20 Fantastic Kali Linux Tools

SwordSec

http://www.swordsec.com
November, 2014

Before beginning your penetration test and security auditing, remember that the best tool available is your own mind. Kali Linux is a suite of tools built to help gather information and exploit weaknesses, but the logical decision making and analysis is yours. Outside of the technical aspects of attacking, being calm and organized will help you more than anything. Further, always make sure you have direct permission or ownership of the sites involved in your penetration testing. Once you have limited your risk to undue outside influences, it is time to begin phase one of the penetration test. In order to be sufficiently thorough, illegal tools and actions must be considered as weapons the attackers may implement.

> *“A complete and adequate penetration test involves penetration testers conducting illegal activities on systems external or internal to an organization’s network. Organizations must understand that penetration testers performing the tests in most cases are breaking the law. “*
> SANS on penetration testing

Tools for Phase One

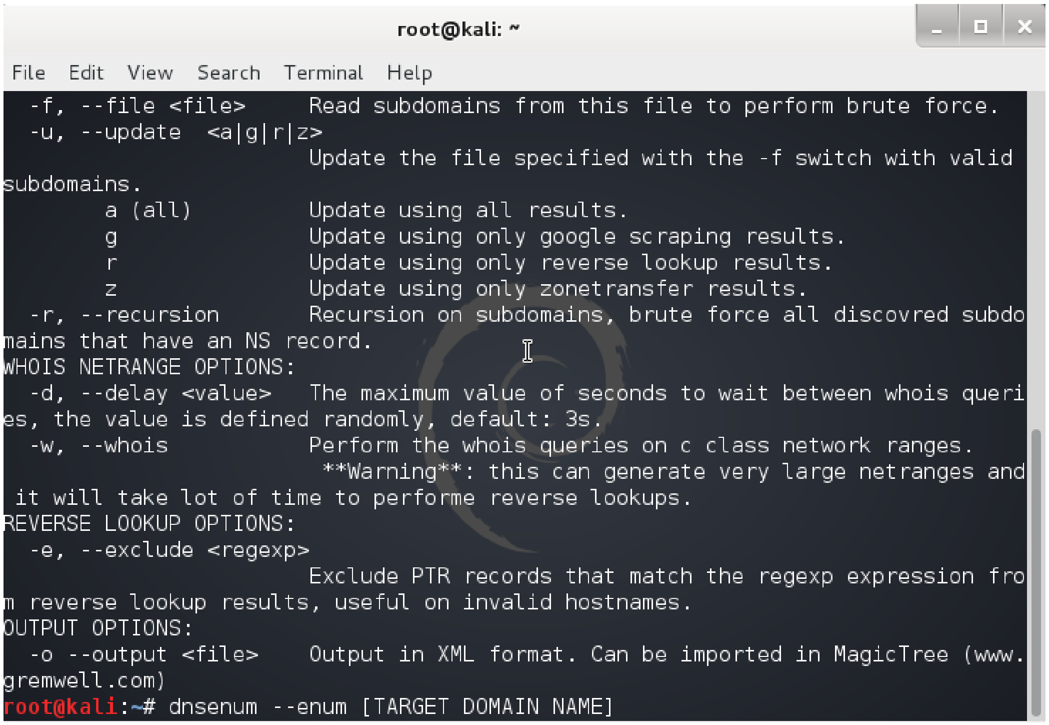
Information Gathering and Analysis

Kali Linux has a wonderful set of tools for gathering data on your target. The end goal of phase one is to have a logical map of the target’s network, both of people and of machines. Any information discovered now may be key to a pivot later on, so thoroughness is your ally. Most tools in this stage are very quiet, so if time is not a critical factor in your attack, this is the best time to move slowly and dig deep. The more you sweat now, the less you’ll bleed later.

1. DNSenum - Enumerating the Servers
   The first high level maps of an organization’s network will come from locating its DNS servers. Starting with a good foundation here will help you find the key footholds you’ll need later. DNSenum is a high level tool that is very often the first step in mapping your targets network. Using the format ...

