bilgi Toplama | Aktif Bilgi Toplama

3-Nslookup Kullanımı

DNS sorgulaması yapmamızı sağlayan güzel bir araçtır.

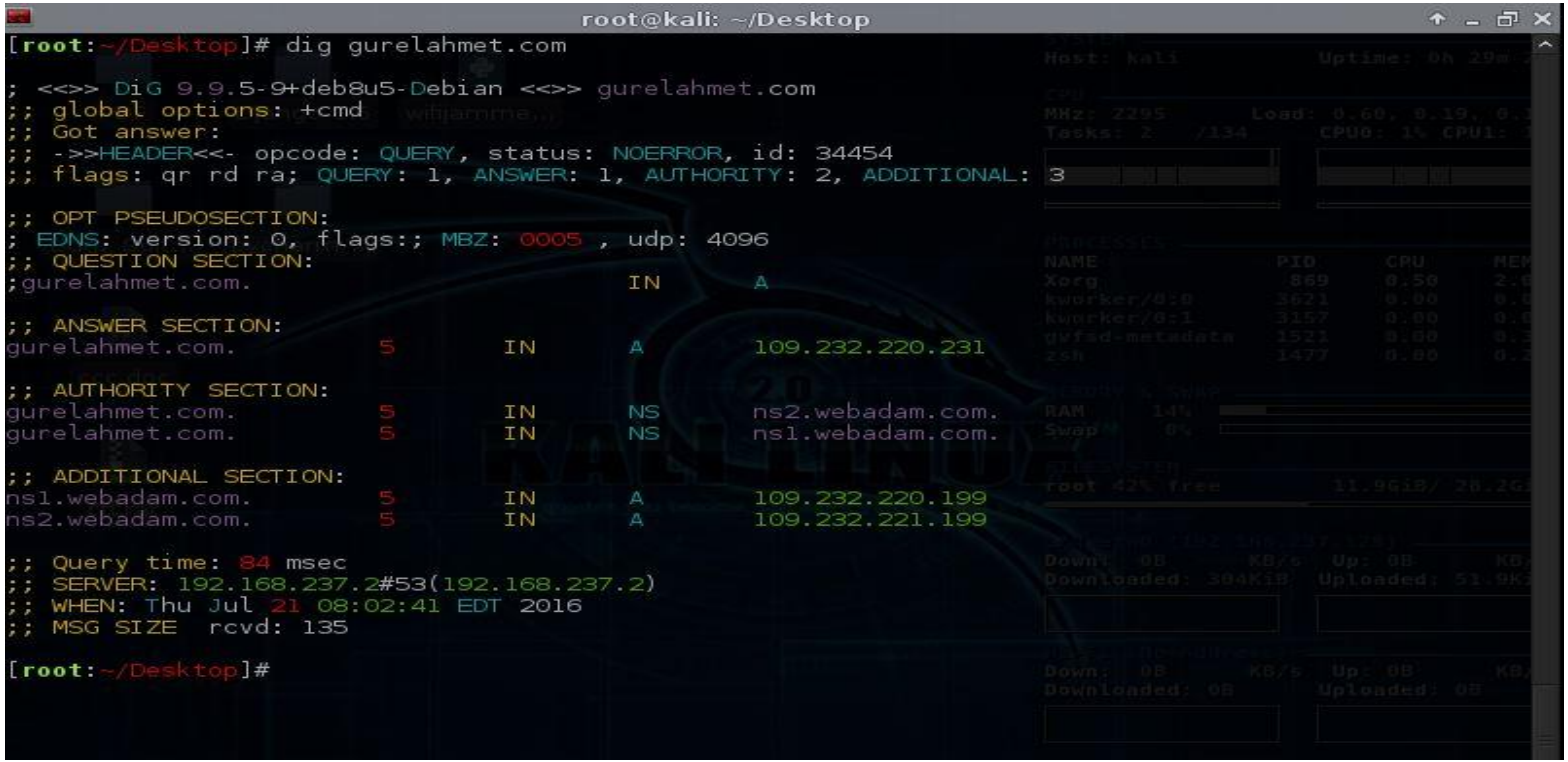


Bilgi Toplama | Aktif Bilgi Toplama

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

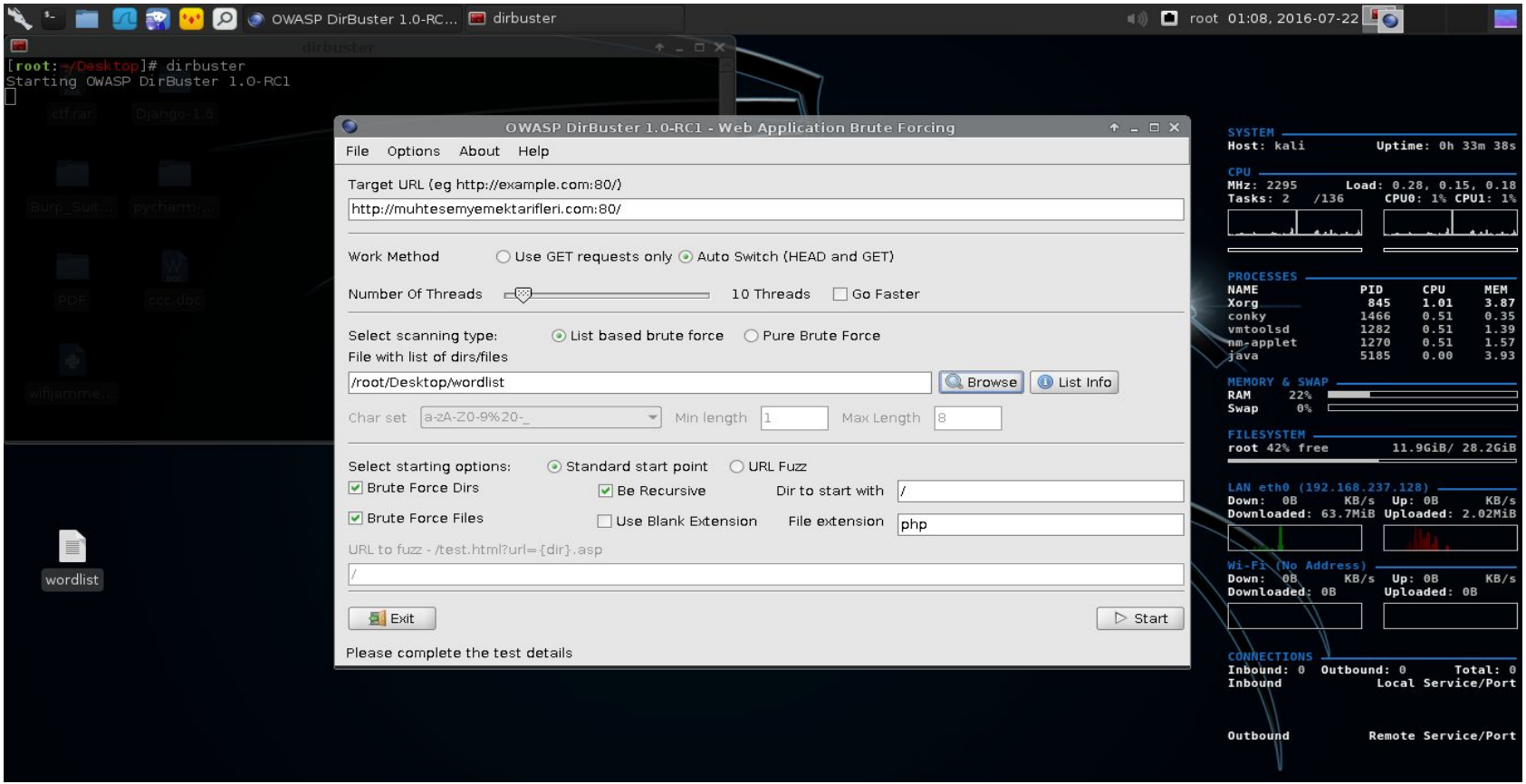


Bilgi Toplama | Aktif Bilgi Toplama

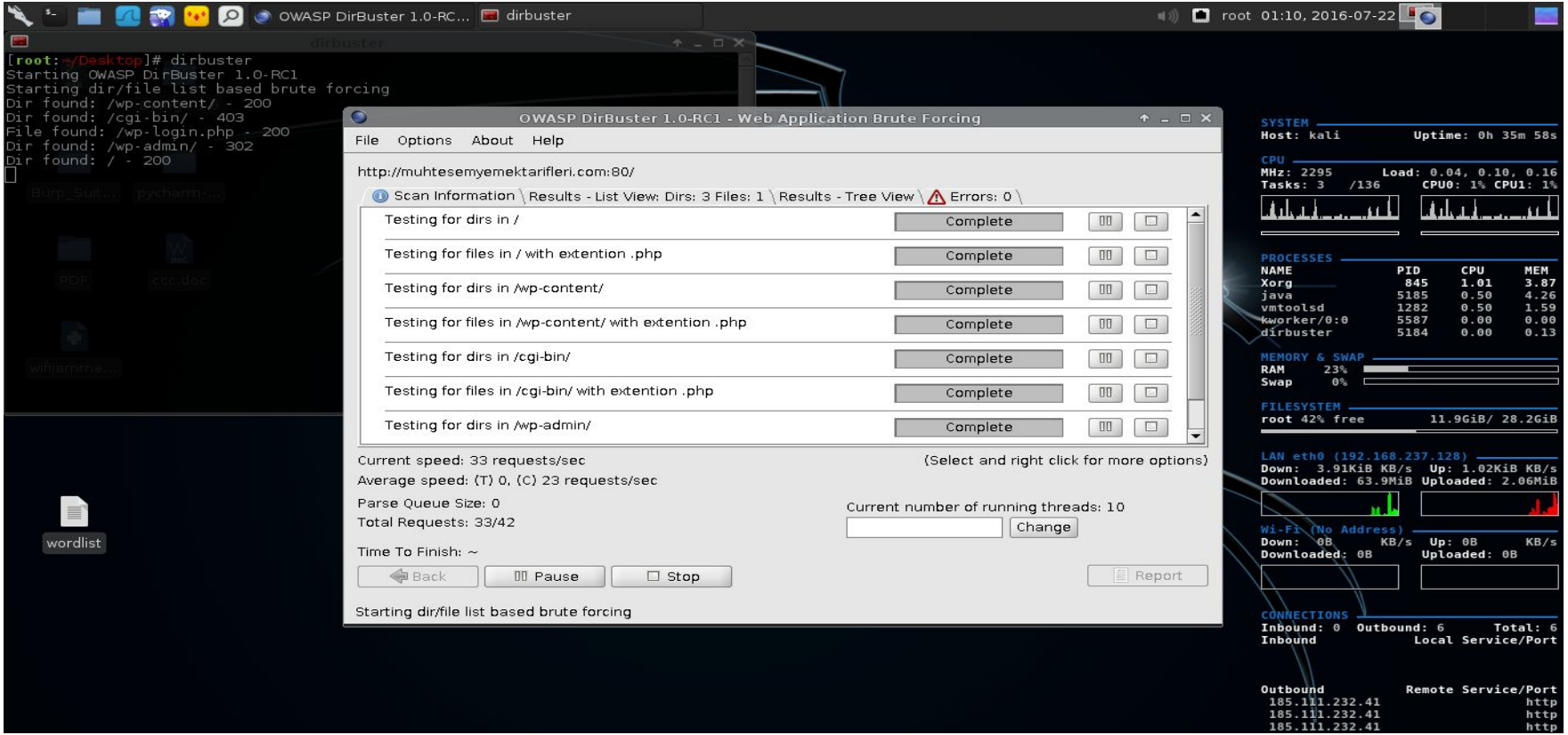
5-dirbuster Kullanımı

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.

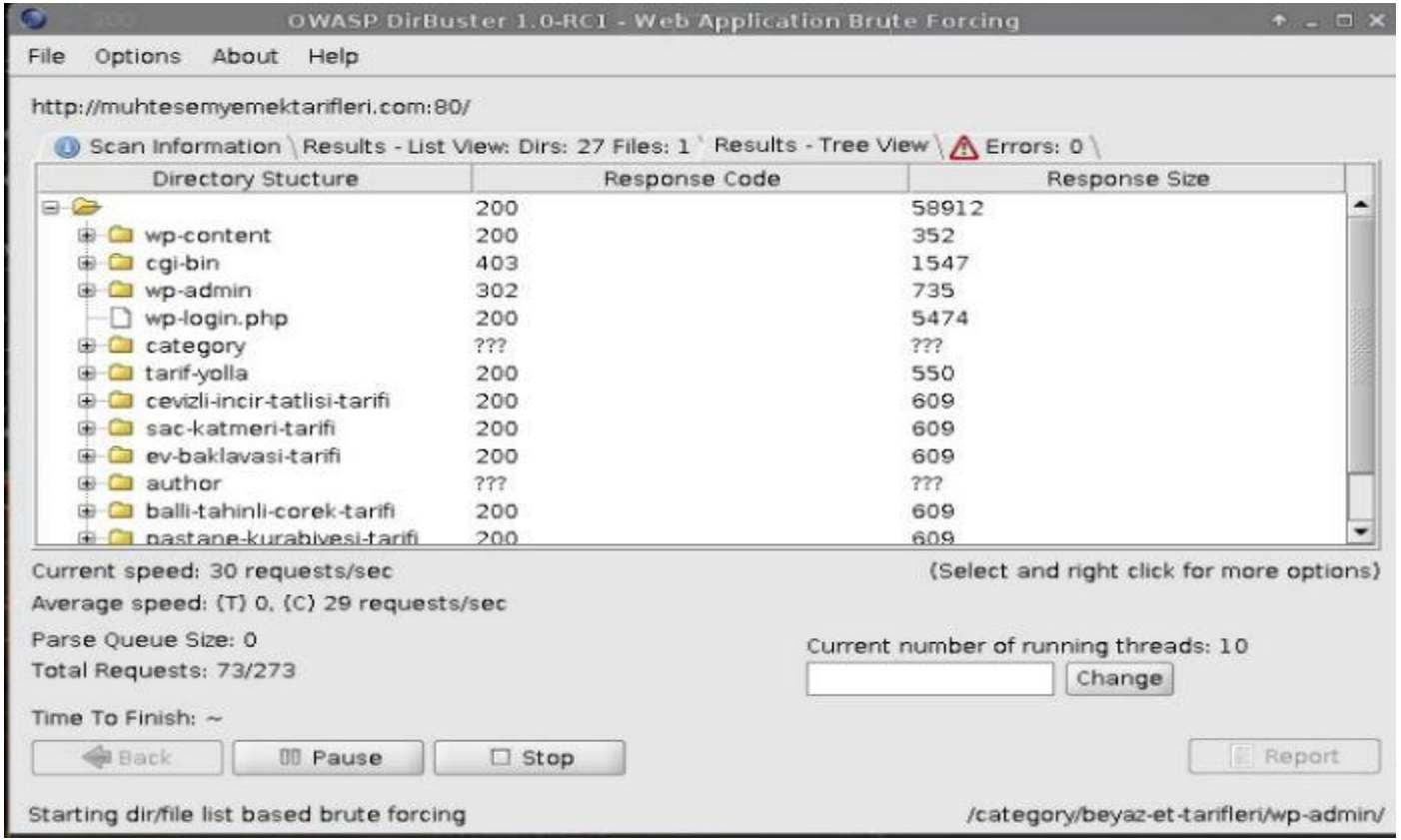
Bilgi Toplama | Aktif Bilgi Toplama



Bilgi Toplama | Aktif Bilgi Toplama



Bilgi Toplama | Aktif Bilgi Toplama



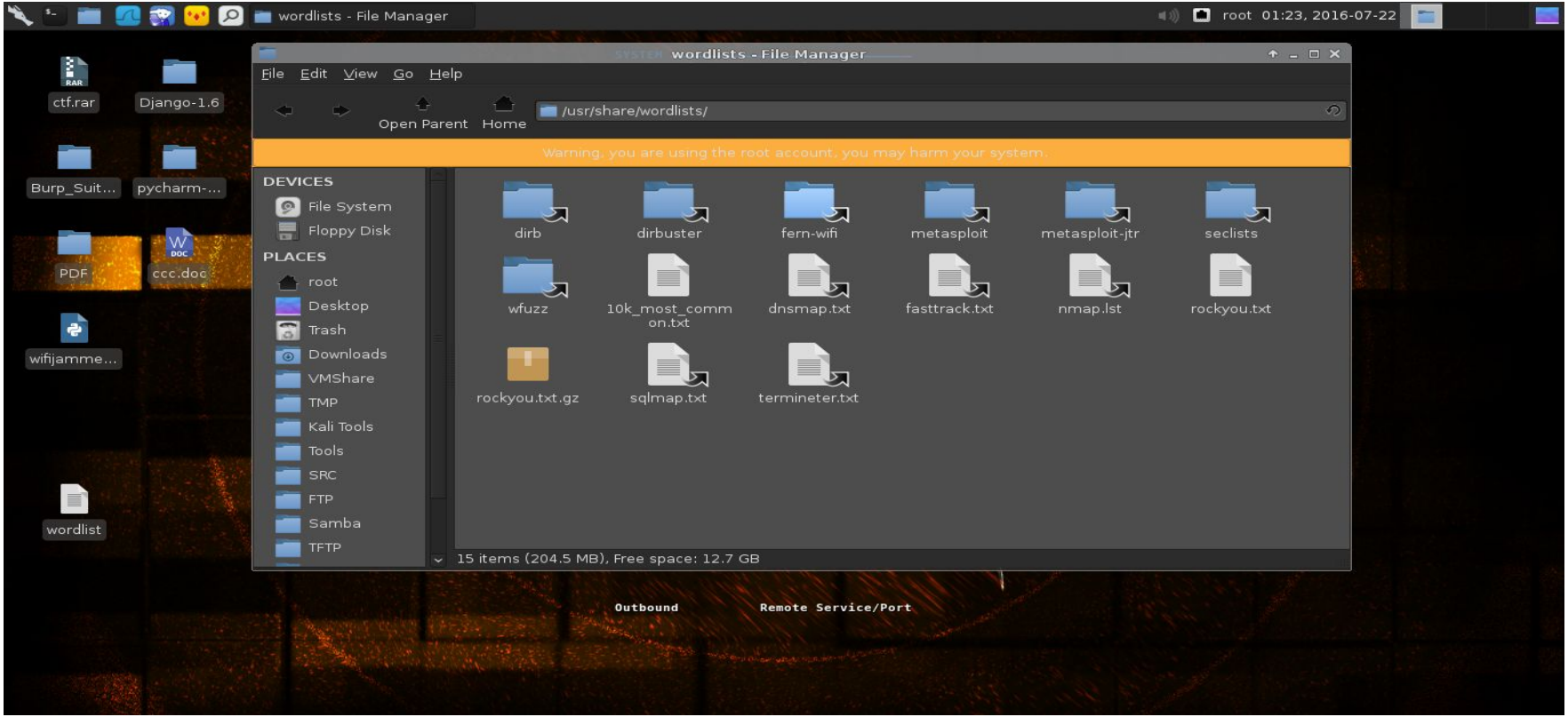
Bilgi Toplama | Wordlist

Bilgi toplamada ve diğer bir çok güvenlik aracı wordlist kullanır ya da ister. Hiç bilgisi olmayanlar için **wordlist** içinde çok sayıda kelime barındıran dosyalar kendiniz bile elle oluşturduğunuz 10-100 kelimelik bir text dosyası wordlist olarak kabul edilir.Şimdi gelelim hedefe uygun işinize yaracak wordlistleri nasıl oluşturup nasıl bulabilirsiniz?

Crunch adlı bir uygulama ile kendi wordlistinizi oluşturabilirsiniz yada

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

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 parametlerini inceleyeceğiz.

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

Temel Nmap Kullanımı | Nmap Dönen Sonuçlar

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

Open(Açık): Portun erişilebilir olduğu üzerinde bir uygulamanın TCP yada UDP baglantısı 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 ın 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 döndürecektir.

Eğer açık portuna gelirse hedef makinadan herhangi bir tepki dönmeyecektir.

nmap -sF -v 192.168.237.129

Temel Nmap Kullanımı | Nmap Tarama Türleri

ACK Scan

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

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

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

nmap -sA -v 192.168.237.129

Temel Nmap Kullanımı | Nmap Tarama Türleri

Xmas Scan

Kaynak bilgisayarın TCP segmentine URG,PSH ve FIN bayraklarını set edeceği ("1" 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

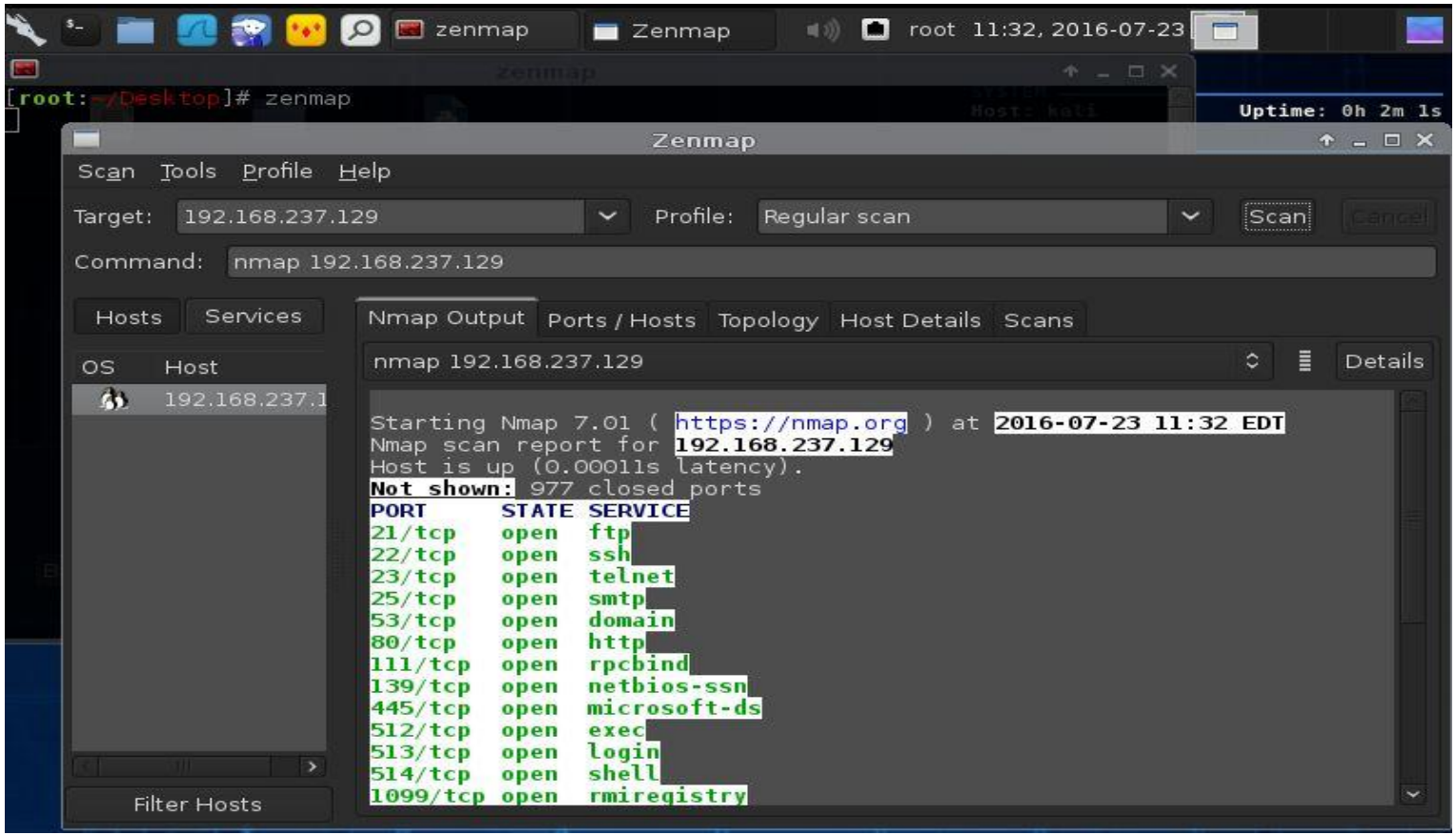
Window Scan, ACK Scan türüne benzer ancak bir önemli farkı vardır.

