

آموزش کاربردی تست نفوذ

با

Kali Linux

مهندس علیرضا عظیمزاده میلانی

مهندس حمیدرضا نیکخواه

انتشارات پندار پارس

سرشناسه	: عظیمزاده میلانی، علیرضا، ۱۳۷۰ -
عنوان و نام پدیدآور	: آموزش کاربردی تست نفوذ با Kali Linux / علیرضا عظیمزاده میلانی، محمدرضا نیکخواه.
مشخصات نشر	: تهران : پندار پارس ، ۱۳۹۳ .
مشخصات ظاهری	: ۳۶۸ ص. : مصور، جدول.
شابک	: 978-600-6529-66-0 : ۲۵۰۰۰۰ ریال: همراه با دو حلقه لوح فشرده دیجیتال
وضعیت فهرست نویسی	: فیبا
موضوع	: سیستم عامل لینوکس
موضوع	: سیستم‌های عامل (کامپیوتر)
موضوع	: آزمایش نفوذ (ایمن‌سازی کامپیوتر)
موضوع	: هکرها
شناسه افزوده	: نیکخواه، حمیدرضا، ۱۳۶۴ -
رده بندی کنگره	: ۱۳۹۳ ۷۶/۷۶۰۸ : ۹۴۶س/
رده بندی دیویی	: ۴۳۲/۰۰۵
شماره کتابشناسی ملی	: ۳۶۷/۸۲۴

انتشارات پندارپارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ www.pendarepars.com

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴ info@pendarepars.com



نام کتاب : آموزش کاربردی تست نفوذ با **Kali Linux**

ناشر : انتشارات پندار پارس

تالیف : علیرضا عظیمزاده میلانی، حمیدرضا نیکخواه

چاپ نخست : دی ماه ۹۳

شمارگان : ۱۵۰۰ نسخه

طرح جلد : رامین شکرالهی

لیتوگرافی، چاپ، صحافی : ترام سنچ، فرشویه، خیام

قیمت : ۲۵۰۰۰ تومان به همراه دو حلقه **DVD** شابک : ۹۷۸-۶۰۰-۶۵۲۹-۶۶-۰



*هرگونه کپی برداری کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

فهرست

۱	پیش‌گفتار
۵	فصل نخست، آغاز کار با KALILINUX
۵	مقدمه - تفاوت BackTrack با KaliLinux
۶	لینوکس - گنو لینوکس
۶	ویژگی‌های سیستم‌عامل کالی لینوکس
۷	دانلود سیستم‌عامل کالی لینوکس
۸	روش نخست: نصب کالی بر روی ماشین مجازی (VirtualBox)
۱۳	نصب Guest-Additions بر روی VirtualBox
۱۴	روش دوم: نصب کالی در کنار سیستم‌عامل‌ها (Dual-Boot یا Multi-Boot)
۲۲	روش سوم: نصب کالی بر روی USB:Flash-Memory
۲۳	روش چهارم: نصب کالی در گوشی‌های هوشمند آندروید
۲۶	Root کردن سیستم‌عامل آندروید
۲۷	ترمیم Boot-GRUB، پس از نصب سیستم‌عامل جدید
۲۷	درباره‌ی گراب (GRUB)
۲۹	فعال‌سازی سرویس‌های لینوکس
۳۰	راه‌اندازی شبکه وایرلس
۳۱	تغییر رمزعبور کاربر ریشه (root)
۳۲	ایجاد چند زبانی در Keyboard
۳۲	رفع مشکلات احتمالی پس از نصب کالی لینوکس
	۱. نصب و بازسازی مخزن‌ها: 33
۳۵	۲. نصب Flash:
۳۵	۴. نصب Archive Manager:
۳۶	۵. فعال‌سازی Network-Manager:
۳۷	مدیریت بسته‌ها به صورت گرافیکی
۳۸	مدیریت بسته‌های توزیع دبیان با dpkg
۴۱	کار با خط فرمان و دستوره‌های لینوکس (Command-line)
۴۹	انواع symbolها
۵۱	فصل دوم، سفارشی‌سازی کالی لینوکس
۵۱	مدیریت بسته‌های توزیع دبیان با apt-get
۵۴	آماده‌سازی Kernel-Headers
۵۴	اجزای نسخه‌های کرنل لینوکس
۵۵	نصب درایور وای‌فای BroadCom
۵۸	تنظیم پروکسی‌ها با ProxyChains
۵۹	به اشتراک گذاشتن منابع بین Windows و KaliLinux با Samba
۶۲	رمزنگاری دایرکتوری‌ها با TrueCrypt
۶۵	ساخت اهداف اضافی در VirtualBox

۶۷.....	حمله به WordPress و دیگر برنامه‌های کاربردی
۷۱.....	فصل سوم، جمع‌آوری اطلاعات (INFORMATION GATHERING)
۷۱.....	DNS Enumeration چیست؟
۷۳.....	ابزار dnsenum
۷۴.....	درباره‌ی WHOIS
۷۴.....	ابزار dnsdict6
۷۵.....	ابزار dnsmap
۷۶.....	ابزار dnswalk
۷۷.....	ابزار fierce
۷۷.....	ابزار urlcrazy
۷۸.....	SNMP Enumeration چیست؟
۷۹.....	MIB چیست؟
۷۹.....	ابزار snmpwalk
۸۱.....	ابزار snmpcheck
۸۲.....	NetBIOS Enumeration و SMB چیست؟
۸۴.....	تعیین‌کردن بازه شبکه
۸۴.....	ابزار dmitry
۸۶.....	ابزار scapy
۸۸.....	شناسایی و تشخیص ماشین‌های فعال با Nmap
۹۰.....	تکنیک‌های Nmap-Scanning
۹۰.....	TCP-SYN-scan
۹۲.....	TCP-FIN-scan
۹۴.....	TCP-Xmas-scan
۹۵.....	TCP-Null-scan
۹۷.....	TCP-IDLE-scan
۹۸.....	مراحل انجام TCP-IDLE-scan در وضعیت پورت باز
۹۸.....	مراحل انجام TCP-IDLE-scan در وضعیت پورت بسته
۹۹.....	مراحل انجام TCP-IDLE-scan در وضعیت پورت فیلتر
۱۰۰.....	نکات تکنیک IDLE-scan
۱۰۱.....	UDP-scan
۱۰۳.....	Ping-scan
۱۰۵.....	TCP-Connect-scan
۱۰۶.....	IP-Protocol-scan
۱۰۹.....	TCP-ACK-scan
۱۱۱.....	TCP-Window-scan
۱۱۲.....	RPC-scan
۱۱۳.....	کشف پورت‌های باز - انگشت نگاری سیستم‌عامل و سرویس‌ها با Nmap
۱۱۷.....	نمایش وضعیت پورت‌ها با Nmap
۱۲۲.....	ارزیابی تهدید با Maltego
۱۲۹.....	فصل چهارم، ارزیابی آسیب‌پذیری‌ها (VULNERABILITY ASSESSMENT)