   ```
   ./dnsenum --enum [TARGET DOMAIN NAME]
   ```

   … we can begin enumeration of the higher level servers available to our target.



```
  -f, --file <file>     Read subdomains from this file to perform brute force.
  -u, --update  <a|g|r|z>
                        Update the file specified with the -f switch with valid
subdomains.
        a (all)         Update using all results.
        g               Update using only google scraping results.
        r               Update using only reverse lookup results.
        z               Update using only zonetransfer results.
  -r, --recursion       Recursion on subdomains, brute force all discovred subdo
mains that have an NS record.
WHOIS NETRANGE OPTIONS:
  -d, --delay <value>   The maximum value of seconds to wait between whois queri
es, the value is defined randomly, default: 3s.
  -w, --whois           Perform the whois queries on c class network ranges.
                         **Warning**: this can generate very large netranges and
 it will take lot of time to performe reverse lookups.
REVERSE LOOKUP OPTIONS:
  -e, --exclude <regexp>
                        Exclude PTR records that match the regexp expression fro
m reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
  -o --output <file>    Output in XML format. Can be imported in MagicTree (www.
gremwell.com)
root@kali:~# dnsenum --enum [TARGET DOMAIN NAME]
```

DNSenum in terminal

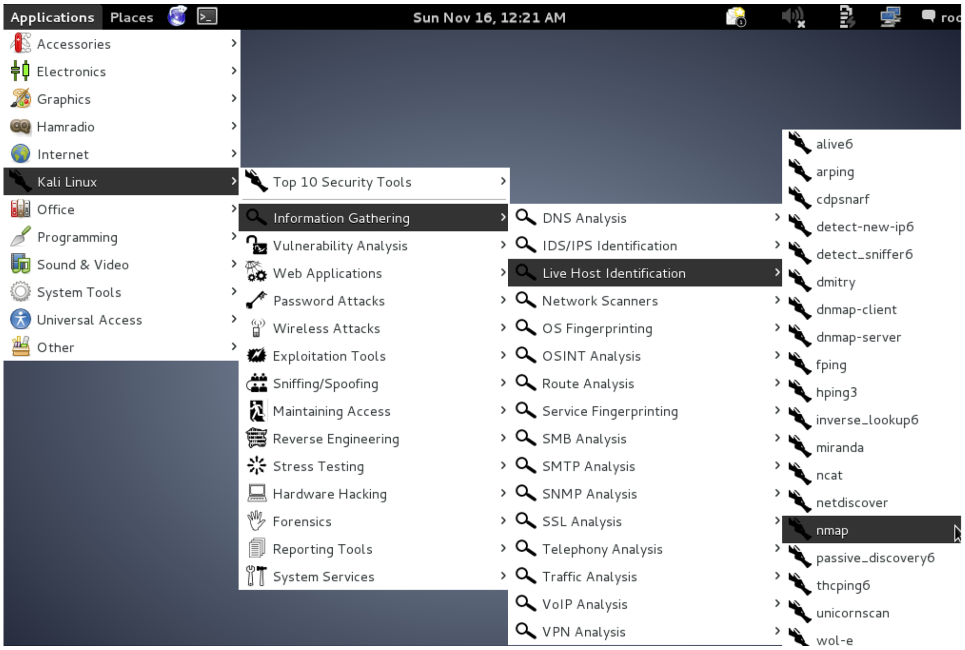
2. dmitry - The Network Rangefinder

    Once your DNSenum information has come back, you will have a range of servers used by your target. The goal of the dmitry rangefinder is to find out which IP's are used on those servers. This is done using a TCP traceroute command which can be threaded, and displayed graphically with dmitry commands.

3. Nmap

    The Nmap (Network Map) project is famous for its standalone application and open source code. The Nmap tool in Kali Linux is used to determine if a host is alive, active, and gives a bounty of other information in one quick scan. Nmap is an essential tool for quickly gathering specific details on any active machine.