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

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

nmap -sW -v 192.168.237.129

Temel Nmap Kullanımı | Zenmap



Temel Nmap Kullanımı | Nmap Tarama Örnekleri

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

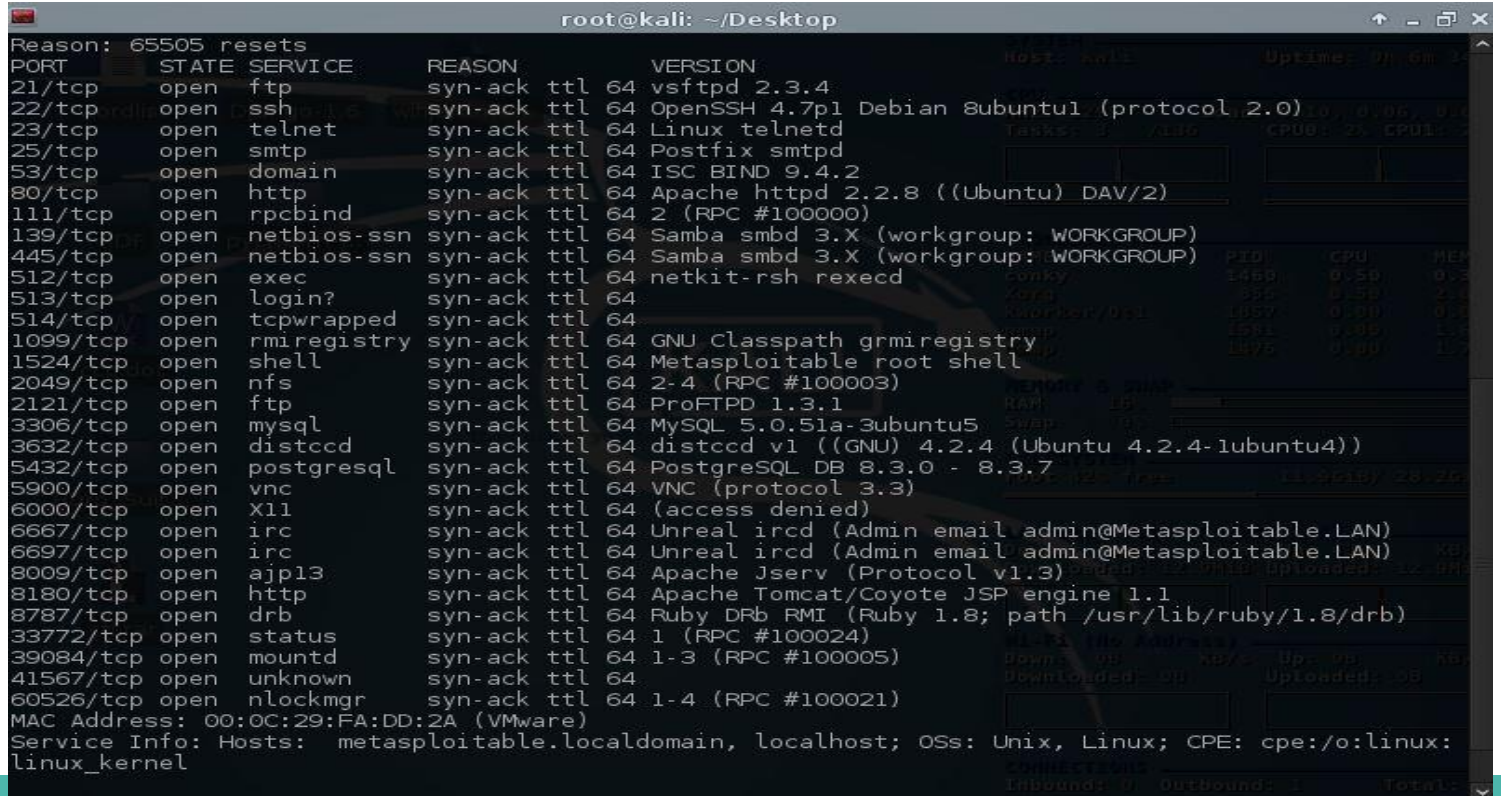
-sS: Syn Taraması **-sV :** Versiyon bilgisi **-Pn:** ping atma **-top-ports10:** en çok kullanılan 10 portu tara

```
[root:~/Desktop]# nmap -sS -sV -Pn -top-ports 10 192.168.237.129

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:37 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00025s latency).
Not shown: 3 closed ports
Reason: 3 resets
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp  open  smtp        syn-ack ttl 64 Postfix 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

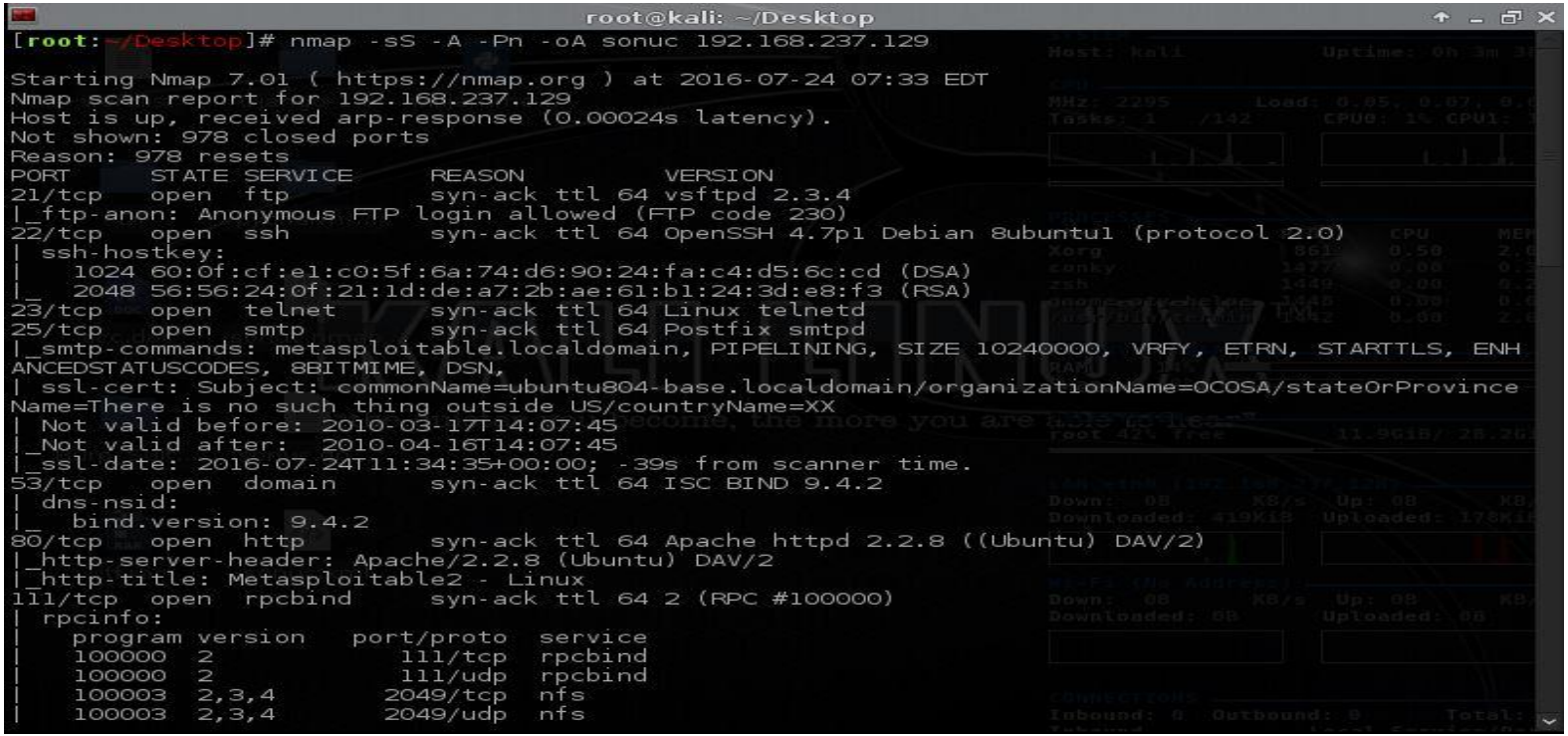
-sS: Syn Taraması **-sV :** Versiyon bilgisi **-Pn:** ping atma**-T4:** Tarama hızı hızlı bir tarama **-p-:** tüm portları tara



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.



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 taramasıda yapılabilmektedir.

Temel Metasploit Kullanımı | Terimler

Vulnerability: Türkçede zayıflık anlamına gelen sistemde bulunan açıklıktır.

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

Exploit: Türkçesi sömürmek olan sistem açıklığından 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

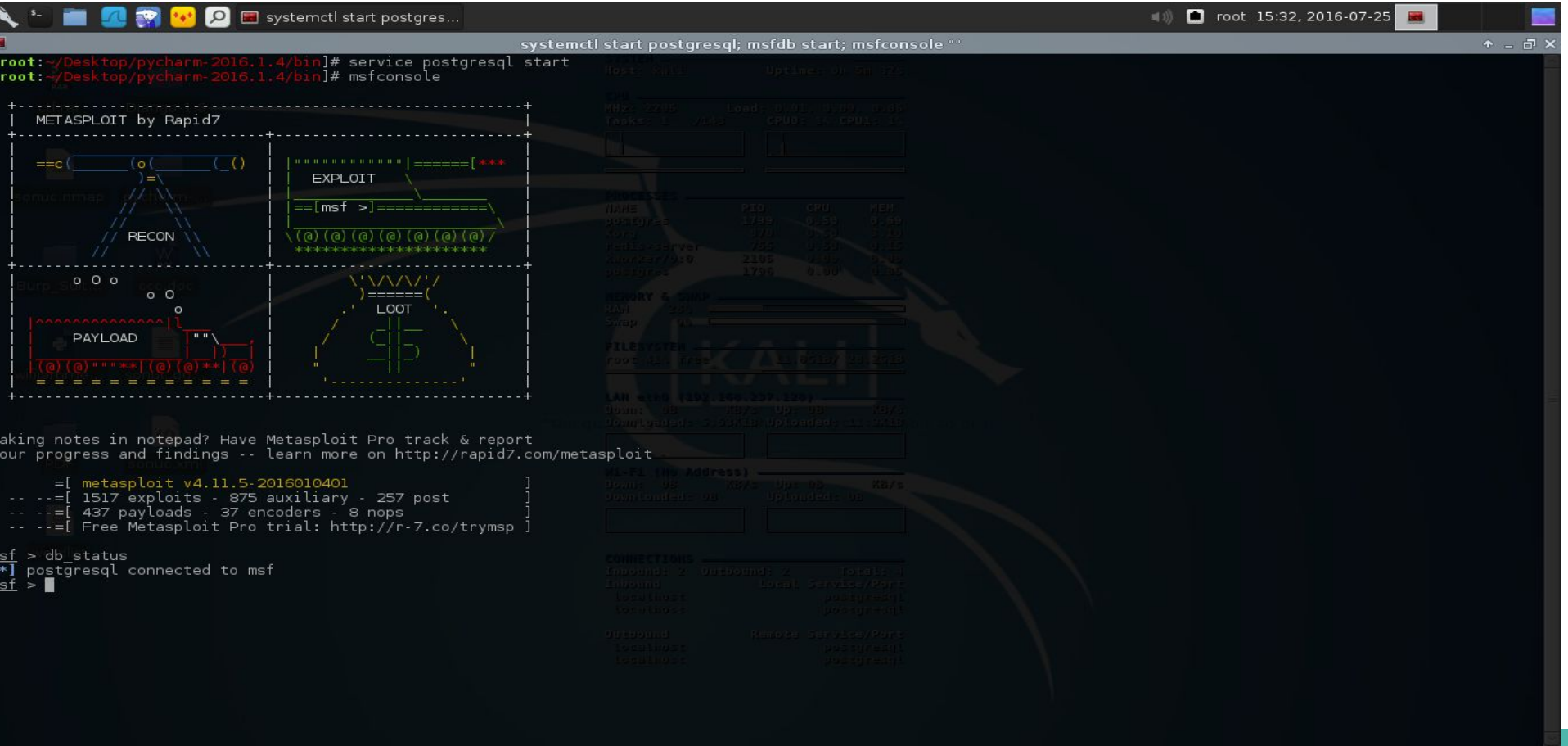