۱۲۹	Vulnerability چیست؟
۱۳۰	نصب، پیکربندی و اجرای Nessus + Plugins
۱۳۴	کشف آسیب‌پذیری‌های محلی با Nessus
۱۳۸	کشف آسیب‌پذیری‌های شبکه با Nessus
۱۴۳	کشف آسیب‌پذیری‌های لینوکس با Nessus
۱۴۸	کشف آسیب‌پذیری‌های ویندوز با Nessus
۱۵۳	نصب، پیکربندی و اجرای OpenVAS + Plugins
۱۵۸	استفاده از OpenVAS-Desktop
۱۵۸	کشف آسیب‌پذیری‌های محلی با OpenVAS
۱۶۳	کشف آسیب‌پذیری‌های لینوکس با OpenVAS
۱۶۵	کشف آسیب‌پذیری‌های ویندوز با OpenVAS
۱۶۹	کشف آسیب‌پذیری‌های شبکه با OpenVAS
۱۷۳	فصل پنجم، بهره‌برداری از آسیب‌پذیری‌ها (EXPLOITING VULNERABILITIES)
۱۷۴	طبقه‌بندی پیلودهای متاسپلویت
۱۷۷	طبقه‌بندی اکسپلویت‌های متاسپلویت
۱۸۱	انواع اکسپلویت‌ها از نظر نوع دسترسی
۱۸۱	نصب و پیکربندی شبیه‌ساز (Emulator) آندروید
۱۸۷	نصب و پیکربندی Metasploitable
۱۹۰	مدیریت متاسپلویت با ابزار گرافیکی Armitage
۱۹۱	استفاده از محیط کنسول متاسپلویت (MSFCONSOLE)
۱۹۴	استفاده از واسط کاربری متاسپلویت (MSFCLI)
۱۹۶	کار با Meterpreter متاسپلویت
۲۰۳	افزودن ماژول جدید به متاسپلویت
۲۰۴	حمله به گوشی‌های هوشمند آندروید
۲۰۶	Metasploitable MySQL
۲۰۸	Metasploitable PostgreSQL
۲۰۹	Metasploitable Tomcat
۲۱۰	Metasploitable PDF
۲۱۳	Metasploitable Samba-Symlink
۲۱۶	پیاده‌سازی خودکار حملات با Browser_Autopwn
۲۱۸	نصب برنامه و ماشین‌های مجازی آسیب‌پذیر (لابراتور)
۲۲۰	نصب و پیکربندی برنامه آسیب‌پذیر Mutillidae + یک حمله SQLi
۲۲۲	SQL Injection چیست؟
۲۲۴	نصب آخرین نسخه متاسپلویت از طریق GitHub
۲۲۵	فصل ششم، کسب مجوز (PRIVILEGE ESCALATION)
۲۲۶	استفاده از نشان‌های جعلی
۲۳۰	گریز از دستان آنتی‌ویروس
۲۳۹	ساخت درپشتی (Backdoor) ماندگار
۲۴۵	پاکسازی ردپا
۲۴۶	پیاده‌سازی حمله MITM

۲۵۳	آشنایی با حملات مهندسی اجتماعی (SET)
۲۵۵	Website-Cloning با SET
۲۵۹	پیاده‌سازی حمله فیشینگ (Phishing) با SET
۲۶۲	پیاده‌سازی حملات تحت‌وب با BeEF
۲۶۷	فصل هفتم، حمله به شبکه‌های وایرلس (WIRELESS INJECTION)
۲۶۷	پروتکل‌های امنیتی در شبکه‌های وایرلس
۲۷۱	فیلدهای ابزار airodump-ng
۲۷۵	کلیدهای میانبر تعاملی در هنگام کار با airodump-ng
۲۷۷	4-Way Handshake
۲۸۱	کشف گذرواژه شبکه وایرلس WEP با Client
۲۹۴	کشف گذرواژه شبکه وایرلس WEP بدون Client
۲۹۹	کشف گذرواژه شبکه وایرلس WPA(2) با PasswordList
۳۰۴	کشف گذرواژه شبکه وایرلس WPA(2) بدون PasswordList
۳۰۵	آشکارسازی نام اکسس پوینت‌های پنهان (Hidden-SSID)
۳۰۷	نرم‌افزار وایرشارک (wireshark) چیست؟
۳۰۹	حملات تکذیب سرویس DOS
۳۱۲	حمله به استاندارد WPS (Wi-Fi Protected Setup)
۳۱۷	افزایش توان خروجی کارت شبکه وایرلس (WNIC Booster)
۳۱۹	پیاده‌سازی حملات Evil-Twin در پروتکل امنیتی WPA(2)-PSK
۳۲۳	پیکربندی Wi-Fi HoneyPot
۳۲۸	پیاده‌سازی حمله Fake-Page + Evil-Twin
۳۳۴	پیاده‌سازی حمله MITM (Man-In-The-Middle)
۳۳۹	حمله به RADUIS و WPA(2)-Enterprise(EAP-MD5)

پیش‌گفتار

خواندن این کتاب برای کسانی مفید خواهد بود که با مباحث Network+ و سیستم‌عامل‌های لینوکسی آشنایی دارند. همچنین افرادی که می‌خواهند به صورت کاربردی و عملی دوره "تست‌نفوذ با کالی لینوکس" را فرا گیرند نیز می‌توانند از این کتاب استفاده کنند.

مطالب مورد بحث در این کتاب شامل مثال‌های زیادی از کارهای عملی دوره‌های CEH^۱، PWK^۲، WiFu^۳، AWE^۴ و تشریح خط به خط دستورها می‌باشد. به گونه‌ای که خواننده این کتاب توانایی کار عملی در پروژه‌های مربوط به دوره‌های نام برده در بالا را کسب نماید.

مطالب این کتاب به صورت کاملاً ساده و همراه با تصاویر و آخرین تغییرات در ابزارها تشریح شده است که نیاز دانشجویان را برای یادگیری کاربردی چهار دوره نام برده شده در بالا را بر طرف می‌نماید. همچنین در نگارش این کتاب اطلاعات فنی و تجربی بسیاری که برای یادگیری آنها نیاز به چند سال تجربه می‌باشد گنجانده شده است.

پیشنهاد می‌شود که خوانندگان، هر فصل را یکبار تا پایان بخوانند و سپس بهترین روش را برای یادگیری انتخاب کنند. به نکات، اخطارها و پیشنهادهایی که در فصل‌ها به آن اشاره شده است دقت نمایید. هرگونه ایراد یا خطای فنی در کتاب را به ایمیل نویسنده (ali.azimzadeh70@gmail.com) با موضوع "کتاب کالی لینوکس" ارسال فرمایید.

از حمایت‌های مادی و معنوی شما خوانندگان عزیز که از کپی برداری، اسکن و الکترونیکی کردن کتاب پرهیز می‌نمایید و مؤلفان و ناشر را برای تألیف و نشر کتاب‌های بعدی یاری می‌رسانید، بسیار سپاسگزار می‌نمایم.

به همراه کتاب دو عدد DVD ارائه شده است. DVD نخست شامل نسخه ۳۲ بیتی سیستم‌عامل کالی لینوکس، و DVD دوم شامل ابزارهای مورد نیاز برای کار با دستورات کتاب می‌باشد.

¹ Penetration-Testing With KaliLinux

² Certified Ethical Hacker

³ Offensive Security Wireless Attacks

⁴ Advanced Windows Exploitation

(ali.azimzadeh70@gmail.com)**درباره علیرضا عظیم زاده میلانی**

مهندس علیرضا عظیم زاده میلانی فارغ التحصیل رشته مهندسی کامپیوتر- نرم افزار از دانشگاه آزاد اسلامی واحد کرج می باشد. وی دارای مدارک دوره های تخصصی CCNA، CEH، Security+ و از مؤسسه سایبرک تهران و متخصص در زمینه های WiFu، LPIC، RHCSA، IDS، LinuxFirewalls و Programming می باشد و در پروژه VLAN بانک تجارت استان زنجان نیز همکاری داشته است. همچنین برگزار کننده و سخنران سمینارهای علمی درباره "راهکارهای نفوذ و مقابله با تهدیدها در شبکه ها" در قم، نیشابور و کرج بوده است و همچنین مؤلف و مترجم کتاب های الکترونیکی "هک و امنیت با بک ترک" و "مدیریت سرورهای لینوکسی با CentOS" می باشد.

(info@hrnikkhah.com)**درباره حمیدرضا نیک خواه**

مهندس حمیدرضا نیک خواه، طراح و مشاور امنیت شبکه های کامپیوتری و مدرس امنیت اطلاعات و شبکه های کامپیوتری می باشند. ایشان با بیش از سیزده سال تجربه کاری در زمینه ی IT و یازده سال Certified میکروسافت، به عنوان طراح و مشاور و مجری پروژه های شبکه و امنیت اطلاعات برای سازمان های متوسط و بزرگ با تمرکز بر طراحی و مدیریت امنیت، ارتباطات شبکه و برنامه ها برای بانک ها و سازمان های توسعه یافته، مشغول به فعالیت هستند. بیش از دوازده هزار ساعت تدریس شبکه و امنیت اطلاعات برای مؤسسات و سازمان های بزرگ، سخنران سمینارهای امنیت اطلاعات در دانشگاه ها و نمایشگاه ها و حضور در برنامه های تلویزیونی مرتبط با فناوری اطلاعات و امنیت به عنوان متخصص امنیت، از جمله فعالیت های آموزشی ایشان به شمار می رود.

