June 2014 WMLUG Meeting

Kali Linux

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

Patrick TenHoopen

Kali Linux

Kali Linux is a free and open source penetration testing Linux distribution designed for IT and security professionals for testing defenses by simulating attacks.

Home page: http://www.kali.org/

Downloads: http://www.kali.org/downloads/

Kali Linux

- Kali Linux is funded by Offensive Security, a security training and penetration testing consulting company.
- First released on 3/13/2013, it is a complete rebuild of BackTrack Linux resulting in an easier to use tool.
- It has over 300 penetration testing tools.
- While BackTrack was based on Ubuntu, Kali is based on Debian.
- The current version is 1.0.7, released on 5/27/2014.
- It is available in a live or installable ISO.

About Offensive Security

Offensive Security was founded in 2007 with the belief that in order to have the best defense against security attacks, one must take an offensive approach. They practice attacking systems to test defenses and offer training and free tools.

They maintain the Exploit Database (http://www.exploit-db.com/) which is an archive of exploits and vulnerable software.

They have a free training course titled “Metasploit Unleashed” that explains how to use Metasploit. It is available at http://www.offensive-security.com/metasploit-unleashed/Main_Page.

Kali's Top Ten Security Tools

1. **aircrack-ng** - Aircrack-ng is an 802.11 WEP and WPA-PSK key cracking program.
2. **burpsuite** - The Burp Suite is a platform for testing security of web apps.
3. **hydra** - Hydra is a tool for guessing/cracking valid login/password pairs.
4. **john** - John the Ripper is a password cracker.
5. **maltego** - Maltego is an open source intelligence gathering and forensics program written in Java that paints a threat picture in a graphical interface by showing relationships between entities in your environment such as people, web sites, Internet infrastructure, documents and files, among other things.

Kali's Top Ten Security Tools

6. **metasploit framework** - The Metasploit framework is penetration testing software that allows you to complete the testing faster and generate reports of key findings. New exploits are added each day providing you with a tool to find security weak spots before an attacker does.
7. **nmap** - Nmap ("Network Mapper") is a open source utility for network discovery and security auditing.
8. **owasp-zap** - OWASP Zed Attack Proxy (ZAP) is a penetration testing tool for finding vulnerabilities in web apps.
9. **sqlmap** - sqlmap is a penetration testing tool that automates detecting and exploiting SQL injection flaws and taking over database servers.
10. **wireshark** - Wireshark is a network protocol analyzer.

Tool Categories

- Information Gathering
- Vulnerability Analysis
- Web Applications
- Password Attacks
- Wireless Attacks
- Exploitation Tools
- Sniffing/Spoofing
- Maintaining Access
- Reverse Engineering
- Stress Testing
- Hardware Hacking
- Forensics
- Reporting Tools
- System Services

Information Gathering

- DNS Analysis
- IDS/IPS Identification
- Live Host Identification
- Network Scanners
- OS Fingerprinting
- OSINT Analysis
- Route Analysis
- Service Fingerprinting
- SMB Analysis
- SMTP Analysis
- SNMP Analysis
- SSL Analysis
- Telephony Analysis
- Traffic Analysis
- VoIP Analysis
- VPN Analysis

Vulnerability Analysis

- Cisco Tools
- Database Assessment
- Fuzzing Tools
- Misc Scanners
- Open Source Assessment
- OpenVAS

Web Applications

- CMS Identification
- Database Exploitation
- IDS/IPS Identification
- Web Application Fuzzers
- Web Application Proxies
- Web Crawlers
- Web Vulnerability Scanners

Password Attacks

- GPU Tools
- Offline Attacks
- Online Attacks
- Passing the Hash

Wireless Attacks

- 802.11 Wireless Tools
- Bluetooth Attacks
- Other Wireless Tools
- RFID/NFC Tools
- NFC Tools
- RFIDiot ACG
- RFIDiot FROSCH
- RFIDiot PCSC
- Software Defined Radio

Exploitation Tools

- BeEF XSS Framework
- Cisco Attacks
- Exploit Database
- Exploit Development Tools
- Metasploit
- Network Exploitation
- Social Engineering Toolkit

Sniffing/Spoofing

- Network Sniffers
- Network Spoofing
- Voice and Surveilance
- VoIP Tools
- Web Sniffers

Maintaining Access

- OS Backdoors
- Tunneling Tools
- Web Backdoors

Reverse Engineering

- Debuggers
- Disassembly
- Misc RE Tools

Stress Testing

- Network Stress Testing
- VoIP Stress Testing
- Web Stress Testing
- WLAN Stress Testing

Hardware Hacking

- Android Tools
- Arduino Tools

Forensics

- Anti-Virus Forensics Tools
- Digital Anti-Forensics
- Digital Forensics
- Forensic Analysis Tools
- Forensic Carving Tools
- Forensic Hashing Tools
- Forensic Imaging Tools
- Forensic Suites
- Network Forensics
- Password Forensic Tools
- PDF Forensic Tools
- RAM Forensic Tools

Reporting Tools

- Documentation
- Evidence Management
- Media Capture

System Services

- BeEF
- Dradis
- HTTP
- Metasploit
- MySQL
- OpenVas
- SSH

Demo - nmap

Scan a single IP:

```
nmap –v –A 192.168.1.17
```

Scan an IP range:

```
nmap –v –A 192.168.1.1–254
```

Demo - John the Ripper

Download password file word lists (free ones) at http://download.openwall.net/pub/passwords/wordlists/all.gz

Scan using built-in word list:

```
john shadow --format=crypt
```

Scan using custom word list:

```
john shadow --wordlist=/root/john/all
--format=crypt
```

Press any key to get a status while it is running.

Press Ctrl-C to stop and save progress to be resumed using `john --session`.

Demo - johnny

johnny is a GUI for John the Ripper

Demo - ophcrack

How-To: http://sourceforge.net/p/ophcrack/wiki/ophcrack Howto/

Download free rainbow table files at http://sourceforge.net/tables.php

Unzip table file(s) and install into ophcrack (Tables > Import)

Obtain password info from a Windows computer using pwdump (can use live Kali), fgdump, etc.

fgdump downloadable from http://www.foofus.net/goons/fizzgig/