    > *“Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.”*



The Nmap tool is located at Kali Linux / Information Gathering / Live Host Identifcation

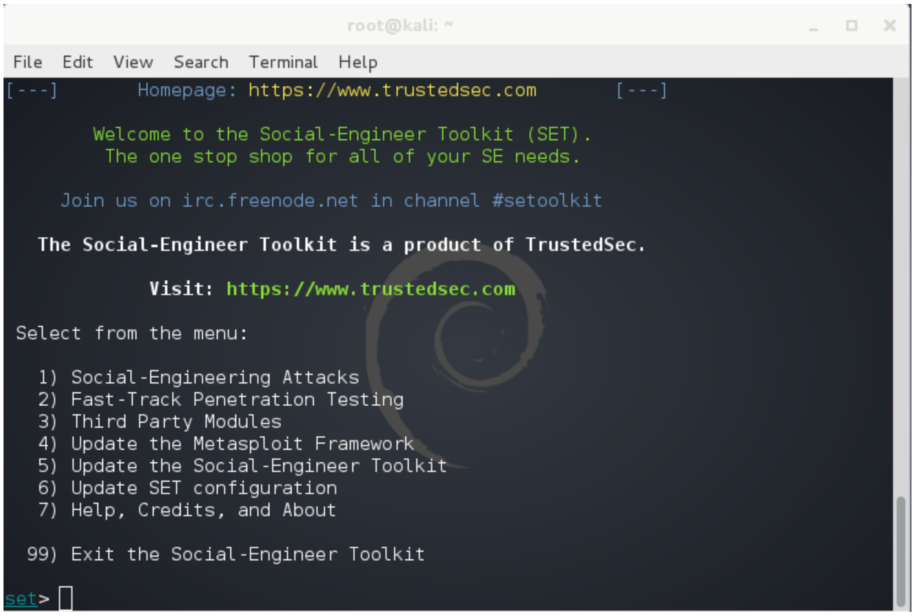
To add to the beauty, the Nmap scan can gather all of this information off only a handful of packets tossed around in such a way as to be quieter than many other available tools.

4. Maltego
Maltego is an excellent built-in tool from the development team at Paterva technologies. The design is unique and with a little time spent learning how to best play with it, Maltego quickly becomes an essential tool for any medium to large scale penetration test. The system is built to determine relationships between actors in an environment. This could be a name, a DNS server, an IP address, a WHOIS lookup, or any number of other bits of information. Maltego will do some rooting around and come up with a logical map that displays these relationships visibly. In invaluable tool for the critical penetration tester, these logical maps will shed light on a messy situation, or reaffirm suspected relationship links.

Once all your information gathered from DNSenum, dmitry, and Nmap has been poured over and filtered into Maltego, a clean and clear logical map of your target’s environment can be formed.

5. Social Engineering Toolkit

The Social Engineering Toolkit (SET) is designed to help the penetration tester work against the human elements of the target’s security environment. Working with a wide variety of tools, SET enables the attacker to exploit weaknesses in security training, as opposed to weaknesses in hardware or software.



```
[---]       Homepage: https://www.trustedsec.com       [---]

       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

    Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

People are often the weakest link in any security system.

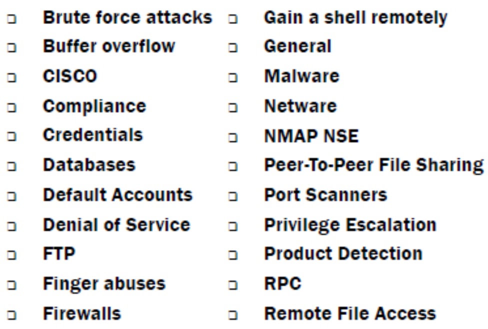
Social Engineering takes on a different attack path at first glance, but information gained through social engineering attacks can quickly be turned into a serious advantage for the penetration testing team. SET can be accessed by opening terminal and entering. “setoolkit”. Experience working with java applets will be helpful when working with SET to plan attacks. SET can also be used during Phase Four : Exploitation, to deliver clickables that will help gain access to a target’s machine. Personally I find it most useful in the information gathering stages, although it can be more invasive and louder depending on the level of security awareness in the target environment.

Tools for Phase Two

Vulnerability Detection and Enumeration

6. Nessus - Working With Vulnerabilities
   Taking your logical map from Maltego, and the wealth of technical information gathered from the time spent in Nmap, it’s time to find vulnerabilities that lie in the target’s system. Neesus takes command of the next step, finding vulnerabilities in the local system, in the local network, and in both Linux and Windows environments. When checking a network for vulnerabilities, Neesus is as thorough as tools come. Although Neesus works on Kali Linux, it is not bundled with the download, and will need to be downloaded and unpackaged on the Kali Linux OS. Registration through the Neesus website is also required to run this tool.

7. OpenVAS - Open Vulnerability Assessment System
   OpenVAS is bundled and packaged with Kali Linux, but is less polished than its cousin. Both OpenVAS and Neesus work to discover vulnerabilities in local systems, networks, and operating systems. After running all your gathered information through one or both of these tools, you will have a list of vulnerabilities that will prove essential in getting into the target system. Using the targeting data we gathered in phase one, you can set OpenVAS to scan each machine in the target’s network for vulnerabilities. After this detailed scan, you can take a step back and scan the target network itself for vulnerabilities. The list of weaknesses is long and varied, and will give the attackers essential data to help target a specific vulnerability to exploit.



□ Brute force attacks
□ Buffer overflow
□ CISCO
□ Compliance
□ Credentials
□ Databases
□ Default Accounts
□ Denial of Service
□ FTP
□ Finger abuses
□ Firewalls
□ Gain a shell remotely
□ General
□ Malware
□ Netware
□ NMAP NSE
□ Peer-To-Peer File Sharing
□ Port Scanners
□ Privilege Escalation
□ Product Detection
□ RPC
□ Remote File Access

A list of different kinds of vulnerabilities OpenVAS can find
from the Kali Linux Cookbook

Tools for Phase Three

Penetration Attempts

At this phase, penetration testers will take the logical maps of the environment, and the list of exploitable vulnerabilities gathered in phases one and two. In a team of attackers, this is the perfect time for a brief pause and gathering of the troops. Up until this point most of the tools used were relatively quiet and noninvasive, and while Kali Linux is generally a very quiet set of tools, the pattern of attacks from here on out is necessarily noisier, and a lot more rides on the quality of the defense. If the attacking team is properly prepared, choosing which attack vector to hit is the next key step.

Wifi Attacking

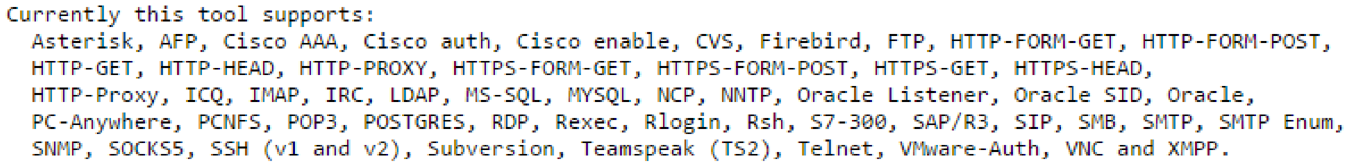
8. Aircrack-ng
   Aircrack-ng is a valuable tool for injecting wireless packets into an active network. This tool relies on the attackers knowledge of wireless cards, both on the attacking machine and on the target machine, so before deploying Aircrack-ng in your offensive environment, be sure you have the requisite information gathered from phase one. Once active, Aircrack-ng can also recover 802.11 WEP and WPA-PSK keys by gathering packets sniffed wirelessly. WEP attacks have been well known and well documented in the security community since at least 2007, but because of the nature of networked communication, injection attacks are still a very popular method of getting access to a network.

Web Application Attacking

9. Burp Suite
   Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

10. Hydra
    Web application exploitation is a growing source of headaches for defensive security teams worldwide. Hydra is an extremely fast password cracking tool which supports attacks in over 50 different protocols. However due to the nature of Hydra’s attack

pattern, it’s much noisier than other methods of password cracking. The brute force methods of password stealing that Hydra allows are very effective and exceptionally fast, but this should be considered a fall-back tool for high-security environments as it will increase your chances of being detected.