بخشی از مدارک تخصصی مدیریت شبکه و امنیت شبکه ایشان:

- 1-Microsoft Certified Professional(MCP)
- 2-Microsoft Certified Systems Administrator(MCSA)
- 3-Microsoft Certified Systems Engineer(MCSE)
- 4-Cisco Certified Network Associate(CCNA)
- 5-Microsoft Certified Technician Specialist (MCTS)
- 6-Microsoft Certified IT Professional(MCITP) Enterprise Administrator
- 7-MCSA Security
- 8-MCSE Security
- 9- Security+ 2008
- 10-Certified Ethical Hacker (CEH)
- 11-EC-Council Education Continuing (ECE)
- 12-Certified Information Systems Security Professional (CISSP)

سخنی با خوانندگان (نامه سرگشاده به ...)

سلام

تیر ۹۳ به همراه همکاران عزیزم در تیم امنیتی ایران برای برگزاری سمیناری با موضوع "تست نفوذ و امنیت در شبکه" به شهر مقدس قم سفر کردیم. پس از اتمام سمینار و استقبال و تشکر مهمانان از سخنرانان سمینار، این پرسش در ذهن حاضران بود که از فارغ التحصیلان یا دانشجویان دانشگاه دولتی هستیم یا خیر؟

این ذهنیت غلط در اذهان عموم جامعه وجود دارد که فارغ التحصیلان و دانشجویان دانشگاه‌های دولتی نسبت به فارغ التحصیلان و دانشجویان دانشگاه‌های آزاد اسلامی نخبه‌تر و با سوادتر هستند. حتی آن دسته از عزیزانی که در دهه‌ی ۷۰ از دانشگاه‌های آزاد اسلامی فارغ التحصیل شده‌اند، حتماً به یاد می‌آورند که شرکت‌ها، کارخانه‌ها و کارآفرینان چندان نسبت به استخدام فارغ التحصیلان دانشگاه‌های آزاد اسلامی مایل نبودند.

اینک دو دهه از آن روزها گذشته است و امسال در تیر ۹۳، من نیز با همان پرسش‌ها مواجه شدم که آیا دانشجوی دانشگاه دولتی هستم؟ خیر. اینجانب علیرضا عظیم زاده میلانی دانشجوی دانشگاه آزاد اسلامی واحد کرج در رشته‌ی مهندسی کامپیوتر - نرم‌افزار می‌باشم. اگر چه قبولی در دانشگاه‌های دولتی به بنیهِی علمی قوی احتیاج دارد؛ مثلاً برای ورود به مقطع کارشناسی باید از بنیهِی علمی خوبی در مقطع دبیرستان برخوردار بود، یا برای ورود به مقطع ارشد باید از بنیهِی علمی خوبی در مقطع کارشناسی برخوردار بود؛ اما این بدین معنا نیست که دانشجوی مقطع کارشناسی یا ارشد به هنگام فارغ التحصیلی از توان علمی خوبی نیز برخوردار است. امروز مهم نیست از دانشگاه آزاد فارغ التحصیل می‌شویم یا دولتی. بلکه آنچه مهم است توان علمی بالای فارغ التحصیلان است.

علیرضا عظیم زاده میلانی

دانشجوی دانشگاه آزاد اسلامی - واحد کرج

رشته مهندسی کامپیوتر - نرم‌افزار

فصل نخست

آغاز کار با KaliLinux

مقدمه – تفاوت KaliLinux با BackTrack

انتخاب میان کالی لینوکس و بکترک برای کاربران، به‌ویژه کاربران تازه وارد، یک انتخاب مبهم است. بکترک یک توزیع لینوکس ویژه‌ی متخصصان امنیت بوده است و می‌باشد. این توزیع برای تست‌های امنیتی طراحی شده است و با بهترین نرم‌افزارهای آزاد و متن باز عرضه می‌شود. آخرین ویرایش این سیستم‌عامل BackTrack 5 R3 است. پس از این ویرایش، توسعه دهندگان تصمیم گرفتند تا توزیع‌شان را بازسازی کنند. نتیجه تلاش آنها کالی لینوکس بود. بنابراین، هم‌اینک بکترک با نام جدید کالی لینوکس شناخته می‌شود، و کالی لینوکس چیزی است که باید به دنبالش باشید. پس، جدا از نرم‌افزارهای به‌روز شده و تغییر نام یافته، واقعا تفاوت بکترک و کالی لینوکس در چیست؟

مهم‌ترین تفاوت‌ها عبارتند از:

- (۱) بکترک بر پایه اوبونتو است، در حالی که کالی لینوکس بر پایه آخرین نسخه دبیان است.
- (۲) تفاوت مهم دیگر این است که چون بسته‌های اوبونتو با بسته‌های دبیان چندان سازگار نیستند، بهتر است خود را برای سوئیچ به سمت کالی لینوکس آماده کنید.
- (۳) آخرین تفاوتی که ارزش توجه کردن دارد این است که، در بکترک حق انتخاب بین دو میزکار KDE و Gnome2 را ندارید؛ اما در کالی لینوکس شما می‌توانید میزکار مورد نظر خود را انتخاب کنید و یا میزکارهای پیش‌فرض که Gnome3 می‌باشد را برگزینید.

لینوکس - گنو لینوکس^۱

لینوکس به تنهایی یک هسته (Kernel) است. هسته، بخش اصلی سیستم‌عامل را تشکیل می‌دهد که کار آن کنترل داده‌ها، مدیریت حافظه، سخت‌افزار، ورود و خروج داده‌ها و تمامی موارد اصلی سیستم‌عامل می‌باشد. لینوکس با استفاده از ابزارهایی که پروژه متن‌باز گنو (GNU) برای آن تولید کرده است، تبدیل به یک سیستم‌عامل کامل می‌شود (به همین دلیل معمولاً لینوکس را گنو/لینوکس یا GNU/Linux می‌نامند) و با اضافه کردن دیگر نرم‌افزارهای متن‌باز به آن، می‌توان از آن در موارد فراوانی مانند سرویس‌دهنده‌ها، کامپیوترهای روی‌میزی، ابزارهای صنعتی و پزشکی که دارای سیستم‌های Embedded می‌باشند و... استفاده کرد.

ویژگی‌های سیستم‌عامل کالی لینوکس

- ۱) داشتن بیش از ۳۰۰ ابزار تست و نفوذ
- ۲) کالی رایگان است و همیشه خواهد ماند
- ۳) پشتیبانی از انواع زبان‌ها از جمله فارسی
- ۴) منبع باز (OpenSource): یعنی قادر خواهید بود هر نوع تغییری را در کالی لینوکس اعمال نمایید.
- ۵) دارای پشتیبانی قوی از کارت‌های شبکه وایرلس: کالی لینوکس را طوری ساخته‌اند که قادر است بیشتر کارت‌های شبکه وایرلس داخلی (internal) و کارت‌های شبکه‌ی وایرلس USB را شناسایی و پشتیبانی کند.
- ۶) محیط توسعه امن: تیم کالی از یک گروه قابل اعتماد تشکیل شده و تنها مخازن امن را در کالی قرار می‌دهند.
- ۷) تعهد GPG: هر بسته در کالی باید امن باشد و تیم توسعه‌ی هر بسته نسبت به امنیت و اعتماد آن بسته تعهد می‌دهد و برای پایبند بودن به این تعهدات، قراردادهای دو طرفه بسته می‌شود.
- ۸) قابل تغییر است: کاربران قادر خواهند بود محیط و تنظیمات دلخواه خود را بر روی کالی لینوکس اعمال کنند.

