Managing Services

systemctl start “servicename”

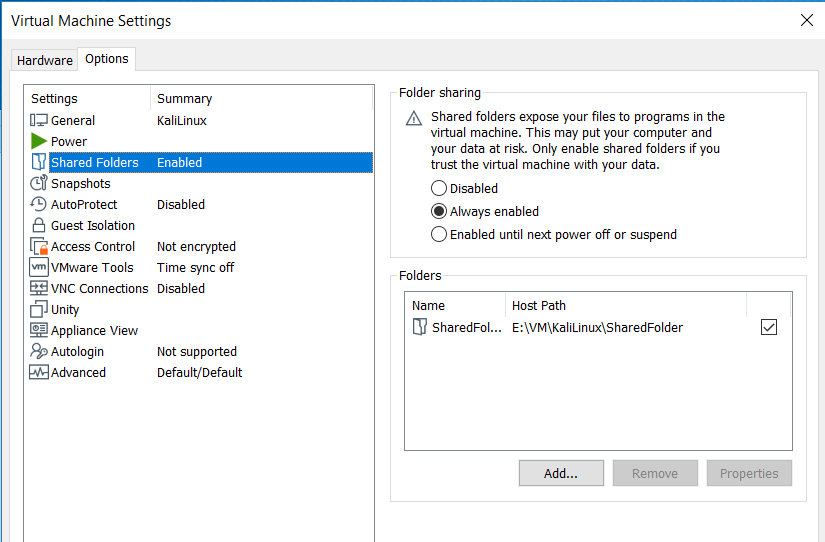
Networking

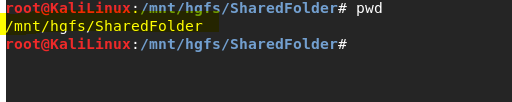
/etc/init.d/networking start

|  |  |
| --- | --- |
|  | vim /etc/network/interfaces |

|  |  |
| --- | --- |
|  | allow-hotplug  iface eth0 inet static  address 192.168.1.130  netmask 255.255.255.0  gateway 192.168.0.1 |

Sharing data between host and Kali





Updating Kali:

vi /etc/apt/sources.list

deb http://http.kali.org/kali kali-rolling main contrib non-free

# For source package access, uncomment the following line

# deb-src http://http.kali.org/kali kali-rolling main contrib non-free

deb http://http.kali.org/kali sana main non-free contrib

deb http://security.kali.org/kali-security sana/updates main contrib non-free

# For source package access, uncomment the following line

# deb-src http://http.kali.org/kali sana main non-free contrib

# deb-src http://security.kali.org/kali-security sana/updates main contrib non-free

deb http://old.kali.org/kali moto main non-free contrib

# For source package access, uncomment the following line

# deb-src http://old.kali.org/kali moto main non-free contrib

apt-get clean

apt-get update

apt-get upgrade

apt-get dist-upgrade -y

apt install “packagename”

getting version details> cat /etc/\*{release,version}

installed packages dpkg -l

Repoları gösterir

cat /etc/ap/sources.list

vi /etc/apt/preferences

(bazı paketlerin update yapmasını engellemek için)

yetkili kullanıcı açmak

useradd -m “username” -G sudo -s /bin/bash

passwd “username”

**INFORMATION GATHERING**

Password common credentials

[**https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials**](https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials)

**/usr/share/wordlists**

Nmap -sV IP -v >> scan.txt (taramaları log’la her zaman)

nmap -sV IP açık port ve servisleri tarar

nmap -e eth0 IP : sadece belirli bir interface üzerinden taramak

Network’deki sadece UP olan hostları taramak ve IP’lerini getirmek

nmap -sn 192.168.1.0/24 -oG - | grep Up | awk '{print $2}'

dnsrecon -d corendonairlines.com (domain’deki srv,soa,A,MX kayıtlarını gösterir)

dnsenum corendonairlines.com

theharvester -d corendonairlines.com -l 300 -b all -f test (sub domainleri getirir)

**--web sitesi içeriği ve dizin yapısı hakkında bilgi toplar--**

skipfish -o skip <http://scanme.nmap.org> (output olarak direktory oluşturup içine bilgilerini index.html’e yazar)

nmap –script http-enum IP -p80

<https://w3techs.com>

wpscan –url something.com -ap -v (wordpress plugin’lerini gösterir)

