www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 9907-9911

Deciphering The Prominent Security Tools Ofkali Linux

Talatam.Durga Rao[1], Vankayalapati.Sai Madhav[2] and Konduri.Sai Ram Kiran[3]

[1]Department of Electronics and Computers,
K.L University, Guntur, India,522 502
durgaraot24@gmail.com

[2]Department of Electronics and Computers,
K.L University, Guntur, India,522 502
saimadhav95@gmail.com

[3] Department of Electronics and Computers,
K.L University, Guntur, India,522 502
kirannarik63@gmail.com

Abstract*: *Kali Linux is the operating system that is reverenced by almost every cyber security professional since 2013.While Kali is extensivelydeveloped for penetration testing and digital forensics, it is considered as quintessential operating system for tenderfoot hackers.Basically Kali is the renaissance of Backtrack which typically means that kali is the offspring of backtrack.When it comes to security Kali has the eminent set of exemplary tools. These tools are panacea for your own security practices before a real intruder does it.Among all such tools,there are tools which are highly enamored by security research professionals. This paper enumerates these top tensecurity tools of Kali Linux and is an epistle that will hanker the sinister powers for the use of good.

Keywords*:*Backtrack, Cyber security, Digitalforensics, Penetrationtesting, Tenderfoot hackers.

1.INTRODUCTION:

Kali isthe new generation of the industry-leading Backtrack Linux penetration testing and security auditing Linux distribution. Kali Linux is a complete re-build of Backtrack from the ground up, adhering completely to Debian development standards. It was developed by Mati Aharoni and Devon Kearns.

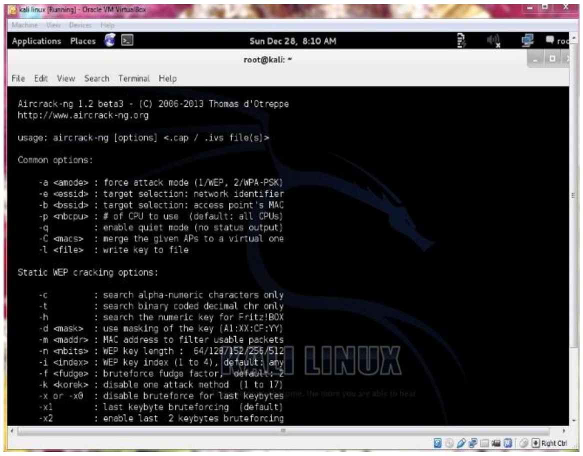
Security is something which is elusive and so everyone needs to be aware of and imminent to deal with. While you can go out and collect a number of tools and utilities to help you out, there is an easier path. There are several Linux distributions out there that provide an entire suite of tools to fit your security needs. One of the more popular ones is Kali Linux (originally Backtrack).This has a unique feature of segregating the top ten security tools such as air cracking, burp suite, hydra, john, malt ego, metasploit framework, nmap, owasp-zap, sqlmap, Wireshark.

2. CLASSIFICATION

The rampant growth of network penetrations is due to increasing number of budding aggressors .As plumber opts his efficient tools so do the curious professionals go for Kali top security tools. They are:

2.1. AIRCRACK-NG

Aircrack-ng is a suite of tools that allows you to monitor, gather packets, inject them and finally crack a network’s key in order to gain access. Nearly all wireless networks now use WPA2 (WIFI Protected AccessII) for security as you will see WEP (Wired Equivalent Privacy) security just won’t meet the requirements any more [1]. Most wireless networks will use either WEP or WPA, to be able to crack either of these you will need to have a wireless card that can both monitor and inject packets.


kali linux [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places
Sun Dec 28, 8:10 AM
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
Right Ctrl

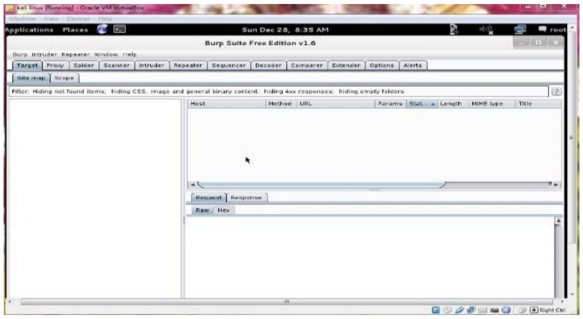
```
Aircrack-ng 1.2 beta3 - (C) 2006-2013 Thomas d'Otreppe
http://www.aircrack-ng.org

usage: aircrack-ng [options] <.cap / .ivs file(s)>

Common options:

    -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
    -e <essid> : target selection: network identifier
    -b <bssid> : target selection: access point's MAC
    -p <nbcpu> : # of CPU to use  (default: all CPUs)
    -q         : enable quiet mode (no status output)
    -C <macs>  : merge the given APs to a virtual one
    -l <file>  : write key to file

Static WEP cracking options:

    -c         : search alpha-numeric characters only
    -t         : search binary coded decimal chr only
    -h         : search the numeric key for Fritz!BOX
    -d <mask>  : use masking of the key (A1:XX:CF:YY)
    -m <maddr> : MAC address to filter usable packets
    -n <nbits> : WEP key length :  64/128/152/256/512
    -i <index> : WEP key index (1 to 4), default: any
    -f <fudge> : bruteforce fudge factor,  default: 2
    -k <korek> : disable one attack method  (1 to 17)
    -x or -x0  : disable bruteforce for last keybytes
    -x1        : last keybyte bruteforcing  (default)
    -x2        : enable last  2 keybytes bruteforcing
```

Fig: 1

The above figure illustrates the terminal view of aircrack-ng where numerous options were displayed.

2.2 BURPSUITE

Burp Suite is an integrated platform for performing security testing of web applications. It is not a point-and-click tool, but is designed to be used by hands-on testers to support the testing process. With a little bit of effort, anyone can start using the core features of Burp to test the security of their applications [2]. Some of Burp's more advanced features will take further learning and experience to master. All of this investment is hugely worth it - Burp's user-driven workflow is by the far the most effective way to perform web security testing, and will take you way beyond the capabilities of any conventional point-and-click scanner.


kali linux [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places
Sun Dec 28, 8:35 AM
root
Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Host Method URL Params Stat... Length MIME type Title
Request Response
Raw Hex
Right Ctrl

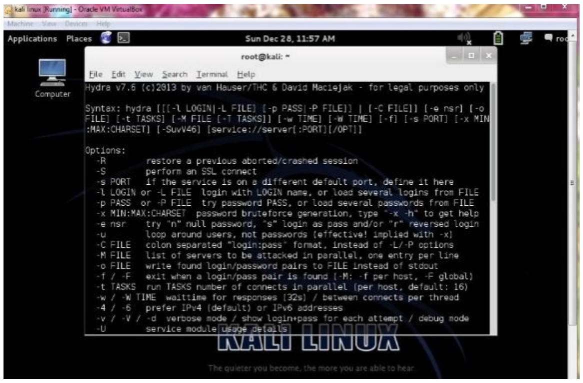
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Fig: 2

Burp is intuitive and user-friendly, and the best way to start learning is by doing**.**

2.3 HYDRA:

Hydra is a online password cracking tool which can be used to dictionary-attack various services by trying lists of user-names and passwords until a successful login is found. It is multi-threaded, and can be very fast,tryingusername/password combinations at a rate of thousands per minute[3].


kali linux [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places
Sun Dec 28, 11:57 AM
Computer
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.

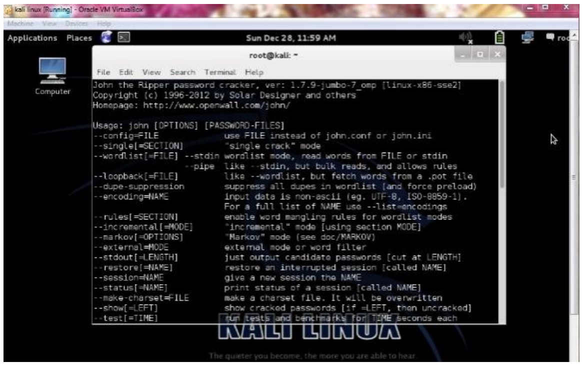
```
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o
FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN
:MAX:CHARSET] [-SuvV46] [service://server[:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to be attacked in parallel, one entry per line
  -o FILE   write found login/password pairs to FILE instead of stdout
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel (per host, default: 16)
  -w / -W TIME  waittime for responses (32s) / between connects per thread
  -4 / -6   prefer IPv4 (default) or IPv6 addresses
  -v / -V / -d  verbose mode / show login+pass for each attempt / debug mode
  -U        service module usage details
```

Fig:3

Hydra can be used to attack many different services including IMAP, SMB(Server Message Bloch), HTTP, VNC(Virtual Network Computing), MS-SQL MySQL, SMTP, SSH(Secure Shell), and many more

2.4 JOHN

John the ripper is a free and fast password cracker that can be effectively used to break weak UNIXpasswords, windowsLM, Hashes, DES, Kerbos, and many more cryptic methodologies. Cracking passwords with john can be done by brute force technique wherein the encrypted password can be provided inside a file.


kali linux [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places
Sun Dec 28, 11:59 AM
Computer
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.

```
John the Ripper password cracker, ver: 1.7.9-jumbo-7_omp [linux-x86-sse2]
Copyright (c) 1996-2012 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--config=FILE             use FILE instead of john.conf or john.ini
--single[=SECTION]        "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but fetch words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--encoding=NAME           input data is non-ascii (eg. UTF-8, ISO-8859-1).
                          For a full list of NAME use --list=encodings
--rules[=SECTION]         enable word mangling rules for wordlist modes
--incremental[=MODE]      "incremental" mode [using section MODE]
--markov[=OPTIONS]        "Markov" mode (see doc/MARKOV)
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset file. It will be overwritten
--show[=LEFT]             show cracked passwords [if =LEFT, then uncracked]
--test[=TIME]             run tests and benchmarks for TIME seconds each
```

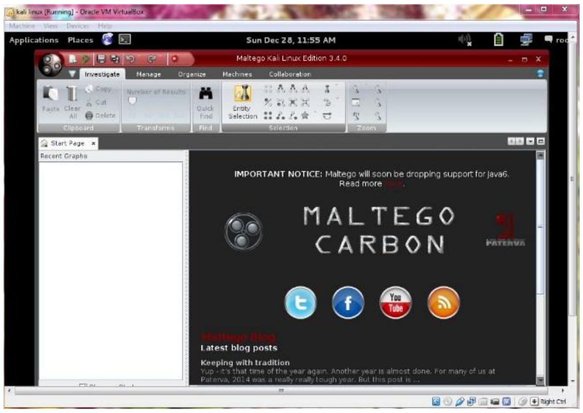
Fig:4

Alternatively, we can also provide a word list of passwords against which we can apply the brute force technique to match the password.

2.5 MALTEGO

Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format. Maltego is basically an information gathering tool that can search the internet for publicly available information about a site or organization [4].

This helps in assessing the amount of information that has reached the public domain and if it poses a security threat [6]. For example it can search google, twitter and other similar sources for the email addresses, domain names related to a particular site, and even names and details of individuals.



IMPORTANT NOTICE: Maltego will soon be dropping support for Java6.
Read more .

Latest blog posts

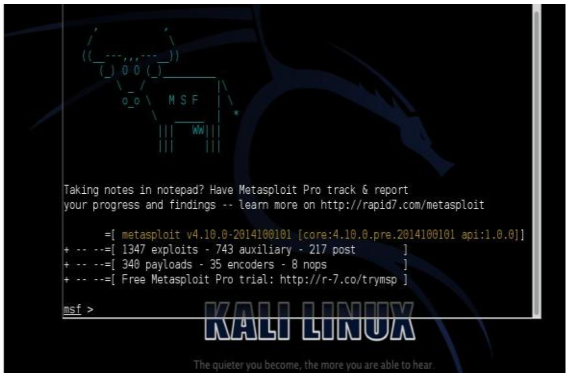
Keeping with tradition
Yup - it's that time of the year again. Another year is almost done. For many of us at Paterva, 2014 was a really really tough year. But this post is ...

Fig:5

The basic idea is to find as much information as possible about someone or some organisation, from free sources on the internet[5].

2.6 METASPLOIT-FRAMEWORK

Metasploit is one of the most popular open source penetration testing frameworks available today. It offers tons of tools that range from scanning utilities to easy to launch exploits that include encoders used to bypass common security defenses. I'll walk you through an example by compromising a Windows based authentication server that is not properly patched.



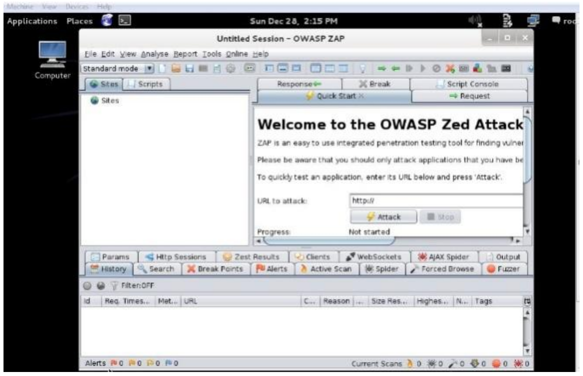
```
Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.0-2014100101 [core:4.10.0.pre.2014100101 api:1.0.0]]
+ -- --=[ 1347 exploits - 743 auxiliary - 217 post        ]
+ -- --=[ 340 payloads - 35 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Fig:6

To start using Metasploit in CLI, open up a terminal, go to /opt/metasploit and type "msfconsole". This brings up the msf > command prompt. Metasploit works by selecting a function defined in various folders such as windows exploits found under the exploit/windows/* folder. You can search the existing catalog of functions using "search" followed by a keyword such as searching RDP with hopes of finding a RDP based exploit. It's almost impossible to guess what exploit would work on a target so the typical use case is using a vulnerability scanner on a target to identify a weakness and matching that to an available exploit in Metasploit. For example, the next screenshots show running a NMAP scan followed running a Nessus vulnerability scan on a target to identify two critical vulnerabilities.

2.7 OWSAP-ZAP

The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.



Welcome to the OWASP Zed Attack

ZAP is an easy to use integrated penetration testing tool for finding vulner

Please be aware that you should only attack applications that you have be

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://

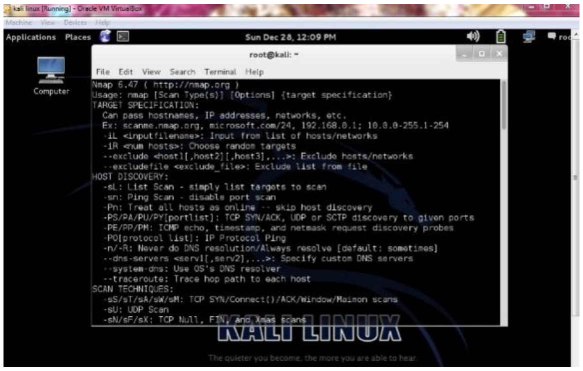
Progress: Not started

Fig: 7

ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually [7].

2.8 NMAP

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. 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. It was designed to rapidly scan large networks, but works fine against single hosts.


kali linux [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places
Sun Dec 28, 12:09 PM
Computer
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.

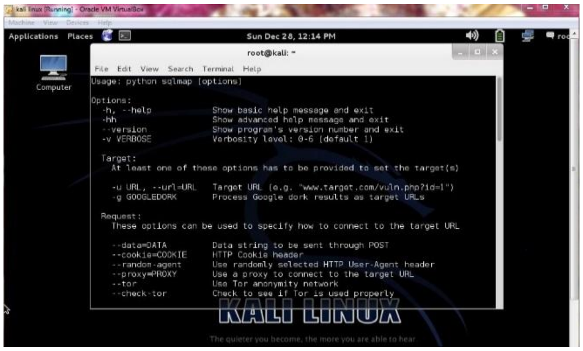
```
Nmap 6.47 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

Fig:8

Now nmap has a new feature called nmap scripts which allows developers to code scripts that can be used with nmap to automate certain kinds of scanning tasks. Nmap has a gui called zenmap, that can be used to save scan settings as profiles and use them later. Nmap also includes a netcat type utility called ncat which is very featureful and is available for both windows and linux.

2.9 SQLMAP

Sqlmap is one of the most popular and powerful sql injection automation tool out there. Given a vulnerable http request url, sqlmap can exploit the remote database and do a lot of hacking like extracting database names, tables, columns, all the data in the tables etc. It can even read and write files on the remote file system under certain conditions. Written in python it is one of the most powerful hacking tools out there. Sqlmap is the metasploit of sql injections.


kali linux [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places
Sun Dec 28, 12:14 PM
Computer
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.

```
Usage: python sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to set the target(s)

    -u URL, --url=URL   Target URL (e.g. "www.target.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST
    --cookie=COOKIE     HTTP Cookie header
    --random-agent      Use randomly selected HTTP User-Agent header
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly
```

Fig:9

- Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB database management systems.
- Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries and out-of-band.
- Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.
- Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack[5].

2.10 WIRESHARK:

Wireshark is a very powerful and popular network analyzer for Windows, Mac and Linux. It's a tool that is used to inspect data passing through a network interface which could be your ethernet, LAN and WiFi.

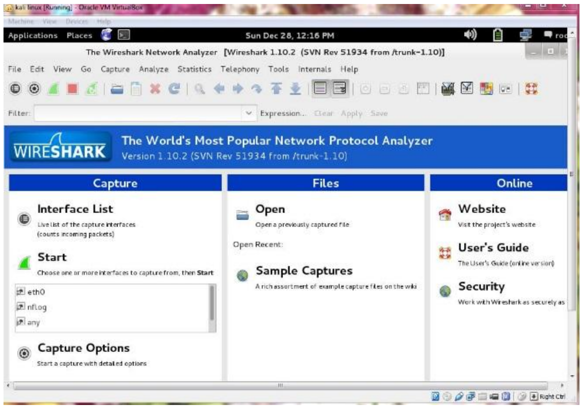

kali linux [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications Places
Sun Dec 28, 12:16 PM
The Wireshark Network Analyzer [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
nflog
any
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as
Right Ctrl

Fig:10

The series of data that Wireshark inspects are called 'Frames' which includes 'Packets'. Wireshark has the ability to capture all of those packets that are sent and received over your network and it can decode them for analysis. When you do anything over the Internet, such as browse websites, use VoIP, IRC etc., the data is always converted into packets when it passes through your network interface or your LAN card[8]. Wireshark will hunt for those packets in your TCP/ IP layer during the transmission and it will keep, and present this data, on its' very own GUI.

3.CONCLUSION

The efficacy of Kali Linux has always been proved from the time it was released. It is not mere flattery while it is the heart felt feeling of all security professionals that Kali is viable.Every tool associated with Kali nonchalantly performs its functions. The present trend and posterity should bear in mind that knowing the evil is only and only to fight against it and mitigate its effects.

REFERENCES

[1].http://www.hackwithkali.com/2013/10/the-aircrack-ng-suite_29.html

[2].http://www.securityninja.co.uk/hacking/burp-suite-tutorial-the-intruder-tool/

[3]. http://fe9.org/showthread.php?73411-Hydra-password-cracking-tool-with-Kali-Linux

[4].http://www.concisecourses.com/security/maltego-for-complete-beginners/

[5].http://www.darkmoreops.com/2014/08/28/use-sqlmap-sql-injection-hack-website-database/

[6]. http://www.binarytides.com/kali-linux-security

[7].https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

[8].http://www.concisecourses.com/security/wireshark-basics/