¹ GNU Linux

۹) پشتیبانی از سیستم‌های ARMEL و ARMHF: تیم توسعه‌ی کالی سعی می‌کند که خود را با بیشتر دستگاه‌های تکنولوژی ARM که رایج نیز می‌باشند، سازگار کند و این قابلیت را هر روز افزایش دهد. هم اکنون، سیستم‌عامل کالی از این ساختار پشتیبانی می‌کند. نام برخی از این مدل‌های مشهور را می‌توان در سایت رسمی این تیم مشاهده نمود:

<http://docs.kali.org/category/armel-armhf>

www.raspberrypi.org

دانلود سیستم‌عامل کالی لینوکس



با توجه به توضیحاتی که در صفحات پیش به آن اشاره شد، اکنون وقت آن است که این توزیع گنو-لینوکسی را دانلود کنیم و کار با آن را از صفر آغاز نماییم. برای دانلود این توزیع لینوکسی می‌توانید از طریق یکی از سه سایت زیر اقدام کنید:

www.kali.org/downloads

www.cdimage.kali.org/kali-images

<http://iso.linuxquestions.org/kali-linux>

در رابطه با نوع دانلود دو نکته قابل ذکر است:

با توجه به ۳۲ یا ۶۴ بیتی بودن CPU سیستم خود، اقدام به دانلود کنید.	
X86 برای سیستم‌عامل‌های ۳۲ بیتی و X86_64 برای سیستم‌عامل‌های ۶۴ بیتی می‌باشد.	

همان‌گونه که از عنوان کتاب مشخص است، تلاش مؤلف بر این است که بهترین و پیشرفته‌ترین روش‌های کار با کالی لینوکس را بدون اینکه آسیبی به هارد دیسک شما وارد شود، به شما آموزش دهد. یکی از مهمترین کارها، نصب کالی لینوکس بر روی هارد دیسک می‌باشد. به جرأت می‌توان گفت، برخی از متخصصان امنیت که سال‌های زیادی در حال فعالیت در این حرفه می‌باشند، هیچ‌گونه ریسکی برای نصب کالی لینوکس بر روی هارد دیسک نمی‌نمایند و ترجیح می‌دهند برای کار با این توزیع امنیتی، از ماشین‌های مجازی بر روی PC یا Laptop خود استفاده نمایند. سیر آموزشی این کتاب از سطح پایه آغاز می‌شود و در ادامه تا سطح پیشرفته نیز پیش خواهد رفت و قطعاً به یاری خدا، مطالب بسیار جدیدی خواهید آموخت.

لطفا برای یکبار، تمام روش‌های نصب کالی لینوکس را بر روی سیستم‌های گوناگون مطالعه کنید و سپس اقدام به نصب این توزیع لینوکسی نمایید. با انجام این کار مطمئن باشید که هیچ‌گونه آسیبی به هارد دیسک و سیستم شما وارد نخواهد شد.

روش نخست: نصب کالی بر روی ماشین مجازی (VirtualBox)

در این کتاب از نسخه 4.2.X نرم‌افزار virtualbox برای آموزش‌ها استفاده شده است. البته نسخه 4.3.x نیز موجود می‌باشد، اما پیشنهاد مؤلفان به شما، دانلود نسخه مربوط به 4.2.x می‌باشد. برای دانلود آخرین نسخه‌های مربوط به این نرم‌افزار می‌توانید از طریق سایت زیر اقدام به دانلود کنید:

www.virtualbox.org/wiki/Downloads

پیش نیازهای نصب:

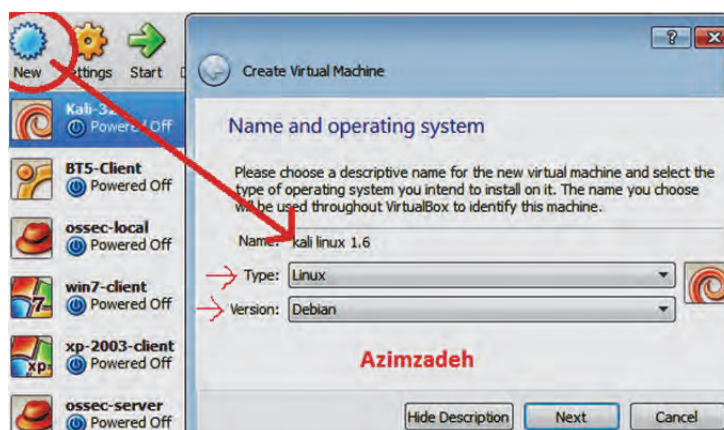
۱) داشتن دست کم 16GB فضای اضافی بر روی هارد دیسک.

۲) داشتن دست کم RAM-512MB اضافی بر روی سیستم.


مراحل نصب:

سعی بر این است که بیشتر قسمت‌ها همراه با شکل توضیح داده شود. پس، طبق مراحل زیر پیش روید:

۱. در ابتدا، انتخاب گزینه New و تخصیص یک نام به ماشین مجازی و کلیک بر روی Next:



۲. تخصیص حافظه RAM به ماشین مجازی:



این میزان حافظه‌ی RAM که از سیستم به این ماشین مجازی اختصاص داده‌اید، پس از خاموش شدن ماشین مجازی (همانند کالی)، دوباره به سیستم باز می‌گردد.

RAM: 512MB

۳. انتخاب گزینه "Create a virtual hard drive now" و سپس کلیک بر روی Create.

۴. در این گام باید نوع هارد دیسک خود را انتخاب نمایید:

VDI: ویژه برای virtualbox

VMDK: ویژه برای VMware

VHD: افزودن این دیسک مجازی به عنوان دیسک درایو در سیستم‌عامل.

پیشنهاد: انتخاب ما VDI و سپس کلیک بر روی Next می‌باشد.

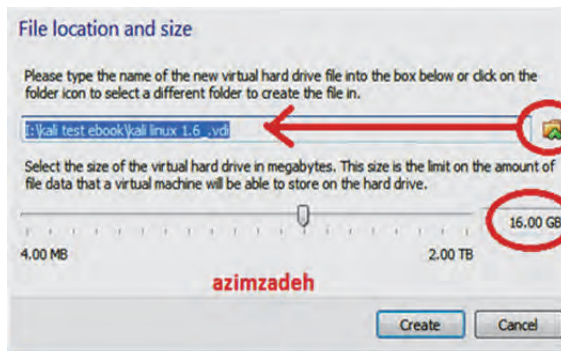
۵. در این گام باید نحوه ذخیره‌سازی این دیسک مجازی را بر روی هارد دیسک سیستم خود مشخص کنید. برای انجام این کار دو گزینه پیش‌رو دارید:

الف) Dynamically (ب) Fixed-size

الف) استفاده از روش Dynamically باعث کاهش سرعت در بالا آمدن ماشین مجازی‌تان می‌شود. اما این روش زمانی می‌تواند کاربردی باشد که شما فضای زیادی بر روی هارد دیسک خود ندارید و می‌خواهید هر آنچه که در ماشین مجازی اشغال شده است، معادل همان فضا از هارد دیسک سیستم شما نیز اشغال شود.

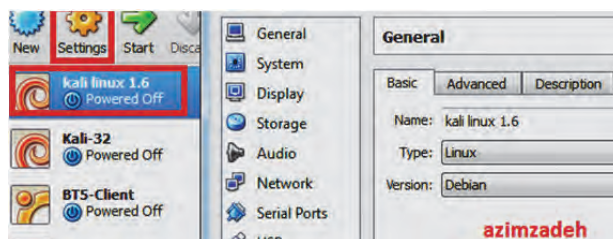
ب) با استفاده از روش Fixed-size با مشکل کاهش سرعت در هنگام بالا آمدن ماشین مجازی مواجه خواهید شد و هر بار که از این روش استفاده نمایید، هر مقدار فضایی را که در گام ششم (گام بعد) به ماشین مجازی خود اختصاص داده‌اید، از هارد دیسک سیستم شما به صورت کامل کسر خواهد کرد و به ماشین مجازی اختصاص خواهد داد. انتخاب ما: dynamic و سپس کلیک بر روی Next می‌باشد.

۶. در این گام باید میزان فضای لازم را برای هارد دیسک به علاوه‌ی مسیر ذخیره‌سازی آن بر روی سیستم خود مشخص نمایید:



۷. در گام پیشین، ماشین مجازی ایجاد شده به لیست virtualbox اضافه شده است. اکنون برای انجام برخی تنظیمات نصب، لازم است مراحل زیر دنبال نمایید.