--wordpress bruteforce attack—

wpscan –url something.com –enumerate u (admin panel kullanıcısını bulur)

wpscan -u something.com/admin –wordlist passwords.txt –username “username”

nikto -h “webserverIP” (web server OS ve version bilgisini verir)

**DMITRY**

dmitry -winseo IP

w: perform whois lookup of domain

i: perform whois lookup of IP

n: retrieve Netcraft.com information

s: search for possible subdomains

e: search for possible e-mail addresses

o: save output

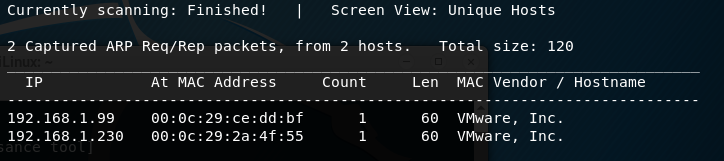
**-belirli bi interface’deki trafiği log’lamak-**

p0f -i eth0 -o log.txt

**NETDISCOVER**

netdiscover --help

netdiscover -r 192.168.1.0/24



**SPARTA**

/etc/sparta.conf

Komut satırından sparta yazılarak scope a network girilir

Nmap’in GUİ’li hali

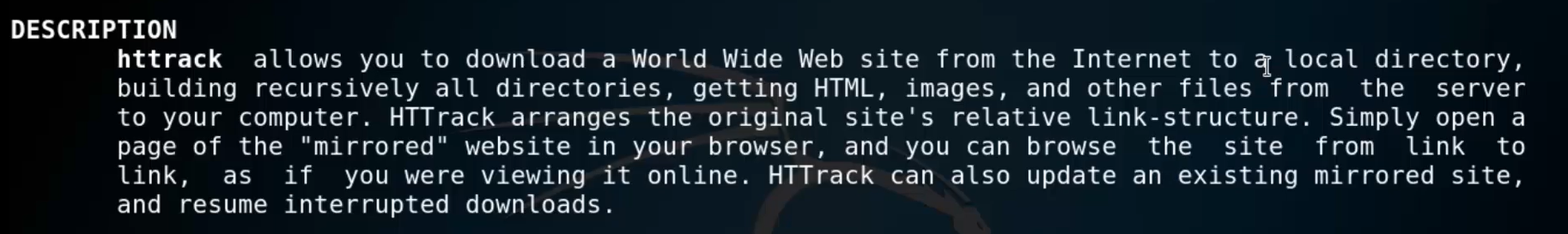
**MALTEGO**

<https://www.paterva.com/web7/community/community.php>

(create account and register for community free edition)

Useful to have graph of web site, domain name, Name servers,

**HTTRACK**



Httrack URL

**VULNERABILITIES**

nmap -sV den gelen servis isimlerinde vulnerability olup olmadığını tara

<https://www.exploit-db.com/>

searchsploit -u (updating exploit db)

işletim sistemine göre exploitlerin bulunduğu konum

/usr/share/exploitdb/exploits

searchsploit “servicename” (lokal konum)

searchsploit -w “servicename” (web)

**(nmap servis taramasındaki sonuca göre zafiyet taramak)>>LİMİTED**

nmap -sV -oX output.xml 192.168.1.99

searchsploit –nmap output.xml

**NMAP Scripts-Getting Help**

locate \*.nse

nmap –script-help “scriptname”.nse

**OPENVAS (open source vulnerability scanner)**

apt-get update  
apt-get dist-upgrade

apt-get install openvas

openvas-nvt-sync

openvas-setup

<https://127.0.0.1:9392>

default user :admin

password(given in installation) = 1345de6e-b2e5-4a96-9ddd-bad7a0b355ff

(change password from console)