İlk olarak postgresql veritabanını başlatıyoruz daha sonra msfconsole yazarak metasploitimizi açıyoruz.

db_status

Komutunu yazarak metasploitin veritabanı bağlantısını kontrol edebilirsiniz.

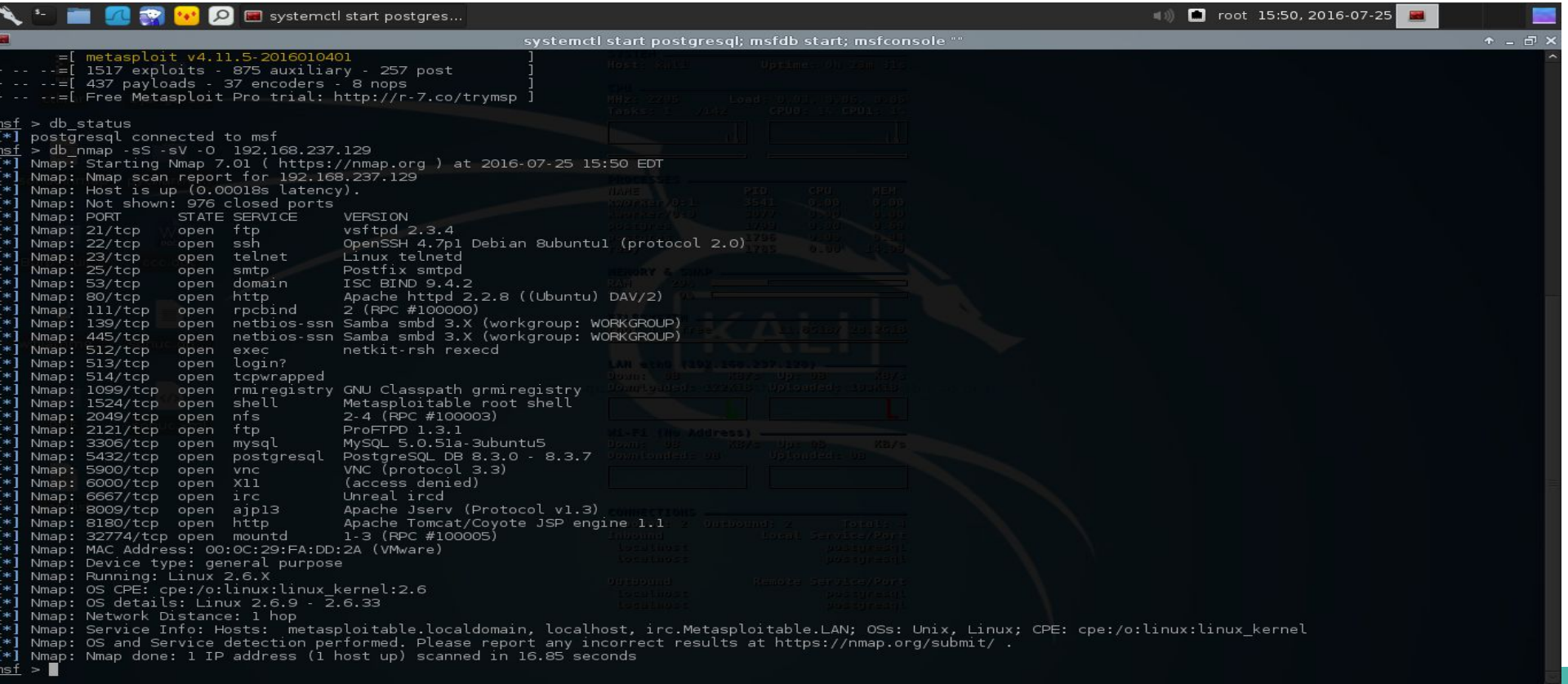
db_connect **db_disconnect** **db_import** **db_export**

Temel Metasploit Kullanımı | Giriş



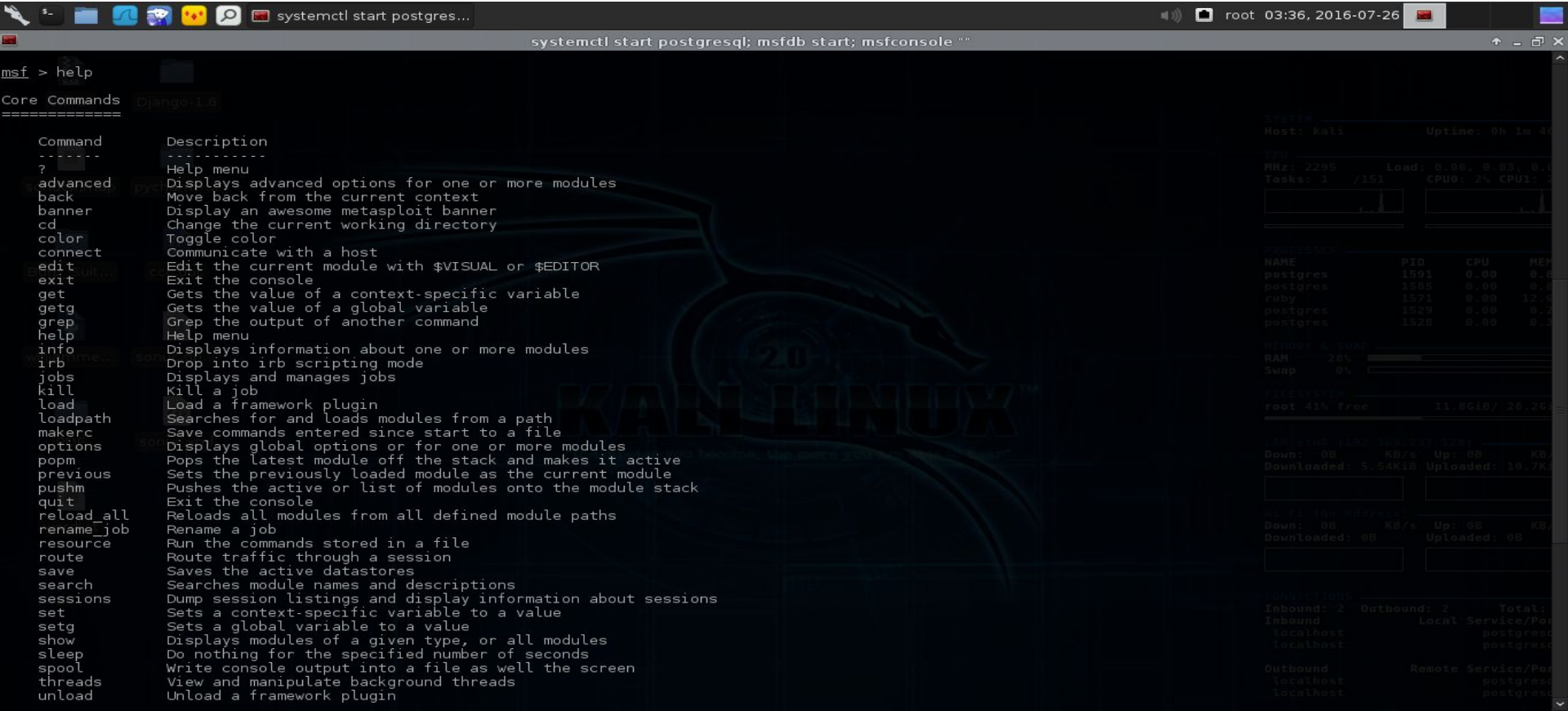
Temel Metasploit Kullanımı | Nmap

db_nmap -sS -sV -O 192.168.237.129

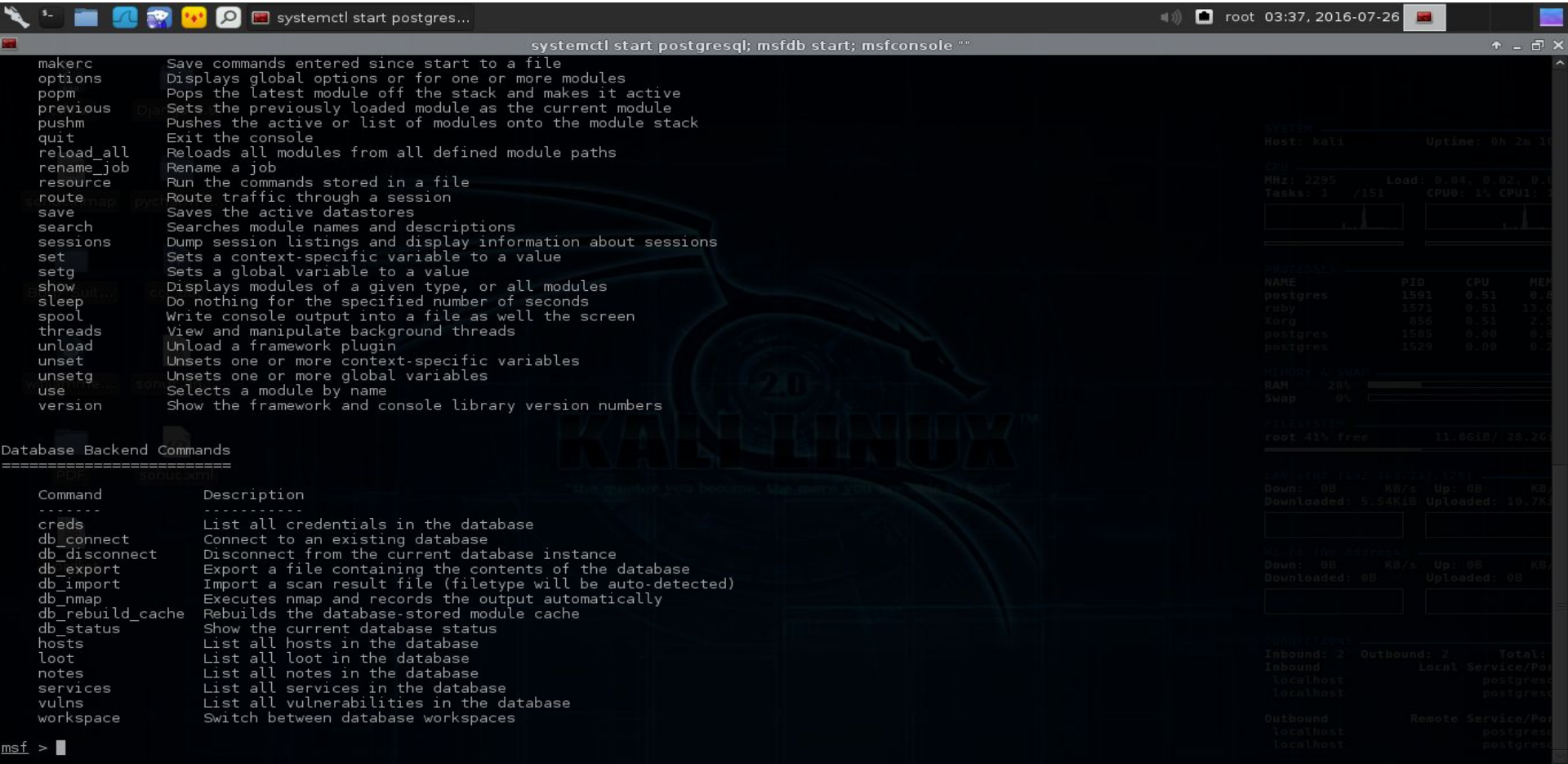


Temel Metasploit Kullanımı

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



Temel Metasploit Kullanımı

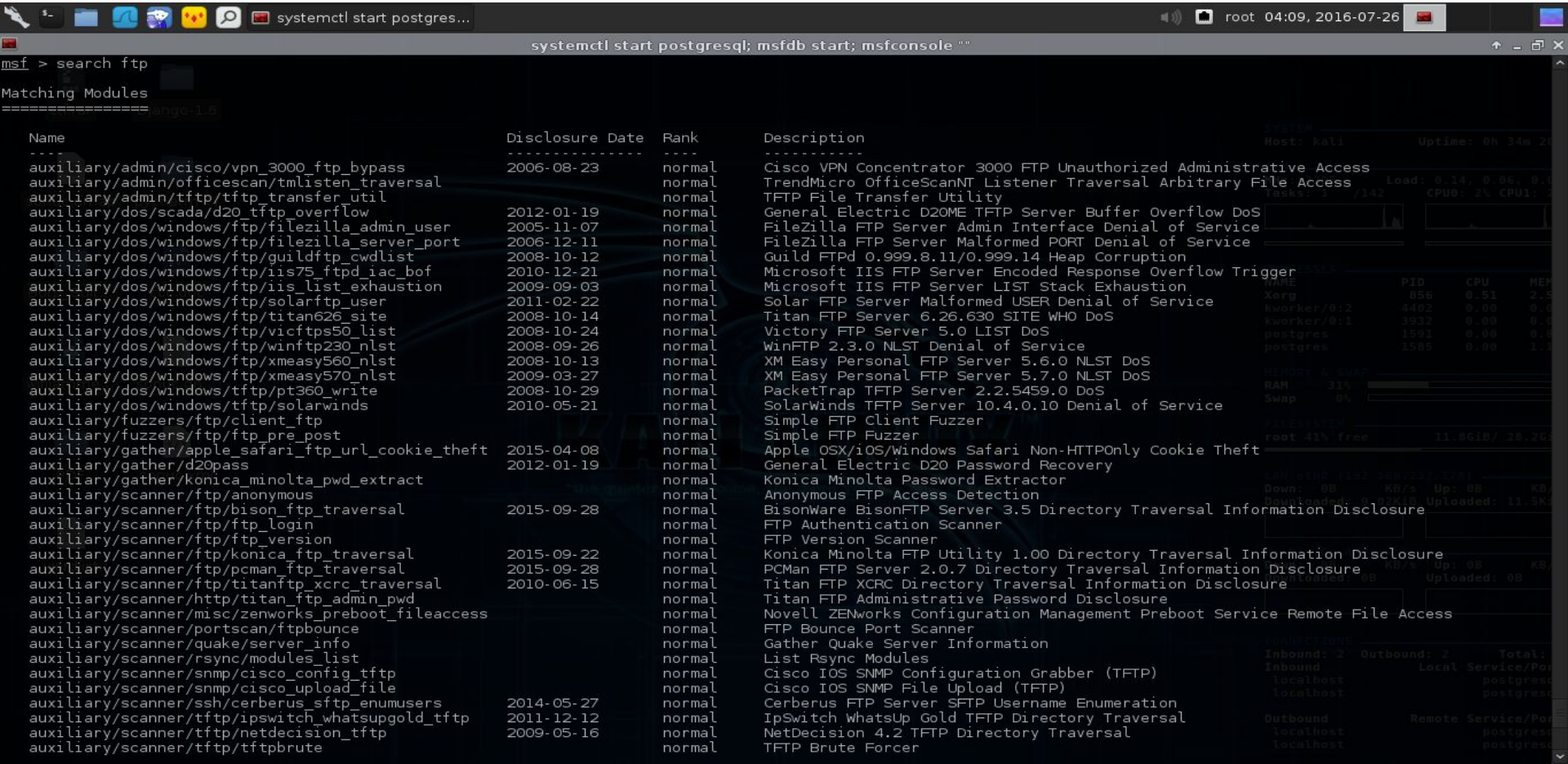


Temel Metasploit Kullanımı

search Komutu

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

Temel Metasploit Kullanımı



Temel Metasploit Kullanımı

show Komutu

İstenilen bileşenleri listeyip görmemizi sağlar.

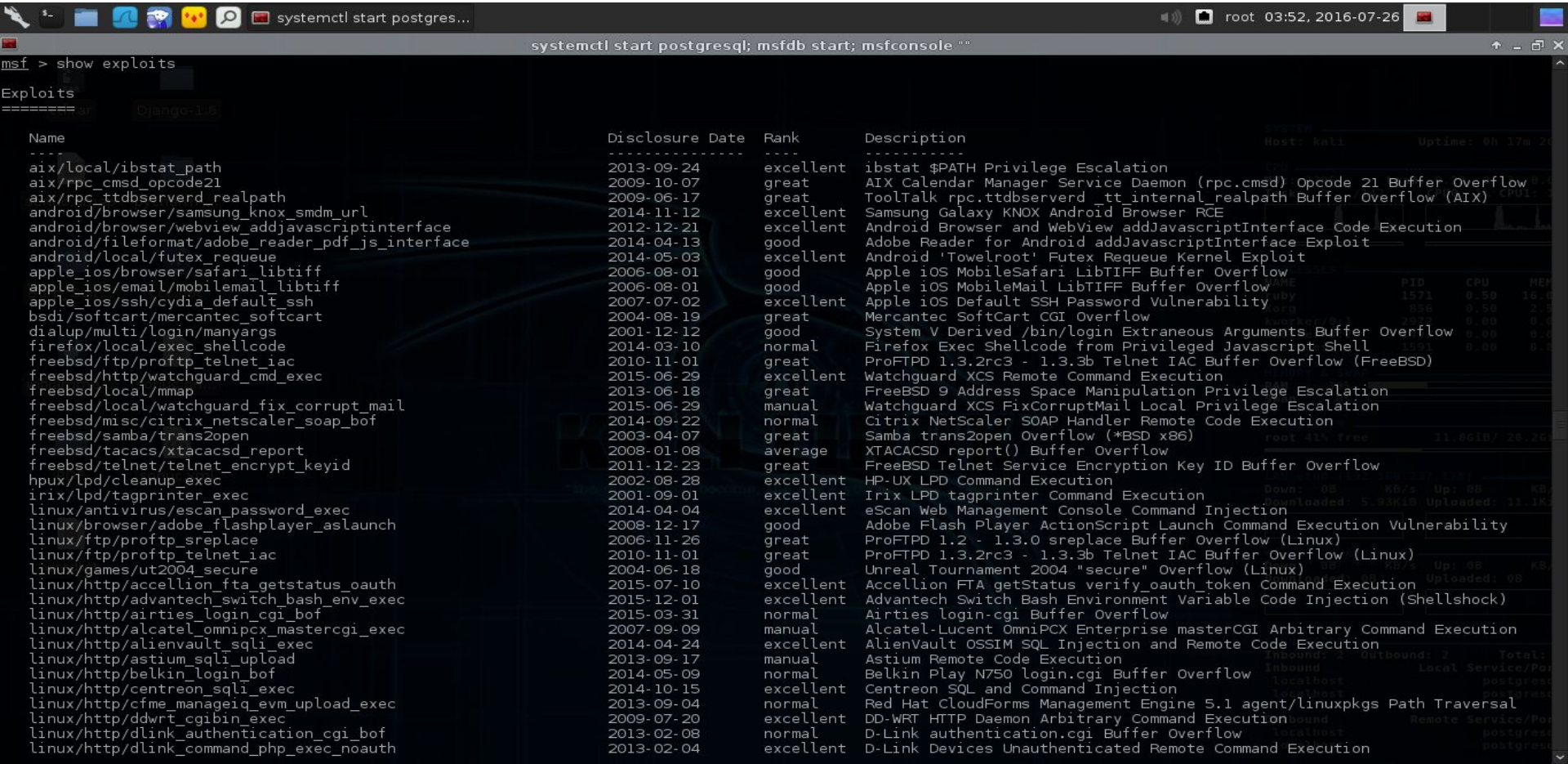
show exploits : Metasploit üzerindeki tüm exploitleri gösterir

show payloads : Metasploit üzerindeki tüm payloadları gösterir

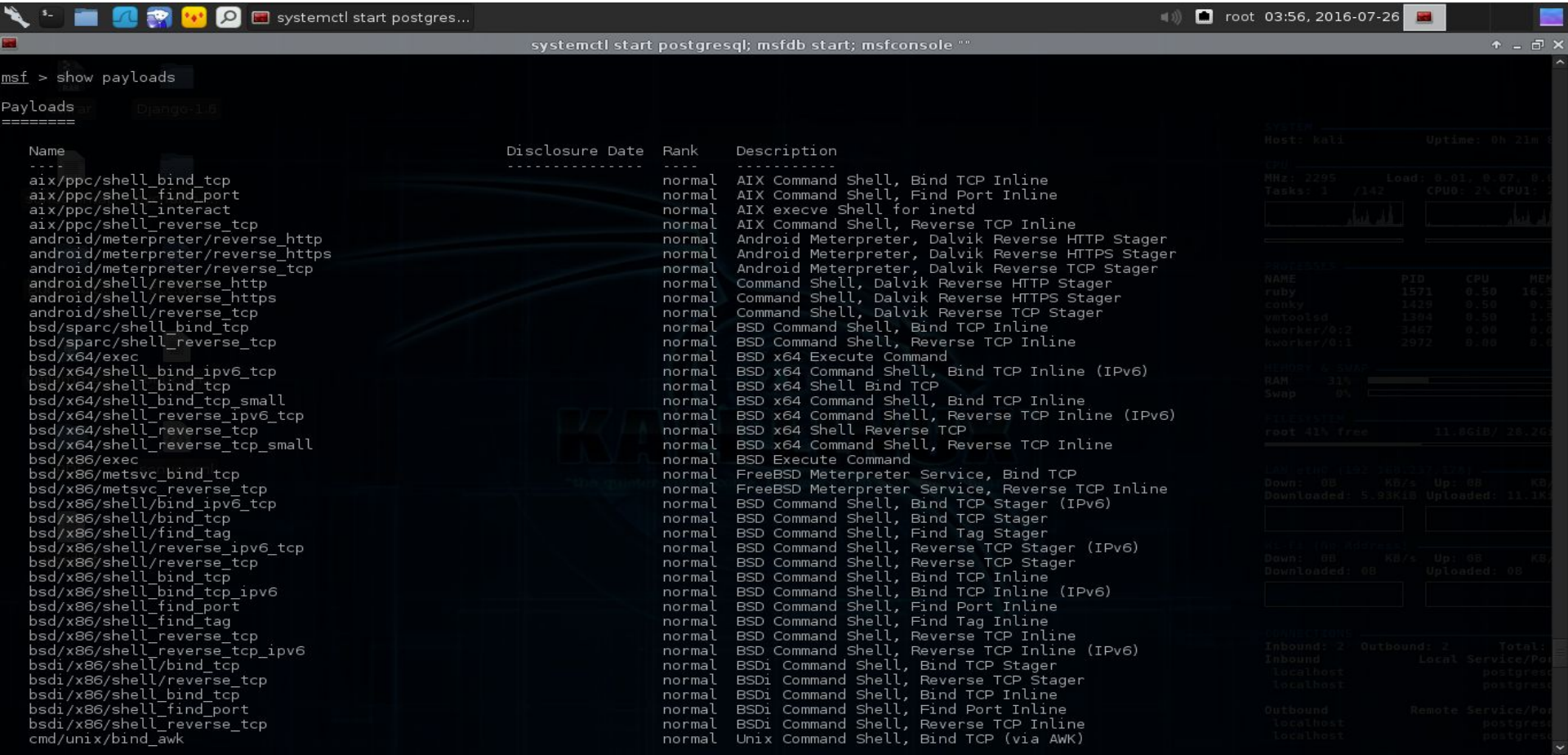
show targets : Bulunan targetları listeler

show options: Exploit yada payloadın tüm ayarlarını gösterir.

Temel Metasploit Kullanımı



Temel Metasploit Kullanımı



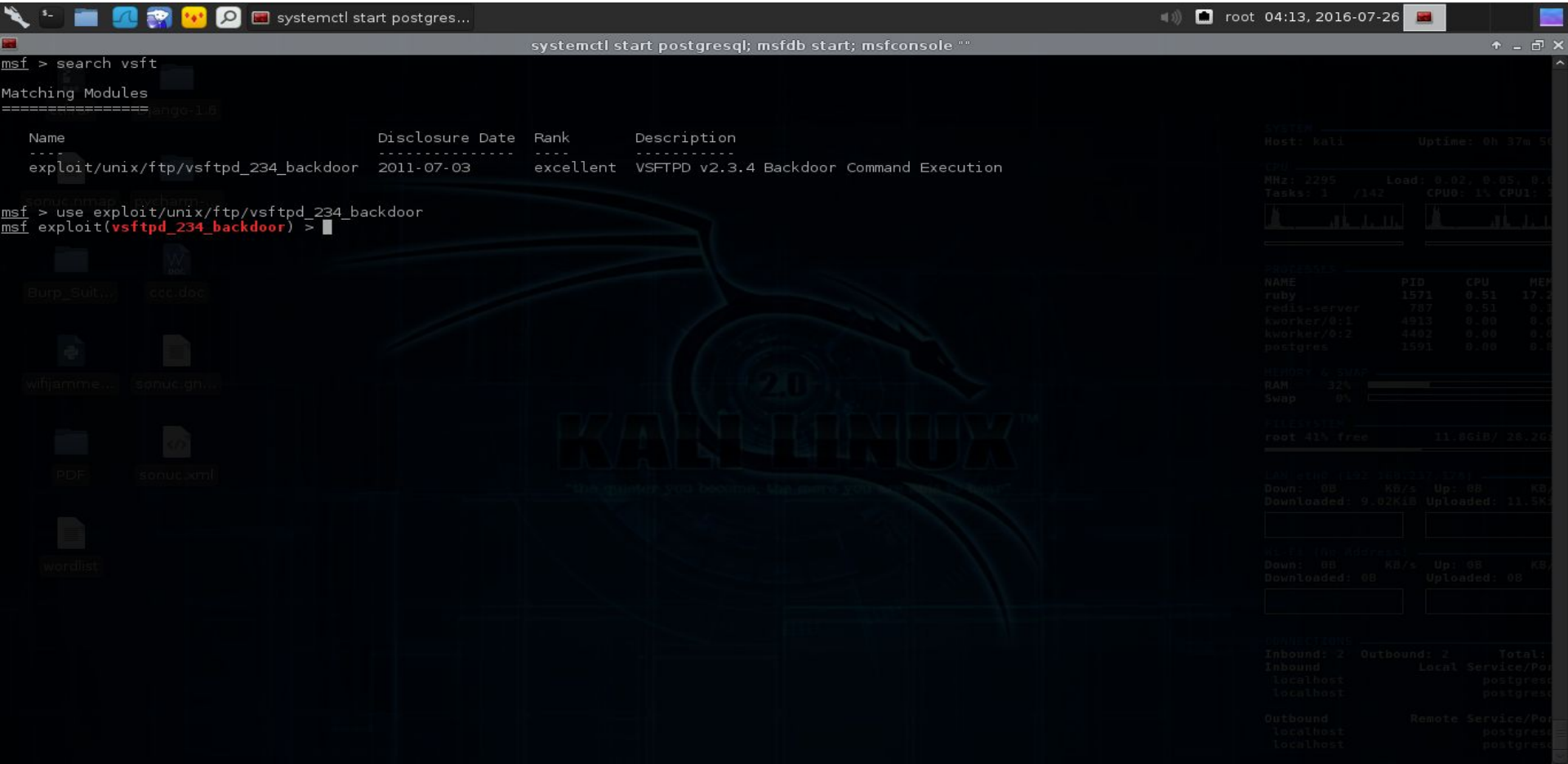
Temel Metasploit Kullanımı

use Komutu

İstenilen exploiti yada payload ı seçmek için kullanılır.

use <exploit_adi> **use <payload_adi>**

Temel Metasploit Kullanımı