الف) بر روی گزینه‌ی Settings کلیک نمایید:

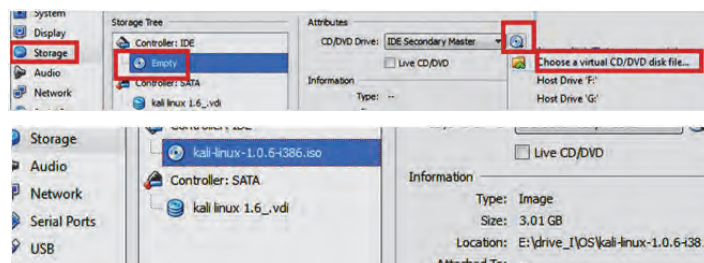


ب) سپس وارد برگه (tab) General شوید و از برگه Advanced آن، گزینه‌های Shared-clipboard و darg and drop را بر روی Bidirectional تنظیم نمایید.

پ) سپس وارد برگه System شوید و از برگه Acceleration آن، تیک تمام گزینه‌های موجود را بزنید.

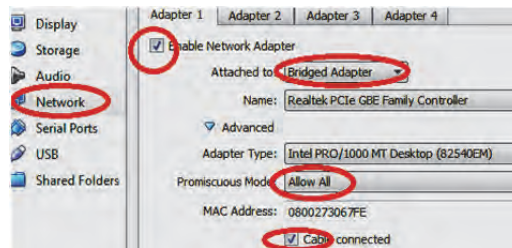
ت) وارد برگه Display شوید و میزان حافظه گرافیک را تعیین نمایید.

ث) وارد برگه Storage شوید و طبق شکل زیر، فایل ایزو کالی لینوکس را که با پسوند .ISO دانلود نموده‌اید، به ماشین مجازی خود برای نصب اضافه نمایید:



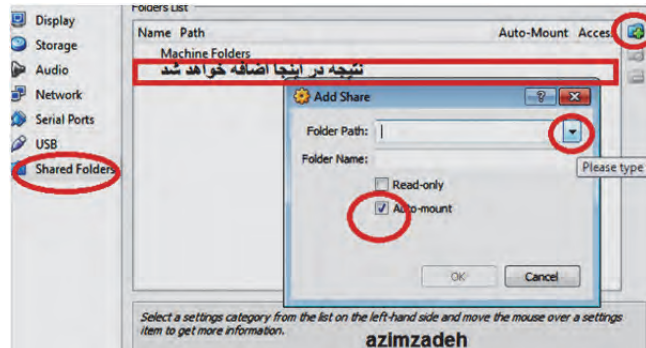
ج) به برگه Network بروید و با توجه به نیاز خودتان، نوع و تعداد کارت‌های شبکه را تعیین کنید. در بخش Adapter1 گزینه‌های زیر را تنظیم کنید:

Attached to: Bridge Adaptere and Promiscuous Mode: Allow All

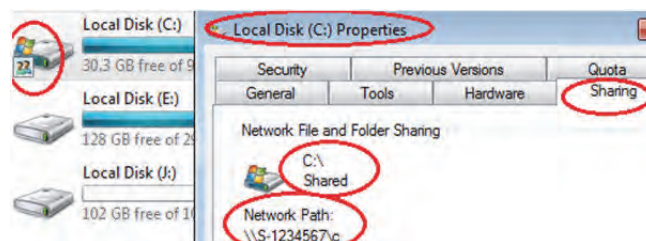


تا چهار آداپتر، حق انتخاب، تنظیم و افزودن آداپتر را به ماشین مجازی کالی لینوکسی خود خواهید داشت.

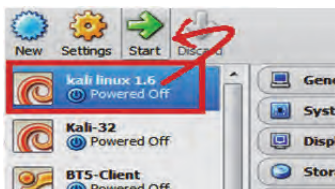
ج) به برگه Shared بروید و طبق شکل زیر یک پوشه برای به اشتراک گذاری منابع بین ماشین مجازی و سیستم عامل اصلی خود انتخاب نمایید:



قابلیت به اشتراک‌گذاری باید بر روی پوشه‌ی مورد نظر نیز فعال شده باشد:



۸. برای آغاز نصب، بر روی Start کلیک نمایید.



۹. گزینه‌ی install یا Graphical install را از لیست گزینه‌ها انتخاب کنید.

انتخاب ما گزینه‌ی Graphical Install می‌باشد.

در صورت تمایل برای انتخاب مد Install، باید برای حرکت بین گزینه‌ها و انتخاب آنها از کلیدهای TAB و Enter کیبورد استفاده نمایید.



سپس به ترتیب، گام‌های زیر را با انتخاب گزینه‌ی دلخواه، دنبال کنید:

۱۰. انتخاب زبان مربوطه.
۱۱. انتخاب موقعیت کشور.
۱۲. انتخاب زبان کار با keyboard.
۱۳. انتخاب یک نام به عنوان Hostname. مانند: azimzadeh
۱۴. در صورت عدم تمایل به تنظیم انتخاب نام دامنه (Domain)، می‌توانید به گام بعدی بروید.
۱۵. انتخاب یک رمز عبور قوی برای کاربر ریشه (root).
۱۶. تنظیم زمان سیستم.
۱۷. چون در حال نصب کالی بر روی ماشین مجازی هستیم، گزینه "use entire disk" را انتخاب می‌نماییم.
۱۸. با توجه به نوع کاربری و میزان امنیت، باید شمای (scheme) پارتیشن‌بندی را در این بخش تعیین نمایید. گزینه انتخابی ما All files in one partition..... می‌باشد.
۱۹. انتخاب گزینه Yes.

نصب کالی لینوکس در کمتر از ۵۰ دقیقه انجام خواهد شد.

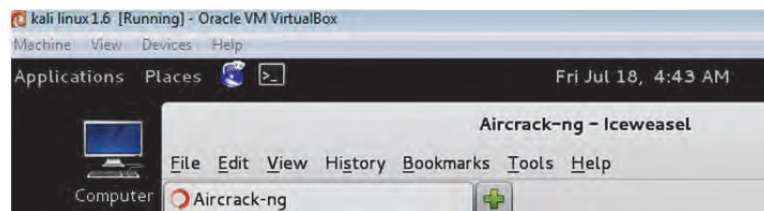


۲۰. چنانچه پرسشی پیرامون پیکربندی Package-Manager مطرح شد، پاسخ مثبت دهید.
۲۱. به پرسش پیرامون نصب grub-boot-loader بر روی Master boot record، پاسخ مثبت دهید.

۲۲. پس از نصب با صفحه GNU-GRUB زیر روبه‌رو می‌شوید، که باید گزینه نخست را انتخاب نمایید:

```
GNU GRUB version 1.99-27+deb7u2
KALI LINUX
Debian GNU/Linux, with Linux 3.12-kali1-686-pae
Debian GNU/Linux, with Linux 3.12-kali1-686-pae (recovery mode)
Memory test (memtest86+)
Memory test (memtest86+, serial console 115200)
Memory test (memtest86+, experimental multiboot)
Memory test (memtest86+, serial console 115200, experimental
```

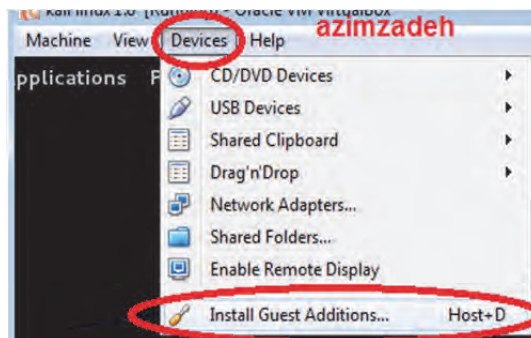
۲۳. سپس برای ورود به سیستم باید نام کاربری (root) و رمزعبور انتخاب شده در هنگام نصب را وارد نمایید. شکل زیر، نتیجه پایانی پس از نصب کامل و بدون اشکال این روش را نشان می‌دهد:



نصب Guest-Additions بر روی VirtualBox

در این کتاب، نصب کالی بر روی VMware پوشش داده نشده است. اما، پس از نصب کالی بر روی هر ماشین مجازی با توجه به نرم افزار (برای نمونه، VirtualBox یا VMware)، باید چند ویژگی دیگر نیز فعال شود. برای فعال‌سازی و استفاده از امکانات اضافی VirtualBox برابر زیر عمل نمایید:

- انتخاب گزینه "Install Guest Additions..." از برگه Devices. همانند شکل زیر:



- پس از انتخاب این گزینه، در داخل ماشین مجازی پنجره‌ای آشکار خواهد شد. بر روی گزینه Run کلیک نمایید و پس از نصب شدن بسته‌های مکمل، کالی را با دستور زیر دوباره راه‌اندازی نمایید:

```
root@kali: reboot
```

روش دوم: نصب کالی در کنار سیستم‌عامل‌ها (Dual-Boot یا Multi-Boot)

بیشتر کاربرانی که به تازگی به جمع خانواده‌های لینوکسی پیوسته‌اند، همیشه نگران از دست دادن اطلاعات ضروری و مهم از روی هارددیسک خود، به هنگام نصب توزیع لینوکسی مربوطه بر روی سیستم خود می‌باشند. جای هیچ‌گونه نگرانی نیست؛ در این کتاب روشی آموزش داده خواهد شد که برای همیشه، این نگرانی از جانب شما کاربران عزیز برطرف گردد. با انتخاب این روش می‌توانید کالی لینوکس را در کنار دیگر سیستم‌عامل‌هایی که هم اکنون دارید و یا در آینده قصد نصب آنها را دارید، با خیالی آسوده نصب نمایید. پیش نیازهای نصب:

۱. دانلود نرم‌افزار Easy-BCD از آدرس‌های:

www.filehorse.com/download-easybcd/

www.techspot.com/downloads/3112-easybcd.html

۲. دانلود نرم‌افزار EaseUS Partition Master Free از آدرس:

www.partition-tool.com/download.htm

روش‌های گوناگونی برای پارتیشن‌بندی دیسک در هنگام نصب وجود دارد. اما در این کتاب، تنها به یک مورد از آنها اشاره خواهیم کرد و آن روش، نصب کالی لینوکس با استفاده از یک فضای

پارتیشن‌بندی نشده (Unallocated) به کمک نرم‌افزار EaseUS می‌باشد. در این روش هیچگونه محدودیتی در ساختن پارتیشن‌ها و اختصاص دادن فضا به آنها نداریم و بهتر می‌توانیم هارد دیسک خود را مدیریت کنیم و امنیت آن را با جداسازی دقیق پارتیشن‌ها افزایش دهیم.

مراحل نصب:

۱. نرم‌افزار EaseUS را اجرا نمایید و وارد بخش Partition-Manager شوید.
۲. اکنون باید یک فضای تعریف نشده (پارتیشن‌بندی نشده) به صورت Unallocated تعریف نمایید. چنانچه هیچگونه فضای خالی ندارید، ابتدا محتویات درایو مورد نظر را به یک درایو دیگر انتقال دهید، سپس از داخل نرم‌افزار EaseUS، آن پارتیشن مورد نظر را انتخاب نمایید و بر روی گزینه Delete Partition کلیک کنید. سپس بر روی گزینه Apply که در بالای نرم‌افزار (سمت چپ) قرار دارد کلیک نمایید و اجازه اعمال تغییرات را بدهید. اکنون یک فضای پارتیشن‌بندی نشده دارید (همانند شکل زیر):

Disk 1 (MBR)							
*: System Reserved	NTFS	100.00 MB	28.13 MB	71.87 MB	System	Primary	
C:	NTFS	14.65 GB	9.60 GB	5.04 GB	Boot	Primary	
*	Unallocated	35.25 GB	0 Bytes	35.25 GB	None	Logical	

۳. فایل KaliLinux.ISO را بر روی DVD رایت نموده و سیستم را دوباره راه‌اندازی کنید و آماده نصب کالی لینوکس بر روی سیستم شوید.
۴. تنظیمات BIOS سیستم را به گونه‌ای تنظیم نمایید که نخست، DVD-ROM بررسی شود و بالا بیاید.
۵. گزینه Install یا Graphical install را از لیست گزینه‌ها انتخاب کنید:
انتخاب ما، گزینه‌ی Graphical Install می‌باشد.

در صورت تمایل برای انتخاب مد Install، برای حرکت بین گزینه‌ها و انتخاب آنها، باید از کلیدهای TAB و Enter کیبورد استفاده نمایید.



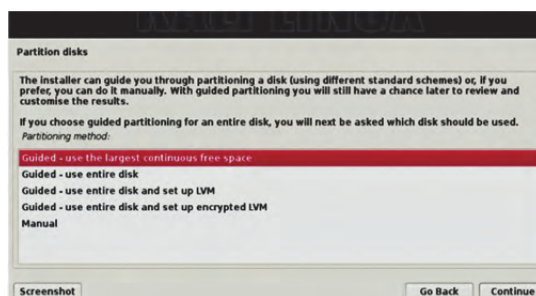
۶. انتخاب زبان مربوط.
۷. انتخاب موقعیت کشور.
۸. انتخاب زبان کار با keyboard.
۹. انتخاب یک نام به عنوان Hostname. همانند: azimzadeh.

۱۰. در صورت عدم تمایل به تنظیم انتخاب نام دامنه (Domain)، می‌توانید به گام بعدی بروید.

۱۱. انتخاب یک رمز عبور قوی برای کاربر ریشه (root).

۱۲. تنظیم زمان سیستم.

۱۳. در این گام لازم است به پارتیشن‌بندی درایوها بر روی هارد دیسک پردازیم:



با توجه به میزان فضایی که در اختیار دارید می‌توانید در ظرفیت‌ها، موقیعت قرارگیری، نوع و تعداد پارتیشن‌ها، تغییرات دلخواه را اعمال نمایید.

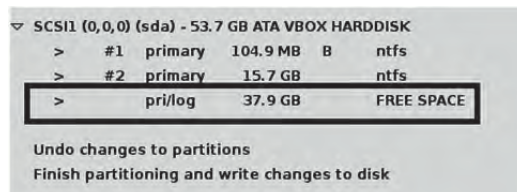


به کمک گام‌های زیر اقدام به پارتیشن‌بندی هارد دیسک می‌کنیم:

۱۴. انتخاب گزینه Manual و سپس کلیک بر روی Continue:

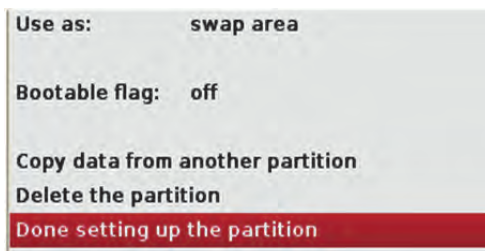


۱۵. در صفحه‌ی بعدی، روی Create a new partition کلیک کنید تا به صفحه زیر برسید.

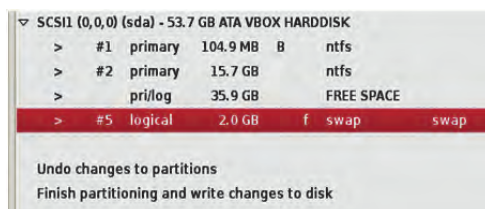


۱۶. میزان فضای لازم برای حافظه‌ی Swap را براساس ویژگی‌های زیر انتخاب کنید:

فضای پارتیشن: 2GB، حالت: Logical، موقعیت: End، گزینه‌ی Use as: در حالت swap area، و در پایان کلیک بر روی Done setting up the partition.