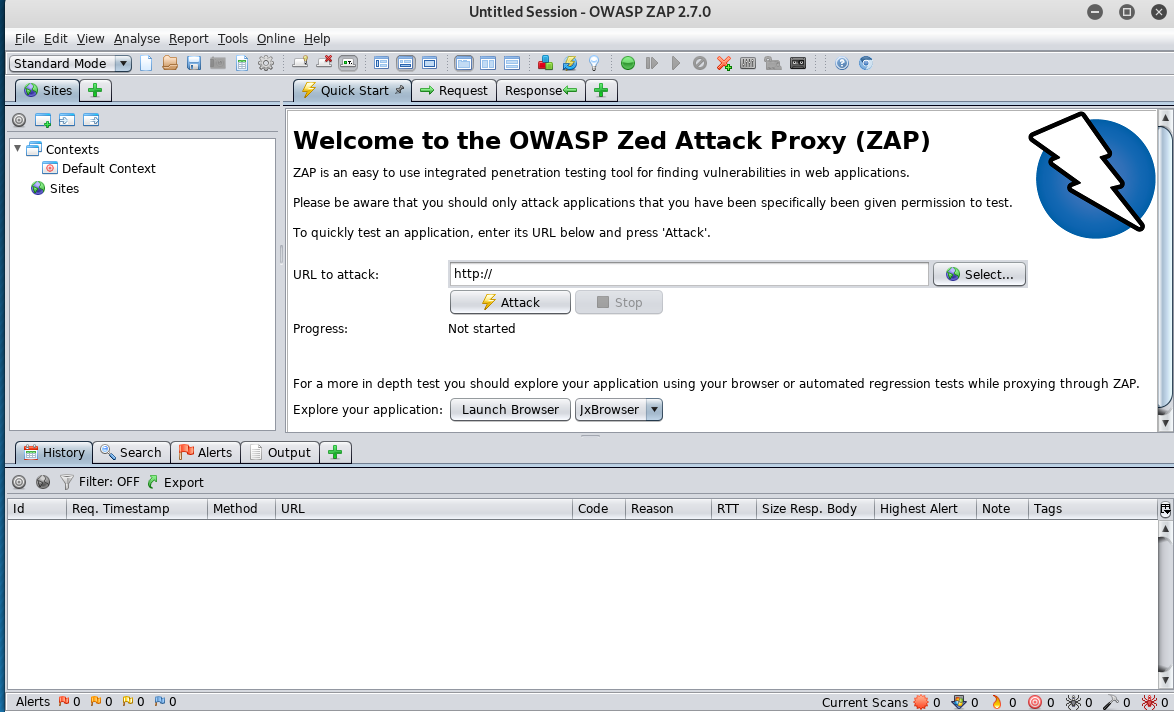
openvasmd –create-user=username (create new user)

openvas-start

openvas-stop

**WEB APPLICATION VULNERABIITY ANALYSIS**

**Owasp-zap**



Siteye ait sub domain’leri de gösterir

**VEGA (web application vulnerability analysis)**

apt-get clean

apt-get update

apt-get upgrade

apt-get dist-upgrade -y

apt install “packagename”

apt-get install vega -y

**Creating Password List**

Crunch minchar maxchar “pattern” -o passwd.txt

Crunch 5 7 yigit -o passwd.txt

rsmangler -a -c -d -e -i -l -p -r -s -u -y –pnb –na –nb -f easypass.txt > goodpass.txt

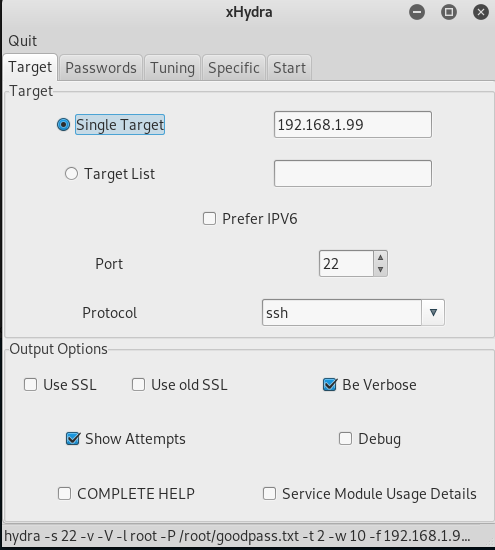
(verilen kelime kombinasyonlarıyla şifre oluşturur)

