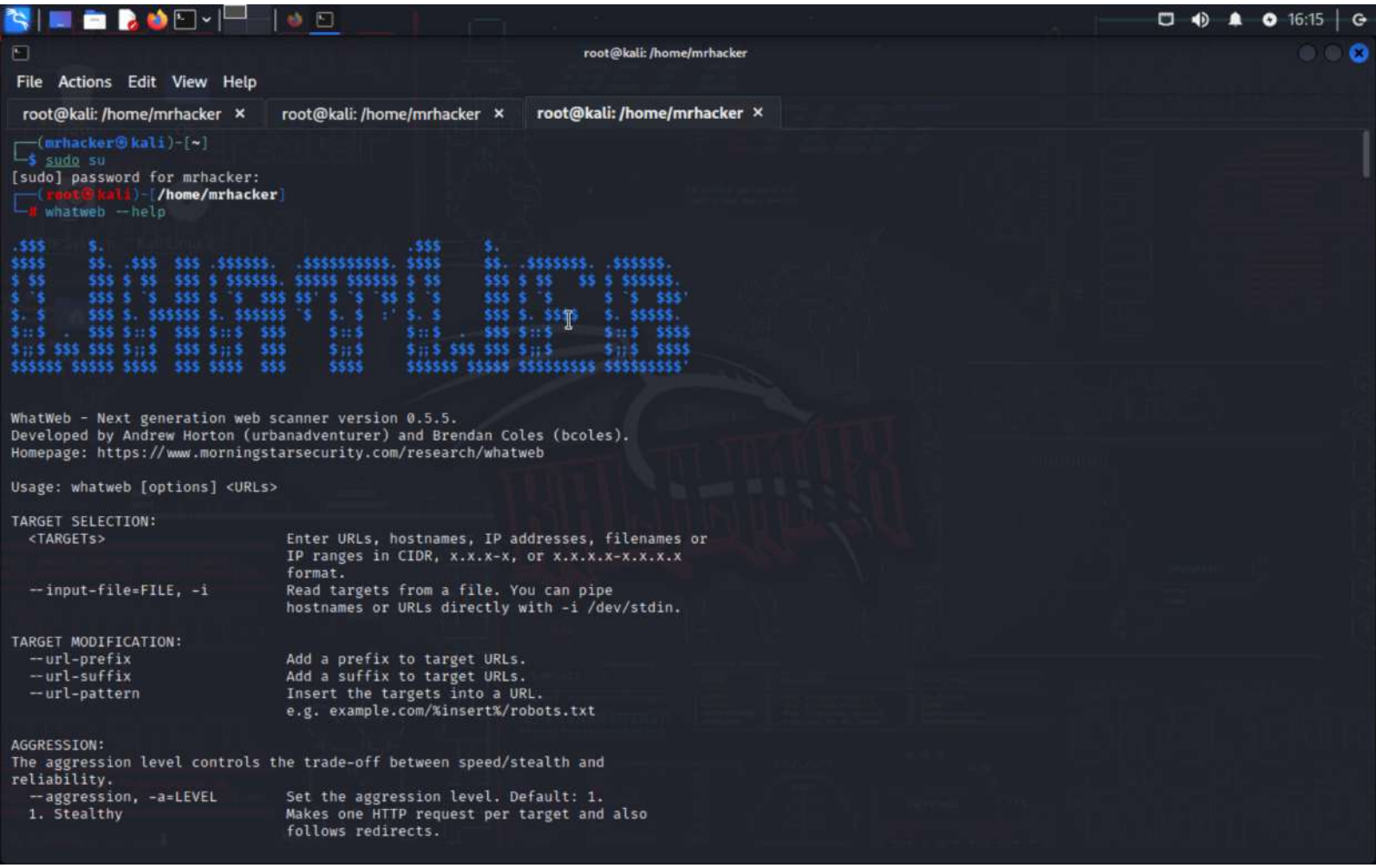
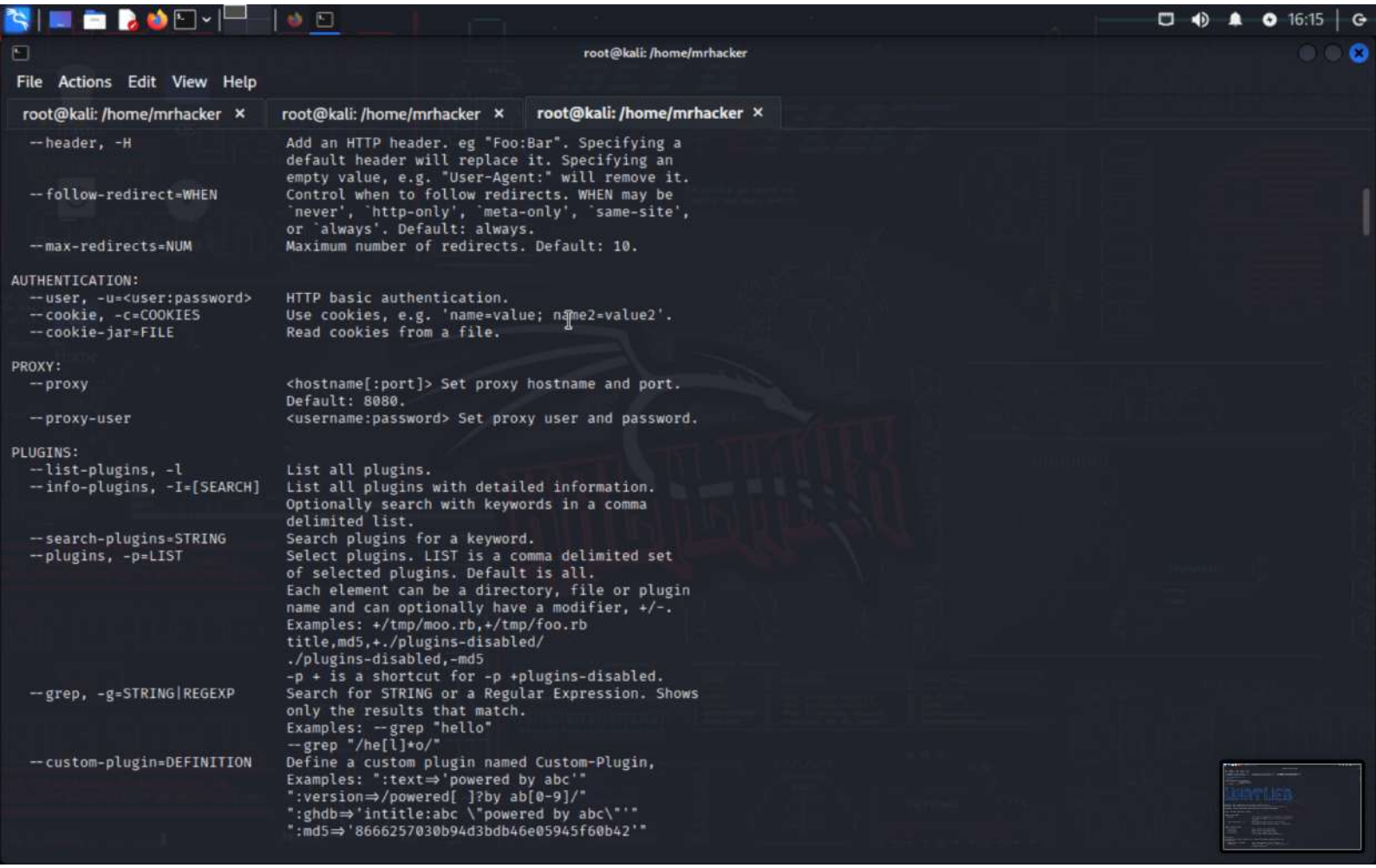
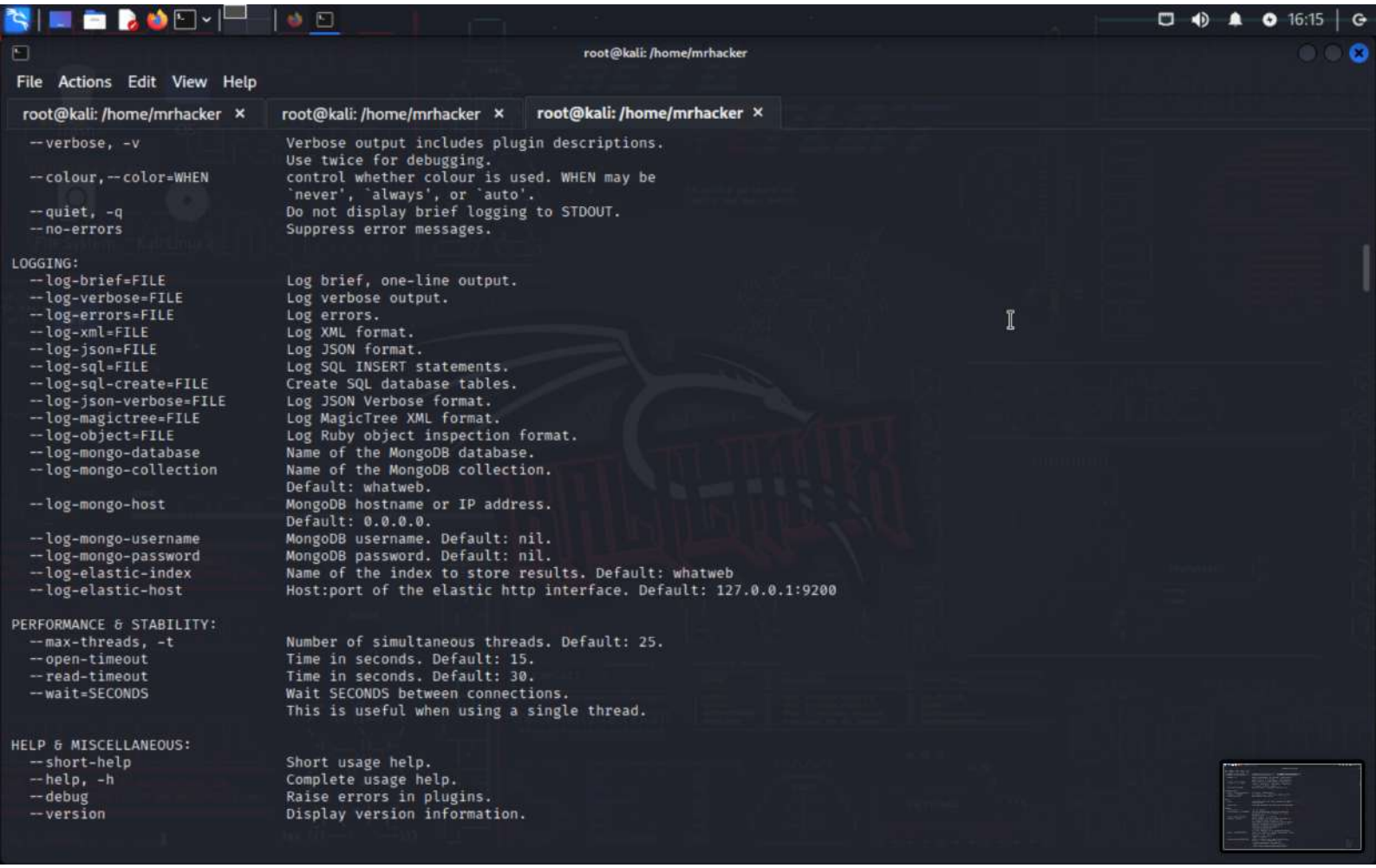
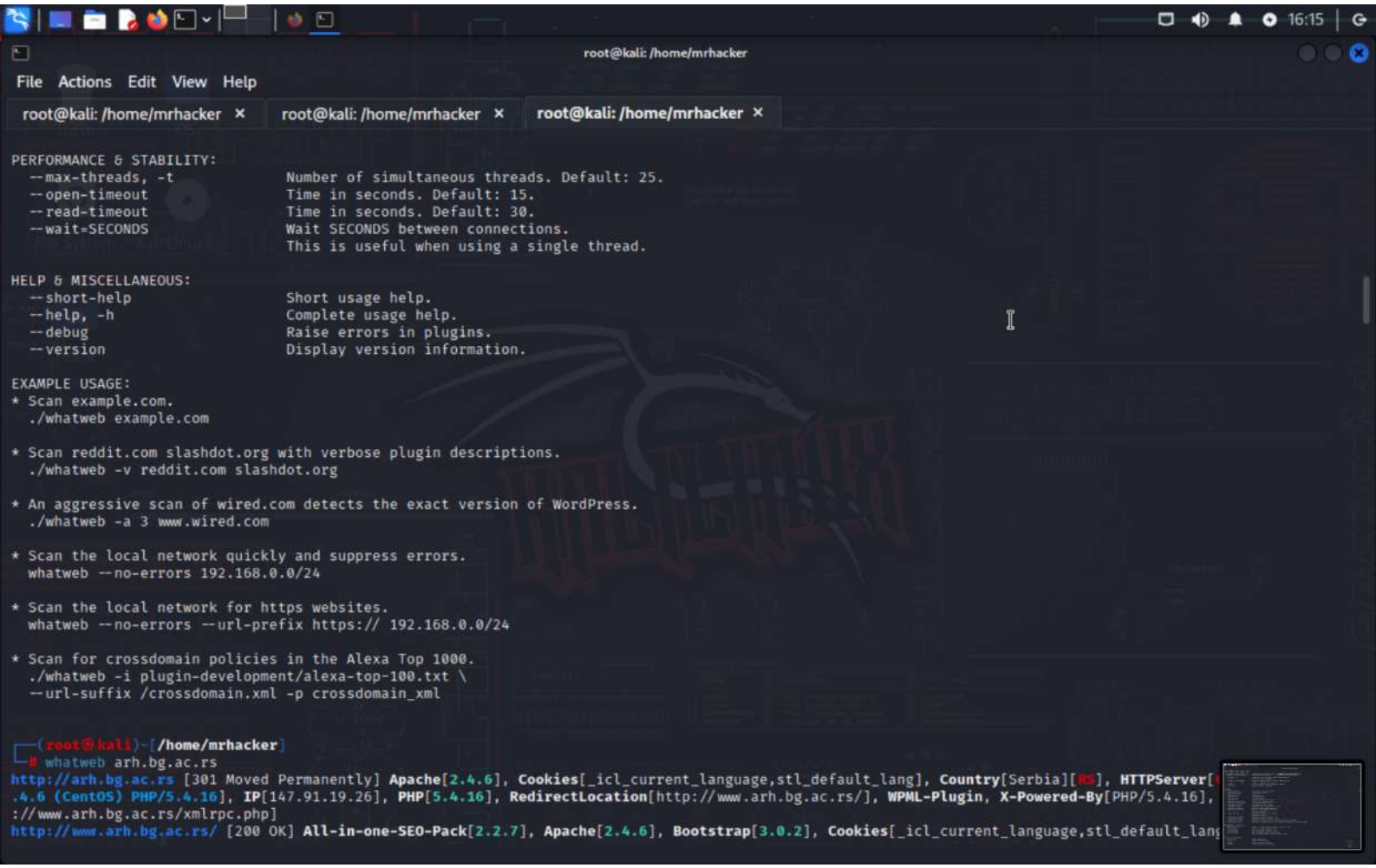
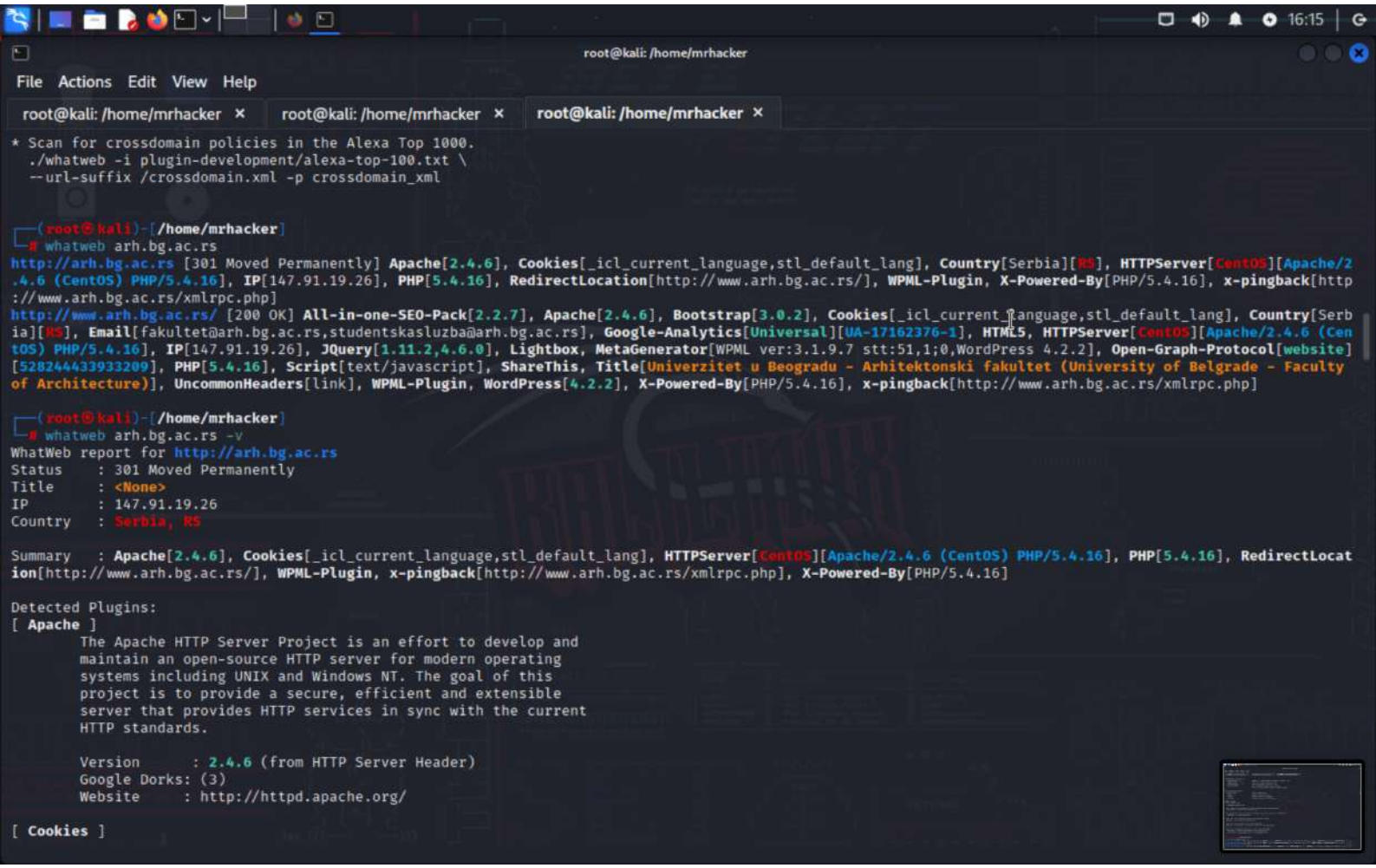
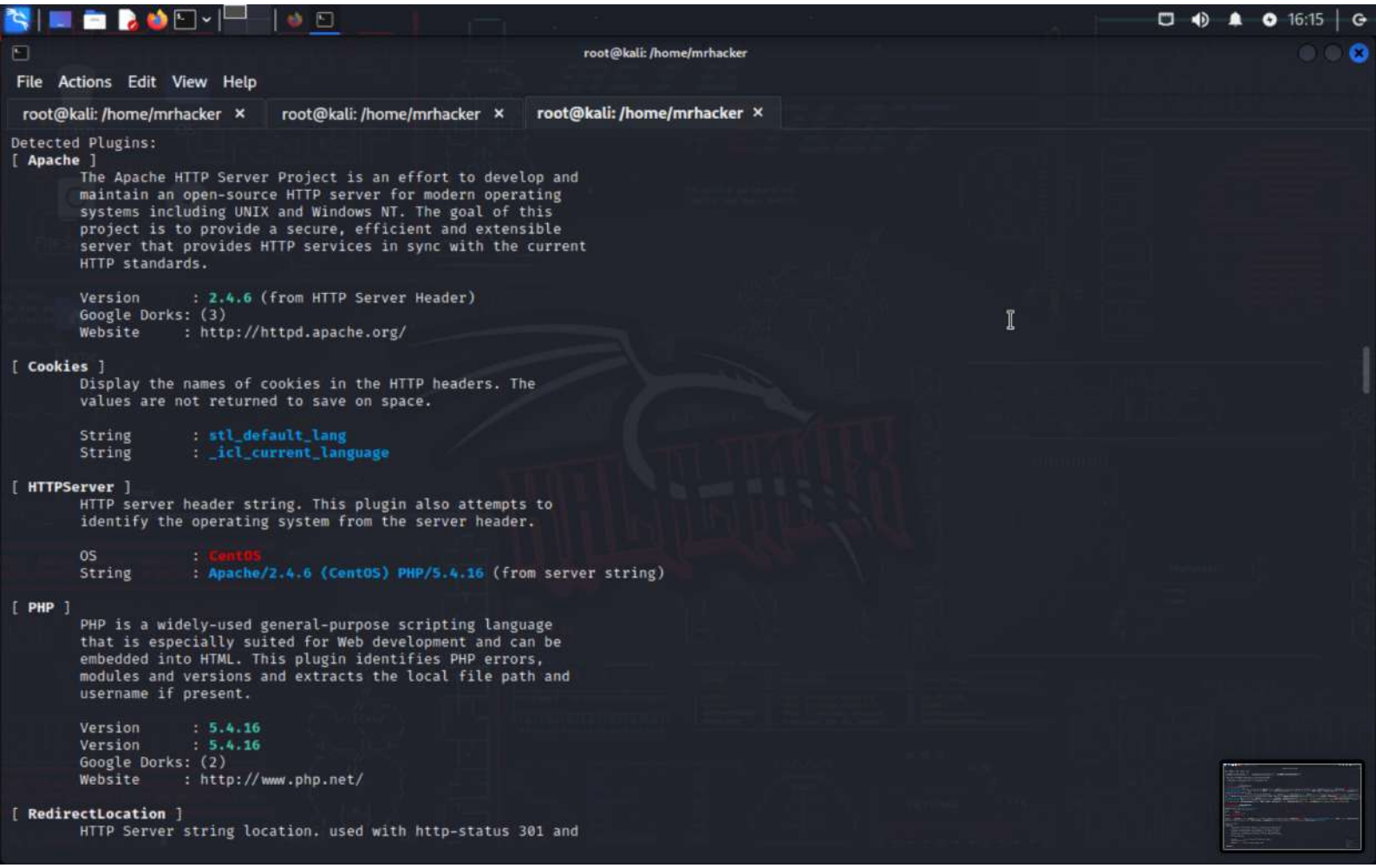