نتیجه پس از ایجاد پارتیشن swap به این شکل است:

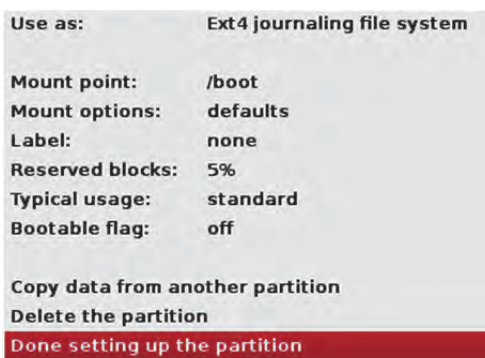


۱۷. انتخاب دوباره‌ی گزینه‌ی FREE SPACE و کلیک بر روی Continue، برای ساختن پارتیشن boot:

- کلیک بر روی Create a new partition و سپس continue.
- انتخاب میزان فضای لازم برای boot، همانند ویژگی‌های زیر:

فضای پارتیشن: 500MB، حالت: Logical، موقعیت: Beginning، برای گزینه Mount Point: انتخاب /boot و برای گزینه Use as: حالت Ext4 journaling file system انتخاب شود.

- در پایان کلیک بر روی Done setting up the partition.



نتیجه، پس از ایجاد پارتیشن boot به شکل زیر خواهد بود.

SCSI1 (0,0,0) (sda) - 53.7 GB ATA VBOX HARDDISK						
>	#1	primary	104.9 MB	B	ntfs	
>	#2	primary	15.7 GB		ntfs	
>	#6	logical	499.1 MB	f	ext4	/boot
>		logical	35.3 GB		FREE SPACE	
>	#5	logical	2.0 GB	f	swap	swap

۱۸. دوباره گزینه‌ی FREE SPACE را انتخاب و برای ساختن پارتیشن root بر روی Continue کلیک کنید:

- کلیک بر روی Create an new partition و سپس continue.
- انتخاب میزان فضای لازم برای root، طبق مشخصات زیر:

فضای پارتیشن: 20GB، حالت: Logical، موقعیت: End، انتخاب گزینه mount Point در حالت: /

انتخاب گزینه Use as در حالت: Ext4 journaling file system.

- در پایان کلیک بر روی Done setting up the partition.

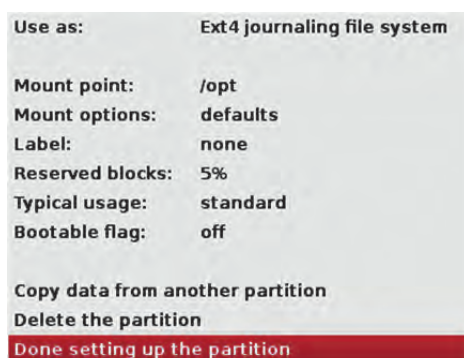
Use as:	Ext4 journaling file system
Mount point:	/
Mount options:	defaults
Label:	none
Reserved blocks:	5%
Typical usage:	standard
Bootable flag:	off
Copy data from another partition	
Delete the partition	
Done setting up the partition	

نتیجه، پس از ایجاد پارتیشن root:

SCSI1 (0,0,0) (sda) - 53.7 GB ATA VBOX HARDDISK						
>	#1	primary	104.9 MB	B	ntfs	
>	#2	primary	15.7 GB		ntfs	
>	#6	logical	499.1 MB	f	ext4	/boot
>		logical	15.3 GB		FREE SPACE	
>	#7	logical	20.0 GB	f	ext4	/
>	#5	logical	2.0 GB	f	swap	swap

۱۹. دوباره گزینه‌ی FREE SPACE را انتخاب و برای ساختن پارتیشن opt بر روی Continue کلیک کنید:

- کلیک بر روی Create a new partition و سپس Continue.
 - انتخاب میزان فضای لازم برای opt، همانند ویژگی‌های زیر:
- فضای پارتیشن: 20GB، حالت: Logical، موقعیت: End، گزینه Mount Point در حالت: /opt
- گزینه Use as در حالت: Ext4 journaling file system.
- در پایان کلیک بر روی Done setting up the partition.



نتیجه، پس از ایجاد پارتیشن opt:

SCSI1 (0,0,0) (sda) - 53.7 GB ATA VBOX HARDDISK						
>	#1	primary	104.9 MB	B	ntfs	
>	#2	primary	15.7 GB		ntfs	
>	#6	logical	499.1 MB	f	ext4	/boot
>		logical	5.3 GB		FREE SPACE	
>	#8	logical	10.0 GB	f	ext4	/opt
>	#7	logical	20.0 GB	f	ext4	/
>	#5	logical	2.0 GB	f	swap	swap

۲۰. دوباره گزینه‌ی FREE SPACE را انتخاب و برای ساختن پارتیشن home بر روی Continue کلیک کنید:

- کلیک بر روی Create a new partition و سپس Continue.
 - انتخاب میزان فضای لازم برای home، همانند ویژگی‌های زیر:
- فضای پارتیشن: 5GB، حالت: Logical، موقعیت: End، گزینه Mount Point در حالت: /home
- و گزینه Use as در حالت: Ext4 journaling file system.
- در پایان کلیک بر روی Done setting up the partition.

Use as:	Ext4 journaling file system
Mount point:	/home
Mount options:	defaults
Label:	none
Reserved blocks:	5%
Typical usage:	standard
Bootable flag:	off
Copy data from another partition	
Delete the partition	
Done setting up the partition	

شکل زیر، نتیجه‌ی پایانی ساخت پارتیشن‌ها، پس از ایجاد پارتیشن home را نشان می‌دهد.

SCSI1 (0,0,0) (sda) - 53.7 GB ATA VBOX HARDDISK						
>	#1	primary	104.9 MB	B	ntfs	
>	#2	primary	15.7 GB		ntfs	
>	#8	logical	499.1 MB	f	ext4	/boot
>	#9	logical	5.3 GB	f	ext4	/home
>	#7	logical	10.0 GB	f	ext4	/opt
>	#6	logical	20.0 GB	f	ext4	/
>	#5	logical	2.0 GB	f	swap	swap

به‌خاطر بسپارید که پارتیشن /boot درمثال ما، در وضعیت #8 قرار دارد و فضای آن 500MB می‌باشد. #8 بیانگر /dev/sda8 است. ممکن است این عدد در سیستم شما متفاوت باشد.

۲۱. اینک بر روی Finish partitioning and write changes to disk کلیک کنید.

۲۲. سپس برای اعمال تغییرات بر روی هارد دیسک، بر روی Yes کلیک کنید.

- ✓ می‌توانید از ساختن پارتیشن‌های دیگری مانند: /home و /opt چشم‌پوشی نمایید و یا هر پارتیشن دیگری را که خواستید، با توجه به میزان فضای هارد دیسک، ایجاد و اضافه نمایید.
- ✓ نسبت دادن تمامی مقادیر (MB,GB) از نظر اشغال کردن میزان فضای هارد دیسک، به نیاز شما بستگی دارد.
- ✓ میزان فضای پارتیشن swap، باید برابر یا دو برابر میزان RAM شما باشد.

✓ میزان فضای پارتیشن boot، باید بین ۵۰۰MB تا 1GB باشد.

۲۳. به پرسش طرح شده درباره‌ی نصب و پیکربندی Package Manager، پاسخ مثبت دهید.

۲۴. به پرسش طرح شده درباره‌ی نصب grub-boot-loader بر روی Master boot record، پاسخ منفی دهید. سپس در کادری که باز می‌شود، عبارت /dev/sda8 را وارد کنید.

این /dev/sda8 مربوط به ساخت پارتیشن boot می‌باشد. در شکل نهایی زیر می‌توانید عدد مربوط به پارتیشن boot را که ۸ می‌باشد مشاهده نمایید. این عدد می‌تواند در سیستم شما عدد دیگری باشد.

SCSI (0,0,0) (sda) - 53.7 GB ATA VBOX HARDDISK					
>	#1	primary	104.9 MB	B	ntfs
>	#2	primary	15.7 GB		ntfs
>	#8	logical	499.1 MB	f	ext4 /boot
>	#9	logical	5.3 GB	f	ext4 /home
>	#7	logical	10.0 GB	f	ext4 /opt
>	#6	logical	20.0 GB	f	ext4 /
>	#5	logical	2.0 GB	f	swap swap

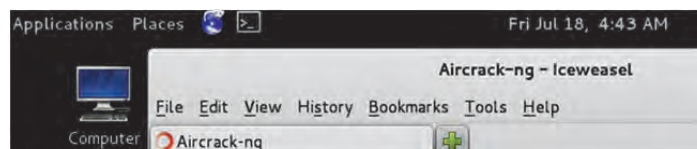
نصب کالی لینوکس در کمتر از ۵۰ دقیقه انجام خواهد شد.