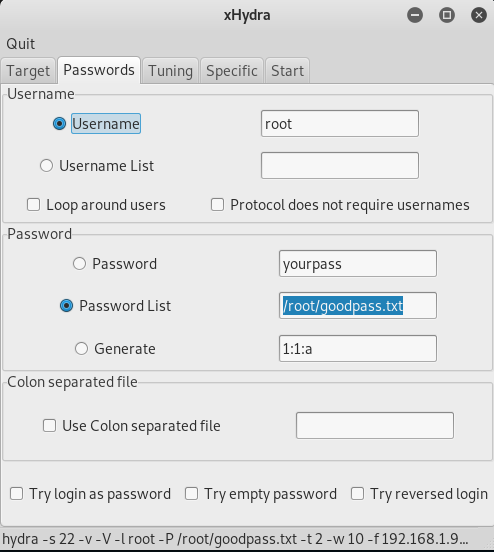
Cewl WEBIP -w pass.txt -d 3

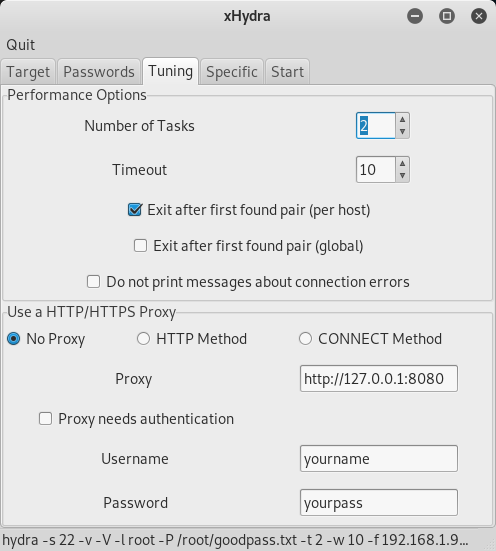
(web uygulamasındaki kelimelerden şifreler oluşturur)

**General Password Cracker (all services)**

xhydra







**FTP Password Cracker**

hydra -t 20 -l admin -P /usr/share/john/password.lst -vV 192.168.1.99 ftp

(-l den sonra kullanıcı ismini .txt’den de alabilir)

(more reliable but slow)

medusa -h 192.168.1.99 -u rte -P password.lst -M ftp

medusa -h 192.168.1.99 -u user.lst -P password.lst -M ftp

**SSH Password Cracker**

hydra -l root -P passwords.txt IP ssh

ncrack -p 22 --user root -P passwdlist 192.168.1.99

**RDP Password Cracker**

ncrack -u administrator -P passwdlist -p 3389 10.212.50.21

**MAC Changer**

macchanger -s eth0 (shows mac address of interface)

macchanger -A eth0 (set any vendor mac address to interface)

macchanger -r eth0 (set random mac address to interface)

macchanger -p eth0 (roll backs to original mac)

macchanger -l (lists all known vendor mac addresses)

**PHISH ATTACK**

SET toolkit

1) Social-Engineering Attacks

2) Website Attack Vectors

3) Credential Harvester Attack Method

1) Web Templates

IP address of host:

2-google

**DATABASE PEN.**

JSQL TOOL

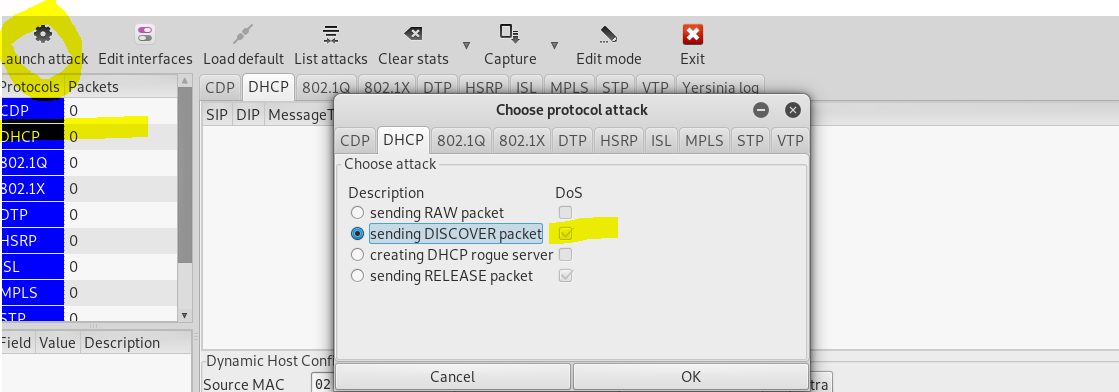
**MISC**

(web sayfasının tamamının ekran görüntüsünü almak)

cutycapt --url=”url” --out=screenshot.jpeg

**DHCP Starvation Attack**

Yersinia -G



Solution port security (minimize requests to DHCP server)

**DNS SPOOFING**

(on Kali, IP:192.168.1.130)

echo 1 > /proc/sys/net/ipv4/ip\_forward

vi /etc/ettercap/etter.dns

\*.yaydog.local A 192.168.1.130

ettercap -T -q -M arp:remote -P dns\_spoof

bütün yaydog.local isteklerini kaliye yönlendirir

**PING’e kapalı sunucuyu tespit etmek**

Nmping “IP”

**ROOTKIT SEARCH**

Apt-get install rkhunter

rkhunter –check (on local system)

OR

Chkrootkit