Table of Contents

Chapter 1 - Introduction

What is Kali?

Kali is the latest and greatest version of the ever popular Backtrack Linux penetration testing

distribution. The creators of the Backtrack series kept Kali in a format very similar to Backtrack, so anyone familiar with the older Backtrack platform will feel right at home.

Kali has been re-vamped from the ground up to be the best and most feature rich Ethical Hacking/ Pentesting distribution available. Kali also runs on more hardware devices greatly increasing your options for computer security penetration testing or "pentesting" systems.

If you are coming to Kali from a Backtrack background, after a short familiarization period you should find that everything is very similar and your comfort level should grow very quickly.

If you are new to Kali, once you get used to it, you will find an easy to use security testing platform that includes hundreds of useful and powerful tools to test and help secure your network systems.

Why Use Kali?

Kali includes over 300 security testing tools. A lot of the redundant tools from Backtrack have been removed and the tool interface streamlined. You can now get to the most used tools quickly as they appear in a top ten security tool menu. You can also find these same tools and a plethora of others all neatly categorized in the menu system.

Kali allows you to use similar tools and techniques that a hacker would use to test the security of your network so you can find and correct these issues before a real hacker finds them.

Hackers usually perform a combination of steps when attacking a network. These steps are summarized below:

Recon – Checking out the target using multiple sources – like intelligence gathering.

Scanning – Mapping out and investigating your network.
Exploitation – Attacking holes found during the scanning process.
Elevation of Privileges – Elevating a lower access account to Root, or System Level.
Maintaining Access – Using techniques like backdoors to keep access to your network.
Covering their Tracks – Erasing logs, and manipulating files to hide the intrusion.
An Ethical Hacker or Penetration Tester (good guys hired to find the holes before an attacker does) mimics many of these techniques, using parameters and guidelines set up with corporate management, to find security issues.
They then report their findings to management and assist in correcting the issues.
We will not be covering every step in the process, but will show you many of the techniques that are used, and how to defend against them.
I would think the biggest drive to use Kali over commercial security solutions is the price. Security
testing tools can be extremely costly, Kali is free! Secondly, Kali includes open source versions of
numerous commercial security products, so you could conceivably replace costly programs by simply
using Kali.
All though Kali does includes several free versions of popular software programs that can be
upgraded to the full featured paid versions and used directly through Kali.
There really are no major tool usage differences between Backtrack and Kali. Kali is basically
Backtrack version 6, or the latest version of Backtrack. But it has been completely retooled from the
ground up, making software updates and additions much easier.
In Backtrack updating some programs seemed to break others, in Kali, you update everything using the

Kali update command which keeps system integrity much better.
Simply update Kali and it will pull down the latest versions of the included tools for you. Just a note
of caution, updating tools individually could break Kali, so running the Kali update is always the best
way to get the latest packages for the OS.
I must admit though, some tools that I liked in the original Backtrack are missing in Kali. It is not too
big of a deal as another tool in Kali most likely does the same or similar thing. And then again you
can install other programs you like if needed.
In addition to stand alone and virtual machine instances of Kali, I also use Kali on a Raspberry Pi - a
mini credit card sized ARM based computer. With Kali, you can do almost everything on a Pi that you
could do on a full sized system. In my book I will cover using the PI as a security testing platform
including testing Wireless networks.
Testing networks with a computer you could fit in your pocket, how cool is that?
Though Kali can't possibly contain all the possible security tools that every individual would prefer,
it contains enough that Kali could be used from beginning to end. Don't forget that Kali is not just a
security tool, but a full-fledged Linux Operating System. So if your favorite tool runs under Linux, but
is not included, most likely you can install and run it in Kali.

Ethical Hacking Issues

Using Ethical Hacking a security tester basically acts like a hacker. He uses tools and techniques that
a hacker would most likely use to test a target network's security. The difference is, the penetration
tester is hired by the company to test its security and when done reveals to the leadership team how
they got in and what they can do to plug the holes.

The biggest issue I see in using these techniques is ethics and law. Some security testing techniques
that you can perform with Kali and its included tools are actually illegal to do in some areas. So it is
important that users check their local, State and Federal laws before using Kali.
Also, you may have some users that try to use Kali, a very powerful set of tools, on a network that
they do not have permission to do so. Or they will try to use a technique they learned but may have not
mastered on a production network.
All of these are potential legal and ethical issues.

Scope of this Book

This book focuses on those with beginning to intermediate experience with Backtrack/ Kali. I think it This is a guide to your IAS Preparations (ias-preparation.html) and we are
giving subjectwise details of strategy to be taken up during your
prepration for the IAS Exam. We are still adding resources to this page
for Civil Services preparation. Please keep a watchout for newer
pages that we keep linking. Please visit our active links for the
information on IAS Preparation (ias-preparation.html).
Note: As you can see there are many subjects for which we have no
resources on Strategy. If you can suggest any Strategy for the
following subjects or know of any links where they may be available,
please send them to us. Civil Service Preparation is a labour of love
and if you are dedicated enough you shall surely make it. All the best for your IAS preprations!