Temel Metasploit Kullanımı

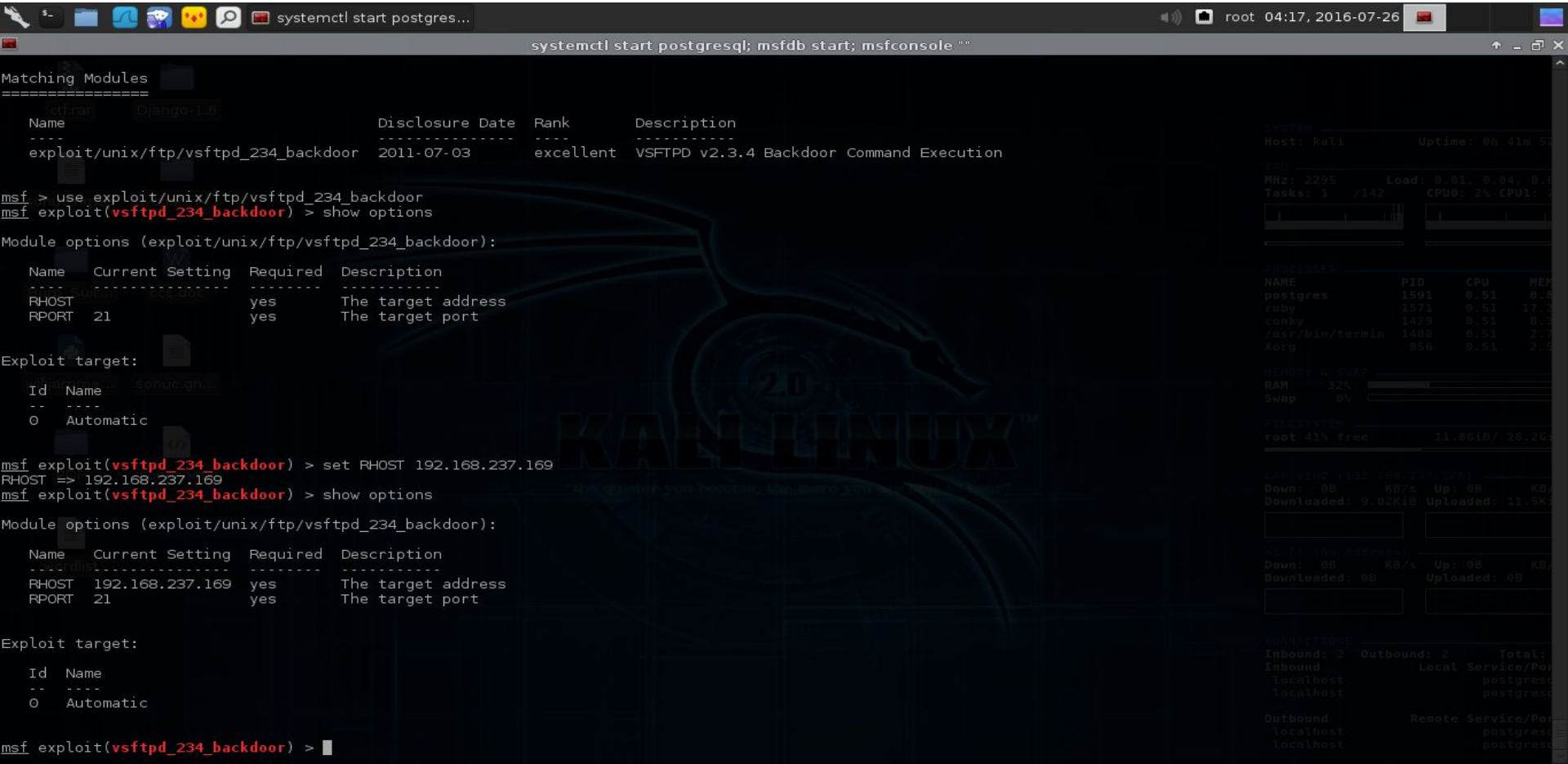
set Komutu

Bir değişkene değer aktarmak için kullanılır.

set RHOST <hedef (kurban)_ip_adresi>

set LHOST <local (kendi)_ip_adresimiz>

Temel Metasploit Kullanımı



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

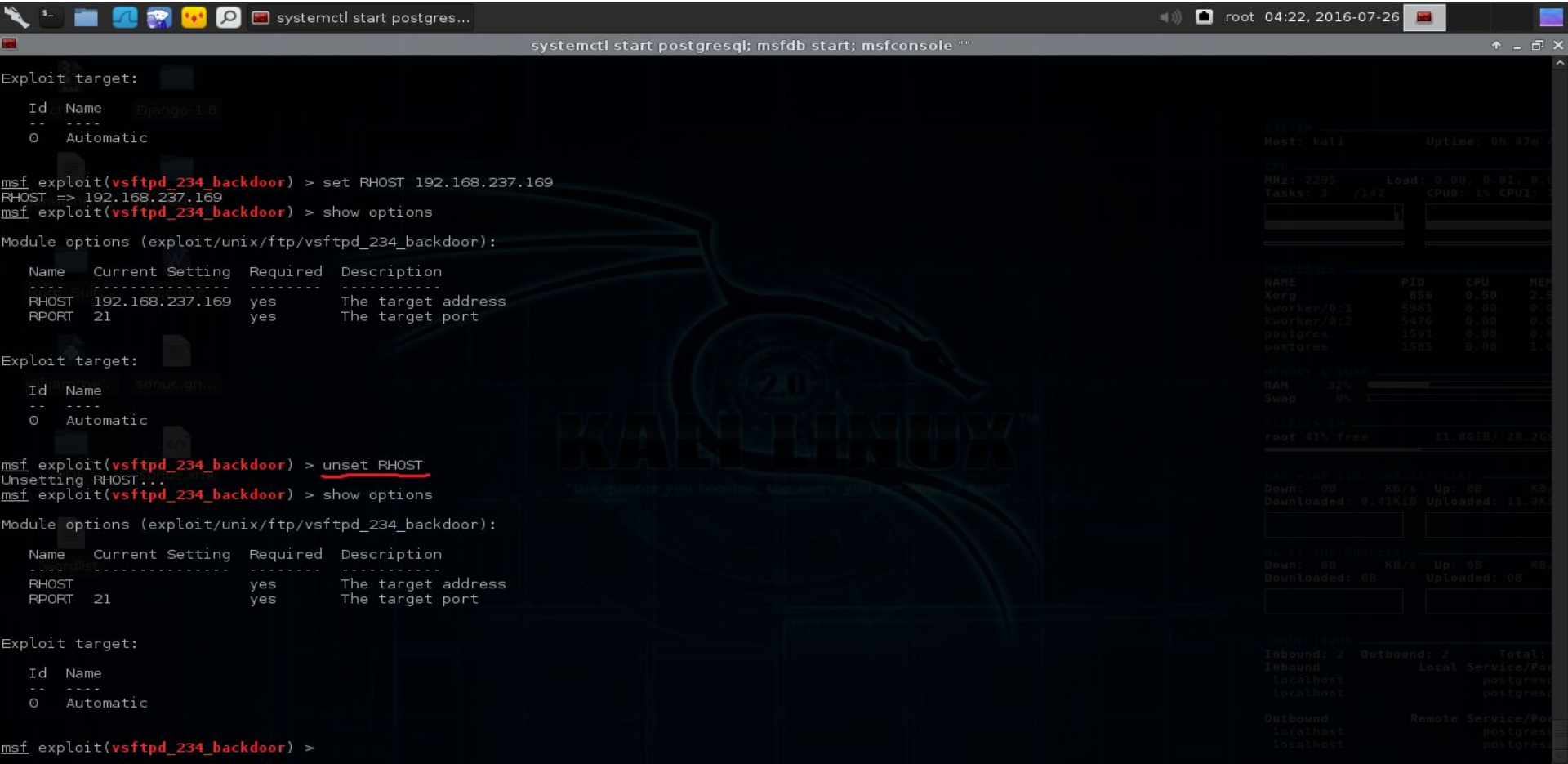
unset Komutu

Değişkene aktarılan değeri iptal eder.

unset LHOST : LHOST değişkeninin değerini iptal eder.

unset RHOST : RHOST değişkeninin değerini iptal eder.

Temel Metasploit Kullanımı



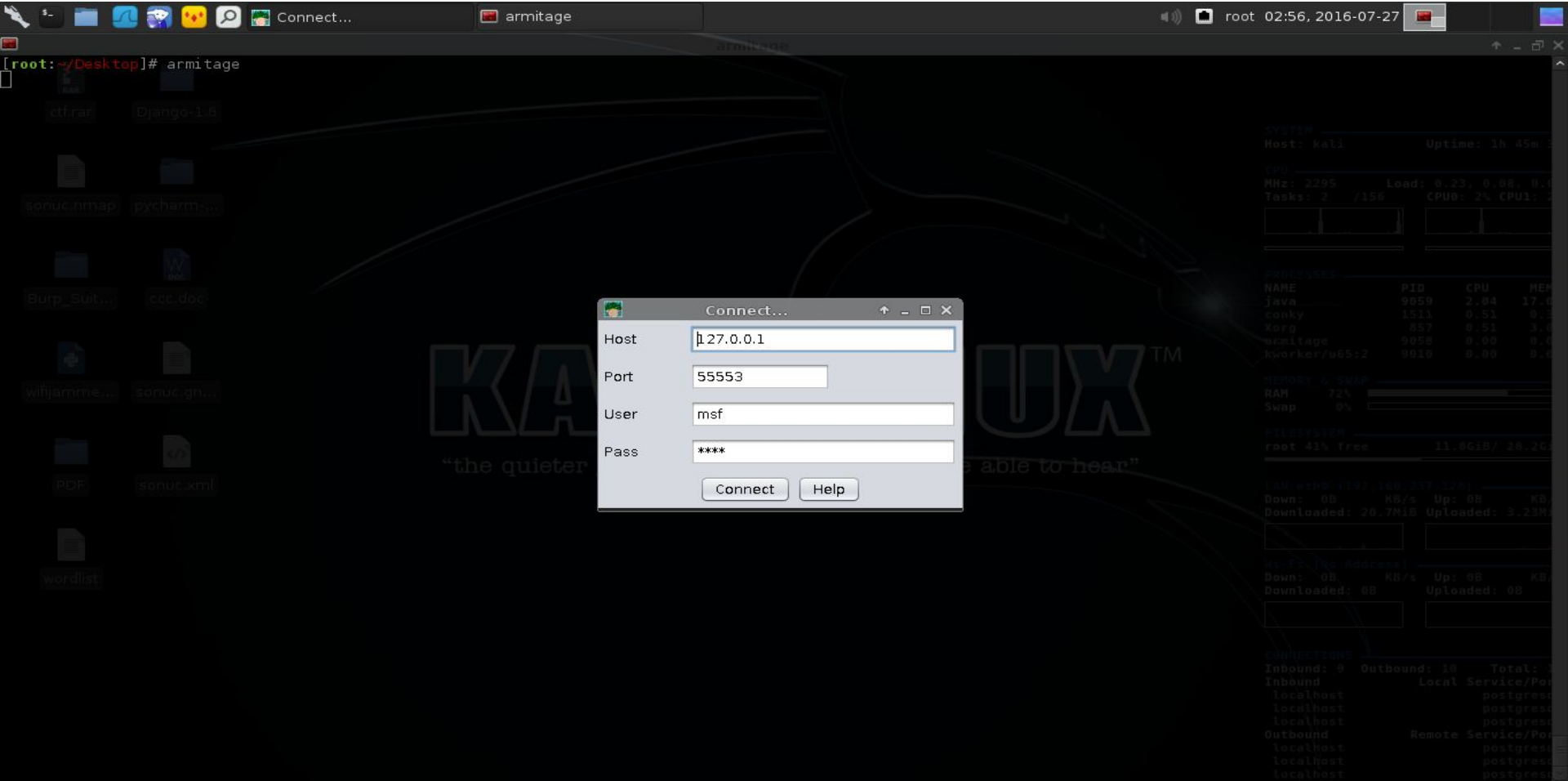
Temel Metasploit Kullanımı

exploit ve run Komutu

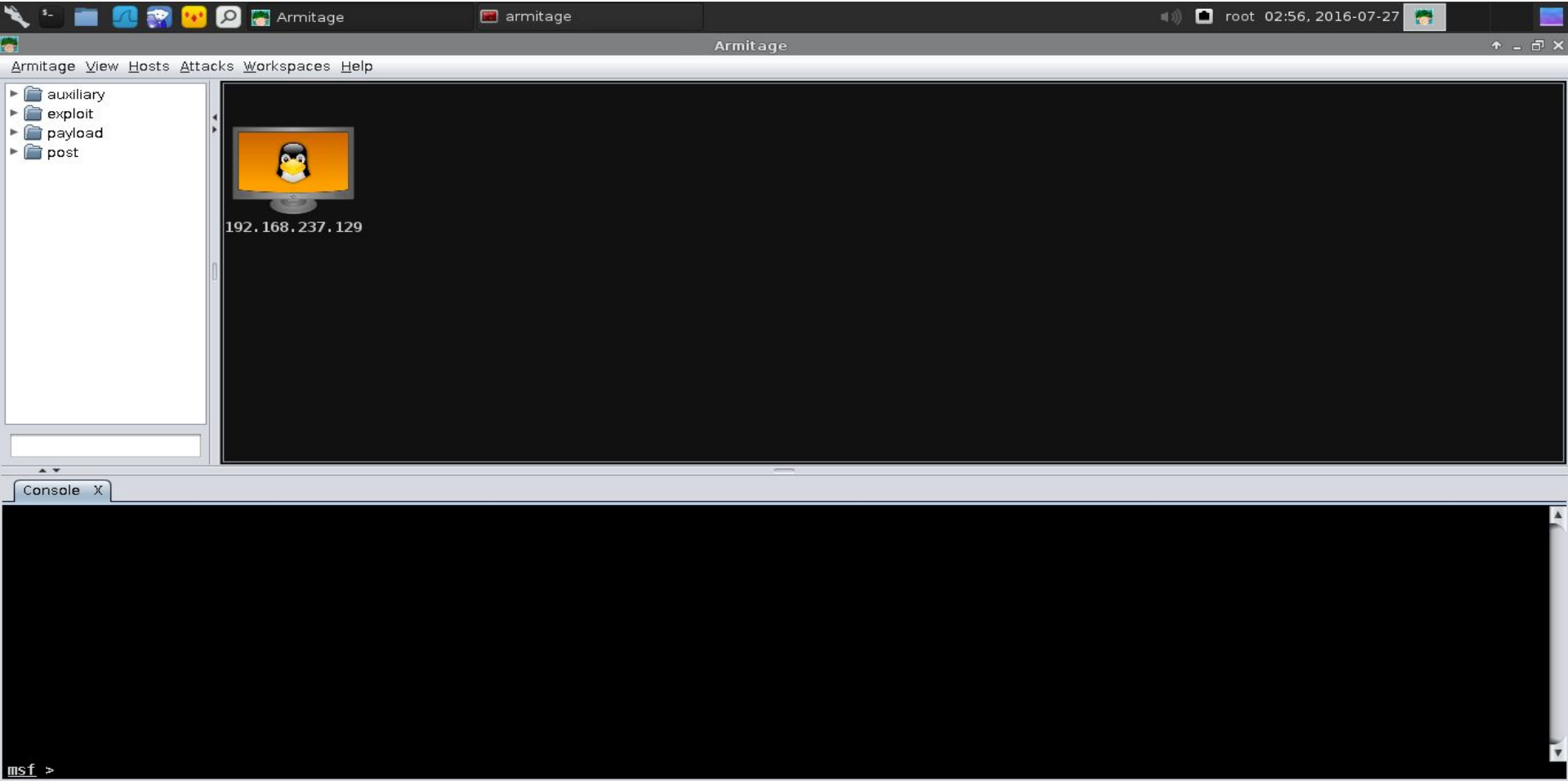
Eğer bir **exploit** seçmiş ve **show options** komutundan sonra istenilen değerleri **set** komutu ile girildikten sonra **exploit** denir ve exploit çalıştırılır.

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

Temel Metasploit Kullanımı | Armitage



Temel Metasploit Kullanımı | Armitage



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.

Temel Metasploit Kullanımı | Meterpreter

run checkvm: Hedef makinanın sanal makina olup olmadığına bakar.

run keylogrecorder : Hedef sistemde keyloger başlatır.

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

run getcountermeasure : Hedef sistemdeki güvenlik programları devre dışı kılar.

backgraund : 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 değindik 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

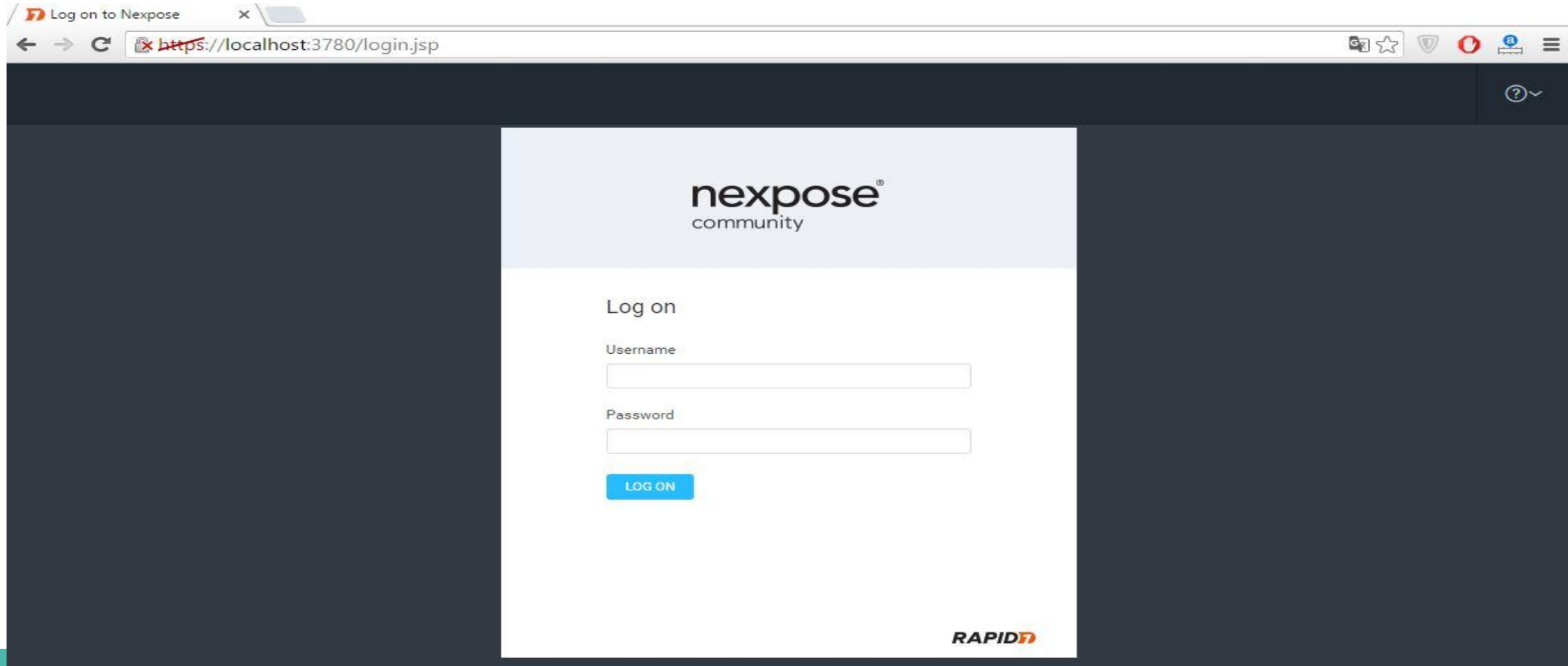
Açıkları taramak için Networkte **Nessus** ve **Nexpose** gibi araçlar bulunmaktadır.Web açıklıkları için **Netsparker** ve **Acunetix** gibi tarama araçları bulunmaktadır.Bu dökümanda ben Nexpose ile açıklık tarayacağım.Nexpose Rapid7 tarafından geliştirilmekte ve Metasploit ile entegre olabilmektedir.Aşağıdaki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

Açıklık Tarama Araçları ve Kullanımı

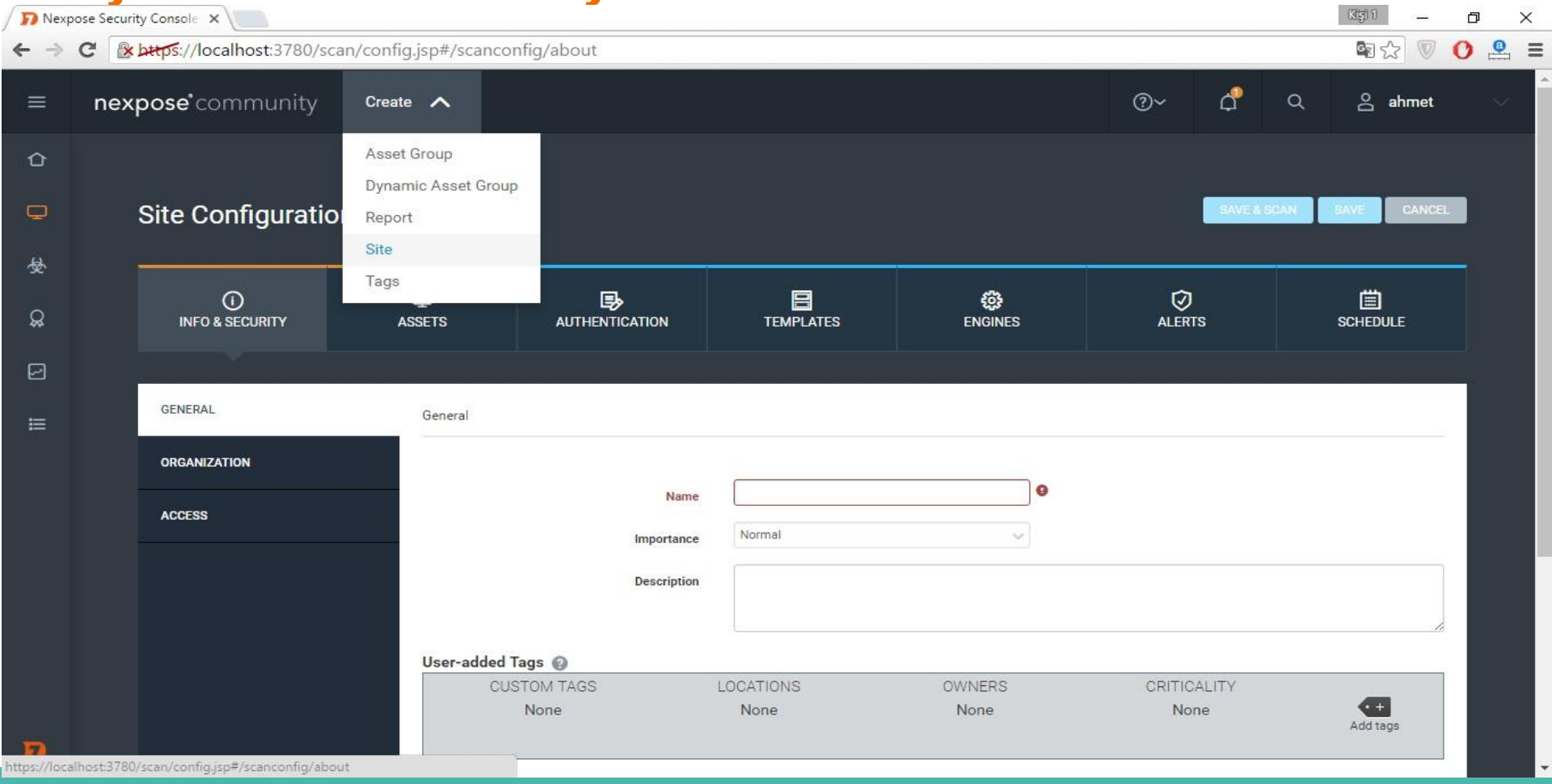
Program kurduktan sonra kurulumda oluşturduğunu username ve password giriyoruz.



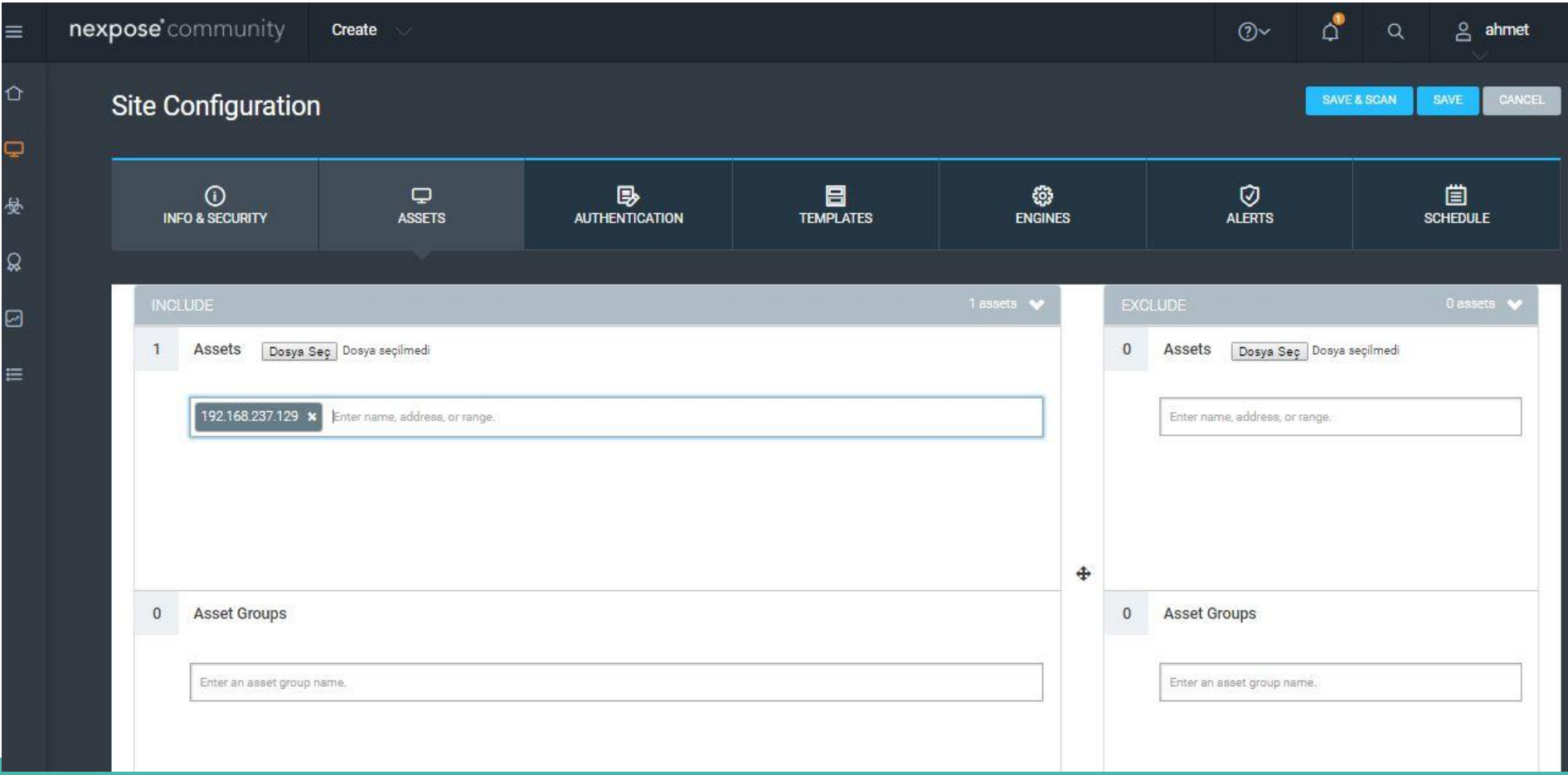
Açıklık Tarama Araçları ve Kullanımı

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

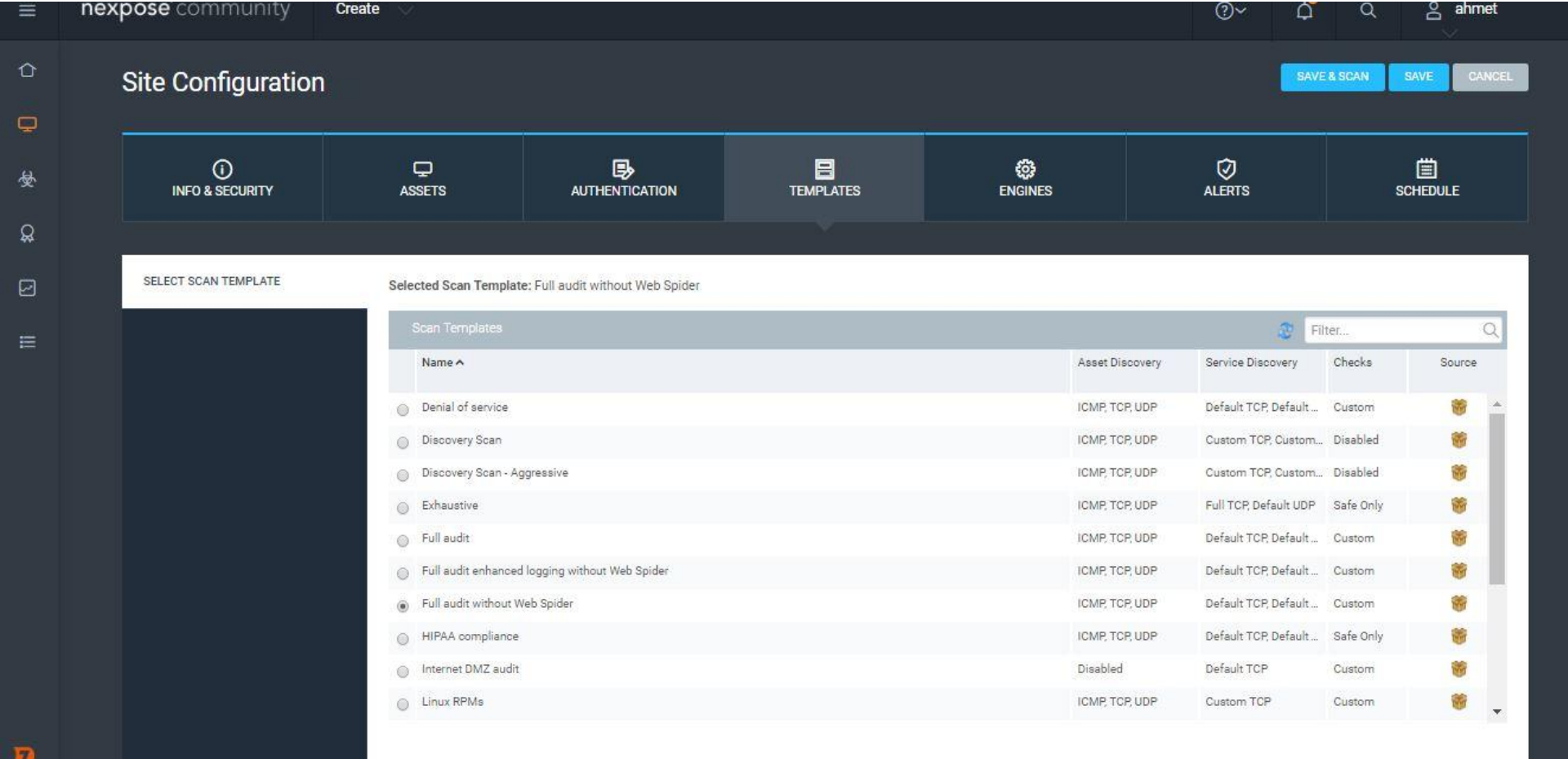
Açıklık Tarama Araçları ve Kullanımı



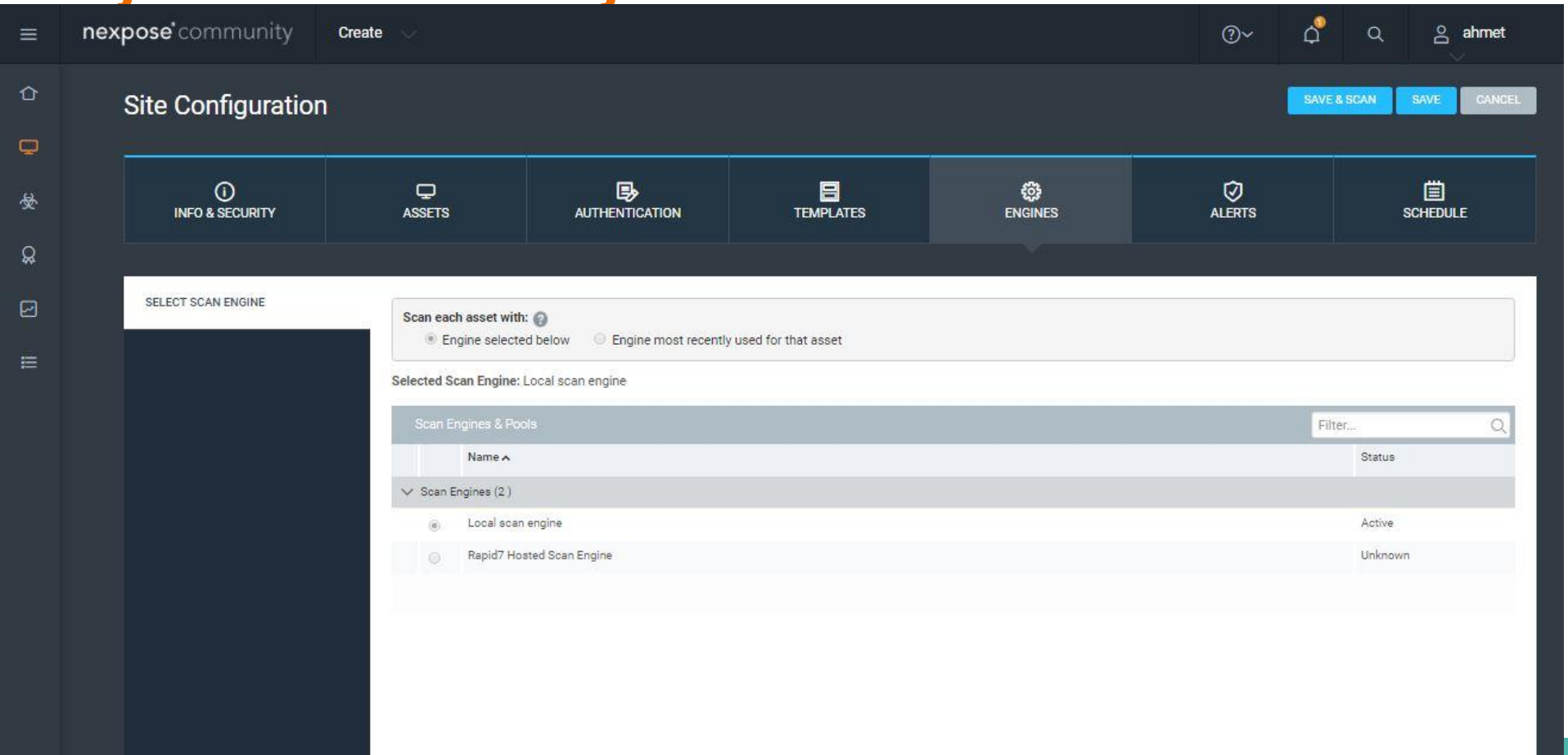
Açıklık Tarama Araçları ve Kullanımı



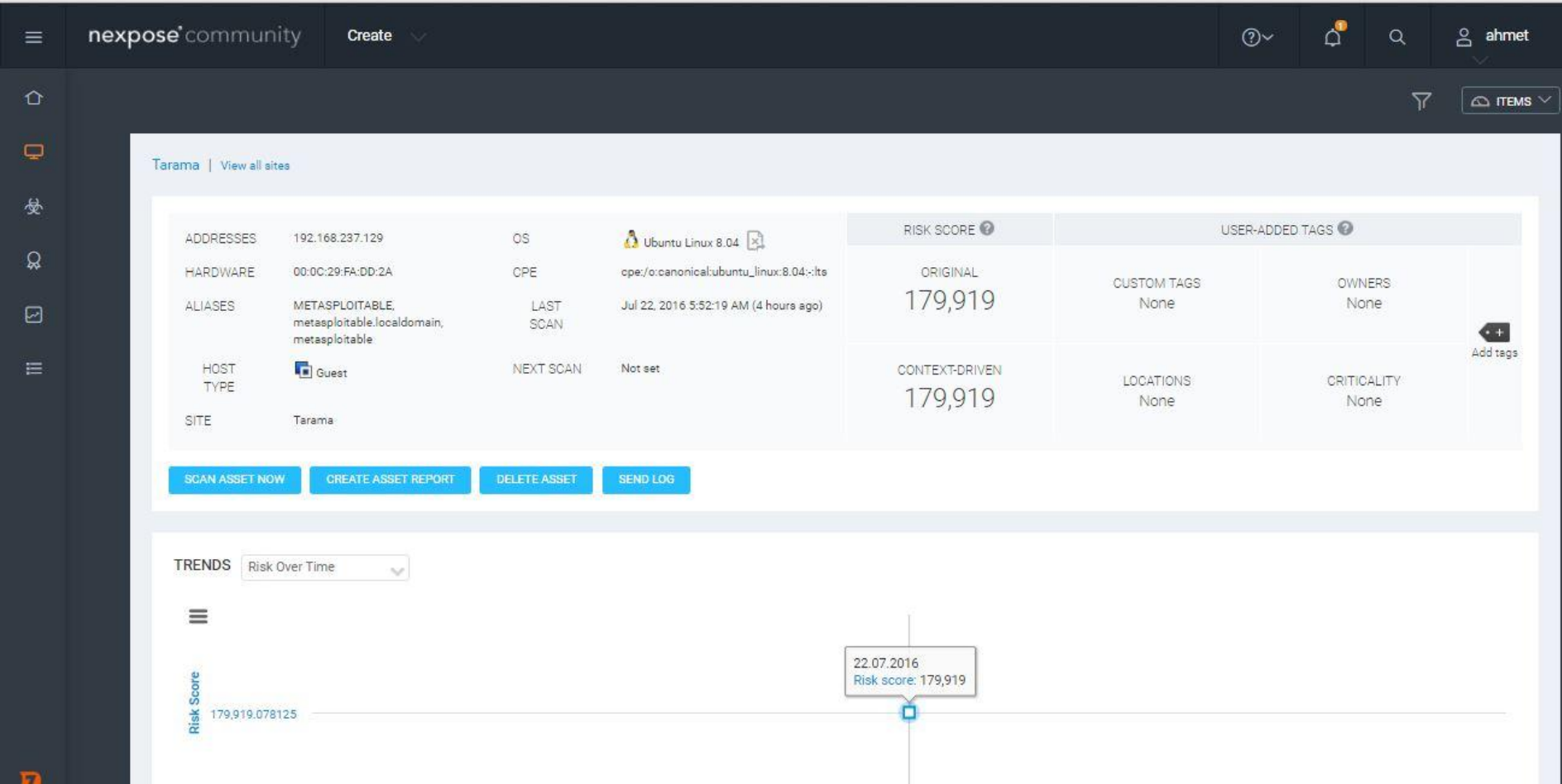
Açıklık Tarama Araçları ve Kullanımı



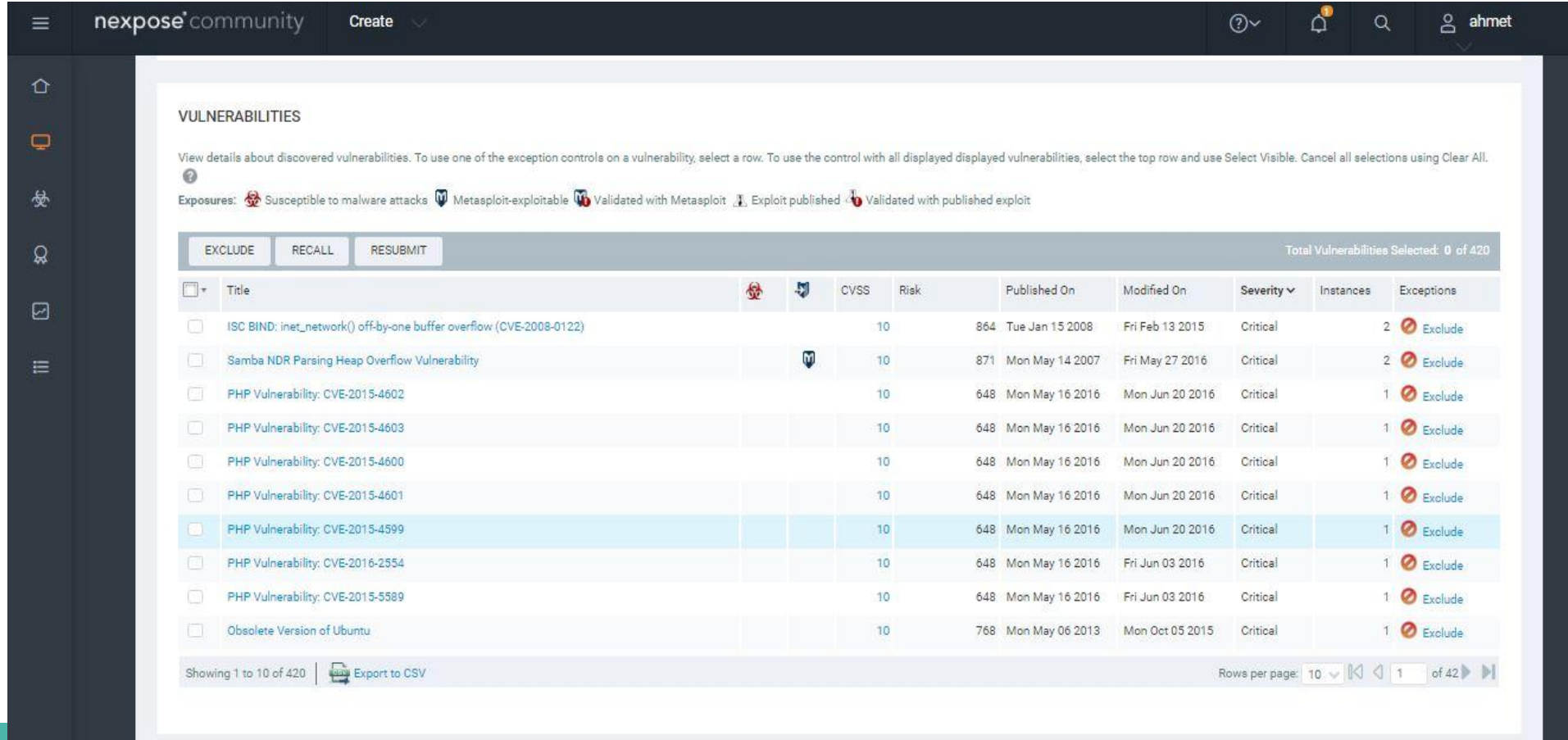
Açıklık Tarama Araçları ve Kullanımı



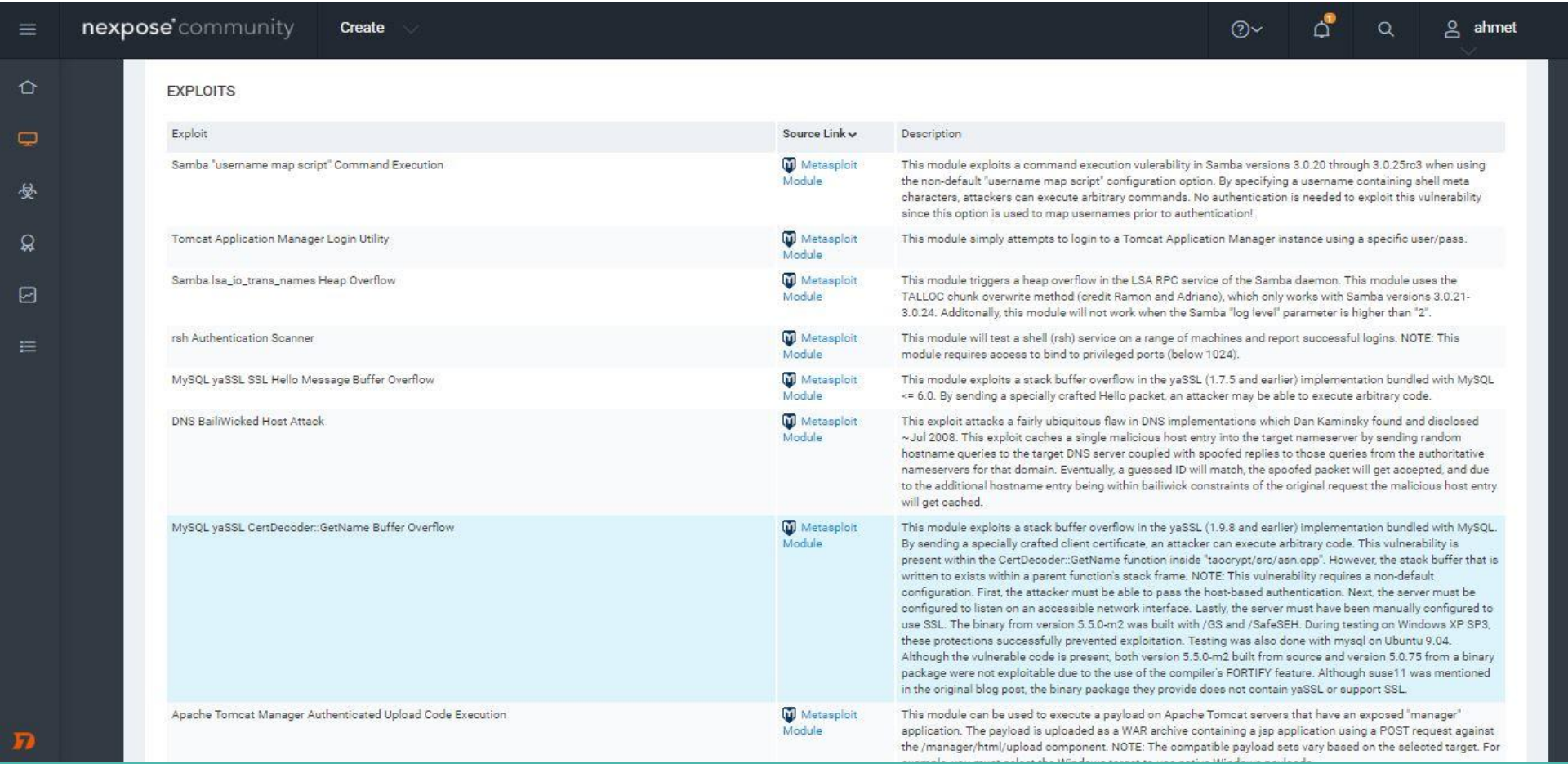
Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları



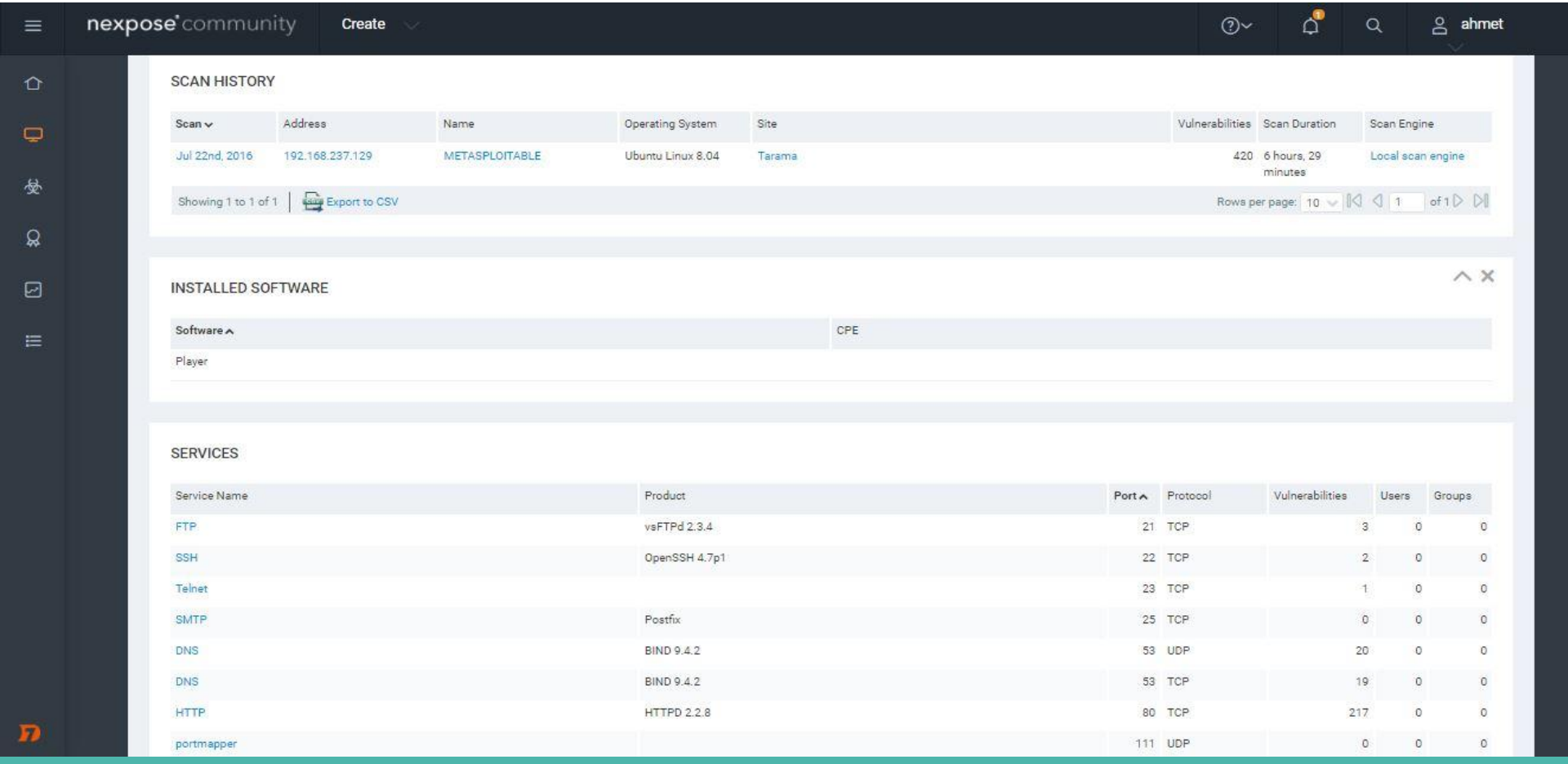
Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları



Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları



Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları



Açıklık Tarama Araçları ve Kullanımı | Tarama Sonuçları

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 gerçekleştireceğiz bir sisteme sızmaktaki hedef o sistemde yetkili kullanıcı olup her şeye erişim sağlamaktır.Bu örnek makina linux olduğu için hedefimiz **root** olmaktır.

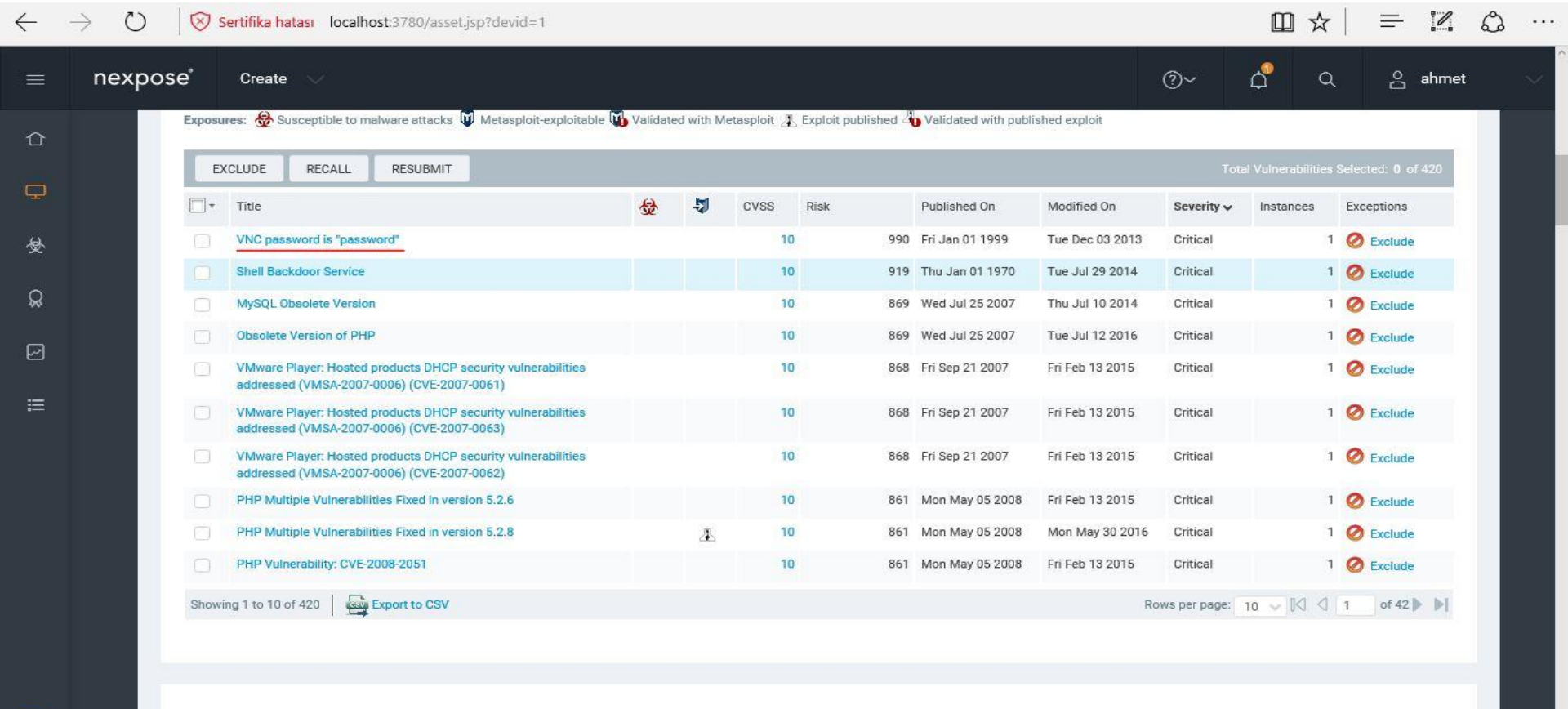
Sızma Testi Örnekleri (Metasploitable2)

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.

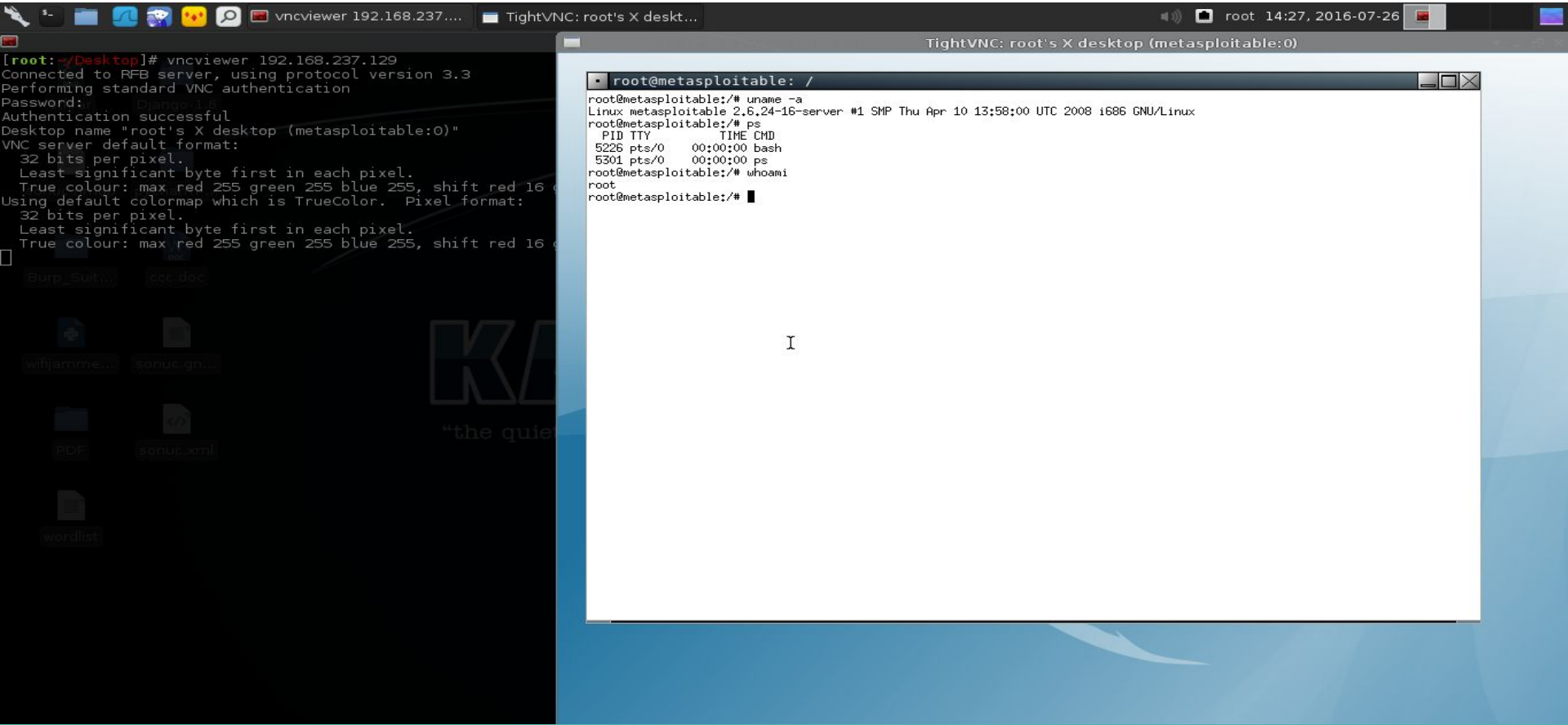
Sızma Testi Örnekleri (Metasploitable2)

Bu nexpose çıktısında VNC nın şifresinin password olduğunu söylemektedir.



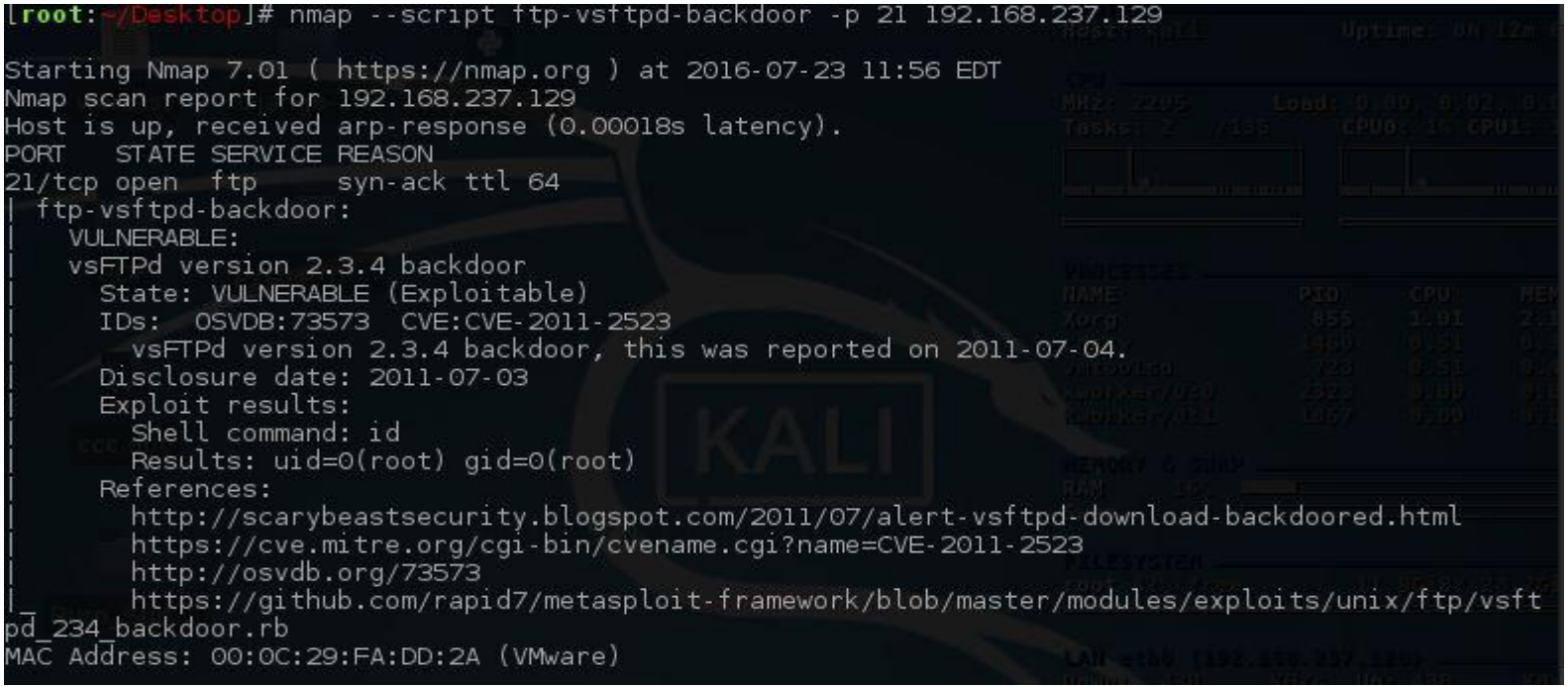
Sızma Testi Örnekleri (Metasploitable2)

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

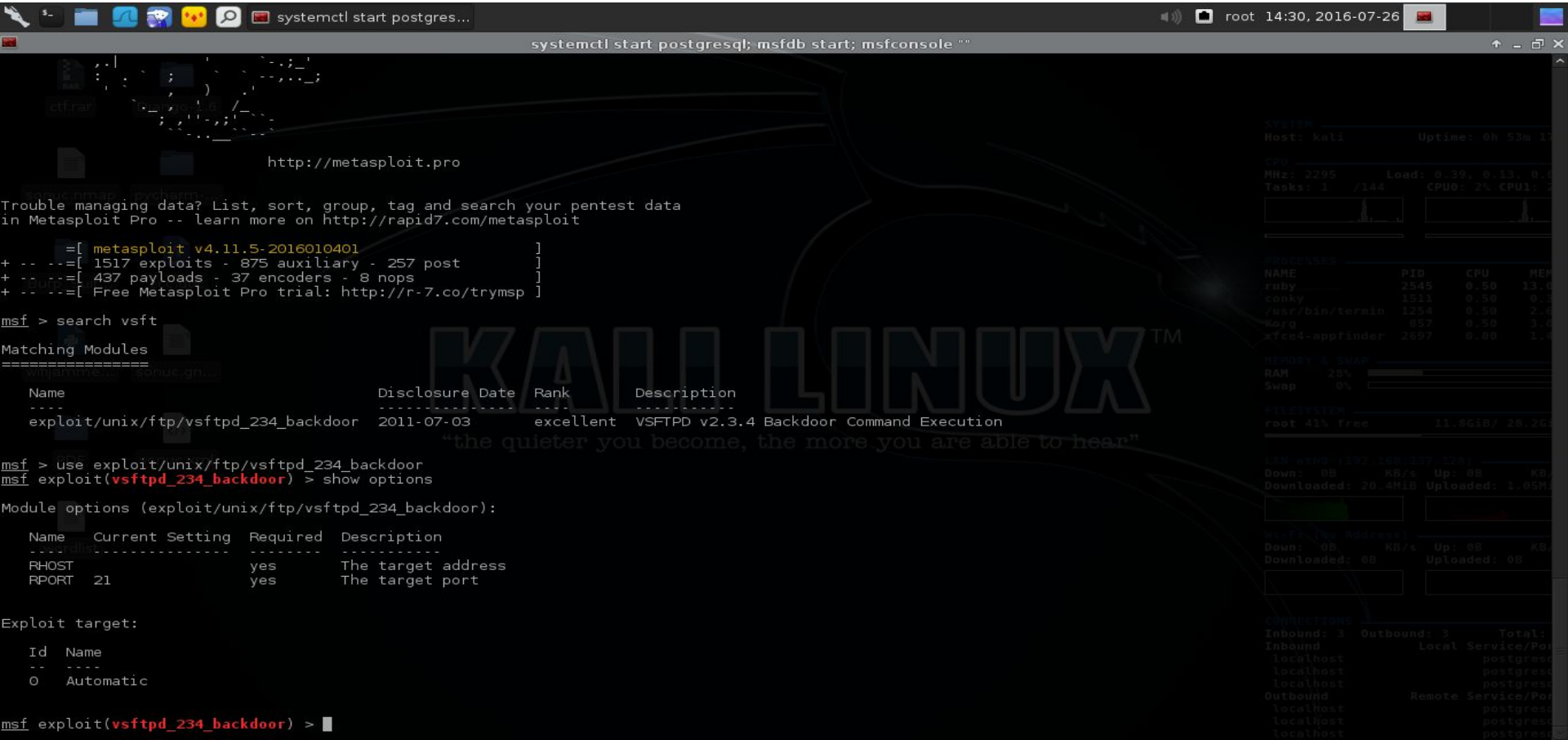


Sızma Testi Örnekleri (Metasploitable2)

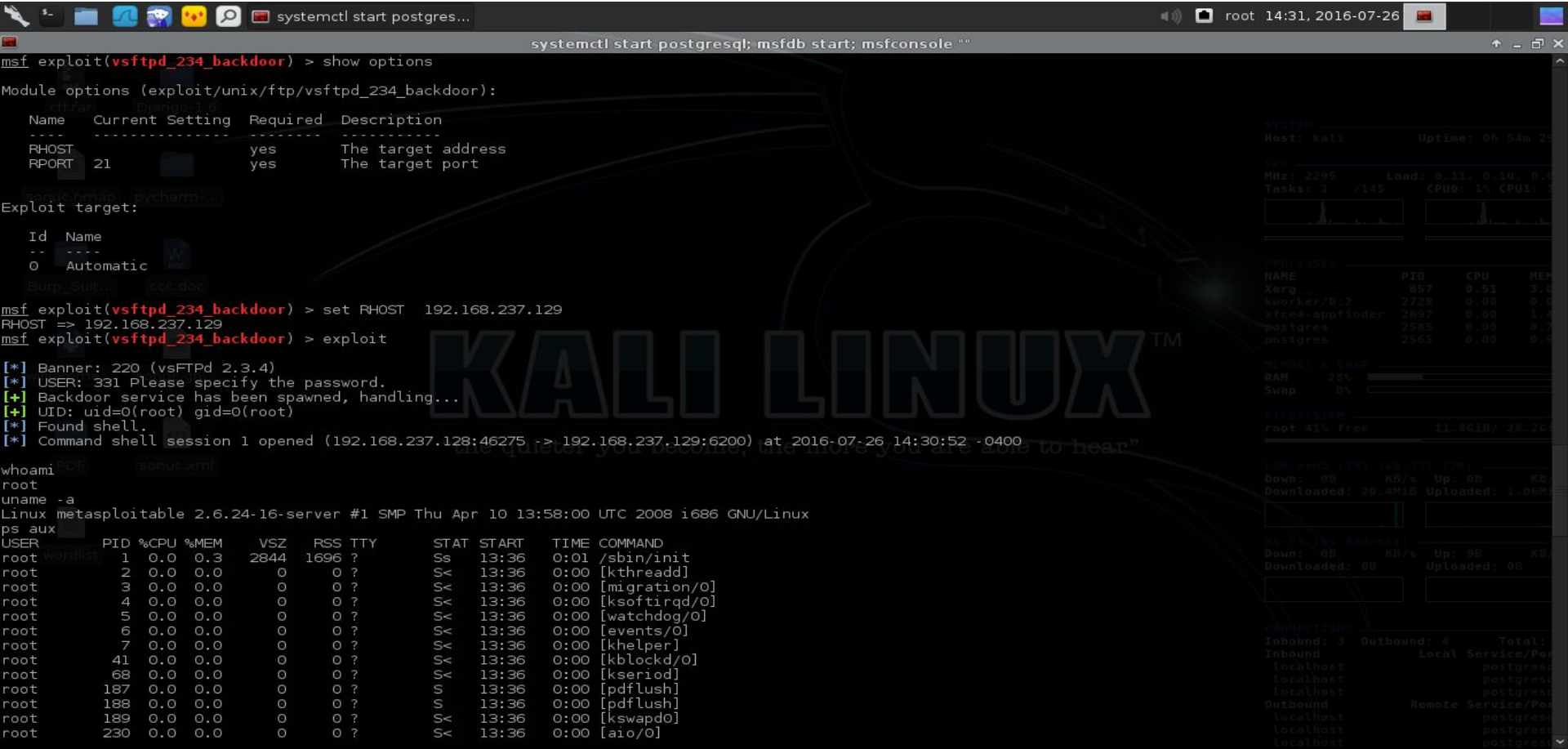
Port taramasında 21.portta FTP vsftpd 2.3.4 sürümünün çalışmakta olduğu görünmekte.Bunu google araması ile yada Nmap scriptleri ile bir backdoor exploitinin olduğunu görmekteyiz.Metasploit ile sisteme sızabilmekteyiz.



Sızma Testi Örnekleri (Metasploitable2)



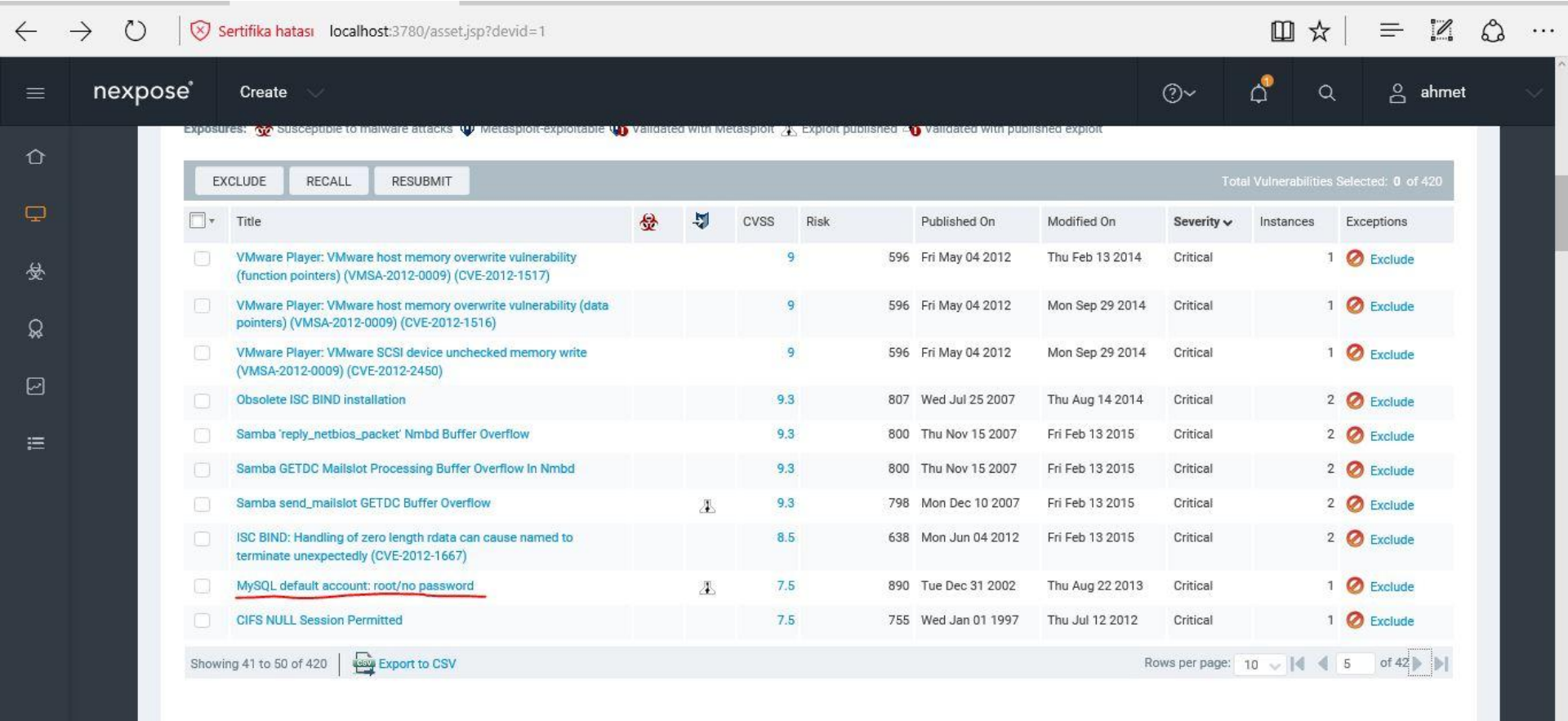
Sızma Testi Örnekleri (Metasploitable2)



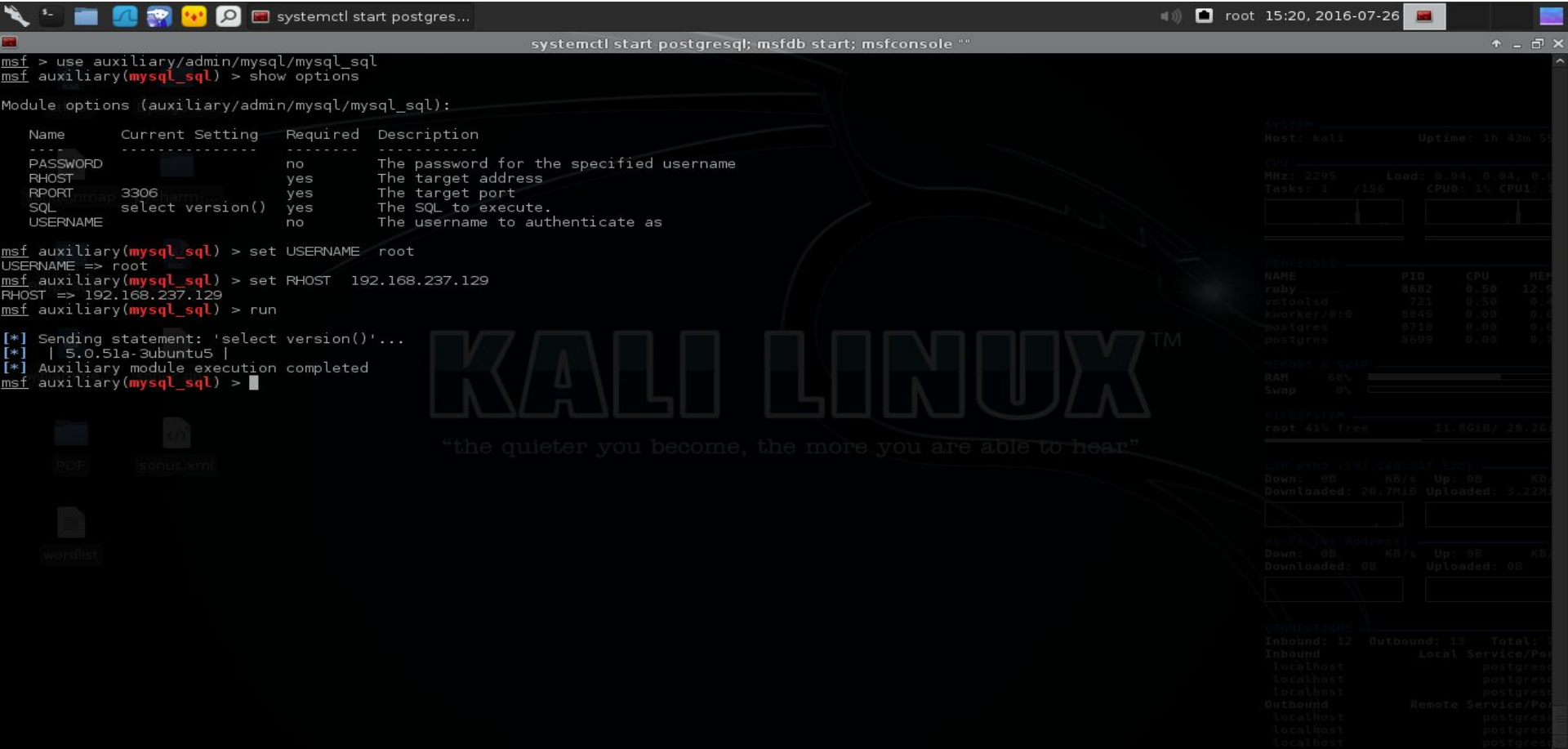
Sızma Testi Örnekleri (Metasploitable2)

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 düşübülebilir.Biz metasploit auxiliary modülü kullanarak veritabanı sorgusu çalıştıracağız.Örnek bir SQL sogusu çalıştıracağız farklı bir çok SQL sorgusu çalıştırabiliriz.

Sızma Testi Örnekleri (Metasploitable2)



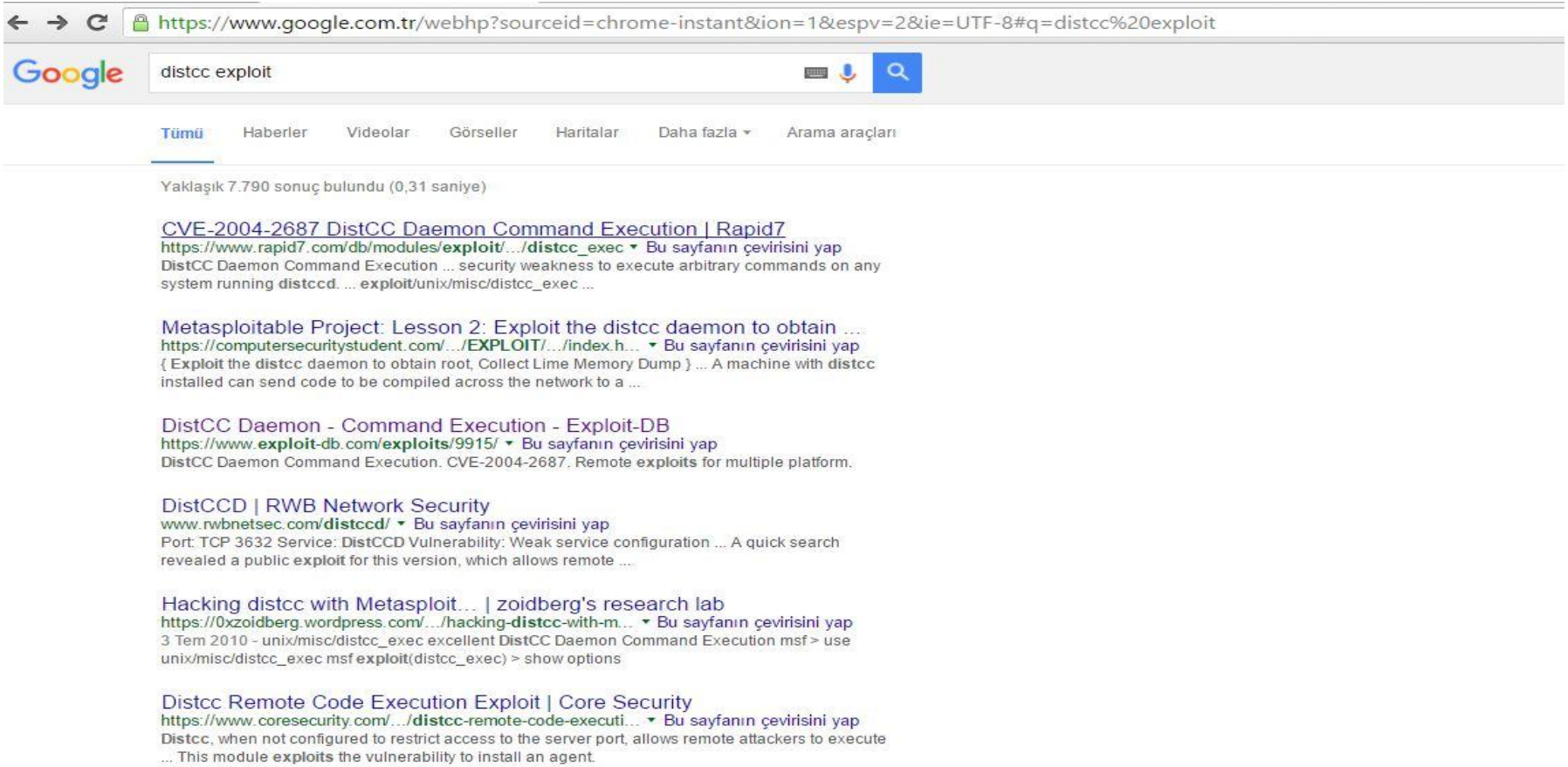
Sızma Testi Örnekleri (Metasploitable2)



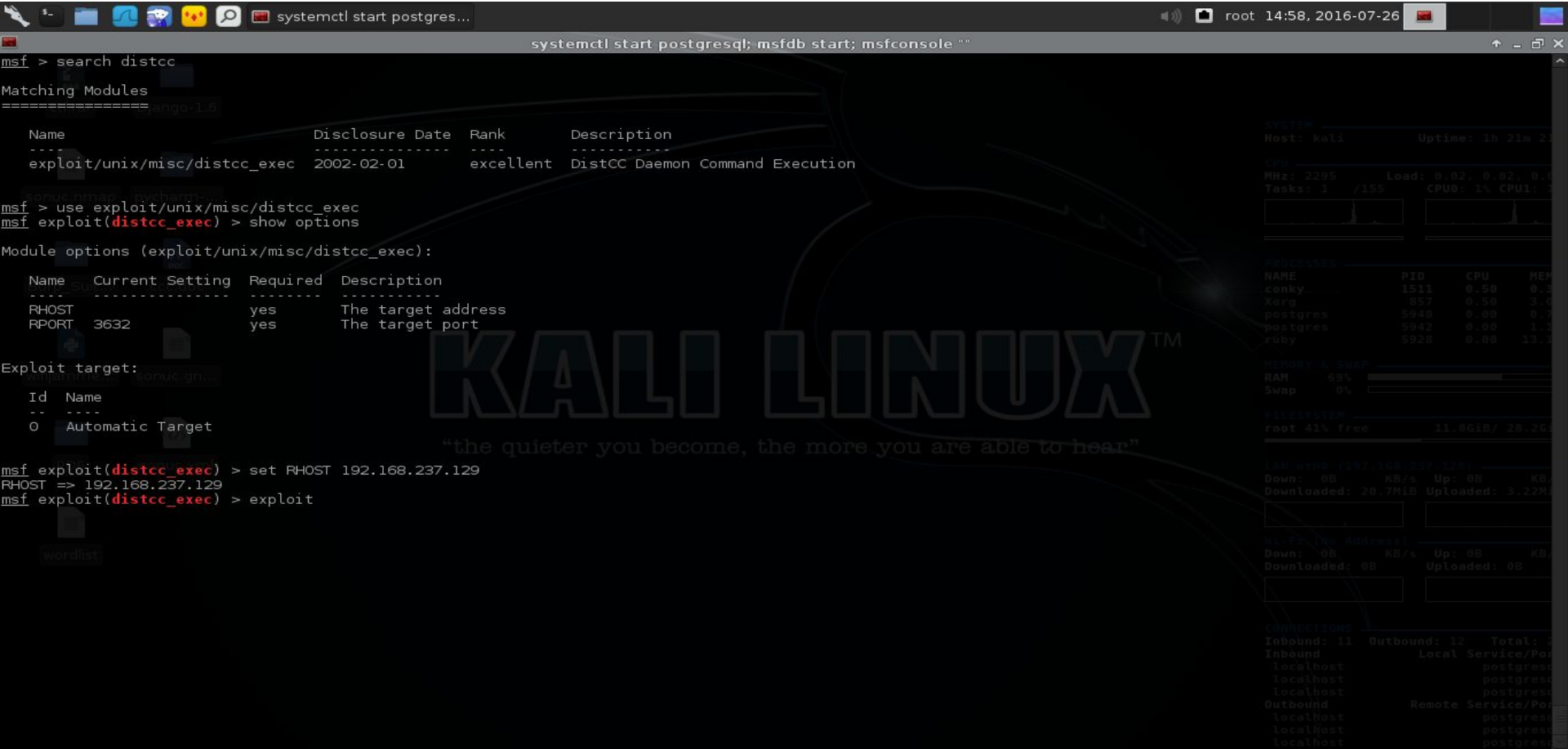
Sızma Testi Örnekleri (Metasploitable2)

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.

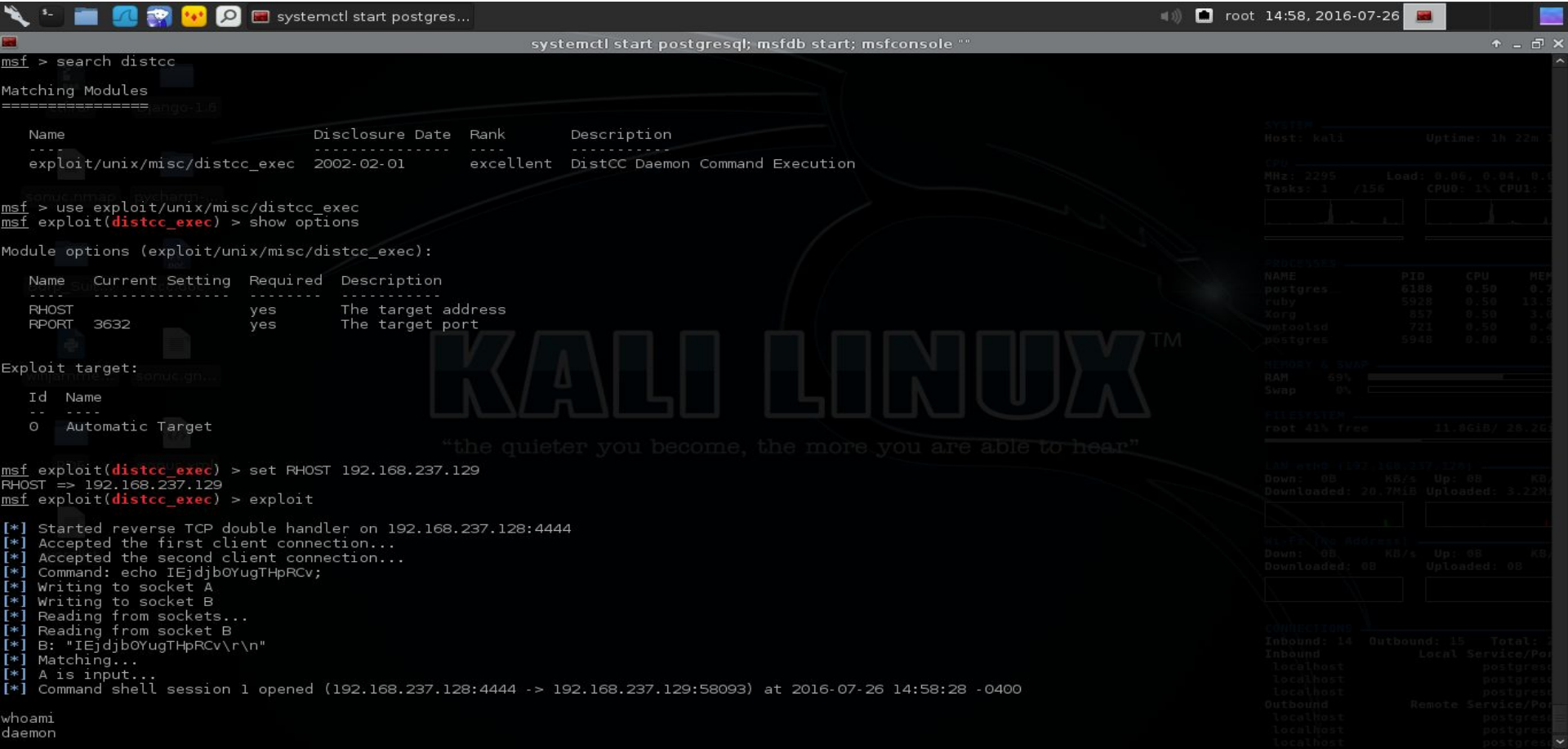
Sızma Testi Örnekleri (Metasploitable2)



Sızma Testi Örnekleri (Metasploitable2)



Sızma Testi Örnekleri (Metasploitable2)

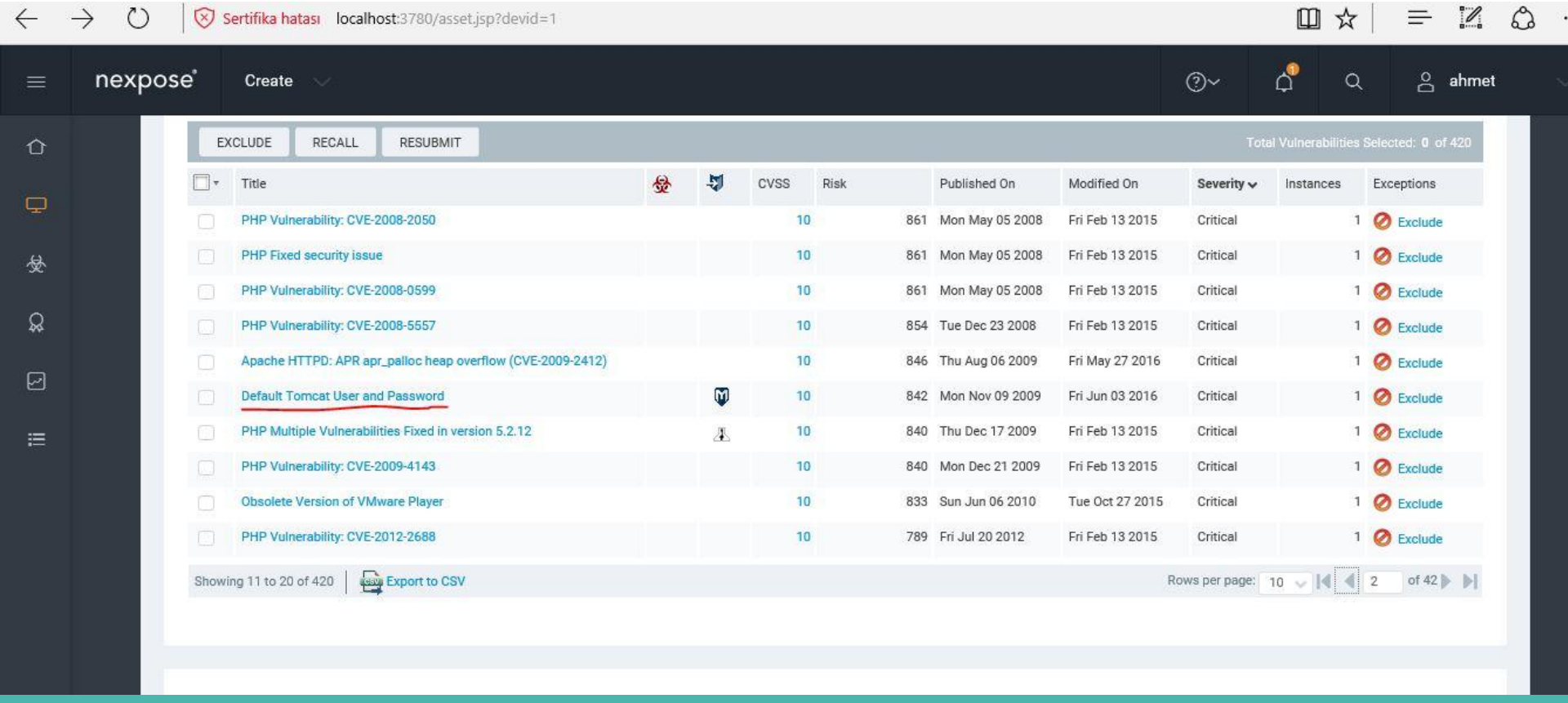


Sızma Testi Örnekleri (Metasploitable2)

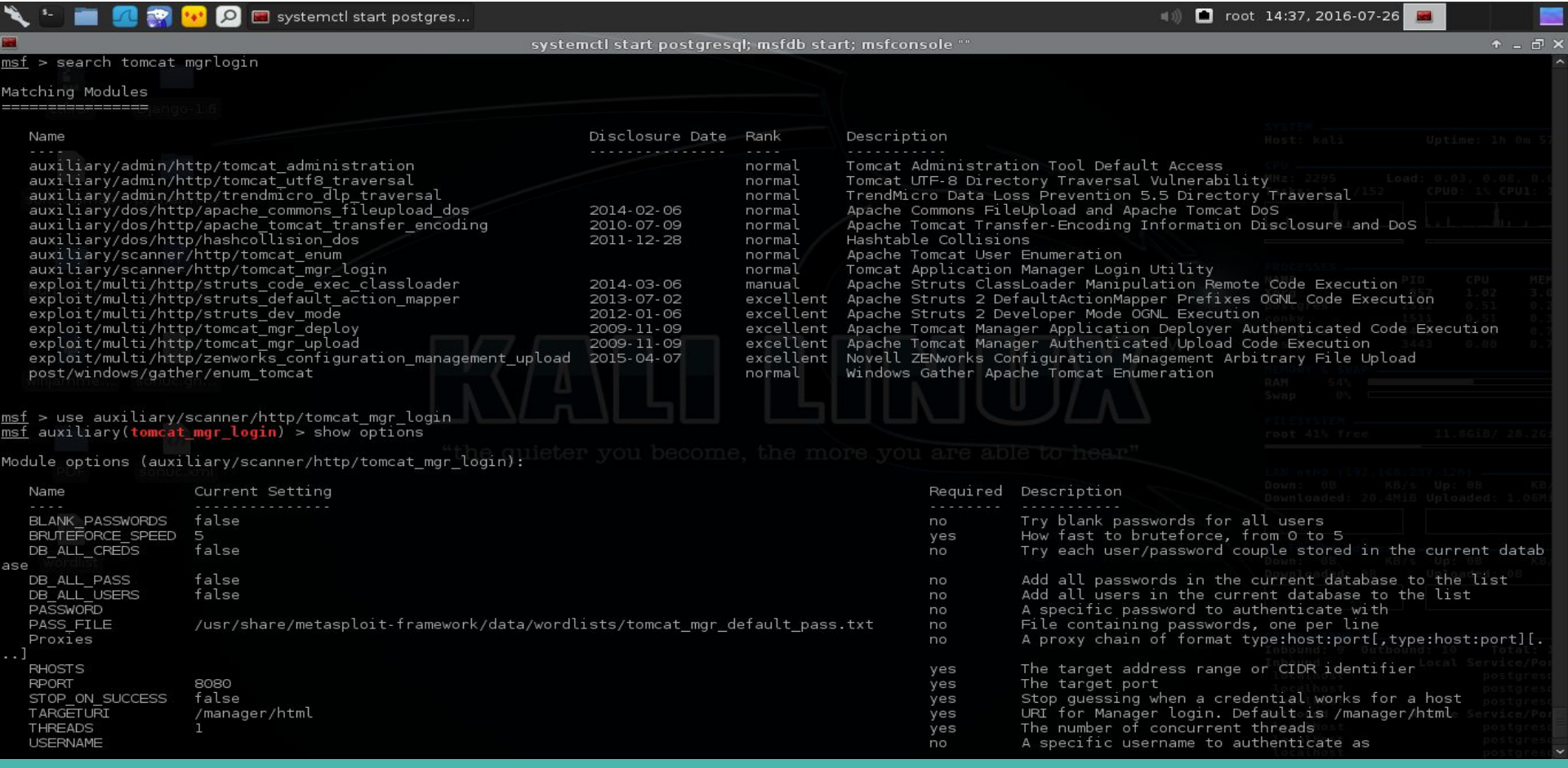
Nmap çıktısında görüldüğü üzere **8180** de Apache Tomcat çalışmakta normalda default olarak **80** yada **8080** de çalışmaktadır.Nexpose çıktısında ise **Default Tomcat User and Password** çıktısı görülmekte.Bunun için **tomcat_mgr_login** adında bir **auxiliary** bulunmakta **Brute Force** (kaba kuvvet) yöntemiyle şifreleri denemekte default yada en çok kullanılan şifreler kısa bir sürede sonuç vermekte.Biz şifrenin default olduğunu bilsekte bu auxliarynin 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)

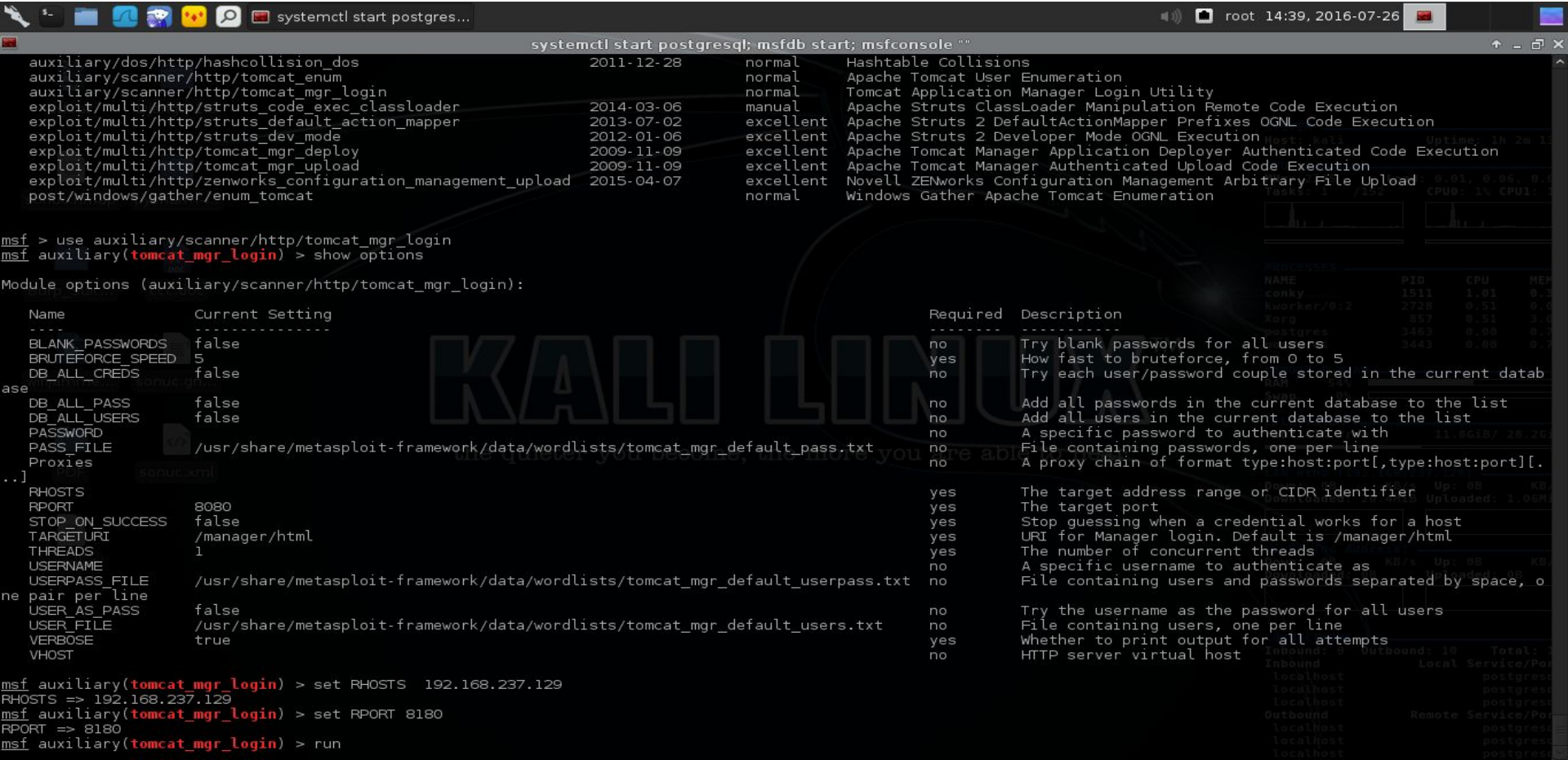
Nexpose çıktısı Default Tomcat Username ve Password



Sızma Testi Örnekleri (Metasploitable2)

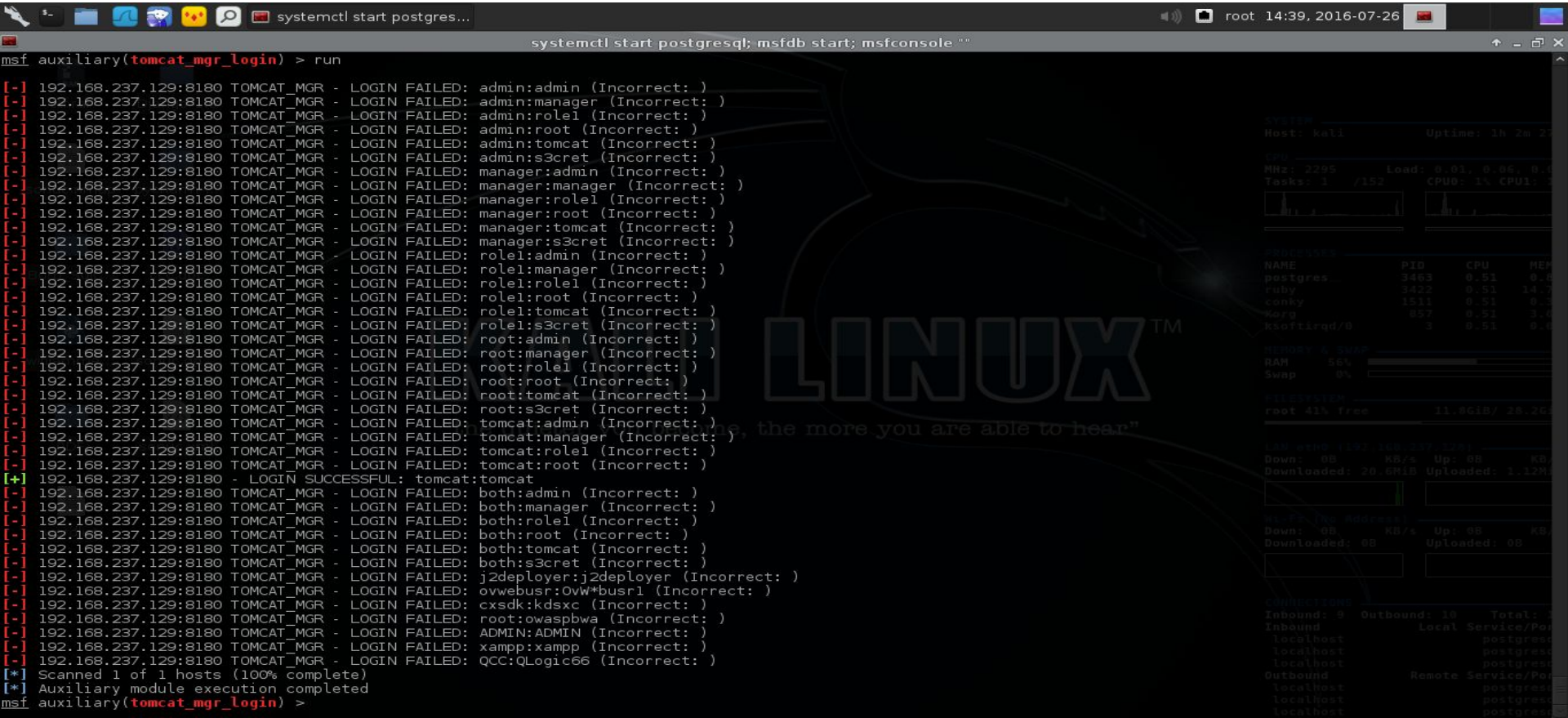


Sızma Testi Örnekleri (Metasploitable2)



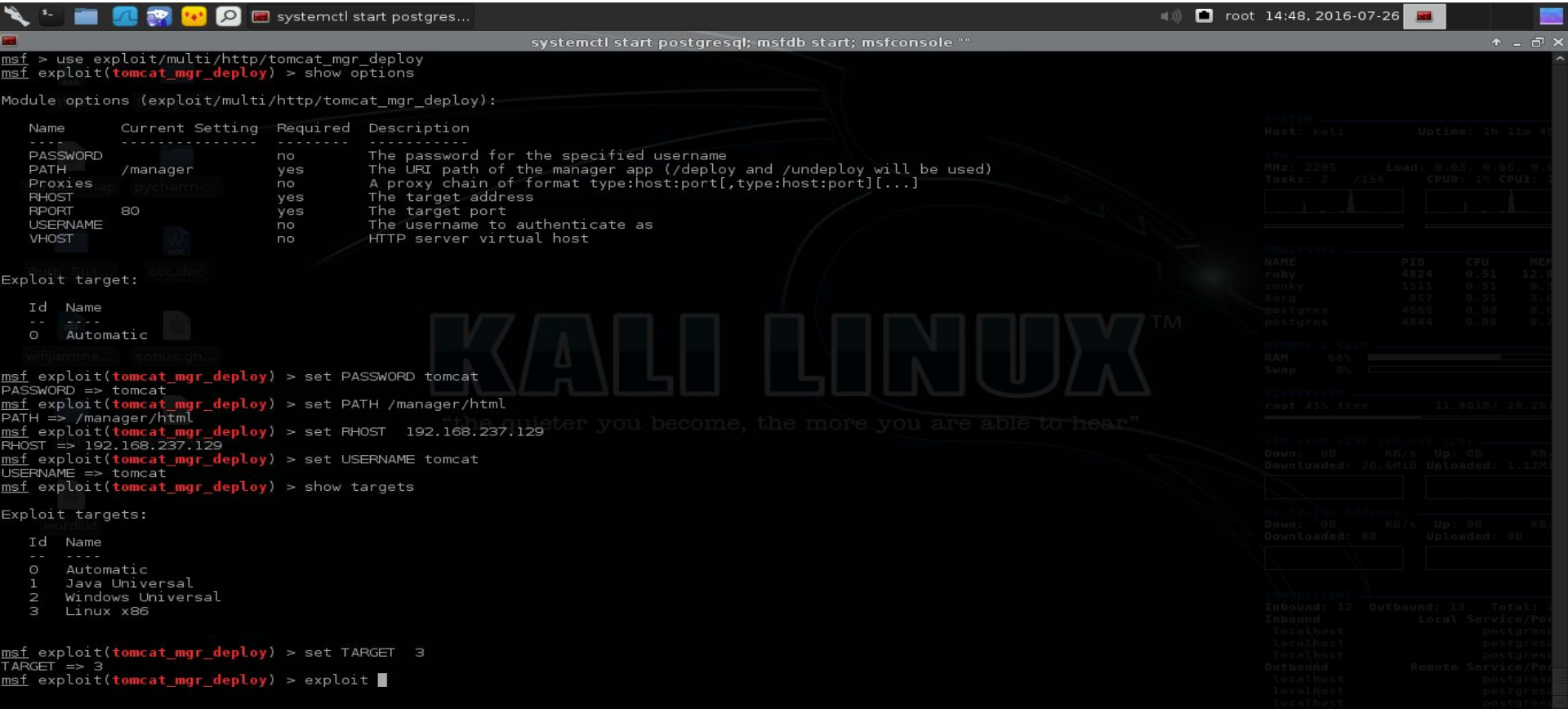
Sızma Testi Örnekleri (Metasploitable2)

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



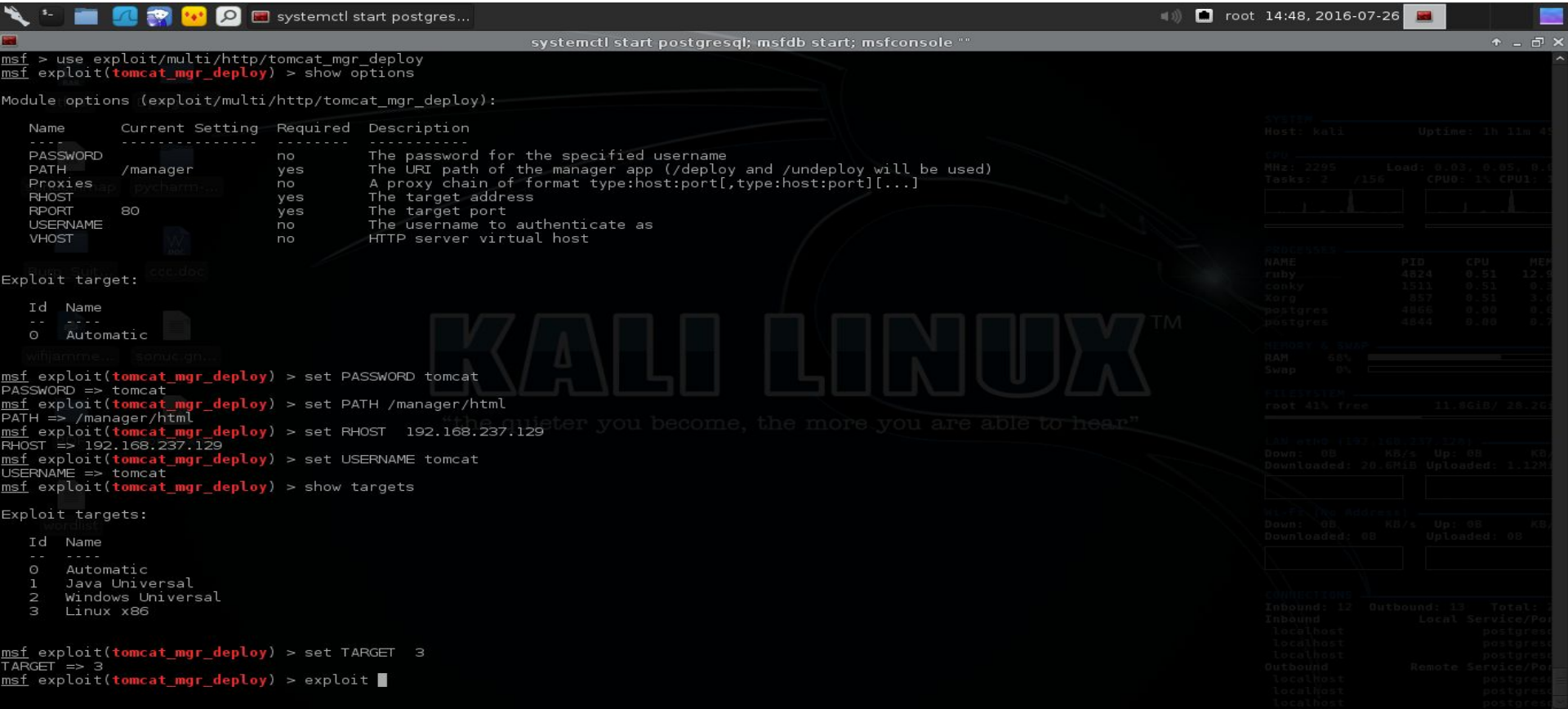
Sızma Testi Örnekleri (Metasploitable2)

Resimdeki gibi tomcat_mgr_deploy exploitimizi seçiyoruz gerekli değerleri atayarak exploiti çalıştırıyoruz.



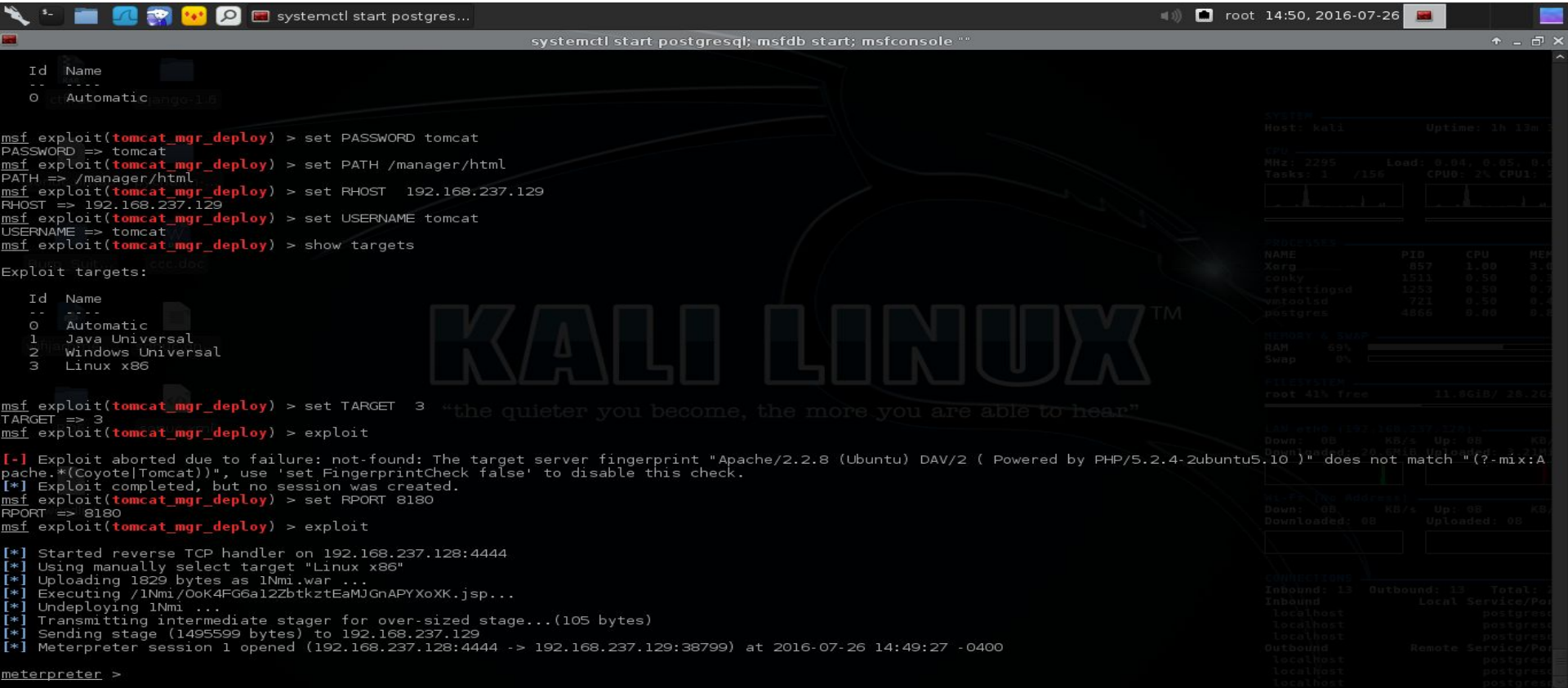
Sızma Testi Örnekleri (Metasploitable2)

Resimdeki gibi tomcat_mgr_deploy exploitimizi seçiyoruz gerekli değerleri atayarak exploiti çalıştırıyoruz.



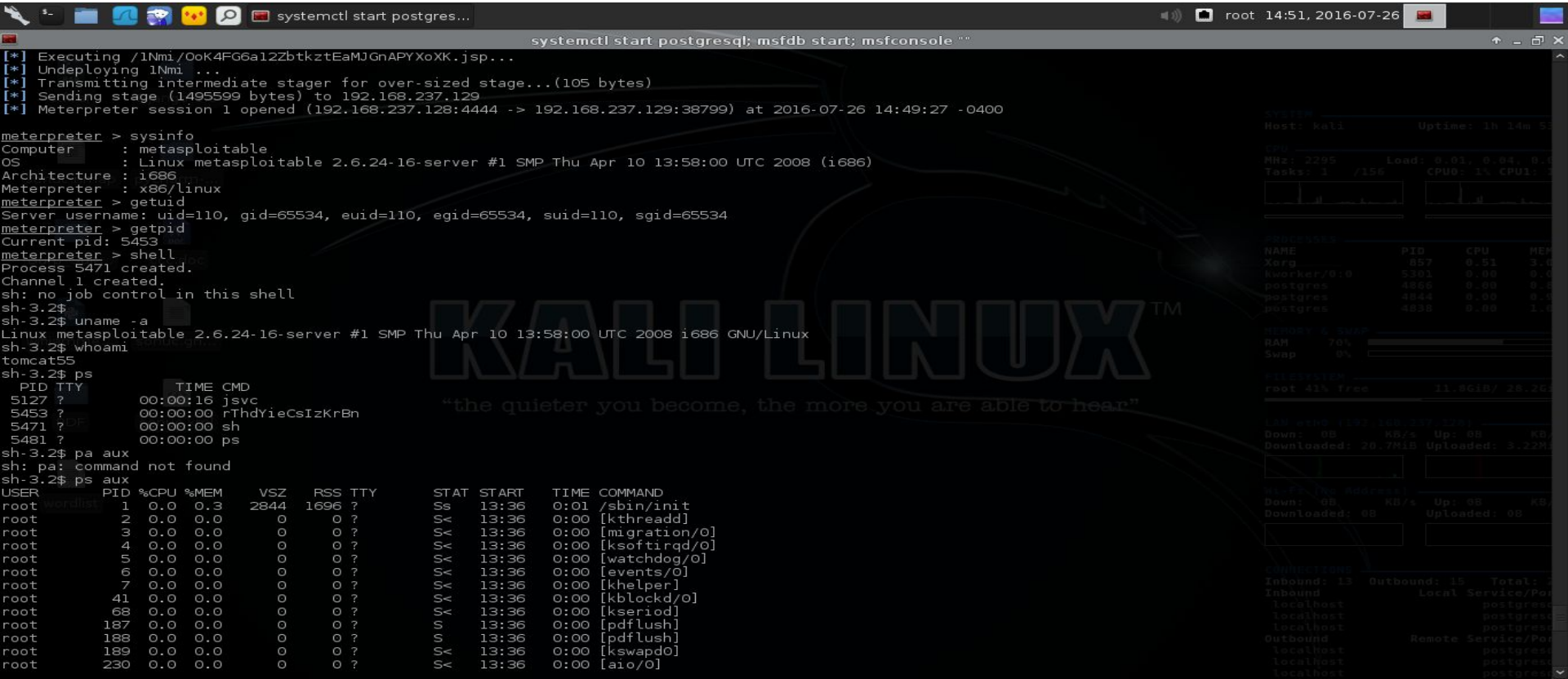
Sızma Testi Örnekleri (Metasploitable2)

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.



Sızma Testi Örnekleri (Metasploitable2)

Meterpreter komutları ile bir kaç bilgi edindik sistem hakkında.



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/cnrkrglu/a-temelleri-caner-krolu

7-http://www.ciscotr.com/subnetting-alt-aglara-bolme.html

8-http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/temel-a%C4%9F-cihazlar%C4%B1

KAYNAKÇA :

9-http://sozluk.cozumpark.com/goster.aspx?id=1379&kelime=information-gathering-for-pentest

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

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

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

13-https://tr.wikipedia.org/wiki/Nmap

14-https://nmap.org/nsedoc/

15-http://gamasec.net/files/msf1.0.pdf

16-http://www.bga.com.tr/calismalar/MetasploitElKitabi.pdf

KAYNAKÇA :

17-https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

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

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