root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
(mrhacker@kali)-[~]
$ sudo su
[sudo] password for mrhacker:
(root@kali)-[/home/mrhacker]
whatweb --help
WhatWeb - Next generation web scanner version 0.5.5.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles).
Homepage: https://www.morningstarsecurity.com/research/whatweb
Usage: whatweb [options] <URLs>
TARGET SELECTION:
<TARGETs> Enter URLs, hostnames, IP addresses, filenames or
IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
format.
--input-file=FILE, -i Read targets from a file. You can pipe
hostnames or URLs directly with -i /dev/stdin.
TARGET MODIFICATION:
--url-prefix Add a prefix to target URLs.
--url-suffix Add a suffix to target URLs.
--url-pattern Insert the targets into a URL.
e.g. example.com/%insert%/robots.txt
AGGRESSION:
The aggression level controls the trade-off between speed/stealth and
reliability.
--aggression, -a=LEVEL Set the aggression level. Default: 1.
1. Stealthy Makes one HTTP request per target and also
follows redirects.

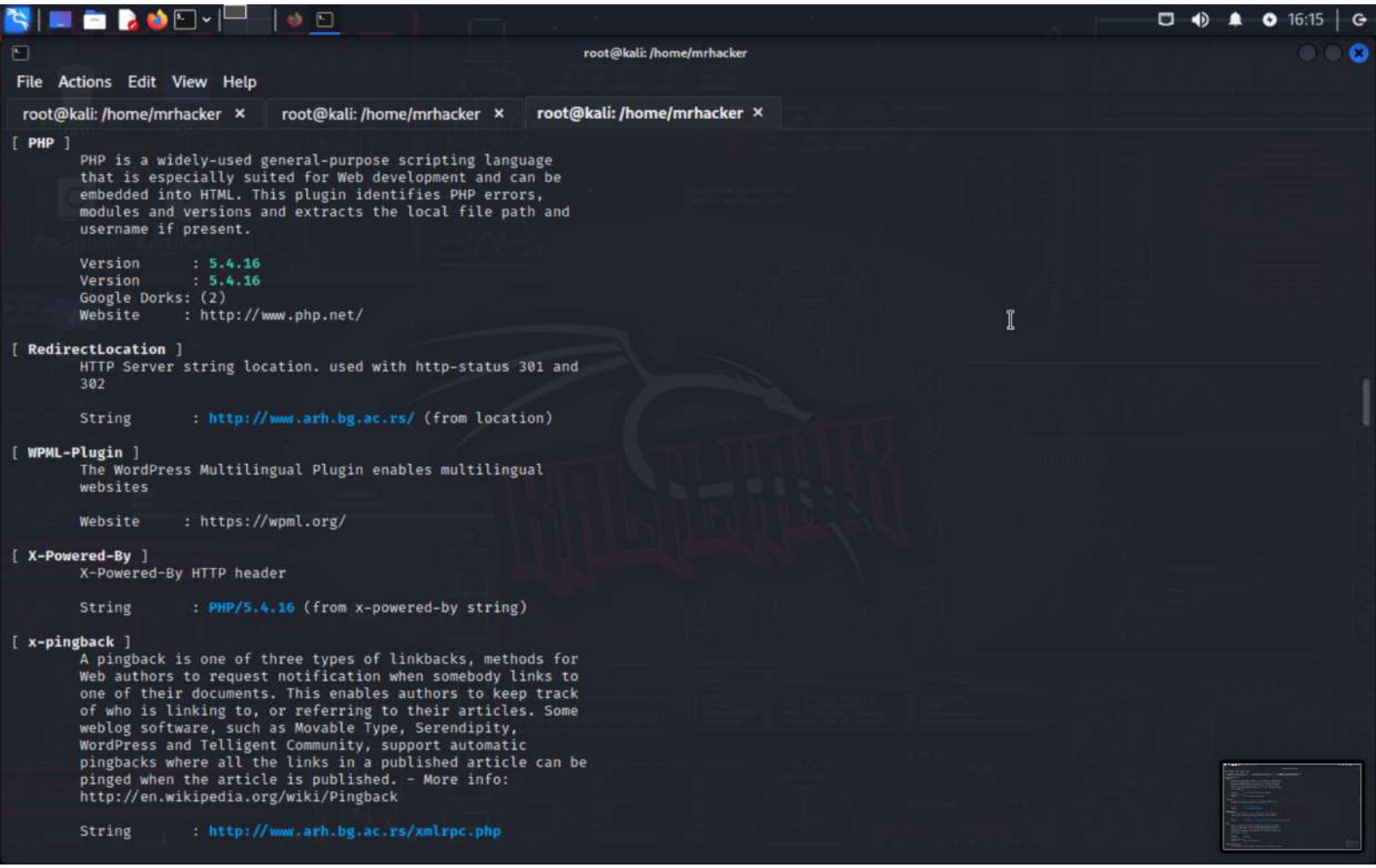

16:15
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
--header, -H Add an HTTP header. eg "Foo:Bar". Specifying a default header will replace it. Specifying an empty value, e.g. "User-Agent:" will remove it.
--follow-redirect=WHEN Control when to follow redirects. WHEN may be `never', `http-only', `meta-only', `same-site', or `always'. Default: always.
--max-redirects=NUM Maximum number of redirects. Default: 10.
AUTHENTICATION:
--user, -u=<user:password> HTTP basic authentication.
--cookie, -c=COOKIES Use cookies, e.g. 'name=value; name2=value2'.
--cookie-jar=FILE Read cookies from a file.
PROXY:
--proxy <hostname[:port]> Set proxy hostname and port. Default: 8080.
--proxy-user <username:password> Set proxy user and password.
PLUGINS:
--list-plugins, -l List all plugins.
--info-plugins, -I=[SEARCH] List all plugins with detailed information. Optionally search with keywords in a comma delimited list.
--search-plugins=STRING Search plugins for a keyword.
--plugins, -p=LIST Select plugins. LIST is a comma delimited set of selected plugins. Default is all. Each element can be a directory, file or plugin name and can optionally have a modifier, +/-. Examples: +/tmp/moo.rb,+/tmp/foo.rb title,md5,+./plugins-disabled/ ./plugins-disabled,-md5 -p + is a shortcut for -p +plugins-disabled.
--grep, -g=STRING|REGEXP Search for STRING or a Regular Expression. Shows only the results that match. Examples: --grep "hello" --grep "/he[l]*o/"
--custom-plugin=DEFINITION Define a custom plugin named Custom-Plugin, Examples: ":text⇒'powered by abc'" ":version⇒/powered[ ]?by ab[0-9]/" ":ghdb⇒'intitle:abc \"powered by abc\"'" ":md5⇒'8666257030b94d3bdb46e05945f60b42'"