```
Currently this tool supports:
  Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST,
  HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD,
  HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle,
  PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP, SMTP Enum,
  SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.
```

Supported protocols in Hydra

11. Owasp - ZAP
    For the security-minded, Owasp should be a familiar name. The Open Web Application Security Project is well known as one of the most respected and active open source security projects on the internet. Founded as a nonprofit in 2001, the Owasp team has been active in information security, development of penetration tools and digital freedom movements. ZAP is the “Zed Attack Proxy Project”. The tool is simple enough for new penetration testers, and robust enough for professional environments. Both passive and active scanners are built in, and brute force attacks can be used to break in and hunt for files even if there are no direct links to the files to be detected.

Password Attacks

12. John The Ripper
    Known by the nickname “John”, John the Ripper is a well developed free password attacking tool developed as an all purpose attacking tool. Being able to call on different libraries of password guessing methods, from dictionary attacks to hybrid cracks to the cumbersome brute-force methods used in other tools, John is a catch-all for password guessing software.

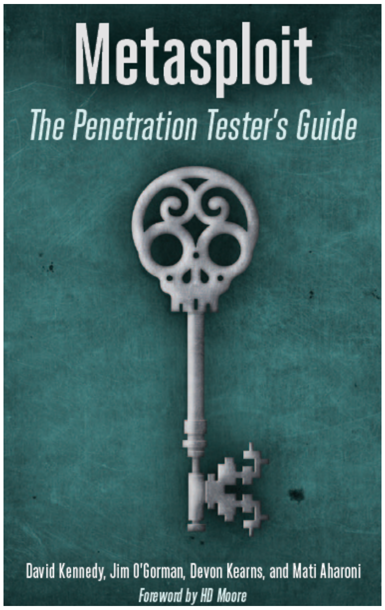
13. Pass the Hash Toolkit
    While John goes straight for the password in an attempt to reveal it, the Pass the Hash Toolkit enables attackers to gather the hash from an accepted password and use the data after the password is accepted to get through into systems without having to use noisy and slow password guessing techniques. In a very informative whitepaper out of the SANS institute, we get a good overview of PtH techniques, and where it fits in contextually with other penetration testing tools.

Phase Four

Exploitation

This is the real meat of any penetration test. All the above tools are used to gain information and access to a system. Some offensively minded security professionals find the early stages of a penetration test to be tedious and dry. I believe the first three phases are not unlike playing a game of chess, where phase four is the final execution of your intricate plans just before a checkmate. Exploitation is the proof of all the work you've done in mapping the system and opening the doors. Even more so than before, you must be careful not to permanently damage any systems you are testing. Make note and document that they could have been damaged, and when the time comes to present your findings, be clear and honest about the state of security. Doing permanent damage to a system is a quick way for a professional penetration tester to find himself unemployed and unemployable.

14. Metasploit Framework
    The Metasploit Framework run through the Metasploit Framework Console is among the most advanced tools in the Kali Linux arsenal. The Metasploit team is legendary, and their work in the offensive info-sec field is without parallel. Kali Linux itself was based on developing an OS that incorporated all the tools of Metasploit and Backtrack together. Metasploit itself could be considered an all-in-one penetration testing tool, and for many it still is. Of all the tools in this list, only Burp Suite comes close in robustness and polish that Metasploit offers, and the Burp Suite tools are a distant second when compared to the depth of Metasploit's toolkit. Truly the top of the line for a dedicated offensive security professional. Metasploit offers tools that can be used in every phase of a penetration test, from passive information gathering tools to vulnerability scans. The most exciting portion of the toolkit comes at exploit payload development and delivery.


Metasploit
The Penetration Tester's Guide
David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni
Foreword by HD Moore

Metasploit is an incredibly robust penetration testing toolkit.

15. The Browser Exploitation Framework (BeEF)

BeEF is an excellent tool for exploiting vulnerabilities in the browser and browser cached information blocks. At the time of writing the BeEF tool in Kali Linux is still being smoothed out, with a couple errors and some general usability issues being touched up. BeEF specializes in client-side attacks, focusing on the web browser itself. No other tool on this list has reached the level of usability and specialization in specific location attacks as BeEF. With special methods of attacking a web browser, BeEF allows the attacker to hit the system directly from a security vector often overlooked by defensive development teams.

16. Armitage

Ignoring the quirky anime style of the website, Armitage is actually a very advanced tool for finding and executing exploits to allow the penetration testing team to gain access to a network. Bundled with Metasploit, Armitage is not the script-kiddie plaything it appears to be stylistically, but is actually advanced enough for professional environments. With built in automation of many different attacks, and options to find and exploit several attack vectors on the same target, Armitage is a quality weapon in the arsenal even if it is branded in a peculiar way.

17. Yersinia

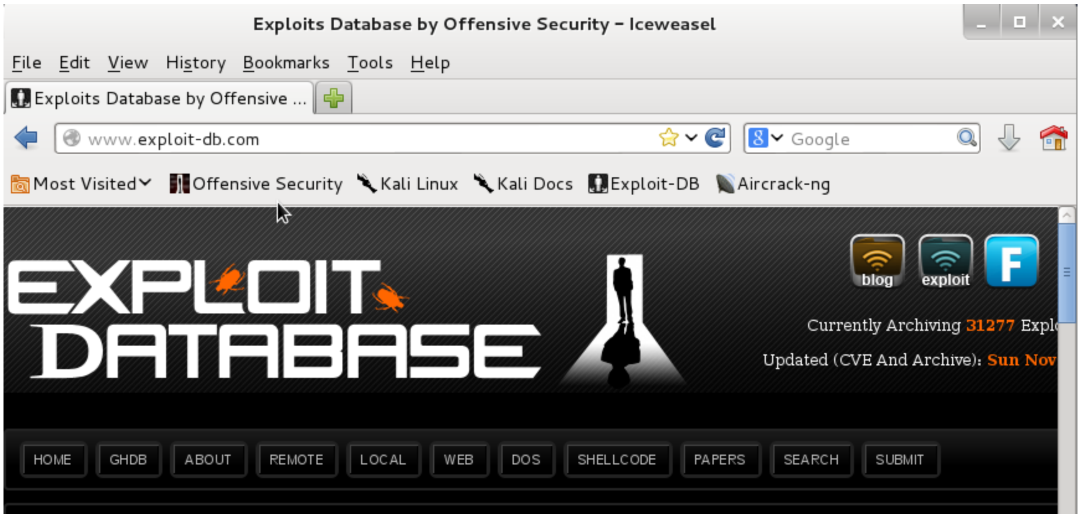
A relatively older tool launched by the S21Sec team in 2005, Yersinia has returned to popularity as a reliable tool that attacks Layer 2 network systems. Instead of more traditional attacks like ARP poisoning or cache attacks, Yersinia is able to go after switches and hubs. With many networks having limited defenses and poorly organized or configured networking hardware, Yersinia is a prime example of a tool striking where your target is weakest. Further, as these most defensive security tools guard web portals, databases and workstations, Yersinia is working in an environment where noise is the standard and detection is generally weaker.

18. Durandal's Backdoor (DBD)

DBD is an new and often overlooked tool used to maintain access to compromised systems. This is an absolutely essential part of a successful penetration test, especially in light of recent high profile attacks to Home Depot and Target where attackers stayed in the system for weeks after gaining access. DBD is currently operating in only TCP/IP protocol. Reconnection testing is a less exciting part of exploitation, but key to making sure defensive systems have had their problems actually solved. Successful DBD testing will make sure the security hole was actually closed, instead of simply throwing the attackers out while leaving the door open.

19. Exploit Database (EDB)

While not directly an offensive exploit tool, the exploit database built in to Kali Linux is the best location for the most up-to-date exploits available. Maintained by the Kali Linux, Metasploit, and Offensive Security teams, EDB is the possibly the best place on the internet to find exploits in any number of areas. Searchable by description, author, platform, type, language or port, EDB is currently holding over 30,000 known exploits at the time of writing.



In Kali open up your Iceweasel browser. Exploit DB is already bookmarked.

Phase Five

Reporting

20. RecordMyDesktop

While working with all the above tools, we leap over the line from safe to illegal and work directly with tools that could easily break a business. The point of a penetration test is to attack an environment in a controlled way so the defenders can have accurate and honest information on their weaknesses. Offensive security is a defensive tool. As flashy as exploits may be, everything in your offensive arsenal comes down to a simulated attack. Wargaming is only as good as the lessons learned at the end. RecordMyDesktop is the least technical tool on this list, but in my opinion, the most important. Showing exactly how an exploit worked, and having a clear and objective record of the attack taking place will be essential for the analysis and cleanup stages after the penetration test has completed.

Remember to ask questions when in doubt. The tools listed here can be used for great evil, and that’s exactly why they were included. Knowing the enemy is half the battle.

Keep yourself safe, and happy hacking.