Tips For Civil Services Preparation

How to Cope with Stress of Civil Services Exam
(http://www.civilserviceindia.com/subject/how-to-copewith-
stress-of-civil-services-exam.html)
How to fill the UPSC Application Form (http://www.civilserviceindia.com/subject/how-to-fill-the-upscapplication-
form.html)
IAS Strategy (strategy.html)
How to Prepare Notes (notes.html)
How to Write Answers (writing-answers.html)
How to Read (how-to-read.html)
Time Management (time-management.html)
How To Prepare For Prelims (how-to-prepare-for-prelims.html)
Gaining Mental Power for UPSC (gainingmentalpower.html)
UPSC Question Papers (question-papers.html)
Sugested Reading (suggested-reading.html)
How to Choose Mains Subjects (http://www.civilserviceindia.com/subject/subject-strategy.html)

IAS Preparation Strategies

General Strategy

Well formulated strategy along with optimum time management is the only two ladders for your dream goal. It's very important to formulate your own strategy as it pays to be yourself. However for the general guidance to tackle Civil Services examination, here are some of the guidelines which will help the aspirant to achieve success.

1. Familiarity with the optional syllabi: Get yourself well informed about the content of the syllabi and the topics it covers. A thorough familiarity with your optional reduces your mental burden at the first sight itself.

2. Thorough insight of the question papers: It is the most important part of your strategy as investing your time skillfully will reap rich dividends. Go through the question papers of past ten years to identify the pattern and select the topics which are asked very frequently. Simultaneously, identify those topics which are particularly useful for conventional essay type questions. Once you have clearly demarcated the topics for the conventional and the objective types, the rest will be an easier task. A thorough insight of the past papers will therefore solve two of your purposes. It would boost your confidence level initially as you come to know the standards of the question asked and secondly it guides constantly through your preparation.

3. Selection of books: It is advisable not to go through a lot of books, instead go through one quality book on each topic which clarifies your basic concept. Standard books not only save your precious time but also guide you as a perfect teacher. So always rely on standard good books.
Also it is advisable to collect various books on my topics in advance so as to save time for the last minute hassle.

4. Prefer you own notes: It is always advisable to make notes of the related topics. A well crafted note solves two purposes. On the one hand the aspirant goes through the syllabus once and on

the other hand it is of immense help on the eve of examination.
5. A specific strategy for the general studies: General studies cover everything under the sun. But
there is nothing to get panic, a glance over the last years question' paper will make things easier.
Broadly we can categories this topic under the following heads.
a. History: A huge stress is given to modern history and freedom movement. Also emphasis is
given to Ancient India. A cursory glance over the medieval history would serve the purpose.
b. Geography: A huge stress is to be given to physical geography and maps related questions. Get
yourself well-acquainted with maps with the help of a good Atlas.
c. General Science: It covers a major chunk, so be well-versed with the topics of general science
from a standard guidebook.
d. Current affairs: Going daily through a standard news paper thoroughly will suffice.
e. General awareness: Any good guide book or year book will be suited for the purpose.
Some more important points:
As already said, always rely on yourself prepared notes. Go through your short notes rigorously.
Prepare out short notes of important topics with relevant points and just before the examination

rely solely on it.
Always rely on revisions.
Take a good sleep on the eve of examination. It is most important for your brilliant performance.
Never go through any book on the eve of examination.
Don't read any new topic.
Don't get engaged with any confusing question or problem as your prior investment (with studies)
will only bring dividends to you.
Do not loose your confidence.
General Studies (General-Studies/strategy.html)
Essay (Essay/strategy.html)
Agriculture (Agriculture/strategy.html)
Animal Husbandry and Veterinary Science (Animal-Husbandry/strategy.html)
Botany (Botany/strategy.html)
Chemistry (Chemistry/strategy.html)
Civil Engineering (Civil-Engineering/strategy.html)
Commerce (Commerce/strategy.html)
Economics (Economics/strategy.html)
Electrical Engineering (Electrical-Engineering/strategy.html)
Geography (Geography/strategy.html)
Geology (Geology/strategy.html)
Indian History (History/strategy.html)
Law (Law/strategy.html)
Mathematics (Mathematics/strategy.html)

Mechanical Engineering (Mechanical-Engineering/strategy.html)
Medical Science (Medical-Science/strategy.html)
Philosophy (Philosophy/strategy.html)
Physics (Physics/strategy.html)
Political Science (Political-Science/strategy.html)
Psychology (Psychology/strategy.html)
Public Administration (Public-Administration/strategy.html)
Sociology (Sociology/strategy.html)
Statistics (Statistics/strategy.html)
Zoology (Zoology/strategy.html)
Anthropology (Anthropology/strategy.html)
Management (Management/strategy.html)
Arabic
Assamese
Bengali
Chinese
English
French
German
Gujarati
Hindi
Kannada
Kashmiri
Konkani
Malayalam
Manipuri
Marathi
Nepali
Oriya
Pali
Persian
Punjabi
Russian
Sanskrit
Sindhi
Tamil
Telugu
Urdu