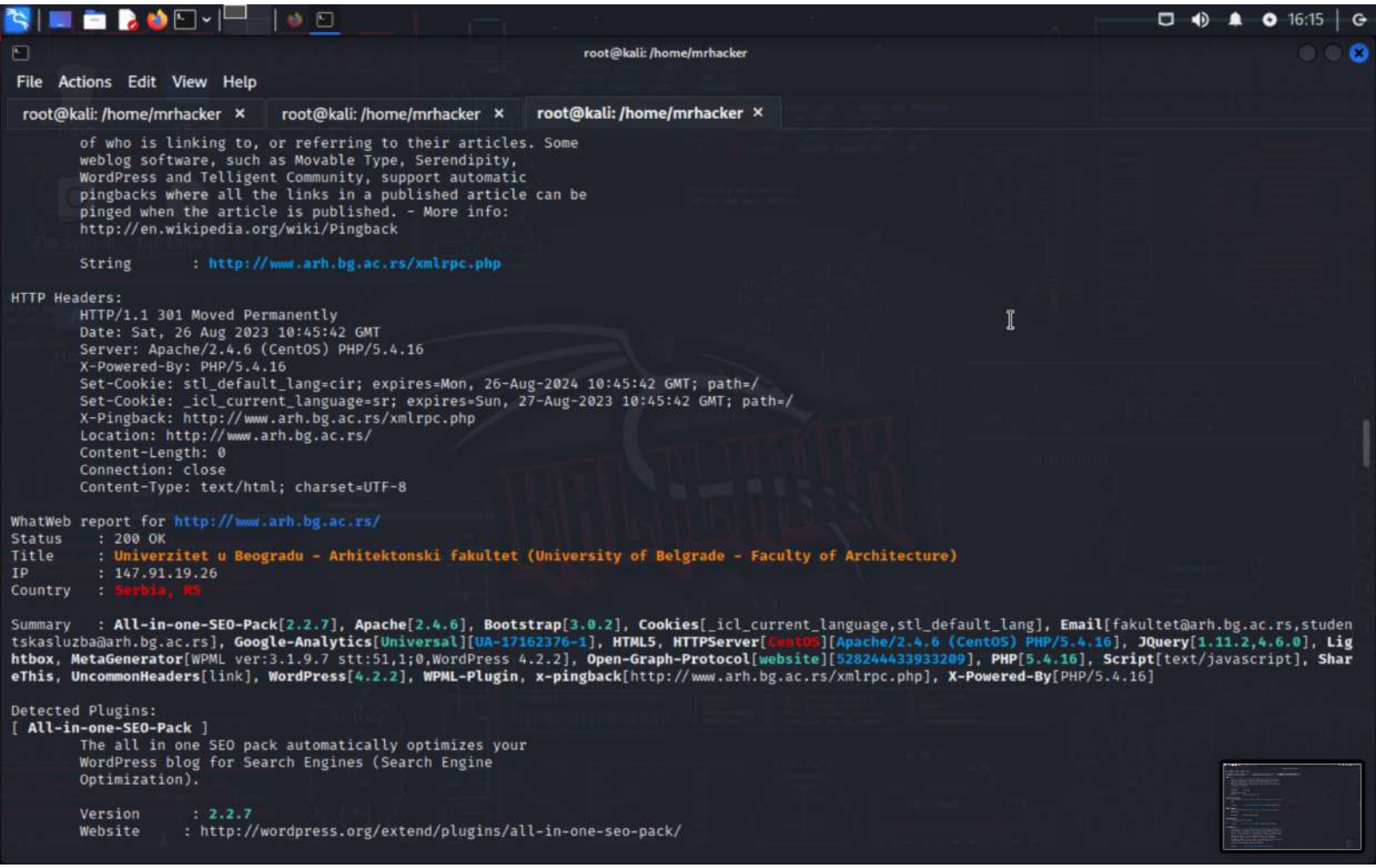

16:15
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
--verbose, -v Verbose output includes plugin descriptions.
Use twice for debugging.
--colour,--color=WHEN control whether colour is used. WHEN may be
`never', `always', or `auto'.
--quiet, -q Do not display brief logging to STDOUT.
--no-errors Suppress error messages.
LOGGING:
--log-brief=FILE Log brief, one-line output.
--log-verbose=FILE Log verbose output.
--log-errors=FILE Log errors.
--log-xml=FILE Log XML format.
--log-json=FILE Log JSON format.
--log-sql=FILE Log SQL INSERT statements.
--log-sql-create=FILE Create SQL database tables.
--log-json-verbose=FILE Log JSON Verbose format.
--log-magictree=FILE Log MagicTree XML format.
--log-object=FILE Log Ruby object inspection format.
--log-mongo-database Name of the MongoDB database.
--log-mongo-collection Name of the MongoDB collection.
Default: whatweb.
--log-mongo-host MongoDB hostname or IP address.
Default: 0.0.0.0.
--log-mongo-username MongoDB username. Default: nil.
--log-mongo-password MongoDB password. Default: nil.
--log-elastic-index Name of the index to store results. Default: whatweb
--log-elastic-host Host:port of the elastic http interface. Default: 127.0.0.1:9200
PERFORMANCE & STABILITY:
--max-threads, -t Number of simultaneous threads. Default: 25.
--open-timeout Time in seconds. Default: 15.
--read-timeout Time in seconds. Default: 30.
--wait=SECONDS Wait SECONDS between connections.
This is useful when using a single thread.
HELP & MISCELLANEOUS:
--short-help Short usage help.
--help, -h Complete usage help.
--debug Raise errors in plugins.
--version Display version information.

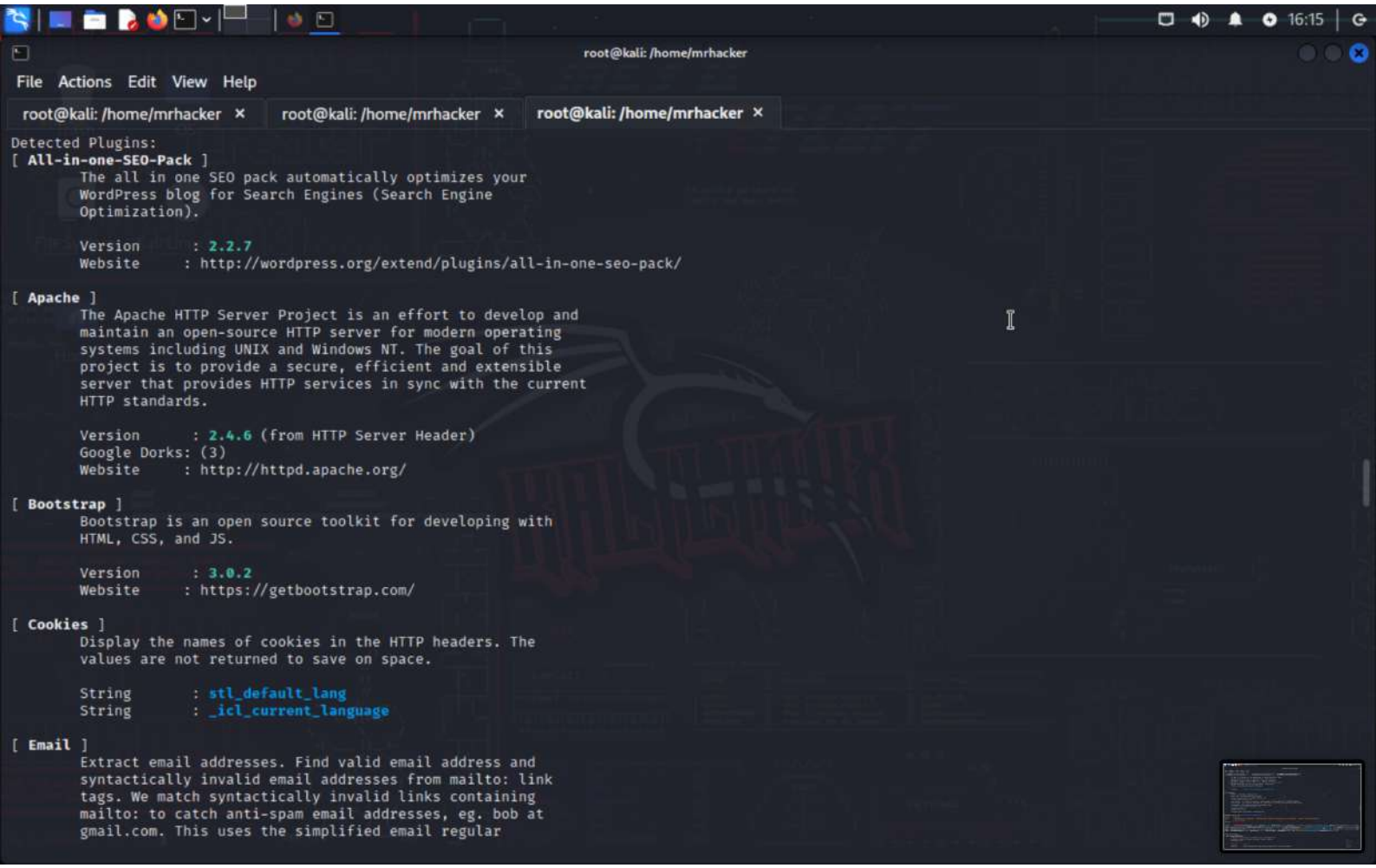

16:15
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
PERFORMANCE & STABILITY:
--max-threads, -t Number of simultaneous threads. Default: 25.
--open-timeout Time in seconds. Default: 15.
--read-timeout Time in seconds. Default: 30.
--wait=SECONDS Wait SECONDS between connections.
This is useful when using a single thread.
HELP & MISCELLANEOUS:
--short-help Short usage help.
--help, -h Complete usage help.
--debug Raise errors in plugins.
--version Display version information.
EXAMPLE USAGE:
* Scan example.com.
./whatweb example.com
* Scan reddit.com slashdot.org with verbose plugin descriptions.
./whatweb -v reddit.com slashdot.org
* An aggressive scan of wired.com detects the exact version of WordPress.
./whatweb -a 3 www.wired.com
* Scan the local network quickly and suppress errors.
whatweb --no-errors 192.168.0.0/24
* Scan the local network for https websites.
whatweb --no-errors --url-prefix https:// 192.168.0.0/24
* Scan for crossdomain policies in the Alexa Top 1000.
./whatweb -i plugin-development/alexa-top-100.txt \
--url-suffix /crossdomain.xml -p crossdomain_xml
(root@kali)-[/home/mrhacker]
whatweb arh.bg.ac.rs
http://arh.bg.ac.rs [301 Moved Permanently] Apache[2.4.6], Cookies[_icl_current_language,stl_default_lang], Country[Serbia][RS], HTTPServer[
.4.6 (CentOS) PHP/5.4.16], IP[147.91.19.26], PHP[5.4.16], RedirectLocation[http://www.arh.bg.ac.rs/], WPML-Plugin, X-Powered-By[PHP/5.4.16],
://www.arh.bg.ac.rs/xmlrpc.php]
http://www.arh.bg.ac.rs/ [200 OK] All-in-one-SEO-Pack[2.2.7], Apache[2.4.6], Bootstrap[3.0.2], Cookies[_icl_current_language,stl_default_lang

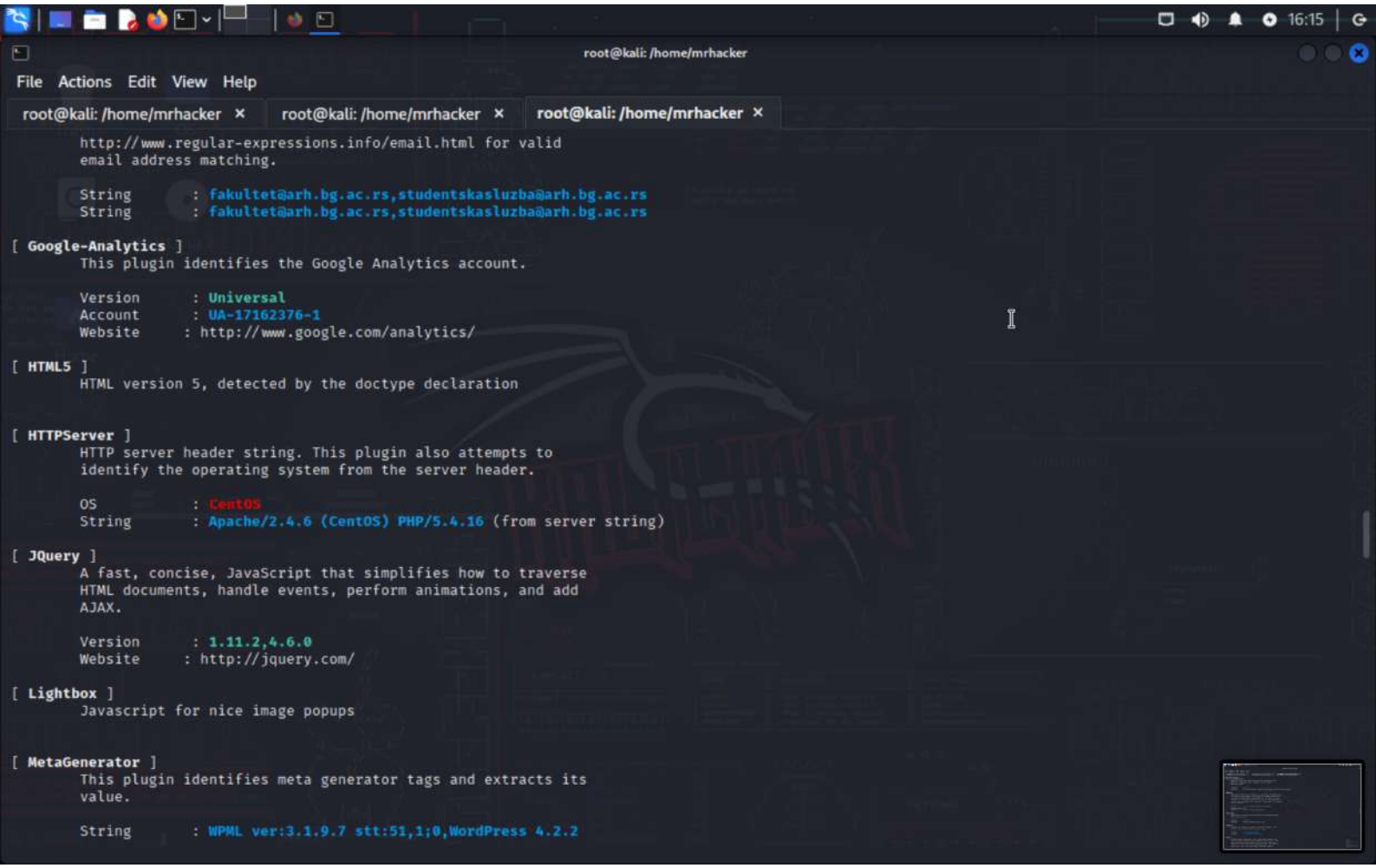

root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
* Scan for crossdomain policies in the Alexa Top 1000.
./whatweb -i plugin-development/alexa-top-100.txt \
--url-suffix /crossdomain.xml -p crossdomain_xml
(root@kali)-[/home/mrhacker]
whatweb arh.bg.ac.rs
http://arh.bg.ac.rs [301 Moved Permanently] Apache[2.4.6], Cookies[_icl_current_language,stl_default_lang], Country[Serbia][RS], HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], IP[147.91.19.26], PHP[5.4.16], RedirectLocation[http://www.arh.bg.ac.rs/], WPML-Plugin, X-Powered-By[PHP/5.4.16], x-pingback[http://www.arh.bg.ac.rs/xmlrpc.php]
http://www.arh.bg.ac.rs/ [200 OK] All-in-one-SEO-Pack[2.2.7], Apache[2.4.6], Bootstrap[3.0.2], Cookies[_icl_current_language,stl_default_lang], Country[Serbia][RS], Email[fakultet@arh.bg.ac.rs,studentskasluzba@arh.bg.ac.rs], Google-Analytics[Universal][UA-17162376-1], HTML5, HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], IP[147.91.19.26], JQuery[1.11.2,4.6.0], Lightbox, MetaGenerator[WPML ver:3.1.9.7 stt:51,1;0,WordPress 4.2.2], Open-Graph-Protocol[website][528244433933209], PHP[5.4.16], Script[text/javascript], ShareThis, Title[Univerzitet u Beogradu - Arhitektonski fakultet (University of Belgrade - Faculty of Architecture)], UncommonHeaders[link], WPML-Plugin, WordPress[4.2.2], X-Powered-By[PHP/5.4.16], x-pingback[http://www.arh.bg.ac.rs/xmlrpc.php]
(root@kali)-[/home/mrhacker]
whatweb arh.bg.ac.rs -v
WhatWeb report for http://arh.bg.ac.rs
Status : 301 Moved Permanently
Title : <None>
IP : 147.91.19.26
Country : Serbia, RS
Summary : Apache[2.4.6], Cookies[_icl_current_language,stl_default_lang], HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], PHP[5.4.16], RedirectLocation[http://www.arh.bg.ac.rs/], WPML-Plugin, x-pingback[http://www.arh.bg.ac.rs/xmlrpc.php], X-Powered-By[PHP/5.4.16]
Detected Plugins:
[Apache]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.
Version : 2.4.6 (from HTTP Server Header)
Google Dorks: (3)
Website : http://httpd.apache.org/
[Cookies]

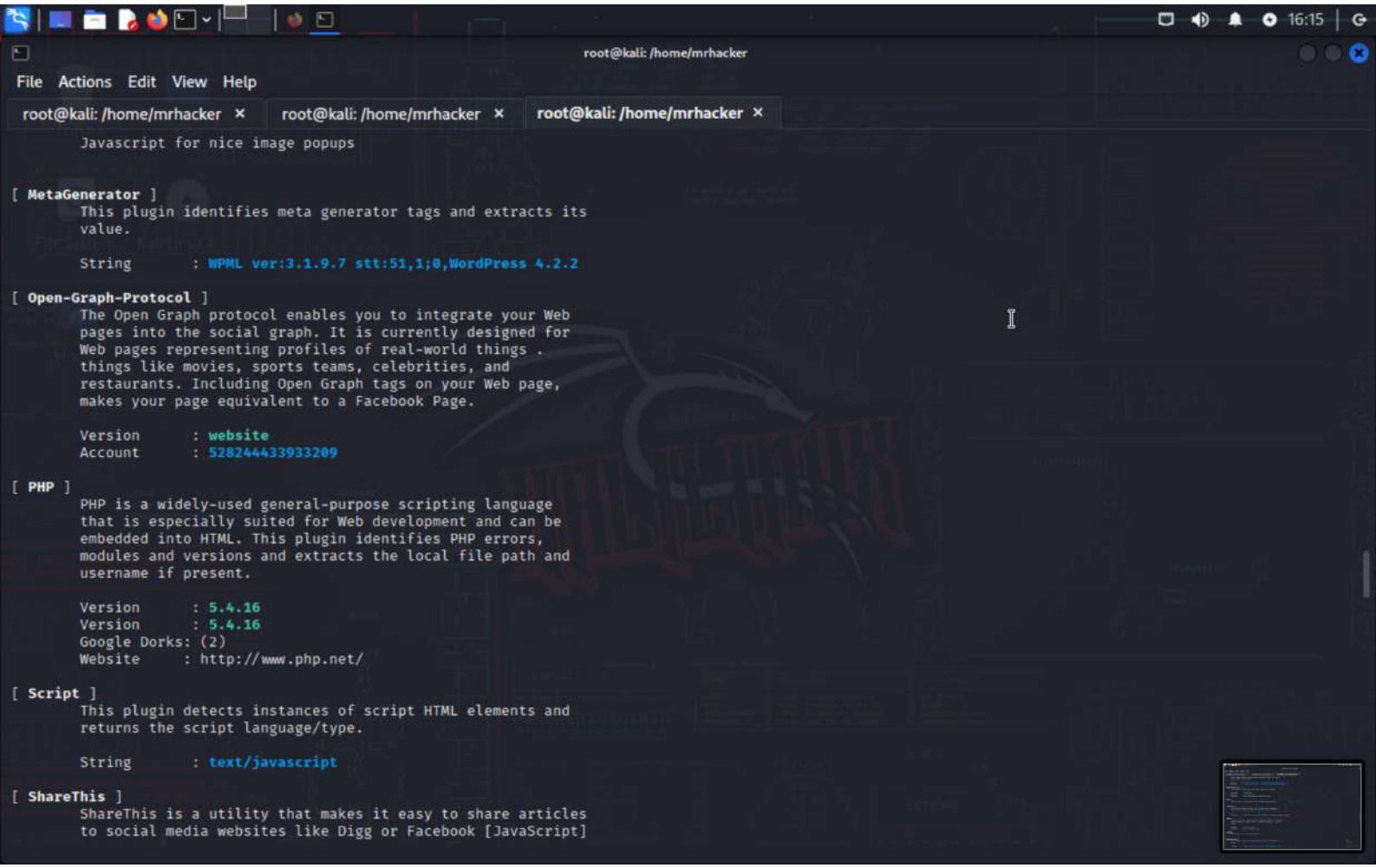

root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
Detected Plugins:
[Apache]
The Apache HTTP Server Project is an effort to develop and
maintain an open-source HTTP server for modern operating
systems including UNIX and Windows NT. The goal of this
project is to provide a secure, efficient and extensible
server that provides HTTP services in sync with the current
HTTP standards.
Version : 2.4.6 (from HTTP Server Header)
Google Dorks: (3)
Website : http://httpd.apache.org/
[Cookies]
Display the names of cookies in the HTTP headers. The
values are not returned to save on space.
String : stl_default_lang
String : _icl_current_language
[HTTPServer]
HTTP server header string. This plugin also attempts to
identify the operating system from the server header.
OS : CentOS
String : Apache/2.4.6 (CentOS) PHP/5.4.16 (from server string)
[PHP]
PHP is a widely-used general-purpose scripting language
that is especially suited for Web development and can be
embedded into HTML. This plugin identifies PHP errors,
modules and versions and extracts the local file path and
username if present.
Version : 5.4.16
Version : 5.4.16
Google Dorks: (2)
Website : http://www.php.net/
[RedirectLocation]
HTTP Server string location. used with http-status 301 and

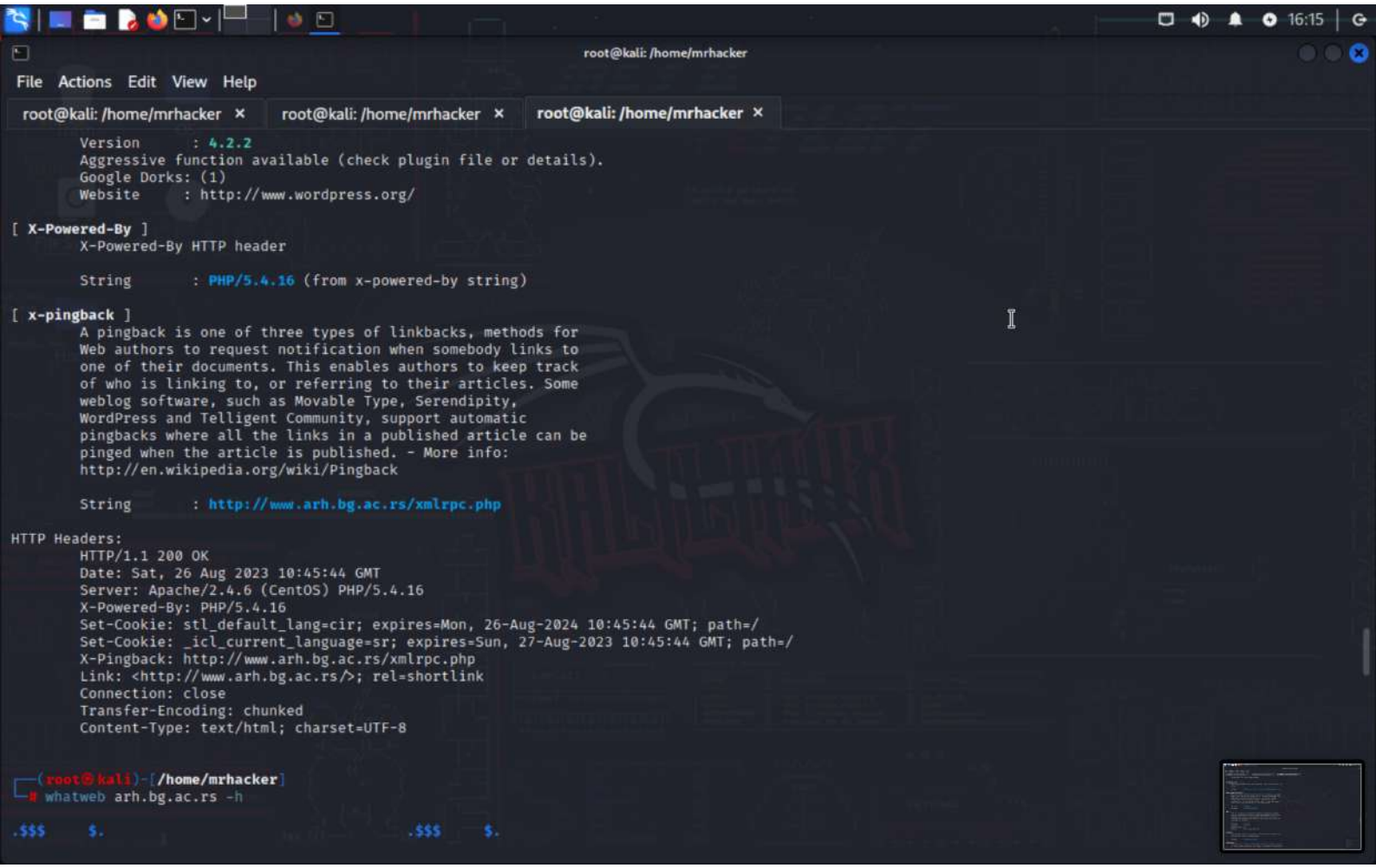

16:15
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
[PHP]
PHP is a widely-used general-purpose scripting language
that is especially suited for Web development and can be
embedded into HTML. This plugin identifies PHP errors,
modules and versions and extracts the local file path and
username if present.
Version : 5.4.16
Version : 5.4.16
Google Dorks: (2)
Website : http://www.php.net/
[RedirectLocation]
HTTP Server string location. used with http-status 301 and
302
String : http://www.arh.bg.ac.rs/ (from location)
[WPML-Plugin]
The WordPress Multilingual Plugin enables multilingual
websites
Website : https://wpml.org/
[X-Powered-By]
X-Powered-By HTTP header
String : PHP/5.4.16 (from x-powered-by string)
[x-pingback]
A pingback is one of three types of linkbacks, methods for
Web authors to request notification when somebody links to
one of their documents. This enables authors to keep track
of who is linking to, or referring to their articles. Some
weblog software, such as Movable Type, Serendipity,
WordPress and Telligent Community, support automatic
pingbacks where all the links in a published article can be
pinged when the article is published. - More info:
http://en.wikipedia.org/wiki/Pingback
String : http://www.arh.bg.ac.rs/xmlrpc.php

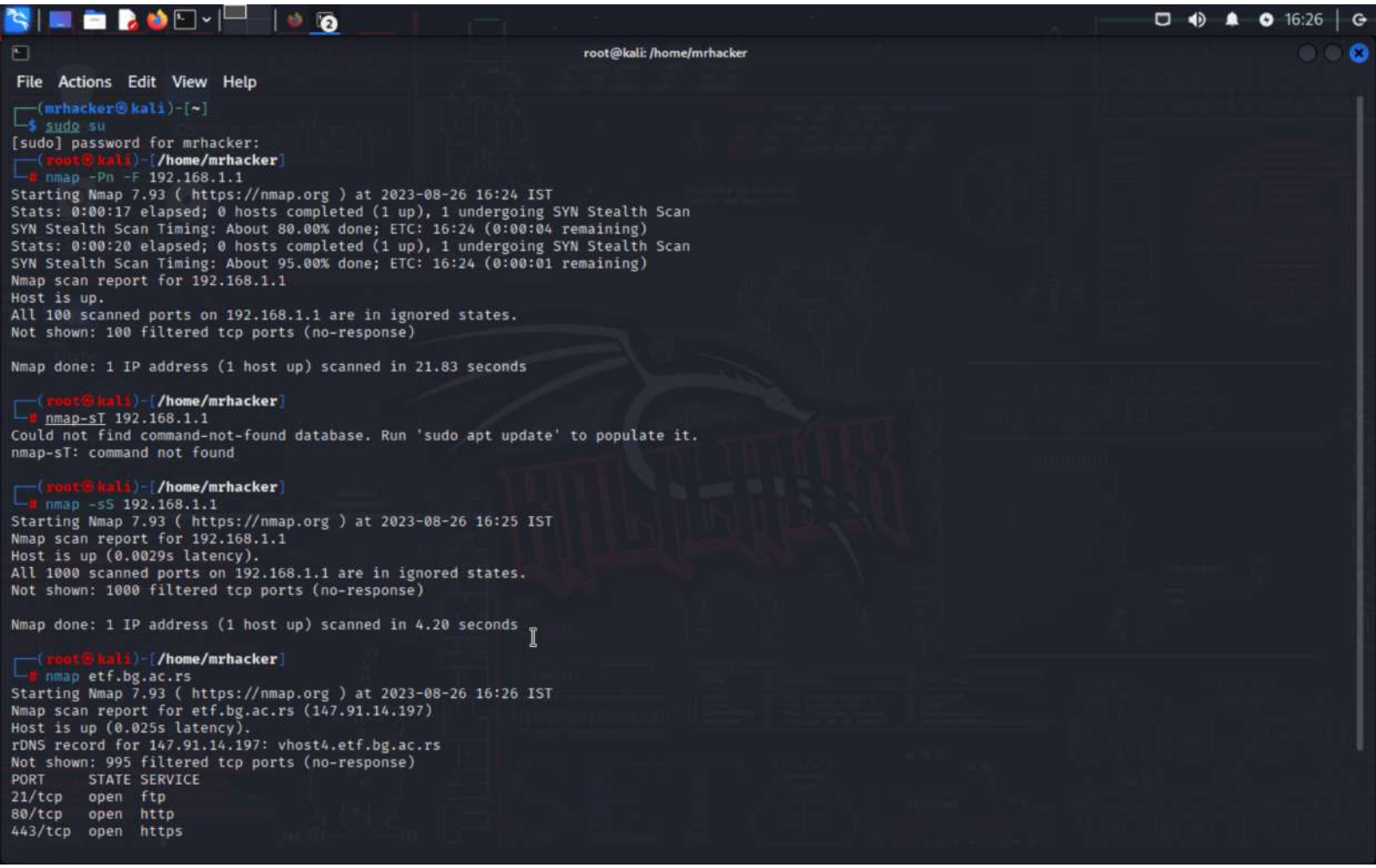

16:15
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
of who is linking to, or referring to their articles. Some
weblog software, such as Movable Type, Serendipity,
WordPress and Telligent Community, support automatic
pingbacks where all the links in a published article can be
pinged when the article is published. - More info:
http://en.wikipedia.org/wiki/Pingback
String : http://www.arh.bg.ac.rs/xmlrpc.php
HTTP Headers:
HTTP/1.1 301 Moved Permanently
Date: Sat, 26 Aug 2023 10:45:42 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Set-Cookie: stl_default_lang=cir; expires=Mon, 26-Aug-2024 10:45:42 GMT; path=/
Set-Cookie: _icl_current_language=sr; expires=Sun, 27-Aug-2023 10:45:42 GMT; path=/
X-Pingback: http://www.arh.bg.ac.rs/xmlrpc.php
Location: http://www.arh.bg.ac.rs/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
WhatWeb report for http://www.arh.bg.ac.rs/
Status : 200 OK
Title : Univerzitet u Beogradu - Arhitektonski fakultet (University of Belgrade - Faculty of Architecture)
IP : 147.91.19.26
Country : Serbia, RS
Summary : All-in-one-SEO-Pack[2.2.7], Apache[2.4.6], Bootstrap[3.0.2], Cookies[_icl_current_language,stl_default_lang], Email[fakultet@arh.bg.ac.rs,studentskasluzba@arh.bg.ac.rs], Google-Analytics[Universal][UA-17162376-1], HTML5, HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], JQuery[1.11.2,4.6.0], Lightbox, MetaGenerator[WPML ver:3.1.9.7 stt:51,1;0,WordPress 4.2.2], Open-Graph-Protocol[website][528244433933209], PHP[5.4.16], Script[text/javascript], ShareThis, UncommonHeaders[link], WordPress[4.2.2], WPML-Plugin, x-pingback[http://www.arh.bg.ac.rs/xmlrpc.php], X-Powered-By[PHP/5.4.16]
Detected Plugins:
[All-in-one-SEO-Pack]
The all in one SEO pack automatically optimizes your
WordPress blog for Search Engines (Search Engine
Optimization).
Version : 2.2.7
Website : http://wordpress.org/extend/plugins/all-in-one-seo-pack/

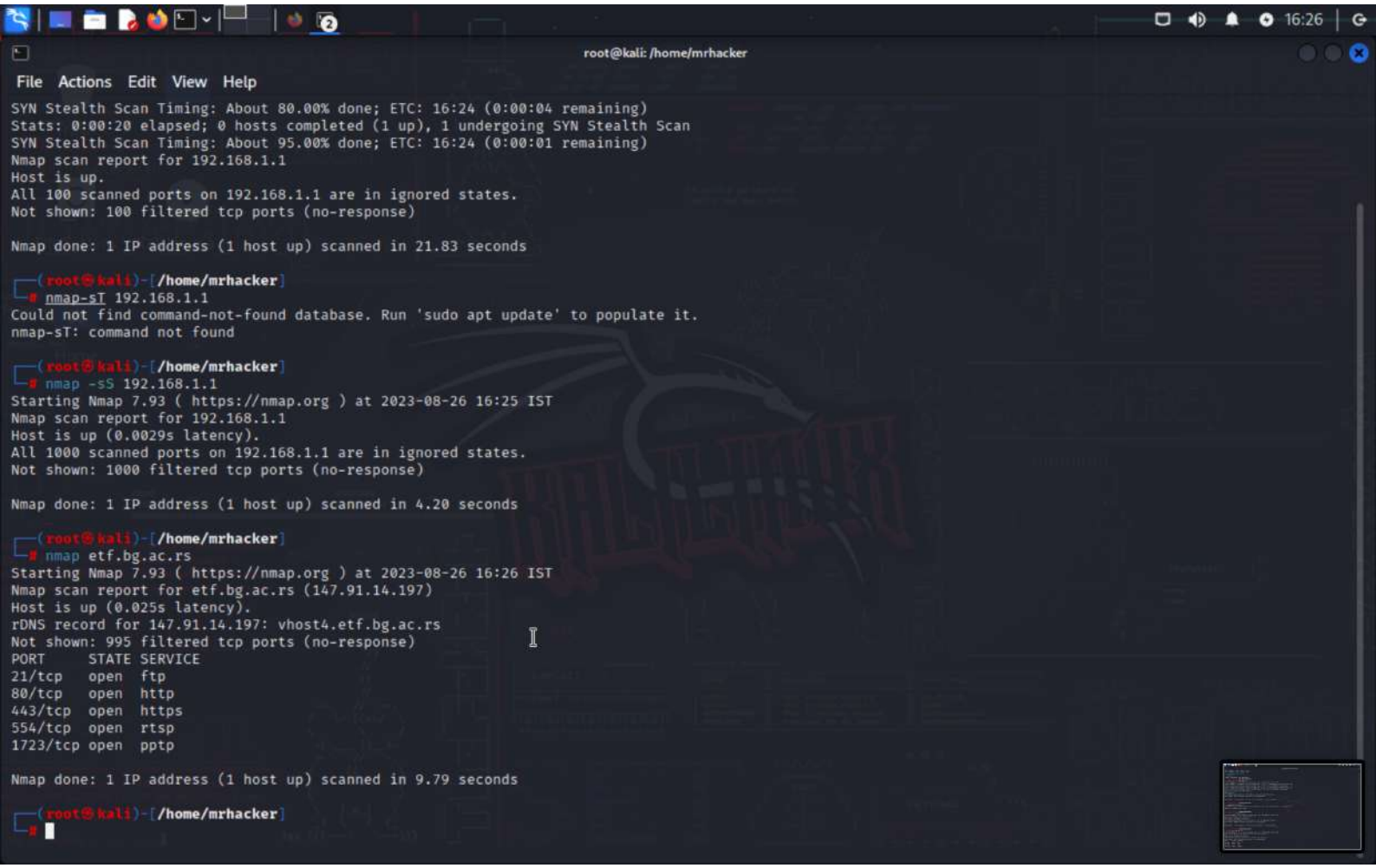

16:15
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
Detected Plugins:
[All-in-one-SEO-Pack]
The all in one SEO pack automatically optimizes your
WordPress blog for Search Engines (Search Engine
Optimization).
Version : 2.2.7
Website : http://wordpress.org/extend/plugins/all-in-one-seo-pack/
[Apache]
The Apache HTTP Server Project is an effort to develop and
maintain an open-source HTTP server for modern operating
systems including UNIX and Windows NT. The goal of this
project is to provide a secure, efficient and extensible
server that provides HTTP services in sync with the current
HTTP standards.
Version : 2.4.6 (from HTTP Server Header)
Google Dorks: (3)
Website : http://httpd.apache.org/
[Bootstrap]
Bootstrap is an open source toolkit for developing with
HTML, CSS, and JS.
Version : 3.0.2
Website : https://getbootstrap.com/
[Cookies]
Display the names of cookies in the HTTP headers. The
values are not returned to save on space.
String : stl_default_lang
String : _icl_current_language
[Email]
Extract email addresses. Find valid email address and
syntactically invalid email addresses from mailto: link
tags. We match syntactically invalid links containing
mailto: to catch anti-spam email addresses, eg. bob at
gmail.com. This uses the simplified email regular

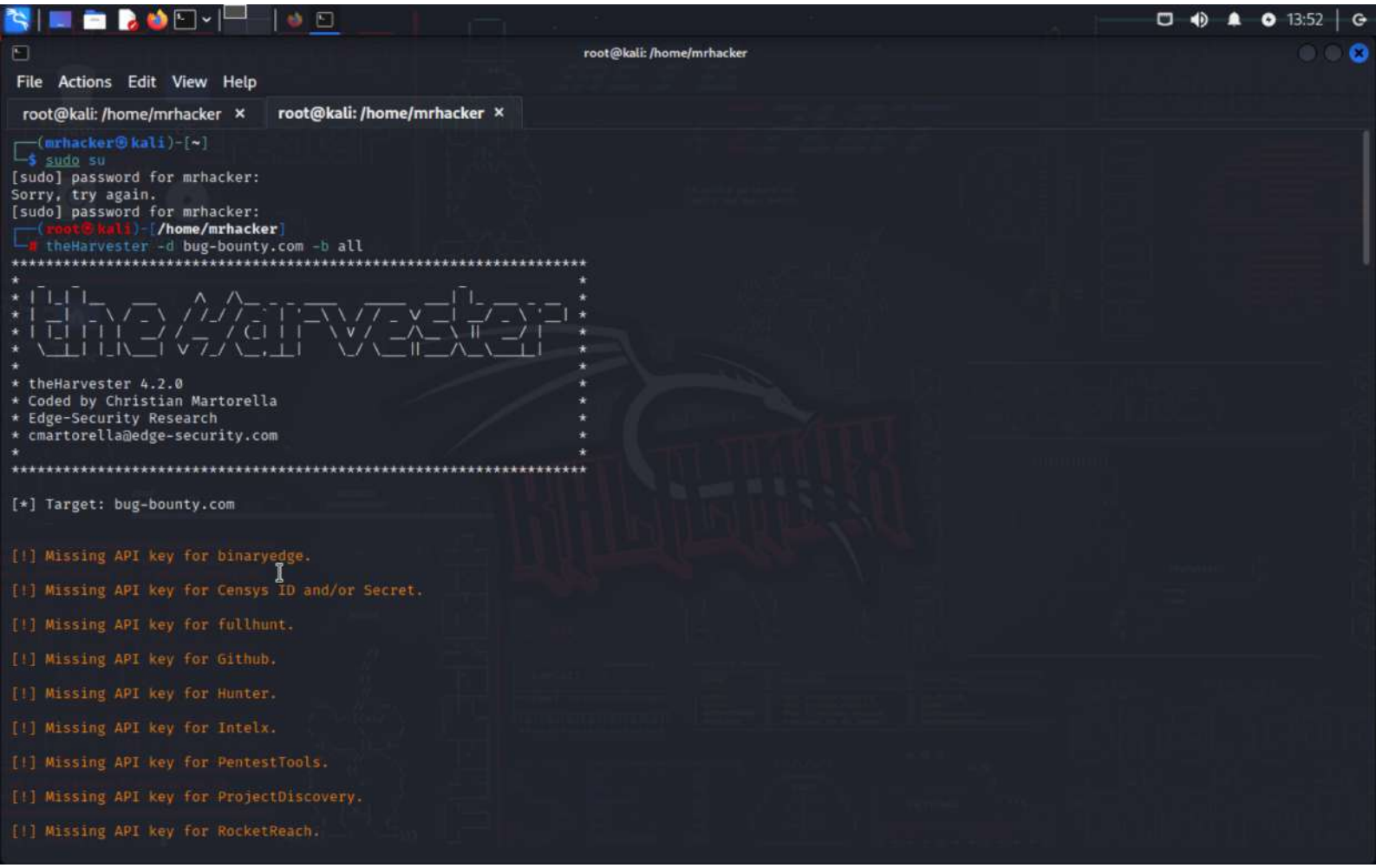

16:15
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
http://www.regular-expressions.info/email.html for valid
email address matching.
String : fakultet@arh.bg.ac.rs,studentskasluzba@arh.bg.ac.rs
String : fakultet@arh.bg.ac.rs,studentskasluzba@arh.bg.ac.rs
[Google-Analytics]
This plugin identifies the Google Analytics account.
Version : Universal
Account : UA-17162376-1
Website : http://www.google.com/analytics/
[HTML5]
HTML version 5, detected by the doctype declaration
[HTTPServer]
HTTP server header string. This plugin also attempts to
identify the operating system from the server header.
OS : CentOS
String : Apache/2.4.6 (CentOS) PHP/5.4.16 (from server string)
[JQuery]
A fast, concise, JavaScript that simplifies how to traverse
HTML documents, handle events, perform animations, and add
AJAX.
Version : 1.11.2,4.6.0
Website : http://jquery.com/
[Lightbox]
Javascript for nice image popups
[MetaGenerator]
This plugin identifies meta generator tags and extracts its
value.
String : WPML ver:3.1.9.7 stt:51,1;0,WordPress 4.2.2

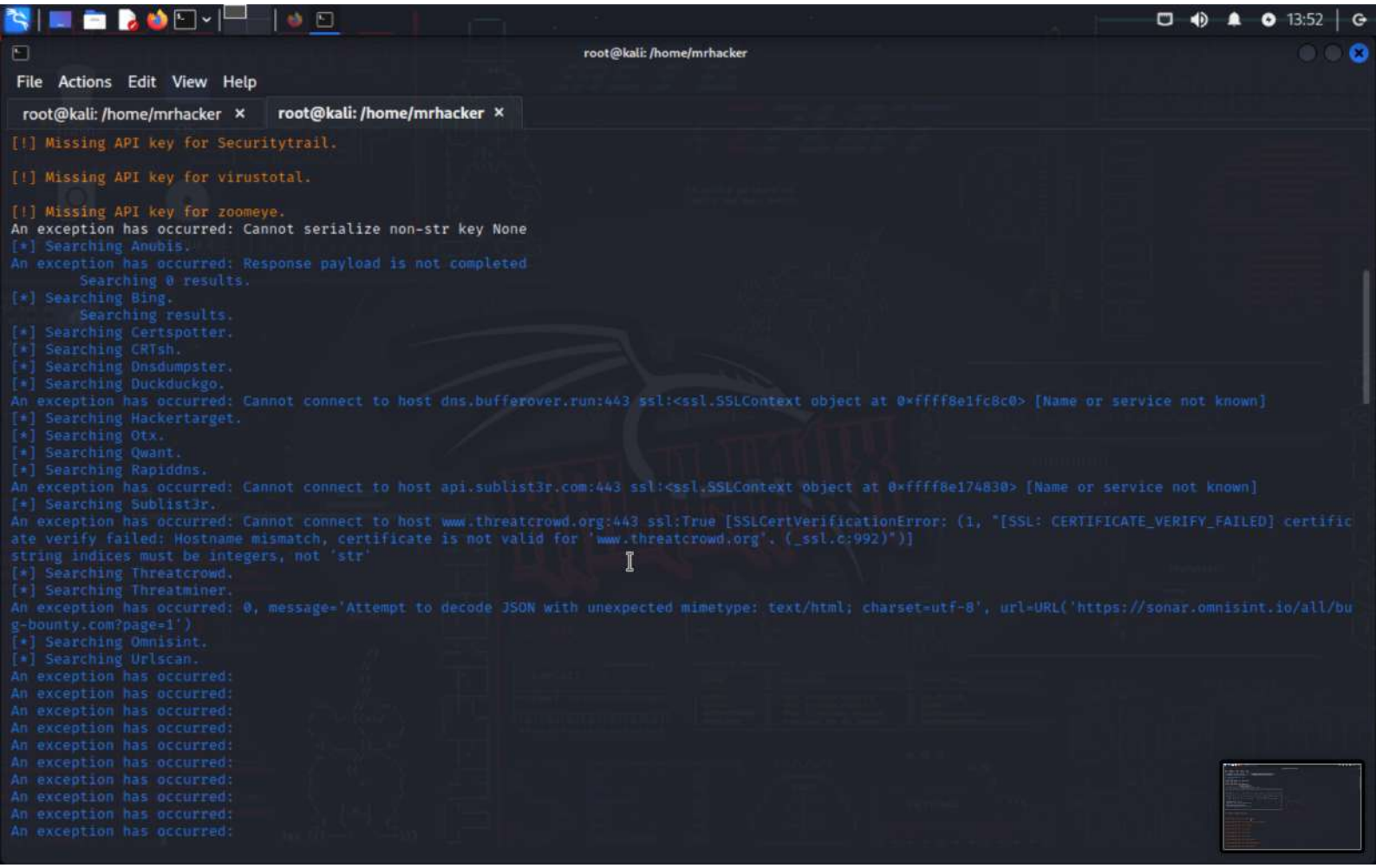

root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
Javascript for nice image popups
[MetaGenerator]
This plugin identifies meta generator tags and extracts its value.
String : WPML ver:3.1.9.7 stt:51,1;0,WordPress 4.2.2
[Open-Graph-Protocol]
The Open Graph protocol enables you to integrate your Web pages into the social graph. It is currently designed for Web pages representing profiles of real-world things . things like movies, sports teams, celebrities, and restaurants. Including Open Graph tags on your Web page, makes your page equivalent to a Facebook Page.
Version : website
Account : 528244433933209
[PHP]
PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. This plugin identifies PHP errors, modules and versions and extracts the local file path and username if present.
Version : 5.4.16
Version : 5.4.16
Google Dorks: (2)
Website : http://www.php.net/
[Script]
This plugin detects instances of script HTML elements and returns the script language/type.
String : text/javascript
[ShareThis]
ShareThis is a utility that makes it easy to share articles to social media websites like Digg or Facebook [JavaScript]

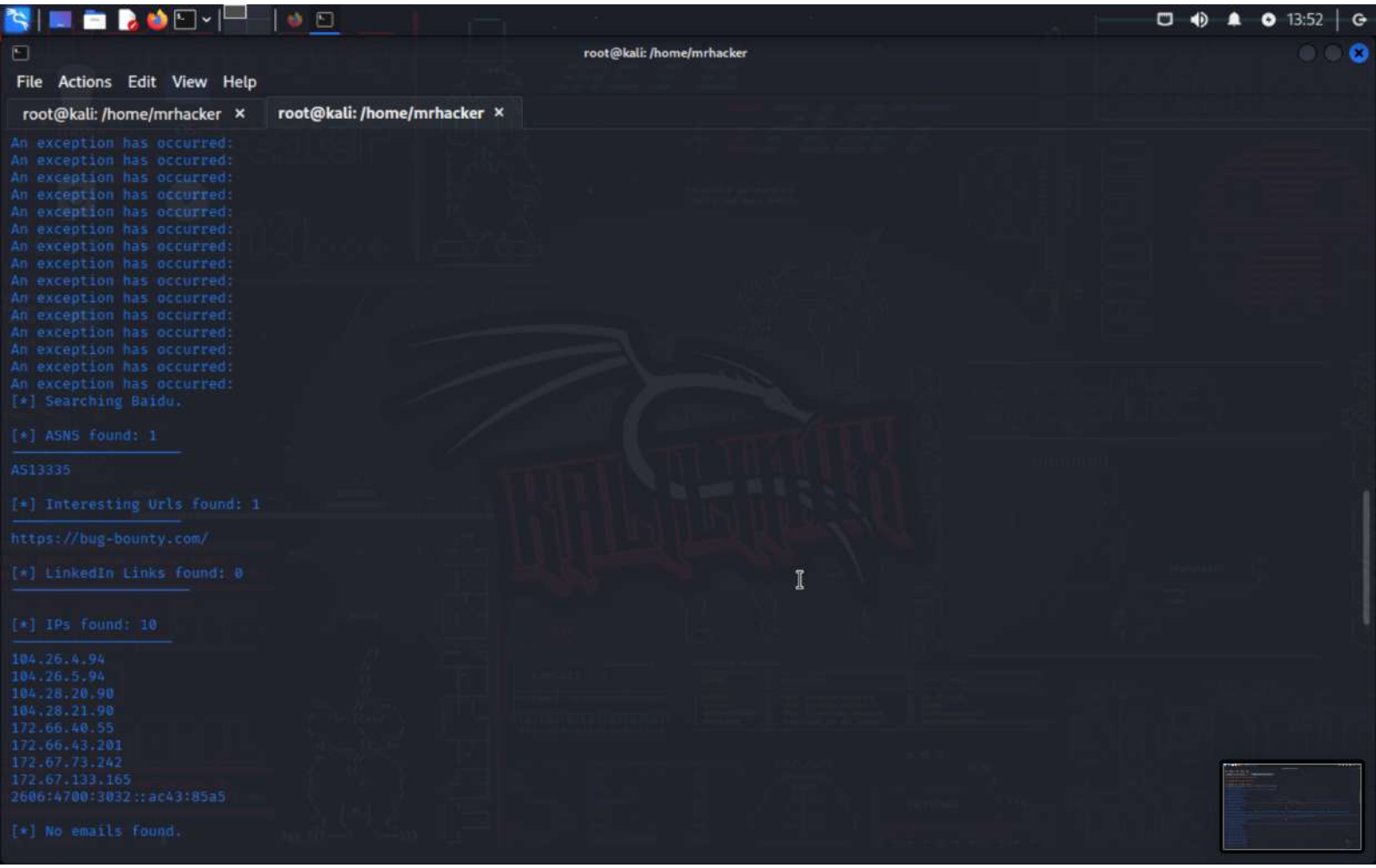

root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
root@kali: /home/mrhacker
Version : 4.2.2
Aggressive function available (check plugin file or details).
Google Dorks: (1)
Website : http://www.wordpress.org/
[X-Powered-By]
X-Powered-By HTTP header
String : PHP/5.4.16 (from x-powered-by string)
[x-pingback]
A pingback is one of three types of linkbacks, methods for
Web authors to request notification when somebody links to
one of their documents. This enables authors to keep track
of who is linking to, or referring to their articles. Some
weblog software, such as Movable Type, Serendipity,
WordPress and Telligent Community, support automatic
pingbacks where all the links in a published article can be
pinged when the article is published. - More info:
http://en.wikipedia.org/wiki/Pingback
String : http://www.arh.bg.ac.rs/xmlrpc.php
HTTP Headers:
HTTP/1.1 200 OK
Date: Sat, 26 Aug 2023 10:45:44 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Set-Cookie: stl_default_lang=cir; expires=Mon, 26-Aug-2024 10:45:44 GMT; path=/
Set-Cookie: _icl_current_language=sr; expires=Sun, 27-Aug-2023 10:45:44 GMT; path=/
X-Pingback: http://www.arh.bg.ac.rs/xmlrpc.php
Link: <http://www.arh.bg.ac.rs/>; rel=shortlink
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
(root@kali)-[/home/mrhacker]
whatweb arh.bg.ac.rs -h
.$$$ $. .$$$ $.

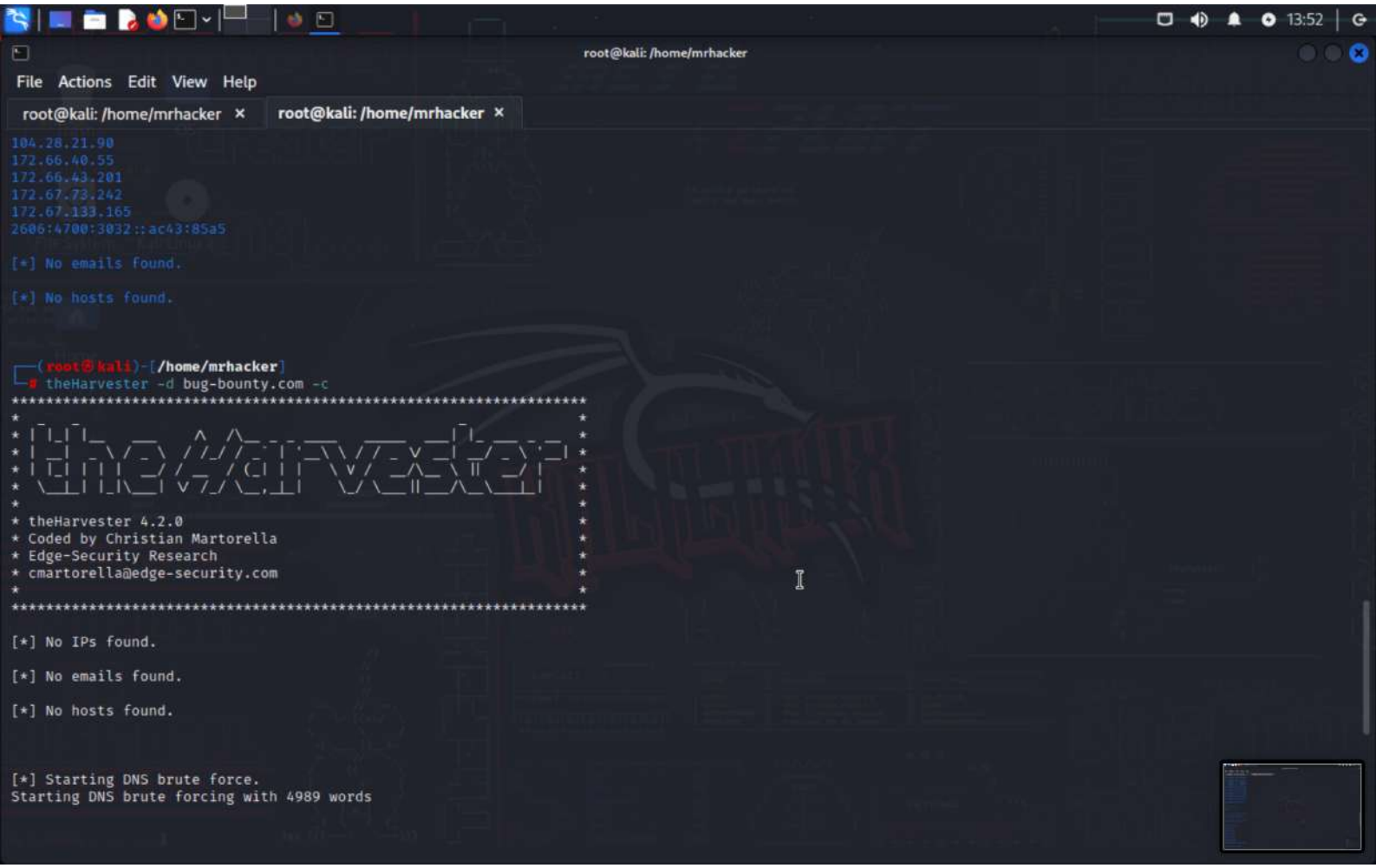

16:26
root@kali: /home/mrhacker
File Actions Edit View Help
(mrhacker㉿kali)-[~]
$ sudo su
[sudo] password for mrhacker:
(root㉿kali)-[/home/mrhacker]
nmap -Pn -F 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-08-26 16:24 IST
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.00% done; ETC: 16:24 (0:00:04 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.00% done; ETC: 16:24 (0:00:01 remaining)
Nmap scan report for 192.168.1.1
Host is up.
All 100 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 21.83 seconds
(root㉿kali)-[/home/mrhacker]
nmap-sT 192.168.1.1
Could not find command-not-found database. Run 'sudo apt update' to populate it.
nmap-sT: command not found
(root㉿kali)-[/home/mrhacker]
nmap -sS 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-08-26 16:25 IST
Nmap scan report for 192.168.1.1
Host is up (0.0029s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
(root㉿kali)-[/home/mrhacker]
nmap etf.bg.ac.rs
Starting Nmap 7.93 (https://nmap.org) at 2023-08-26 16:26 IST
Nmap scan report for etf.bg.ac.rs (147.91.14.197)
Host is up (0.025s latency).
rDNS record for 147.91.14.197: vhost4.etf.bg.ac.rs
Not shown: 995 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https

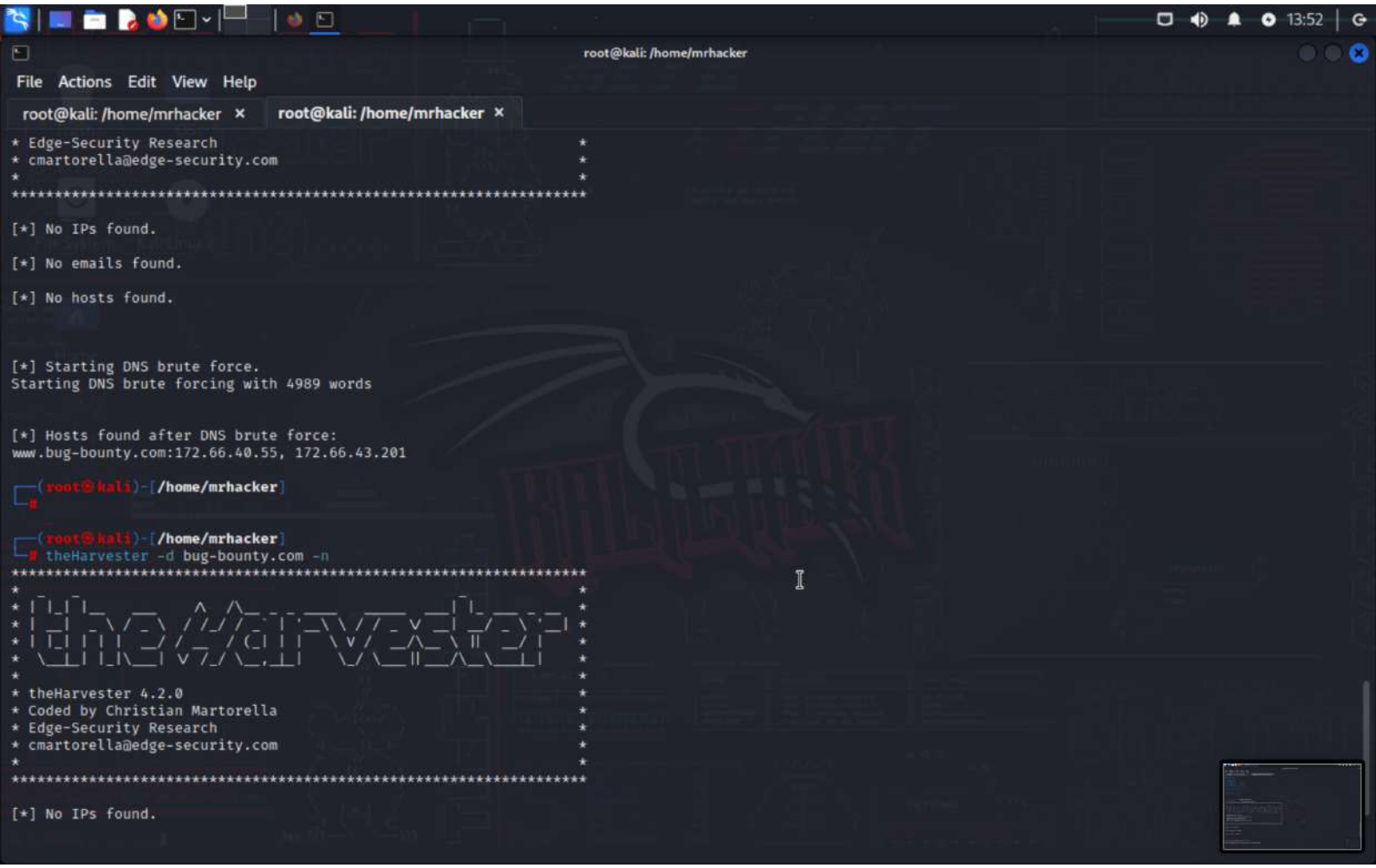

16:26
root@kali: /home/mrhacker
File Actions Edit View Help
SYN Stealth Scan Timing: About 80.00% done; ETC: 16:24 (0:00:04 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.00% done; ETC: 16:24 (0:00:01 remaining)
Nmap scan report for 192.168.1.1
Host is up.
All 100 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 21.83 seconds
┌──(root㉿kali)-[/home/mrhacker]
└─# nmap-sT 192.168.1.1
Could not find command-not-found database. Run 'sudo apt update' to populate it.
nmap-sT: command not found
┌──(root㉿kali)-[/home/mrhacker]
└─# nmap -sS 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-08-26 16:25 IST
Nmap scan report for 192.168.1.1
Host is up (0.0029s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
┌──(root㉿kali)-[/home/mrhacker]
└─# nmap etf.bg.ac.rs
Starting Nmap 7.93 (https://nmap.org) at 2023-08-26 16:26 IST
Nmap scan report for etf.bg.ac.rs (147.91.14.197)
Host is up (0.025s latency).
rDNS record for 147.91.14.197: vhost4.etf.bg.ac.rs
Not shown: 995 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
443/tcp open https
554/tcp open rtsp
1723/tcp open pptp
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
┌──(root㉿kali)-[/home/mrhacker]
└─#

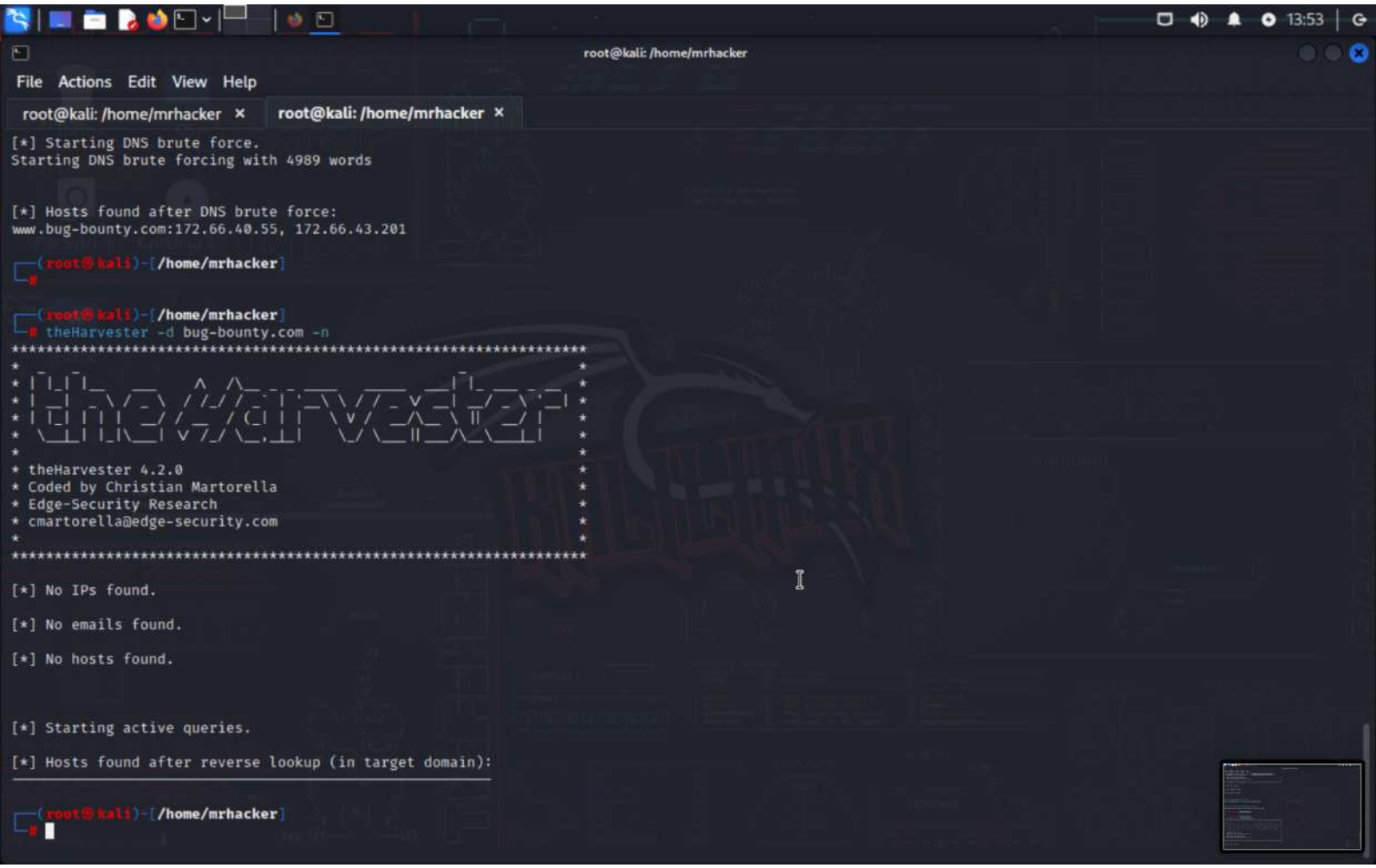

13:52
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
(mrhacker㉿kali)-[~]
$ sudo su
[sudo] password for mrhacker:
Sorry, try again.
[sudo] password for mrhacker:
(root㉿kali)-[/home/mrhacker]
theHarvester -d bug-bounty.com -b all
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: bug-bounty.com
[!] Missing API key for binaryedge.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for fullhunt.
[!] Missing API key for Github.
[!] Missing API key for Hunter.
[!] Missing API key for Intelx.
[!] Missing API key for PentestTools.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for RocketReach.

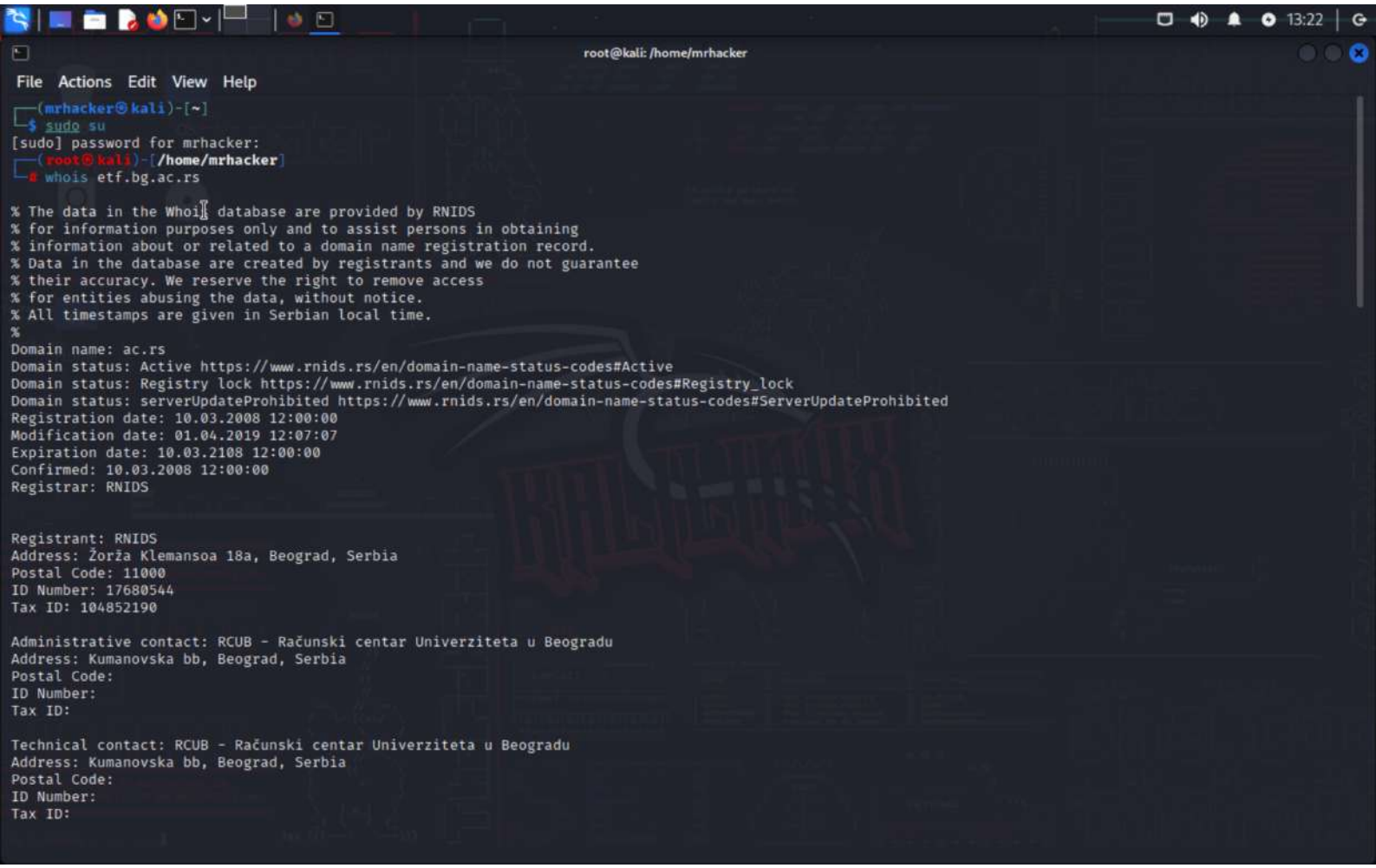

13:52
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
[!] Missing API key for Securitytrail.
[!] Missing API key for virustotal.
[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
[*] Searching Anubis.
An exception has occurred: Response payload is not completed
Searching 0 results.
[*] Searching Bing.
Searching results.
[*] Searching Certspotter.
[*] Searching CRTsh.
[*] Searching Dnsdumpster.
[*] Searching Duckduckgo.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0xffff8e1fc8c0> [Name or service not known]
[*] Searching Hackertarget.
[*] Searching Otx.
[*] Searching Qwant.
[*] Searching Rapiddns.
An exception has occurred: Cannot connect to host api.sublist3r.com:443 ssl:<ssl.SSLContext object at 0xffff8e174830> [Name or service not known]
[*] Searching Sublist3r.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certific
ate verify failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:992)")]
string indices must be integers, not 'str'
[*] Searching Threatcrowd.
[*] Searching Threatminer.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/bu
g-bounty.com?page=1')
[*] Searching Omnisint.
[*] Searching Urlscan.
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:

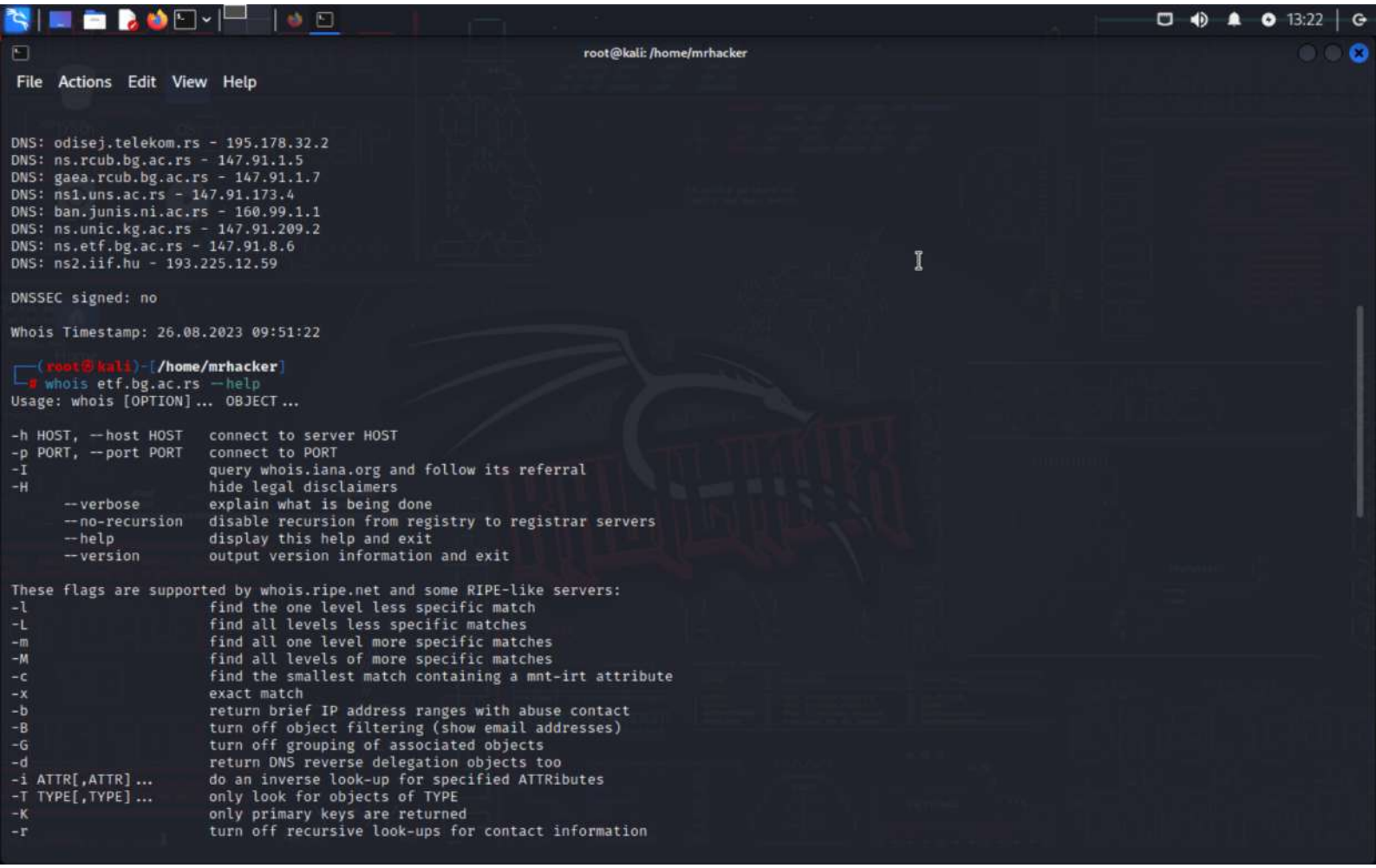

13:52
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
[*] Searching Baidu.
[*] ASNS found: 1
AS13335
[*] Interesting Urls found: 1
https://bug-bounty.com/
[*] LinkedIn Links found: 0
[*] IPs found: 10
104.26.4.94
104.26.5.94
104.28.20.90
104.28.21.90
172.66.40.55
172.66.43.201
172.67.73.242
172.67.133.165
2606:4700:3032::ac43:85a5
[*] No emails found.

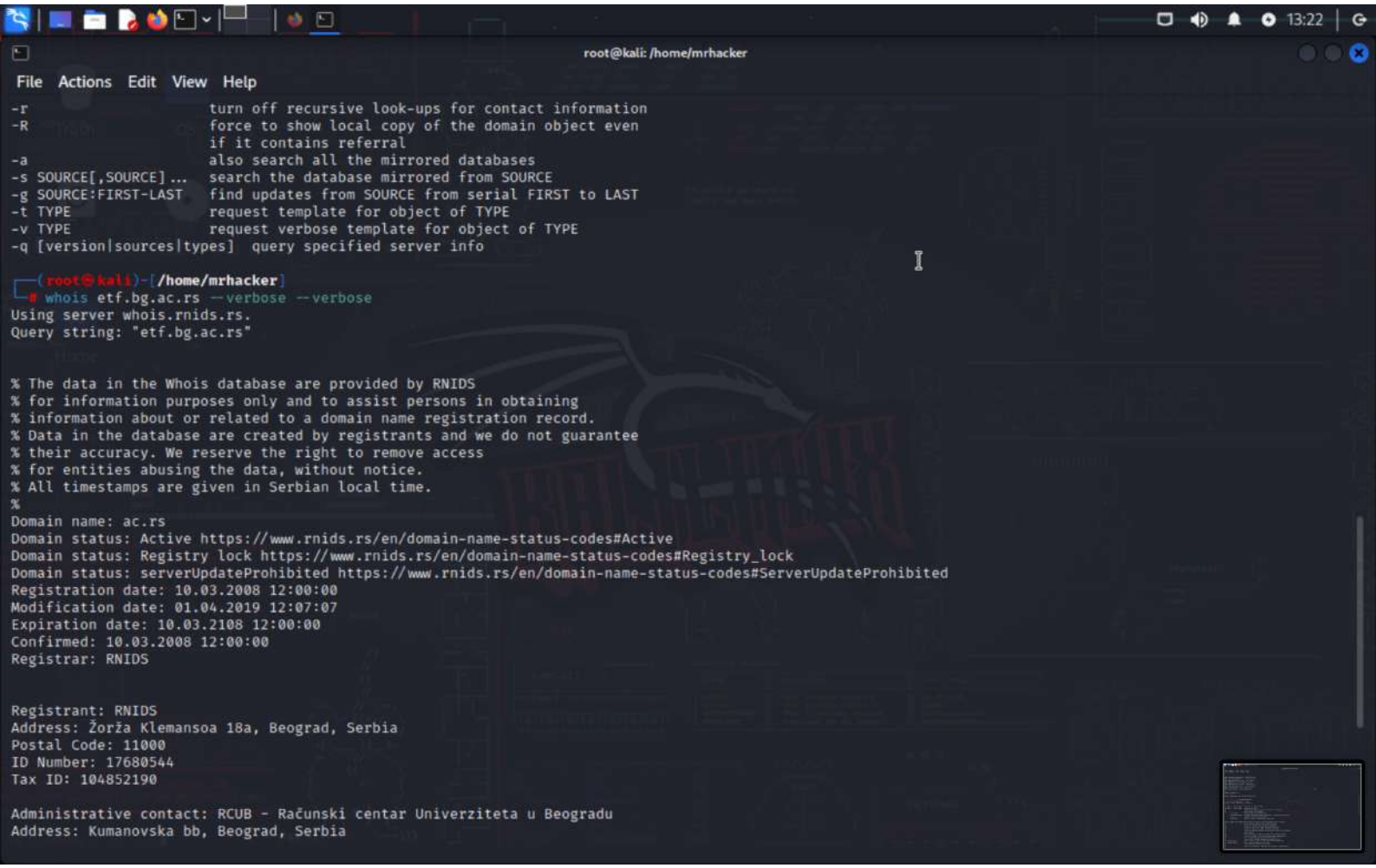

13:52
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker
root@kali: /home/mrhacker
104.28.21.90
172.66.40.55
172.66.43.201
172.67.73.242
172.67.133.165
2606:4700:3032::ac43:85a5
[*] No emails found.
[*] No hosts found.
(root@kali)-[/home/mrhacker]
theHarvester -d bug-bounty.com -c
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] No IPs found.
[*] No emails found.
[*] No hosts found.
[*] Starting DNS brute force.
Starting DNS brute forcing with 4989 words

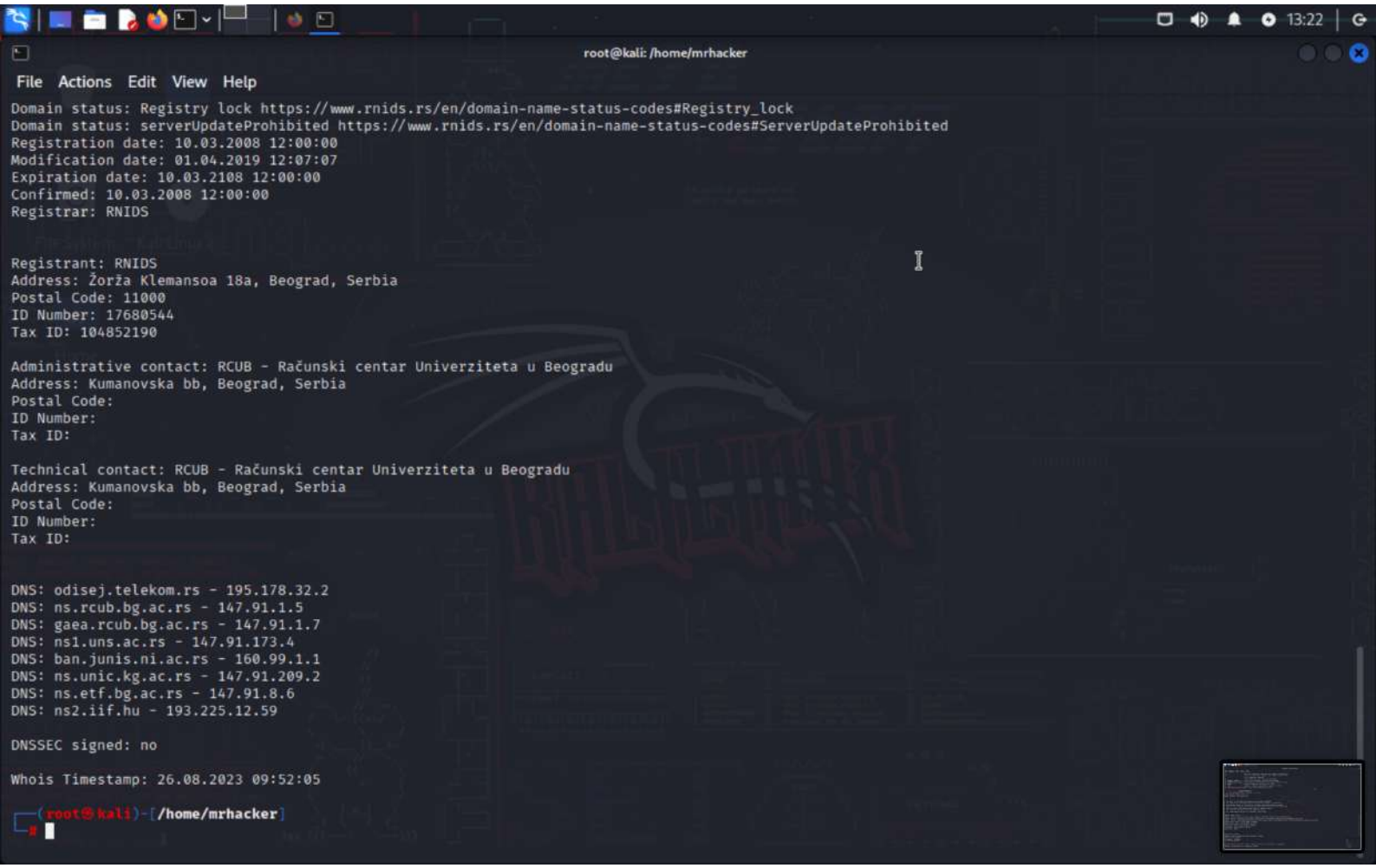

13:52
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
* Edge-Security Research *
* cmartorella@edge-security.com *
[*] No IPs found.
[*] No emails found.
[*] No hosts found.
[*] Starting DNS brute force.
Starting DNS brute forcing with 4989 words
[*] Hosts found after DNS brute force:
www.bug-bounty.com:172.66.40.55, 172.66.43.201
(root@kali)-[/home/mrhacker]
(root@kali)-[/home/mrhacker]
theHarvester -d bug-bounty.com -n
* theHarvester 4.2.0 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
[*] No IPs found.

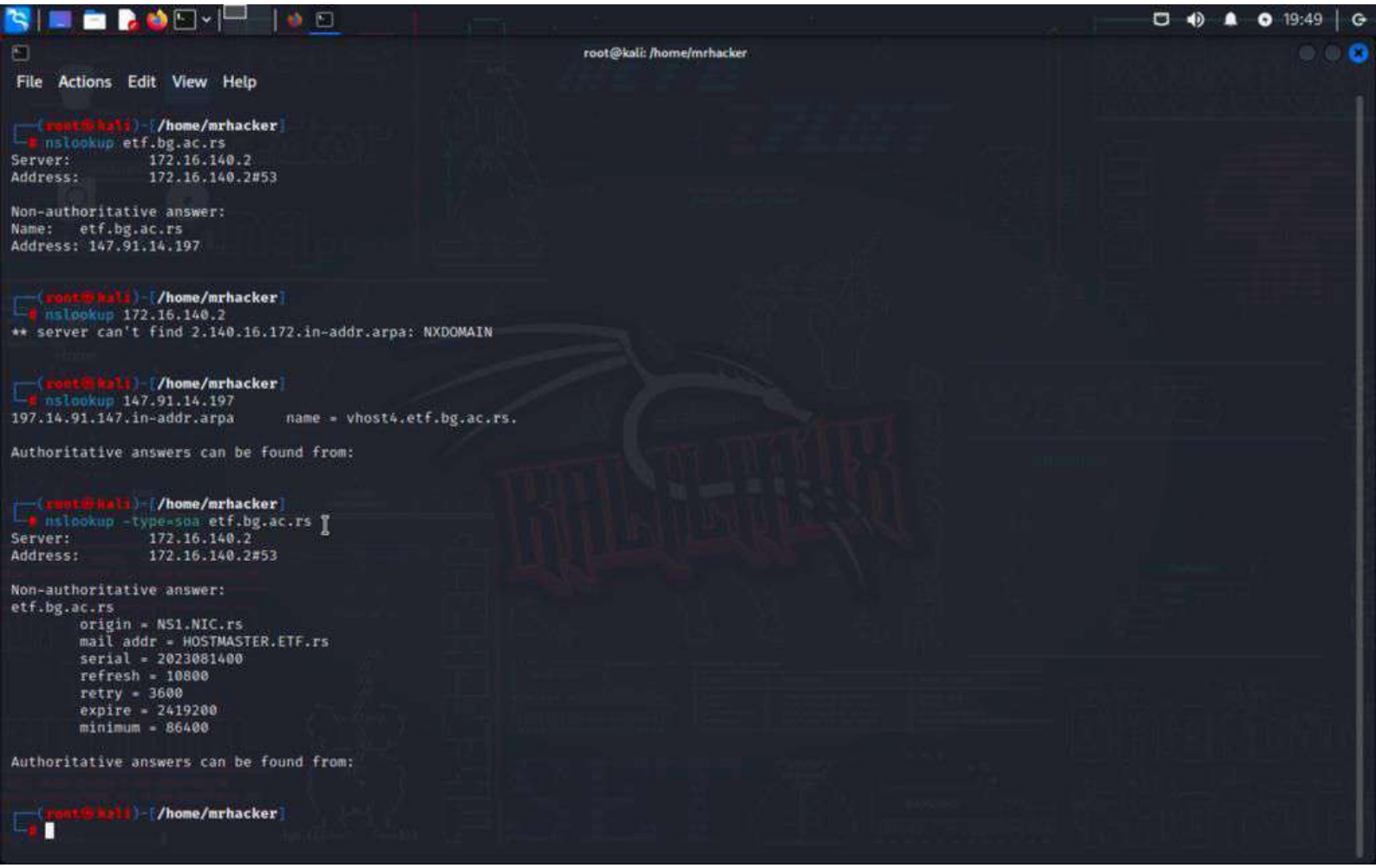

13:53
root@kali: /home/mrhacker
File Actions Edit View Help
root@kali: /home/mrhacker ×
root@kali: /home/mrhacker ×
[*] Starting DNS brute force.
Starting DNS brute forcing with 4989 words
[*] Hosts found after DNS brute force:
www.bug-bounty.com:172.66.40.55, 172.66.43.201
(root@kali)-[/home/mrhacker]
#
(root@kali)-[/home/mrhacker]
theHarvester -d bug-bounty.com -n
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] No IPs found.
[*] No emails found.
[*] No hosts found.
[*] Starting active queries.
[*] Hosts found after reverse lookup (in target domain):
(root@kali)-[/home/mrhacker]
#


13:22
root@kali: /home/mrhacker
File Actions Edit View Help
(mrhacker㉿kali)-[~]
$ sudo su
[sudo] password for mrhacker:
(root㉿kali)-[/home/mrhacker]
whois etf.bg.ac.rs
% The data in the Whois database are provided by RNIDS
% for information purposes only and to assist persons in obtaining
% information about or related to a domain name registration record.
% Data in the database are created by registrants and we do not guarantee
% their accuracy. We reserve the right to remove access
% for entities abusing the data, without notice.
% All timestamps are given in Serbian local time.
%
Domain name: ac.rs
Domain status: Active https://www.rnids.rs/en/domain-name-status-codes#Active
Domain status: Registry lock https://www.rnids.rs/en/domain-name-status-codes#Registry_lock
Domain status: serverUpdateProhibited https://www.rnids.rs/en/domain-name-status-codes#ServerUpdateProhibited
Registration date: 10.03.2008 12:00:00
Modification date: 01.04.2019 12:07:07
Expiration date: 10.03.2108 12:00:00
Confirmed: 10.03.2008 12:00:00
Registrar: RNIDS
Registrant: RNIDS
Address: Žorža Klemansoa 18a, Beograd, Serbia
Postal Code: 11000
ID Number: 17680544
Tax ID: 104852190
Administrative contact: RCUB - Računski centar Univerziteta u Beogradu
Address: Kumanovska bb, Beograd, Serbia
Postal Code:
ID Number:
Tax ID:
Technical contact: RCUB - Računski centar Univerziteta u Beogradu
Address: Kumanovska bb, Beograd, Serbia
Postal Code:
ID Number:
Tax ID:


13:22
root@kali: /home/mrhacker
File Actions Edit View Help
DNS: odisej.telekom.rs - 195.178.32.2
DNS: ns.rcub.bg.ac.rs - 147.91.1.5
DNS: gaea.rcub.bg.ac.rs - 147.91.1.7
DNS: ns1.uns.ac.rs - 147.91.173.4
DNS: ban.junis.ni.ac.rs - 160.99.1.1
DNS: ns.unic.kg.ac.rs - 147.91.209.2
DNS: ns.etf.bg.ac.rs - 147.91.8.6
DNS: ns2.iif.hu - 193.225.12.59
DNSSEC signed: no
Whois Timestamp: 26.08.2023 09:51:22
(root@kali)-[/home/mrhacker]
whois etf.bg.ac.rs --help
Usage: whois [OPTION]... OBJECT...
-h HOST, --host HOST connect to server HOST
-p PORT, --port PORT connect to PORT
-I query whois.iana.org and follow its referral
-H hide legal disclaimers
--verbose explain what is being done
--no-recursion disable recursion from registry to registrar servers
--help display this help and exit
--version output version information and exit
These flags are supported by whois.ripe.net and some RIPE-like servers:
-l find the one level less specific match
-L find all levels less specific matches
-m find all one level more specific matches
-M find all levels of more specific matches
-c find the smallest match containing a mnt-irt attribute
-x exact match
-b return brief IP address ranges with abuse contact
-B turn off object filtering (show email addresses)
-G turn off grouping of associated objects
-d return DNS reverse delegation objects too
-i ATTR[,ATTR]... do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]... only look for objects of TYPE
-K only primary keys are returned
-r turn off recursive look-ups for contact information


13:22
root@kali: /home/mrhacker
File Actions Edit View Help
-r turn off recursive look-ups for contact information
-R force to show local copy of the domain object even
if it contains referral
-a also search all the mirrored databases
-s SOURCE[,SOURCE]... search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST find updates from SOURCE from serial FIRST to LAST
-t TYPE request template for object of TYPE
-v TYPE request verbose template for object of TYPE
-q [version|sources|types] query specified server info
(root@kali)-[/home/mrhacker]
whois etf.bg.ac.rs --verbose --verbose
Using server whois.rnids.rs.
Query string: "etf.bg.ac.rs"
% The data in the Whois database are provided by RNIDS
% for information purposes only and to assist persons in obtaining
% information about or related to a domain name registration record.
% Data in the database are created by registrants and we do not guarantee
% their accuracy. We reserve the right to remove access
% for entities abusing the data, without notice.
% All timestamps are given in Serbian local time.
%
Domain name: ac.rs
Domain status: Active https://www.rnids.rs/en/domain-name-status-codes#Active
Domain status: Registry lock https://www.rnids.rs/en/domain-name-status-codes#Registry_lock
Domain status: serverUpdateProhibited https://www.rnids.rs/en/domain-name-status-codes#ServerUpdateProhibited
Registration date: 10.03.2008 12:00:00
Modification date: 01.04.2019 12:07:07
Expiration date: 10.03.2108 12:00:00
Confirmed: 10.03.2008 12:00:00
Registrar: RNIDS
Registrant: RNIDS
Address: Žorža Klemansoa 18a, Beograd, Serbia
Postal Code: 11000
ID Number: 17680544
Tax ID: 104852190
Administrative contact: RCUB - Računski centar Univerziteta u Beogradu
Address: Kumanovska bb, Beograd, Serbia


13:22
root@kali: /home/mrhacker
File Actions Edit View Help
Domain status: Registry lock https://www.rnids.rs/en/domain-name-status-codes#Registry_lock
Domain status: serverUpdateProhibited https://www.rnids.rs/en/domain-name-status-codes#ServerUpdateProhibited
Registration date: 10.03.2008 12:00:00
Modification date: 01.04.2019 12:07:07
Expiration date: 10.03.2108 12:00:00
Confirmed: 10.03.2008 12:00:00
Registrar: RNIDS
Registrant: RNIDS
Address: Žorža Klemansoa 18a, Beograd, Serbia
Postal Code: 11000
ID Number: 17680544
Tax ID: 104852190
Administrative contact: RCUB - Računski centar Univerziteta u Beogradu
Address: Kumanovska bb, Beograd, Serbia
Postal Code:
ID Number:
Tax ID:
Technical contact: RCUB - Računski centar Univerziteta u Beogradu
Address: Kumanovska bb, Beograd, Serbia
Postal Code:
ID Number:
Tax ID:
DNS: odisej.telekom.rs - 195.178.32.2
DNS: ns.rcub.bg.ac.rs - 147.91.1.5
DNS: gaea.rcub.bg.ac.rs - 147.91.1.7
DNS: ns1.uns.ac.rs - 147.91.173.4
DNS: ban.junis.ni.ac.rs - 160.99.1.1
DNS: ns.unic.kg.ac.rs - 147.91.209.2
DNS: ns.etf.bg.ac.rs - 147.91.8.6
DNS: ns2.iif.hu - 193.225.12.59
DNSSEC signed: no
Whois Timestamp: 26.08.2023 09:52:05
(root@kali)-[/home/mrhacker]
#


19:49
root@kali: /home/mrhacker
File Actions Edit View Help
(root@kali)-[/home/mrhacker]
nslookup etf.bg.ac.rs
Server: 172.16.140.2
Address: 172.16.140.2#53
Non-authoritative answer:
Name: etf.bg.ac.rs
Address: 147.91.14.197
(root@kali)-[/home/mrhacker]
nslookup 172.16.140.2
** server can't find 2.140.16.172.in-addr.arpa: NXDOMAIN
(root@kali)-[/home/mrhacker]
nslookup 147.91.14.197
197.14.91.147.in-addr.arpa name = vhost4.etf.bg.ac.rs.
Authoritative answers can be found from:
(root@kali)-[/home/mrhacker]
nslookup -type=soa etf.bg.ac.rs
Server: 172.16.140.2
Address: 172.16.140.2#53
Non-authoritative answer:
etf.bg.ac.rs
origin = NS1.NIC.rs
mail addr = HOSTMASTER.ETF.rs
serial = 2023081400
refresh = 10800
retry = 3600
expire = 2419200
minimum = 86400
Authoritative answers can be found from:
(root@kali)-[/home/mrhacker]
#