۲۵. پس از نصب، باید با صفحه GNU-GRUB زیر روبه‌رو شوید، آنگاه گزینه‌ی نخست را انتخاب نمایید:

```

GNU GRUB version 1.99-27fa6b7a2
KALI LINUX
Debian GNU/Linux, with Linux 3.12-kali1-686-pae
Debian GNU/Linux, with Linux 3.12-kali1-686-pae (recovery mode)
Memory test (memtest86+)
Memory test (memtest86+, serial console 115200)
Memory test (memtest86+, experimental multiboot)
Memory test (memtest86+, serial console 115200, experimental multiboot)
Windows 7 (loader) (on /dev/sda1)
  
```

۲۶. سپس برای ورود به سیستم باید نام کاربری (root) و رمز عبور انتخاب شده در هنگام نصب را وارد نمایید. نتیجه پایانی به شکل زیر است.



۲۷. در این گام لازم است سیستم را دوباره راه‌اندازی کنید و وارد محیط ویندوز شوید و برنامه EasyBCD را اجرا نمایید.

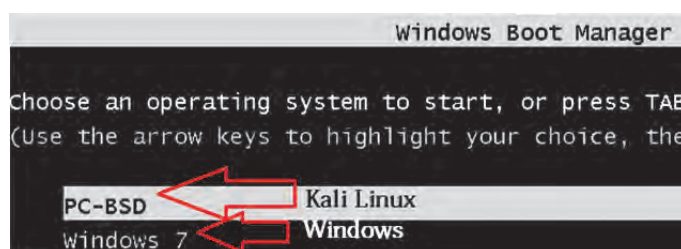
۲۸. سپس گزینه Add New Entry را انتخاب نمایید.

۲۹. به برگه Linux/BSD بروید و Type را روی Grub2 قرار دهید.

۳۰. Drive را هم، پارتیشن boot قرار دهید. اما چون در اینجا نامی از آن نیامده است، باید میزان حافظه اختصاص یافته به آن را به یاد داشته باشید (درمثال ما: 500MB). در آخر بر روی Add Entry کلیک نمایید.

۳۱. وارد برگه Edit Boot Menu شوید و گزینه Save Settings را انتخاب کنید.

هم اکنون نصب کالی به پایان رسیده است و شما یک boot manager دیگر افزون بر Boot-GRUB کالی لینوکس خود دارید:



روش سوم: نصب کالی بر روی USB:Flash-Memory

با استفاده از این روش می‌توانید کالی لینوکس خود را بر روی یک فلش مموری رایت نمایید و آن را با خود حمل کنید و در هر لحظه که به آن نیاز دارید از آن استفاده نمایید. پیش نیازهای نصب:

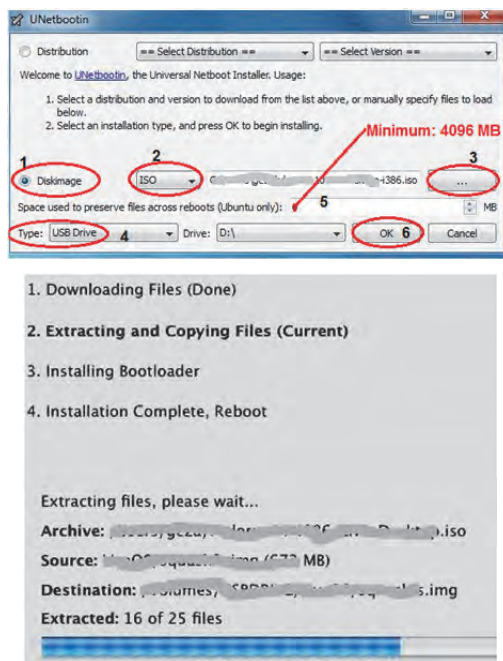
الف. دانلود نرم‌افزار UNetbootin از آدرس: <http://unetbootin.sourceforge.net>

ب. داشتن یک فلش مموری با دست‌کم 8GB فضا.

مراحل نصب:

۱. فلش مموری را به سیستم وصل نمایید.

۲. نرم‌افزار UNetbootin را اجرا کنید و فایل kali-linux.iso خود را انتخاب و بر روی OK کلیک و صبر کنید تا عمل رایت این فایل ایمیج بر روی فلش مموری به پایان برسد:



در پایان، بر روی گزینه‌ی Restart Now کلیک کنید.

برای بوت شدن از طریق فلش مموری، تنظیمات لازم را در BIOS سیستم حتماً انجام دهید.



روش چهارم: نصب کالی در گوشی‌های هوشمند اندروید

یکی از نکات برجسته سیستم‌عامل‌های اندروید این است که، بر اساس هسته سیستم‌عامل لینوکس توسعه یافته است. در واقع مدیریت و بهینه‌سازی حافظه، ارتباط با سخت‌افزار و سرویس‌های سیستم، امنیت، مدیریت پردازش‌ها و مدیریت منابع دستگاه موبایل را هسته لینوکس انجام می‌دهد و اندروید، تنها لایه‌ایست که ارتباط میان کاربر و سیستم‌عامل را برقرار می‌سازد. این لایه‌ی نرم‌افزاری به‌وسیله جاوا پیاده‌سازی شده است و به همین دلیل قادر به اجرای کدهای Native نخواهد بود. اندروید همانند لینوکس یک متن-باز است که توسعه دهندگان بی‌شماری بر روی آن

کار می‌کنند. در این بخش، به توضیح در مورد نصب و استفاده از کالی لینوکس در دستگاه‌های آندرویدی خواهیم پرداخت. در طول این آموزش از یک سری برنامه‌های کاربردی آندرویدی استفاده خواهیم کرد که در پایان، چند جایگزین نیز برای آنها معرفی می‌شود.

پیش نیازهای نصب:

الف. دست‌کم، داشتن 5GB یا 6GB فضای خالی در حافظه‌ی داخلی یا خارجی.

ب. اینترنت پرسرعت.

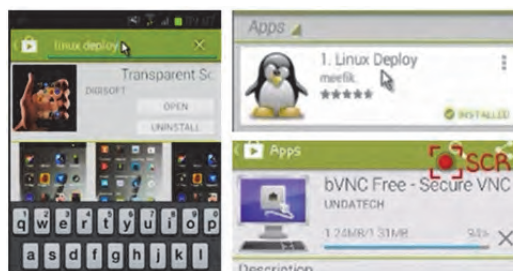
ج. دستگاه هوشمند root شده با سیستم‌عامل آندروید ۲.۱ به بالا (در مثال ما: Galaxy Note 3).

مراحل نصب کالی لینوکس در گوشی‌های هوشمند آندروید چنین است:

دقت داشته باشید که گوشی شما باید در حالت root (ریشه) قرار داشته باشد. چون در این کتاب از گوشی G.N.3 استفاده می‌کنیم برای یادگیری آموزش روت شدن، می‌توانید به سایت زیر مراجعه کنید:

galaxynote3root.com/galaxy-note-3-root/how-to-root-galaxy-note-3

۱. پس از اتصال به اینترنت، به سایت Google Apps (برنامه‌های کاربردی و رایگان گوگل) بروید و نرم‌افزارهای Linux Deploy، bVNC Free و Terminal Emulator را، بر روی گوشی خود نصب کنید. (سه شکل از نصب bVNC و Deploy):



۲. سپس باید ایمیج کالی را بر روی حافظه گوشی خودتان کپی کنید.

۳. پس از نصب، وارد محیط Linux Deploy شوید و در برگه Properties، از بخش Distribution، گزینه Kali Linux را انتخاب نمایید و در ادامه با توجه به مشخصات CPU گوشی خود (ARMHF یا ARMEL)، آن را هم انتخاب نمایید: